Online Reporting Platform (ORP)

Activate Account

04 JUly 2025

[Activate Account 2](#_Toc200012175)

[Audience 2](#_Toc200012176)

[Email notifications 2](#_Toc200012177)

[Support 2](#_Toc200012178)

[Part 1: Access ORP 3](#_Toc200012179)

[Part 2: Create Account 4](#_Toc200012180)

[Part 3: Setup Multi Factor Authentication 5](#_Toc200012181)

[Appendix A: What is Multi Factor Authentication (MFA)? 7](#_Toc200012182)

[Appendix B: Popular Authenticator Apps 7](#_Toc200012183)

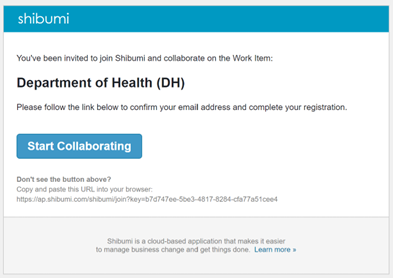
[Appendix C: Obtaining an Authenticator app 7](#_Toc200012184)

[Appendix D: Changing Devices and/or Authenticator apps 7](#_Toc200012185)

# Activate Account

This guide demonstrates how to activate a new account upon receiving an email to confirm your email and complete your registration.

Following assignment of your first Role in the Online Reporting Platform (ORP), you will receive an invitation including a link to register via email:



If you have an active account see user guide: Log In to ORP.

## Audience

All users

## Email notifications

You may receive email notifications from Shibumi related to this process. To avoid missing communications flag Shibumi as a trusted sender in your email application.

## Support

If you have not received an email to confirm your email address and register, email [gateway.helpdesk@dtf.vic.gov.au](mailto:gateway.helpdesk@dtf.vic.gov.au).

## Part 1: Access ORP

|  |  |
| --- | --- |
| Step | What to Do |
|  | Follow emailed link. |
|  | Which screen do you see?   |  |  | | --- | --- | | **Login** | Screenshot of Login screen. Left side bar displaying email address field and Next button. Right of screen Shibumi marketing text and sampled software image depicting a generic screen layout showcasing header, tabs, buttons, data tables and charts.  You’re a VPS user accessing ORP via a recognised network. You’ll be automatically authenticated via Single Sign-On during log in.  See User Guide **Log in to ORP** | | **Create Account** | Screenshot of Create Account screen. Left side bar displaying First name, last name, password, confirm password fields and Create Account button. Right of screen Shibumi marketing text and sampled software images depicting a generic screens layout showcasing a risk matrix and data table.  You’re unable to access ORP via Single Sign-On and must establish Multi Factor Authentication to access ORP.  Proceed to **Part 2. Create External User Account** | |

## Part 2: Create Account

**Pre-requisites:**

* **Part 1. Access ORP** complete
* **Create Account** screen displayed

|  |  |
| --- | --- |
| Step | What to Do |
|  | Type First Name, Last Name, Password in respective fields. |
| Information outline | To show/hide password click eye icon. |
| Information outline | First Name, Last Name, and Password may be administered under My Account at any time. |
|  | Click: **Create Account**  **Setup Multi Factor Authentication** **(MFA)** screen displays:  Screenshot displaying Multi Factor Authentication (MFA) Setup dialog box center of grey screen, and Privacy dialog box bottom right of screen.   The MFA dialog box displays image of black padlock, message “Multi-Factor Authentication is required to access this data Configure MFA to continue“. Below left being link text to Go Back, and right link text to Set Up MFA.   The Privacy dialog box displays message “We value your privacy. This website only stores cookies on your browser that are categorized as "Necessary" as they are essential to the functionality of the application. These cookies do not track users or store any personally identifiable information.” Below left being link text to View Necessary Cookies, and right link text to Accept. |
|  | Proceed to **Part 3. Set up Multi-Factor Authentication**. |

## Part 3: Setup Multi Factor Authentication

**Pre-requisites**

* **Part 2. Create External User Account** complete
* **Setup Multi Factor Authentication (MFA)** screen displayed (see Part 2, step 2)

|  |  |
| --- | --- |
| Step | What to Do |
|  | Click: **Set Up MFA**  **Set up Multi-Factor Authentication** screen displays:  **Screenshot of Set up Multi-Factor Authentication dialog box. Displays three steps to be followed.   Step 1 states “Install an authenticator app for iOS or Android.”   Step 2 states “In the app, add an account and scan the following image below.” Below which is a QR code.   Step 3 states “If the app displays a six-digit code, enter it here and click Validate.”  Below steps is a field ‘6 digit code from verifier app’, below which is two link text buttons. On left Cancel, on right Validate.** |
|  | Do you have an existing Multi Factor Authentication (MFA) application on a personal device?   |  |  | | --- | --- | | **Yes** | Go to next step. | | **No** | Review and action:   * Appendix A: What is Multi Factor Authentication (MFA) * Appendix B: Popular Authenticator Apps * Appendix C: Obtaining an Authenticator app | |
|  | Open your Multi Factor Authentication application (MFA app) on your personal device. |
|  | Using your MFA app, scan **QR Code** displayed on screen. |
|  | In field: **3. If the app displays a six-digit code, enter it here**, type current **Token**. |
| Information outline | **Shibumi Authentication** **Token** **(Token)**  An authentication token named Shibumi should be automatically added to your MFA application. The token is a six-digit codes that changes every 60 seconds. The current token will be requested each time you login.  Deleting or losing access to this token will mean you cannot login to ORP and require your MFA to be reset by the Gateway Unit.  Should you need to change the authentication app you use, see user guide: Re-Configure Multi Factor Authentication before decommissioning your old device or authentication application. |
|  | Click: **Validate**  **Log In** screen displays:  **Screenshot of Login screen. Left side bar displaying email address field and Next button. Right of screen Shibumi marketing text and sampled software image depicting a generic screen layout showcasing header, tabs, buttons, data tables and charts.** |
| Information outline | **Your account has been registered and activated**  For assistance logging in, see user Guide: **Log in to ORP** |

## Appendix A: What is Multi Factor Authentication (MFA)?

Multi-factor authentication (MFA) is a security measure that requires two or more methods of verification to access an account, making it harder for unauthorized individuals to gain access.

**Access to ORP requires Two-step Verification**

After installing an Authenticator App on your mobile device and connecting it with ORP, you’ll be required to provide your current MFA Code each time you log in.

These codes change every 60 seconds.

## Appendix B: Popular Authenticator Apps

Google Authenticator and Microsoft Authenticator are the most commonly used MFA applications. However, all MFA applications compatible with your device will be available for download on Google Play Store for Android and App Store for iOS.

## Appendix C: Obtaining an Authenticator app

To obtain an authenticator app, you'll need to download one from your device's app store.

**Steps to Download and Install:**

1. Open your device's app store: On Android, it's the Google Play Store, and on iOS, it's the App Store.
2. Search for the app: E.g., Type "Google Authenticator" or "Microsoft Authenticator" or “Multi Factor Authentication” into the search bar.
3. Select an app: Find the app from the search results and select it.
4. Install the app: Follow the app store's instructions to download and install the app on your device.
5. Open the app: Once installed, open the authenticator app to start setting up your accounts.

## Appendix D: Changing Devices and/or Authenticator apps

See user guide: Re-Configure Multi Factor Authentication