Online Reporting Platform (ORP)

Re-Configure Multi Factor Authentication (MFA)

04 JULY 2025

[Re-Configure Multi Factor Authentication (MFA) 1](#_Toc200017950)

[Audience 1](#_Toc200017951)

[Email notifications 1](#_Toc200017952)

[Support 1](#_Toc200017953)

[Steps 2](#_Toc200017954)

[Appendix A: What is Multi Factor Authentication (MFA)? 6](#_Toc200017955)

[Appendix B: Popular Authenticator Apps 6](#_Toc200017956)

[Appendix C: Obtaining an Authenticator app 6](#_Toc200017957)

# Re-Configure Multi Factor Authentication (MFA)

This guide demonstrates how to disable and re-configure Multi Factor Authentication on your ORP Account.

Note: This guide does not apply to Victorian Public Sector users accessing ORP through a VPS email address that is authenticated using Single Sign-On (SSO).

There are three events that would result in a user needing to change the MFA configuration they use to access ORP:

1. You’ve obtained a new device and are unbale to port your MFA app and its data from your old device.
2. You wish to change the authenticator app you are using.
3. You lost access to your device or MFA application.

Events (1) and (2) are covered by this guide and can be performed by you as you still have access to your existing MFA app and it’s data.

Event (3) requires your ORP account’s MFA to be reset by the Gateway Unit and ORP Administrators. Please contact Support.

## Audience

All users authenticating via MFA.

## 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

For support email [gateway.helpdesk@dtf.vic.gov.au](mailto:gateway.helpdesk@dtf.vic.gov.au).

## Steps

|  |  |
| --- | --- |
| Step | What to Do |
|  | Login to **ORP**.  **Home Page** displays:  A screenshot of a computer  AI-generated content may be incorrect. |
| Information outline | **Home Page**  Access to the home page is managed by the Gateway Unit. If you do not see a screen similar to above contact a Gateway Unit Analyst.  Information displayed is unique to your Role, and what Projects and Gates you’re assigned to. |
| Information outline | **Show/Hide Left Navigation Menu**  Click hamburger menu top left of screen to show/hide left navigation menu. |
|  | In left navigation menu, click: **My Account**  **My Account** menu displays:  Screenshot of Left Navigation menu, My Account sub menu. Displays name of user logged in, under which three options are presented: link to My Account, link to Enterprise Administration, link to Sign Out. Note: Enterprise Administration option only displays for System Administrators. |
|  | Click: **My Account**  **My Account** screen displays:  Screenshot of My Account screen.   Displays seven panels.   Avatar, which displays uploaded photo and buttons to delete or upload new photo.   General, which displays First Name, Last Name field and Save button (for changes).   Multi Factor Authentication, which advises and manages login authentication method.   Change Password, which displays Old Password field, New Password field, Confirm password field, and Update button.   Homepage, displays Select a homepage field and Save button.  Export Settings, which displays Column Separator field, Decimal Separator field, and Save button.  Scheduled Exports, which displays text “You have no exports scheduled.” |
|  | In panel **Multi-Factor Authentication**, click: **Disable MFA**  Confirmation message displays:  Are you sure you want to disable Multi-Factor Authentication dialog box. Offers two options. Left, link text “Cancel”. Right, link text “Disable MFA”. |
|  | Click: **Disable MFA** |
| Information outline | Note: If you log out before re-configuring MFA you will be forced to re-configure it before your next log in. |
|  | Click: **Configure MFA**  **Setup 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/use an existing Multi Factor Authentication (MFA) application?   |  |  | | --- | --- | | **Yes** | Go to next step. | | **No** | Read 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 (MFA) application. |
|  | Scan QR Code displayed on screen.  An authentication token named Shibumi should be automatically added to your application. |
|  | Type current token code into field: **3. If the app displays a six-digit code, enter it here**. |
|  | Click: **Validate**  Green confirmation message displays and new MFA token enabled.  Screenshot of My Account screen with  confirmation message "Multi Factor Authentication Configured" displayed on green background at bottom right of screen. |

## 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 most common, and are 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: Type "Google Authenticator" or "Microsoft Authenticator" into the search bar.
3. Select the 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.