

Finalise your new, secure access, via AppConnect

July 2026

Who is this for?

This user guide is intended for all current external application end-users. It will walk you through finalising your AppConnect account including setting up Multi Factor Authentication (MFA).

To access AppConnect, click on this link:
<https://myapps.forms.health.vic.gov.au/>

Introduction & Background



Digital Application Access

DH and DFFH engage external partner organisations and health services to deliver services on behalf of the State. This includes providing shared digital applications that enable secure access to sensitive information

Improving Security

Identity and Access Management (IDAM) is a critical control for protecting this data. DH and DFFH are investing in strengthening this capability through improved tools.

AppConnect, Single Sign-On & Multi-Factor Authentication

As part of this uplist, external access will move to AppConnect, a modern identity and access management solution that uses Microsoft Entra ID, Single Sign On (SSO), and Multi Factor Authentication (MFA).

Migrating to the new access method

Application Owners will work with the project team to validate existing users and support a controlled migration. These changes are required to meet departmental security and compliance standards.

What to Expect?



Application Access – Changes coming...

Depending on the application you're accessing, the experience may be slightly different:

- **CIMS & L17/FVP** will transition from the e-Business Portal.
- Users with access to **HiiP/HiiP** repairs will receive a new login prompt.
- For **VHRA and BOND**, the application URL will be replaced.

Microsoft Account Sign-In

Users sign in with their Microsoft account using their registered email and password for authentication.

Mandatory Multi-Factor Authentication

Users complete MFA via authenticator app or verification code to secure their identity before access. You can use different methods depending on your preference: authenticator code, SMS or call.

Seamless Security Experience

Users with existing MFA setups can reuse methods, enhancing security without added complexity.

Please Note

Depending on your organisational settings and software versions, you may see slightly different screens than those presented in this User Guide.

New User Self-Registration – User Verification



Once off – New User Registration

NOTE: This is only required for users that haven't previously accessed the system or been imported during a transition from e-Business

[Click here](#) to access AppConnect.

1

Conditions of Use Acceptance

Click the box to accept the “I have read , understood and agree to abide by the **Conditions of Use**”

Click on the **Register** button. User Verification page is displayed.

2

User Verification

It's important here to register with your Organisation's email address, not a personal email address

Once you've entered your email address, click **Verify**.

3

Complete Verification

Click **OK** and AppConnect will send an email to validate the email address. Check your email inbox for instructions.

1

The screenshot shows the AppConnect Sign In page. At the top is the Victoria logo and 'AppConnect' text. Below is a 'Sign In' heading. There is a checkbox with a blue checkmark and the text 'I have read, understood and agree to abide by the Conditions of Use.' Below this is a link to 'Help' for instructions. At the bottom are two buttons: 'Sign In' and 'Register'. The 'Register' button is highlighted with a red rectangular box.

2

The screenshot shows the AppConnect User Verification page. At the top is the Victoria logo and 'AppConnect' text. Below is a 'User Verification' heading. There is a text input field labeled 'Email address *'. At the bottom are two buttons: 'Cancel' and 'Verify'. The 'Verify' button is highlighted with a red rectangular box.

3

The screenshot shows the AppConnect Verification Completed page. At the top is the heading 'Verification Completed'. Below is a message: 'Please check your email inbox for instructions.' At the bottom is a blue button labeled 'OK', which is highlighted with a red rectangular box.

Accessing your applications – CIMS & L17/FVP

1

CIMS and L17/FVP

The Client Incident Management System and L17 Family Violence Portal applications are currently accessed via the e-Business Portal.

Once instructed to do so, use the Sign in with Microsoft button. After migration this will become the only login methodology.

2

Accessing applications

The URLs remain the same for now while we migrate to the secure login:

CIMS URL:

<https://cims.ace.webapp.dhs.vic.gov.au/CIMS>

L17/FVP URL:

<https://fvpb.ace.webapp.dhs.vic.gov.au/l17siebel/app/l17/enu?>

On the first login you may be requested to manually enter your email address. Enter your Microsoft login email address and click Next.

3

Signing in with Microsoft

On subsequent logins, Microsoft will know you have an account and will simply ask you to 'Pick an account'

1

Security verification

2

3

Housing applications – HiiP, HiiP Repairs, VHRA & BOND

1

HiiP & HiiP Repairs

Access these applications as you normally would. When you access these via the URLs below and open the application, you'll then be prompted to login with Microsoft authentication.

HiiP URL:

<https://install.hiip.vic.gov.au/hiip/prd/public/32-bit/aad/hiip.application>

HiiP Repairs URL:

https://install.hiip.vic.gov.au/repairs/prd/public/32-bit/aad/hiipclient_aad.application

2

VHRA Agency and Bond Agency

After GO Live, you will need to access these via newly issued URLs. You will receive further communications to notify you when these have been activated. See the new links, shown below:

Bond Agency URL (after go live):

<https://bondloan-agency.housing.vic.gov.au>

VHRA Agency URL (after go live):

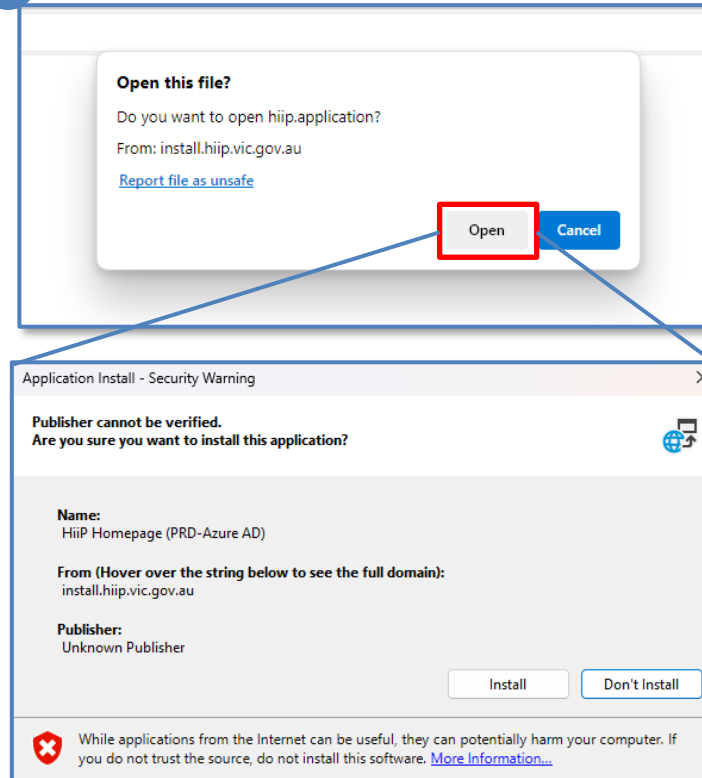
<https://agency.housingapplication.vic.gov.au/>

3

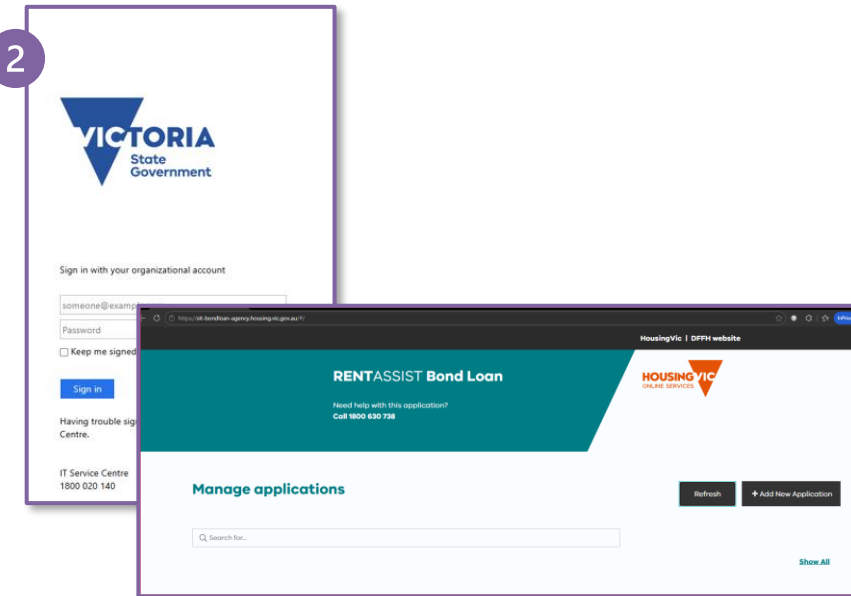
Signing in with Microsoft

On the first login you may be requested to manually enter your email address. However, it's also possible that Microsoft will know you have an account and will simply ask you to 'Pick an account'

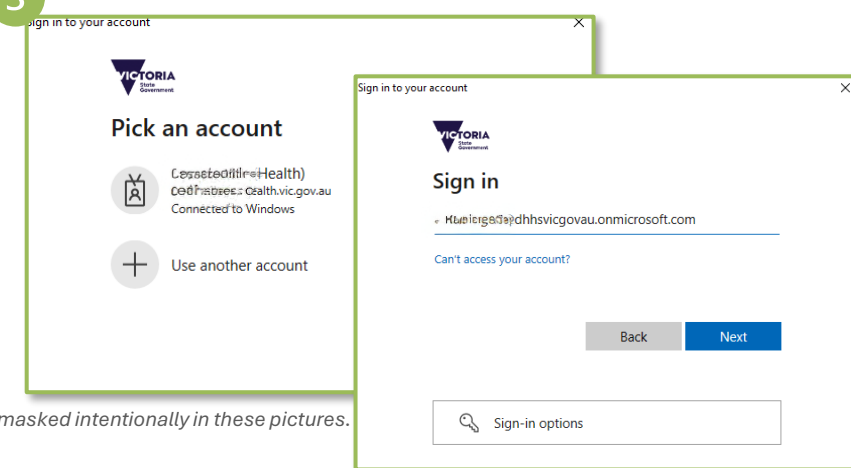
1



2



3



****Note:** Email addresses have been masked intentionally in these pictures.

Setting up Multi-factor Authentication



First sign in

The first time you want to access your application, you'll need to setup multifactor authentication. There will be several screens to advise you of the permissions and security uplift. On the next page we'll show you how to setup Multi-Factor Authentication (MFA)

1

Enter your email address

This should be your organisation email address that you use to access sensitive data.

2

Accept the Permissions request from DFFH, DH Vic

As part of the uplift in securing sensitive data, DFFH and DH Victoria require your permission to setup and receive your profile data, log details of activity.

Click Accept to be able to proceed.

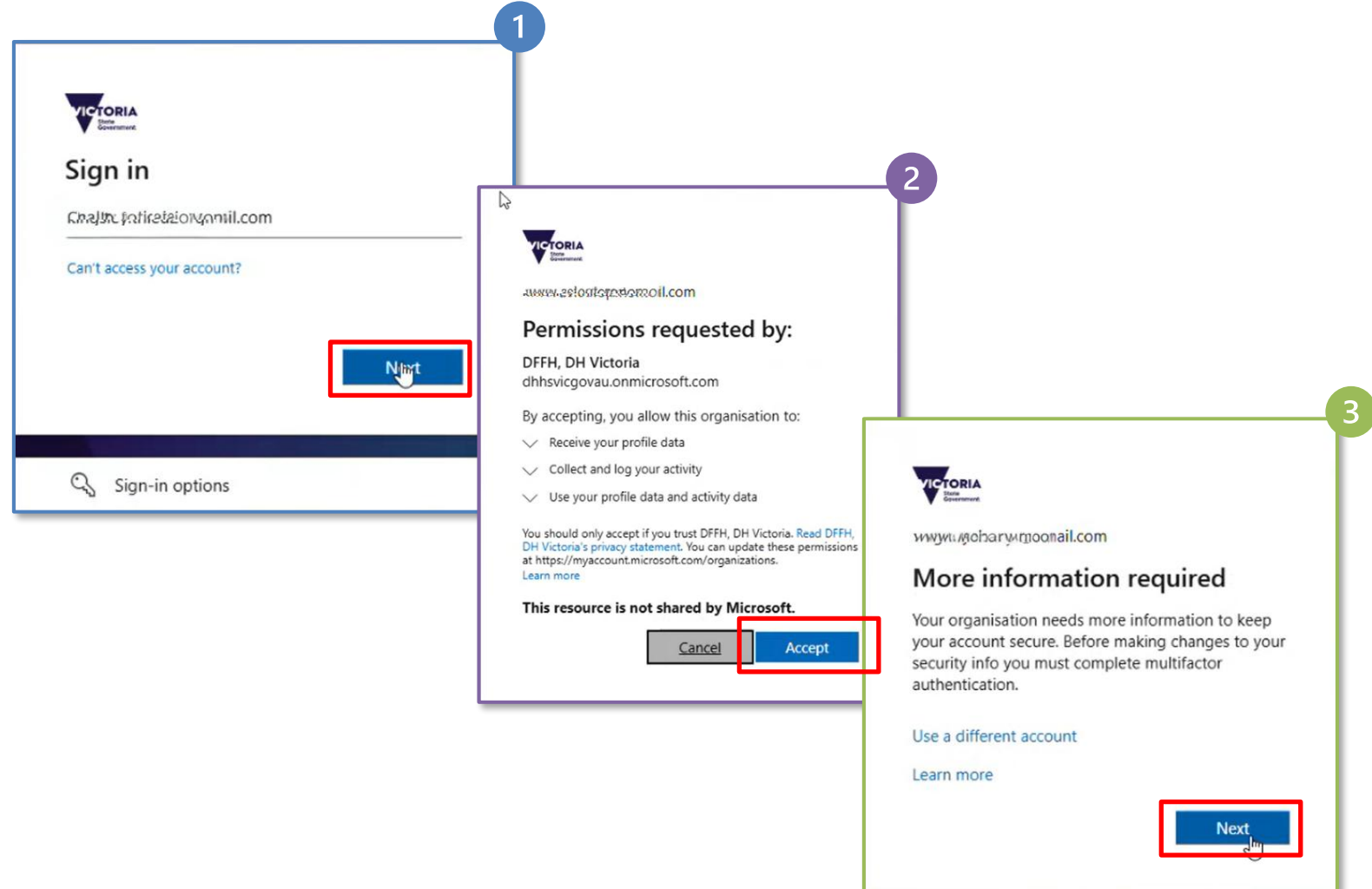
3

More information required.

This screen is to notify you that multi-factor authentication is mandatory as part of the security and protection of the sensitive data you will be accessing.

Select Next to add MFA information

Continued next page...



Setting up Multi-factor Authentication – Using Microsoft Authenticator



Installing the Microsoft Authenticator Application

To setup multifactor authentication via Microsoft Authenticator, you will need to install it on your phone and link it to your organisation email.

While there are several steps, this is a once off install and makes login with MFA easier in the future. Complete the following steps to setup:

1

Download and install Microsoft Authenticator

Using either the App Store or Google Play, download and install the application. Setup the application on your phone using the same email address you entered earlier.

2

Link the phone and your email

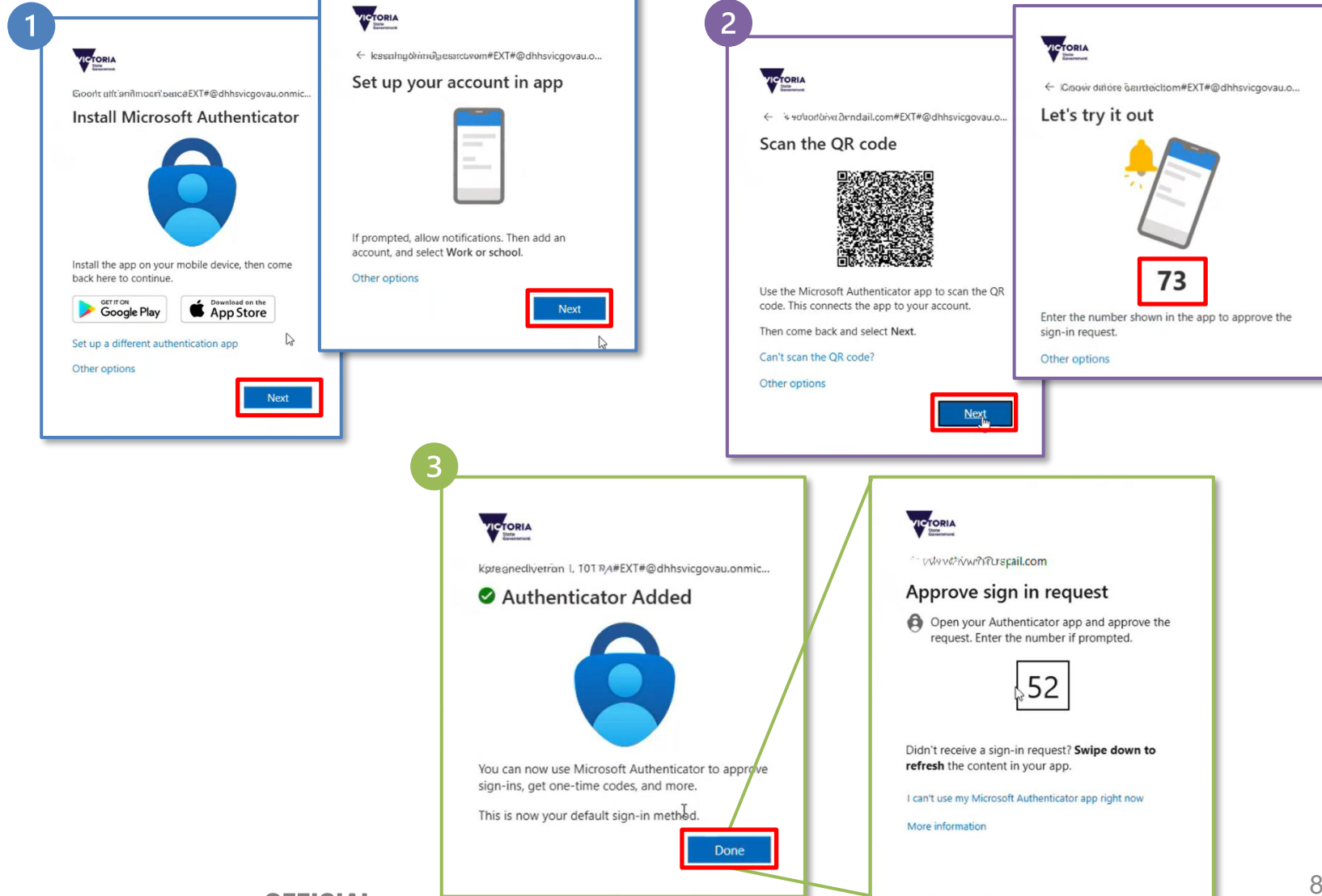
The Microsoft Authenticator app will allow you to scan the QR code on your computer screen to quickly and easily link the device to your email.

You will then be prompted with an initial test to confirm the link is completed. Select or type the number into the Authenticator app as requested.

3

Successful setup and future logins

Great job! You have now successfully linked your Authenticator app for MFA logins! On subsequent logins you will need to open your phone app and select the displayed number to securely log you in.



****Note:** Email addresses have been masked intentionally in these pictures.

Setting up alternative Multi-factor Authentication

1

Setup a different method

Depending on which screen you're presented with, there are alternative methods for MFA. On the Microsoft Authenticator prompt, select:

- "I want to set up a different method"...
- or choose "Other Options"

2

Adding your mobile for SMS or Call authentication

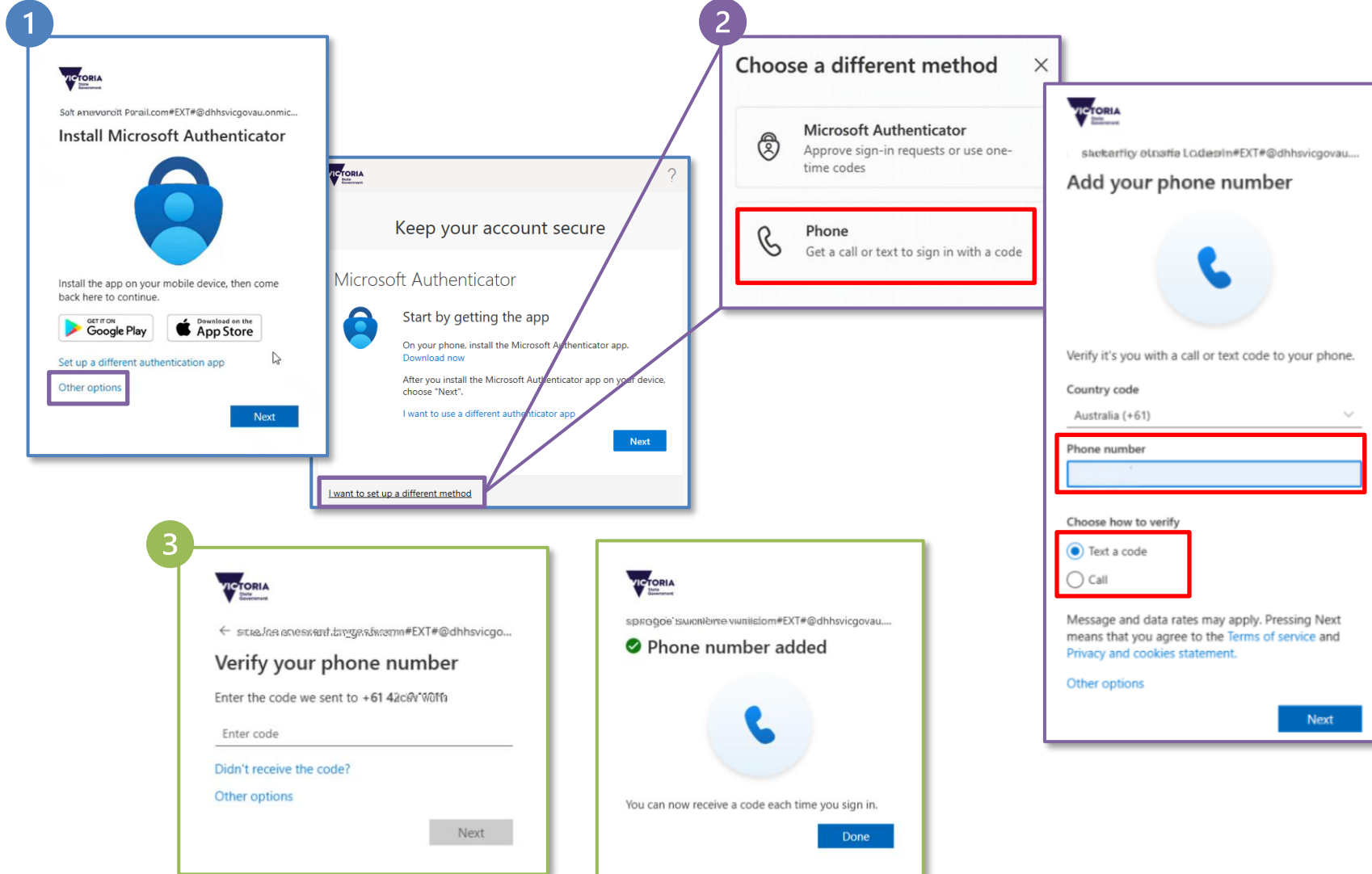
On the Choose a different method prompt, select phone. You'll then be asked to add your mobile phone number. Enter this and then choose whether you want to receive an SMS or a Call where the number will be read out to you.

3

Finalising the setup of your phone

If you selected Text a code, you'll receive a one-time code via SMS. Enter that into the prompt screen and select Next. This screen is similar to what you will receive in the future for MFA.

Once you complete this step, your phone will be linked to your official email account.



****Note:** Email addresses and phone numbers have been masked intentionally in these pictures.

Where do I go for Support?



Before you lodge an IT Support Request...

Depending on the application you are accessing, your support needs will vary. Ensure you have received instruction for your specific application as these are migrating at different timelines. You should only need to setup MFA once, even if you have other applications that you need to access.

Check with your local Org Authority and IT Support

Your Organisation Authority will be able to confirm that you have the required access, and your local IT Support will be familiar with MFA and Microsoft Authenticator applications. They should be your first call.

Support for User Access Issues

If you have any questions about these updates, or you are experiencing technical difficulties:

- For **CIMS**, please email: cims@support.vic.gov.au
- For **L17/FVP**, please email L17portal@dffh.vic.gov.au or telephone 1800 961 690

Please Note

Depending on your organisational settings and software versions, you may see slightly different screens than those presented in this User Guide.