

# **Web Password Filler**

## **Administrator Guide**

Version: 3.10.x

Publication Date: 10/29/2024

## Web Password Filler Administrator Guide

Version: 3.10.x, Publication Date: 10/29/2024

© Delinea, 2024

### Warranty Disclaimer

DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, MAKE NO REPRESENTATIONS ABOUT THE SUITABILITY OF THE INFORMATION CONTAINED IN THE DOCUMENTS AND RELATED GRAPHICS, THE SOFTWARE AND SERVICES, AND OTHER MATERIAL PUBLISHED ON OR ACCESSIBLE THROUGH THIS SITE FOR ANY PURPOSE. ALL SUCH MATERIAL IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, HEREBY DISCLAIM ALL WARRANTIES AND CONDITIONS WITH REGARD TO SUCH MATERIAL, INCLUDING ALL IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT.

THE MATERIAL PUBLISHED ON THIS SITE COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN. DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE MATERIAL DESCRIBED HEREIN AT ANY TIME.

### Disclaimer of Liability

IN NO EVENT SHALL DELINEA AND ITS AFFILIATES, AND/OR ITS AND THEIR RESPECTIVE SUPPLIERS, BE LIABLE FOR ANY SPECIAL, INDIRECT, OR CONSEQUENTIAL DAMAGES (INCLUDING LOSS OF USE, DATA, PROFITS OR OTHER ECONOMIC ADVANTAGE) OR ANY DAMAGES WHATSOEVER, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE, OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF SOFTWARE, DOCUMENTS, PROVISION OF OR FAILURE TO PROVIDE SERVICES, OR MATERIAL AVAILABLE FROM THIS SITE.

# Table of Contents

|  |           |
|--|-----------|
| <b>Web Password Filler</b> .....   | <b>1</b>  |
| <b>Getting Started</b> .....   | <b>1</b>  |
| Enabling Web Services in Secret Server .....   | 1         |
| Connecting to the Delinea Platform and Secret Server .....                             | 1         |
| Connecting to the Delinea Platform .....   | 1         |
| Connecting to Secret Server .....  | 4         |
| Logging in Locally .....   | 6         |
| Specifying Default Protocols .....   | 7         |
| Redirecting to Secret Server via Hyperlink .....                                       | 8         |
| Reviewing Terminology .....  | 9         |
| Using Web Password Filler with Secret Server .....                                     | 9         |
| Installing Browser Extensions .....  | 11        |
| Navigating the Preferences Menu .....  | 11        |
| <b>Using WPF</b> .....   | <b>14</b> |
| Logging in to a Website .....  | 14        |
| Accessing Secrets Guarded by MFA .....   | 15        |
| Autofilling OTP .....  | 16        |
| Recording Web Sessions .....   | 18        |
| Session Recording Disconnecting Warning .....  | 19        |
| Enabling Mouse Path Tracking On Recordings .....                                       | 21        |
| Managing Session Recording Limits .....  | 24        |
| Using RegEx .....  | 24        |
| Using RegEx in WPF .....   | 25        |
| Setting Up Templates in Secret Server .....  | 26        |
| Exploring Resolution Sizes .....   | 28        |
| Determining Supported Screen Resolution Sizes for Windows .....                        | 28        |
| Determining Supported Screen Resolution Sizes for Mac .....                            | 30        |
| Launching Comma-Separated URLs .....   | 30        |
| Creating a Secret Template .....   | 31        |
| Using the Custom Web Launcher .....  | 35        |
| Setting Comment Requirements .....   | 37        |
| Requiring Comments When Enabling the 'Hide Secret Server Version Number' Setting ..... | 37        |
| Creating a Secret for a Website .....  | 38        |
| Selecting a Folder .....   | 40        |
| Adding Accounts .....  | 40        |
| Syncing Recent and Favorite Lists with Secret Server .....                             | 42        |
| Refreshing the Recent and Favorites List .....   | 42        |
| Mapping Login Fields .....   | 44        |
| Mapping Web Page Form Fields to Secret Fields .....                                    | 44        |
| Enabling Field Mapping with Metadata .....   | 46        |

## Table of Contents

|  |           |
|--|-----------|
| Mapping Secrets With Three or More Login Fields .....              | 47        |
| Supporting Incognito Mode .....                                    | 49        |
| Logging Out of Secret Server .....                                 | 50        |
| Using Web Password Filler with Microsoft Online Services .....     | 51        |
| Identifying the Problem .....                                      | 51        |
| Understanding the Issue .....                                      | 52        |
| Fixing the Issue When Creating the WPF Secret .....                | 52        |
| Fixing the Issue After Having Saved the WPF Secret .....           | 53        |
| Managing Port Numbers .....  | 54        |
| Accessing Websites with Self-Signed Certificates on Chrome .....   | 54        |
| Working With Self-Signed Certificates on Manifest V2 .....         | 55        |
| Working With Self-Signed Certificates on Manifest V3 .....         | 56        |
| Supporting Windows Admin Center .....                              | 57        |
| <b>Securing Web Password Filler .....</b>                          | <b>58</b> |
| Setting Up the Native Messaging Host .....                         | 58        |
| Downloading the Native Messaging Host .....                        | 58        |
| Software Requirements .....  | 58        |
| Supported Browsers .....   | 58        |
| Installing the Native Messaging Host .....                         | 58        |
| Registering the Native Messaging Host .....                        | 59        |
| Uninstalling the Native Messaging Host .....                       | 59        |
| Configuring Web Password Filler Settings .....                     | 59        |
| Establishing Default Settings and Browser-Specific Overrides ..... | 59        |
| Formatting the settings.json File .....                            | 60        |
| Excluding Sites and Making Exceptions .....                        | 64        |
| Setting UI Behavior Based on Preferences .....                     | 64        |
| Managing Error Messages .....                                      | 66        |
| Preventing Users from Disabling Session Recording .....            | 67        |
| <b>Troubleshooting .....</b>                                       | <b>68</b> |
| Addressing Usability Issues .....                                  | 68        |
| Logging in with Web Password Filler .....                          | 69        |
| Choosing a Login Method .....                                      | 69        |
| Troubleshooting Login Issues in Chrome or Edge .....               | 69        |
| Enabling Diagnostic Logging .....                                  | 69        |
| Managing Compatibility with Previous Products .....                | 70        |
| Presenting Behaviors and Problems .....                            | 70        |
| Investigating WPF Issues .....                                     | 71        |
| Confirming WPF Version .....                                       | 71        |
| Identifying the Problematic Browser .....                          | 72        |
| Identifying the Affected Sites .....                               | 72        |
| Determining Site Access .....                                      | 72        |
| Identifying the WPF Version with the Issue .....                   | 72        |
| Performing the Action .....  | 73        |

## Table of Contents

|                             |           |
|-----------------------------|-----------|
| Using Templates .....       | 73        |
| <b>Release Notes .....</b>  | <b>73</b> |
| 3.10.3 Release Notes .....  | 73        |
| Fixed Issues .....          | 73        |
| 3.10.2 Release Notes .....  | 73        |
| Bug Fixes .....             | 74        |
| 3.10.1 Release Notes .....  | 74        |
| Bug Fixes .....             | 74        |
| 3.10.0 Release Notes .....  | 74        |
| Improvements .....          | 74        |
| Bug Fixes .....             | 74        |
| 3.9.6 Release Notes .....   | 74        |
| Enhancements .....          | 75        |
| Bug Fixes .....             | 75        |
| 3.9.5 Release Notes .....   | 75        |
| Bug Fixes .....             | 75        |
| 3.9.4 Release Notes .....   | 75        |
| Improvements .....          | 75        |
| Bug Fixes .....             | 76        |
| 3.9.3 Release Notes .....   | 76        |
| Bug Fixes .....             | 76        |
| 3.9.0 Release Notes .....   | 76        |
| Improvements .....          | 77        |
| Bug Fixes .....             | 77        |
| 3.8.0 Release Notes .....   | 77        |
| Improvements .....          | 77        |
| Bug Fixes .....             | 78        |
| Known Issues .....          | 78        |
| 3.7.1 Release Notes .....   | 79        |
| Bug Fixes .....             | 79        |
| 3.7.0 Release Notes .....   | 79        |
| Features .....              | 79        |
| Improvements .....          | 79        |
| Bug Fixes .....             | 79        |
| 3.6.1 Release Notes .....   | 80        |
| Bug Fixes .....             | 80        |
| 3.6.0 Release Notes .....   | 80        |
| Features .....              | 80        |
| General Improvements .....  | 80        |
| Security Improvements ..... | 80        |
| Bug Fixes .....             | 81        |
| Known Issues .....          | 81        |
| 3.5.4 Release Notes .....   | 81        |
| Improvements .....          | 81        |

## Table of Contents

|                             |    |
|-----------------------------|----|
| Bug Fixes .....             | 81 |
| 3.5.3 Release Notes .....   | 81 |
| Features .....              | 82 |
| Bug Fixes .....             | 82 |
| 3.5.2 Release Notes .....   | 82 |
| Features .....              | 82 |
| Bug Fixes .....             | 82 |
| Known Issues .....          | 82 |
| 3.5.1 Release Notes .....   | 82 |
| Bug Fixes .....             | 82 |
| Known Issues .....          | 82 |
| 3.5.0 Release Notes .....   | 82 |
| Features .....              | 83 |
| Bug Fixes .....             | 83 |
| Known Issues .....          | 83 |
| 3.4.4 Release Notes .....   | 83 |
| Bug Fixes .....             | 83 |
| 3.4.3 Release Notes .....   | 83 |
| Features .....              | 83 |
| Security Improvements ..... | 83 |
| Bug Fixes .....             | 83 |
| 3.4.2 Release Notes .....   | 84 |
| Features .....              | 84 |
| General Maintenance .....   | 84 |
| Bug Fixes .....             | 84 |
| Known Issues .....          | 84 |
| 3.4.1 Release Notes .....   | 85 |
| Bug Fixes .....             | 85 |
| 3.4.0 Release Notes .....   | 85 |
| Features .....              | 85 |
| Product Enhancements .....  | 85 |
| Bug Fixes .....             | 85 |
| 3.3.0 Release Notes .....   | 85 |
| Features .....              | 85 |
| Bug Fixes .....             | 86 |
| iOS Specific .....          | 86 |
| 3.2.0 Release Notes .....   | 86 |
| Product Enhancements .....  | 87 |
| Bug Fixes .....             | 87 |
| Known Issues .....          | 87 |
| Browser Related .....       | 88 |
| 3.1.0 Release Notes .....   | 88 |
| Product Enhancements .....  | 88 |
| Known Issues .....          | 88 |

## Table of Contents

|  |     |
|--|-----|
| Bug Fixes .....  | 89  |
| 3.0.1 Hot Fix Release Notes .....  | 89  |
| Product Improvement .....  | 89  |
| Bug Fix .....  | 89  |
| 3.0.0 Release Notes .....  | 89  |
| Improvements .....   | 89  |
| Bug Fixes .....  | 90  |
| Known Issues .....   | 90  |
| Issue .....  | 90  |
| Issue .....  | 90  |
| The user does not have permissions to view the password in Secret Server because the View<br>Launcher Password permission is not assigned to their Role. ....                                  | 90  |
| The secret (under the Security tab) has Viewing Password Requires Edit enabled and the user does<br>not have Edit permissions (or in the older UI, Hide Launcher Password is set to Yes) ..... | 90  |
| The template used for the secret has Viewing Requires Edit enabled for the password field and the<br>user does not have Edit permissions .....   | 91  |
| 2.0.6 Release Notes .....  | 91  |
| Improvements .....   | 91  |
| Bug Fixes .....  | 91  |
| Known Issues/Limitations .....   | 91  |
| 2.0.5 Release Notes .....  | 92  |
| Features .....   | 92  |
| Bug Fixes .....  | 92  |
| Known Issues and Limitations .....   | 94  |
| Answers to FAQs .....  | 94  |
| 2.0.4 Release Notes .....  | 94  |
| Enhancements .....   | 94  |
| Bug Fixes .....  | 94  |
| Known Limitations .....  | 95  |
| 2.0.3 Release Notes .....  | 95  |
| Enhancements .....   | 95  |
| Security .....   | 96  |
| Bug Fixes .....  | 96  |
| Known Issues .....   | 96  |
| 2.0.2 Release Notes .....  | 97  |
| Enhancements .....   | 97  |
| Bug Fixes .....  | 98  |
| Known Issues .....   | 99  |
| 2.0.1 Release Notes .....  | 100 |
| Enhancements .....   | 100 |
| Bug Fixes .....  | 100 |
| 2.0.0 Release Notes .....  | 101 |
| Enhancements .....   | 101 |
| Bug Fixes .....  | 101 |
| 1.1.0 Release Notes .....  | 102 |

## Table of Contents

|                               |     |
|-------------------------------|-----|
| Enhancements .....            | 102 |
| Bug Fixes .....               | 102 |
| Firefox Specific .....        | 102 |
| 1.0.9 Release Notes .....     | 102 |
| Bug Fixes .....               | 102 |
| 1.0.8 Release Notes .....     | 103 |
| 1.0.10 Release Notes .....    | 103 |
| Enhancements .....            | 103 |
| Documentation Changelog ..... | 103 |
| November 2023 .....           | 104 |
| August 2023 .....             | 104 |
| July 2023 .....               | 104 |
| June 2023 .....               | 104 |
| May 2023 .....                | 104 |
| April 2023 .....              | 104 |
| March 2023 .....              | 104 |
| December 2022 .....           | 104 |
| September 2022 .....          | 104 |
| June 2022 .....               | 104 |
| February 2022 .....           | 104 |
| November 2021 .....           | 105 |
| October 2021 .....            | 105 |
| August 2021 .....             | 105 |
| July 2021 .....               | 105 |
| May 2021 .....                | 105 |
| March 2021 .....              | 105 |
| December 2020 .....           | 105 |
| October 2020 .....            | 105 |
| September 2020 .....          | 105 |



# Web Password Filler

Web Password Filler provides easy password autofill and lifecycle management services for web applications and web sites. It allows browsers to find and enter credentials of users, when a Delinea Platform or Secret Server instance has secrets related to that website.

The Delinea Platform and Secret Server stores credentials, as secrets, for different URLs. When you access a URL, WPF fetches the available secrets for that URL. You can then select the appropriate credential.


In addition to the login, WPF enables you to add a new secret or update an existing secret. You can use WPF to generate a strong password for a username. WPF includes a context menu for easy usage.

 **Note:** You can access the WPF extension from Secret Server too.

## Getting Started

Set up Web Password Filler in this order:

1. Verify your conventional login access to Secret Server, and confirm that web services are enabled.
2. If needed, create a folder in Secret Server where the WPF secrets will reside.
3. In Secret Server, enable Web Services.
4. Install the WPF browser extension. For more information, see "Installing Browser Extensions" on page 11
5. Configure WPF to point to the Delinea Platform and Secret Server. For more information, see [Delinea Platform and Secret Server Connection](#).

 **Note:** To ensure the WPF application works correctly with Secret Server, you need to enable Web Services in Secret Server.

## Enabling Web Services in Secret Server

---

Perform the following steps to enable Web Services in Secret Server.


1. Navigate to **Admin > Configuration > Application Settings**.
2. Verify that the **Enable Web Services** option is set to **Yes** under the **View Web Services** section.

## Connecting to the Delinea Platform and Secret Server

---

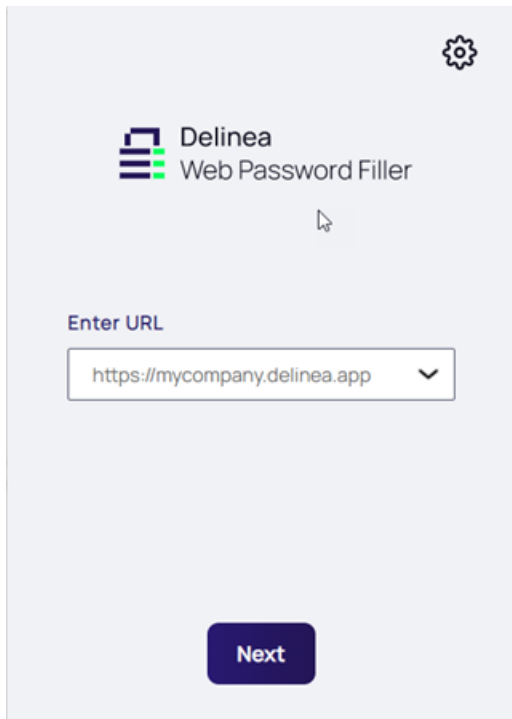
After installation, you must configure Web Password Filler to connect with the Delinea Platform or Secret Server vault of your choice by using the URL field in the WPF window.

### Connecting to the Delinea Platform

1. Open the browser in which you have installed Web Password Filler.
2. Click the  icon to open Web Password Filler. The WPF login window appears.

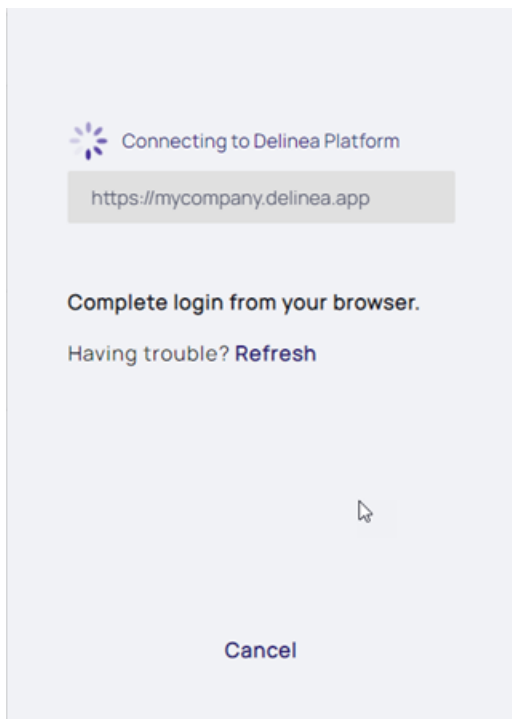
## Getting Started

3. Enter your Delinea Platform URL and click **Next**



The screenshot shows the Delinea Web Password Filler interface. At the top left is the Delinea logo, consisting of three horizontal bars (blue, green, blue) to the left of the text "Delinea" and "Web Password Filler" below it. A gear icon is in the top right corner. Below the logo is a text input field labeled "Enter URL" containing the text "https://mycompany.delinea.app" and a dropdown arrow. At the bottom center is a dark blue button with the text "Next".

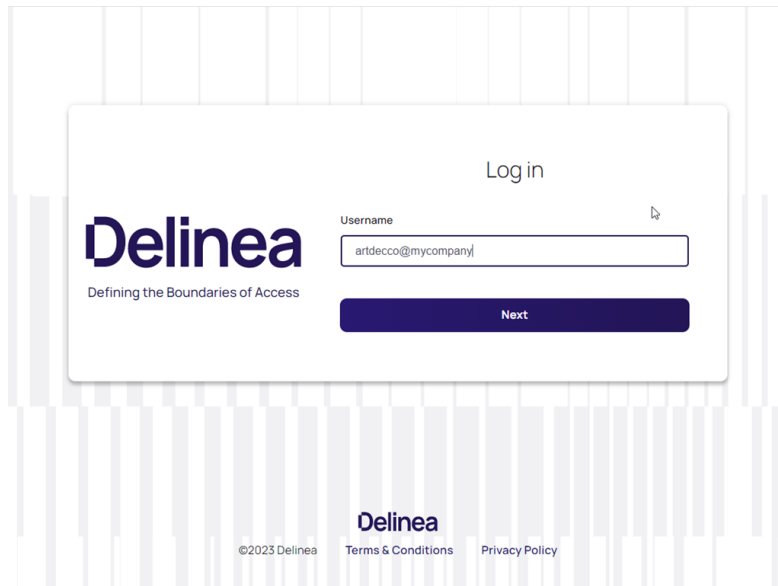
4. Proceed to your browser to complete login



The screenshot shows the "Connecting to Delinea Platform" screen. At the top left is a loading spinner icon followed by the text "Connecting to Delinea Platform". Below this is a grey box containing the URL "https://mycompany.delinea.app". In the center, the text reads "Complete login from your browser." followed by "Having trouble? Refresh" with a blue link. At the bottom center is a blue button with the text "Cancel".

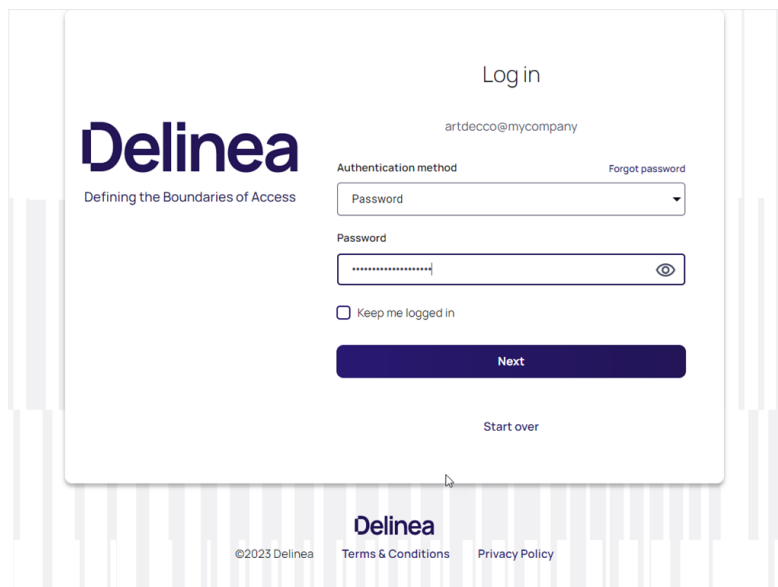
## Getting Started

5. If required, enter your Username and click **Next**



The screenshot shows the Delinea login interface. On the left is the Delinea logo with the tagline "Defining the Boundaries of Access". The main heading is "Log in". Below it is a "Username" label and a text input field containing "artdecco@mycompany". A dark blue "Next" button is positioned below the input field. At the bottom of the page, there is a footer with the Delinea logo, "©2023 Delinea", and links for "Terms & Conditions" and "Privacy Policy".

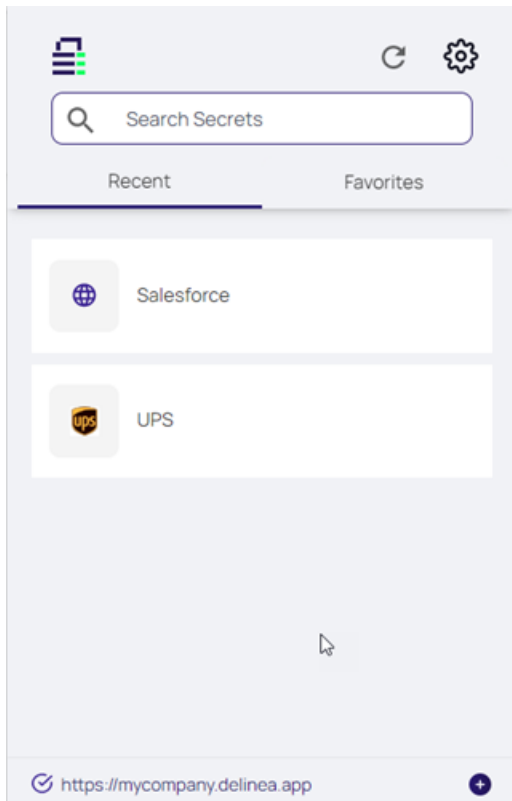
6. If required, select an authentication method, enter your credentials and click **Next**



The screenshot shows the Delinea login interface after the username step. The "Log in" heading is present, followed by the username "artdecco@mycompany". Below this is an "Authentication method" dropdown menu set to "Password" and a "Forgot password" link. A "Password" label is above a text input field containing masked characters and a toggle icon. A "Keep me logged in" checkbox is below the password field. A dark blue "Next" button is at the bottom of the form, and a "Start over" link is below it. The footer at the bottom of the page includes the Delinea logo, "©2023 Delinea", and links for "Terms & Conditions" and "Privacy Policy".

## Getting Started


7. You are now logged in

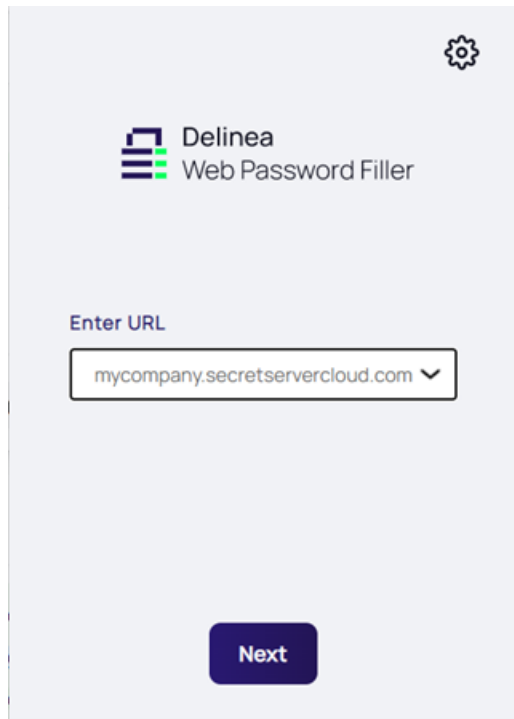


## Connecting to Secret Server

To connect WPF with Secret Server complete the following:

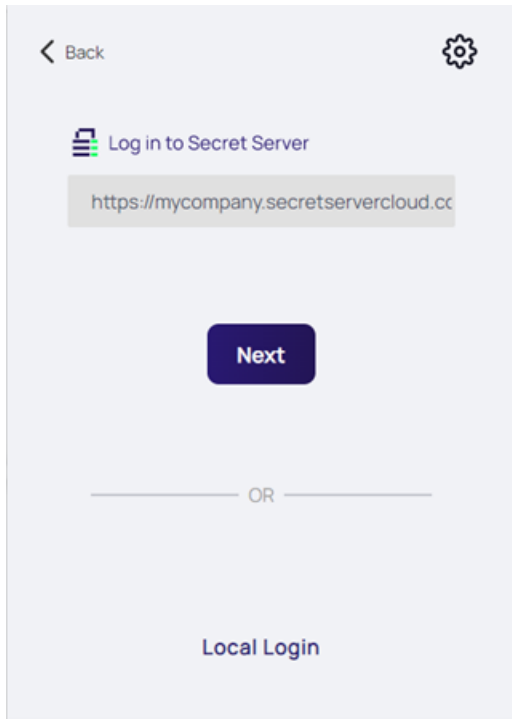
## Getting Started

1. Open the browser in which you have installed Web Password Filler.
2. Click the **Web Password Filler**  icon to open Web Password Filler:

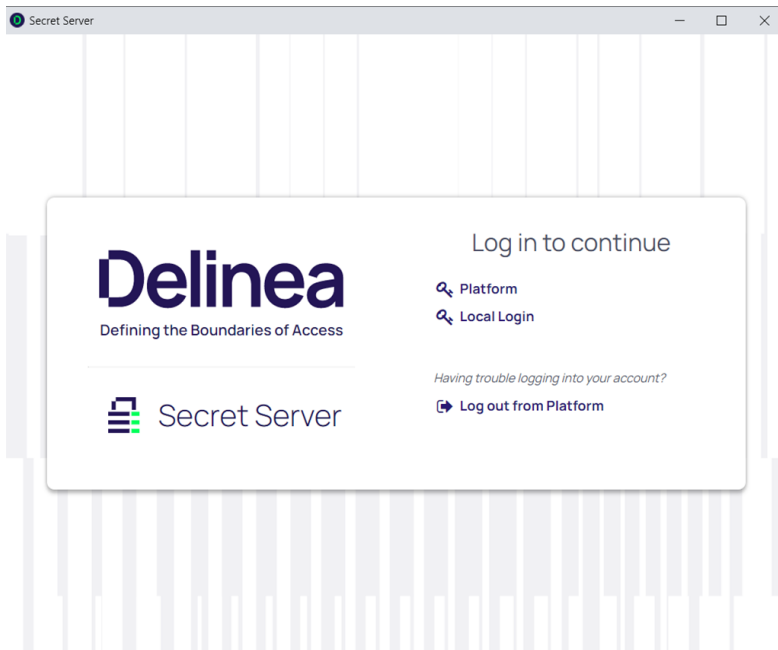


3. Enter your Secret Server URL, for example: `https://mycompany.secretservercloud.com` then click **Next**
4. You can sign in with any of your configured login methods. To use the web login, click **Next**

## Getting Started



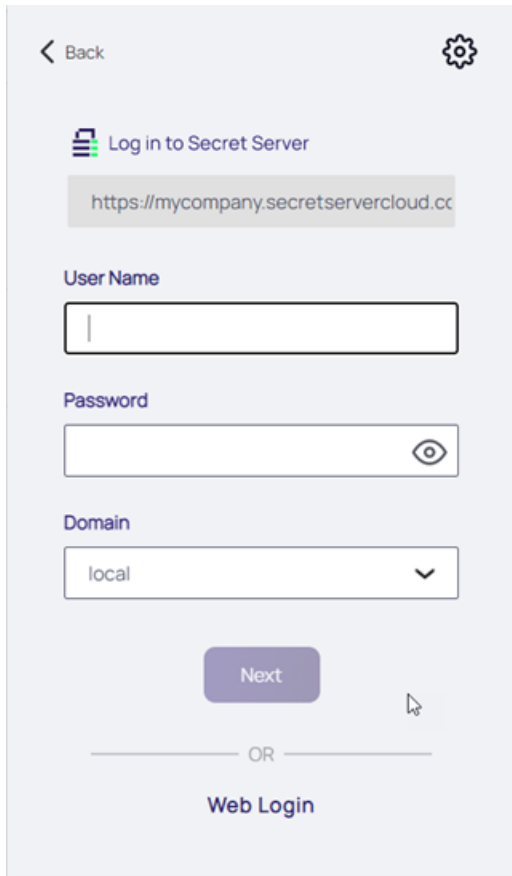
5. Proceed to the browser to complete the login



### Logging in Locally

If you selected **Local Login** in Step 4 of the previous section, enter your Username and Password to login.

## Getting Started

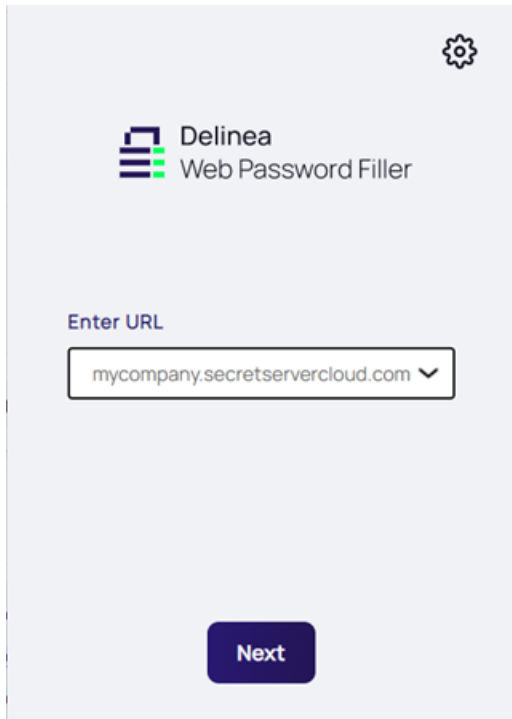


The screenshot shows a mobile application interface for logging into a Secret Server. At the top left is a back arrow and the text 'Back'. At the top right is a gear icon for settings. Below this is the title 'Log in to Secret Server' with a server icon. A text input field contains the URL 'https://mycompany.secretservercloud.cc'. Below the URL are three input fields: 'User Name' (empty), 'Password' (empty with an eye icon for visibility), and 'Domain' (a dropdown menu showing 'local'). A purple 'Next' button is positioned below the domain field. Below the 'Next' button is a horizontal line with 'OR' in the center, and the text 'Web Login' is centered below the line.

## Specifying Default Protocols

If you do not specify a protocol in the Secret Server URL, Web Password Filler will use *https://* by default.

## Getting Started



The screenshot shows the Delinea Web Password Filler interface. At the top right is a gear icon. The Delinea logo and 'Web Password Filler' text are centered. Below is a text input field labeled 'Enter URL' containing the text 'mycompany.secretservercloud.com'. A 'Next' button is located at the bottom of the form.

If you click **Next**, Web Password Filler assumes *https://* is the correct protocol and proceeds as if you had prefixed *https://*.

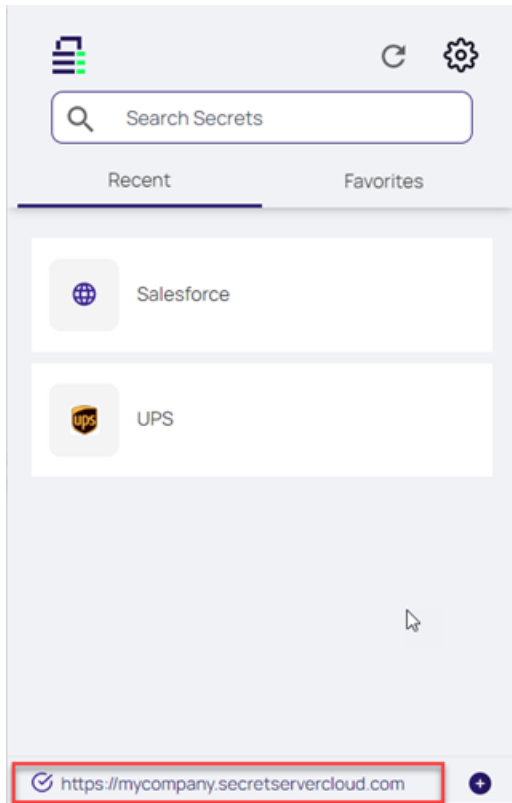
 **Note:** If you specify a protocol, Web Password Filler uses it.

### Redirecting to Secret Server via Hyperlink

When connected to the Delinea Platform or Secret Server vault, Web Password Filler displays the URL at the bottom. Clicking this link takes you to the Delinea Platform or Secret Server vault site.



## Getting Started



## Reviewing Terminology

This section will review and clarify the terms used for each browser add-on to help eliminate any potential confusion, providing some visual points.

### Using Web Password Filler with Secret Server


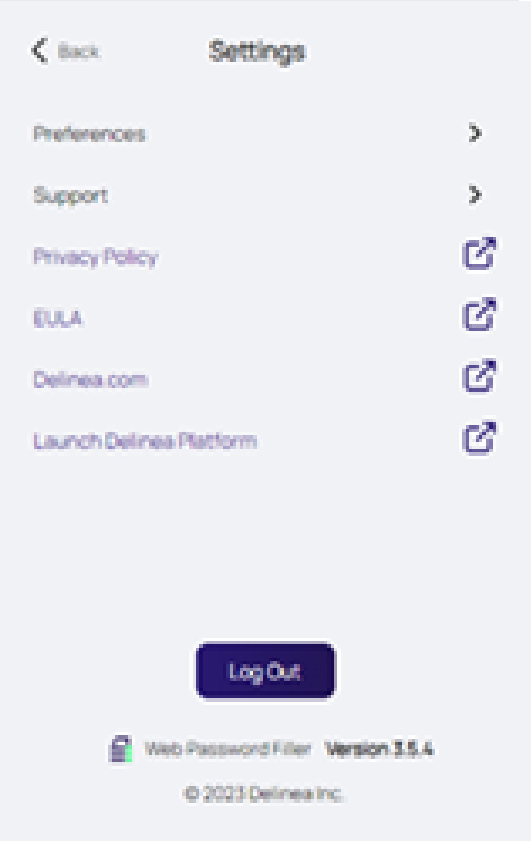
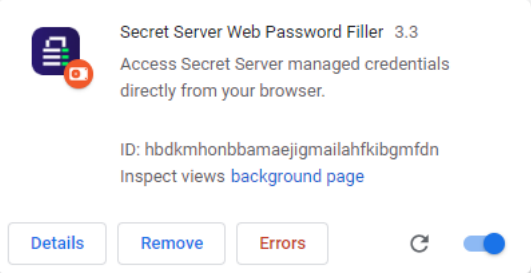
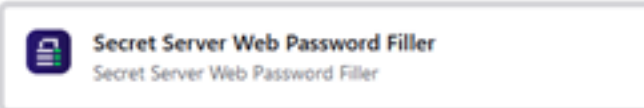
The new Web Password Filler browser extension is included in Secret Server version 10.7.59 and later. Typically, this is referred to as one of the following:

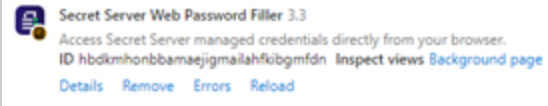
- WPF
- Web Password Filler
- Password Filler

In a browser, you will see the following:

| State      | Location/Browser      | Example  |
|------------|-----------------------|--|
| Logged Out | (In top right corner) |  |

## Getting Started

| State                                  | Location/Browser      | Example  |
|--|-----------------------|--|
| Logged In                              | (In top right corner) |    |
| Application in Browser (Settings Menu) |                       |   |
| Item on Extensions / Add-On page       | Chrome                |  |
|  | Firefox               |  |

| State | Location/Browser        | Example  |
|-------|-------------------------|--|
|       | Edge (chromium version) |  |

## Installing Browser Extensions


---

Install one of the supported browser extensions as described below to use Web Password Filler:

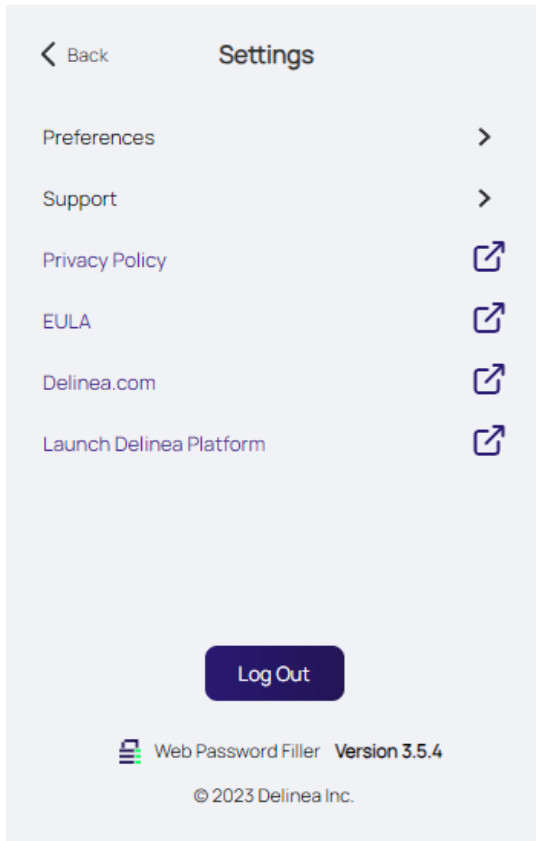
- **Chrome:** Install the extension in one of the following ways:
  - Click the Web launcher icon in a Web Password secret.
  - Download the extension from the Google Chrome add-ons site, located here, [Chrome Web Store](#).  
For more information on securely managing Chrome extensions at scale, see [Managing Extensions in Your Enterprise](#).
- **Edge Chromium:** Install the extension by downloading it from the Microsoft Edge add-ons site, located here [Microsoft Add-ons](#).
- **Firefox:** Install the extension by clicking the Web launcher icon in a Web Password secret, or by downloading it from the Firefox add-ons site, located here, [Firefox Browser Add-ons](#).
- **Safari:** Install the extension by downloading it from '[Use Safari Extensions on your Mac](#)'. For more information, see the notes in the list below:
  - WPF supports Safari running on macOS Monterey and Big Sur 11.1.0, 11.2.1 and later.
  - WPF does not support the Native Messaging Host configuration in Safari browsers.
  - The Safari browser extension does not support Windows Admin Center.
  - Safari 15 and above do not support session recording.

## Navigating the Preferences Menu

---

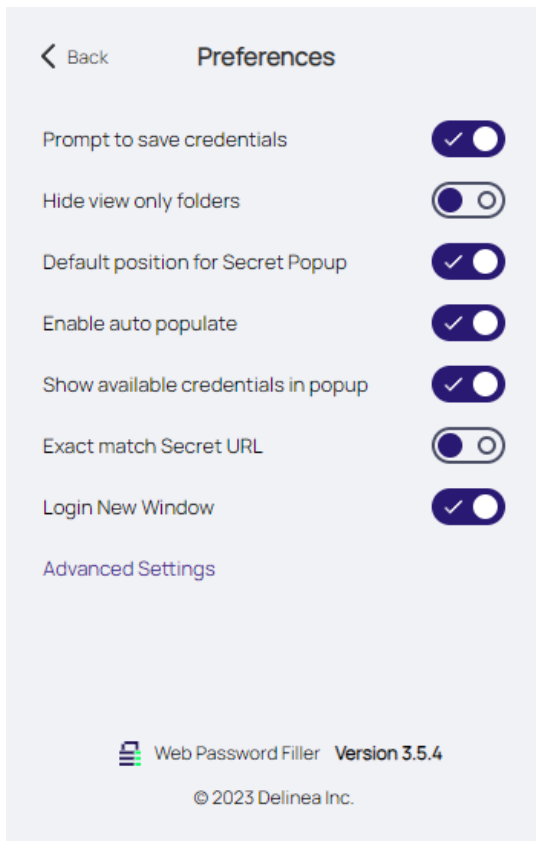
When you are already logged into Web Password Filler, click the WPF icon  The **Settings** screen appears.

## Getting Started



Click **Preferences**. The Preferences screen appears.

## Getting Started



- **Prompt to save credentials:** Select this preference if you want WPF to prompt you to save your login credentials for future logins. Not recommended for shared systems. The prompt only appears if an existing secret is updated, or if a user enters credentials for a site and no Secret was used.
- **Hide view only folders:** Select this preference to prevent users from seeing folders to which they have read access only.
- **Show available credentials in popup:** Select this preference to have available credentials will be displayed in a pop-up dialog.
- **Default position for Secret Popup:** Select this preference to have the Secret popup appear at the top right of the screen. The non-default position is under the Delinea check symbol.
- **Enable auto populate:** Select this preference so that when a Secret is available for a web page, WPF will automatically populate the fields on the page.
- **Exact match Secret URL Exact match.** Select this preference to ensure that WPF populates fields only if the URL exactly matches the URL specified in the Secret, and will not populate fields on variations of the URL, including sub-pages.
- **Secret Server Login New Window.** Web Password Filler can now be configured to have the Secret Server Login Window open in a new browser tab when the user disables or turns off the setting "Secret Server Login New Window."

## Using WPF

- **Advanced Settings > Session Recording Limit** Select this preference to enable setting session recording limits through the UI in hourly increments, from one to eight hours. The default limit is two hours.
- **Advanced Settings > Input Threshold.** Input Threshold is a safety feature that helps Web Password Filler work smoothly on most websites. It sets a limit on how many input fields WPF will check on a page. By default, WPF looks at up to 10 input fields on a page. If there are more than 10, it stops checking to avoid slowing down the website. Increasing this number might slow down some websites.

## Using WPF

Once Web Password Filler is set up and you are logged into the Delinea Platform or Secret Server, you can use WPF to log in to websites for which Secrets are managed via the Delinea Platform or Secret Server.

Refer to [Creating a Secret for a Website](#) if you need to add new accounts.

### Logging in to a Website

---

1. Take a quick look at your WPF button on your browser's button bar. If it is grayed out, you will need to sign into Secret Server and return here.
2. Navigate to the website you want to access. Note there is a purple and green Delinea logo in the site's account name text box:

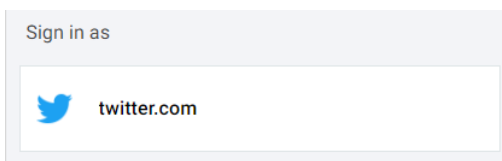
### Sign in



The image shows a sign-in form with two input fields. The top field is labeled 'Email address' and contains a placeholder with a purple and green lock icon on the right. The bottom field is labeled 'Password' and contains a placeholder with a purple and green lock icon on the right.

 **Note:** If you are signed into Web Password Filler and do not see the purple and green lock in the username text box, try refreshing the web page to make it appear.

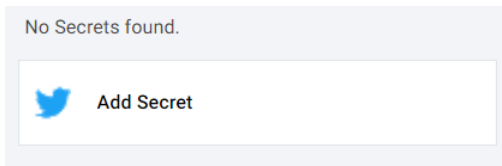
3. Click the **Delinea logo**. A Web Password Filler pop-up opens and one of two things can happen:
  - If you have one or multiple existing secrets for a site, a pop-up will open displaying all of the available secrets available for the site.



The image shows a 'Sign in as' pop-up window. It has a title bar that says 'Sign in as'. Below the title bar, there is a list of secrets. The first secret is for 'twitter.com' and is accompanied by the Twitter logo.

## Using WPF

- If you have no secrets related to the site, then a pop-up will open to give you the option to add a new secret:



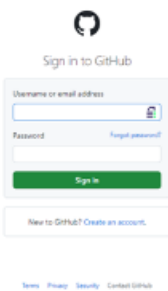
If you see the second possibility, you need to set up a secret for that website. See [Creating a Secret for a Website](#).

4. Click the button for the desired secret, and you are signed in.

## Accessing Secrets Guarded by MFA

---

You can access secrets guarded by MFA through Web Password Filler on the Delinea Platform. When you attempt to login to a portal guarded by MFA, you will see a pop-up that they must complete an additional MFA challenge:



After clicking **Challenge**, you will be redirected to the Delinea Platform portal to complete the MFA challenge. When you have successfully completed the MFA challenge, you can return back to Web Password Filler to view or launch the secret.



## Sign in to GitHub

Username or email address

Password [Forgot password?](#)

[Sign in](#)

[New to GitHub? Create an account.](#)

[Terms](#) [Privacy](#) [Security](#) [Contact GitHub](#)

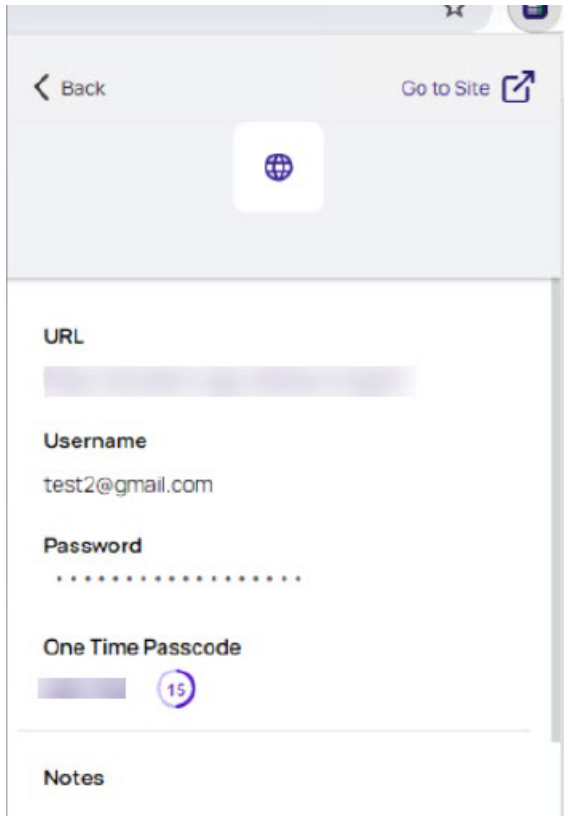
## Autofilling OTP

---

Web Password Filler can now auto fill OTP (time-based one-time passcode or TOTP). When a login form or a login process step prompts you to enter an OTP, and you have configured the secret to generate an OTP code, Web Password Filler will automatically put the current OTP code in the field. When the OTP code expires, it will automatically update the field with the new OTP until you submit the login.



## Using WPF




The screenshot shows a mobile application interface for a web password filler. At the top, there is a navigation bar with a 'Back' button on the left and a 'Go to Site' button with a globe icon on the right. Below the navigation bar is a header area with a globe icon. The main content area contains a form with the following fields:

- URL**: A text input field with a blurred value.
- Username**: A text input field containing 'test2@gmail.com'.
- Password**: A text input field with masked characters represented by dots.
- One Time Passcode**: A text input field with a timer icon showing '15' seconds.
- Notes**: A section at the bottom of the form.

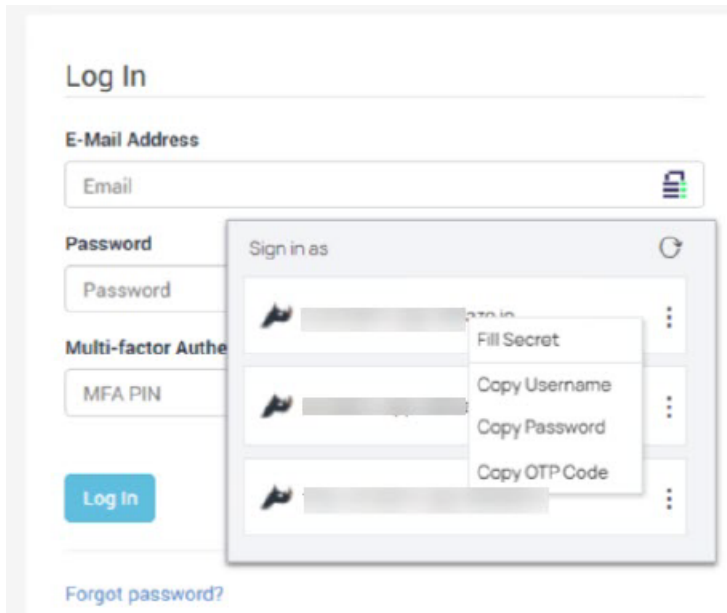
If you do not see Web Password Filler automatically identify an OTP field, you have the option to manually copy and paste the OTP from the secret.

To copy the OTP, complete the following steps:

1. Right-click anywhere on the page and select **Web Password Filler** from the context menu.
2. Select the secret's name and click **Copy OTP**.

 **Note:** You can copy the username and password from this menu, copy them from the details view, or autofill the secret.

However, when you manually paste OTP codes, they will not update automatically. Therefore, you must ensure you are using a current code before submitting the form.



For more information on how to set up OTP on secret templates, see [Enabling OTPs for Launchers](#).

## Recording Web Sessions

Web Password Filler supports Session Recording for web sessions. To record a web session, you must enable Session Recording in the Security settings of the Secret in Secret Server.


When you launch a Secret that has Session Recording enabled, or when you navigate to a web page and select a Secret that you have enabled Session Recording for, the recording begins as soon as the credentials are filled into the login fields (Username/Password, etc.).

Once the session recording starts, you should see a notification message pop up at the upper right side of the browser window indicating that recording has begun. Unless the security settings on the secret hide it, the logo on the tab will alternate between the site logo and the recording icon.

When recording web sessions, the system will limit the recording to the exact match for the domain. It will not record anything *not* included in the exact URL. For example, if you set a Secret with session recording has the URL value `https://delinea.company.com/`, the system will only record browser tabs opened for that URL. If the login page then redirects to `https://company.com`, the system will no longer record the session because the subdomain has changed.

Likewise, you might be recording a session in a tab opened to `https://delinea.company.com`. You then open a second tab to `https://delta.company.com`, which happens to use the same domain as the first tab (`company.com`). When the second tab opens, it becomes the tab 'in focus' and the session recording continues on the second tab. If you wish to keep recording on the original tab, we recommend opening the second tab in an incognito window or in a separate browser session.


If you have session recording enabled for two Secrets that contain the same primary or secondary domain such as `microsoftonline.com` and the same host name (`microsoftonline.com`), AND you are using both secrets when you select the second session, WPF will close the first session and tabs associated with the first Secret.

 **Note:** This is also true for two Secrets with different hosts but the same base domain.

## Using WPF

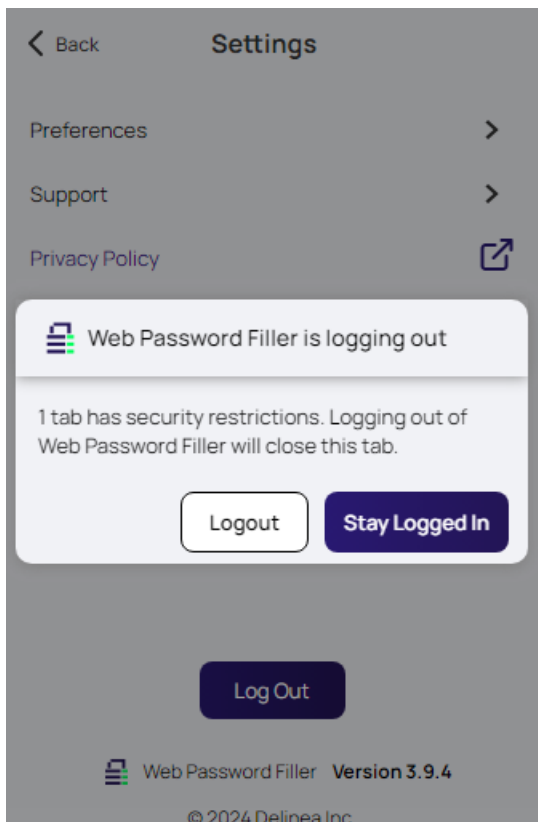
This expected behavior ensures that the system only records sessions associated with Secrets that require session recording. Sites like *microsoftonline* allow only one login / active credential at a time. If you enable session recording for two secrets that do not contain a primary / secondary domain address (such as .net, .com, .co), the system will record both sessions independently. For instance, *red.local.something* differs from *blue.local.something* because 'something' is neither a primary domain nor secondary domain identifier.

The system now treats IP Addresses as entirely unique address (e.g. 10.0.0.61 is not the same as 10.0.0.51) and records them independently.

 **Note:** Chrome versions 92 and newer throttle the number of screenshots per second and may cause impacts to the recording, such as jumpy video or missed keystroke captures.

## Session Recording Disconnecting Warning

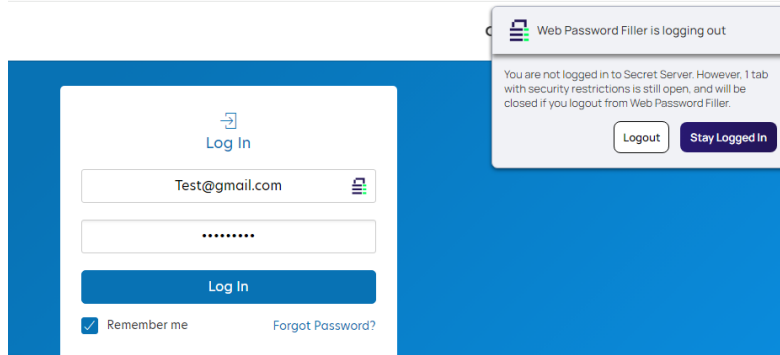
If Web Password Filler has launched any sessions that it is recording, and you log out of Web Password Filler, those sessions must end. We have added a warning to give users the option to stay connected if possible.




This warning can occur in the following circumstances:

- The user logs out of Web Password Filler.
- The user has a tab open to the same Secret Server or platform that Web Password Filler is currently logged into. They then log out of the web tab.

## Using WPF



- The user has a tab open to the same Secret Server or platform that Web Password Filler is currently logged into and that tab times out due to inactivity.

 **Note:** The inactivity timer suspends when the tab is not active. However, if the user switches back to the tab and it has timed out, the system will raise a timeout and log the user out of both the tab and Web Password Filler.

- The user launches a web session from a different Secret Server or platform instance, requiring Web Password Filler to switch login context to the new server. In this case, the system must end recorded sessions to the old server.

Web Password Filler is currently logged into a different Secret Server. There is 1 open tab with security restrictions set by the current Secret Server. This tab will be closed if you switch.

Switch and continue?

**Delinea**

Cancel

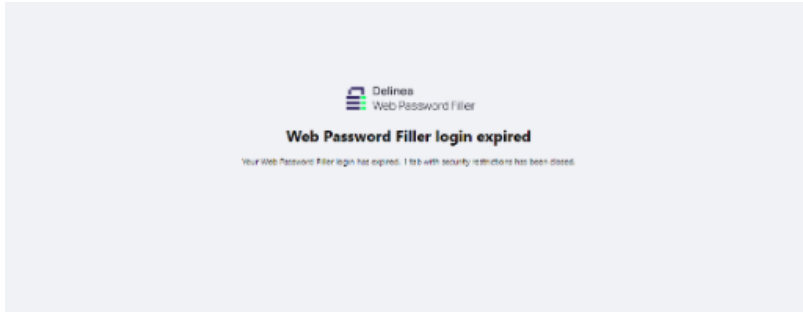
Switch & Launch

- The authentication token used by Web Password Filler expires and cannot be renewed.

In the first four cases above, the user will receive a message explaining that the system will log out Web Password Filler and close any recorded sessions. The user will have the option to continue and close the tabs, or cancel the Web Password Filler log out. If the system logs out Web Password Filler because the user has logged out of the Secret Server or platform tab, then that tab will stay logged out, but Web Password Filler will remain logged in, allowing the session recordings to continue.

In the fifth case, Web Password Filler cannot stay logged in. The system will display a warning message that will not give the option to continue and keep the recorded sessions open. Those sessions will immediately close, and the user must log into Web Password Filler again to get a new authentication token.

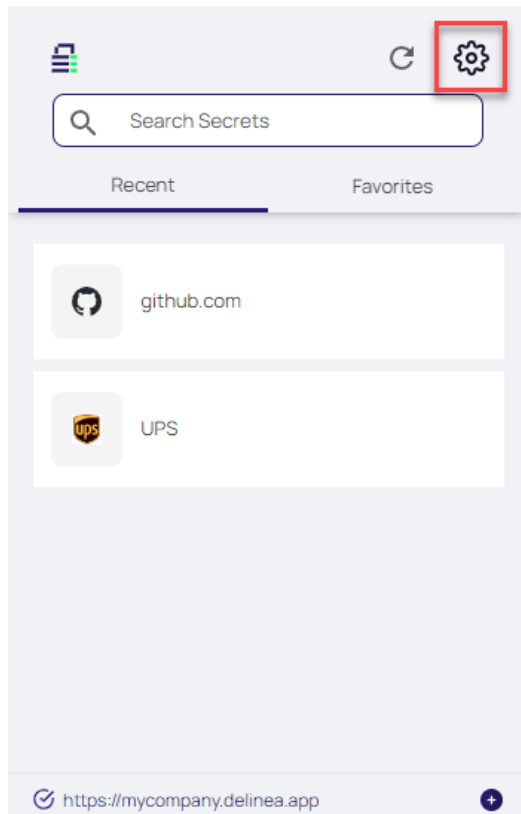
## Using WPF



## Enabling Mouse Path Tracking On Recordings

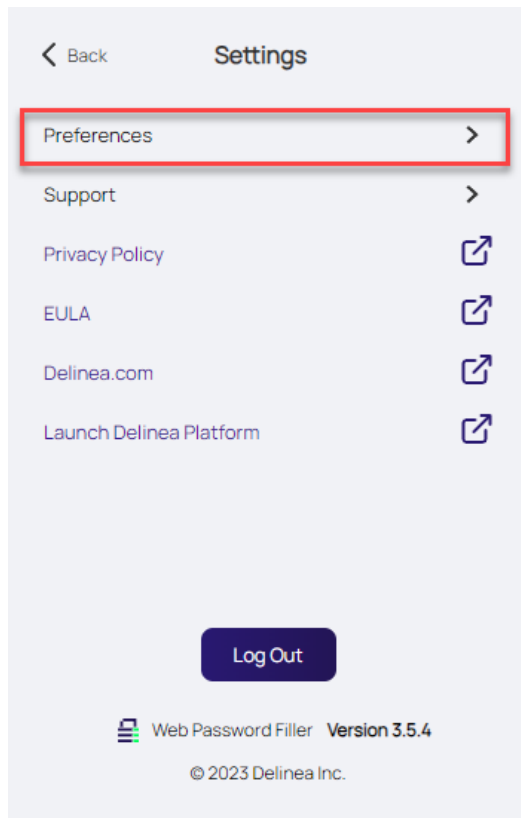
Users can enable mouse path tracking on session recordings by following these steps:

1. Click the **Settings** icon



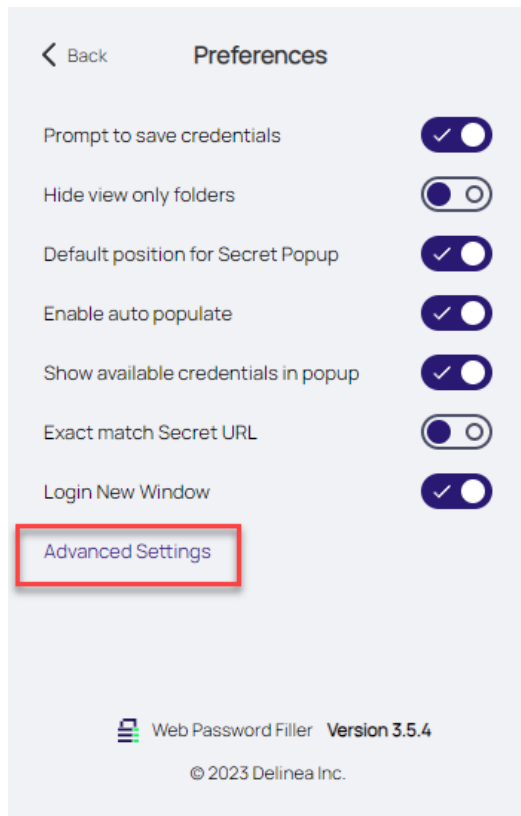
2. Click **Preferences**

## Using WPF



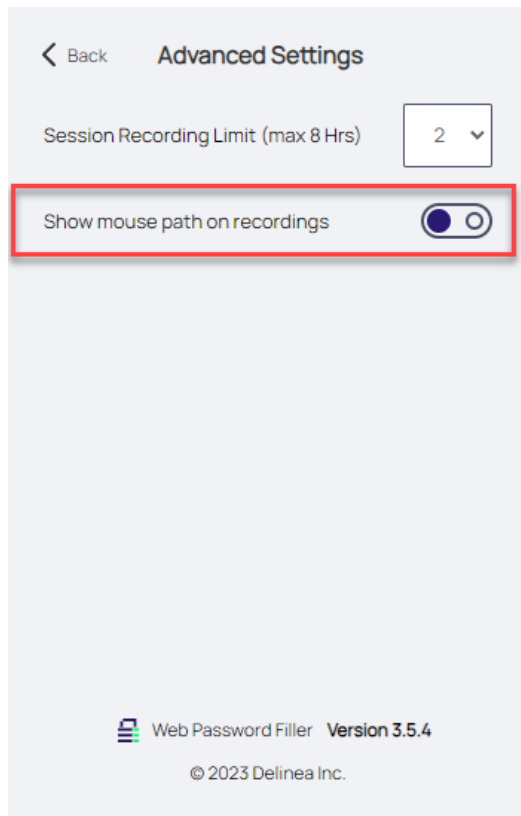
### 3. Click **Advanced Settings**

## Using WPF



4. Enable the **Show mouse path on recordings** toggle

## Using WPF



### Managing Session Recording Limits


Each session has a default maximum recording time of two hours, regardless of how many tabs you have open. If you start session recording on *red.delinea.com*, and then open a tab for *blue.delinea.com*, session recording will continue on *blue.delinea.com* when you focus on it. By default, the system will stop session recording after two hours and close both tabs. You can extend this session recording limit to a maximum of eight hours by configuring the [Native Messaging Host](#) file.

If you want to capture other sites with different subdomains that launch from the same Secret, you must use RegEx to configure the Secret to include the other URLs.

### Using RegEx

RegEx provides a sequence of patterns that Secret Server templates specify and that you can enter as **OtherUrls** during account setup in Web Password Filler. This allows you to record sessions on redirected websites.

When you log into a website using a secret and have session recording enabled, WPF will record a session for that URL. If the website redirects you to another URL and you want session recording to continue for the redirected URL, you can those URLs in the **OtherUrls** field when you add the account. Currently, this field supports only URLs.

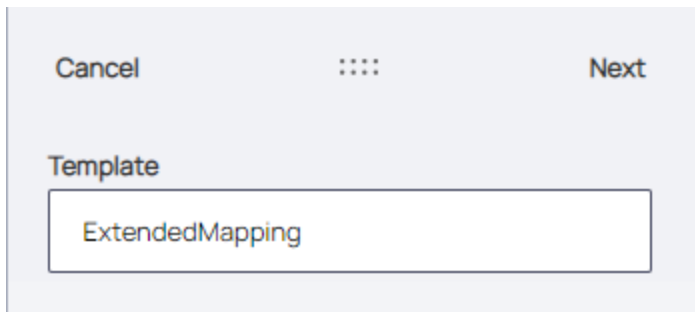
 **Note:** As soon as you access a URL for a website using a secret with session recording enabled, the system will capture everything you do. This includes any actions you take to change the password for that secret.



## Using WPF

### Using RegEx in WPF

1. To add a new secret via WPF, select a Secret Server template that has the RegEx field.

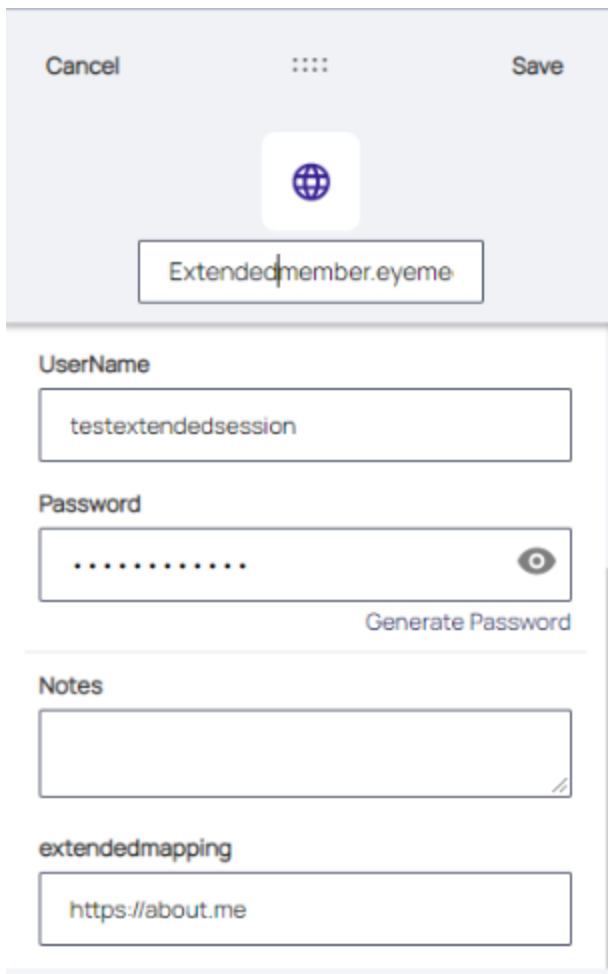


Cancel      ⋮      Next


Template

ExtendedMapping

2. Click **OK**.
3. In the new **Add Account to Secret Server** dialog, add the required details.



Cancel      ⋮      Save




Extendedmember.eyeme

UserName

testextendedsession

Password

..... 

Generate Password

Notes

extendedmapping

https://about.me

Enter any other URL in the **Extended Mapping** field for which you should enable session recording, in case the

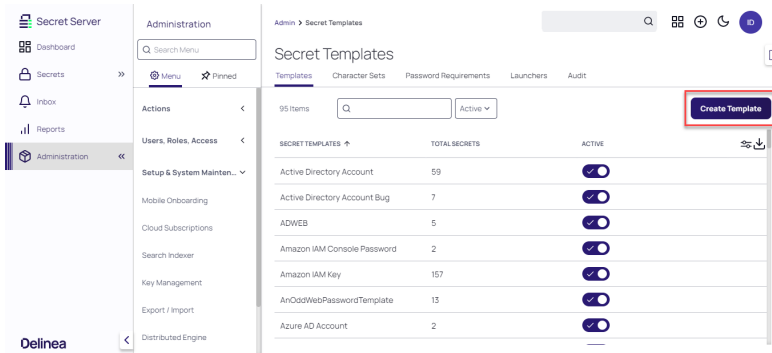
## Using WPF

user gets redirected to those URLs.

4. Click **Save**.

## Setting Up Templates in Secret Server

1. Sign into Secret Server and navigate to **Admin > Secret Templates**.



2. Click **Create Template**.
3. Name the new template and click **Save**.

### Create Template

Name your new Secret Template, or import one from an XML file.

New / Import \*  New  Import XML

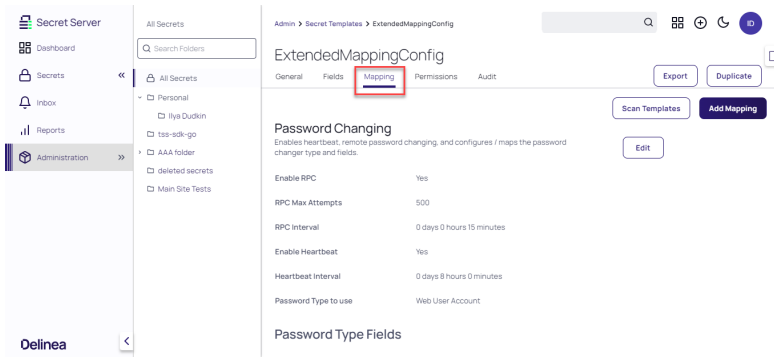
Template Name \*

Cancel

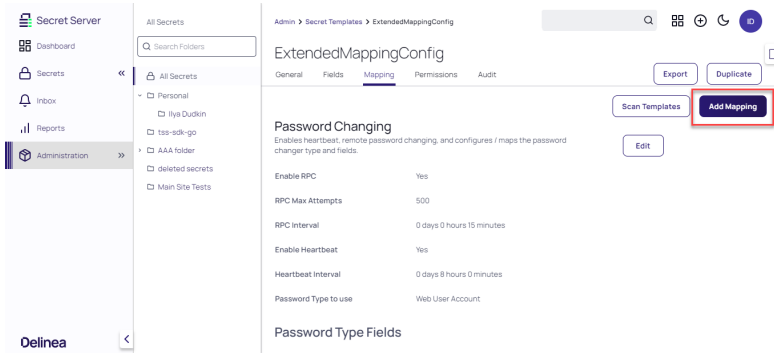
Save

4. Inside the secret template, click **Mapping**.

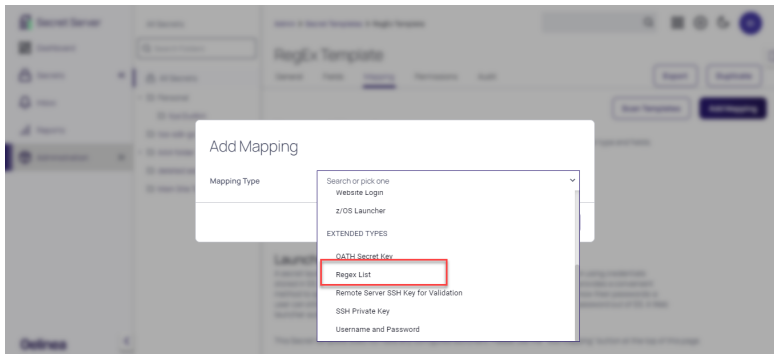
## Using WPF



5. In the **Mappings** page, click **Add Mapping**.

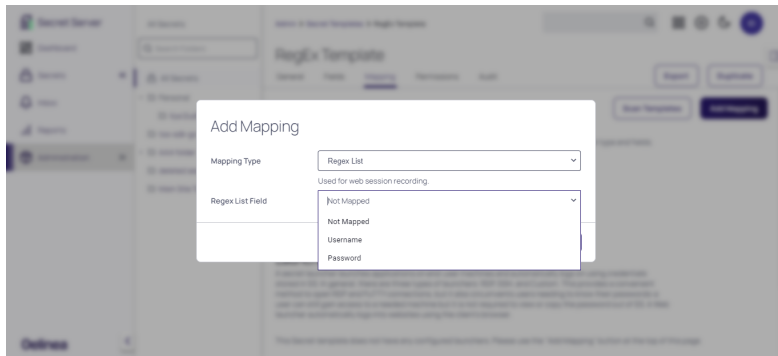


6. From the **Mapping Type** drop-down, select **Regex List**



7. From the **Regex List Field** drop-down, select the fields you would like to map.

## Using WPF




### 8. Click **Save**.

You can now use the template in WPF.

If you enable session recording for two secrets that contain the same primary or secondary domain (e.g. *microsoftonline.com*) and the same host name (e.g. *microsoftonline.com*), and you use both secrets, WPF will close the first session when you select the second session. It will also close the tabs associated with the first secret. This ensures that WPF only records sessions associated with secrets that require session recording. Sites like *microsoftonline.com* only allow one login/active credential at a time.

If you have session recording enabled for two secrets that do not contain a primary / secondary domain address (e.g. *.net*, *.com*, *.co.in*), both secrets will be recorded independently. For instance, *red.local.something* is not the same as *blue.local.something* because 'something' is neither a primary domain or secondary domain identifier.

IP Addresses are now treated as an entirely unique address (e.g. 10.0.0.61 is not the same as 10.0.0.51) and will be recorded independently.

 **Note:** WPF records sessions for the account that logged directly into the Windows Admin Center. However, WPF **cannot** record RDP sessions that you log into after that initial login. This is because the main browser window still refers to the Windows Admin Center URL, and **not** to the RDP window nested inside the browser page.

## Exploring Resolution Sizes

In the sections below, you will find the supported screen resolution sizes for session recording for both Windows and Mac. The tables also include information on display scaling percentages and which display sizes are supported in each browser.

### Determining Supported Screen Resolution Sizes for Windows

| Display Resolution | Display Scaling in % | Does WPF support Session Recording on Browser |      |         |
|--------------------|----------------------|---|------|---------|
|                    |                      | Chrome  | Edge | Firefox |
| 1920*1080          | 100                  | Yes   | Yes  | Yes     |
|                    | 125                  | Yes   | Yes  | Yes     |

## Using WPF

| Display Resolution | Display Scaling in % | Does WPF support Session Recording on Browser |     |     |
|--------------------|----------------------|---|-----|-----|
|                    | 150                  | Yes   | Yes | Yes |
|                    | 175                  | Yes   | Yes | Yes |
| 1680*1050          | 100                  | Yes   | Yes | Yes |
|                    | 125                  | Yes   | Yes | Yes |
|                    | 150                  | Yes   | Yes | Yes |
|                    | 175                  | Yes   | Yes | Yes |
| 1600*900           | 100                  | Yes   | Yes | Yes |
|                    | 125                  | Yes   | Yes | Yes |
|                    | 150                  | Yes   | Yes | Yes |
|                    | 175                  | N/A   | N/A | N/A |
| 1440*900           | 100                  | Yes   | Yes | Yes |
|                    | 125                  | Yes   | Yes | Yes |
|                    | 150                  | Yes   | Yes | Yes |
|                    | 175                  | N/A   | N/A | N/A |
| 1366*768           | 100                  | Yes   | Yes | Yes |
|                    | 125                  | Yes   | Yes | Yes |
|                    | 150                  | N/A   | N/A | N/A |
|                    | 175                  | N/A   | N/A | N/A |
| 1280*1024          | 100                  | Yes   | Yes | Yes |
|                    | 125                  | Yes   | Yes | Yes |
|                    | 150                  | Yes   | Yes | Yes |
|                    | 175                  | N/A   | N/A | N/A |
| 1280*800           | 100                  | Yes   | Yes | Yes |

## Using WPF

| Display Resolution | Display Scaling in % | Does WPF support Session Recording on Browser |     |     |
|--------------------|----------------------|---|-----|-----|
|                    | 125                  | Yes   | Yes | Yes |
|                    | 150                  | N/A   | N/A | N/A |
|                    | 175                  | N/A   | N/A | N/A |
| 1280*720           | 100                  | Yes   | Yes | Yes |
|                    | 125                  | N/A   | N/A | N/A |
|                    | 150                  | N/A   | N/A | N/A |
|                    | 175                  | N/A   | N/A | N/A |
| 1024*768           | 100                  | Yes   | Yes | Yes |
|                    | 125                  | Yes   | Yes | Yes |
|                    | 150                  | N/A   | N/A | N/A |
|                    | 175                  | N/A   | N/A | N/A |
| 800*600            | 100                  | Yes   | Yes | Yes |
|                    | 125                  | N/A   | N/A | N/A |
|                    | 150                  | N/A   | N/A | N/A |
|                    | 175                  | N/A   | N/A | N/A |

### Determining Supported Screen Resolution Sizes for Mac

| MAC OS   | Display Resolution | Browser |
|----------|--------------------|---------|
|          |                    | Chrome  |
| Monterey | 1280*1024          | Yes     |
|          | 1024*768           | Yes     |
| BigSur   | 1024*768           | Yes     |

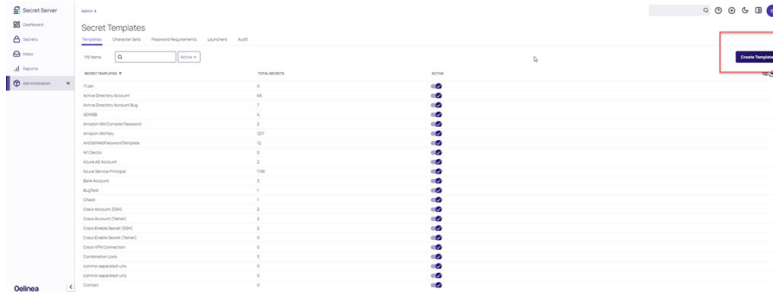
### Launching Comma-Separated URLs

When you save multiple URLs under the URL field for a secret, the system displays these URLs in a dropdown list on a new row. You can select and launch your desired URL using the custom web launcher.

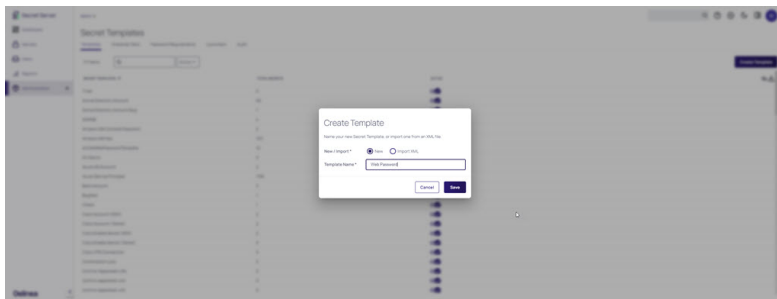
## Creating a Secret Template

To use the custom web launcher, you first need to create a secret template:

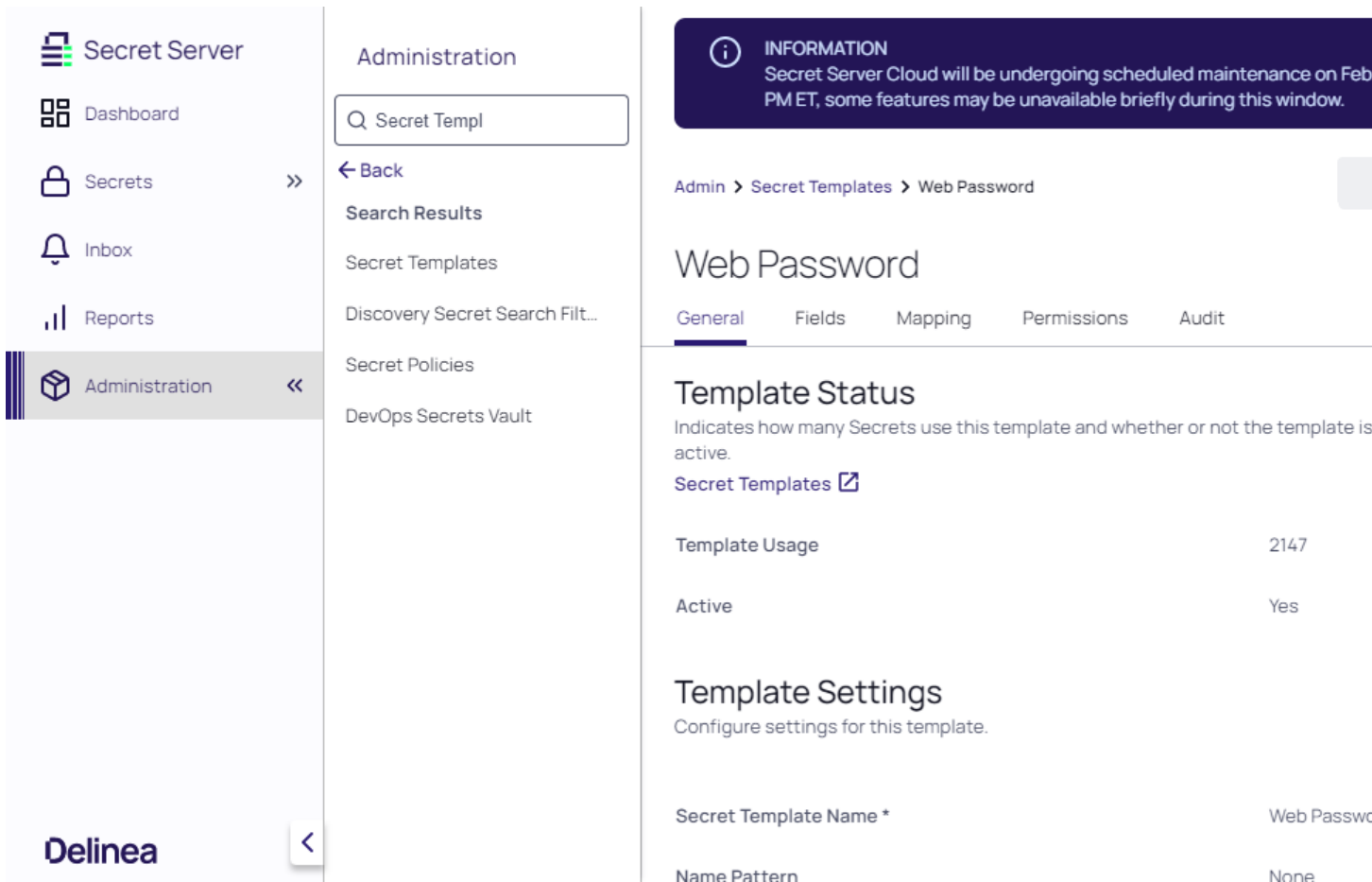
1. In the **Secret Templates** tab inside Secret Server, click **Create Template**.



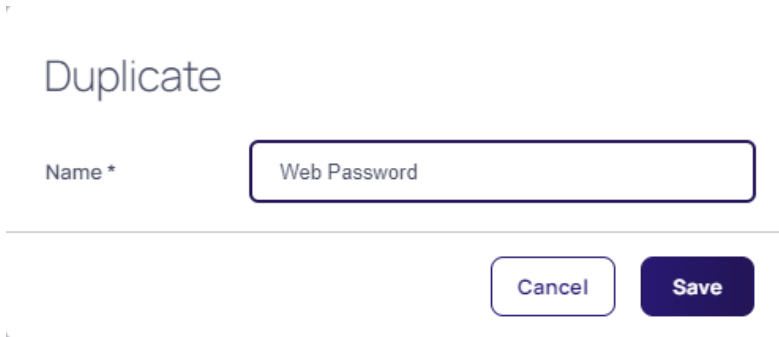
2. Give the new template a name and click **Save**.



3. In the **Secret Templates** tab inside Secret Server, find the secret template you just created and click **Duplicate**.



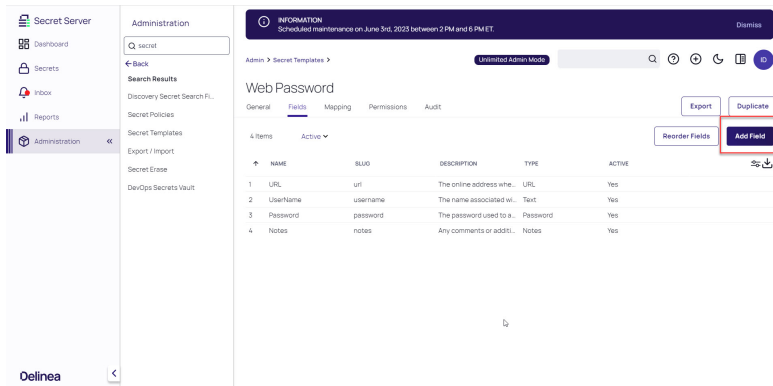
- 4. Choose a name for the duplicate template and click **Save**.




- 5. Inside the duplicate template, navigate to the **Fields** tab and click **Add Field**.

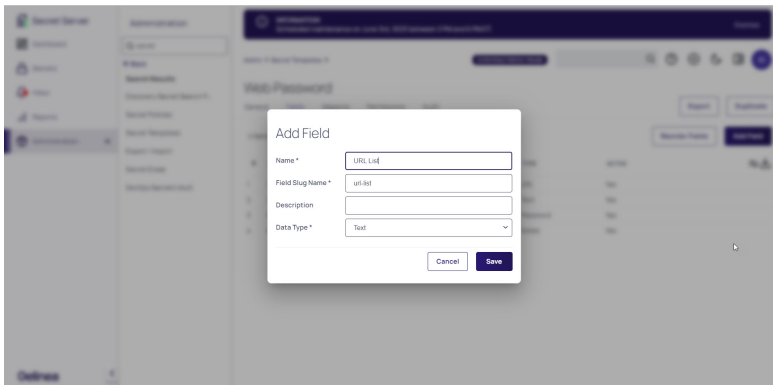


## Using WPF

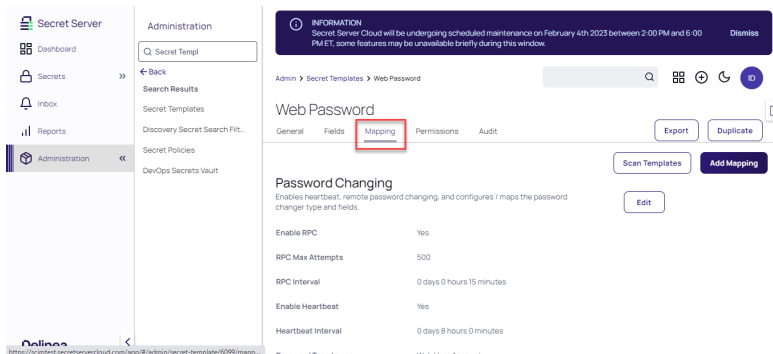


6. Create a new field with the name 'URL List'. Click **Save**.

 **Note:** You can choose any *Data Type* except *URL List*, *List* or *URL*.



7. Click the **Mapping** tab.



8. In the **Launcher Mapping** section, click **Edit**.

## Using WPF

Administration

Web Password

Web Password

General Fields Mapping Permissions Audit

Export Duplicate

Launchers

A secret launcher launches applications on end-user machines and automatically logs on using credentials stored in SS. In general, there are three types of launchers: RDP, SSH, and Custom. This provides a convenient method to open RDP and PuTTY connections, but it also circumvents users needing to know their passwords—a user can still gain access to a needed machine but it is not required to view or copy the password out of SS. A Web launcher automatically logs into websites using the client's browser.

| Launcher Name | Restrict User Input | Fields  |
|---------------|---------------------|---|
| Website Login | No                  | LAUNCHERFIELD<br>SECRETFIELD<br>Password Password |

9. In the **URL** dropdown menu, select **user input** and click **Save**.

Administration

Website Login

Website Login

Launcher Mapping

Define which fields from the Secret will be passed to the launcher.

Password Password

URL LURL

Username user input

URL

UserName

Password

Notes

Launcher Restrictions

Restrict values that can be passed to a launcher.

Restrict User Input No

10. In the **Launcher Restriction** section, enable **Restrict User Input**.

Administration

Website Login

Website Login

Username UserName

Launcher Restrictions

Restrict values that can be passed to a launcher.

Restrict User Input

Use List Fields  In order to restrict user input with categorized lists the secret template must have at least one field.

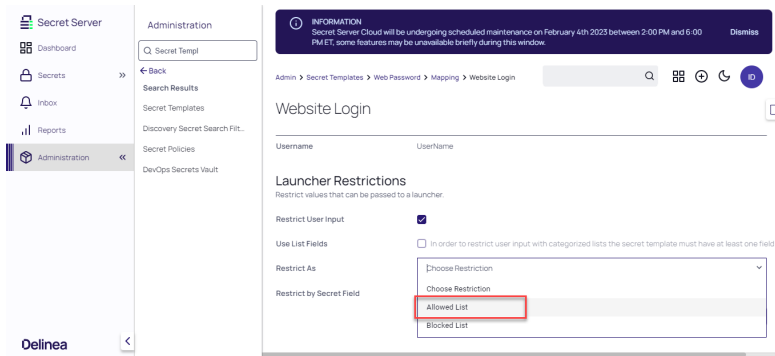
Restrict As Choose Restriction

Restrict by Secret Field Search or pick one

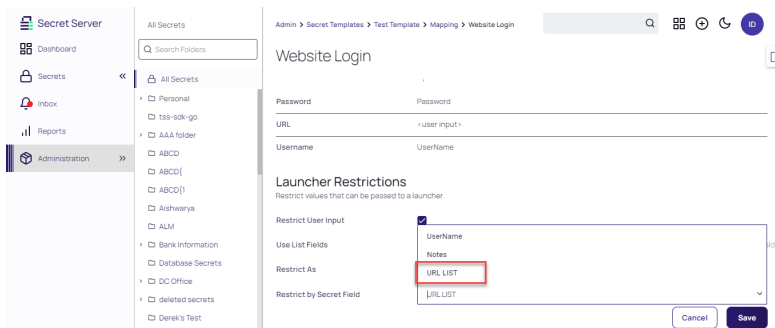
Cancel Save

11. In the **Restrict As** dropdown menu, select **Allowed List**.

## Using WPF



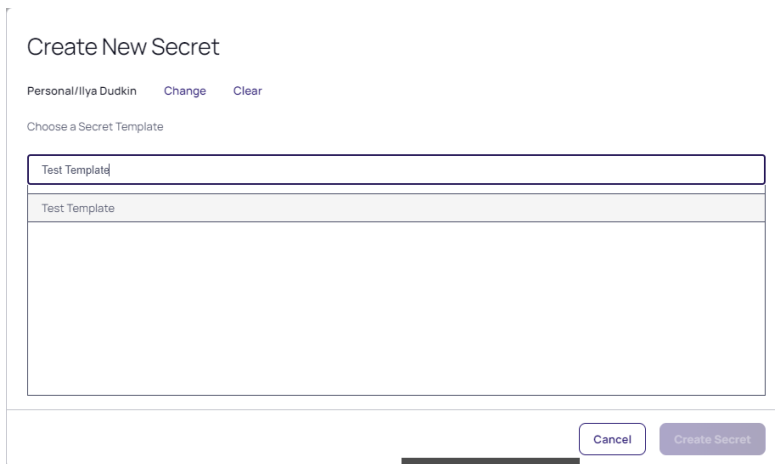
12. In the **Restrict by Secret Field** dropdown menu, select **URL List** and click **Save**.



## Using the Custom Web Launcher

To use the custom web launcher, follow these steps:

1. Create a secret with the newly created template.



2. Input the *Secret Name*, *URL*, *Username* and *Password*.

## Using WPF

Create New Secret

Secret Template: Test Template Change

Folder: Personal/Ilya Dudkin

Secret Name \*

UserName

Password

Notes

URL LIST

3. In the **URL List**, enter the needed URLs, separated by a comma and click **Create Secret**.

Create New Secret

Password

Notes

URL LIST: about.me,https://greenshadesonline.com/sso/admin/,https://www.tomorrow.do/

Site: Default

4. Inside the secret, navigate to the **Launchers** section and click **Web Password Filler**.

Secret Server Administration

Secrets > Test-Comma-Separated-URL

Test-Comma-Separated-URL

General Security Audit Remote Password Changing Dependencies Sharing Settings Metadata

URL: https://about.me/login

Username: test

Password: \*\*\*\*\*

Notes: https://about.me/login, https://greenshadesonline.com/sso/admin/, https://www.tomorrow.do/

Launchers

Provides a launcher to easily access an account using your secret's credentials.

No Active Sessions

Expiration and Heartbeat

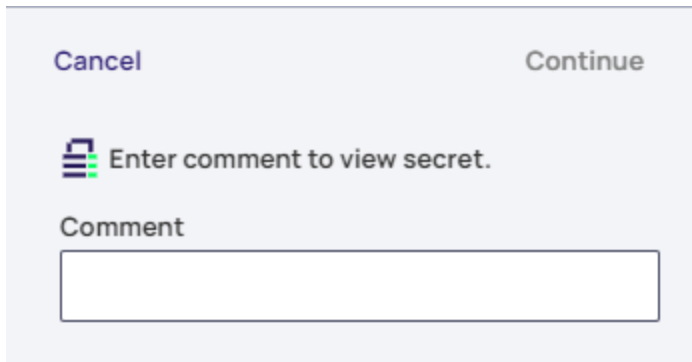
## Setting Comment Requirements


---

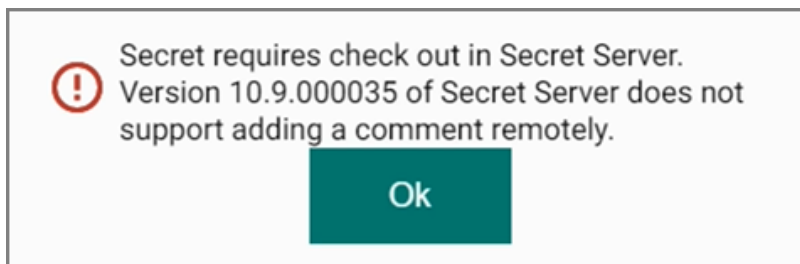
When a Secret in Secret Server requires a comment for checkout, you can supply that comment via the **Enter Comment** pop-up. Once you enter and submit the comment, WPF will populate the fields and give you access.

There are two levels of support for access to Secrets:

- If you only need to provide a comment, the pop-up shows the comment field and **Submit** button.
- If the Secret requires checkout, the pop-up shows the comment field and **Checkout** button.



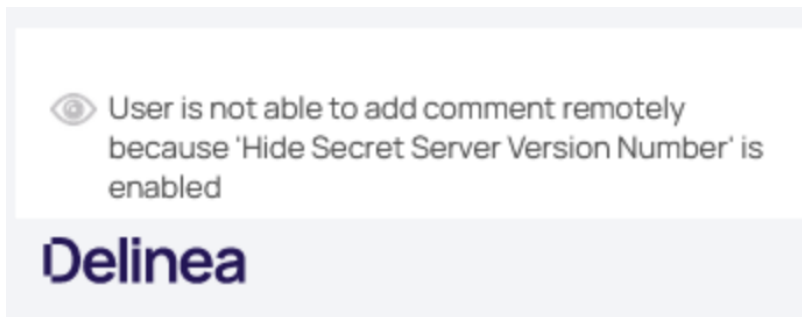
 **Note:** Secret Server versions above 11.1.000004 support this feature. If you use it on version 11.1.000004 or earlier, you will see the following message:



## Requiring Comments When Enabling the 'Hide Secret Server Version Number' Setting

To add a comment to any secret, Web Password Filler requires the actual Secret Server version number. However, when you enable the 'Hide Secret Server Version Number' setting, the API calls will not return information about the Secret Server version.

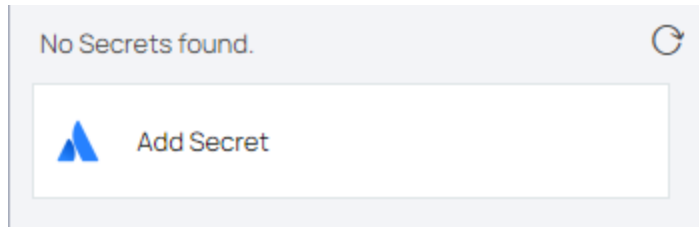
In this case, you will see a pop-up informing you that you cannot add a comment remotely because you have enabled 'Hide Secret Server Version Number'.



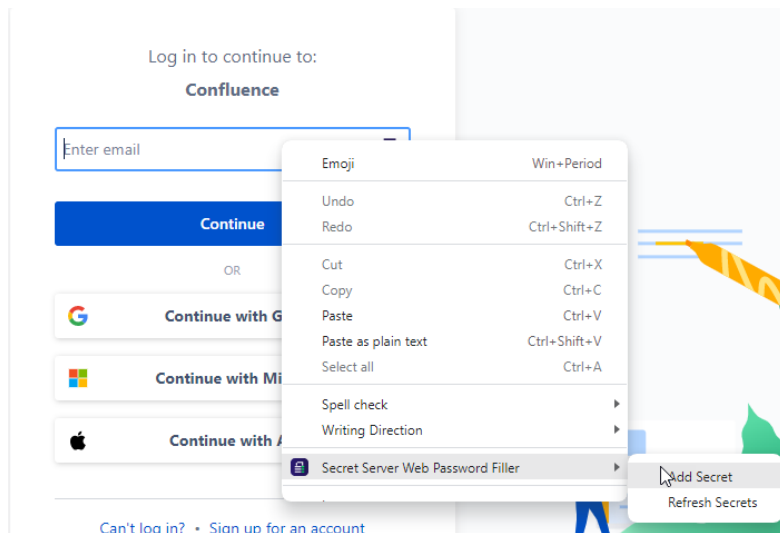
## Creating a Secret for a Website

To create a new secret:

1. Navigate to the page to create a new account on a website.
2. Click the WPF icon in the password text box. A popup window appears:



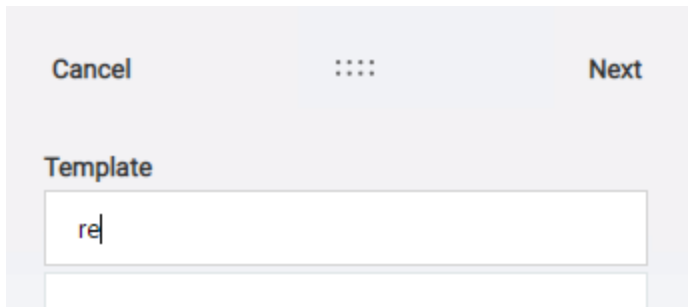
You can also right-click in the username or password field and select **Secret Server Web Password Filler | Add Secret**.



3. Select a **Template** for the newly added Secret. The default entry for the Choose a Secret Template field is **Web Template** because users choose that template most frequently. You can leave the default entry or click into the

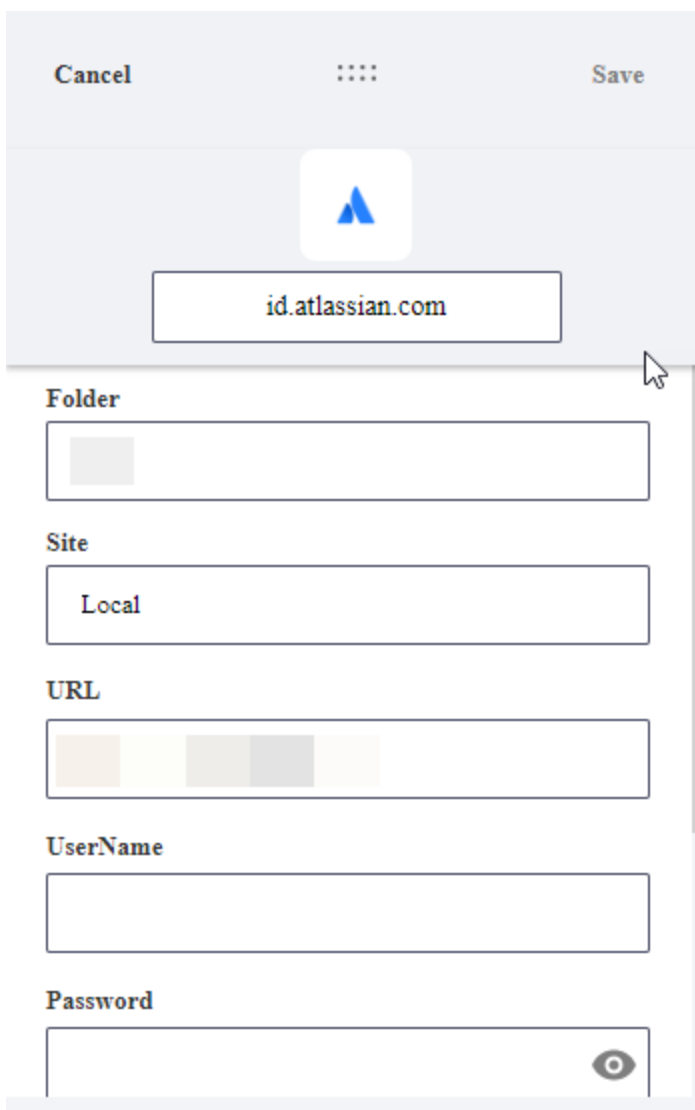
## Using WPF

field to change it. When you begin typing, the application will display options based on your input, which you can click to select. Click **Next** to continue.



A dialog box with a light gray header containing 'Cancel', a three-dot menu icon, and 'Next'. Below the header is a section titled 'Template' with a text input field containing the text 're|'. Below the input field is a scrollable list of options, which is currently empty.

4. The **Add Account to Secret Server** pop-up appears:



A dialog box with a light gray header containing 'Cancel', a three-dot menu icon, and 'Save'. Below the header is a central area with the Atlassian logo and a text input field containing 'id.atlassian.com'. Below this is a scrollable list of fields: 'Folder' (empty), 'Site' (containing 'Local'), 'URL' (containing a color-coded bar), 'UserName' (empty), and 'Password' (empty with a visibility toggle icon).

## Selecting a Folder

The default entry for the Choose a Folder field is a folder that was created automatically for you, named after your login name. You can leave the default entry or click into the field to change it. When you begin typing, the application will display options based on your input, which you can click to select.

The default folder can be changed by the user via the Add Secret pop-up by typing a folder name and selecting from the list.

Cancel    ⋮    Save

id.atlassian.com

**Folder**

m

- Max\000 Bulk Connect Test
- Max\000---NEW
- Max\111-NEW
- Max\a folder
- Max\RDP\A new

**User.Name**

**Password**

## Adding Accounts

The default entry for this field is **Local**. You can leave the default entry or click the drop-down arrow to choose from the available options.




## Using WPF

1. Click **OK**. Another **Add Account to Secret Server** pop-up appears, with some fields filled automatically based on the current website.



Cancel    ⋮    Save



www.facebook.com

Folder

Max

Site

Local

URL

https://www.facebook.com/


UserName

Password

If you are setting up a secret for Microsoft Online, leave the pop-up as is (do not close it) and read [Using WPF with Microsoft Online Services](#) before continuing.

2. The **Secret Name** text box is pre-filled by WPF, you may customize to a sensible name that identifies the secret well in a multi-user environment.
3. Type your username for the website for **User Name**.
4. If this is a new account, click **Generate** to create a strong password for the site. Otherwise, use the existing password for the website.
5. Click **Save**. WPF closes The Add Account Secret Server pop-up and populates the "new account" based on the entered information. A secret is now available for the password and name on this website main login page.

## Using WPF

 **Note:** Not all websites work with WPF populating the "new account" information for you. There are ways around that, like creating the website account first outside of WPF, and then using those credentials.

### Syncing Recent and Favorite Lists with Secret Server

Users' Recent lists are synced between Web Password Filler and Secret Server. WPF currently displays all secrets in the Recents tab as there currently is no 'All Secrets' tab. Secrets are ordered from most-recent to least-recent where the least-recent would include web-based secrets that have never been used in Web Password Filler. You can search for web secrets from the Recent list in Web Password Filler using any searchable field.

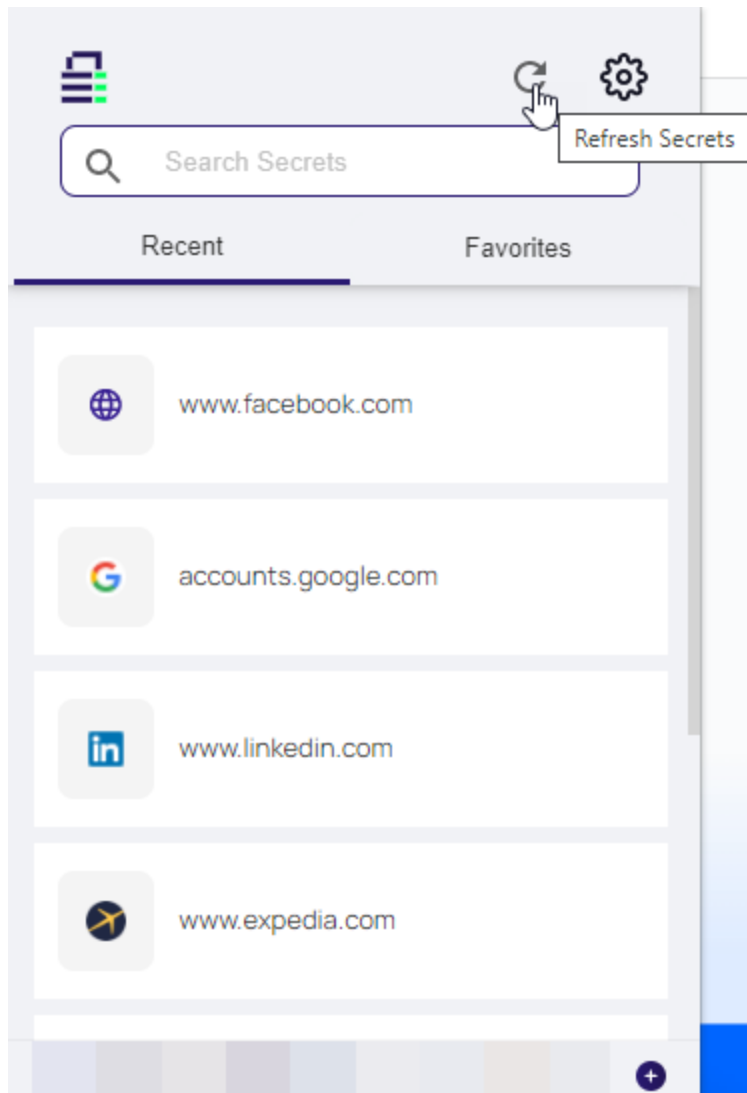
 **Note:** Web Password Filler lists secrets from any templates with a URL field or a URL list.

Web Password Filler also syncs the Favorite list between the browser extension and Secret Server.

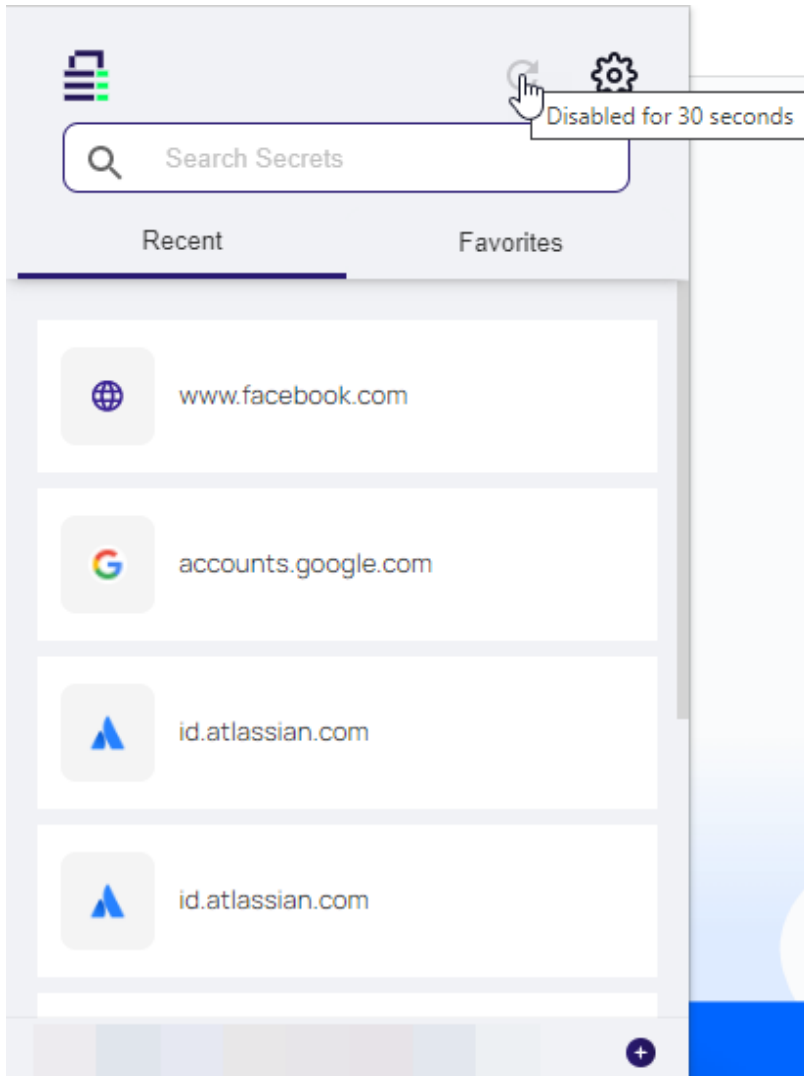
### Refreshing the Recent and Favorites List

The refresh button on the Recent and Favorites page allows a user to update their lists after adding/editing or deleting a Secret. The Refresh is supported by hover text **Refresh Secrets**.

## Using WPF



After refreshing the refresh button is deactivated for 30 seconds.



Recents are pulled from Secret Server and can be secrets that were recently accessed through Web Password Filler, through the Secret Server web UI, or through other means, such as the Delinea Mobile app. Secrets under Favorites are pulled from the Secret Server favorites list for the user account.

## Mapping Login Fields

Some websites use unconventional labels to internally identify their username, password, and other login fields, which Web Password Filler cannot automatically identify. You can map the fields on the Web page to the fields in the Secret using drag-and-drop functionality.

### Mapping Web Page Form Fields to Secret Fields

1. While creating a new Secret for a website, hover your cursor over the field you want to map in the Secret. The system highlights the field in a gray oval and provides instructions for you to drag the field to the corresponding

## Using WPF

field on the web page.

The screenshot shows a mobile-style interface for mapping a web form. At the top, there is a header bar with 'Cancel', a menu icon (three dots), and 'Save'. Below the header is a blue logo and a text field containing 'id.atlassian.com'. The main form area is divided into sections: 'UserName' with a text field containing 'ilya.dudkin@softvarium.net'; 'Password' with a text field containing seven dots and a visibility icon (an eye), and a 'Generate Password' link below it; 'Notes' with a large empty text area; and 'URL list' with an empty text area. A hand icon is positioned over the 'Password' label, and a tooltip bubble above it says 'Drag this to the Password field on the page'.

2. Drop the field into the field on the web page form that you want to map.

## Using WPF

The screenshot shows a web form for `id.atlassian.com`. It features several input fields:

- UserName:** A text field containing the email address `ilya.dudkin@softwarium.net`.
- Password:** A text field with masked characters (dots) and a visibility toggle icon.
- Generate Password:** A button located below the password field.
- Notes:** A large empty text area.
- URL list:** A text field containing the word `Password`. A tooltip with the text `Drag this to the Password field on the page` is positioned over the `Password` text in this field.

### Enabling Field Mapping with Metadata

To enable the field mapping function for Web Password Filler end users, a Secret Server administrator must create a metadata section named **WPFHints**. In the **WPFHints** section, the administrator must assign a name for each mappable template field. The administrator must also include a string value with the XPath to the field Web Password Filler should populate.

In the example below, you can see the open Metadata tab displaying the **WPFHints** section. The WPFHints section shows the names of the mappable template fields: **accno**, **Password**, and **Username**. It also displays the corresponding XPath string values of `//*[@id="account"]`, `//*[@id="password"]`, and `//*[@id="username"]`.

## Using WPF

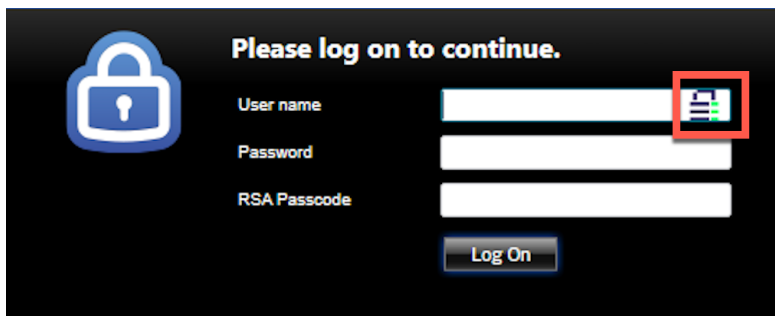
| General  | Security | Audit | Remote Password Changing | Dependencies | Sharing             | Settings | Metadata             |
|----------|----------|-------|--------------------------|--------------|---------------------|----------|----------------------|
| WPFHints |          |       |                          |              |                     |          |                      |
|          |          |       |                          | accno        | //*[@id="account"]  |          | <a href="#">Edit</a> |
|          |          |       |                          | Password     | //*[@id="password"] |          | <a href="#">Edit</a> |
|          |          |       |                          | UserName     | //*[@id="username"] |          | <a href="#">Edit</a> |

## Mapping Secrets With Three or More Login Fields

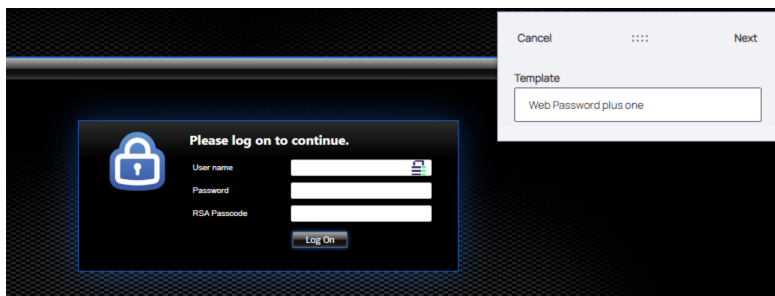
If a web login has three or more fields, you will need to create a customized secret template based on a specific web login. You will also need to map the login fields that Web Password Filler needs to populate.

Follow these steps to map secrets with three or more fields:

1. Navigate to the web login with at least three fields and click on the Web Password Filler icon.

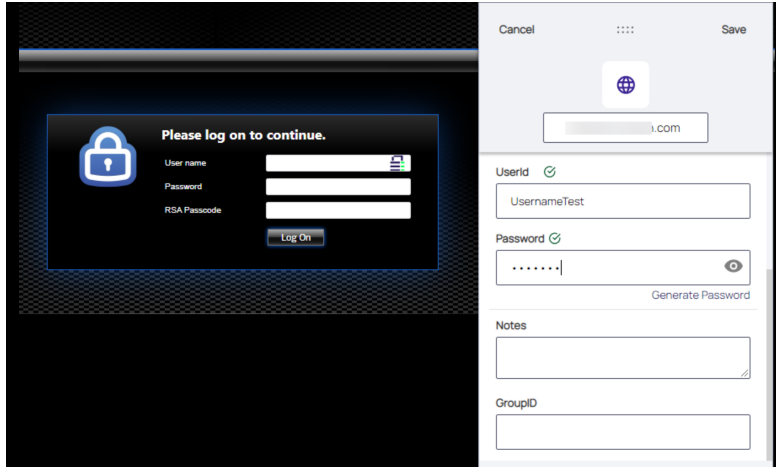


2. When adding a secret, select a customized template that has more fields than the standard web password template. This example includes one additional field:

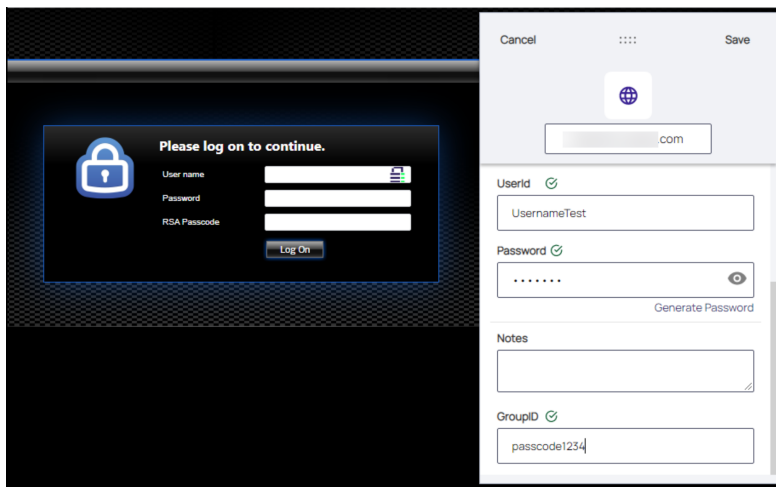


3. Drag the template **User ID** field to the web login Username

## Using WPF



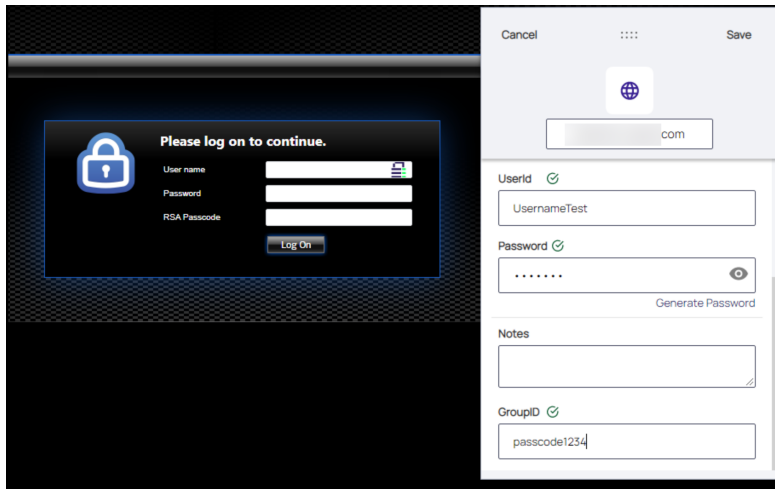
4. Drag the template password field to the web login's Password field



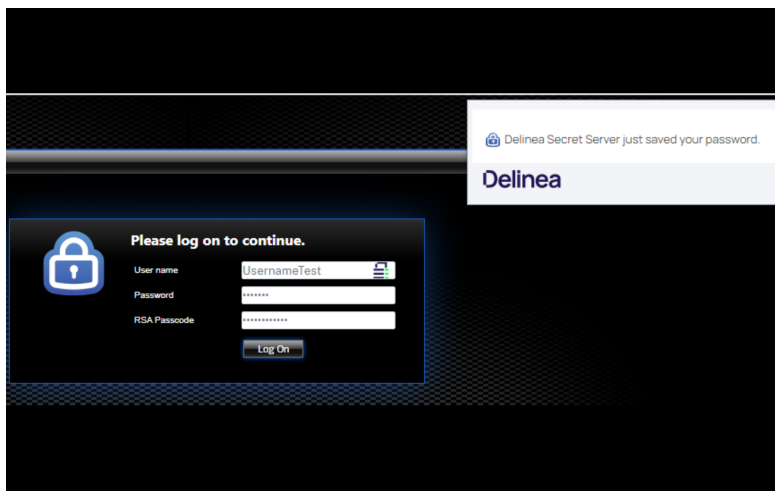
5. Drag the third field template to the web login's third field




## Using WPF



6. Click **Save**.



 **Note:** For Web Password Filler to function correctly, you should map all the fields in the form to the respective secret fields while creating the secret.

## Supporting Incognito Mode

Follow these prerequisite steps to ensure Web Password Filler can launch secrets in incognito mode:

1. On the secret via the secret template in Secret Server enable the setting **Web Launcher required Incognito Mode**.
2. On the extension's management page, enable the following settings for:
  - Chrome: **Allow in incognito**
  - Edge: **Allow in InPrivate**
  - Firefox: **Run in Private Windows**


## Using WPF

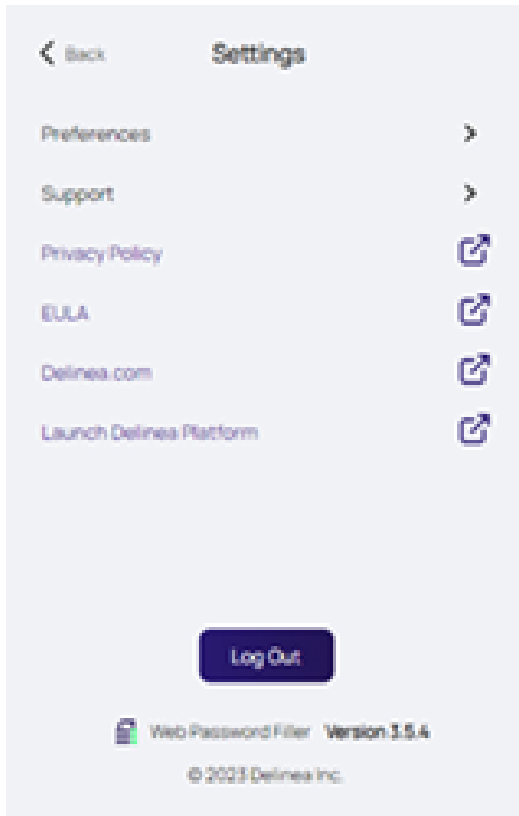
- Safari: **Run in Private Window**. You only need to enable extensions on macOS Sonoma (14) or higher. Safari automatically enables extensions on older macOS versions. To enable this setting, complete the following steps:
  - a. Choose **Safari > Settings**.
  - b. Click **Extensions**
  - c. Select the extension in the sidebar, then select **Allow in Private Browsing** on the right.
- 3. Login to WPF.

## Logging Out of Secret Server

---

Use the Web Password Filler icon to logout:

1. On the upper-right of the browser, click the WPF icon: 
2. You will see the WPF logout pop-up open.



## Using WPF

Click **Logout**.




3. The WPF icon changes to:

## Using Web Password Filler with Microsoft Online Services

---

In this section, you'll learn how to use the Web browser extension to leverage Secret Server Web Password Filler for logging into Microsoft Online. When you launch Microsoft Online secrets with WPF, you'll need to perform some additional configuration. This section explains the issue you'll encounter and suggests remedies you can implement.

 **Note:** This version of WPF is available in Secret Server release 10.7.59 and later. These instructions assume you have WPF installed correctly and are connected to Secret Server. If you're using WPF With Microsoft Online for the first time, we recommend you test your installation on another site first.

### Identifying the Problem

When you try to open a Microsoft Online secret with WPF, you might encounter two different error messages. You may see the first as: 'AADSTS900561: The endpoint only accepts POST requests. Received GET request.'



Sign in

Sorry, but we're having trouble signing you in.

AADSTS900561: The endpoint only accepts POST requests. Received a GET request.

Or you may see the second error message: "AADSTS900144: The request body must contain the following parameter: 'client\_id'."



Sign in

Sorry, but we're having trouble signing you in.

AADSTS900144: The request body must contain the following parameter: 'client\_id'.

## Using WPF

These errors don't explain the real problem. However, you're facing a simple issue with an easy solution that you can implement on your own.

### Understanding the Issue

Normally, WPF captures the URL of the website you are on when it creates a secret. It stores this URL (and other data) for logging into that website. This is very convenient and usually works great. Unfortunately, with Microsoft Online, when you try to log in with that secret, you get an error. This occurs because the log in URL initially stored in the secret points to a redirected page that no longer exists. Fortunately, WPF uses the URL stored in the secret, so once you update that URL, you never have to do it again.

Web Password Filler initially stores this errant URL:

```
https://login.microsoftonline.com/common/oauth2/authorize
```

You need to replace it with the permanent (real) URL:

```
https://login.microsoftonline.com
```

To fix this issue, you must ensure that the secret stores the permanent URL instead of the original one.

Choose between these two methods to update the URL:

- **Before Saving the WPF Secret:** You can change the URL when WPF initially stores it, right from WPF, *before* saving the secret. You can use this method if you create a new WPF secret using the WPF **Add Secret** button or the browser's context (right-click) menu.
- **After Saving the WPF Secret:** You need to change the URL after you've stored the WPF secret in Secret Server. You must use this method if you've already saved the WPF secret in Secret Server with the one-time redirected URL. This situation can occur if an earlier WPF version created the WPF secret, or if you created the secret using the automatic secret creation feature, which captures the one-time redirected URL instead of the permanent one.

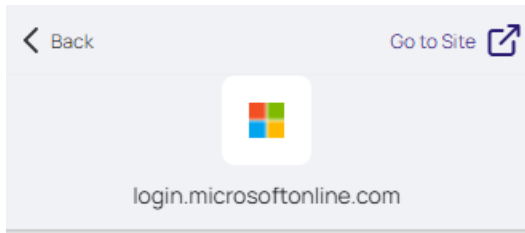
### Fixing the Issue When Creating the WPF Secret

 **Important:** Before you begin, read these instructions in their *entirety*.

If you have not created the secret yet, complete the following steps:

1. Go to the Microsoft Online log on (you already have an account and log in) or log-on setup page (you are setting up a new log in).
2. Follow the [Creating Secrets](#) procedure.
3. When you get to the *second* 'Add Account to Secret Server' pop-up, which looks like this:

## Using WPF



### URL

<https://login.microsoftonline.com>

### UserName

.....

### Password

.....

### URL list

### Notes

.....

<https://connmanagerss.thycotic.net/ss-current>

You now see the website URL that WPF inferred, which is incorrect. WPF also inferred the secret name—you can leave it as is or change it to whatever you like.

4. Delete all the text after '.com' in the **URL** text box. Your URL should look like this:  
<https://login.microsoftonline.com>
5. Return to and complete the rest of the instructions for the [Creating Secrets](#) procedure.

## Fixing the Issue After Having Saved the WPF Secret

1. Log in to Secret Server.
2. Navigate to the WPF secret for that Microsoft Online site. It is most likely named **login.microsoftonline.com**, which is the inferred name from WPF.
3. On the **General** tab for the secret, click the **Edit** link next to the **URL** text box:

## Edit Field

**URL \***

The online address where the information is being secured.

`https://login.microsoftonline.com/common/oauth2/au`

Cancel

Save

4. Delete all the text after '.com' in the **URL** text box. Your URL should look like this:  
`https://login.microsoftonline.com`
5. Click **Save**.
6. Log out of Secret Server.
7. Return to Microsoft Online to test the secret. You will need to log in again.

## Managing Port Numbers

Browsers strip default ports and treat URLs with these ports the same as URLs without them. For example, browsers consider these URLs the same:

- `http://someurl`
- `http://someurl:80`
- `https://someurl`

For non-primary or secondary domains, the port becomes part of the unique identifier. The browser records these independently. For example:

- `10.0.0.61:55` is different from `10.0.0.61:555` or `10.0.0.61`
- `blue.local.something` is different from `blue.local.something:8080`

## Accessing Websites with Self-Signed Certificates on Chrome

Google now requires all browser extensions to support Manifest V3 and is actively disabling those that still use Manifest V2. Manifest V3 enforces stronger validation processes around certificate validation. However, due to a bug in Chrome's implementation of this validation for extensions, it is currently rejecting all self-signed certificates.

For more information about this bug, see [Chromium Issue Tracker](#).

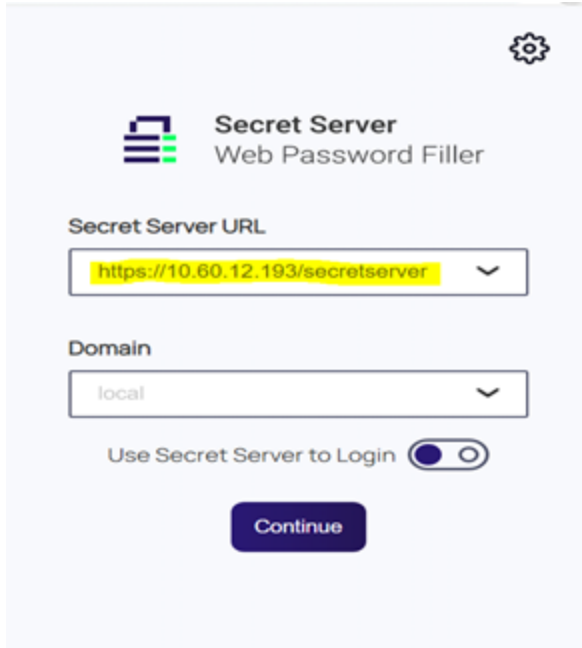
Below, you will find some differences in how Web Password Filler handled websites with self-signed certificates on Manifest V2 compared to how it will handle them in Manifest V3.

## Working With Self-Signed Certificates on Manifest V2

When you use Web Password Filler with Secret Server URLs that have self-signed certificates, it will load the self-signed URLs (e.g. local sites like ('https://localhost/somesite')) You will then encounter an error and be redirected to the same URL in another tab. This new tab will display the following error: net::Err\_CERT\_COMMON\_NAME\_INVALID. If you accept the certificate through WPF, the extension will proceed further.

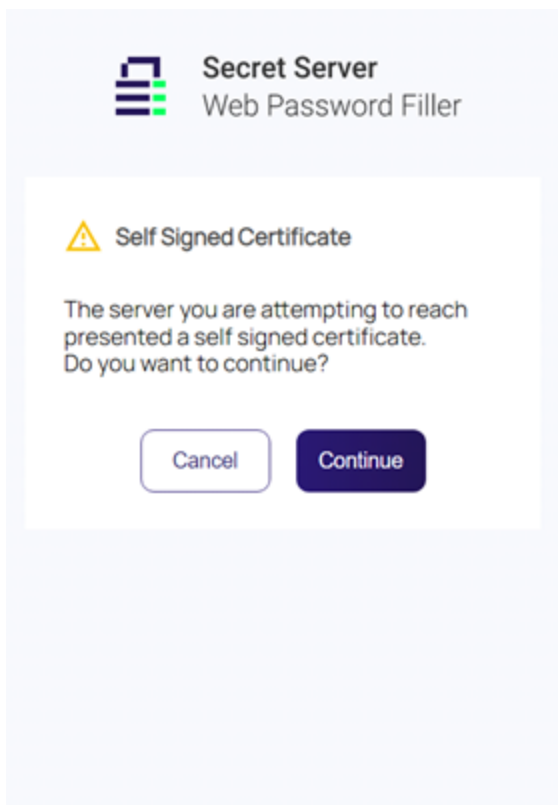
You can reproduce this error by following these steps:

1. Load local sites ('https://localhost/somesite').

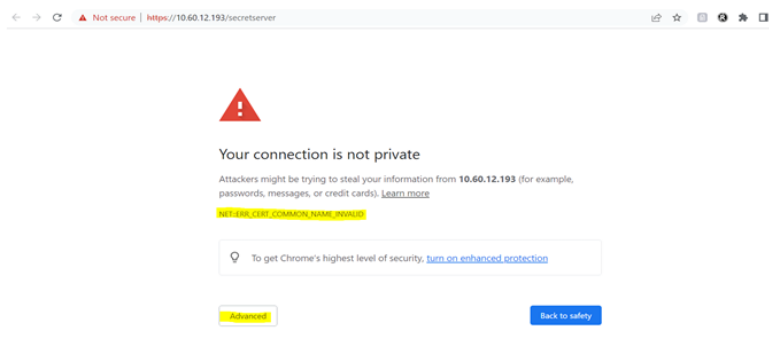


2. You will encounter the certificate error displayed below:

## Using WPF



3. After you click **Continue**, you will be redirected to another tab where you will see the following error message: `net::Err_CERT_COMMON_NAME_INVALID`



4. After you click **Advanced** WPF will accept the self-signed certificate, allowing the extension to proceed further.

## Working With Self-Signed Certificates on Manifest V3


With Secret Server URLs that have self-signed certificates, Web Password Filler:

1. Loads the self-signed URLs (e.g. local sites like 'https://localhost/somesite').
2. Displays an error in the extension and redirects you to the same URL in another tab.
3. Shows the following error on the new tab: `net::Err_CERT_COMMON_NAME_INVALID`



## Using WPF

4. Continues to display the same error even if it accepts the certificate.
5. Cannot make any API calls to Secret Server.
6. The extension cannot proceed further

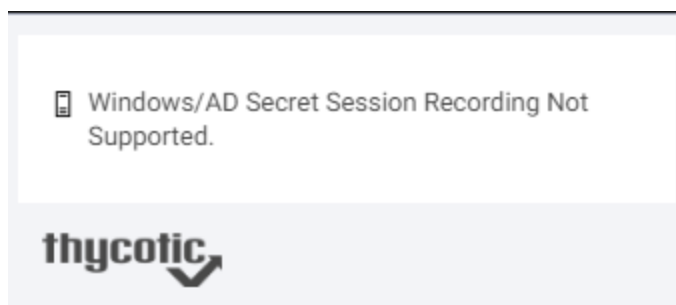
 **Note:** To workaround the self-signed certificate issue in Manifest V3, you need to set up a local CA and install the CA root certificate as a trusted certificate authority on your computer. Then, create a certificate using the CA and install that certificate on your Secret Server nodes.

## Supporting Windows Admin Center

---

Windows Admin Center now supports secrets that contain machine name / IP address combinations:

- The new user name will default to using a web password template only (Windows Admin Center does not support Windows and AD templates).
- When you click the **Connect** button in Windows Admin Center, it will not show secrets associated with the selected machine.
  - Workaround: You can select the machine link to retrieve the associated secrets.
- When you update passwords, the system updates the password in the current secret regardless of the template.
- How the system returns secrets:
  - Secrets with Host Name (As machine name)
    - link text --> IP (Host Name) --- Secrets will be returned
    - link text --> Host Name --- Secrets will be returned
    - link text --> IP Address --- Secrets will **NOT** be returned
  - Secrets with IP Address (As machine name)
    - link text --> IP(Host Name) --- Secrets will **NOT** be returned
    - link text --> Host Name --- Secrets will **NOT** be returned
    - link text --> IP Address --- Secrets will be returned
- WPF does not allow Session Recording for non-web password templates. If you attempt to use a secret with Session Recording enabled to log into an RDP session, WPF will prevent you from proceeding and will display the following message:



# Securing Web Password Filler

The following Securing Web Password Filler topics are available:

- "Setting Up the Native Messaging Host" below
- "Preventing Users from Disabling Session Recording" on page 67

## Setting Up the Native Messaging Host

---

The Delinea Native Messaging Host makes it easier to manage settings for the Delinea Web Password Filler. It also provides a more robust method of storing the settings so they are not impacted when the browser cache is deleted.

Without the Native Messaging Host, Web Password Filler runs normally, but the end user will be required to supply the Secret Server URL and to modify other settings to meet their needs.

The Native Messaging Host includes one executable file and one configuration file. You install these files on your computer. Each time you launch your browser, the Native Messaging Host silently sends default configurations and settings to Web Password Filler.

You can prevent Web Password Filler from functioning on specific URLs by adding those URLs to an exclusion list. Web Password Filler will not access Secrets for URLs on the exclusion list, nor will it fill or auto-populate credentials or other information for those URLs.

 **Note:** To use an exclusion list with Web Password Filler, the Native Messaging Host is required.

## Downloading the Native Messaging Host

You can download the Native Messaging Host installer [here](#).

## Software Requirements

- .NET version 4.8 or later
- Delinea Web Password Filler version 3.10 or later

## Supported Browsers

- Chrome
- Edge Chromium
- FireFox

You can find additional information regarding Native Messaging at:

- <https://developer.chrome.com/extensions/nativeMessaging>
- [https://developer.mozilla.org/en-US/docs/Mozilla/Add-ons/WebExtensions/Native\\_messaging](https://developer.mozilla.org/en-US/docs/Mozilla/Add-ons/WebExtensions/Native_messaging)


## Installing the Native Messaging Host

You install the Delinea Native Messaging Host on your computer by copying the `ThycoticMessagingHost.exe` and `settings.json` files into an accessible directory such as `C:\Thycotic\web password filler\`.

### Registering the Native Messaging Host

You must then register the `ThycoticMessagingHost.exe` with the browsers by running `ThycoticMessagingHost.exe` with a `--register` command line option, for example, by entering `C:\Thycotic\web Password Filler\ThycoticMessagingHost.exe --register` into a command window. Native Messaging Host cannot interact with Web Password Filler until this registration is completed.

Once you have successfully registered the Native Messaging Host, it will check the configuration file for updates automatically each time you launch your browser. You do not have to unregister and re-register each time you make a change to the configuration file.

 **Note:** If you manually add the WPF extension to the browser instead of getting it from the browser store, the extension ID changes. In that case, you **MUST** update the `settings.json` to reflect the new extension ID. Whenever you change the extension ID, you must run the `--register` command line option again before the extension will be able to communicate with the Native Messaging Host. Refer to the `settings.json` example below.

Changing other options or settings in the `settings.json` will automatically be reflected once you launch your browser.

During the registration process, the Native Messaging Host creates a folder for each browser (Chrome, Edge, Firefox, and Opera) containing the “native messaging host configuration” information required by each browser. Additionally, registry entries are created for each browser in either the current user registry or the local machine registry.

For example, you will find `HKEY_CURRENT_USER\Software\Google\Chrome\NativeMessagingHosts\com.thycotic.wpf.host` with a default value that is the path to the “native messaging host configuration” file. If you register using the `EnableForAllUsers = true` option, you must run the registration as an administrator.

### Uninstalling the Native Messaging Host

To disable or remove the Native Messaging Host, use the `--unregister` option, for example `C:\Program Files\Thycotic\Web Password Filler\ThycoticMessagingHost.exe --unregister`. Once unregistered, the Native Messaging Host can no longer communicate with Web Password Filler.

### Configuring Web Password Filler Settings

The Native Messaging Host facilitates the management of Web Password Filler settings through modification of a `settings.json` file. Each time you launch your browser, the Native Messaging Host reads the default configurations and settings in the json file and silently sends them to Web Password Filler. Web Password Filler then updates the local storage with the new settings and configurations.

### Establishing Default Settings and Browser-Specific Overrides

The `settings.json` file begins with a line for each browser, with the browser's identification code. In the image below, these lines are identified by the label, **Browser IDs**. The next lines in the file, labeled **Default Settings** in the image, establish your default settings for the Native Messaging Host. The default settings apply to all browsers unless a browser-specific setting overrides the default. Each browser has its own section of code for overrides, labeled **Default Overrides per Browser** in the image. The first line in the section identifies the browser with the same identifier used at the beginning of the file. The lines that follow in the section mirror the lines used to establish

## Securing Web Password Filler

the Native Messaging Host default settings. For each line where the browser-specific value differs from the default value, the browser-specific value takes precedence, overriding the default value.

```
1 {
2   "chromeExtensionId": "mfpddejbpbjckjoaicfedaljnfeollkh",
3   "edgeExtensionId": "kjldmpkefedgljefehmmfifbhnjngmbh",
4   "operaExtensionId": "eemnadjdifcpcncpalohpepihhbbo",
5   "firefoxExtensionId": "mailto:dd1e31d5-3623-45cb-b1ad-64074d36b360@thycotic.com",
6   "ConfigSSUrl": "https://someurl/SecretServer",
7   "ConfigDomain": "local",
8   "SettingUserSSLogin": true,
9   "SettingPromptToSave": true,
10  "SettingShowPopup": true,
11  "SettingEnableAutoPopulate": true,
12  "EnableForAllUsers": false,
13  "PopupDefaultPosition": true,
14  "ExactMatchUrl": false,
15  "SecretServerLoginWindow": true,
16  "maxSessionRecordingLimit": 120,
17  "matchSessionByHost": true,
18  "Exclude": [
19    "http://*"
20  ],
21  "ExcludeException": [],
22  "PerExtensionOverride": [
23    {
24      "id": "mfpddejbpbjckjoaicfedaljnfeollkh",
25      "ConfigSSUrl": "https://someurl/SecretServer",
26      "ConfigDomain": "",
27      "SettingUserSSLogin": true,
28      "SettingPromptToSave": true,
29      "SettingShowPopup": true,
30      "SettingEnableAutoPopulate": true,
31      "EnableForAllUsers": false,
32      "PopupDefaultPosition": false,
33      "ExactMatchUrl": true,
34      "SecretServerLoginWindow": false,
35      "maxSessionRecordingLimit": 120,
36      "matchSessionByHost": true,
37      "Exclude": [
38        "http://*",
39        "http://endoftheinternet.com",
40        "https://www.mycompanysite.com",
41        "https://live.com/"
42      ],
43      "ExcludeException": [
44        "https://MyCompanySite.com/Login.html",
45        "https://login.live.com/login.srf"
46      ]
47    }
48  ]
49 }
```

## Formatting the settings.json File

Below is an example *settings.json* file that sets the Secret Server URL to <https://SomeURL/SecretServer>, sets the domain to “local” and enables various other options for the Delinea Web Password Filler.

We recommend validating the *settings.json* file prior to deployment to ensure that the json is formatted correctly. There are many free online tools for validating json files.

```
{
  "chromeExtensionId": "mfpddejbpbjckjoaicfedaljnfeollkh",
  "edgeExtensionId": "kjldmpkefedgljefehmmfifbhnjngmbh",
  "operaExtensionId": "eemnadjdifcpcncpalohpepihhbbo",
  "firefoxExtensionId": "dd1e31d5-3623-45cb-b1ad-64074d36b360@thycotic.com",
  "ConfigSSUrl": "https://SomeURL/SecretServer",
  "ConfigDomain": "local",
  "HideConfigPage": false,
  "HideSettingPage": false,
  "SettingUserSSLogin": true,
```

## Securing Web Password Filler

```
"SettingPromptToSave": true,
"SettingShowPopup": true,
"SettingHideReadOnlyFolders": true,
"SettingEnableAutoPopulate": true,
"EnableForAllUsers": false,
"PopupDefaultPosition": true,
"ExactMatchUrl": false,
"maxSessionRecordingLimit": 120,
"Exclude": [ "http://*" ],
"ExcludeException": [],
"PerExtensionOverride": [
  {
    "id": "mfpddejbpbjkbjkaicfedaljnfeollkh",
    "ConfigSSUrl": "https://SomeURL/SecretServer",
    "ConfigDomain": "",
    "HideConfigPage": true,
    "HideSettingPage": false,
    "SettingUserSSLogin": true,
    "SettingPromptToSave": true,
    "SettingShowPopup": true,
    "SettingHideReadOnlyFolders": true,
    "SettingEnableAutoPopulate": true,
    "EnableForAllUsers": false,
    "PopupDefaultPosition": false,
    "ExactMatchUrl": true,
    "maxSessionRecordingLimit": 120,
    "Exclude": [
      "http://*",
      "http://endoftheinternet.com",
      "https://www.MyCompanySite.com",
      "https://live.com/"
    ],
    "ExcludeException": [
      "https:// MyCompanySite.com/Login.html",
      "https://login.live.com/login.srf"
    ]
  }
],
},
{
  "id": "kjldmpkefedgljefehmmfifbhnjngmbh",
  "ConfigSSUrl": "https://localhost/SecretServer/",
  "ConfigDomain": "",
  "HideConfigPage": false,
  "HideSettingPage": false,
  "SettingUserSSLogin": false,
  "SettingPromptToSave": false,
  "SettingShowPopup": false,
  "SettingHideReadOnlyFolders": false,
  "SettingEnableAutoPopulate": false,
  "PopupDefaultPosition": false,
  "ExactMatchUrl": false,
  "maxSessionRecordingLimit": 120,
  "Exclude": [ "http://*" ],
  "ExcludeException": []
}
```

## Securing Web Password Filler

```
    },  
    {  
      "id": "dd1e31d5-3623-45cb-b1ad-64074d36b360@thycotic.com",  
      "hideConfigPage": false  
    },  
    {  
      "id": "eemnnadjdifcpcnpalolohpepihhbbo"  
    }  
  ]  
}
```

A boolean controls the menu's position on the screen; if set to true, the menu appears in the upper right corner, and if set to false, the popup will display below the credentials fields. Additionally, a boolean setting configures Web Password Filler to recognize only exact URL matches, meaning that if it's set to true, WPF will only accept URLs that match the specified pattern. The duration allowed for a session recording is specified in minutes, with a default setting of 120 minutes and a maximum limit of 480 minutes. If a value in this section differs from the default value defined at the top of the JSON file, the value specified here takes precedence for that browser, overriding the default setting.

| Parameter           | Default   | Description  |
|---------------------|---|--|
| chromeExtensionID   | "mfpddejbpbjkbjoaicfedaljnfeollkh"                  | This is the ID required for the Chrome browser registration.                     |
| edgeExtensionId     | "kjldmpkefedgljefehmmfifbhnjngmbh"                  | This is the ID required for the Edge browser registration.                       |
| operaExtensionId    | "eemnnadjdifcpcnpalolohpepihhbbo"                   | This is the ID required for the Opera browser registration.                      |
| firefoxExtensionId  | "dd1e31d5-3623-45cb-b1ad-64074d36b360@thycotic.com" | This is the ID required for the Firefox browser registration.                    |
| ConfigSSUrl         | "https://SomeURL/SecretServer"                      | This is the URL for your Secret Server instance.                                 |
| ConfigDomain        | "local"   | This is the domain identification either local or your corporate network domain. |
| SettingUserSSLogin  | true  | Boolean that sets the checkbox to enable the Secret Server Login option.         |
| SettingPromptToSave | true  | Boolean that sets the checkbox to enable the Prompt to Save option.              |

| Parameter                 | Default | Description   |
|---------------------------|---------|---|
| SettingShowPopUp          | true    | Boolean that enables login credentials to pop up automatically. If false you just need to click the Delinea checkmark.  |
| SettingEnableAutoPopulate | true    | Boolean that sets the checkbox to enable the Auto Populate option for secrets and passwords.  |
| EnableForAllUsers         | false   | Boolean specifying if the Native Messaging Host is available under the local user context only or made available for all users. If set to true, it allows all users on the machine to access the settings.json file as long as it's in a shared location. If set to false it only applies to the current logged in user no matter where the file is stored. Changes impacting the registry keys also require admin permissions if EnableForAllUsers is set to true. |
| PopupDefaultPosition      | true    | Boolean that positions the menu in the upper right corner of the screen. If false the popup appears below the credentials fields.   |
| ExactMatchUrl             | false   | Boolean that configures WPF to recognize only exact URL matches   |
| maxSessionRecordingLimit  | 120     | The number of minutes allowed for a session recording. Default is 120 minutes and maximum allowed is 480 minutes.   |
| Exclude                   | [list]  | Refer to <a href="#">Site Exclusions and Exceptions</a> below. Accepts wildcards.   |
| ExcludeException          | [list]  | Refer to <a href="#">Excluding Sites and Making Exceptions</a> below. Does NOT accept wildcards.  |

| Parameter              | Default   | Description  |
|------------------------|---|--|
| SecretServerLoginWindo | false   | If disabled then login window used to open in new tab in same browser.   |
| matchSessionByHost     | true  | If enabled use host/origin instead of base domain to determine if two tabs record to the same session. If disabled use the base domain. By Default, it's enabled that is by host/origin. |
| PerExtensionOverride   | Contains a section for each browser type, with custom values for the 15 settings described in this table (ConfigSSUrl, ConfigDomain, HideConfigPage, etc.). | If a value in this section differs from the default value established at the top of the JSON file, the value here takes precedence for that browser, and overrides the default value.    |

### Excluding Sites and Making Exceptions

The Delinea Web Password Filler is an “inclusive” extension. Any website that contains a username and password has the potential to have a secret retrieved from or stored in Secret Server. However, some sites are simple web forms that contain user name, password, and a variety of other field types. Registration forms, for instance, would not require interaction or population of the username and password from WPF. The Delinea Native Messaging Host allows you to add exclusions as well as exclusion exceptions so those sites you do not want Web Password Filler to interact with will be ignored. Add exceptions for any site you wish WPF to ignore. For example, to login to an application, you want WPF to retrieve a secret for the login page. However, if you would like WPF to ignore every other page for that same site, add the specific page URL to the exclusion exception list.

To exclude all sites, a wild card can be used ([https://\\*](https://*) and/or [http://\\*](http://*)) and then simply add the sites where secrets are available (<https://MyCompanySite.com/login.aspx>) to the exclusion exception list.



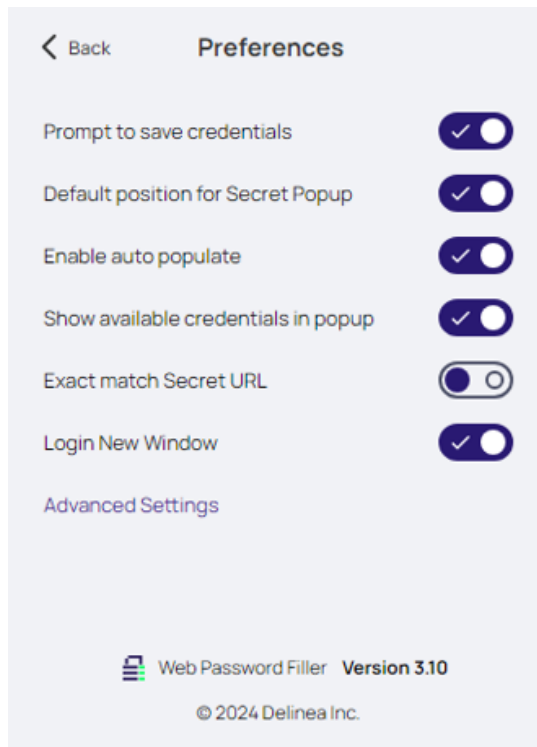
**Note:** Only the “Exclude” section accepts a wild card. You must enter the “ExcludeException” as the exact URL without a query string.

### Setting UI Behavior Based on Preferences

You can set each preference on the **Preferences** page to “true” or “false” in the *settings.json* file.



## Securing Web Password Filler



You can set the Secret Server URL and Domain by including strings (text wrapped up in quotations).

## Securing Web Password Filler

Back

Log in to Secret Server

https://scimtest.secretservercloud.com

Username

Password

Domain

local

Next

OR

Web Login

Additionally, you can choose to hide these pages from the end user so that the settings and configuration options cannot be changed.

### Managing Error Messages

Error messages are recorded in the file named `native-messaging`, which is stored in the same folder where you installed Native Messaging Host. The error messages in this file are especially useful when contacting Delinea support services.

- The following error message indicates that there are missing elements in the `settings.json`.

There are elements missing from `settings.json`. Review the documentation and update `setting.json` with the missing attributes.

Review the `settings.json` format and ensure all elements are provided and the json file is well formatted.

- The following message indicates that the setting “EnableForAllUsers” is set to true. However, the user attempting to register the Delinea Native Messaging Host does not have administrator permissions and cannot

## Securing Web Password Filler

update or create the key local machine registry key required for browser registration.

This application must be run as an administrator when registering for All Users

- The following error message indicates that the *ThycoticMessagingHost.exe* was executed without the required command line option.

```
To register the Native Messaging Host, run cmd.exe ThycoticMessagingHost.exe -register
To unregister the Native Messaging Host, run cmd.exe ThycoticMessagingHost.exe --
unregisterPress any key to exit
```

- The following message indicates that only `--register` and `--unregister` are valid command line options.

```
Incorrect command line. Review the documentation to register or unregister this
application.
```

## Preventing Users from Disabling Session Recording

---

Session Recording now uses a new background system called *service workers* instead of the old background page. Service workers help run your web apps even when you're not actively using them. Users can accidentally stop service workers through a Chrome settings page (<chrome://serviceworker-internals>), which could interrupt session recording.

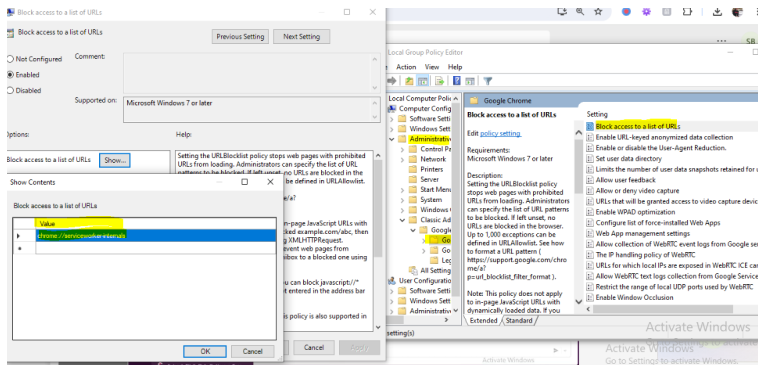
Browser extensions like Web Password Filler can't prevent users from disabling service workers due to technical limitations. If a user stops the service worker, it will interrupt session recording. However, administrators can prevent users from disabling service workers by implementing a group policy.

Complete these steps to set up policies that prevent users from disabling service workers:

1. Download and install Chrome policy templates:
  - a. Download the Chrome policy templates from [Google Admin Template](#).
  - b. Extract the contents of the zip file.
2. Load the policy templates.
  - a. Open the **Group Policy Management Editor** if you're managing the policy via a Windows Group Policy.
  - b. Right-click on your desired Group Policy Object (GPO) and select **Edit**.
  - c. Navigate to **User Configuration** or **Computer Configuration** > **Policies** > **Administrative Templates**.
  - d. Right-click on **Administrative Templates** and select **Add/Remove Templates**.
  - e. Add the .admx file for Chrome.
3. Configure the URLBlocklist policy:

## Troubleshooting

- Navigate to **User Configuration** or **Computer Configuration**, go to **Administrative Templates > Google > Google Chrome > URL Blocking**.
- Double-click **Block access to a list of URLs** and enable this policy.
- Click the **Show** button to open the list of blocked URLs.
- Add `chrome://serviceworker-internals/*` to the list.
- Click **OK** to apply the changes.



- Apply the group policy:
  - Close the **Group Policy Management Editor**.
  - Update the policy on client machines by running `gpupdate /force` in the command prompt, or wait for the next automatic policy refresh.

## Troubleshooting

The following Troubleshooting topics are available for Web Password Filler:

- "Enabling Diagnostic Logging" on the next page
- [WPF Issue Investigation](#)
  - "Managing Compatibility with Previous Products" on page 70
  - "Logging in with Web Password Filler" on the next page
  - "Presenting Behaviors and Problems" on page 70
  - [Using Web Password Filler with Microsoft Online Services](#)

## Addressing Usability Issues

Web Password Filler may fail to return a Secret when a large number of Secrets are associated with a single URL.

The issue could be that the following endpoint is not utilizing the `NumberOfBookmarkletSecretsToSelect` advanced configuration setting:

```
/api/v1/secret-extensions/search-by-url
```

## Troubleshooting

The system only returns 500 records when this setting is not assigned. Increase the value to return more records. A value of 0 will cause the endpoint to not return any records.

You cannot access Advanced Configuration through Secret Server's UI, but you can access it by following these instructions:


1. Go to `https://{your_secret_server_url}/ConfigurationAdvanced.aspx`
2. Click **Edit** at the bottom of the page.

## Logging in with Web Password Filler

---


Check if you're logged into Web Password Filler.

If you log in to Secret Server via web login, the system will automatically log you in to Web Password Filler. If you log in to Secret Server via local login, you will need to log in to WPF separately.

 **Note:** To automatically log in to WPF after successfully logging in to Secret Server, you must ensure that the Secret Server site you're logging into matches the URL currently in Web Password Filler.

Additionally, you can quickly tell if you are logged in or not by checking the icon in the browser.

▪ Not Logged in 

▪ Logged in 

## Choosing a Login Method

You can log in using two different methods:

1. Username and Password
2. SAML authentication through Secret Server.

For more information on SAML, refer to the Secret Server documentation on [SAML](#).

## Troubleshooting Login Issues in Chrome or Edge

You may experience issues logging in on Chrome or Edge if you use Web Password Filler version 3.2 or earlier. These issues occurred after Chrome and Edge made internal improvements. The 3.3 release fixed this issue.

## Enabling Diagnostic Logging

---

When Diagnostic Logging is enabled in Web Password Filler, the **View Log** option appears in the WPF interface.

Logged items include:

- Unsupported API methods that attempt to access Secret Server and generate errors.
- Secret Server URL.

## Troubleshooting

- Date/Time stamp.
- Log Download via **View Log** access.

WPF offers functionality to print logs to a log file including these details:

- The API that was called
- The users active Secret Server
- The API call response
- The status code to the log file

This makes it easier for users to go through logs and find the root cause of any issue, instead of referring to developer tools.

## Managing Compatibility with Previous Products

---

First, check to see whether you have the old Login Assist or Secret Server Clipboard Utility installed.

If you have installed **either** of these old browser extensions, **disable** them from the extensions page. After disabling them, **refresh** your page. If possible, completely close and re-open your browser. However, if you don't want to lose work in other tabs, refreshing the page should work.

After you disable the old extensions, refresh or close the browser and then try again. Check to see if the issue still occurs.

If the issue still occurs, check for other installed extensions that might interfere.

We recommend you do **NOT** run the new Web Password Filler while the old Login Assist and Clipboard Utilities are active. These tools attempt to perform similar functions, which can lead to conflicts and cause issues. Therefore, avoid enabling them simultaneously.

## Presenting Behaviors and Problems

---

When you report problems or ask for help with Web Password Filler, providing more information about the actual behavior you experience will help others find a resolution faster.

All of the previous troubleshooting topics help narrow things down. The more specific you are, the better.

Some examples:

1. Are you unable to login to WPF?
  - Are they getting any error messages?
  - Are you logging in and then getting logged out again?
  - What authentication types are enabled and are you using them?
  - Is the **Login** button greyed out?
  - Is the Secret Server URL (and optional: Domain) entered in the **Configuration** tab?
  - Can you reach the Secret Server UI from the same machine/browser?
2. Do you see the Secret displayed on the site?

## Troubleshooting

- Does the site have only one Secret?
    - a. If no, can you see all the Secrets? Or can you only see some Secrets?
  - Does your logged-in account have access to that Secret?
3. Are the credential fields populated correctly?
- If No, which fields are populating?
  - Do you see the green Delinea check logo in the Username/email field?
    - a. We **ONLY** display this in the Username or email fields, **NOT** in the password field
  - Are the right-click options available in any of the login fields?
  - Which fields are not populated?
  - Do you see the credentials populated in the wrong field?
  - Does the site require a drop-down or other action to be taken before the credential fields are available?
  - Does the site use a multi-page login (like O365)? Or single page login (like LinkedIn)?
4. Is it some kind of visual issue on the page?
- Is the green Delinea log visible?
  - Is the green Thycotic logo in the wrong place on the page?
  - Is the page displaying as blank?
  - Are the icons for the Secrets not showing up?
5. Is it a newly added Secret that is not showing up?
- When you add a Secret in Secret Server or in WPF, it might not appear immediately on the site. WPF needs Secret Server to index the Secret, which typically takes some time (depending on the size of the environment).
  - Usually if you wait a few minutes and refresh the page you should be able to see it appear.
  - Release 1.1.0 of WPF introduced a short-term caching option. You can see this as a refresh button on the drop down for the credentials. This caching means that we should keep the Secret in memory for that browser session so we don't have to wait for Secret Server to index it.
6. Are you experiencing any other issues? If so, what are they?

## Investigating WPF Issues

---

When investigating issues with Web Password Filler, the following questions should help narrow down the issue or provide needed information to troubleshoot.

### Confirming WPF Version

Confirm that the issue relates to the new Web Password Filler, which Delinea first released in Dec 2019 alongside Secret Server v10.7.59.

Do not consider problems with other browser extensions or plugins (e.g. Login Assist, Clipboard Utility, etc.) as WPF issues.

## Identifying the Problematic Browser

What browser is the issue occurring on?

- We currently support: Chrome, Firefox, Edge (Chromium) and Opera.  
General Chromium should work as well, but we do not officially support it.
- Does the issue only occur on one browser? Or does it reproduce for multiple/all browsers?
- If it only reproduces on one browser, which one?

## Identifying the Affected Sites

Is the issue occurring on a Specific site? Or all sites?

- If the issue only happens on one site, what is the URL for that site?  
For example, if the issue only occurs on Facebook, we need the URL of the Facebook page where the browser fails.
- For WPF login failures, if you change the web page you are on when you try logging in, does the issue still occur?
- We always need to know the **URL** where an issue occurs, as some web pages may interfere with WPF.

## Determining Site Access

How are you accessing the site to use WPF?

There are typically two ways to access a page to use WPF:

1. Logging into the Secret Server Web UI and clicking the Web Launcher option to open a new tab
2. Opening a web browser and navigating to a page manually (using a bookmark or typing/searching for the URL).  
Once on the page we'll fill the credentials or provide options in a pop-up.

## Identifying the WPF Version with the Issue

Web Password Filler does not display its version number. You need to check the Extensions/Add-on page to find the version number. The location to get this value varies slightly between browsers.

Follow these basic steps to find the version number:

1. Go to the **Settings** menu in your browser. This is typically in the top right corner and looks like a hamburger menu. (☰)
2. In the drop-down list, select:
  - **Chrome**: More tools > Extensions
  - **Firefox** : Add-ons
  - **Edge (Chromium)**: Extensions
  - **Opera**: Extensions (in the left-hand menu).
3. You can find the version number in the following locations:



## Release Notes

- **Chrome:** At the top of the extension, in-line with the name.
- **Firefox:** Click on the add-on to view its details. Look for the "Version" field.
- **Edge (Chromium):** At the top of the extension, in-line with the name.
- **Opera:** At the top of the extension, directly under the extension name.

## Performing the Action

What type of action are you trying to perform?

A user might try to take a few basic actions, including:

1. Login to WPF
2. Launching a Secret for a web page (from Secret Server or by going to the page manually)

This includes filling credentials for a site

1. Trying to add a new Secret for a site.
2. Trying to update a password for an existing Secret.

## Using Templates

What Secret template are you using?

Web Password Filler primarily works with Secrets that use the Web Password template, but it can also work for Secrets using other templates.

To work with other Secret templates, those templates must have a URL field.

1. WPF uses this field to match the URL from the site back with the URL in the Secret.



**Note:** You must list the URL field as "Searchable" in the **Edit Templates** screen in Secret Server.

# Release Notes

This section includes the most recent Web Password Filler Release Notes.

## 3.10.3 Release Notes

---

*October 22, 2024*

### Fixed Issues

- Web Password Filler did not set the folder for new secrets to the user's personal folder by default.


## 3.10.2 Release Notes

---

*October 14, 2024*

## Bug Fixes

- The session recording indicator wasn't hidden when the Recording Indicator was set to On.
- The Update Password popup did not appear.
- The ADP login page did not autofill.
- The Save Password popup continues to appear even after a secret has already been created.
- Web Password Filler did not auto-populate the email field for some sites when launching.
- The kebab menu did not appear on the secret list for the X (previously known as Twitter) site.
- The save and update popup frequently appeared when users tried to save credentials for some sites.
- The WPF icon did not appear in the Username field during the first attempt on some sites.

 **Note:** Safari versions below 18.0 do not allow checking if an extension can run in Incognito mode; this means that WPF will not work correctly in Incognito mode.

## 3.10.1 Release Notes

---

*October 04, 2024*

### Bug Fixes

- Fixed an issue that caused tabs logged into Secret Server or Platform to reload whenever the browser stopped the Web Password Filler service worker. This issue occurred only in Chrome.

## 3.10.0 Release Notes

---

*September 30, 2024*

### Improvements

- Web Password Filler now tracks browser tabs that need session recording based on the full host name instead of the base domain. You can change this behavior in Advanced Settings.

### Bug Fixes

- Fixed an issue on sites with specific event handling of login fields that prevented the first character of the username and password from autofilling.
- Web Password Filler auto-populated a field that was not a username or password field.
- Web Password Filler did not log out of Platform when the user clicked Log Out in WPF.
- If Thycotic Messaging Host is installed and Web Password Filler is logged in, WPF would not auto-log in even when the token was valid.

## 3.9.6 Release Notes

---

*August 27th, 2024*

## Enhancements

- Allow the system to identify and autofill login pages using a search field as the username when someone manually maps the field.
- Updated the session expiration messages to include the site of the tabs being closed.

## Bug Fixes

- Fixed an issue autofilling the FortiMail login..
- Web Password Filler fixed an issue where recorded sessions from secrets requiring checkout would terminate before the checkout expired. This occurred when the secret also required MFA and the MFA pass-through time was shorter than the checkout time.
- Fixed a premature logout issue in WPF when sharing a login session with a web login in a browser tab.
- Changed WPF login for platform to prevent WPF logout when a platform session in a browser tab times out due to inactivity. This change also means platform will not automatically log in if opened in the browser while WPF is logged in.
- Fixed an issue with detecting the username field on some Cisco login pages.
- Fixed an issue affecting platform logins using Microsoft SSO when Native Messaging Host is installed.

## 3.9.5 Release Notes

---

*July 26th, 2024*

### Bug Fixes

- Removed unnecessary extra calls to search-by-url that were affecting performance for some users.
- Web Password Filler now handles new 401 status code results sent by Secret Server API calls as invalid tokens, in addition to 403 status codes returned by previous versions of Secret Server.

## 3.9.4 Release Notes

---

*June 10th, 2024*

### Improvements

- Due to new security restrictions in the latest versions of Safari, the browser can no longer differentiate between different types of connection errors. As a result, Web Password Filler now displays a more general error message: 'Unable to reach server. Verify that the server URL is correct, and that the server has a valid certificate.' This message appears for both certificate and network issues.
- The caching of autofill matches have been removed. Web Password Filler now calls Secret Server every time it finds a login page. This change prevents issues where the system did not present new secrets to users for autofill.

### Bug Fixes

- A bug in the caching logic caused some secrets to not show up in the autofill match list.
- The refresh icon appeared in the popup if the user did not have the 'Add Secret' permission and no secrets were present for that site.
- Web Password Filler would sometimes display the 'Add Secret' dialog in the wrong browser window when adding a secret.
- When working in Mimecast, the Web Password Filler icon was displayed for some email fields, even though those fields were not valid for autofill.
- <https://sso.cloud.com> would not autofill in Web Password Filler.
- Fixed an issue that caused visual corruption in some recorded sessions.
- When using the Web Password Filler popup window to generate a password, the generated password contained duplicate letters. The passwords generated did not follow the Secret Server password policy.
- The system sometimes displayed 404 errors to the user when making background network calls to check the validity of login URLs.
- Updated the autofill field detection logic to handle login forms in Italian.
- Web Password Filler did not close launched Chrome sessions upon secret check in or when the secret timeout limit was reached.
- Web Password Filler reloaded the username page after the user submitted the username on some sites.
- An OTP API call occurred every 30 seconds, even if the user did not have the secret information page open.

### 3.9.3 Release Notes

---

*May 6th, 2024*

#### Bug Fixes

- Fixed an issue where launching a recorded secret with a list of URLs to a redirected URL was not autofilling properly.
- Fixed an issue with the copy password functionality in the new autofill menu, allowing users to successfully copy passwords from it.
- Updated the OTP field detection logic to prevent a case where a password field was misinterpreted as an OTP field

### 3.9.0 Release Notes

---

*April 8th, 2024*

### Improvements

- The secret details view now displays the current passcode for secrets with associated TOTP codes.
- The dialog that appeared when users switched to a tenant that hadn't been used before has been removed.
- If TOTP is configured on the autofill secret, the TOTP field will now autofill.

### Bug Fixes

- Secret Servers with 5000+ folders would encounter performance issues during the addition of secrets and folder filtering processes.
- A "Bad Request" error has been resolved when "Exact Match URL" is disabled, autofilling using a secret with a categorized list, and the URL of the current page only partially matches the URL selected from the categorized list.
- Fixed the issue of the Delinea icon not displaying on the username field on some websites.
- The Delinea icon was not visible on the username field for some sites.
- When launching an incognito tab in Safari 17.1, it did not show a warning when the extension was not allowed in private browsing mode.
- When using autofill on secrets, Web Password Filler would remove the first character in both the password and username fields on some sites.
- The dropdown list on Web Password Filler's ticketing system was not aligned properly with other input methods.
- In Safari, certain images failed to display when the `<img>` tag provided the path `'webkit-masked-url://hidden/'`. To address this issue, it has been converted into SVG.
- The username and password was not being autofilled on some sites.
- If a secret was selected from the secret list, the password was not being autofilled.
- Fixed an issue where the secret list wouldn't load when 50 or more templates contained a URL field. This fix also requires upgrading to Secret Server 11.6 or higher.
- The Web Password Filler icon appeared on the wrong input element on some sites.
- Web Password Filler was trimming the 'www' from URLs when launching secrets.
- Previously, Web Password Filler only checked if the site URL contained the Secret Server domain, resulting in the exclusion of sites where the site URL domain was a substring of the Secret Server domain. Now, Web Password Filler verifies that the site URL domain precisely matches the Secret Server domain.

## 3.8.0 Release Notes

---

*January 31st, 2024*

### Improvements

- When the Web Password Filler token expires and cannot be renewed, and the active recordings are still ongoing, the system will redirect the user to the session timeout page. This page will inform the user that the

## Release Notes

ongoing recording has been terminated.

- When a user attempts to log out from Secret Server or the Platform portal while a session recording is ongoing, they will see a confirmation dialog. This dialog will give the user the choice to either remain logged in or proceed with logging out.
- Web Password Filler now displays the folder name under Secret Details instead of the folder ID. When a user hovers the mouse over folders, the folder path is revealed as a tooltip. Shared secrets with restricted access will show the folder name as 'Restricted Folder'. Root folders will display the folder name as 'None', and when hovering the mouse over a root folder, it will display as 'No Folder'.
- When a user attempts to launch from a different server than the one currently logged into in Web Password Filler and there are active recordings, a confirmation dialog will appear. This dialog will give the user the choice to either launch and close the existing recordings or cancel the launch and keep recording.

## Bug Fixes

- Web Password Filler would continuously open new tabs if users turned off the 'Secret Server Login New Window' setting through the Native Messaging Host.
- When users selected the '+' button on the Web Password Filler pop-up to add a secret, it would close the pop-up and not display the 'Add Secret' dialog.
- The Web Password Filler pop-up displayed an invalid logo when saving updated user inputs for username or password.
- Corrected an issue where the Web Password Filler required the 'Session Recording Limit' and 'Input Threshold' drop-down values to be the same number.
- Previously, when Web Password Filler encountered an error logging in it displayed a continually connecting window. In this release, Web Password Filler shows a connecting window with an error message.
- Web Password Filler sometimes automatically logged in when a user logged into Secret Server or Platform in the browser, even though the current URL in Web Password Filler did not match.
- Previously, if the platform user had clicked the 'Cancel' button during a challenge, logged out, then attempted to log in again while the Web Password Filler pop-up was open, the user encountered a challenge pop-up instead of logging in.
- When using Safari 17 the Web Password Filler pop-up would close once the MFA challenge was completed.
- When Safari 17.1 was used, it displayed font weights incorrectly for field labels.
- In Safari 17.1, it did not show a warning when a user launched an incognito tab and the extension was not allowed in private browsing mode.
- In Safari 17.1, certain images in Web Password Filler failed to display.

## Known Issues

- When Web Password Filler is logged into platform and a browser tab is open to the same platform tenant that is logged out or times out, Web Password Filler will not be able to refresh its token and will log out. This will be fixed in a future release.

## 3.7.1 Release Notes

---

December 13th, 2023

### Bug Fixes

- Fixed an issue in Safari 17.1 on the MAC Sonoma platform where the login window stayed minimized in the task bar.
- Fixed an issue when logged into Platform the user would get logged out before their session expired.
- Fixed an issue so that users can now launch a secret successfully if Native Messaging Host is configured with the URL without any protocol.

## 3.7.0 Release Notes

---

November 7th, 2023

### Features

- Users will now see a list of Recent web secrets that is consistent with the Recent secrets list they see in their Secret Server web portal view.
- Users will now see a list of Favorite web secrets that is consistent with the Favorite secrets list they see in their Secret Server web portal view.
- Users can **search** for any of their web secrets from the Recent list in the Web Password Filler using any searchable field.

### Improvements

- Web Password Filler now displays a message when launched from a different Secret Server vault than what is configured for that Web Password Filler by the Native Messaging Host
- Improved the usability of the template selector drop-down menu

### Bug Fixes

- Fixed an issue where the Save button was getting enabled after filling in mandatory fields in the *Add Secret* window.
- Fixed an issue where Web Password Filler displayed an "Platform Identity Authentication has failed" error message when logged into the Delinea Platform.
- Fixed an issue with slow page performance when Web Password Filler is enabled.
- Fixed an issue where Web Password Filler was accepting a "0" value in numerical dropdown fields.
- Fixed an issue where Web Password Filler was displaying improper styling on certain sites.
- Fixed an issue where keyboard shortcuts were not working correctly.
- Fixed an issue where Web Password Filler failed to launch a secret for users who did not have the *Add Secret* permissions.

## Release Notes

- Fixed an issue where users were unable to click the *Login* button.
  - Fixed an issue where Web Password Filler was not auto-filling BitBucket login pages and for a few other sites.
  - Fixed an issue where session recordings missed a few seconds at the beginning.
  - Fixed an issue where the *Add Secret* button was not disabled on blank pages.
  - Fixed an issue where *Save* and *Update* features were not working on some sites.
  - Fixed an issue where Web Password Filler displayed an "Invalid URL" error message while refreshing secret.
  - Fixed an issue where Web Password Filler was adding extra spaces when copying the username to the clipboard.
  - Fixed an issue where Web Password Filler was not displaying a "Bad Request" message if a user entered an invalid URL.
  - Fixed an issue where the copy button was causing URL text or usernames to be overridden.
- 

### 3.6.1 Release Notes

---

August 22nd, 2023

#### Bug Fixes

- Fixed an issue where Web Password Filler was displaying an *Invalid email* or *Invalid password* error when users attempted to access the password page on certain sites.
- 

### 3.6.0 Release Notes

---

August 21st, 2023

#### Features

- When logged into the Delinea Platform, users can access secrets guarded by an MFA challenge. Upon successful completion of the MFA challenge, users can launch the site, copy the password if permitted, see secret details, and complete other allowed actions.

#### General Improvements

- Improved session recording stability.

#### Security Improvements

- Updated third-party libraries to address discovered security vulnerabilities.



## Bug Fixes

- Fixed an issue where passwords were not being auto-filled on certain sites.
- Fixed an issue where the Web Password Filler icon was appearing in fields that were not login form fields.
- Fixed an issue where the *Check in* functionality was not logging out users from the site when they checked in the secret.
- Fixed an issue where the session recording was not stopping when the user was logged out due to check out expiring.
- Fixed an issue where users were not able to log in to Web Password Filler automatically via SAML.
- Fixed an issue where all URL fields were being autofilled with the site URL value.
- Fixed an issue where Web Password Filler was not displaying correctly when users upgraded to the latest version of Chrome.

## Known Issues

- As a result of fixing the issue with false positive field matches, secrets are not being autofilled on Microsens portals. This will be fixed in the next release.
- 

## 3.5.4 Release Notes

---

July 20th, 2023

### Improvements

- When users attempt to access a secret that is guarded by MFA, they will see a message that the secret is blocked by an MFA challenge.
- Added a usability improvement to make the drop down URL field less confusing when there is no URL selected.
- Added a toggle to enable/disable cursor tracking on session recording.

### Bug Fixes

- Fixed an issue where a **Continue** button was being displayed in the *Comment required* popup, instead of **Checkout**.
- Fixed an issue where the "Add Secret" button was not disabled on a blank page on Firefox.
- Fixed an issue where Web Password Filler was not launching a secret without an *http* protocol.

## 3.5.3 Release Notes

---

June 20th, 2023

## Features

- Users can login to their Delinea Platform tenant URLs with Web Password Filler. Web Password Filler will connect seamlessly to their Platform tenant vault and users will be able to use web-based secrets in the vault in the same way as they do today with a direct Secret Server vault integration.

## Bug Fixes

- Fixed an issue where the self-signed certificate message was being displayed on various sites with valid certificates.

## 3.5.2 Release Notes

---

May 30th, 2023

### Features

- Users can login to their Delinea Platform tenant URLs with Web Password Filler. WPF will connect seamlessly to their Platform tenant vault and users will be able to use web-based secrets in the vault in the same way as they do today with a direct Secret Server vault integration.

### Bug Fixes

- Fixed an issue where Web Password Filler was not recognizing previously trusted vaults.
- Fixed an issue where a label was missing on the *Preferences* page when no URL was configured.
- Fixed an issue where Web Password Filler was displaying an error with the text *Null is not an object* instead of *Invalid error*.

### Known Issues

- Audit session recordings can be found in the vault direct web portal (Secret Server web UI). The ability to send audit session recordings to the Delinea Platform will be added in a future release.

## 3.5.1 Release Notes

---

May 12th, 2023

### Bug Fixes

- Fixed an issue where Web Password Filler did not recognize previously trusted vaults.

### Known Issues

- Web Password Filler 3.5.1 temporarily removes support for the Delinea Platform. This feature will be reinstated in a future version.

## 3.5.0 Release Notes

---

May 8th, 2023

## Features

- Users can login to their Delinea Platform tenant URLs with Web Password Filler. WPF will connect seamlessly to their Platform tenant vault and users will be able to use web-based secrets in the vault in the same way as they do today with a direct Secret Server vault integration.

## Bug Fixes

- Fixed an issue where users could not press "Enter" in the *Enter URL* field to advance to the next step of the setup wizard.

## Known Issues

- Audit session recordings can be found in the vault direct web portal (Secret Server web UI). The ability to send audit session recordings to the Delinea Platform will be added in a future release.
- Users may see a popup saying *Web Password Filler does not recognize vault URL as a trusted vault*. The workaround is to login to the vault from the WPF popup login screen. A successful login would create a trusted-vault entry in the Web Password Filler cache. This is a one-time action that the user would not need to repeat again for that browser.

## 3.4.4 Release Notes

---

April 3rd, 2023

### Bug Fixes

- Fixed an issue where Web Password Filler was not filling out user credentials for certain sites.
- Fixed an issue where the *Add Secret* window remained open after logging out of Web Password Filler.
- Fixed an issue where Web Password Filler was not autofilling secrets enabled to work only in incognito mode.

## 3.4.3 Release Notes

---

March 15th, 2023

### Features

- If a user enters a Secret Server URL without a protocol, Web Password Filler will set *https://* as the default protocol and will allow the user to login as if they entered *https://* from the outset.

### Security Improvements

- Added security improvements that prevent malicious pages from exploiting Web Password Filler functionality to change the URL of a user's Secret Server and read user requests to fill out forms.

### Bug Fixes

- Fixed an issue where Web Password Filler was cropping the session recording videos
- Fixed an issue where Web Password Filler was not filling out passwords for certain sites

## Release Notes

- Fixed an issue where the *Add Secret* button was enabled for users who did not have permissions to add secrets

### 3.4.2 Release Notes

---

December 5th, 2022

#### Features

- Web Password Filler now redirects Secret Server URLs containing *http* to *https*
- If a user mistakenly types *https:/* or *https:///* in the URL field, Web Password Filler will auto-correct these to *https://*

#### General Maintenance

- The EULA link in *Settings* was updated to point to Delinea's Master Subscription and License Agreement

#### Bug Fixes

- Fixed an issue where nothing would happen when the user clicked "+" to add a secret in Chrome on a Mac
- Fixed an issue where Web Password Filler would not auto-populate when using URL lists
- Fixed an issue where users with *View Only* permissions were unable to use URL lists
- Fixed an issue where Web Password Filler was not properly handling special characters when adding a secret
- Fixed an issue where the *Copy Generated Password* functionality was not working
- Fixed an issue where Web Password Filler was not filling in passwords for some sites
- Fixed an issue where session processing would take too long for sites mentioned in extended mapping
- Fixed an issue where Web Password Filler was overwriting other mapped fields if the input type was "password"
- Fixed an issue where the *Comment Required* popup was not appearing when the "Hide Secret Server Version Number" setting was enabled
- Fixed an issue where the silent login window was not disappearing once the user disabled the *Use Secret Server To Login* toggle
- Fixed an issue where the Secret Server configuration URL field remained clickable when native messaging host was configured
- Fixed an issue where Web Password Filler would display an error message when redirecting from *http://* to *https://*
- Fixed an issue where the session recording icon continued to appear even after the user logged out from Web Password Filler.

#### Known Issues

- The "+" icon is not working properly on Safari version 15.1. However, the "+" icon is working properly on Safari versions 15.2 and newer

## 3.4.1 Release Notes

---

*September 23rd, 2022*

### Bug Fixes

- Fixed an issue where users were denied access to Viewing Secrets, Adding Secrets and Editing Secrets in Web Password Filler version 3.2
- Fixed an issue where Web Password Filler was prompting users to create a secret when logging into a site that already has a secret
- Fixed an issue where the web launcher was not honoring field mapping for the Username
- Fixed an issue where Web Password Filler was not working properly on the VMWare Horizon login page

## 3.4.0 Release Notes

---

*August 18th, 2022*

### Features

- Users can now add comments when checking out secrets that are configured to integrate with ticketing systems. Additionally, this workflow also applies to sites that are restricted to incognito mode access.

### Product Enhancements

- Implemented updates to support autofill with:
  - <https://auth.ncloud.com>
  - <https://reporting.retire-it.com>
  - <https://sso.redhat.com>

### Bug Fixes

- Fixed an issue where Web Password Filler did not fill in the username and password when launching a site from the URL field and Session Recording was enabled on the secret.
- Fixed an issue where Google profiles would get logged out when session recording is enabled.
- Fixed an issue where Web Password Filler would not autofill websites launched from Secret Server when Web Launcher required Incognito Mode to be enabled.

## 3.3.0 Release Notes

---

*June 21th, 2022*

### Features

- Web Password Filler has been updated to reflect Delinea Inc.'s rebranding along with our new company colors and icons.

## Release Notes

- Web Password Filler now offers dropdown functionality for selecting domains fields on the configuration page.
- Web Password Filler now offers a dropdown list for logging on to more than one Secret Server.

## Bug Fixes

- Fixed an issue where Web Password Filler intermittently shows an error popup after populating secret for <https://www.portal.azure.com> or <https://portal.office.com>
- Fixed an issue where an add comments popup appears on the Current Active tab instead of launching the URL in another tab if a Requires Comment-enabled secret launches from the Recent/Favorite tab.
- Fixed an issue where Web Password Filler was not showing a popup message when the connection with Secret Server was lost while session recording was in progress.
- Fixed an issue where the Thycotic icon would appear while creating a new user in Secret Server version 11.1.6.
- Fixed an issue where the Secret list was not appearing and the Web launcher was not working for SSO sites.
- Fixed an issue where an update password popup would appear after a user updates the username of a secret.
- Fixed an issue where the user would need to manually reload Secret Server webpages opened in the browser.
- Fixed an issue where the Customized Web Launcher UI Popup was not displaying properly.
- Fixed an issue where the secret name was overlapping with other secrets in the Recent tab if the name was very long.
- Fixed an issue where the Metadata (xpath) for Web Password Filler was not working.
- Fixed an issue where the Add Secret "+" button was enabled when a user, who does not have permission to add a secret, logged into Web Password Filler.
- Fixed an issue where Web Password Filler was displaying an error popup when updating a password.
- Fixed an issue where Web Password Filler was not refreshing secrets properly.
- Fixed an issue where UI elements on the Configuration page were not properly aligned when Web Password Filler was displaying an error.
- Fixed an issue where Web Password Filler closed launched tabs when left idle for 5 - 25 minutes and caused Google Chrome to freeze.
- Fixed an issue where Web Password Filler was showing a blank secret information page.

## iOS Specific

- Fixed an issue where the iCloud - Secret template dropdown was not working properly.
- Fixed an issue where the Notes field didn't resize in the Add Secret window in Safari.

## 3.2.0 Release Notes

---

*February 9th, 2022*

## Product Enhancements

- Added support to list minimum supported version on logging page and log file downloads as .txt file formats. Refer to [Enable Diagnostic Logging](#).
- UI overhaul of the [Add Secret](#) workflow.
- A comment or note can now be added to a Secret. Refer to [Comment Required](#).
- After adding, changing, or deleting a Secret, users have the option to refresh their [favorites](#) list. Recent is a list of recently accessed secrets through WPF, whereas Favorites is a list based on the favorites setting of secrets in Secret Server.

## Bug Fixes

- Support was added for the web launcher, mapping, and session recording to correctly work with <https://dcwebc.farelogix.com/sprk-lhg/>
- Secret policy didn't apply when the was secret added via WPF.
- Fixed an issue which caused a 400 error when launching Secrets, despite the users being logged in.
- WPF with recording - Crowdstrike Falcon agent on MacOS causes Chrome thread high CPU and unresponsive browser when launching to [myapps.microsoft.com](https://myapps.microsoft.com).
- Resolved an issue when after an URL change the session recording stopped.
- Resolved issues with the Recent and Favorites tab in version 3.1.
- Infinite loop issue with WPF 3.1 with Microsoft Edge when logging in with the option "Secret Server - Login New Window disabled".
- Fixed problems with multiple URL fields not being recognized as URLs and as such not being auto-populated.
- Issues with auto population of username and password in WPF 3.1.
- WPF does not autofill passwords for sites with SSO.
- WPF 3.1 does not populate fields on secrets with Incognito Mode and Hide Launcher Password set to Yes.
- Resolved an issue with WPF secrets being opened in new Window, which left users on the last tab following the token generation.
- Resolved permission issues for "portal.azure.com" and subsequent sites.
- Resolved an MSFT Edge issue with unused secrets.
- Improved error messaging with Password Validation on Create relating to specific templates.

## Known Issues

- The drop-down divider is missing when selecting a template other than Web Password.
- WPF is unable to map secrets when the mapping field is in an IFrame.
- On integrations with ticketing system, secrets with checkout that are requiring a ticket number for the comment may not get checked out successfully.
- Metadata won't work for cases where a comment is required with the secret checkout.

## Browser Related

- With Safari v15 or above, Session Recording is not supported. This issue is due to Safari not executing RDP calls and as such session recording is not working.
- When using the Safari browser on a virtual machine, the WPF extension UI does not render correctly, causing text overlays.

## 3.1.0 Release Notes

---

*October 21, 2021*

### Product Enhancements

The user interface of the Web Password Filler has been redesigned for improved usability.

- The main WPF window, which opens when you click the active Web Password Filler icon in the upper right corner of your browser, displays two new tabs. One tab lists Recently-used secrets and the other lists secrets the user has marked as Favorites, for quick access.
- The footer of the main WPF window now indicates the URL of the Secret Server the user is logged into.
- When a user hovers their cursor over a Secret in the main WPF window, a Fill icon appears. If the URL in the secret matches the URL of the active browser tab, clicking the icon fills in the user's credentials on the page. If the URL in the Secret does not match the active browser tab, clicking the icon brings the user to the page matching the URL in the Secret, where credentials can be filled in.
- When a user clicks anywhere on a Secret panel in the main WPF window, the Secret Details view opens. When a user hovers their cursor over the URL, Username, or Password fields, a new Copy icon appears that the user can click to copy the content of that field. The user receives a Toaster confirmation when the information is copied. If the user attempts to copy a password that they lack permissions to view, a popup explains that they cannot copy it.
- Web Password Filler can now be configured to have the Secret Server Login Window open in a new browser tab when the user disables or turns off the setting "Secret Server Login New Window."
- When a user is accessing a website with a checked-out secret and the maximum checkout time has passed, WPF closes the associated path and deletes the cookies, ending the user's logged-in session for improved security. The user then needs to check out the secret again to re-access the site through the Web Password Filler.

### Known Issues

- Chrome Version 92 and higher limits the screenshot rate to two screenshots per second. This may impact session recording, resulting in jumpy video, or in missed captures of clicks and keystrokes.
- Safari does not support HTTP, so you must use a properly-formed HTTPS URL to connect to Secret Server.
- If a user requests access to a Secret that requires approval but the user does not have that approval, the user receives a message indicating that access to the secret is denied.
- When RegEx values are not valid, Web Password Filler displays an error message indicating that the user



## Release Notes

should contact their administrator for more information. Your Administrator may need to correct the RegEx pattern in the template on Secret Server.

### Bug Fixes

- Web Password Filler now populates login information for Blumira.com.
- Web Password Filler now populates login information for jira.
- Web Password Filler now populates login information for oasis.thig.com/.
- Web Password Filler now supports login using Smart Cards.

## 3.0.1 Hot Fix Release Notes

---

August 3, 2021

### Product Improvement

Resolved an issue where the client side cache got cleared on a version update, causing simultaneous API calls to Secret Server to rebuild the cache. Added client side storage to reduce the number of API calls made by WPF when the cache gets cleared by the browser.

### Bug Fix

In some situations, the Web Password Filler 3.0.0 extension populated the password field with ***Not Valid For Display*** instead of the real password. This happened when the user did not have permission to view the password due to a newer method used in that release. This issue has been resolved in this hot fix.

Please refer to [3.0.0 Release Notes](#) for more updates.

## 3.0.0 Release Notes

---

July 16, 2021

### Improvements

- **New User Interface Elements:** New UI design elements have been added to several pages including the home page, login experience, preferences with toggle switches, and a link to launch Secret Server via WPF.
- **Session Recording:** Previously when a session recording was active on a Chrome browser tab but the user was inactive in the browser/tab for more than five minutes, Secret Server assumed the session had ended. Now a "heartbeat" is sent every two minutes to let Secret Server know that the session is still alive even though the user is not interacting with it.
- **Field Mapping:** Some websites use unconventional labels to internally identify their username, password, and other login fields, and the Web Password Filler cannot automatically identify these fields. Users can map the fields on the Web page to the fields in the Secret using intuitive drag-and-drop functionality. To enable the field mapping function in the Web Password Filler, an administrator must add a new metadata section in Secret Server named WPFHints, which saves the field tag mapping information on the Secret.

## Release Notes

- **Safari Support:** The Safari Web Password Filler extension now supports all functionality available in the other supported browser extensions.
- **Switch to the logged-in Secret Server:** When a Web Password Filler user launches a Secret from an instance of Secret Server that is not configured for WPF, WPF now prompts the user with the message, "Do you want to switch to the logged in Secret Server?" The user can then switch to the appropriate instance of Secret Server to complete their web login process.
- **Performance:** Fixed performance issues users were experiencing when installing or re-enabling the WPF extension for their browser.

## Bug Fixes

- Resolved issues on Hivemanager.krome.co.uk where WPF was filling the key value incorrectly.
- Resolved issues on the workday website where the username field was not being populated correctly.
- Resolved issues on the Data Domain System Manager website where the username field was not being filled in. In situations where this still poses an issue, customers can now use the field mapping wizard to map the username field so WPF can recognize the field and fill in values from the secret.
- Resolved issues and validated that WPF can fill in values on <https://falcon.crowdstrike.com/login/>

## Known Issues

### Issue

Some cloud customers may experience temporary latency issues when connecting to Secret Server. This issue should automatically resolve itself and no action is required.

### Issue

In some situations, the Web Password Filler 3.0.0 extension for Google Chrome will populate a password field with `***Not valid For Display***` instead of the real password. This happens when the user does not have permission to view the password due to a newer method used in this version. To resolve this issue, Delinea is releasing a hot fix. The three scenarios where this issue may occur are described below:

**The user does not have permissions to view the password in Secret Server because the *View Launcher Password* permission is not assigned to their Role.**

Solution: Assign the *View Launcher Password* permission to the role in which the user is a member.

**The secret (under the Security tab) has *Viewing Password Requires Edit* enabled and the user does not have Edit permissions (or in the older UI, *Hide Launcher Password* is set to Yes)**

Choose one of these three work-arounds:

- Set "Viewing Password Requires Edit" to **No**.
- Give the user **Edit** permissions.
- Use Microsoft Edge, Firefox, or Safari to access the web sites.

### The template used for the secret has *Viewing Requires Edit* enabled for the password field and the user does not have Edit permissions

Choose one of these three work-arounds:

- Set "Viewing Password Requires Edit" to **No**.
- Give the user **Edit** permissions.
- Use Microsoft Edge, Firefox, or Safari to access the web sites.

## 2.0.6 Release Notes

---

May 25, 2021

### Improvements

Web Password Filler now provides improved performance for session recording.

### Bug Fixes

- Resolved issues where WPF was not working on some sites; `massmutual.okta.com`, `hitachi IAM`, `idp.secureworks.com`, `online.adp.com`, `photovisi.com`, `oracle weblogic server`, and `greenshadesonline.com`.
- Resolved an issue of WPF failing to exclude very long URLs that were on the Native Messaging Host (NMH) exclusion list. Web Password Filler now optimizes the query string and evaluates it for exclusion before sending the URL to the NMH.
- Resolved an issue of the Time-based One Time Password (TOTP) function failing in Web Password Filler when the browser language was not set to English. Web Password Filler now includes the localized TOTP messages that ship with Secret Server.
- Resolved an issue of session recording failing on sites that contained `iframe` or `frame` sets if the SRC value was in both the parent and child. WPF now ensures that it does not attempt to record the same tab twice regardless of child window source.
- Resolved an issue of Web Password Filler incorrectly displaying the **Login with Secret Server** window on some high resolution screens not being positioned optimally or appearing minimized.
- Web Password Filler now correctly identifies a username field when the element type is a `textarea`.
- "USER\_IDENT" is used on some websites to identify the username field, and is now included in the Web Password Filler criteria for identifying a username field.

### Known Issues/Limitations

- When you click on a URL from a secret in Secret Server and you are not already logged into WPF, you will have to click the URL two times to launch it. The first click logs you into WPF and the second click launches the URL.
- On some sites with a single secret and auto-populate enabled, the username and password field are not immediately populated. Workaround: select the Delinea checkmark, then select the desired secret to populate.

## 2.0.5 Release Notes

---

March 30, 2021

### Features

- When you are signing into Secret Server through WPF, a token is automatically generated for you. A window opens briefly showing the Generate Token button being pushed automatically, then the window closes.
- When you are logged into both Secret Server and Web Password Filler and you then log out of Secret Server, you are now automatically logged out of Web Password Filler.
- When you are logged into Secret Server and you click on a URL where you have a Secret configured, you will now be automatically logged into WPF, have a token generated for you, and have your credentials populated into the sign-in fields for the website.
- You can now specify the position for your pop-up Secrets list to appear: in the upper right corner of your window (default) or just below the username field, using the [Native Messaging Host](#) configuration file.
- When you are connected to WPF and you close your browser window without logging out, you will remain connected to WPF when you re-open your browser. You will still be logged into WPF for the duration of your web session timeout specified in Secret Server. In enable this feature, you must use the [Native Messaging Host](#) configuration file.
- When you are recording a session in an incognito window and the session recording ends due to a recording timeout limit (default 2 hours), WPF will close only those tabs where the session recording ended due to a timeout limit.
- Users and administrators can now extend the default recording time of two hours for a session to a maximum of eight hours, using the [Native Messaging Host](#) configuration file.
- You can now choose to have WPF require exact URL matches. If you choose this setting and the URL you browse to is not an exact match for the URL stored in the Secret, WPF will not display the Delinea checkmark logo and will not automatically populate your credentials into the website's username/password fields. See [Native Messaging Host](#).
- In Safari, WPF now prompts the user with a message when using a secret that requires check out.
- When WPF encounters errors in the Native Messaging Host JSON file, it now logs those errors in the native-messaging.log file.
- You can now manually refresh your list of available Secrets by right-clicking the Delinea checkmark logo in a credentials field, clicking Secret Server Web Password Filler, and clicking Refresh Secrets. See [Native Messaging Host](#).

### Bug Fixes

- Resolved an issue of WPF automatically populating values on some websites even when auto populate was deselected.
- For security reasons when you log out of Secret Server, you will be logged out of WPF as well, even if you were logged in as two different users. This is expected behavior.

## Release Notes

- Resolved an issue of WPF not adding some alphabet characters to fields when adding a Secret using “Add Account to Secret Server.”
- Resolved an issue of WPF generating an error related to Secrets with Checkout enabled.
- Resolved an issue of WPF generating a 400 Error when launching Secrets from Secret Server via WPF.
- Resolved an issue of WPF not detecting Secret Server login when using Duo MFA.
- Resolved an issue of WPF opening an extra blank tab when launching a webpage in Incognito mode.
- Resolved an issue of WPF filling the username field on the Microsoft authentication TOTP page.
- Resolved an issue of the Login button being grayed out when the WPF launcher populates credentials or launches a Secret.
- Resolved an issue of WPF being unable to find username controls on the Oracle WebLogic Console login page.
- Added logic to retry and stop when pages became unresponsive attempting to overwrite WPF changes to the background image.
- Resolved an issue of WPF prompting the user to enter credentials on a new page after they have already logged into that website.
- Resolved an issue with service now incident time logs page being auto filled by secret credentials
- Resolved an issue in the Safari browser after the user clicks “Show All,” of WPF displaying only the window in focus while leaving the non-focused windows in the background.
- Resolved an issue in the Safari browser of WPF not closing the About popup window.
- Resolved an issue in the Safari browser of WPF not correctly identifying a username field named “usr.”
- Resolved issues of WPF filling undesired form fields on multiple websites, including the following:
  - IBM Storewize V7000
  - Imperva Securesphere Management
  - Kaseya VSA, Daffron Customer Information Systems
  - Oracle netsuite and slm.saas.services
  - Various sites reported by IH Mississippi Valley Credit Union
  - Various internally-developed Web apps
  - <http://isupportsvr1/rep>
  - <http://premieragent.zillow.com/crm/agentlogin>
  - <https://cmpame.cmpa.org>
  - <https://comp.makonetworks.com>
  - <https://hqprrsa02.cmpa.org:7004/console-ims>
  - <https://nystateofhealth.ny.gov/>
  - <https://prtg.centergrid.com/>

## Release Notes

- <https://secure.trust-provider.com/>
- [www.logicmonitor.com](http://www.logicmonitor.com)

## Known Issues and Limitations

- If session recording is ON and you make changes to the extensions settings via managed extensions, the recording may take a few minutes to stop. This is because when changes are made to the extension, the WPF connection is broken and has to be reestablished.
- If you are attempting to log into WPF using the Firefox browser and you do not have a valid and active license for Secret Server, the generate token page refreshes repeatedly. In chrome and chromium the page appears just once.

## Answers to FAQs

- On macOS Big Sur 11.0.1 and 11.2.0, some WPF tabs can appear distorted. To correct this issue, please upgrade your macOS OS to the newest version.
- WPF now supports Safari running on the following macOS versions: Catalina, Mojave, Big Sur 11.1.0, 11.2.1 and later.
- Live Session Monitoring is not supported for sessions recorded by WPF.
- The Diagnostic button is visible when you are on a website. It is not visible when you open a blank tab or a new window.
- If you are logged into Secret Server and WPF as the same user or as different users, when you log out of Secret Server you will be logged out of WPF also. This is expected behavior because, for security reasons all cookies are cleared for the instance when you log out of Secret Server.
- [accounts.booking.com](https://accounts.booking.com), [login.booking.com](https://login.booking.com), [trips.booking.com](https://trips.booking.com) are all the same "site" and do not violate cross scripting rules so everything that is accessed in one, can be accessed in another. They share a token / login. When a session ends, all associated sites / pages / tabs are closed and cookies are deleted for security reasons to prevent accidental capture. Using the incognito window eliminates this issue by allowing you to have an independent recording session for [accounts.booking.com](https://accounts.booking.com) and another for [login.booking.com](https://login.booking.com).

## 2.0.4 Release Notes

---

*December 23, 2020*

### Enhancements

- The WPF Safari browser extension currently supports macOS versions Catalina, Mojave, and Big Sur 11.1 and later. Also refer to Known Limitations below pertaining to the Safari browser.
- [Incognito Support](#) for web launched secrets in a browser.

### Bug Fixes

- Resolved issue with WPF icon not rendering correctly in login dialogs.
- Resolved issues for DUO login sites that prevented admin/owner tasks such as updates to the password:

## Release Notes

- Firefox: Solved duplicate drop-down entries.
- Opera: Solved login issues.
- Resolved issue with misleading error message being returned upon unauthenticated secret launch.
- Resolved a redirect issue with SAML enable for Okta and One Login integration.
- Resolved issue for sites that prevented the username or password for an existing Secret from being updated/populated:
  - premieragent.zillow.com/crm/agentlogin, fx.tourfactory.com, https://telepizza-sso.awsapps.com/start/#, https://www.spectera.com/PWP/Landing


## Known Limitations

- The WPF Safari browser extension currently does not include:
  - Support for macOS Big Sur 11.00 to 11.09x
  - Session Recording: If Session Recording is enabled on a secret, that secret will not be auto-populated/launched.
  - Windows Admin Center: The Safari Browser extension does not have Windows Admin Center support.

## 2.0.3 Release Notes

---

### Enhancements

- Added ability to set an exclusion list for site URLs:
  - Sites listed in the exclusion list will not have Secrets populated into the Username/Password fields by default. Secrets can still be populated in these fields by clicking the Green check icon to autofill. This should help prevent none username/password fields from having values filled in them automatically even if they are identified as username/password type fields
  - An “Exclusion exception” list also exists so specific pages on the site domain will still auto-populate as normal.
  - This can be set per-user or generally on the machine and WPF reads the information from a [local Json file using the web browser’s native services](#). This does require an additional .NET 4.5.2 app to help roll out the local JSON file.
    -  **Note:** The user story is that the exclusion list is set to exclude a site at URL `Company1.site1.com` but has an exclusion exception for `Company1.site1.com/login.aspx`. In this case if they navigate to the login page then the secret will auto-populate in the login fields (if users only have 1 secret). After users login and go to any other page on the site that also has fields which are detected as username/password type fields, the Web Password Filler will not do anything unless directed by the user. This is to prevent the Web Password Filler from auto filling values in fields, when the auto fill action is unwanted.
- Added a new “Site” drop down option to the “Add Secret” dialog in the Web Password Filler, to allow users to select which Secret Server Distributed Engine site a Secret should be saved to (defaults to “Local” value)

## Security

- Added sanitization on Secret Server Secret name on the pop-up display to prevent JavaScript code (using script code in the Secret name) from allowing the website to create an opening using the Secret name for access.

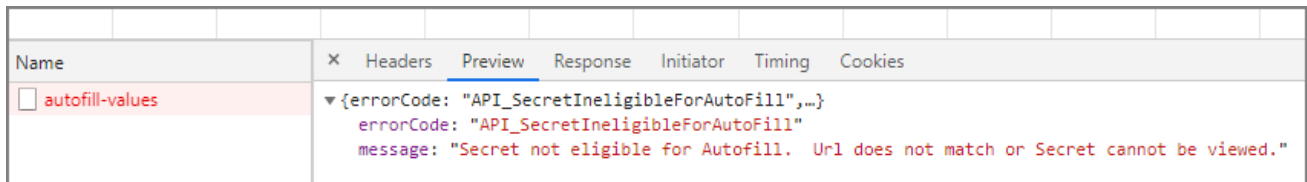
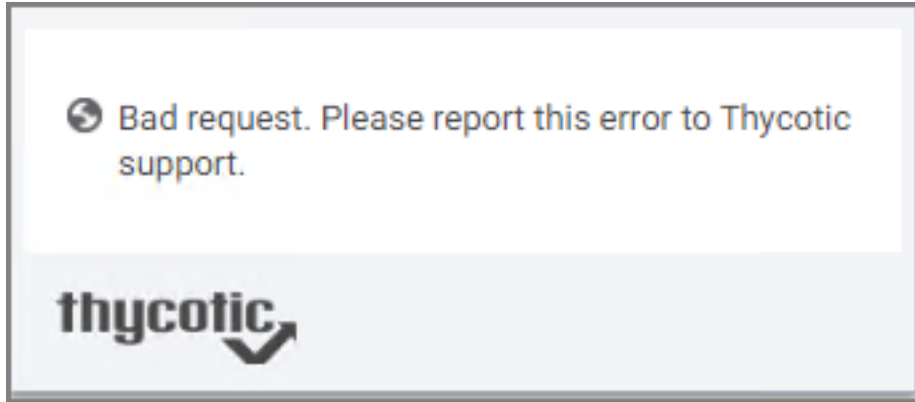
## Bug Fixes

- Resolved an issue with a PaloAltoNetwork site that prevented the Password from auto filling after selecting the Secret.
- Resolved an issue with the Cisco APIC console returning a “Token Error” message after the login fields were populated and the user tried to log in.
- Resolved an issue for a Wells Fargo site login (<https://wellsoffice.ceo.wellsfargo.com>) where the “Login” button was still disabled by the site after the login fields were populated with valid values.
- Resolved an issue with the Delinea Force Customer portal login that prevented the site from reading valid values in the login fields when the “Log in” button is clicked.
- Resolved an issue that returned the message “Enter a value in the User Name field” even when a value was entered by the Web Password Filler on <https://delinea.force.com/support/s/login>.
- Resolved an issue that displayed a deleted Secret in the Secret list for a site, if the user deleted the secret in Secret Server after they logged into the Web Password Filler, but before the WPF refreshed its list.
- Resolved an issue for DUO login sites that prevented the page URL from being captured in the “URL” field when adding a new Secret on the “Add Account to Secret Server” dialog.
- Resolved an issue that prevented users from logging into the Web Password Filler with multiple Identity Providers configured and the Secret Server URL ending with a double slash (for example, <https://Domain.Company/SecretServer/>)
- Resolved issue for sites that prevented the username or password for an existing Secret from being updated:
  - <https://adobeid-na1.services.adobe.com>, <https://secureb.eyefinity.com>, <https://admin.zscaler.net>, <https://app.zipbooks.com>, <https://mibank.com>, <https://www.economist.com>, <https://www.internic.ca>, <https://www.svbconnect.com>, <https://id.getharvest.com>, <https://login.bnymellonwealth.com>, <https://www.sumopaint.com>

## Known Issues

- A delay may occur and trigger an error message due to indexing on the Secret Server side after a URL change for Secrets that are setup for an exact URL match. The error message will state that the exact domain doesn't exist.





The **workaround** is to try again after about a minute.

## 2.0.2 Release Notes

---

### Enhancements

- Added a Secret Server-side check to determine if launching a Secret from Secret Server should always use the URL from the Secret or the value from an internal Secret Server table (requires Secret Server release version 10.9). To enable this, refer to Secret Server Configuration information.

| LAUNCHER SETTINGS                                   |                  |
|---|------------------|
| Enable Launcher                                     | Yes              |
| Launcher Deployment Type                            | Protocol Handler |
| Enable Protocol Handler Auto-Update                 | Yes              |
| Send Secret URL to Launcher                         | Yes              |
| Allow Secret Server to Retrieve Website Content     | Yes              |
| Allow Web Launcher Mappings to be Downloaded        | Yes              |
| Allow Web Launcher Mappings to be Uploaded Off-site | Yes              |
| Check In Secret On Launcher Close                   | Yes              |
| Close Launcher on Check In Secret                   | Yes              |

- Added Windows Admin Center support. Refer to [Windows Admin Center](#) topic for details.
- Added an additional check on user name related fields (like User name, phone number and email) to see if they have a "searchable" attribute and will no longer populate the Delinea check logo in the field.

### Bug Fixes

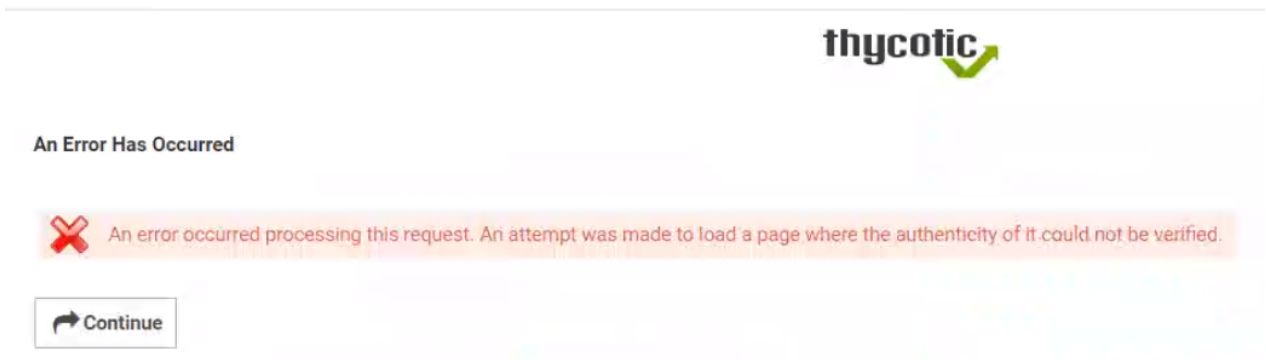
- Resolved an issue when a website used multi-page logins or page redirect during while launching a web password secret from Secret Server, resulting in Secret Server sending a different URL to Web Password Filler. This is resolved by the above Secret Server-side check and setting the launcher option in Secret Server.
- Resolved an issue that prevented the password from being filled for logins on sites:
  - www.businessdirect.att.com
  - login.tenable.com
- Resolved an issue where Secret Server instances that use Windows Authentication caused Web Password filler to prompt users to generate a new login token (for a second time) even if they had already generated a token.

## Release Notes

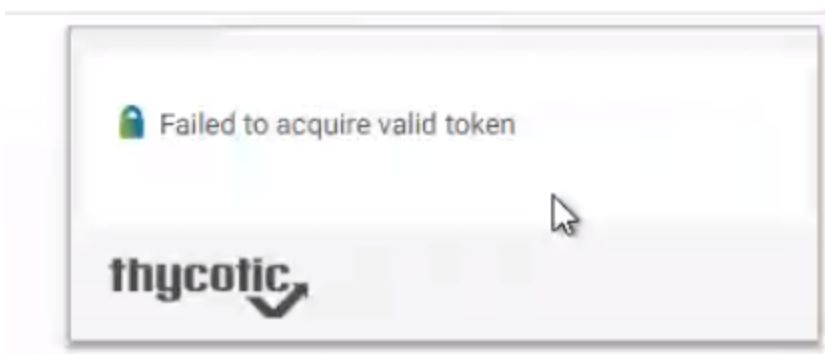
- Resolved an issue where logging into a Microsoft Online account with a username that is in all capital letters results in the password field being cleared (by the site) when it redirects to the password page.
- Resolved an issue for browser tabs being closed when multiple Secrets (with session recording) are launched in the same browser for the same IP address (but with different port numbers). Resolution does require an additional IP address: port value pair to be added to the RegEx field in Secret Server.
- Resolved issue for a site where the auto-fill values from the secret were being entered into the fields and then cleared out by the site.

## Known Issues

- If you have multiple identity providers and attempt to log in multiple times (for example, open WPF and click login, then open WPF again and click login a second time) an error is triggered after clicking the login button the second time, and one of the following messages can appear:
  - Secret Server displays an error that the authenticity of the page could not be verified.



- WPF shows an error on those pages that were not used to log in



This is expected behavior. The first log in will be successful and the user will be logged into WPF. There is no reason to have the additional tabs open and the user can simply close the additional tabs.

- If WPF Secret Server configuration has two back slashes at the end of the URL, the generated token does not appear to work. Resolution, remove one of the back slashes:
  - incorrect -> `https://mysecretServer//`
  - correct -> `https://mysecretServer/` OR `https://mysecretServer`

## 2.0.1 Release Notes

---

### Enhancements

- Added ability to check permissions for logged in users and only display options/folders based on those permissions.
  - Users only see the “Add Secret” option if they have permissions to add a Secret.
  - When adding a Secret, users see folders in the drop-down based on their permissions only and they won't see folders with “Read” permissions.
  - Secrets with "Read" access only have improved error messages.
- Improved support for Microsoft Online login sites that use multiple domains for Username/password logins on separate pages.
  - This applies for sites like login.live.com, microsoftonline.com, etc.
  - This is WPF side support for page “refer” links in page header.
- Added “alarm” notification for when users are reaching maximum session recording timeout of 2 hours.
- Modify back-end support for Refresh Tokens to use “alarm” based system.
  - This helps to prevent token read errors for the browser.
- Improved support for sites that force the username list to display on top of the Web Password Filler drop-down on the Username field (and prevent the overlap).
- Added additional “Remember for this site” options on WPF security pop-ups for sites with multiple domain logins.

### Bug Fixes

- Security: Fixed a JavaScript code injection issue.
- Fixed an issue where the “Refresh” icon is not displayed on the Secret list intermittently.
- Fixed styling issues for “Save your password” dialog for “Launchpad” site.
- Improved error handling and error message when no folders are found on “Add Secret” action.
- Fixed an issue where the web browser was improperly reading the login token and preventing login from the Web Password Filler.
- Fixed an issue where the password values was not entered for site: Infragard.
- Fixed an issue where an incorrect "Bad request" message was being displayed during login on some Microsoft sites.
- Fixed an issue for multiple sites where the prompt to save a new set of credentials is skipped/cleared too fast because the login page transitions to the completed login page before the prompt can be displayed for the normal time delay is complete.
- Fixed an issue with the site: QRadar that had the site prompting an error due to a conflict with the WPF extension/add-on.
- Fixed an issue where the password does not populate correctly for the site: Knowbe4.com.

## Release Notes

- Fixed an issue where the username and password fields do not fill correctly for Cisco WebEx login pages.
- Resolved an issue where login credentials for site: [www.client-central.com](http://www.client-central.com) did not populate in the appropriate fields.
- Firefox: Resolved an issue where web browser was not redirected to SAML login page.

## 2.0.0 Release Notes

---

### Enhancements

- Web session recording is now supported in the Web Password Filler. If a web Secret is configured for recording, the Web Password Filler will now record the web session and any additional web browser tabs that are opened from that session (provided they stay on URLs that require recording). Refer to [Session Recording Redirects](#).
- If web session recording is configured to run for a site, but the site prevents the recording icon from being placed in the browser tab's title bar, the Web Password Filler will instead display a pop-up message that the session is being recorded.
- Improved support for the Refresh token. Secret Server improved the refresh token to better support SAML configured Secret Server environments, and the Web Password Filler has been updated to use this improved token. This also improves the timeout setting utilization for the SAML token.
- Added timing restricting to the "Refresh" button on the "Sign in as" pop-up window in the Web Password Filler. This is to limit the number of calls that can be made in a 10 second time frame from going back to Secret Server to update the list of Secrets.
- Added a new feature to match URLs by exact path. This option will look at the domain value in the URL and will only list secrets that have an exact match. When enabled this option will exactly match the cursive values in the example URL.  
  
Example, <https://Company.Sub.Primary.Domain/subsite>
- Improved support for sites that have multi-part top level domains, or parent domains in the URL. For example, this would include sites that have ".co.uk" or ".online.com", etc.

### Bug Fixes

- Fixed an issue, that returned a 500 error in the background when users tried to save a new Secret (using WPF) when the new User Interface is disabled in Secret Server.
- Fixed an issue, that did not display the "Add Accounts to Secret Server" dialog if you entered credentials (that are not in a Secret) into a site and tried to automatically save it as a Secret when Personal Folders are disabled for the Secret Server instance.
- Fixed an issue, where not all folders were being returned when adding a Secret, if the user had access to more than 1,000 folders.

## 1.1.0 Release Notes

---

### Enhancements

- WPF now identifies the Secret Server tab on browsers. No WPF pop-ups, icons, or other entities will appear on the Secret Server tab.
- Added some local caching. The calls to get Secrets and Secret templates was moved from login to when you click "Add Secret". This was done to help with performance when connecting to Secret ServerCloud. As a result, we will cache some of the Secret and Secret template information to help with overall performance instead of calling back on a frequent basis.
- New login has been implemented for fetching the fav icons. This has helped reduce a number of issues for fetching icons when displaying, listing, or adding Secrets.

### Bug Fixes

- Fixed an issue when after install if you saved the settings for "Use Secret Server to Login", the setting was not preserved after upgrade.
- Resolved issues on a few sites for the Delinea icon being added to the wrong place on the page (not displayed in the Username/email fields)
- Fixed an issue where the Delinea logo was added in the "First Name" field instead of in the Username/email field.
- Updated the text for the "Delinea Secret Server just updated your password" message so it is all displayed on the same line.
- Fixed an issue where on specific sites if you selected a Secret on the login page, the browser would navigate back to the previous page.
- Fixed an issue where a specific site was displaying two search bars and icons when the list of Secrets for the site is displayed in the drop-down.
- Addressed multiple issues with page "mutators" for specific sites.
- Fixed an issue when adding a Secret for some sites, the Template fields pop-up is not displayed until you refresh the page.

### Firefox Specific

- Fixed an issue specific to Firefox browsers where conflicting calls were causing delays for loading site, blank pages on some sites, or credentials not filled in credential fields.
- Fixed an issue where on Firefox a scroll bar is displayed for some of the pop-up dialog.

## 1.0.9 Release Notes

---

### Bug Fixes

- Changed the default refresh request time from 20 minutes to 24 hours only when logging in through Secret Server.

## 1.0.8 Release Notes

---

This plug in will connect back to the Secret Server instance to populate user accounts/passwords into the appropriate fields in a web browser session. In the web browser session users should be able to:

- Authenticate back to the Secret Server instance without directly logging into the Secret ServerUI - via REST API
  - Support Username/Password style login
  - Support Secret Server SAML login (Login using Secret Server)
- Identify the user/password fields for a login screen
- Identify and notify users that the web page login has an existing Secret Server Secret
- Allow the user to select a related Secret that they have access to, to use the credentials
- Take the selected Secret and auto populate the credentials in the correct fields
- Create a new Secret based on the web browser login page
  - Search for a specific Secret Server Folder to save the Secret/credentials into
  - Save the new credentials that are in the Login page fields as a Secret and send that data to the Secret Server instance
- Update/modify the passwords/account for an existing Secret and have that push back to Secret Server
  - Add a new password to an existing Secret and have that push back to Secret Server
- Allow users to generate a new Password for the Secret directly from the web browser
  - Base password generation on the standards that are configured in Secret Server
  - Give an indicator if an entered password meets the security requirements
  - Allow copying of this generated password to the clipboard to paste into the Password field (in case there are Password verification fields)
- Support 2FA and other authentication types that are currently supported for Secret Server
- Add information on the accessing/updating/creation of any Secrets to the Secret ServerAudit logs for that Secret
- Be able to identify that this access was from the Web Password Filler and not the Secret Server console

## 1.0.10 Release Notes

---

### Enhancements

- Increased the refresh interval for calling back to Secret Server to refresh the list of folders/templates.
- Moved the call to fetch Secret templates/folders from "on login" to when the "Add New Secret" option is selected to reduce network calls.
- Reduced the web browser based permissions required to run the Web Password Filler in the web browsers as an extension/add-on.

### Documentation Changelog

---

This topic provides a chronological list of documentation changes. Minor content alterations are not tracked.

## Release Notes

### November 2023

- ["3.7.0 Release Notes" on page 79](#)

### August 2023

- ["3.6.1 Release Notes" on page 80](#)
- ["3.6.0 Release Notes " on page 80](#)

### July 2023

- [3.5.4 Release Notes](#)

### June 2023

- [3.5.3 Release Notes](#)

### May 2023

- [3.5.2 Release Notes](#)
- [3.5.1 Release Notes](#)
- [3.5.0 Release Notes](#)

### April 2023

- [Release Notes](#)

### March 2023

- [Release Notes](#)

### December 2022

- [Release Notes](#)

### September 2022

- [Release Notes](#)

### June 2022

- [Release Notes](#)
- [Comma Separated URLs](#)

### February 2022

- [Release Notes](#)
- [Refresh](#) option and hover.



## Release Notes

- [Comment and Checkout](#) option.
- [View Logs and download](#) option.

## November 2021

- Screen shot, description updated under [Logging Into Secret Server](#) to document **Recent** and **Favorites** tabs in main WPF window.
- Screen shot, description updated under [Preferences Menu](#) to document **Secret Server Login New Window** option.

## October 2021

- [Release Notes](#)

## August 2021

- [Release Notes](#)

## July 2021

- [Release Notes](#)

## May 2021

- [Release Notes](#)

## March 2021

- [Release Notes](#)

## December 2020

- [Release Notes](#)

## October 2020

### 2.0.3 Release Updates

- [Release Notes](#)
- [Native Messaging Host](#)

## September 2020

- Added Security Scans section.