



Passwordstate Browser Extension Manual

Table of Contents

Foreword	0
Part I Browser Extension Manual	3
Part II Prerequisites	3
Part III Installation	5
Part IV Browser Extension Usage	11
Part V Web Authentication Passkeys	32
Part VI Browser Extension Settings	34
Part VII Detection and Advanced Functionality	36

1 Browser Extension Manual




Welcome to the Passwordstate Browser Extension Manual.

The Click Studios Browser Extensions for Passwordstate enables the secure storing of website credentials in your Passwordstate instance. These credentials can then be used to automatically form-fill the credential input fields, such as the username and password fields, when you next visit that sites URL (Uniform Resource Locator) or web address.

The Browser Extensions are currently available for all Chromium based browsers, including Google Chrome, Microsoft Edge, the Brave Browser and Mozilla's Firefox.

The following table summarizes each of the key areas for configuring and using our Passwordstate Browser Extensions.

 Note: Our Browser Extensions require you to have cookies enabled in your browser

Prerequisites	How to configure Passwordstate ready to save credentials
Installation	How to install the Browser Extension, and configure for use
Browser Extension Settings	Explains the various settings for the Browser Extension
Browser Extension Usage	Provides instructions for basic usage of the Browser Extension for Chromium based browsers and Firefox
Web Authentication Passkeys	Instructions for using Passkeys with web sites and Passwordstate
Detection and Advanced Functionality	Provides guidance on issues with certain web sites not prompting to save login credentials

2 Prerequisites

In order to use our Browser Extensions, you'll need to have the following:

1. A supported Web Browser. The Passwordstate Browser Extensions are available for all Chromium based browsers, including Google Chrome, Microsoft Edge, the Brave Browser and Mozilla's Firefox,

2. An installation of Passwordstate, on a host matching our webserver requirements <https://www.clickstudios.com.au/passwordstate-system-requirements.aspx>, that you can log into, and,
3. One or more Password Lists in Passwordstate, that have the URL field enabled.

To create a new Password List with the URL field enabled, create a new **Private** or **Shared** Password List based on the **Web Site Logins** Template:

Passwordstate V9.5 (Build 9577)

Search Passwords or Hosts ...

PASSWORDS HOSTS ADMINISTRATION

Passwords

Passwords Home

Add Folder

Add Private Password List

Add Shared Password List

Administer Bulk Permissions

Expiring Passwords Calendar

Password List Templates

Pending Access Requests

Request Access to Passwords

Toggle All Password List Visibility

Add Private Password List Wizard

To create your Private Password List, please specify details below and select the type of Password List you would like based off the available Templates.

Password List Details Confirmation

Site Location: Internal

Password List: * Personal Website Logins

Description:

Template: Web Site Logins

Image: website.png

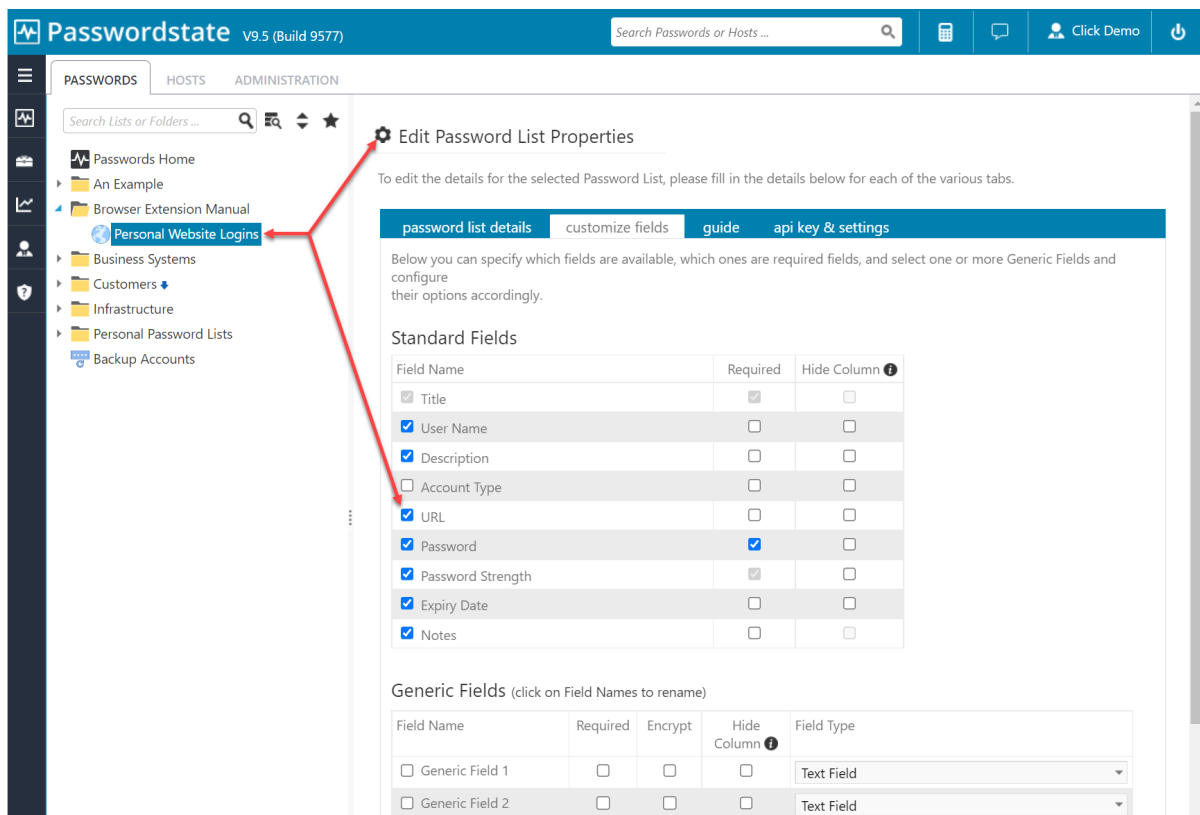
Template Description: Store web site logins, which can also be used with Browser Extensions feature

☐ Link this Password List to the selected Template. ☐ Disable future use of this Wizard

Cancel Next


Note: Additional settings can be changed after the Password List has been created.


Alternatively, you can edit an existing Password List and enable the **URL** field under the **customize fields** tab:




3 Installation

Please follow these steps for installing and configuring our Browser Extension. The majority of the screenshots provided in this manual have been taken using the Brave Browser with the Browser Extension obtained from the Chrome Web Store. The screenshots for Chrome, Edge and Firefox look similar to those of the Brave Browser.

 **Note 1:** In order to use one of the Browser Extensions, to save and automatically form-fill credentials for websites, you must have access to one or more Password Lists configured to use the 'URL' field.

 **Note 2:** Our extensions support websites with multiple login fields, not just the typical username and password input fields. A total of 13 input fields can be catered for by using the **Username**, **Password**, **OTP** (enabled at the Password List Level) and up to 10 **Generic Fields**.

 **Note 3:** Click Studios does not provide a Browser Extension for the Apple Safari browser. We recommend using Chrome on Apple MACs as a work around if required.

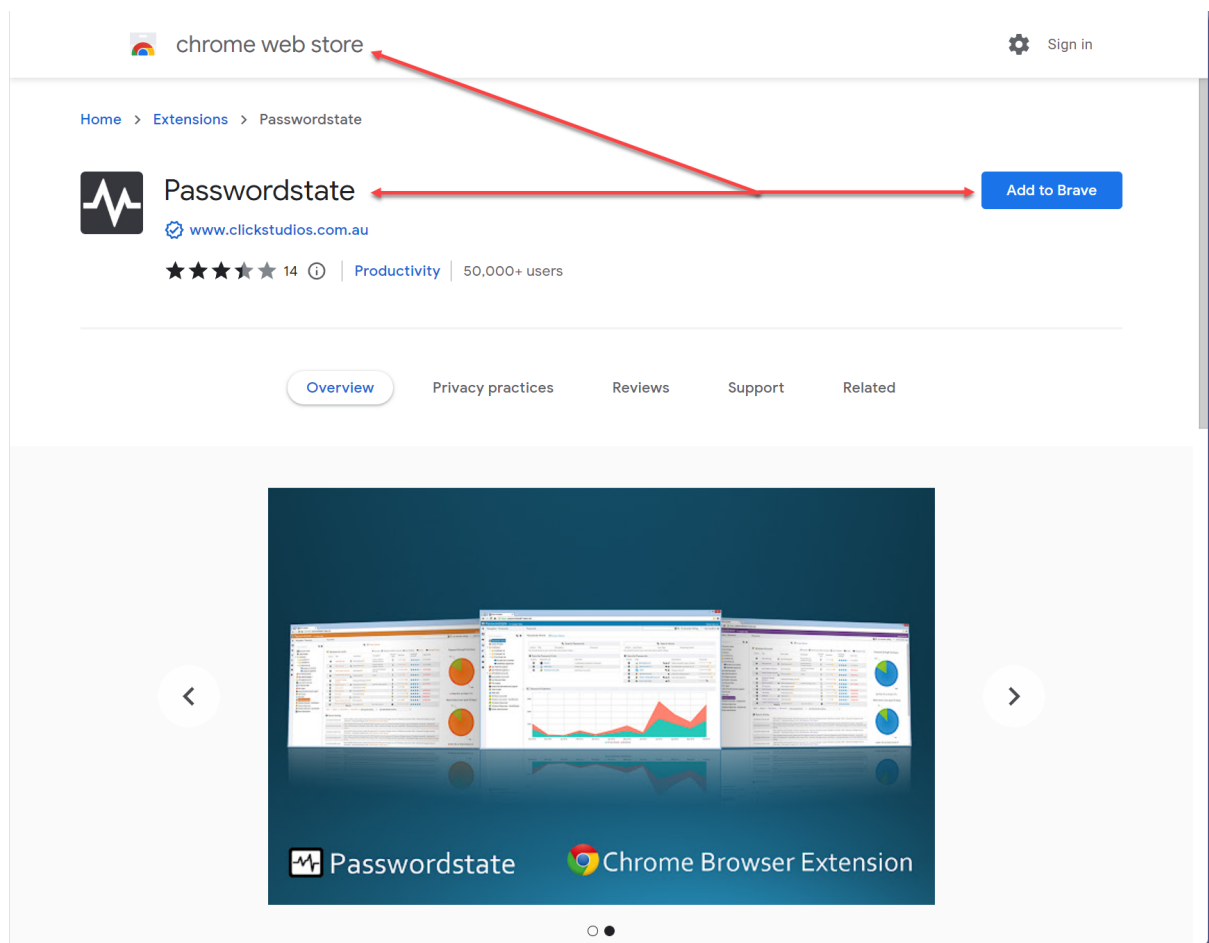
Brave Installation

1. Visit the Google Chrome Web Store URL <https://chrome.google.com/webstore/category/extensions> and search for the extension name **Passwordstate**.

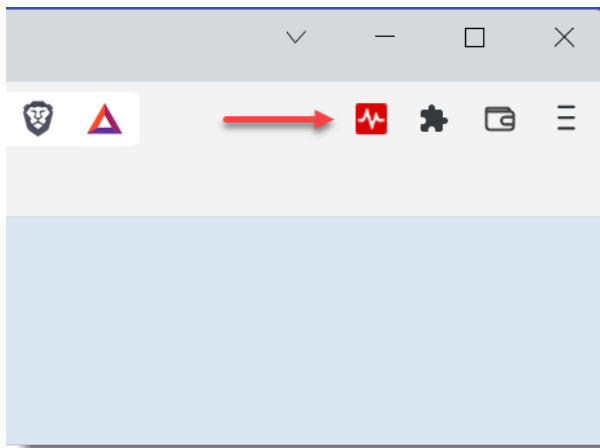
Alternatively, you can download it directly from

<https://chrome.google.com/webstore/detail/passwordstate/appojfilnpgkhkebigcdkmopdfcjhim>

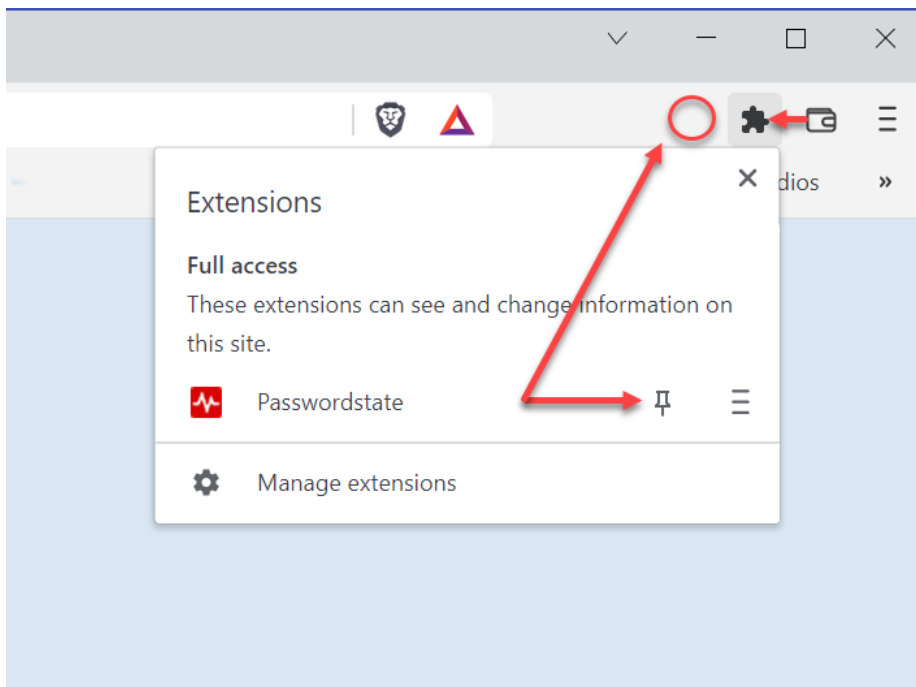
2. Click the **Add to Brave** button to install the extension, then click the **Add Extension** button



3. Once installed, you should see the Passwordstate icon in the top toolbar



4. If you don't see the Passwordstate extension, click on the **Extensions** button and pin the extension as per the screen shot below:



Chrome Installation

1. Visit the Google Chrome Web Store URL <https://chrome.google.com/webstore/category/extensions> and search for the extension name **Passwordstate**.

Alternatively, you can download it directly from

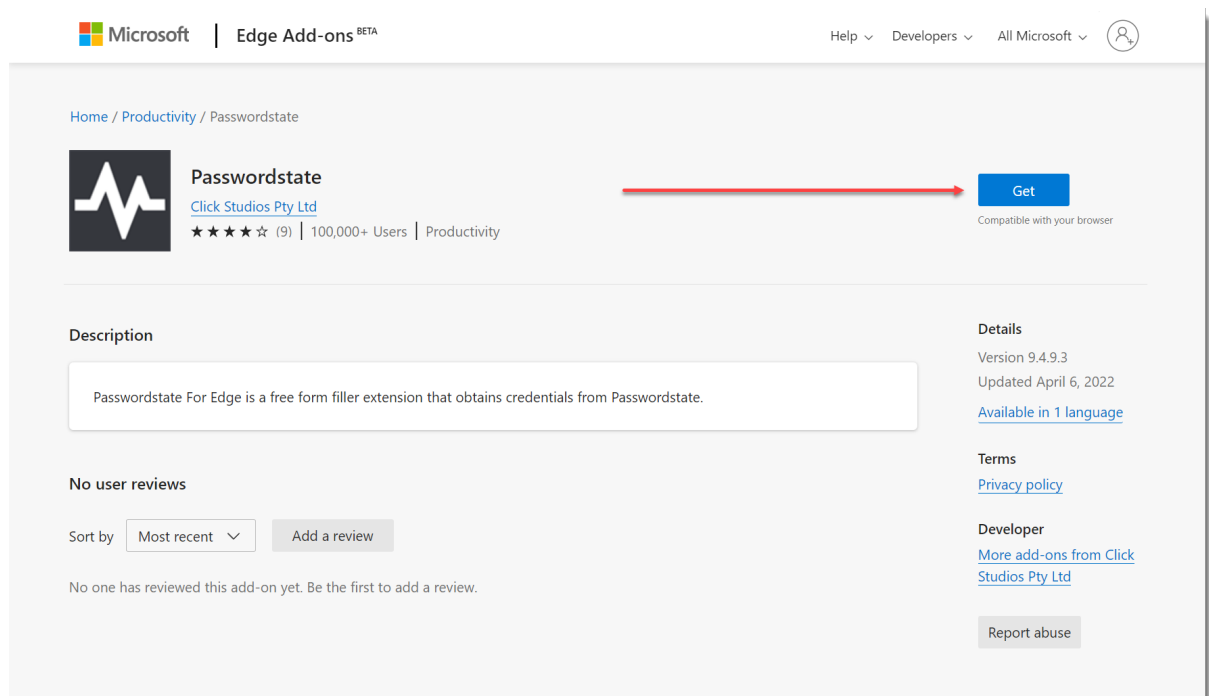
<https://chrome.google.com/webstore/detail/passwordstate/appojfilknpgkhkebigcdkmopdfcjhim>

2. Click the **Add to Chrome** button to install the extension, and click the **Add Extension** button. The images for this will appear very similar to those for the Brave installation in the section above.
3. Once installed, you should see the Passwordstate icon in the top toolbar.
4. If you don't see the Passwordstate extension, click on the **Extensions** button and pin the extension as per the Brave Installation image.

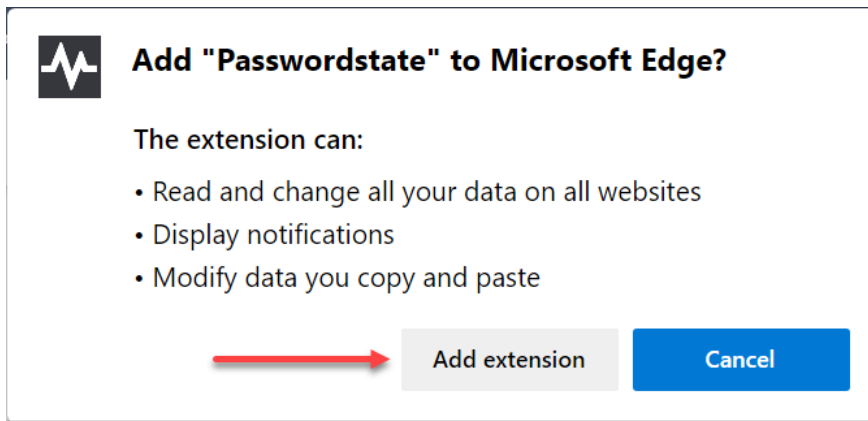
Edge Installation

1. Open Microsoft Edge and browse to

<https://microsoftedge.microsoft.com/addons/detail/passwordstate/pbbamlchainnpdodbeobfpgcpffpclka?hl=en-US> and click the **Get** button:



2. Click the **Add extension** button:



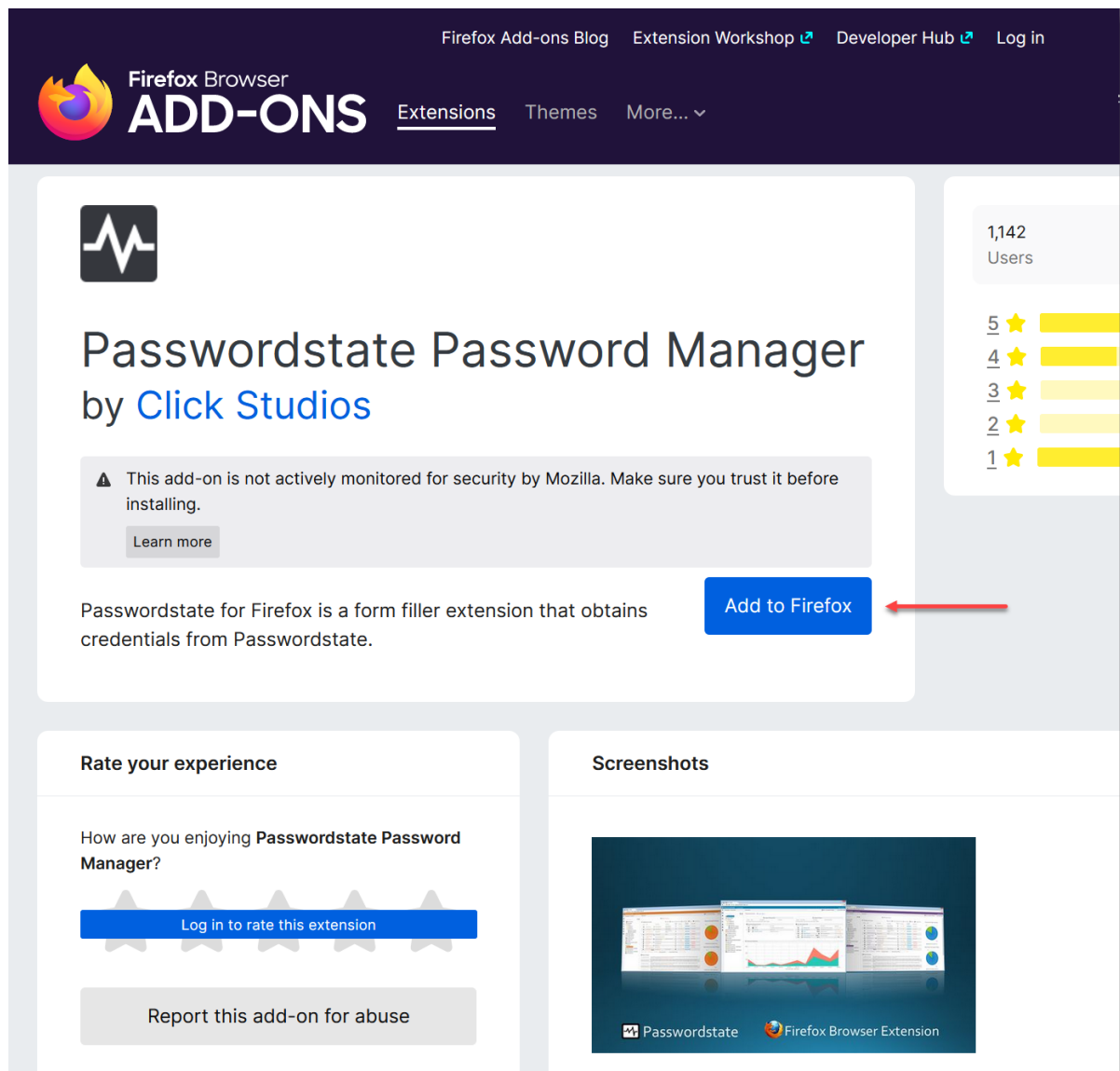
3. Once installed, you should see the Passwordstate icon in the top toolbar Similar to the Brave installation image.

Firefox Installation

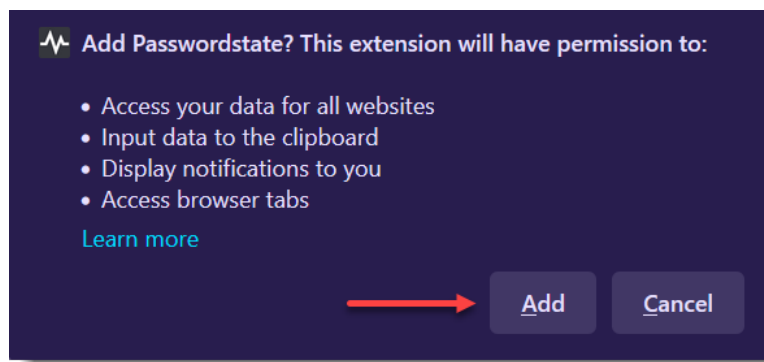
1. Visit the Mozilla Add-ons store URL <https://addons.mozilla.org/en-US/firefox/> and search for the extension name **Passwordstate**.

Alternatively, you can download it directly from <https://addons.mozilla.org/en-US/firefox/addon/passwordstate-password-manager/>

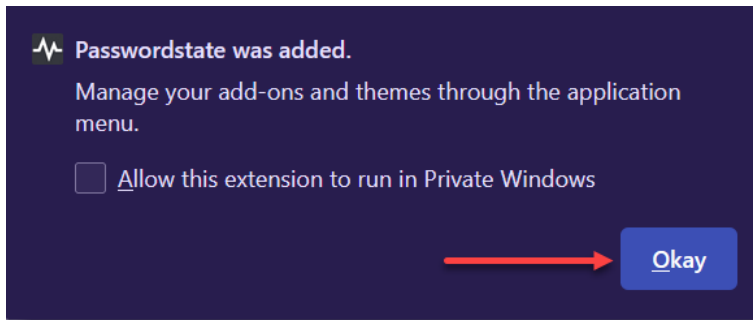
2. Click the **Add to Firefox** button



3. Click the **Add** button



4. Once installed, you should see the Passwordstate icon in the top toolbar similar to the Brave installation. You may also receive the following prompt



Simply click **Okay** to close this prompt.

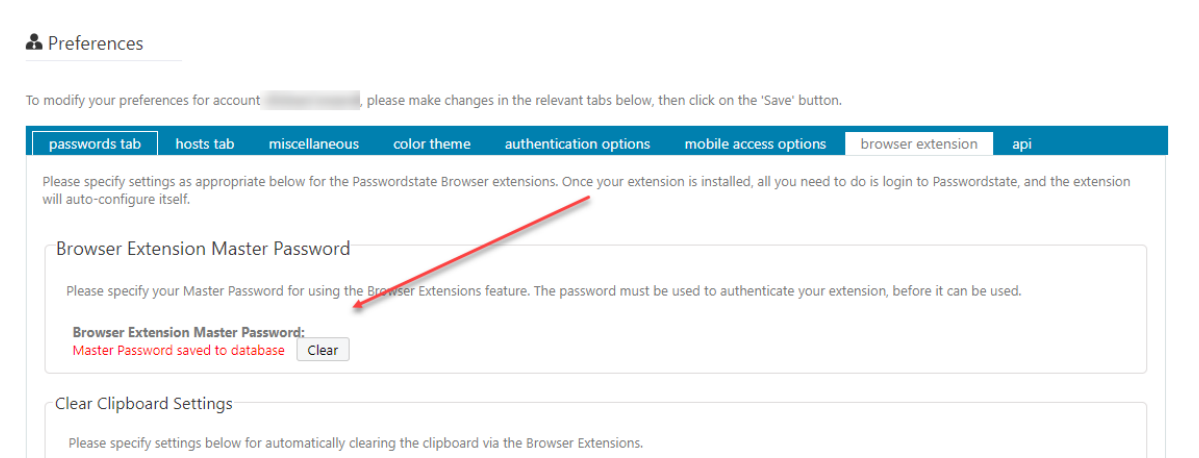
Your extension is now ready to configure for the first time, and more information about this can be found in the [Browser Extension Usage](#) section of this manual.

4 Browser Extension Usage

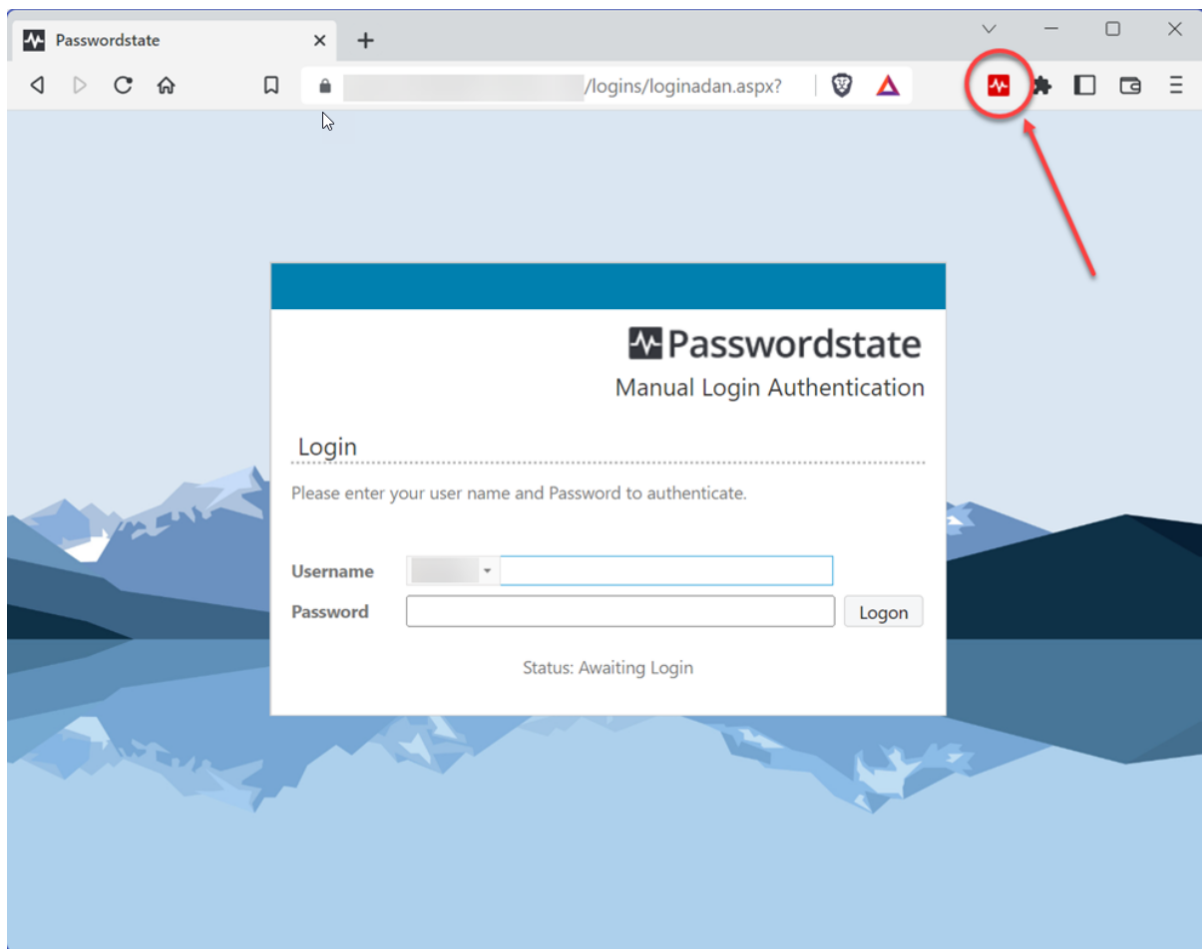
This section of the manual applies to our Chromium based browsers and Firefox Extensions.

Configuring the Browser Extension

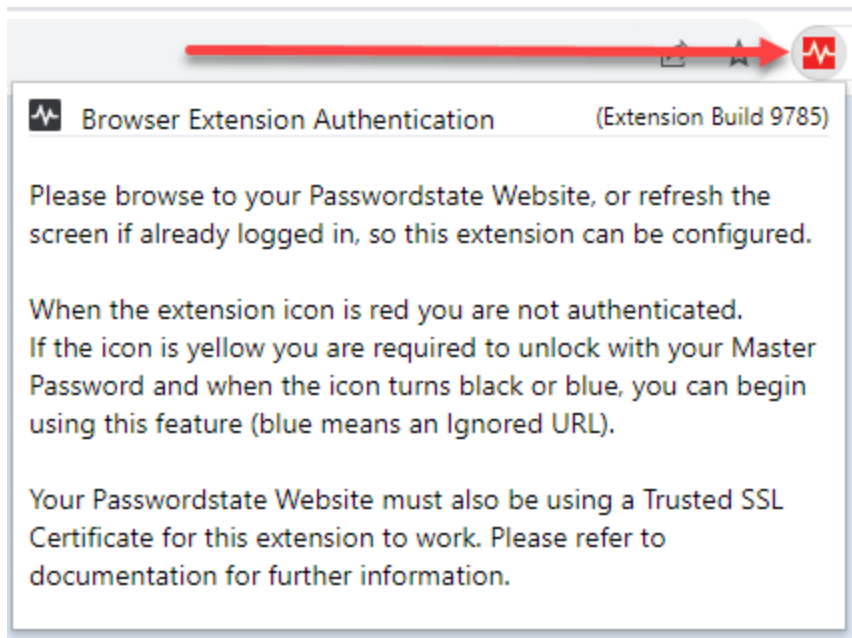
Prior to using the browser extensions, you must go to your Preferences screen, and specify a Master Password to be used for authentication.



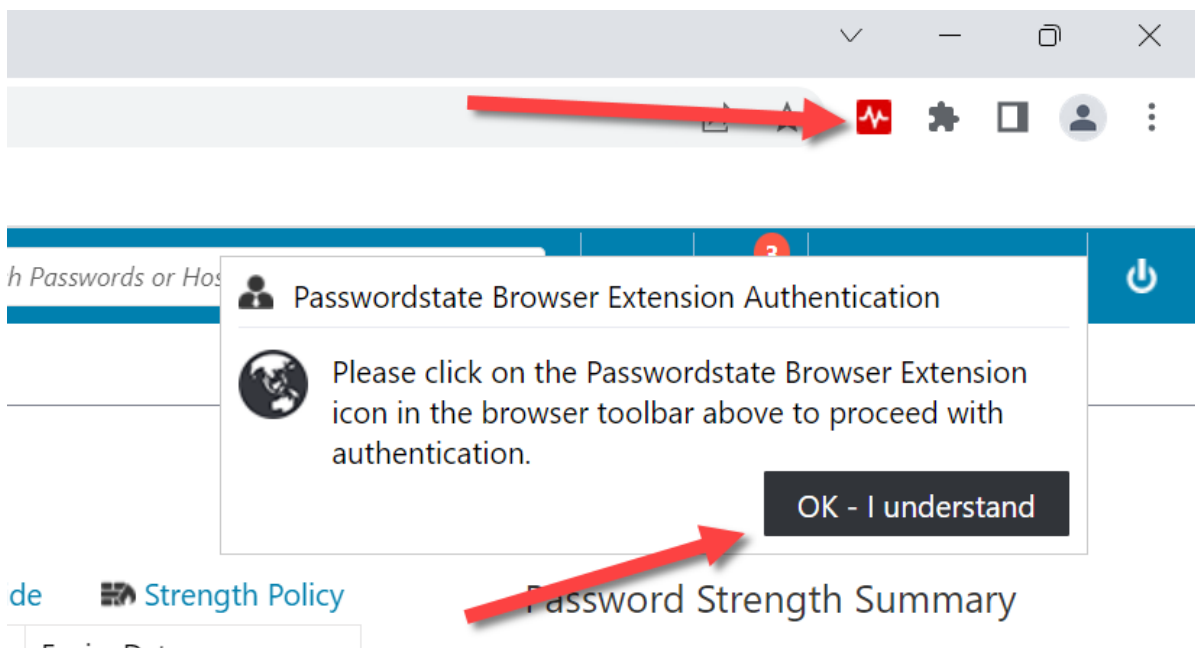
When your Browser Extension is first installed its icon will show as **red**, indicating it is not currently configured and syncing with your Passwordstate instance. Note, it will also show as **red** if your Browser Extension is currently logged out.



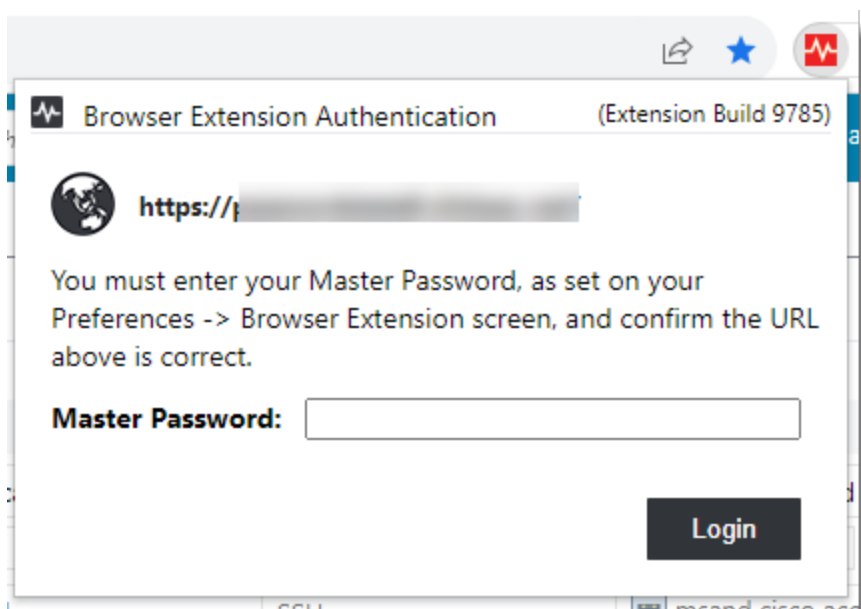
If you click on your extension, you will see a message advising that you need to browse to your Passwordstate website which will initiate the connection process:




To connect your extension to your Passwordstate instance, first browse to your Passwordstate URL, and log in. You will receive a message asking you to click on the Passwordstate browser extension. Click the **"OK - I Understand"** button, and then click on the **red** Extension icon:



You will then be presented with a pop up asking to confirm the URL is correct, and to enter your Master Password. Please ensure this is the URL you use to log into Passwordstate with every day, specify your Master Password, then click on the **"Login"** button to finish the connection process:





The Browser Extension will now connect to your Passwordstate instance and authenticate using the credentials you logged in with. Your Browser Extension icon will now turn **blue**.


 **Note:** You are asked to confirm the Passwordstate website URL is correct as mitigation against a phishing style attack, where you could be asked to click on a link to login to an imitation of your Passwordstate environment. If you believe the URL is suspicious in anyway, report this to your Passwordstate Security Administrators.


ICON Status

Our Browser Extensions use different colors as a quick visual indicator or status of the Browser Extension. The 4 different colors and their meanings are,

 This indicates the Browser Extension is active and authenticated to your Passwordstate instance. It also indicates the URL on the active tab in your browser is set to be ignored by the Browser Extension. Ignored URLs will not automatically form-fill existing, or prompt to save new, credentials for that website. By default, your Passwordstate URL is an Ignored URL.

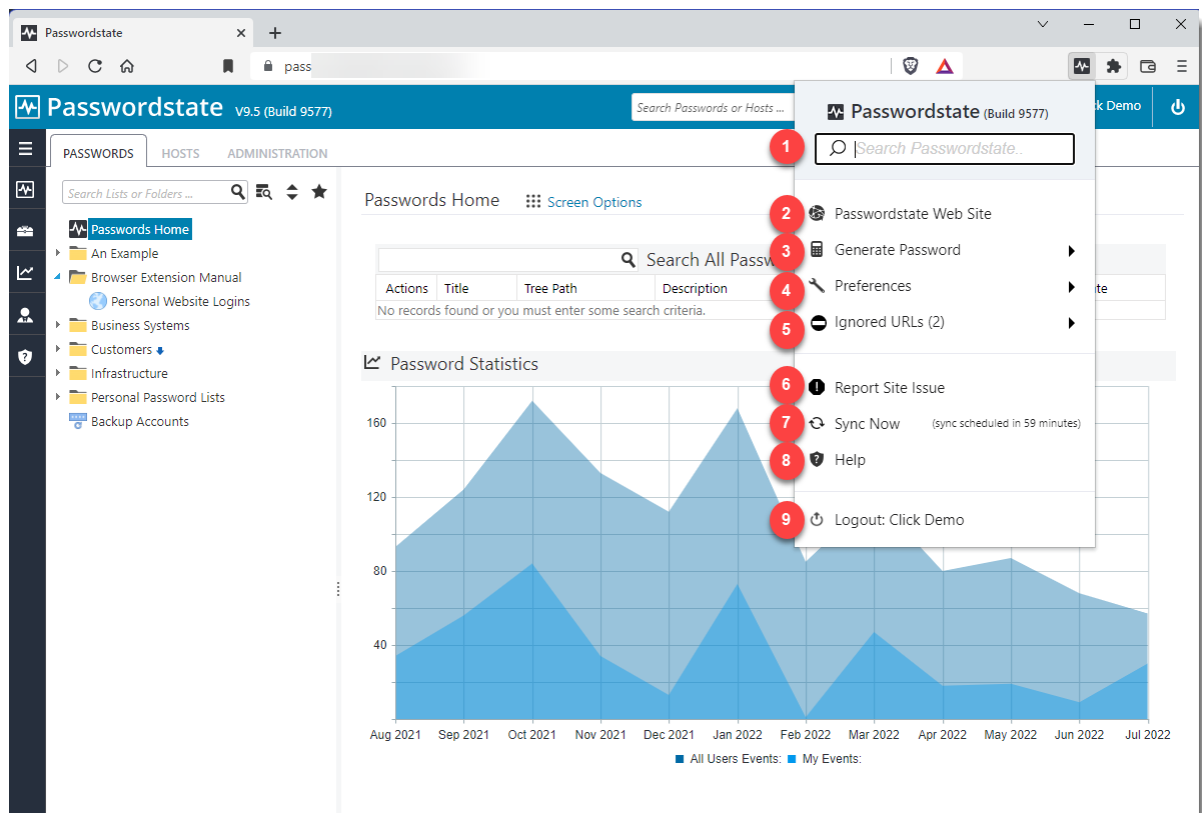
 This indicates the Browser Extension is active and authenticated to your Passwordstate instance. When the icon is **black** you are able to automatically form-fill any saved credentials for a website. You will also be prompted to save any new credentials you enter while on a website. These credentials are saved to your Passwordstate instance that you are authenticated against.

 This indicates the Browser Extension is not active. It is either logged out of your Passwordstate Instance, or requires the initial configuration to point to the correct Passwordstate instance's base URL. In both cases, simply browse to your Passwordstate website login URL and login as normal. This will authenticate the user if they are logged out, or prompt to confirm the URL presented is the same as your Passwordstate instance's base URL.

 Your browser extension is in a "locked" state, and you will need to unlock it using your Master Password.

User Interface

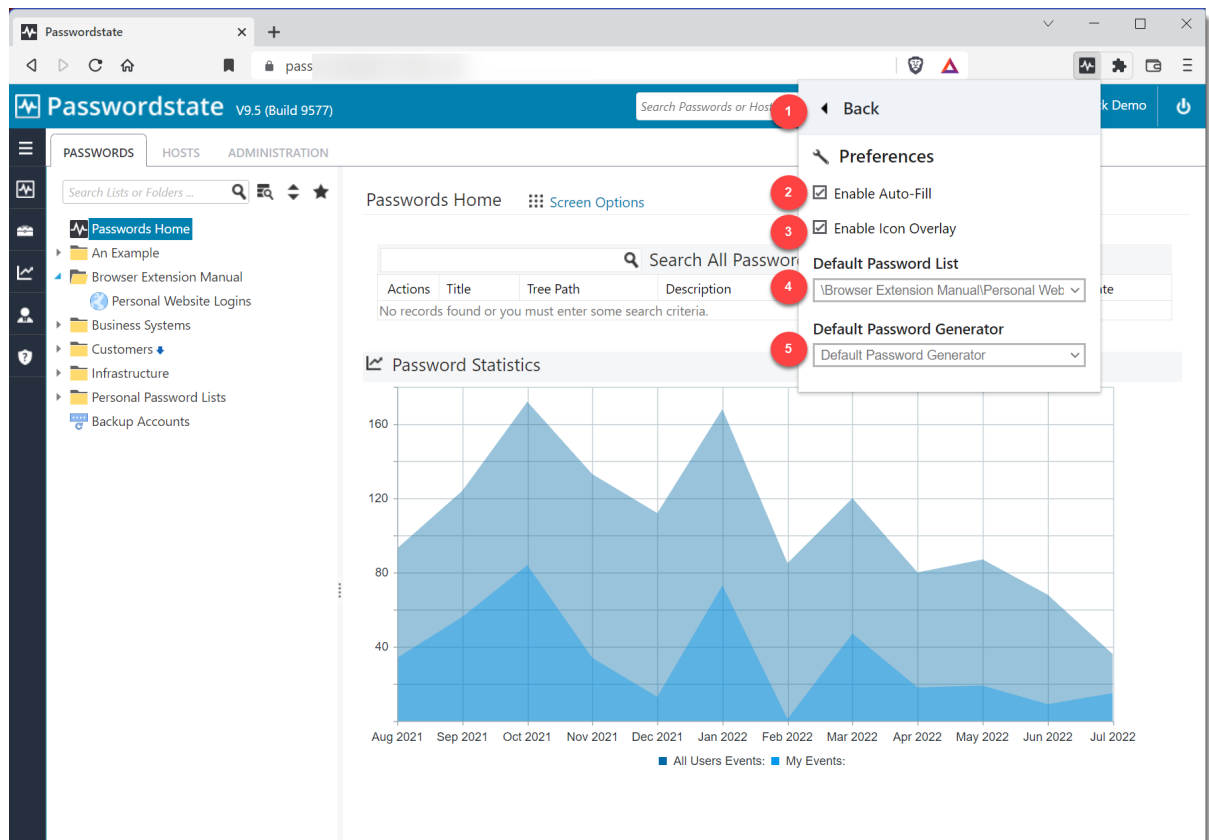
The Browser Extension interface provides a range of features and options. The following image is taken using the Brave browser, with the Browser Extension loaded from the Google Chrome Web Store.



1. A **Search** box, which can be used to quickly search for website credentials across all Password Lists you have been granted access to
2. A link directly to your **Passwordstate website**
3. **Generate Password**, by clicking this you can generate random passwords with different complexities. This is highly recommended when creating new passwords for a website
4. **Preferences** - more about this is explained below
5. **Ignored URLs** – again, more information is provided later in this manual
6. **Report Site Issue**, If the browser extension is not automatically form-filling a website, or does not capture the log in credentials correctly for you, you can use this to report it directly to **Click Studios** for testing
7. **Sync Now**, which allows you to immediately resynchronize your Browser Extension and pickup any changes made to permissions and credentials within Passwordstate
8. A link to open the Browser Extension **Help** Manual
9. **Logout** button, used to disconnect your extension from your account in Passwordstate

Preferences

On the Preferences screen you have five options:

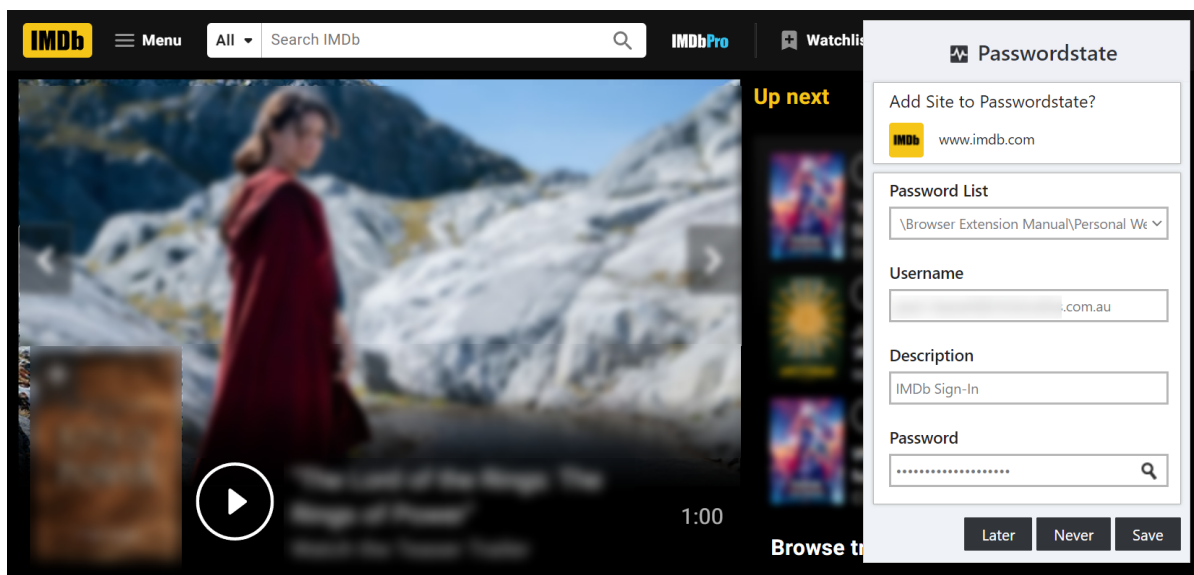


1. A **Back** Button to return to the main page
2. A check box to **Enable Auto-Fill** on websites. With this enabled your Browser Extension will automatically form-fill credential input fields. Disabling this will prevent the Browser Extension from automatically form-filling login credentials on any website you visit. You can manually force the Browser Extension to fill the credentials while this is disabled
3. The **Enable Icon Overlay** when enabled will insert the Passwordstate heartbeat icon in all credential input fields. This can be clicked on to select the correct credentials for that site. When disabled it prevents the browser extension icon in the login fields on all websites
4. The **Default Password List** drop down allows you to select which Password List all new login credentials will be saved to. If you have multiple Password Lists with the URL field configured, you can still choose another Password List to save credentials to at the time of saving them
5. The **Default Password Generator** allows you to set a Password Generator of your choice from those available to you in Passwordstate. This is then used by the Browser Extension to

generate new random passwords in accordance with the selected generator's complexity settings

Saving Log in Credentials

When logging into a website for the first time with your Browser Extension active, you will be presented with a page asking if you want to **Add Site to Passwordstate?** This will save the credentials into Passwordstate if you haven't already saved them. It won't ask you to save them a second time.



On this screen you have the option to choose which **Password List** to store the data into, and the **Username**, **Description** and **Password** fields are editable prior to clicking **Save**. Use the magnifying glass icon to toggle the visibility of the password if required.

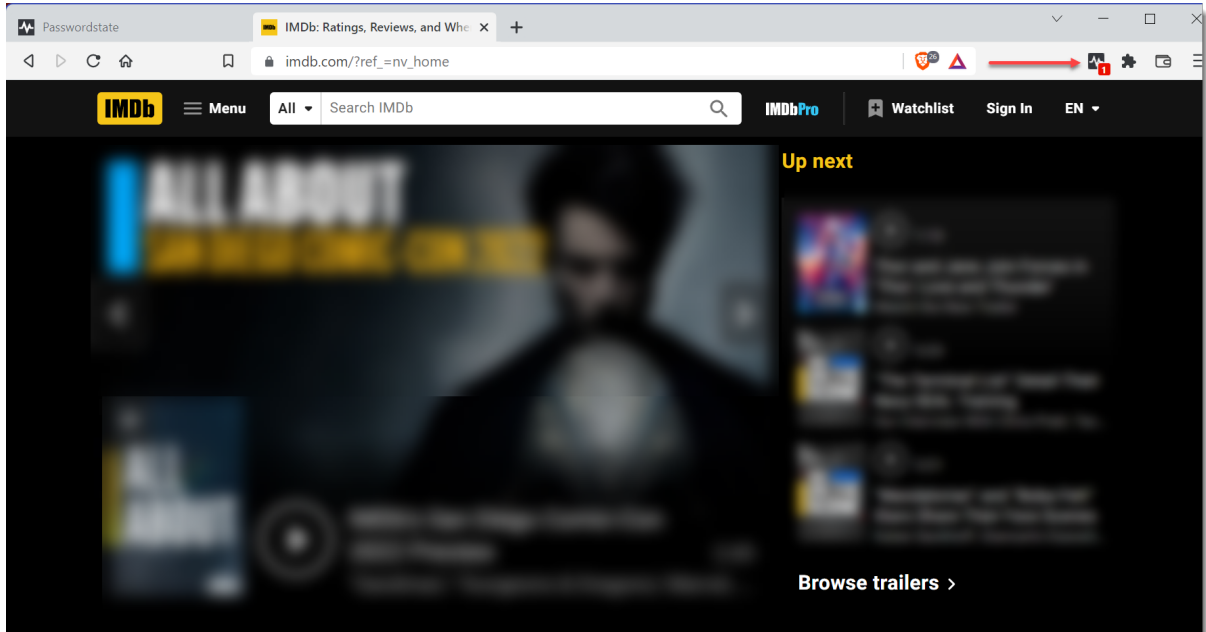
Clicking on the **Later** button will not save the credentials to the Password List this time. Instead, you will be prompted to save the credentials the next time you login to that website.

Clicking on the **Never** button will save the URL as an **Ignored URL** in Passwordstate. This will prevent the Browser Extension from asking you to save your login credentials for that website. It will also prevent automatic form-filling for this website even if you have other credentials already saved.

Ignored URLs are saved under your personal **Preferences** in Passwordstate. If needed, URLs can be removed from or added to your Preferences, or from within the **Ignored URLs** option on the main Browser Extension screen.

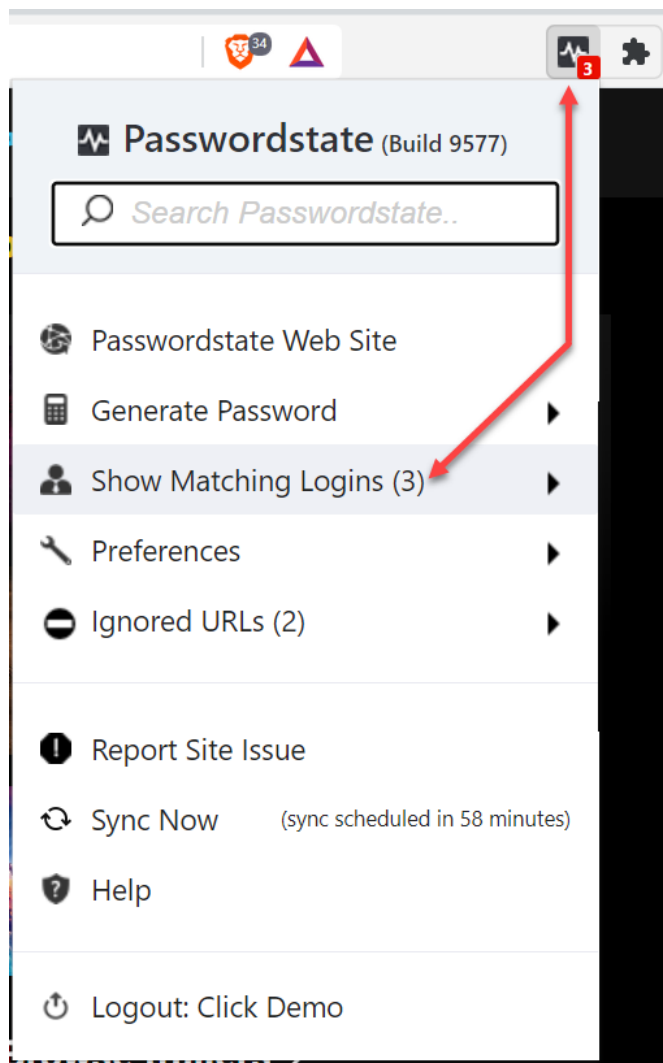
Auto-Filling Login Credentials

When you visit a website that you have a credential already saved for, the Browser Extension will display a number in **red**. The value of this number indicates how many credentials for that particular website you have saved in Passwordstate.

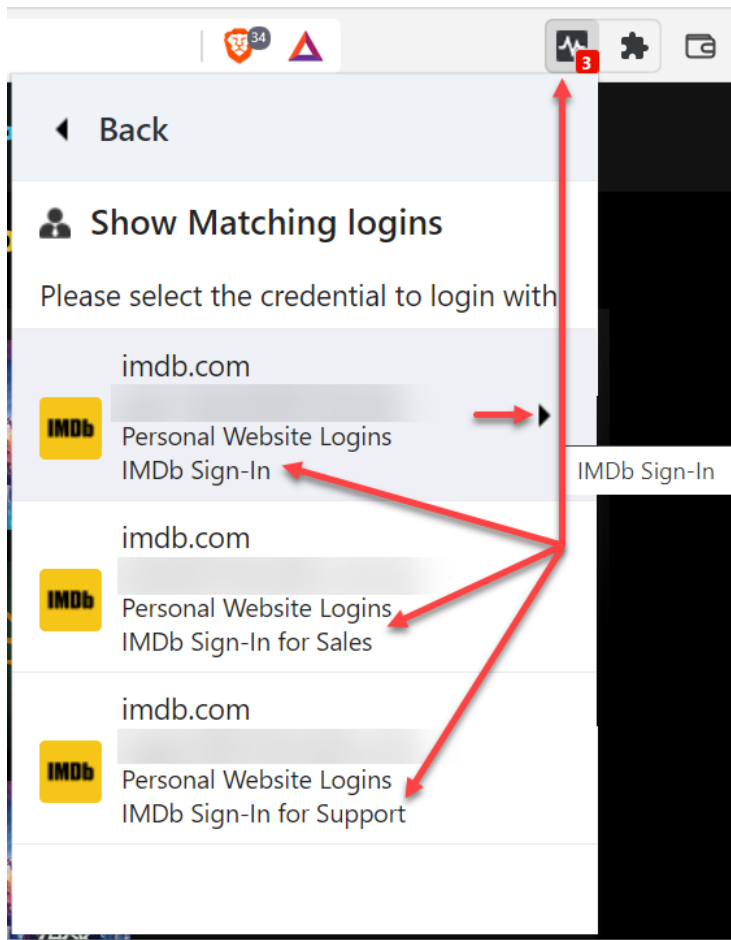


If you only have one set of credentials saved for the webpage, then the browser extension will automatically form-fill that **Username** and **Password** for you when you attempt to log in to that page.

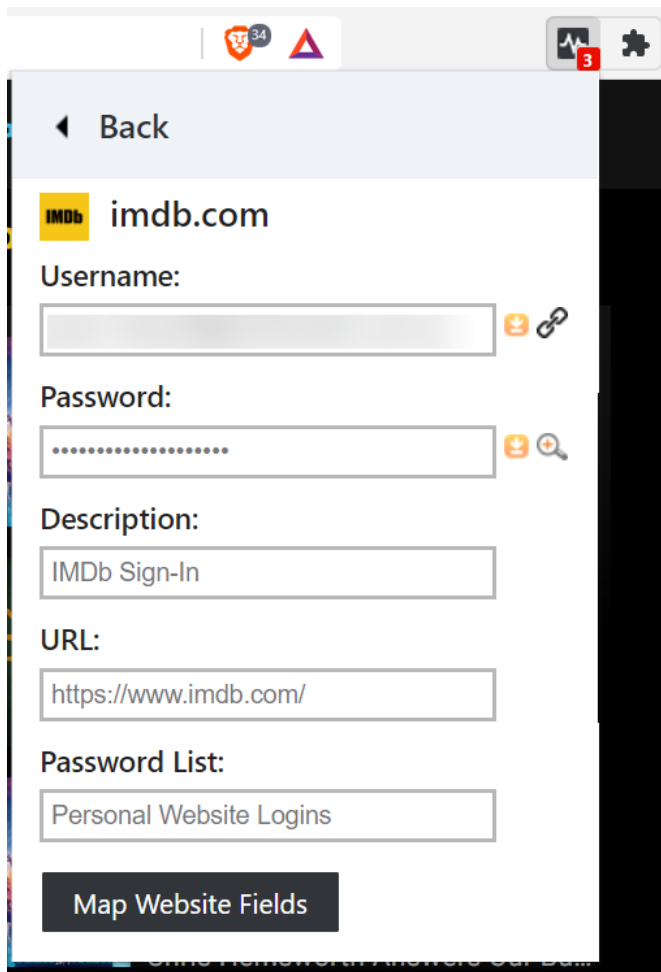
If you have multiple credentials saved, then you should click the browser extension icon, select **Show Matching Logins** and then choose the appropriate login to automatically form-fill:



Each login you have saved for the site shows the **Username**, the **Password List** where it is stored, and also the **Description**. This will help you determine which credential you should select.



If you need more information about each Password Record, you can click the advance arrow which will take you to another page with more details about the credential:



On this page, you can copy the **Username** or **Password** to the clipboard, **toggle the visibility** of the password, or click the **link icon next to the Username field** which will open up a new browser tab with the Password Record open in Passwordstate.

The **MAP Website Fields** button is discussed later in this manual.

Web Authentication Paskeys (beta)

The Browser Extension can act as an authenticator for websites that support W3C's Web Authentication (WebAuthn) standard.

Create and Register a Passkey

To create and register a Passkey, you must have an existing record for the website in Passwordstate that does not already have an associated Passkey. Additionally, the Browser Extension must also be unlocked/authenticated.

When the above conditions are met, and a supported website initiates a WebAuthn

Registration Ceremony the Browser Extension will show a pop-up dialog offering to save the Passkey.

Note: Records that already have a Passkey will not show in the drop down.

Authenticate with a Passkey

Similarly, when the Browser Extension is unlocked/authenticated and a supported website initiates a WebAuthn Authentication Ceremony then a pop-dialog will offer to login using a Passkey.

Deleting a Passkey

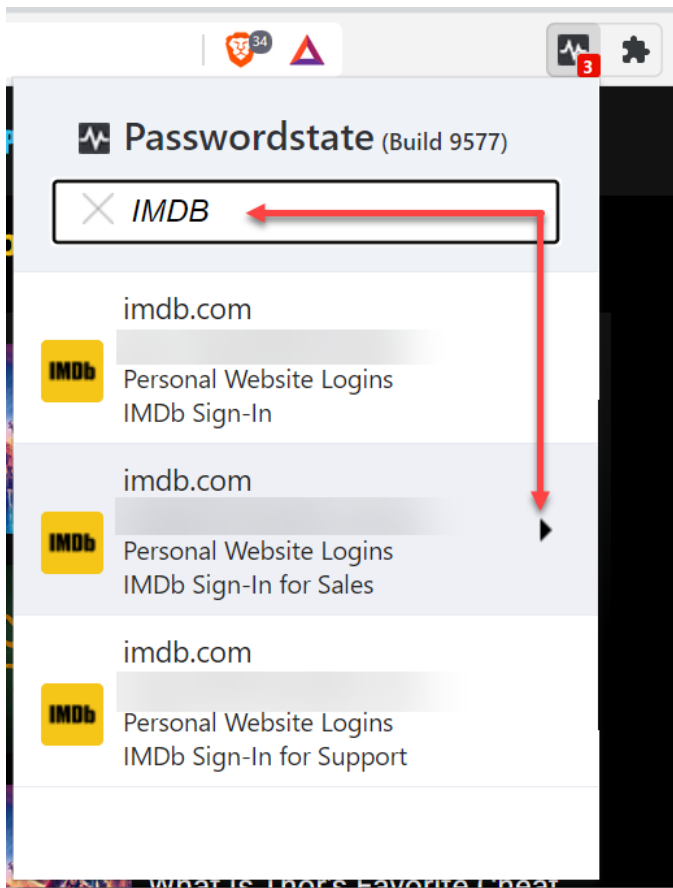
If you wish to delete or replace a Passkey, you will need to clear it via editing a record in Passwordstate's core web UI and also at the website itself.

Once the Browser Extension has synced these changes you will then be able to create and register a Passkey for this record again.

Using the Search Feature

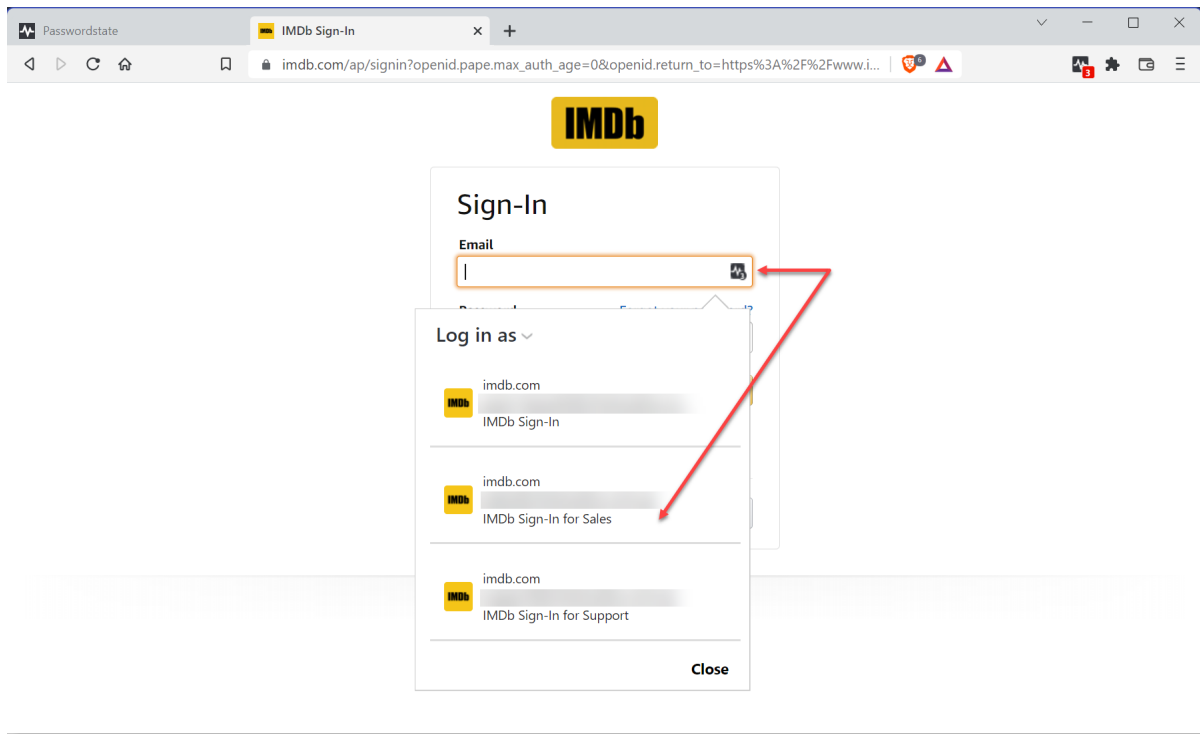
Another way to use the Browser Extension is to search for a website you have previously saved.

When you find a credential via the search feature, you can either click directly on the credential itself, which will open the website in a new tab, or you can click the **arrow** icon which will open a new page with more details about the password record.



Icon Overlay

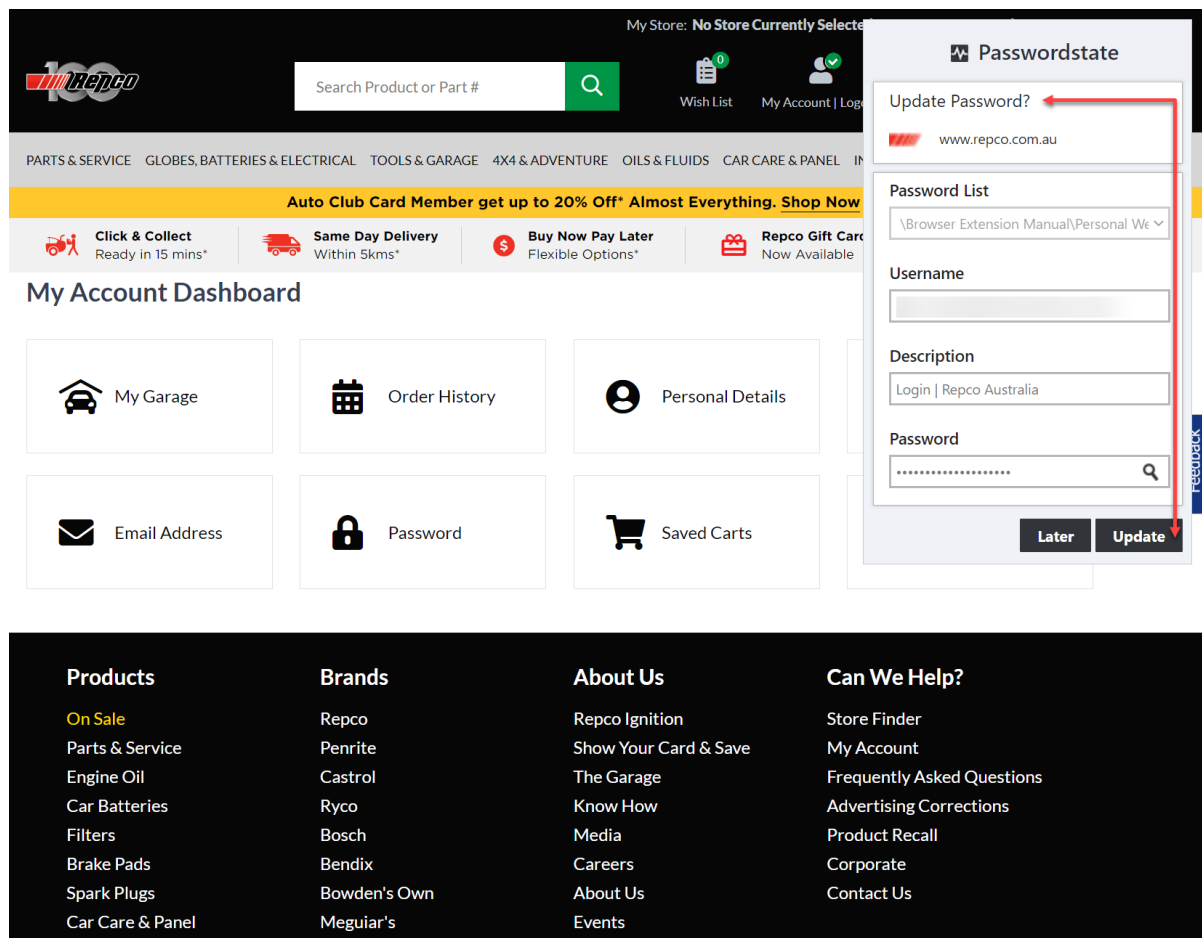
The **Icon Overlay** is displayed by default in the **Username** and **Password** fields. If you have mapped additional input fields then the Icon Overlay will appear in those fields as well.



Clicking on the icon overlay will allow you to choose which credential you want to log in with. It also has its own search feature to make finding saved credentials easy if you have more than 10 saved Password Records for that website.

Updating Passwords on a website


When you change a password, from within the website itself, the Browser Extension will prompt you with **Update Password?** for the existing Password Record in Passwordstate.



To do this simply click on the **Update** button. Alternatively, you can click **Later** to not update your password record within Passwordstate at this time.

One-Time Passwords

If you have any Password Lists configured in Passwordstate for the One-Time Password feature, these OTP codes can be both copied from the Browser Extension and also automatically form-filled into the website's input fields.

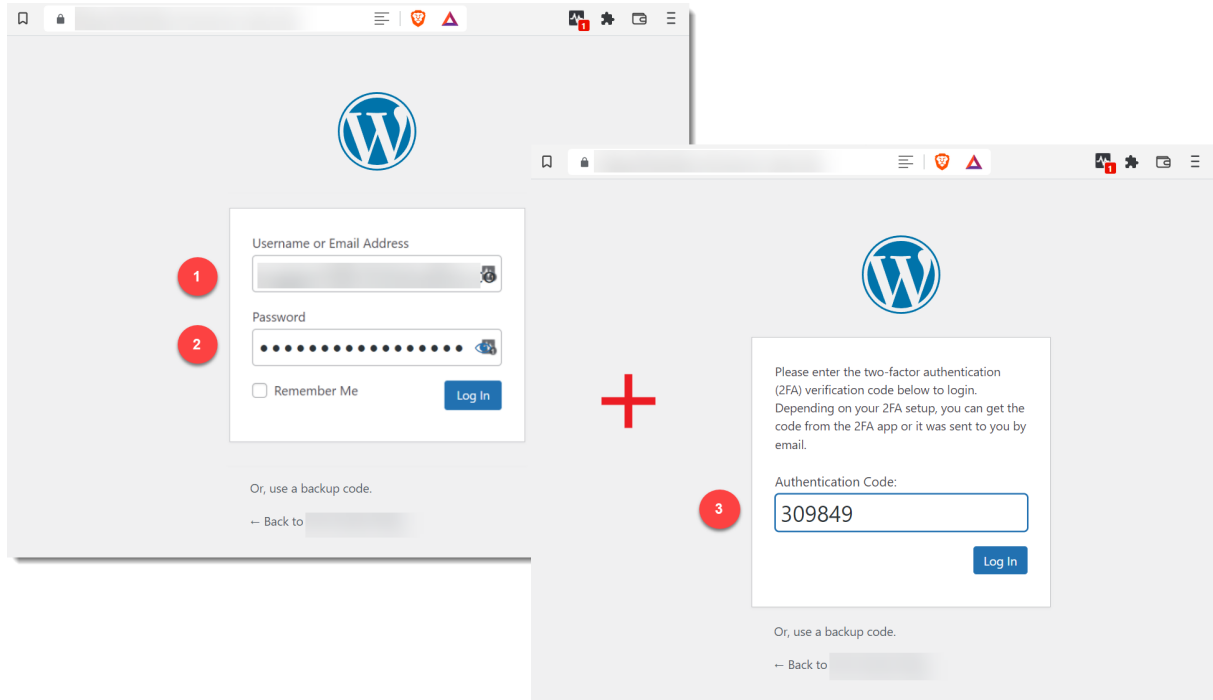
 **Note:** The setting **Enable Form-Filling of OTP Codes** must be enabled in **Administration -> Browser Extension Settings**, and this will be disabled by default for a fresh install or upgrade from a build prior to 9583. In addition to this, the password record must have a Website Field ID set for OTP.

The first image shows the automatic form-filling of 3 fields from a Password Record, those being,

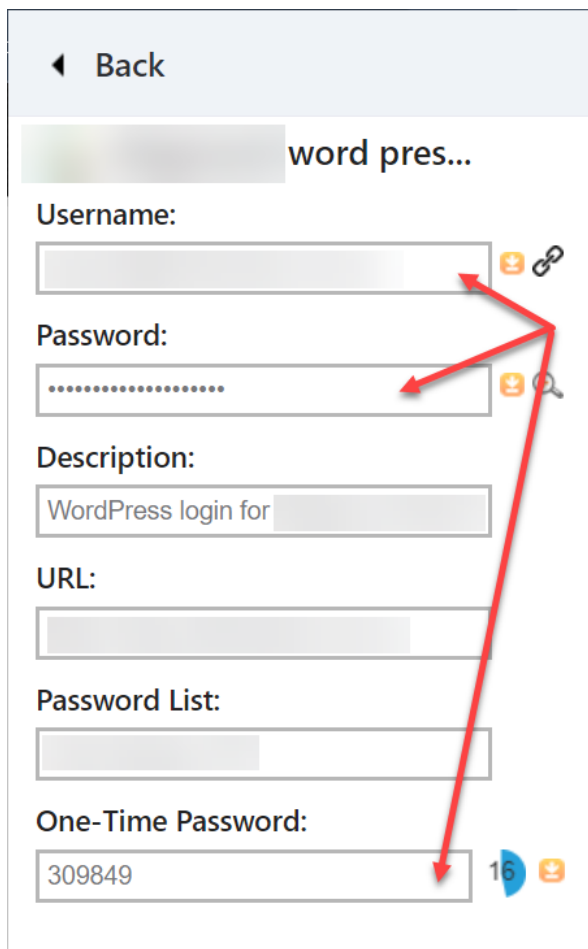
1. **Username**, in this case the Email Address

2. Password

3. One-Time Password code



The image is a composite image showing the first screen, which automatically form-fills the **Username** and **Password**. On clicking the **Login** button, the second screen is shown with the **OTP Code** automatically form filled. From here the **Login** button is clicked again to login using the 3 credential elements.



Back

word pres...

Username:

Password:

Description:

URL:

Password List:

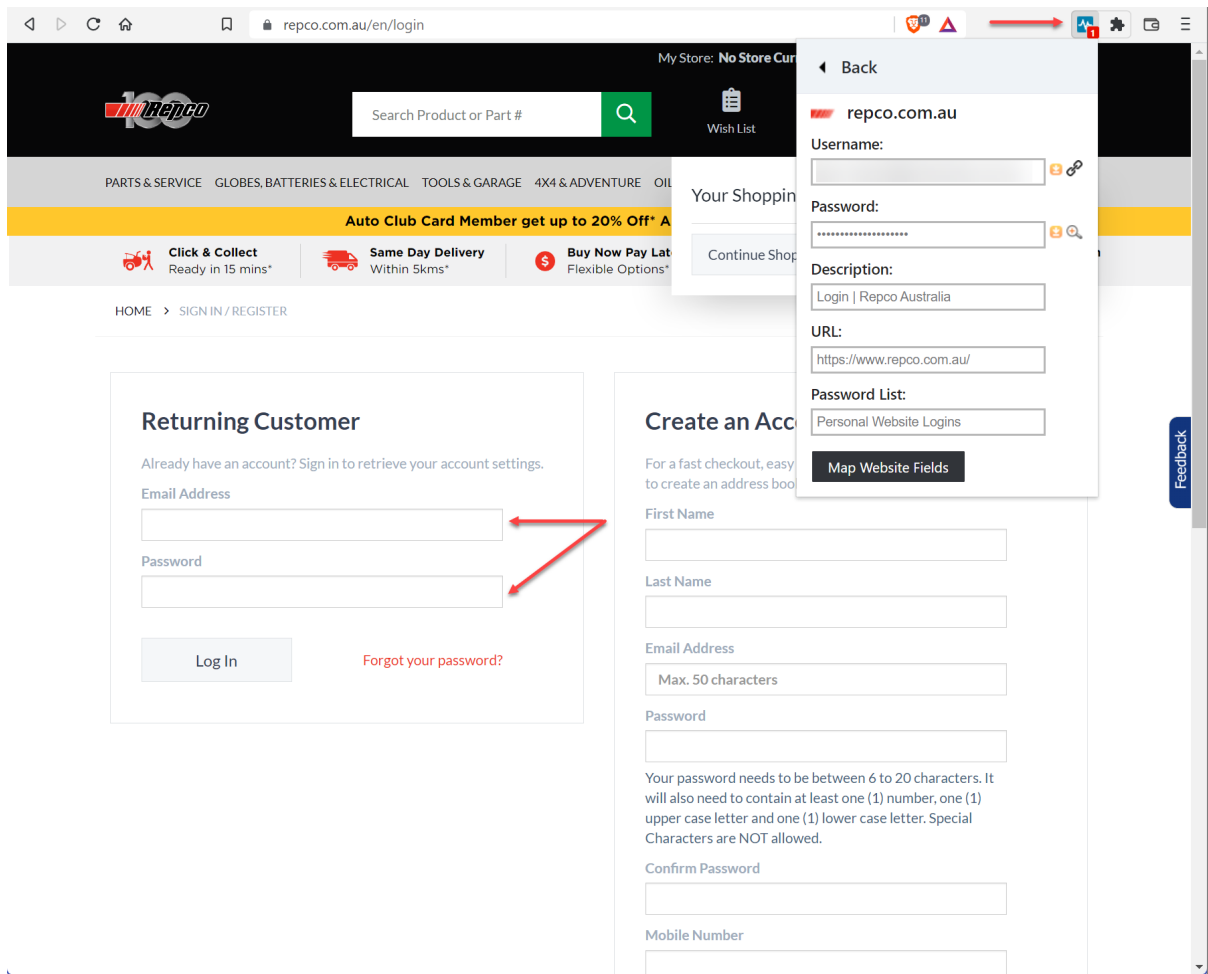
One-Time Password:

You can also access all 3 credential elements by clicking on the Password Record's advance arrow. This takes you to the page with all the details about the credential. From here you can copy any of the fields and paste them into the website's input fields.

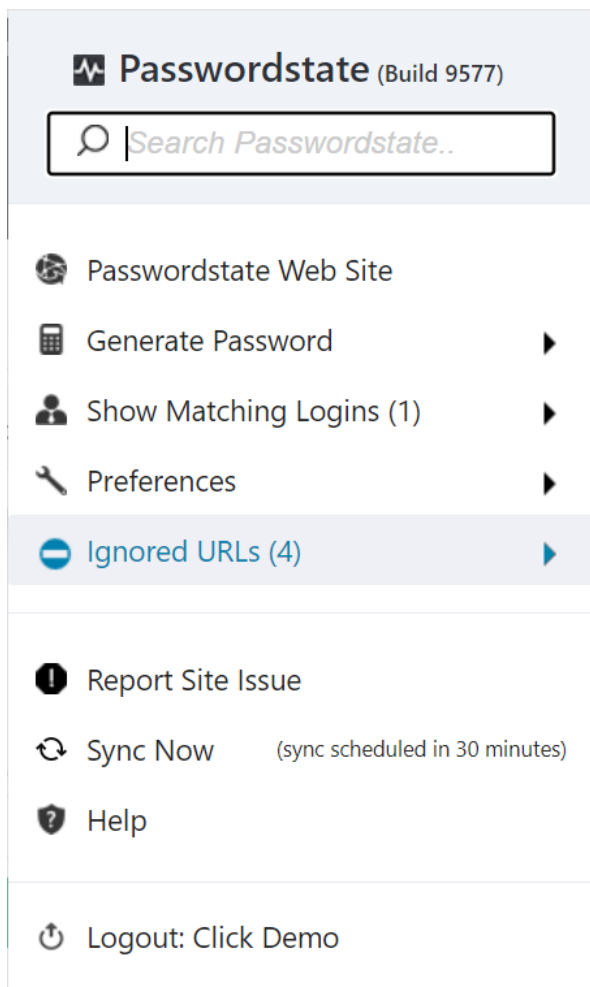
Ignored URLs

If you find the Browser Extension doesn't work as expected on a particular website, we recommend setting that website as an Ignored URL. This will set the Browser Extension to not interact with any input fields for the site and the Icon Overlay will be turned off.

If you have an existing Password Record saved for this site you can still click on the Browser Extension icon in the top right hand corner of your browser, and select the Password Record advance arrow and click on the copy icon next to the **Username** and **Password** fields to manually paste into the input fields.

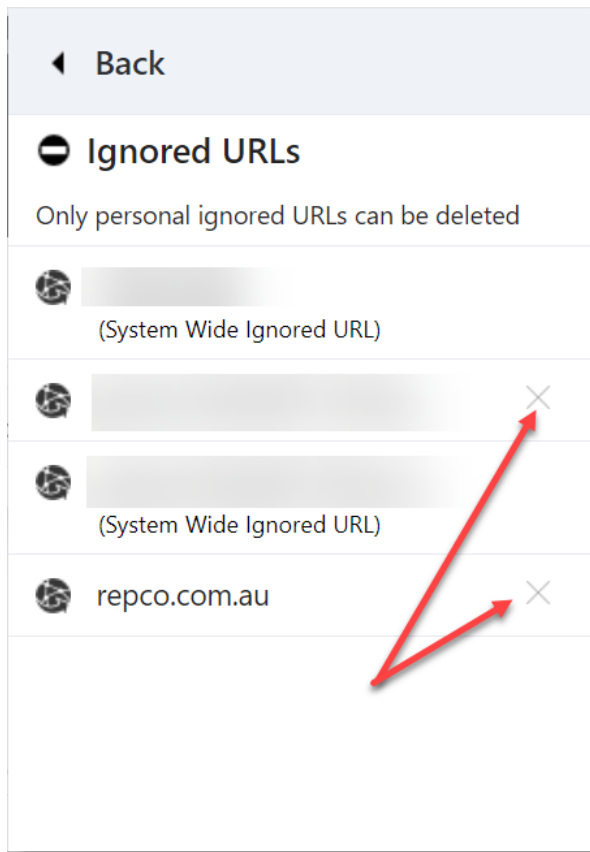


When browsing to a website set as an Ignored URL your Passwordstate Extension icon will turn **Blue**. You will also see an ignored URL menu in your Browser Extension as per below screenshot:



In the screenshot above, there is a counter on the Ignored URLs item with a value of 4. This value is a combination of any personal Ignored URLs previously set, and any that your Passwordstate Security Administrator has set from within the Passwordstate Administration area.

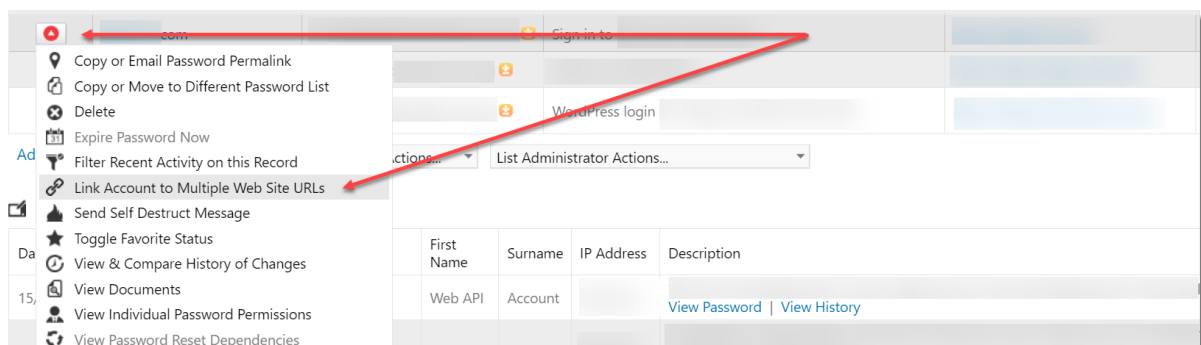
When clicking on the **Ignored URLs** menu you'll be taken to another page showing all of the URLs the Browser Extension is set to ignore. On this page you can delete any URL in your own Preferences by clicking on the **X** to the right of the entry. Entries without an **X** to the right are System Wide Ignored URLs set by your Security Administrator. These can only be removed by your Passwordstate Security Administrator.



Linking Multiple URLs to one Password Record

Linking Multiple URLs to one Password Record has multiple uses. The first is where your AD Account is used to login to multiple internal websites. In this example you can use the one Password Record linked to URLs for each of the internal websites.

A second use is where some websites use multiple URLs for the login process. As an example, a website may use one URL for the **Username** input field and a separate URL for the **Password** input field.



In this situation you can still have the one Password Record but link it to multiple URLs. When saving the Password Record the primary URL will be for the **Username** input field. The second URL can be added by navigating to the **Password Record** in Passwordstate, selecting the **Action Icon** and choosing to Link Account to Multiple Web Site URLs.

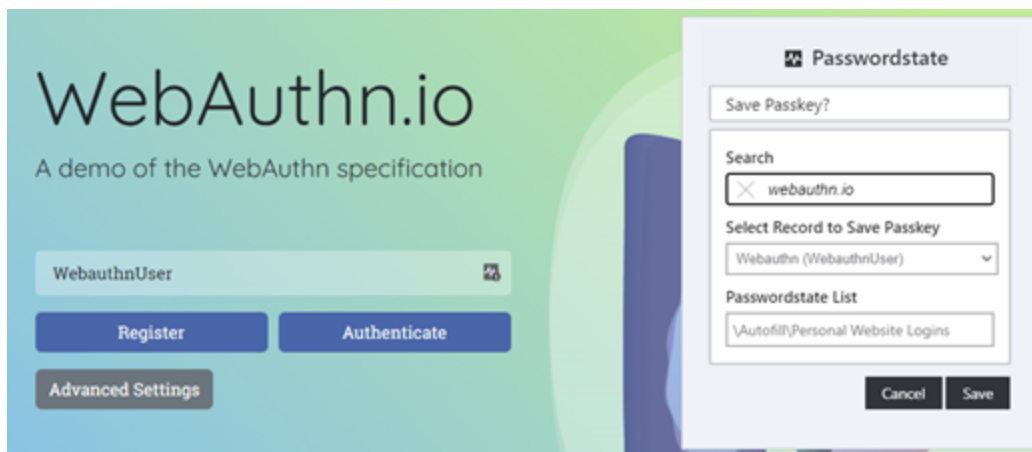
5 Web Authentication Passkeys

The Browser Extension can act as an authenticator for websites that support W3C's Web Authentication (WebAuthn) standard.

Create and Register a Passkey

To create and register a Passkey, you must have an existing record for the website in Passwordstate that does not already have an associated Passkey. Additionally, the Browser Extension must also be unlocked/authenticated.

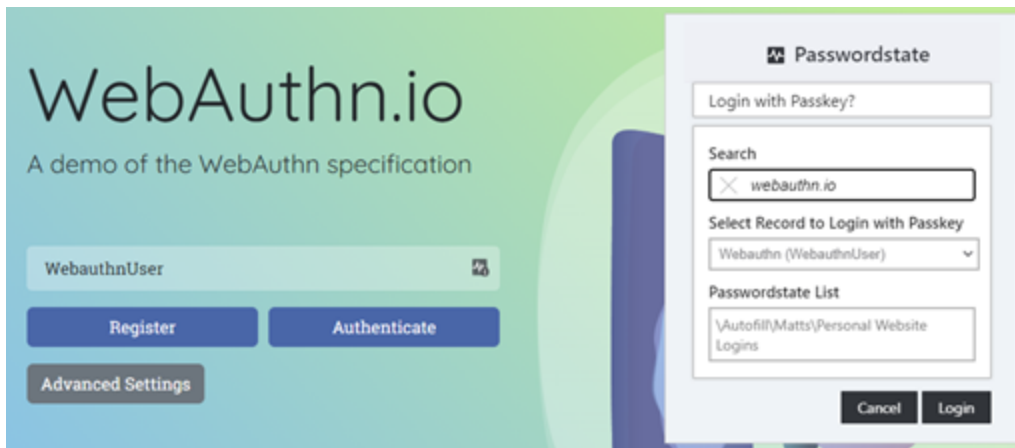
When the above conditions are met, and a supported website initiates a WebAuthn Registration Ceremony the Browser Extension will show a pop-up dialog offering to save the Passkey.



Note: Records that already have a Passkey will not show in the drop down.

Authenticate with a Passkey

Similarly, when the Browser Extension is unlocked/authenticated and a supported website initiates a WebAuthn Authentication Ceremony then a pop-dialog will offer to login using a Passkey.



Warning: Logging into a website will increment the Passkey internal counter as per the WebAuthn specification. Some websites choose to compare the count value from the previous successful authentication, and then deny access if they are out of sync. **If you are restoring data from old backups** this can cause this issue, and will require using a recovery method for the website to re-create the Passkey.

Deleting a Passkey

If you wish to delete or replace a Passkey, you will need to clear it via editing a record in Passwordstate's core web UI and also at the website itself.

Edit Password

Please edit the password below, stored within the "Personal Website Logins" Password List (Tree Path = \Autofill).

password details | notes | security | website fields | url matching

Title * Webauthn

UserName WebauthnUser

Description

URL https://webauthn.io

Passkey **Passkey saved to database** Clear

Password Generator 15 Character Passwords

Password

Confirm Password

Password Strength ★★★★★ Compliance Strength ★★★★★

Strength Status:

Reset Tasks (0) Added via Discovery Compliance Mandatory Prevent Bad Password

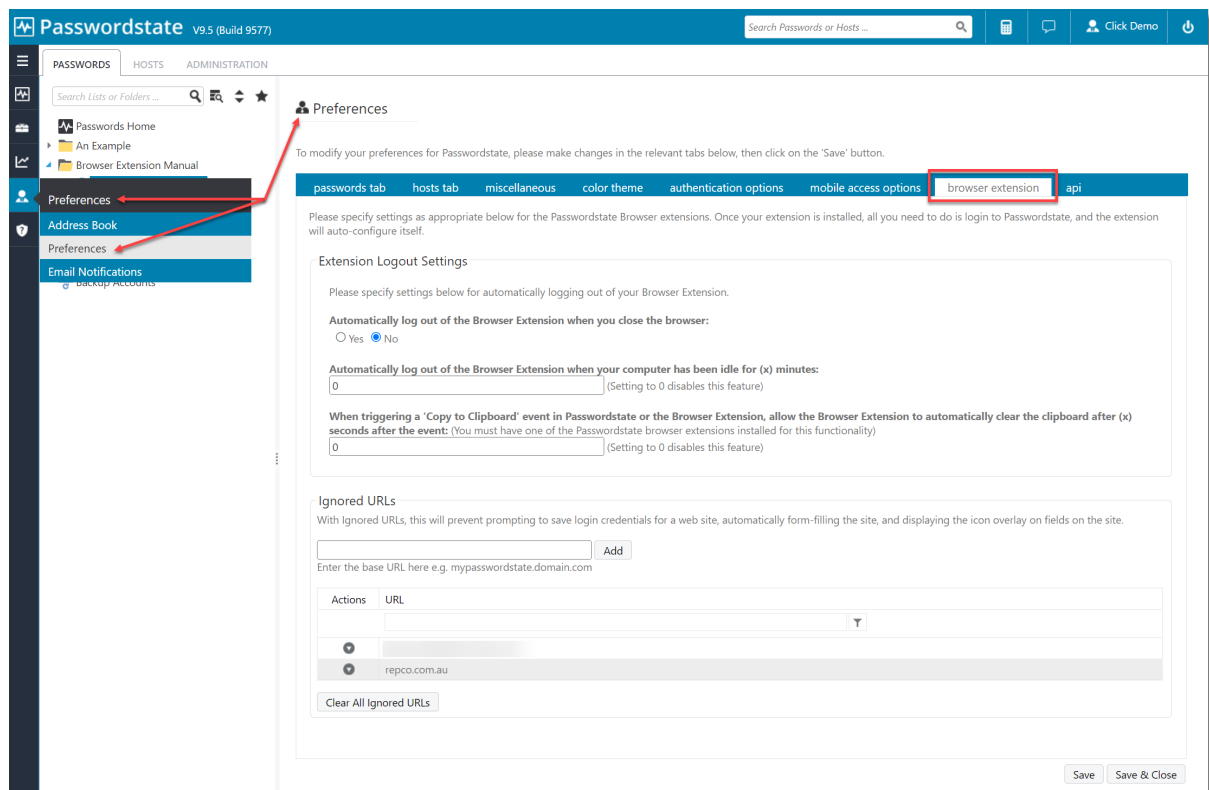
Save Cancel

6 Browser Extension Settings

There are various settings within Passwordstate which governs how the Browser Extension can be used. These settings can be configured per user or System Wide.

Browser Extension Per User Settings

In the Preferences Screen, located on the browser extension tab, you can find settings for automatically logging out of the Browser Extension, clearing the clipboard of data on a schedule, and also for ignoring certain URLs.

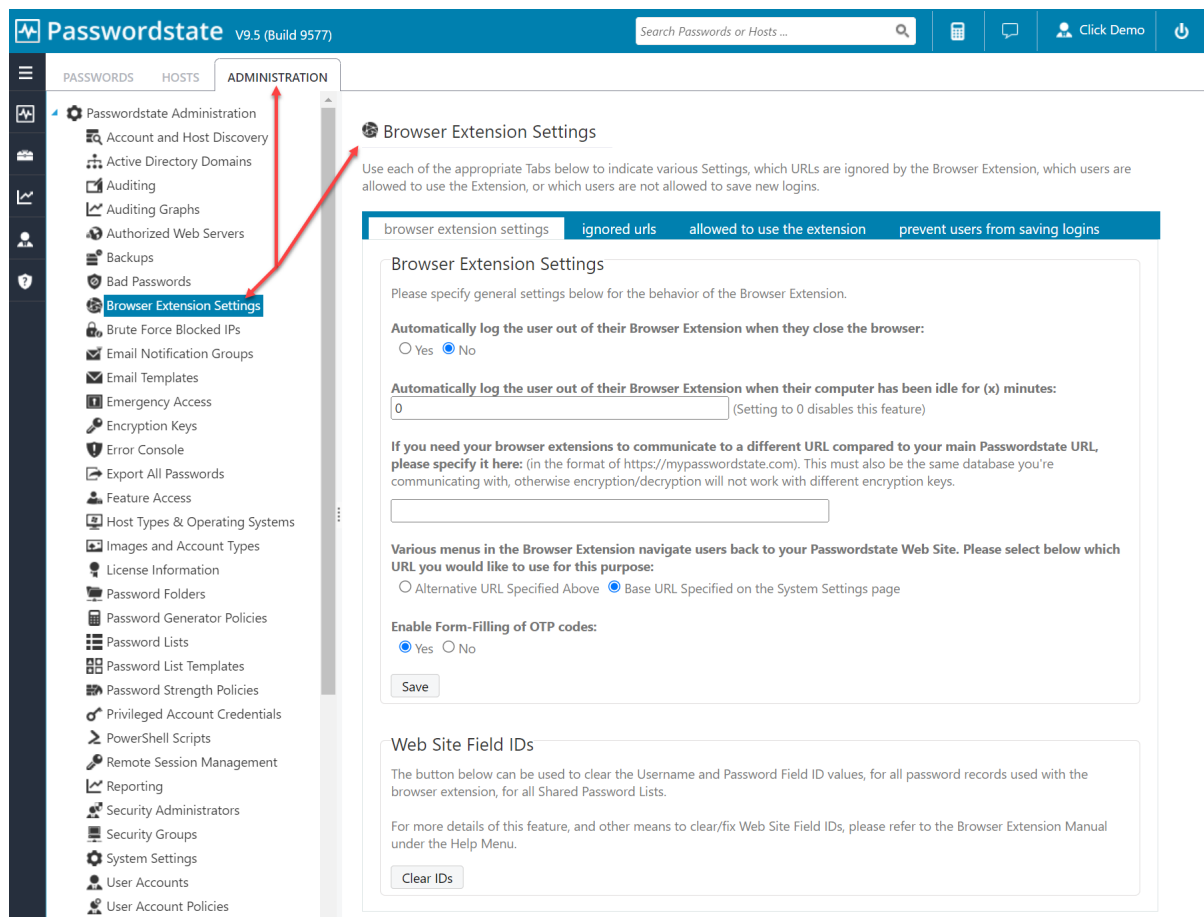


You can delete individual Ignored URLs by using the Action Icon for individual entries or by clicking on the **Clear All Ignored URLs** button.

System Wide Settings

Your Security Administrators have access to a number of configuration options under **Administration -> Browser Extension Settings**. These settings relate to;

- Browser Extension Settings
- System Wide Ignored URLs
- Users allowed to use the extension, and,
- Prevent users from saving logins.



If you believe there is a system setting preventing you from saving, using or logging into our Browser Extensions please contact your Passwordstate Security Administrator. More information on the Passwordstate configuration options for our Browser Extensions can be found in our **Security Administrators Manual**.


7 Detection and Advanced Functionality

When first saving credentials into Passwordstate, the Browser Extension will not save any website field ID's for the record. This allows the extension to form fill the username and password based on the in-built input detection which mitigates against websites that use dynamic field IDs.

The field ID's are only necessary for the OTP and Generic Fields or for websites where the extension does not form fill the username and password as expected.

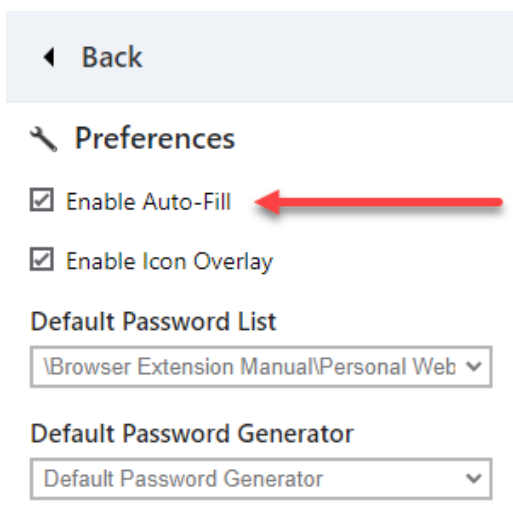
Edit Password

Please edit the password below, stored within the '**Personal Website Logins**' Password List (Tree Path = \Browser Extension Manual).


password details	notes	security	website fields	url matching																										
<p>The Browser Extension for Passwordstate uses the 'names' of the HTML elements for form-filling. If you need to manually change these, you can do so by modifying the values below.</p> <p> If the UserName and/or Password field ID values are left blank then the extension will do its best to search and fills these. However, for OTP and Generic Fields the field ID values must be correct or form-filling of these fields will not occur.</p> <table><tbody><tr><td>UserName Field ID:</td><td><input type="text"/></td></tr><tr><td>Password Field ID:</td><td><input type="text"/></td></tr><tr><td>OTP Field ID:</td><td><input type="text"/></td></tr><tr><td>Generic Field 1 ID:</td><td><input type="text"/></td></tr><tr><td>Generic Field 2 ID:</td><td><input type="text"/></td></tr><tr><td>Generic Field 3 ID:</td><td><input type="text"/></td></tr><tr><td>Generic Field 4 ID:</td><td><input type="text"/></td></tr><tr><td>Generic Field 5 ID:</td><td><input type="text"/></td></tr><tr><td>Generic Field 6 ID:</td><td><input type="text"/></td></tr><tr><td>Generic Field 7 ID:</td><td><input type="text"/></td></tr><tr><td>Generic Field 8 ID:</td><td><input type="text"/></td></tr><tr><td>Generic Field 9 ID:</td><td><input type="text"/></td></tr><tr><td>Generic Field 10 ID:</td><td><input type="text"/></td></tr></tbody></table>					UserName Field ID:	<input type="text"/>	Password Field ID:	<input type="text"/>	OTP Field ID:	<input type="text"/>	Generic Field 1 ID:	<input type="text"/>	Generic Field 2 ID:	<input type="text"/>	Generic Field 3 ID:	<input type="text"/>	Generic Field 4 ID:	<input type="text"/>	Generic Field 5 ID:	<input type="text"/>	Generic Field 6 ID:	<input type="text"/>	Generic Field 7 ID:	<input type="text"/>	Generic Field 8 ID:	<input type="text"/>	Generic Field 9 ID:	<input type="text"/>	Generic Field 10 ID:	<input type="text"/>
UserName Field ID:	<input type="text"/>																													
Password Field ID:	<input type="text"/>																													
OTP Field ID:	<input type="text"/>																													
Generic Field 1 ID:	<input type="text"/>																													
Generic Field 2 ID:	<input type="text"/>																													
Generic Field 3 ID:	<input type="text"/>																													
Generic Field 4 ID:	<input type="text"/>																													
Generic Field 5 ID:	<input type="text"/>																													
Generic Field 6 ID:	<input type="text"/>																													
Generic Field 7 ID:	<input type="text"/>																													
Generic Field 8 ID:	<input type="text"/>																													
Generic Field 9 ID:	<input type="text"/>																													
Generic Field 10 ID:	<input type="text"/>																													


If you find you are having issues with automatically form-filling your credentials for a website there are a couple of ways to fix this.

First you should confirm that you still have **Enable Auto-Fill** selected. This is found on your Preferences screen:



◀ Back

 Preferences

☒ Enable Auto-Fill 

☒ Enable Icon Overlay

Default Password List

\Browser Extension Manual\Personal Web ▾

Default Password Generator

Default Password Generator ▾

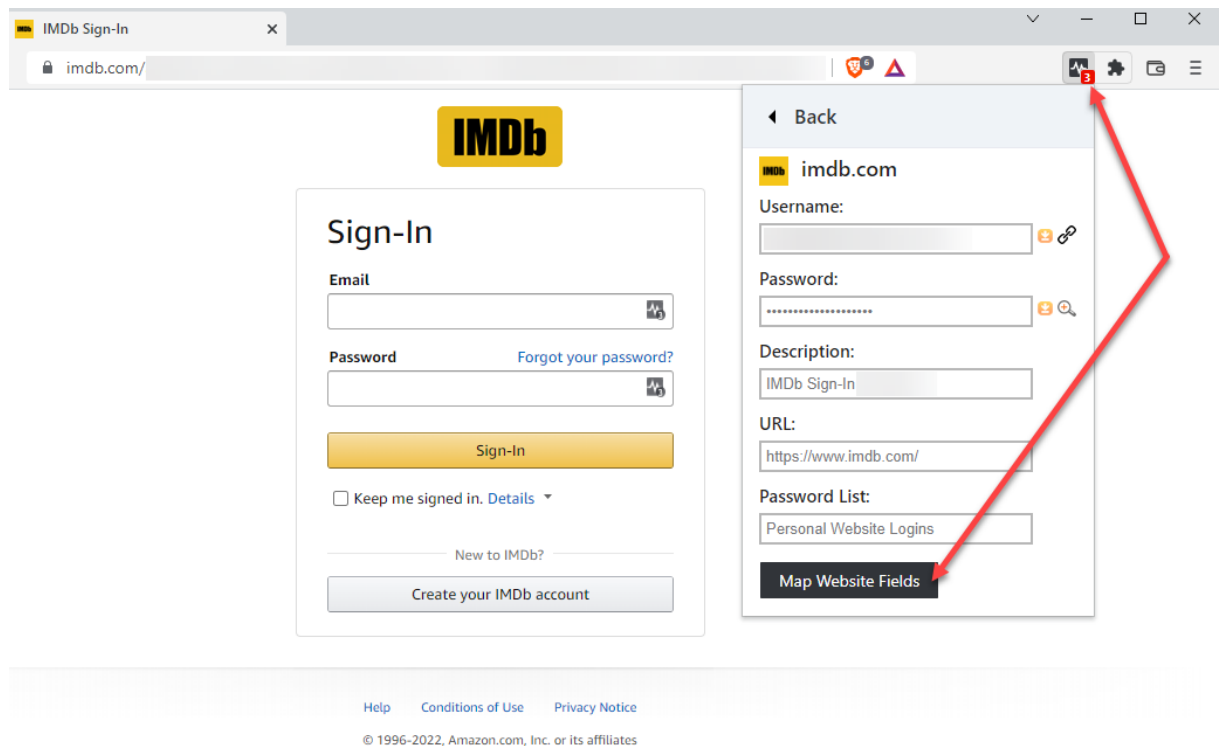
Next, check if the website you have browsed to has an **Ignored URL** set under either your preferences, or has been set globally by your Security Administrator. Refer to the section on Ignored URLs in this Manual for more information.

Finally, try mapping the website fields either manually via editing the password record or using the **Map Website Fields** helper tool in the extension to override the in-built input detection.

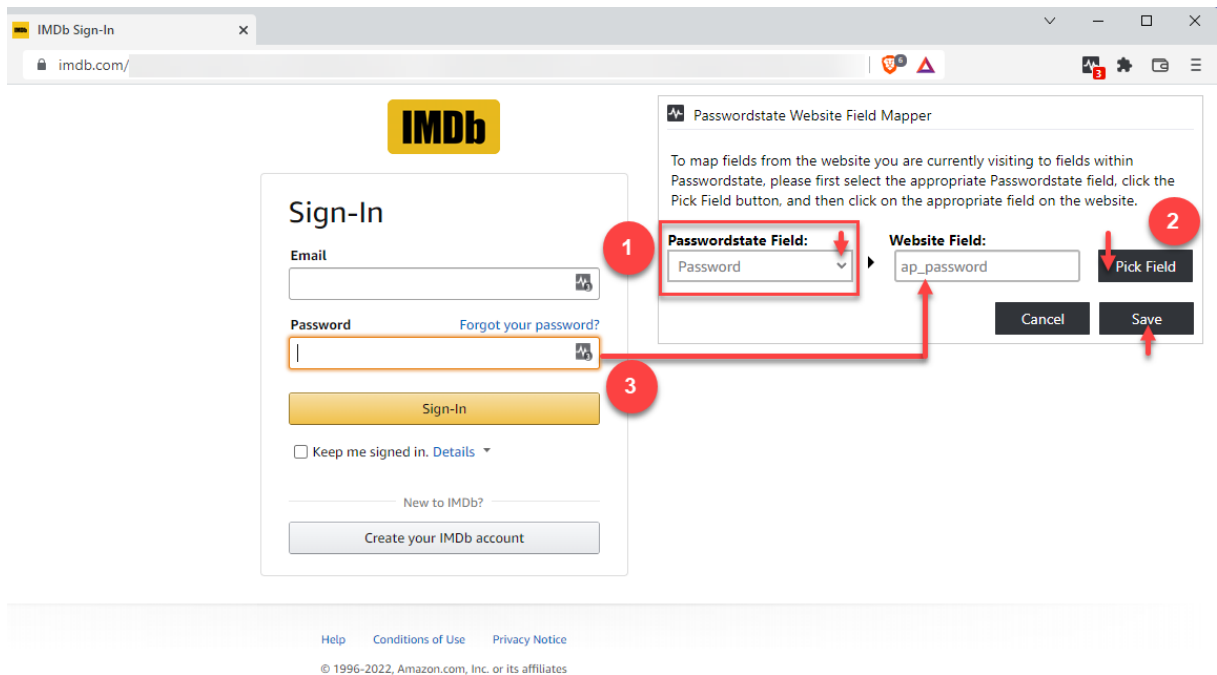
Mapping Website Fields

As mentioned above, occasionally you may be faced with a particularly hard website where our Browser Extension does not automatically form-fill.

In this situation you can use additional functionality built-in to the Browser Extension to correctly map the website Field IDs which may help depending on the website. To do this select the Password Record in your Browser Extension and click on the **arrow** icon to open a new page with more details about the Password Record. From here click on the **Map Website Fields** button,



This will open the **Passwordstate Website Field Mapper** dialog. From here it's a simple process of mapping each input field;



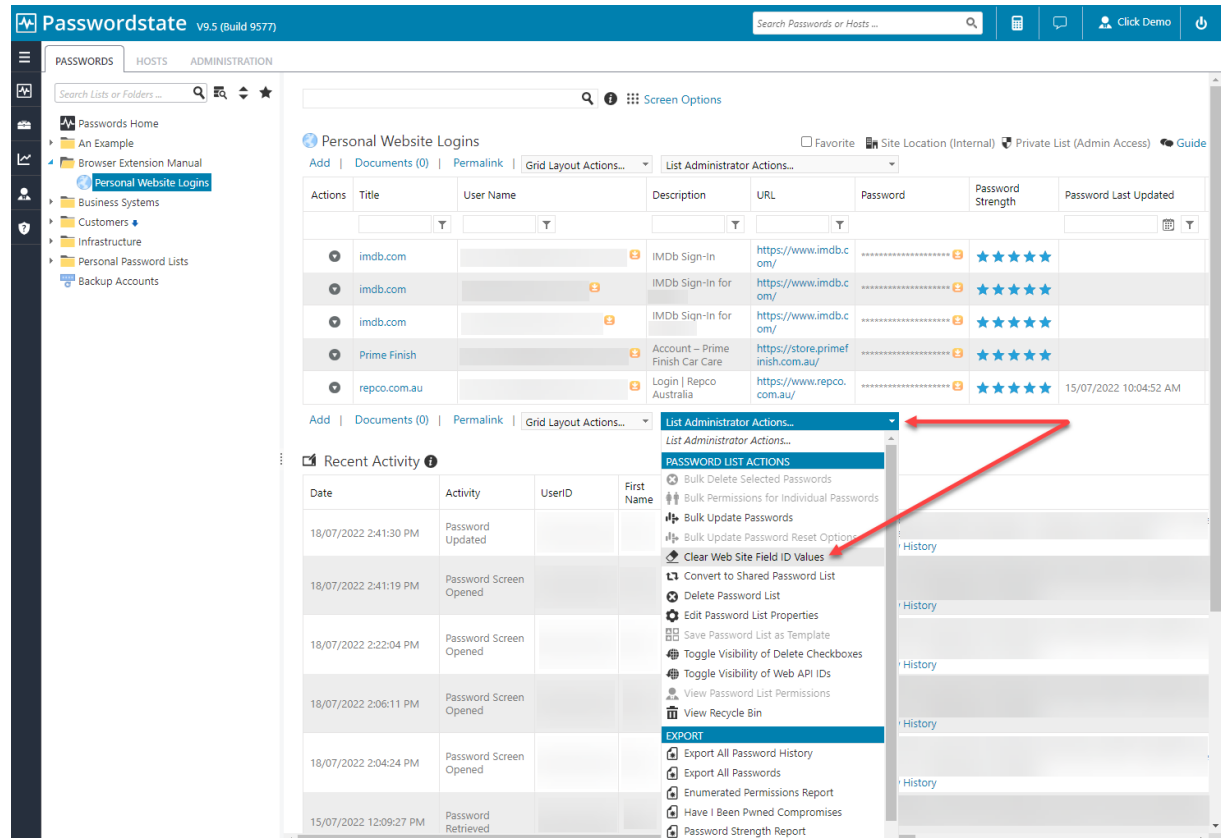
1. Select the type of **Passwordstate Field** to map,
2. Click on the **Pick Field** button,
3. Move the mouse cursor to the input field, in this case the **Password** input field on the website and click on it to select it,
4. Repeat the process for all required input fields,
5. Click the Save button

This will now save the correct website Field IDs, for all input fields you have selected, to the **website fields** tab for that **Password Record**.

Clearing Website Fields

If you find you are having problems with multiple Password Records not automatically form filling, you can clear the username and password website Field IDs for all **Password Records** in a **Password List**. This doesn't affect the credentials, only the associated Field IDs that have been recorded and stored on the website fields tab for each Password Record.

To clear all the website Field IDs, for all Password Records in a Password List, simply login to Passwordstate, navigate to the Password List you want to perform the action against and click on **List Administrator Actions...**, then click on **Clear Web Site Field ID Values**,



Security administrators have the ability to clear all username and password website Field IDs for Shared Password Lists via **Administration -> Browser Extension Settings -> Website Field IDs**,

Web Site Field IDs

The button below can be used to clear the Username and Password Field ID values, for all password records used with the browser extension, for all Shared Password Lists.

For more details of this feature, and other means to clear/fix Web Site Field IDs, please refer to the Browser Extension Manual under the Help Menu.

Clear IDs

URL Matching

You can specify the **URL Matching** option for each individual Password Record in Passwordstate. This is particularly helpful in instances where the **Username** and **Password** input fields are located on different URLs.

There are 3 URL Matching options available, **Starts With**, **Base Domain** and **Host Name** with the default being **Starts With** which should cater for most situations.

Edit Password

Please edit the password below, stored within the '**Personal Website Logins**' Password List (Tree Path = \Browser Extension Manual).

password details **notes** **security** **website fields** **url matching**

The Browser Extension for Passwordstate uses one of following URL matching options for form-filling this record:

URL Match Option: ☒ Starts With ☐ Host Name ☐ Base Domain

Starts With: the website URL must start with the record's URL.
I.e. *contoso.com/forums* will match *contoso.com/forums* and *contoso.com/forums/login*

Base Domain: matches against top-level domain and second-level domain of the record's URL.
I.e. *contoso.com* will match *mail.contoso.com* and *login.contoso.com*

Host Name: matches against the host name and port number (if applicable) of the record's URL.
I.e. *contoso.com:8414* will match *contoso.com:8414* and *contoso.com:8414/path*
I.e. *sub.contoso.com* will match *sub.contoso.com* and *sub.contoso.com/path*

Save **Cancel**