Delinea

Web Password Filler

Table of Contents

The Delinea Web Password Filler (WPF) is a Web browser extension to help users log on their sites. It allows browsers to find and enter credentials of users, when a Secret Server instance has secrets related to that website.

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

Please set up WPF in the following order:

1. Ensure you can log in to Secret Server the conventional way and that web services are enabled.
2. If necessary, 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](#).
5. [Configure WPF to point to Secret Server](#).
6. [Login to Secret Server via WPF](#).

   Note: In order for the WPF to work correctly with Secret Server, Web Services need to be enabled in Secret Server.

1. Navigate to **Admin I Configuration I Application Settings**.
2. Verify that under View Webservices the **Enable Webservices** option is reflecting **Yes**.

Installing Browser Extensions

To use the Web Password Filler, install one of the supported browser extensions as described below:

- **Chrome:** Install the extension by clicking the Web launcher icon in a Web Password secret, or by downloading it from the Google [Chrome](#) add-ons site. Also see [Managing Extensions in Your Enterprise](#) on securely managing Chrome extensions at scale.

- **Edge Chromium:** Install the extension by downloading it from the Microsoft [Edge](#) add-ons site.

- **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.

- **Safari:** Install the extension by downloading it from [How to install Safari extensions on your Mac](#). See the notes in the list below:

  - WPF supports Safari running on macOS Catalina, Mojave, 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.
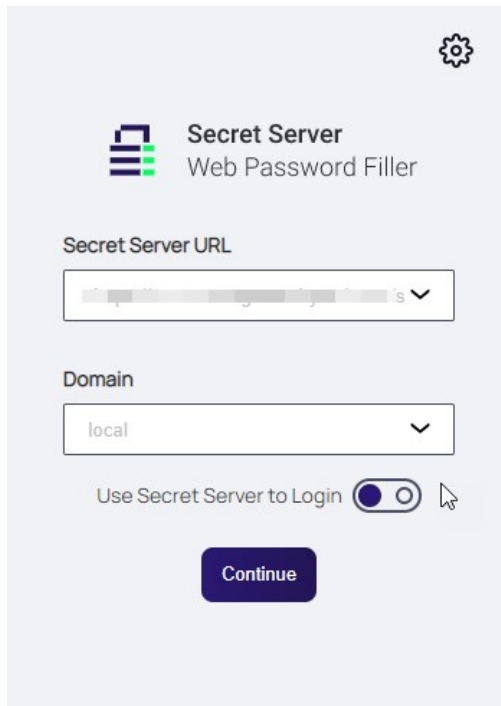
    Note: WPF versions newer than 2.0.2 do not support Opera. If you are using WPF v 2.0.2 or older and you need to use Opera, you can download the extension from the [Opera](#) add-ons site.

Connecting with Secret Server

After installation, you must configure WPF to connect with Secret Server before logging on the Website. You can use the Configuration tab on WPF to configure it with the Secret Server instance of your choice.
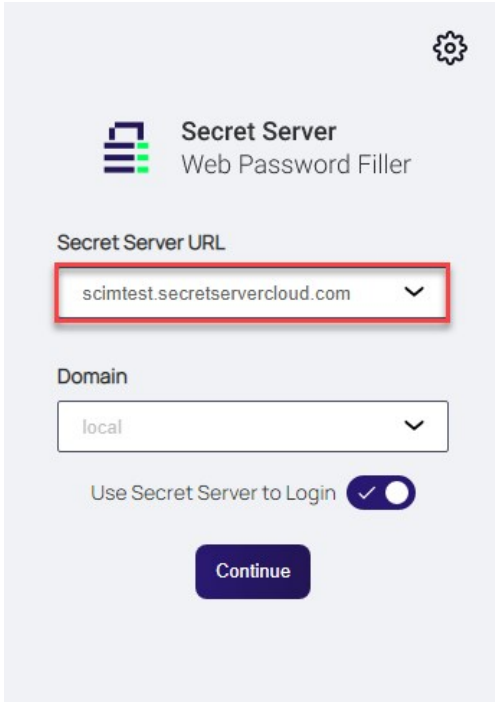
To connect WPF with Secret Server:

1. Open Google Chrome or any other supported browser.

2. In the upper-right corner of the browser, click the **Web Password Filler** icon. The WPF login window appears:

3. In the **Secret Server URL** field, type your Secret Server URL. For example: https://myserver/secretserver/

4. In the **Domain** field, type the domain of Secret Server. This only applies if you set up Secret Server to use a domain otherwise it is Local by default.

5. Click **Continue**.

6. Log in using your identity provider

If the user does not specify a protocol in the Secret Server URL, Web Password Filler will automatically redirect the Secret Server URL to *https://*

If the user clicks **Continue**, Web Password Filler assumes *https://* is the correct protocol and proceeds as if the user had prefixed *https://* in the vey beginning. Users will users will then be logged in successfully.

> **Note:** If a user enters a protocol in the Secret Server URL, Web Password Filler will honor that protocol.

When connected to Secret Server, Web Password Filler will show the Secret Server URL at the bottom of the page. A user can also redirect to Secret Server via hyperlink which they used to log into Web Password Filler
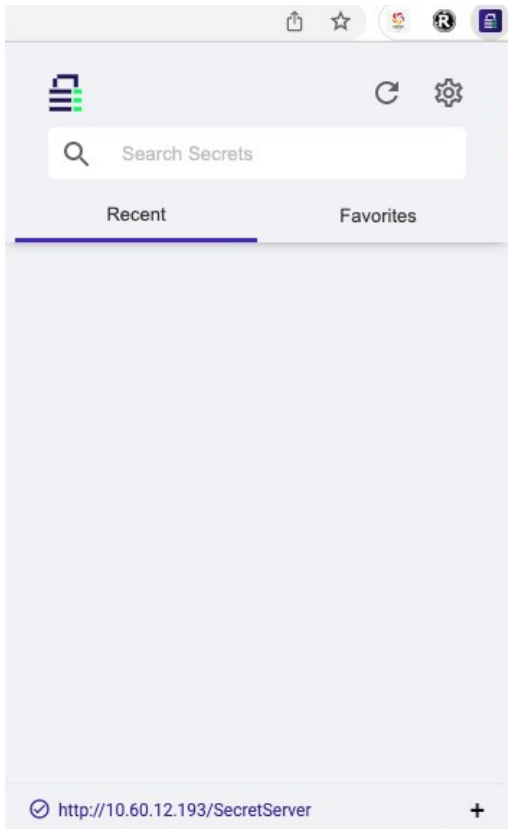
Login to Secret Server

Before you have access to any secrets that apply to your websites, you must first log in and connect WPF to Secret Server. There are two ways to do this. The first is by entering your credentials into WPF and having it verify back with Secret Server. The second is by redirecting the login (through a new browser tab) back to Secret Server and using the Secret Server Web login to make the connection.
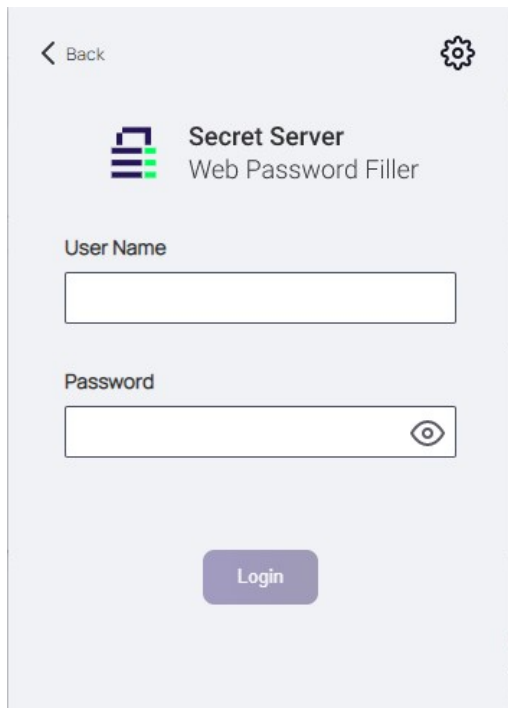
The examples below use Google Chrome and Duo. However other browsers and two-factor authentication applications are supported. Refer to information about supported extensions and Secret Server's list of two-factor applications that are supported.

Web Password Filler offers a dropdown list for selecting Secret Server URLs and domains. The Secret Server URL and domain are added to the drop down list after a successful login. Users can delete Secret Server URLs and domains from the drop down.

To use the **Password Filler** icon of WPF to log on Secret Server:

Note: Before logging in, ensure that WPF is configured with Secret Server. If you do not have the Secret Server instance in the Configuration tab, WPF prompts you to enter it and switches to that tab before trying to log on. This ensures you know what you are logging into.

1. Open, for example, **Google Chrome**.

2. In the upper-right corner of the browser, click the inactive (grayed-out) **Web Password Filler** icon. The WPF login window appears:

3. For **Username**, type the username you use to access Secret Server. This is your Secret Server user name and not your email address.

4. For **Password**, enter the password for your account.

   Note: These are the same credentials you use for logging on Secret Server.

5. Click the **Login** button. If you do not have two-factor authentication enabled in Secret Server, you are now logged in.

6. If you have two-factor authentication enabled in Secret Server (and your login was authenticated), you are sent to the **Two Factor** screen to complete the second authentication. Click **Push Duo** to authenticate with your Duo app, or click **Phone** to receive an authentication text message with a PIN code to enter in the **Pin Code** field, then click **Login**.

   You are now logged in to Secret Server, and the WPF icon changes to the active version ⬛ . If you click the active WPF icon, the main Web Password Filler window appears, with a Secret search field, one tab displaying a stack of panels with Recent secrets, and another tab displaying Favorites.
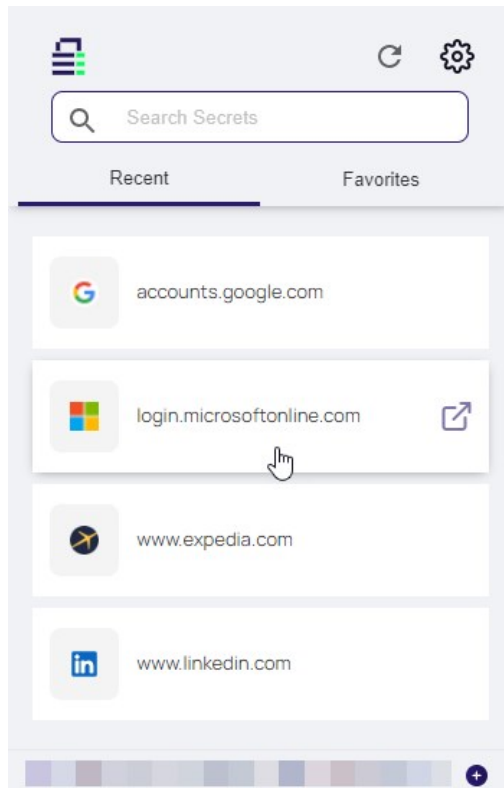
The **Login with Secret Server** button allows you to log in to WPF using a redirect through the Secret Server log in, also known as SAML or single sign on. This replaces the User Name and Password text boxes on the Login tab in WPF.

1. Open, for example, **Google Chrome**.

2. In the upper-right corner of the browser, click the **Password Filler** ▦ icon. If you already have enabled the **Use Secret Server to login** option, the Login screen will display fields for your Secret Server URL and Domain, as well as a **Login with Secret Server** toggle button.
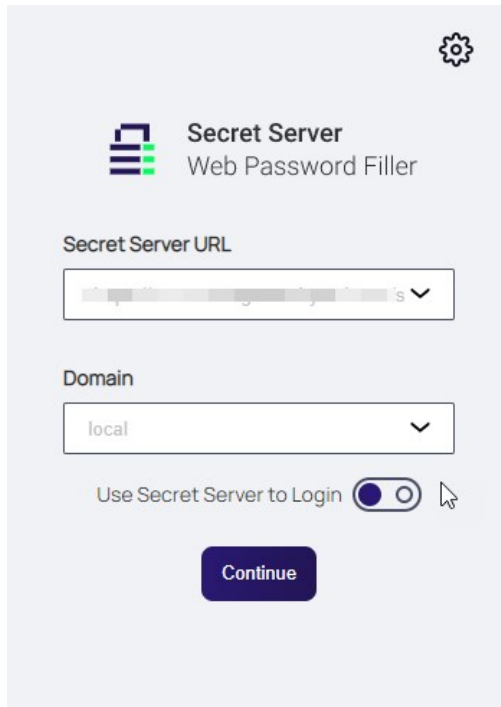
3. Click the **Login with Secret Server** toggle button. WPF opens a new tab for Secret Server in the browser, where you can log into Secret Server. After logging into Secret Server, a token is automatically generated for you. A window opens briefly showing the Generate Token button being pushed automatically, then the window quickly closes.

Preferences Menu

When you are already logged into Web Password Filler, click the WPF icon 🗐 The **Settings** screen appears.
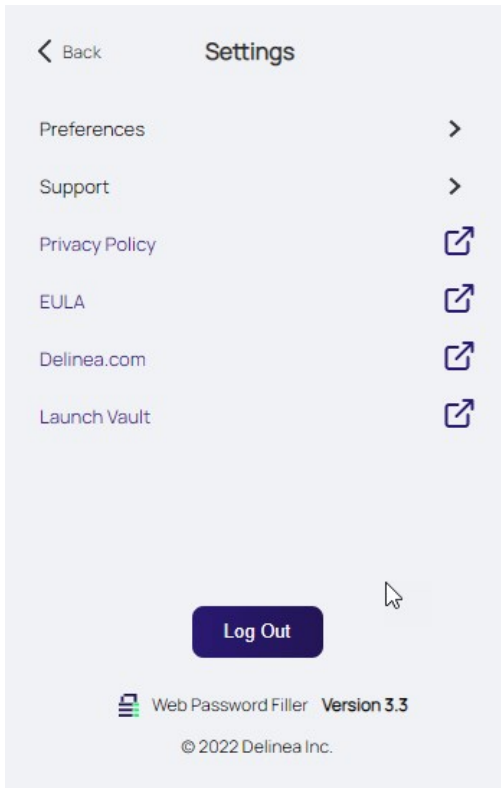
Click **Preferences**. The Preferences screen appears.
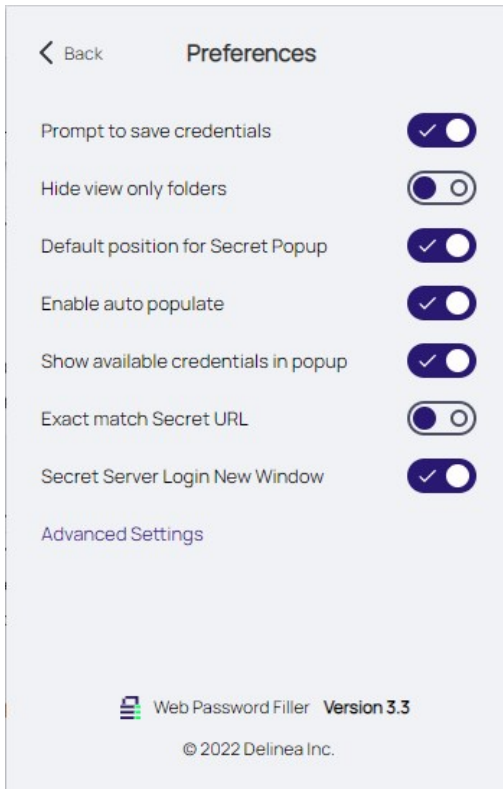
- **Prompt to save credentials**: Select this preference is you want WPF to prompt you to save your login credentials for future logins. Not recommended for shared systems. The prompt only appears if an existing secret is updated, or if a user enters credentials for a site and no Secret was used.

- **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."

- **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.

Terminology
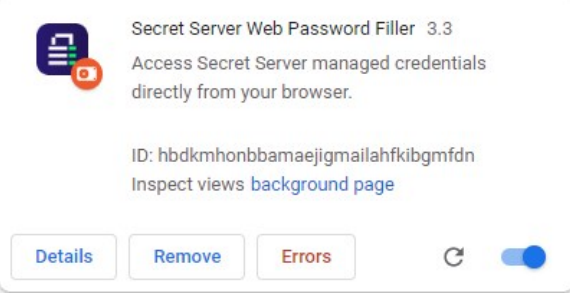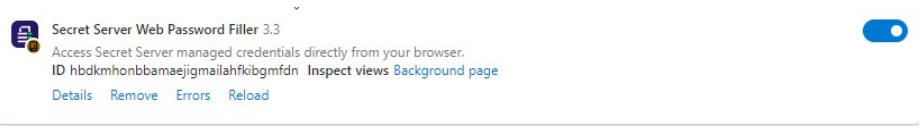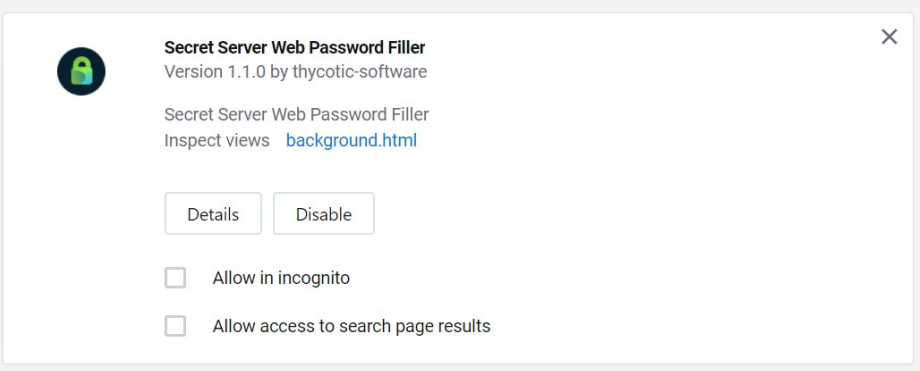
To help eliminate any potential confusion for terminology for the different browser add-ons, this section will review what terms were being used for each add-on and provide some visual points.

This is the new Web Password Filler browser extension that was release with Secret Server version 10.7.59 and later. Typically, this will be referred to as:

- WPF
- Web Password Filler
- Password Filler

When looking in a browser this is represented by the following:

Logged Out	(In top right corner)	🔒
Logged In	(In top right corner)	🗄
Application in Browser (Settings Menu)		

Item on Extensions / Add-On page	Chrome	Secret Server Web Password Filler 3.3 Access Secret Server managed credentials directly from your browser. ID: hbdkmhonbbamaejigmailahfkibgmfdn Inspect views background page Details Remove Errors
	Firefox	Secret Server Web Password Filler Secret Server Web Password Filler
	Edge (chromium version)	Secret Server Web Password Filler 3.3 Access Secret Server managed credentials directly from your browser. ID hbdkmhonbbamaejigmailahfkibgmfdn Inspect views Background page Details Remove Errors Reload
	Opera	Secret Server Web Password Filler Version 1.1.0 by thycotic-software Secret Server Web Password Filler Inspect views background.html Details Disable ☐ Allow in incognito ☐ Allow access to search page results

This is the previous version of the Web Password Filler/Login assist extension. It is typically referred to as:

- WPF (Term No longer used in relation to this extension)
- Web Password Filler (Term No longer used in relation to this extension)
- Login Assist (Still used)

When looking in a browser this is represented by the following:

Logo in top right corner	

Application in Browser	**Secret Server Login Assist** HAVE A SECRET FOR THIS URL? All matching Secrets will be listed below the password field.
Drop down option on field	No Secrets found. Add Secret
Item on Extensions / Add-On page	Secret Server Web Password Filler 3.3 Access Secret Server managed credentials directly from your browser. ID: hbdkmhonbbamaejigmailahfkibgmfdn Inspect views background page Details Remove Errors

This is the Clipboard Utility that was available with previous versions of Secret Server. The options and functionality of this extension have NOT be added into the NEW Web Password Filler (as of Feb 28, 2020).

It is typically referred to as:

- Clipboard Utility (Still used)
- Clipboard tool (Still used)

When looking in a browser this is represented by the following:

Logo in top right corner	
or	
Application in Browser	Secret Server Clipboard Utility Can't read or change site's data Options Remove from Chrome... Hide in Chrome menu Manage extensions
Item on Extensions / Add-On page	Secret Server Web Password Filler 3.3 Access Secret Server managed credentials directly from your browser. ID: hbdkmhonbbamaejigmailahfkibgmfdn Inspect views background page Details Remove Errors
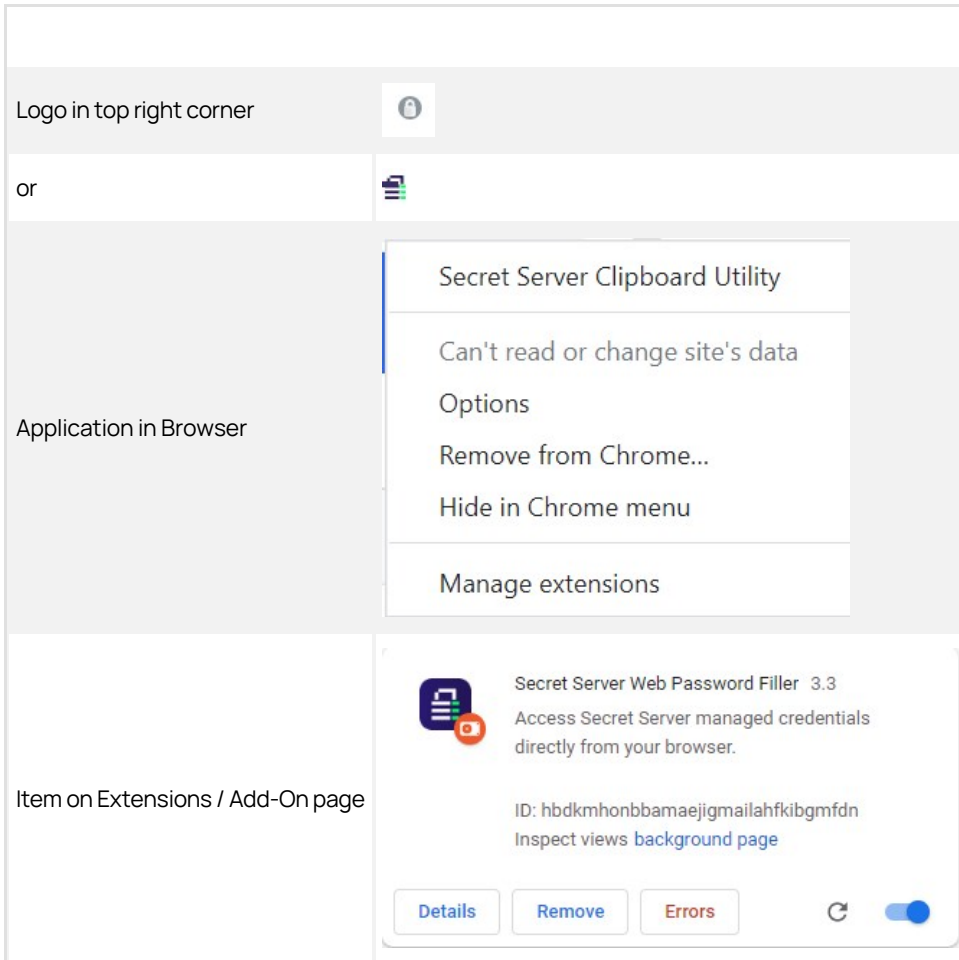
Native Messaging Host

The Delinea Native Messaging Host makes it easier to manage settings for the Delinea Web Password Filler (WPF). 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, the 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.

Native Messaging Host consists of one executable file and one configuration file installed on the user's computer. Each time the user's browser is launched, the Native Messaging Host silently sends default configurations and settings to the Web Password Filler.

Users 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/auto populate credentials or other information.

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

Download Location

Download the Native Messaging Host installer [here](#).

Requirements
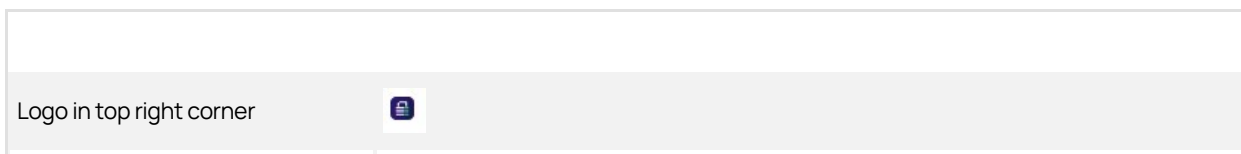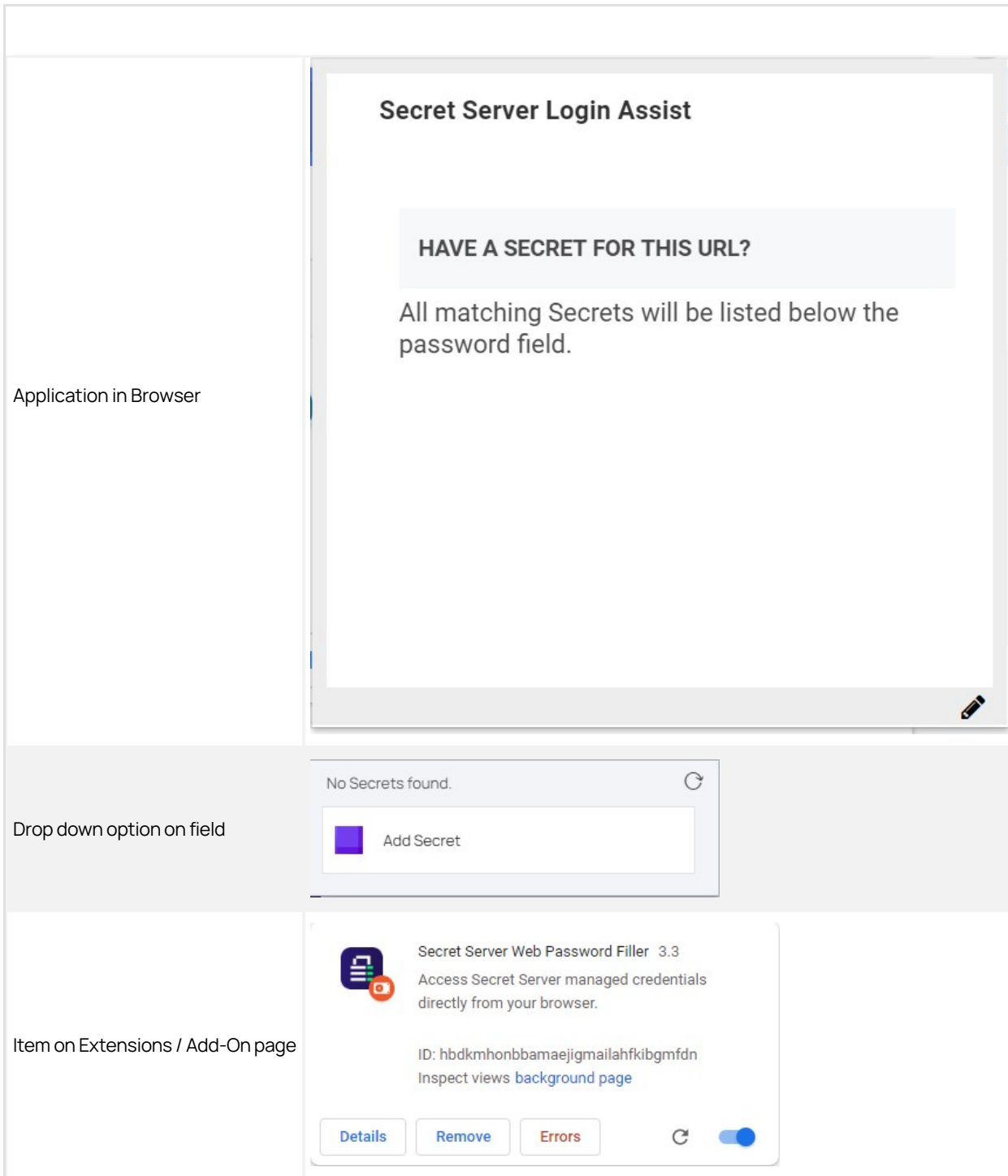
- .NET version 4.5.2 or later
- Delinea Web Password Filler version 2.0.3 and later

Supported Browsers

- Chrome
- Edge Chromium
- FireFox
- Opera

Additional information regarding Native Messaging can be found at

- https://developer.chrome.com/extensions/nativeMessaging
- https://developer.mozilla.org/en-US/docs/Mozilla/Add-ons/WebExtensions/Native_messaging

Installation

The user installs the Delinea Native Messaging Host on their computer by copying the ThycoticMessagingHost.exe and *settings.json* files into an accessible directory such as C:\Thycotic\Web Password Filler\.

Registration

The user 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 the Web Password Filler until this registration is completed.

Once the user has successfully registered the Native Messaging Host, the configuration file will be checked for updates automatically each time the user launches their browser. The user does not have to unregister and re-register each time they make a change to the configuration file.

Note If the user manually adds the WPF extension to the browser instead of getting it from the browser store, the extension ID changes. In that case, the user **MUST** update the *settings.json* to reflect the new extension ID. Whenever the user changes the extension ID, they 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 the user launches their 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, 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 registering using the EnableForAllUsers = true option, the user must run the registration as an administrator.

Uninstalling the Delinea 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 the Web Password Filler.

Native Messaging Host facilitates the management of Web Password Filler settings through modification of a *settings.json* file. Each time the user's browser is launched, the Native Messaging Host reads the default configurations and settings in the json file and silently sends them to the Web Password Filler. The 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 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.

```
                  {
Browser   |"chromeExtensionId": "mfpddejbpnbjkjoaicfedaljnfeollkh",
   IDs     |"edgeExtensionId": "kjldmpkefedgljefehmmfifbhnjngmbh",
          |"operaExtensionId": "eemnnadjdifcpkcnpalolohpepihhbbo",
          |"firefoxExtensionId": "dd1e31d5-3623-45cb-b1ad-64074d36b360@thycotic.com",
Default   |"ConfigSSUrl": "https://SomeURL/SecretServer",
Settings  |"ConfigDomain": "",
          |"HideConfigPage": false,
          |"HideSettingPage": false,
          |"SettingUserSSLogin": true,
          |"SettingPrompToSave": true,
          |"SettingShowPopup": true,
          |"SettingHideReadOnlyFolders": true,
          |"SettingEnableAutoPopulate": true,
          |"EnableForAllUsers": false,
          |"PopupDefaultPosition": true,
          |"ExactMatchUrl": false,
          |"maxSessionRecordingLimit": 120,
          |"Exclude": [ "http://*" ],
          |"ExcludeException": [],
          |"PerExtensionOverride": [
              {
Default       |"id": "mfpddejbpnbjkjoaicfedaljnfeollkh",
Overrides     |"ConfigSSUrl": "https://SomeURL/SecretServer",
per Browser   |"ConfigDomain": "",
              |"HideConfigPage": true,
              |"HideSettingPage": false,
              |"SettingUserSSLogin": true,
              |"SettingPrompToSave": 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"
               ]
              },
```

Settings.json Format

Belowis 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": "mfpddejbpnbjkjoaicfedaljnfeollkh",
  "edgeExtensionId": "kjldmpkefedgljefehmmfifbhnjngmbh",
  "operaExtensionId": "eemnnadjdifcpkcnpalolohpepihhbbo",
  "firefoxExtensionId": "dd1e31d5-3623-45cb-b1ad-64074d36b360@thycotic.com",
  "ConfigSSUrl": "https://SomeURL/SecretServer",
  "ConfigDomain": "local",
  "HideConfigPage": false,
  "HideSettingPage": false,
  "SettingUserSSLogin": true,
  "SettingPrompToSave": true,
  "SettingShowPopup": true,
  "SettingHideReadOnlyFolders": true,
  "SettingEnableAutoPopulate": true,
  "EnableForAllUsers": false,
  "PopupDefaultPosition": true,
  "ExactMatchUrl": false,
```

```
    "maxSessionRecordingLimit": 120,
    "Exclude": [ "http://*" ],
    "ExcludeException": [],
    "PerExtensionOverride": [
      {
        "id": "mfpddejbpnbjkjoaicfedaljnfeollkh",
        "ConfigSSUrl": "https://SomeURL/SecretServer",
        "ConfigDomain": "",
        "HideConfigPage": true,
        "HideSettingPage": false,
        "SettingUserSSLogin": true,
        "SettingPrompToSave": 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,
        "SettingPrompToSave": false,
        "SettingShowPopup": false,
        "SettingHideReadOnlyFolders": false,
        "SettingEnableAutoPopulate": false,
        "PopupDefaultPosition": false,
        "ExactMatchUrl": false,
        "maxSessionRecordingLimit": 120,
        "Exclude": [ "http://*" ],
        "ExcludeException": []
      },
      {
        "id": "dd1e31d5-3623-45cb-b1ad-64074d36b360@thycotic.com",
        "HideConfigPage": false
      },
      {
        "id": "eemnnadjdifcpkcnpalolohpepihhbbo"
      }
    ]
}
```

Where:

chromeExtensionID	"mfpddejbpnbjkjoaicfedaljnfeollkh"	This is the ID required for the Chrome browser registration.
edgeExtensionId	"kjldmpkefedgljefehmmfifbhnjngmbh"	This is the ID required for the Edge browser registration.
operaExtensionId	"eemnnadjdifcpkcnpalolohpepihhbbo"	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.
HideConfigPage	false	Boolean that controls if the Configuration tab is visible or not.
HideSettingPage	false	Boolean that controls if the Settings tab is visible or not.
SettingUserSSLogin	true	Boolean that sets the checkbox to enable the Secret Server Login option.
SettingPrompToSave	true	Boolean that sets the checkbox to enable the Prompt to Save option.
SettingShowPopUp	true	Boolean that enables login credentials to pop up automatically. If false you just need to click the Delinea checkmark.
SettingHideReadOnlyFolders	true	Boolean that sets the checkbox to enable the Hide Read Only Folder option.
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 Site Exclusions and Exceptions below. Accepts wildcards.
ExcludeException	[list]	Refer to Site Exclusions and Exceptions below. Does NOT accept wildcards.
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.

Site Exclusions and 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 the Delinea Web Password Filler. The Delinea Native Messaging Host allows you to add exclusions as well as exclusion exceptions so those sites you do not want the Delinea Web Password Filler to interact with will be ignored. Add exceptions for any site you wish the Delinea Web Password Filler to ignore. For example, to login to an application you want the Delinea Web Password Filler to retrieve a secret for the login page, however you would like the Web Password filler 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://* and/or http://*) and then simply add the sites where secrets are available (https://MyCompanySite.com/login.aspx) to the exclusion exception list.
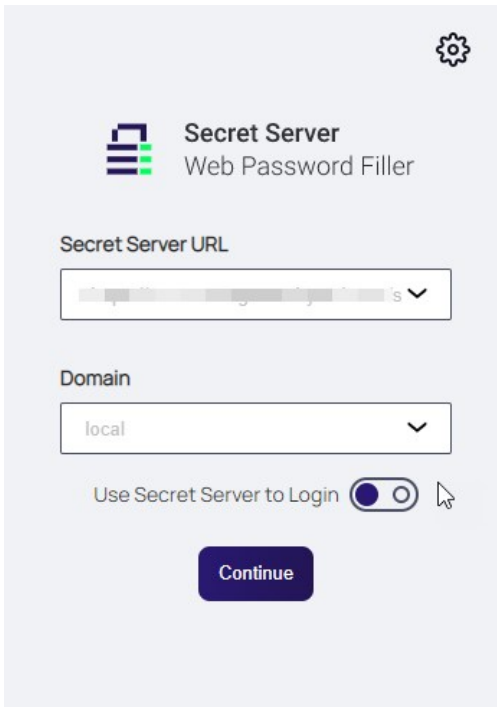
> **Note**: Only the "Exclude" section accepts a wild card. The "ExcludeException" must be the exact URL without a query string.

UI Behavior Based on Preferences

Each preference on the Preferences page can be set using "true" or "false" in the *settings.json*.
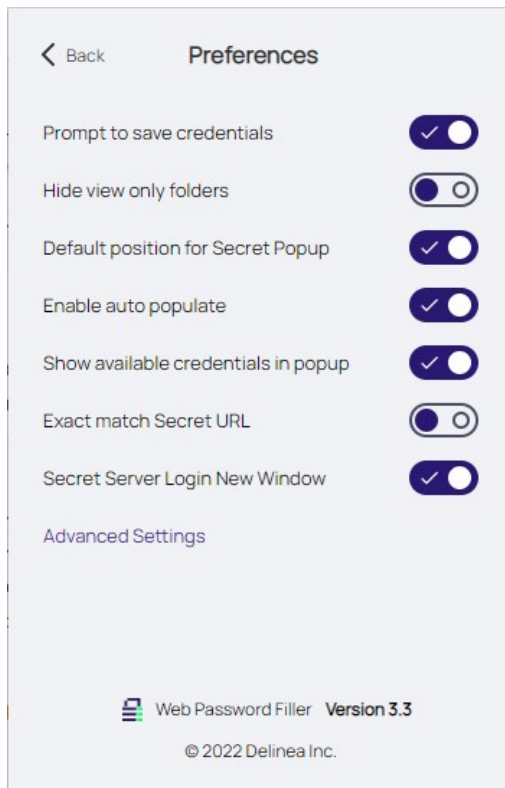
The Secret Server URL and Domain can be set by including strings (text wrapped up in quotations).

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

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 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 update or create the hkey 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 he 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 --unregister
  Press 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.
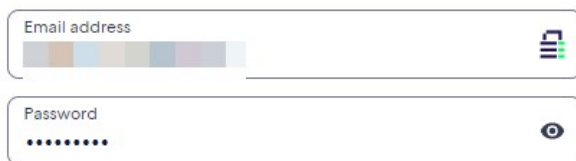
Using WPF

Once WPF is set up and you are logged into Secret Server, you can use WPF to log in to websites for which Secrets are managed via Secret Server.

Refer to Creating a Secret for a Website if you need to add new accounts.

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

Email address

Password

● ● ● ● ● ● ● ●

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

3. Click the Delinea logo. A WPF popup opens and one of two things can happen:

   - If you have one or multiple existing secrets for a site, a popup will open displaying all of the available secrets available for the site. For instance:

     Sign in as

     twitter.com
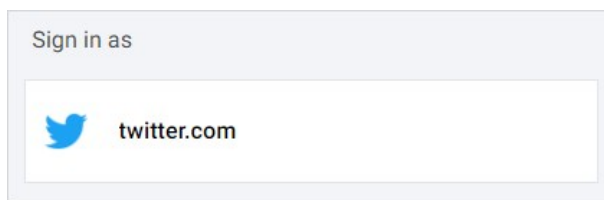
   - If you have no secrets related to the site, then a popup will open to give you the option to add a new secret:

     No Secrets found.
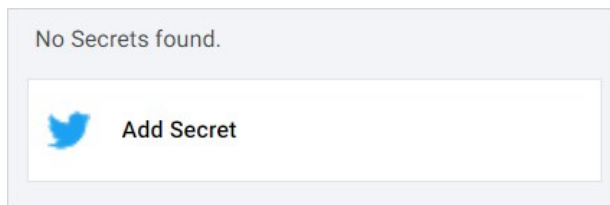
     Add Secret

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

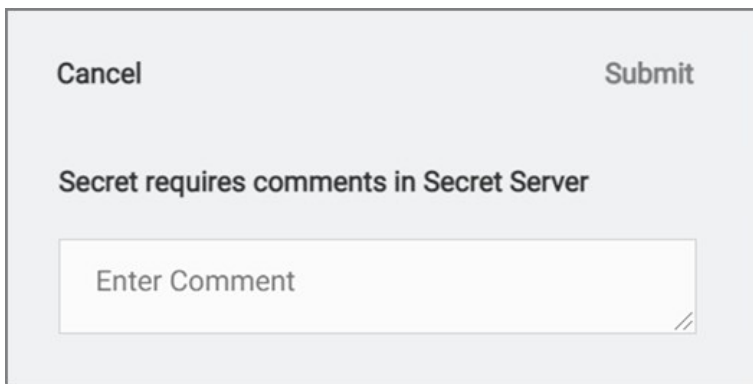4. Click the button for the desired secret, and you are signed in.

   Note: Web Password Filler functionalities are disabled on [tenant].delinea.app domains

Comment Required Option

When a Secret in Secret Server requires that a comment for checkout, the user can supply that comment via the **Enter Comment** modal. Once the comment is entered and submitted WPF will populate the fields and access is given.

There are two levels of support for access to Secrets:

- If the user only needs to provide a comment, the modal shows the comment field and **Submit**.
- If the Secret requires checkout, the modal shows the comment filed and **Checkout**.

Cancel	Submit

Secret requires comments in Secret Server

Enter Comment

Note: This feature is only supported with Secret Server versions above 11.1.000004. If used on version 11.1.000004 or earlier, the following message will be displayed.

Secret requires check out in Secret Server. Version 10.9.000035 of Secret Server does not support adding a comment remotely.

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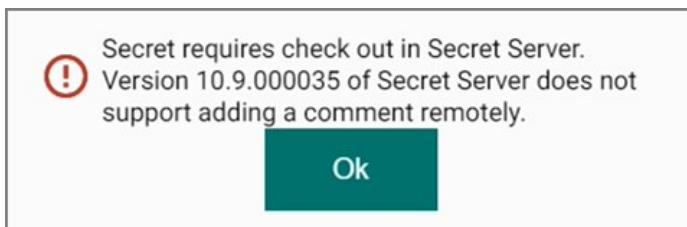
To add a comment to any secret, Web Password Filler requires the actual Secret Server version number. However, when the "Hide Secret Server Version Number" setting is enabled, the API calls will not return information about the Secret Server version.

In this case, users will see a popup that they are not able to add a comment remotely because "Hide Secret Server Version Number" is enabled:

👁 User is not able to add comment remotely because 'Hide Secret Server Version Number' is enabled

Delinea

Creating a Secret for a Website

1. Navigate to the page to create a new account on a website.

2. Click the Delinea icon in the password text box. A modal appears:
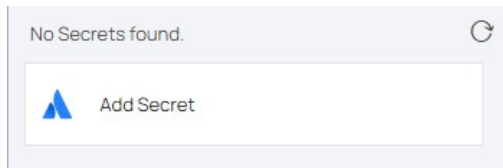
You can also right-click in the username or password field and select **Secret Server Web Password Filler | Add Secret**.
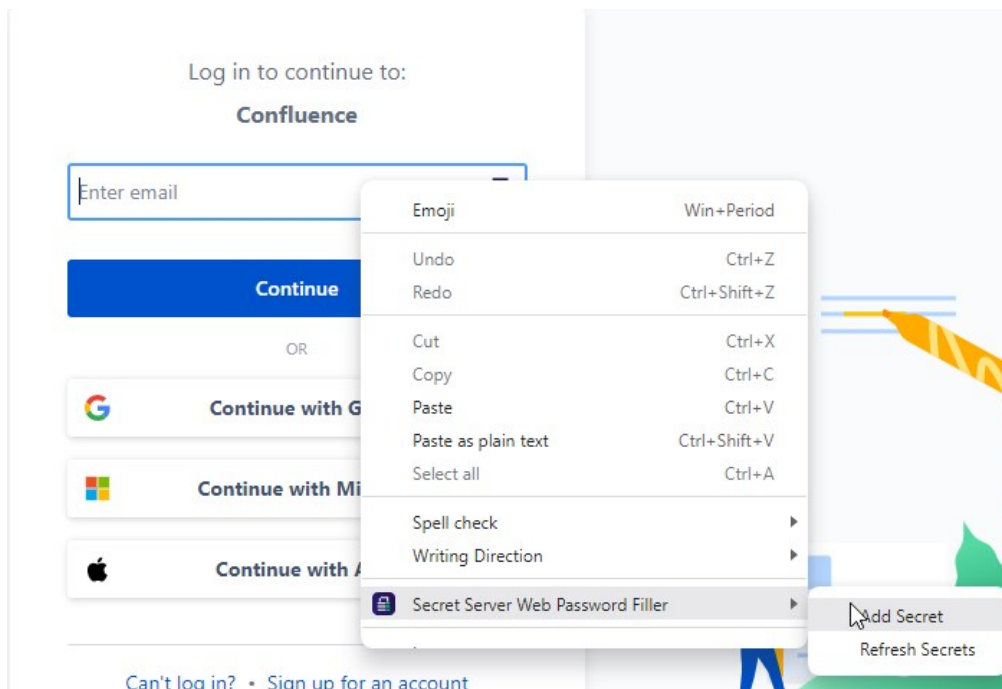
A **Template** can be selected for the newly added Secret. And navigation buttons for **Next** and **Cancel** are available.
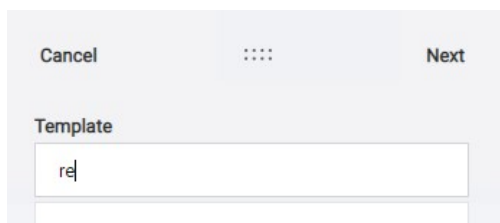
3. The **Add Account to Secret Server** modal appears with seven fields:

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 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 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 modal by typing a folder name and selecting from the list.

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.

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

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

1. 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.
2. Type your username for the website for **User Name**.
3. If this is a new account, click **Generate** to create a strong password for the site. Otherwise, use the existing password for the website.
4. Click **Save**. WPF closes The Add Account Secret Server modal 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.

   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.

The Search option allows users to type and search a list of folder/secrets.
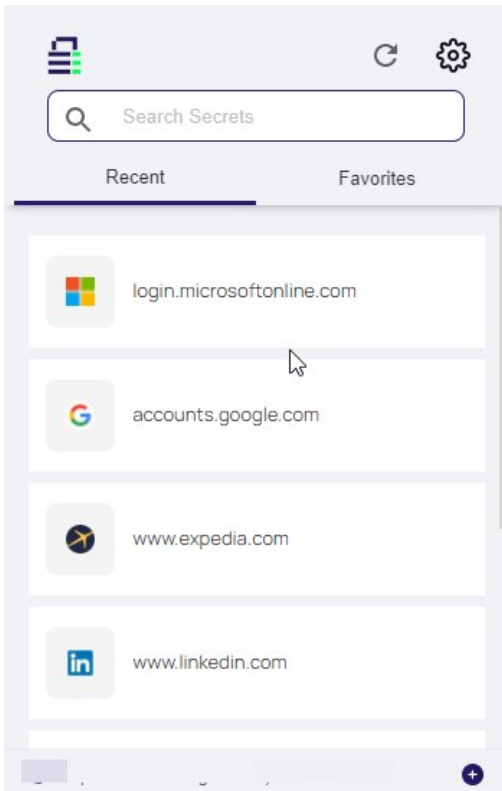
Users are also able to search for secrets in the *Recent* tab and view matches via a combination of Secret Server URL and secret name, even if the user never accessed those secrets before.
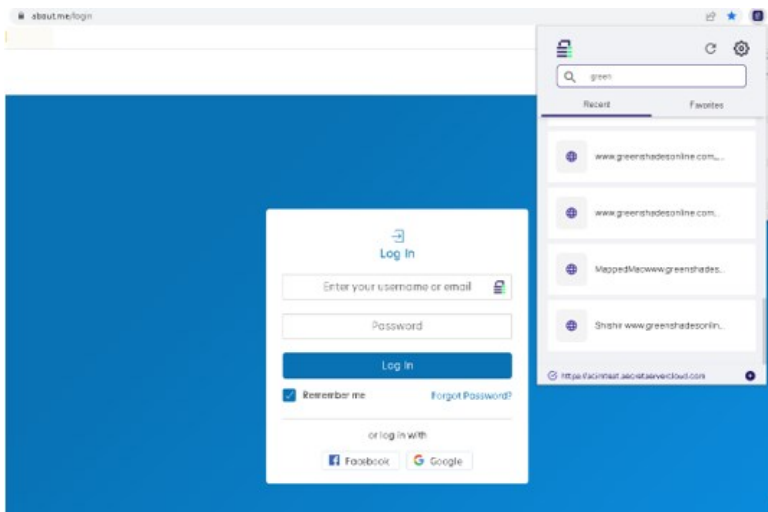
Users can also search the *Favorites* tab for secrets, just like in Secret Server:
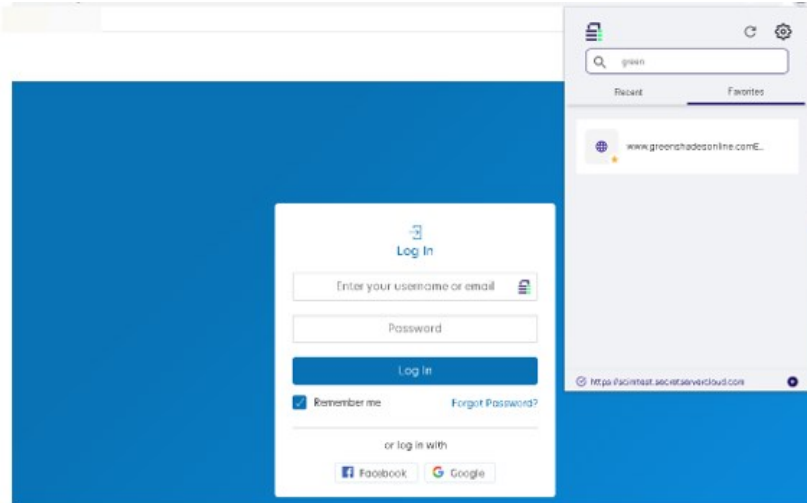
Note: If a user has more than 100 secrets in their *Favorites* or *Recent* tabs or in the search functionality, Web Password Filler enables infinite scrolling. When a user scrolls through the first 100 secrets, the next 100 will appear automatically.

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**.
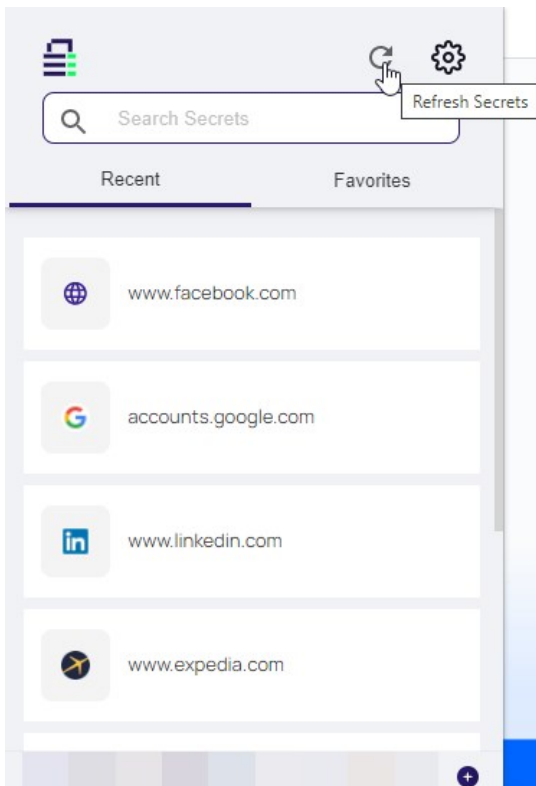
After refreshing the refresh button is deactivated for 30 seconds.
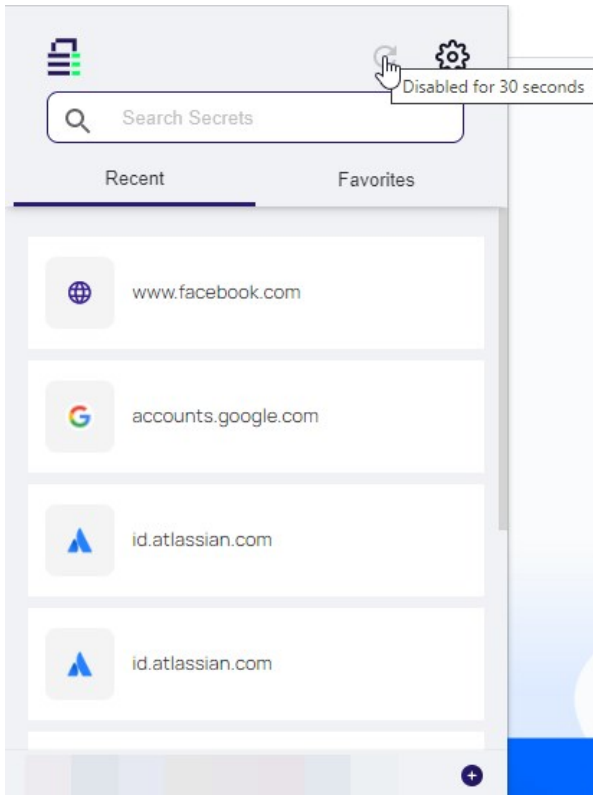
Secrets listed under the Recent tab are secrets recently accessed from the local browser extension. Secrets under Favorites are pulled from the Secret Server favorites list for the user account.

Mapping Login Fields

Some websites use unconventional labels to internally identify their username, password, and other login fields, 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 drag-and-drop functionality.

1. While creating a new Secret for a website, hover your cursor over the field you want to map in the Secret. The field is highlighted in a gray oval, with instructions to drag the field to the corresponding field on the web page.

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

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 template field that can be mapped, accompanied by a string value with the XPath to the field that should be populated.

In the example below, the Metadata tab is open and the WPFHints section is displayed. The names of the template fields that can be mapped are **accno**, **Password**, and **Username**, with the corresponding XPath string values of //*[@id="account"], //*[@id="password"], and //*[@id="username"].

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

The steps listed below will guide users on how 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.
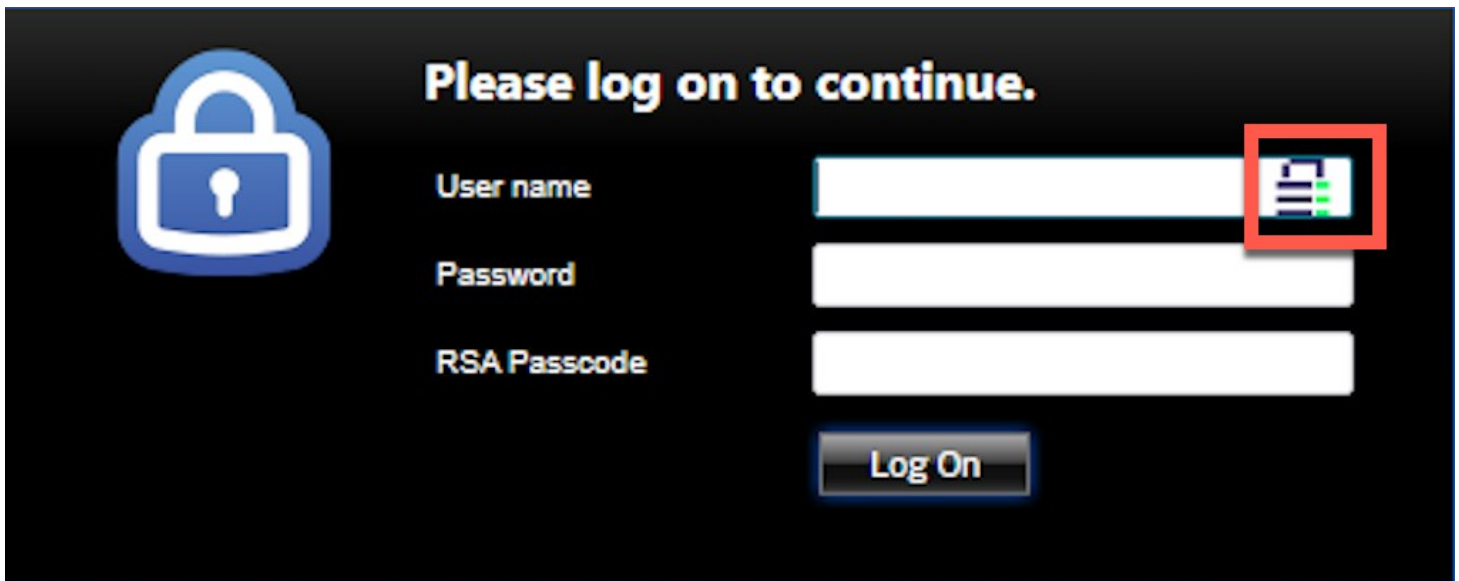
2. When adding a secret, select a customized template that has more fields than the standard web password template. In this case, there is one additional field.
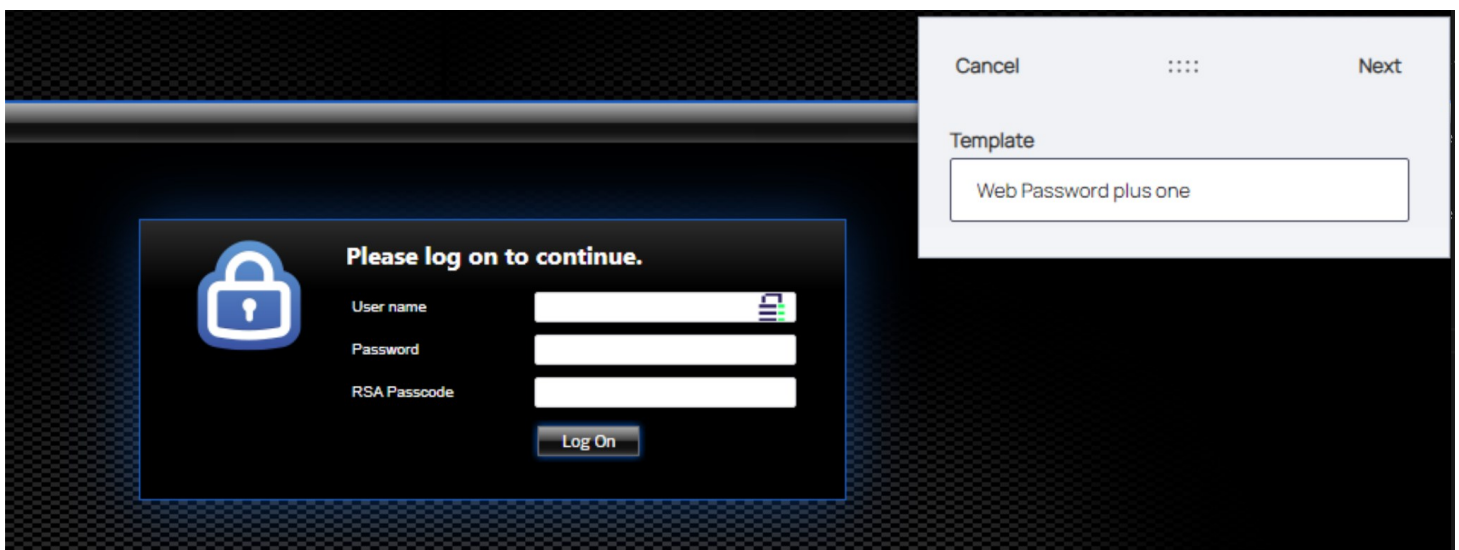
3. Drag the template User ID field to the web login Username
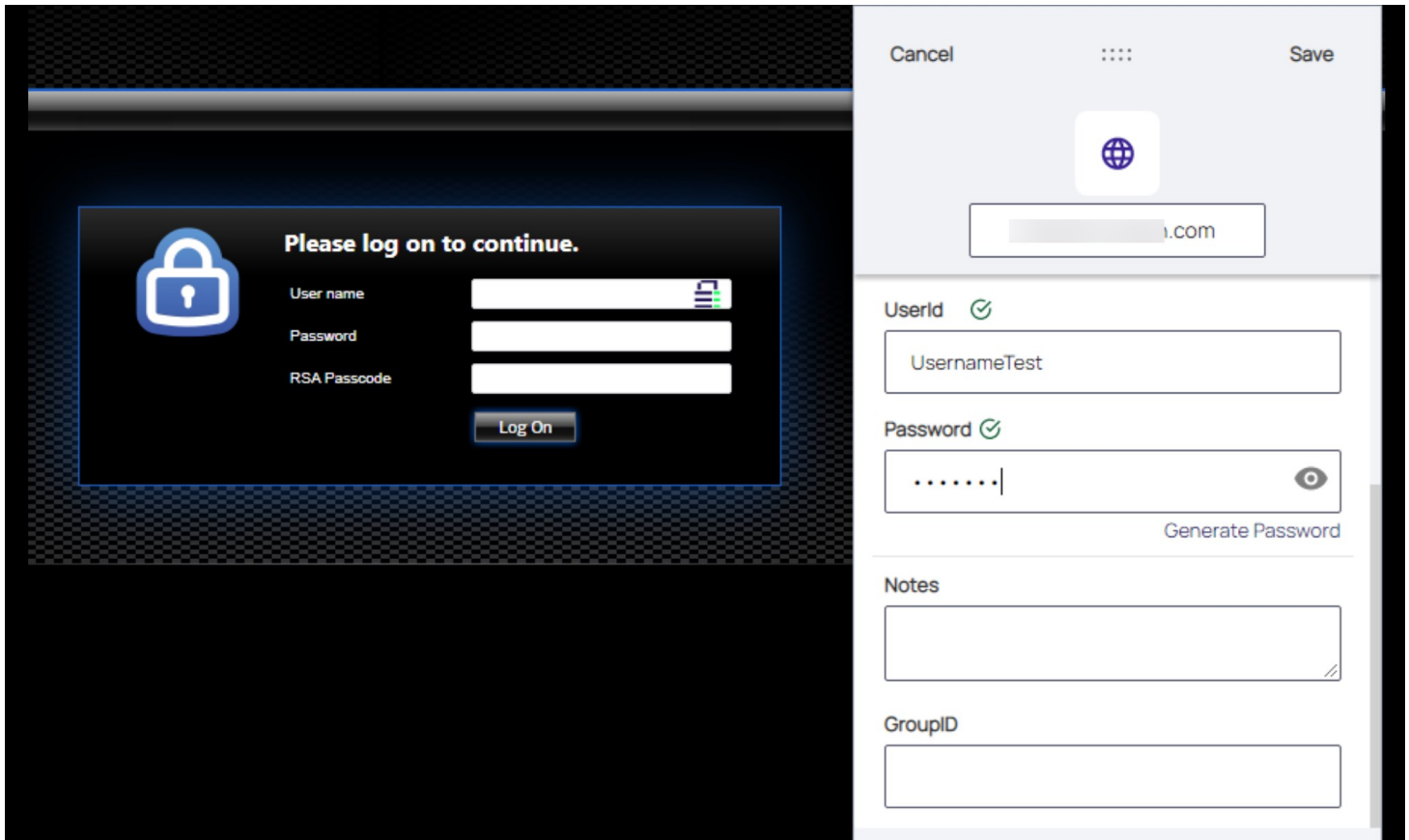
4. Drag the template password field to the web login's Password field
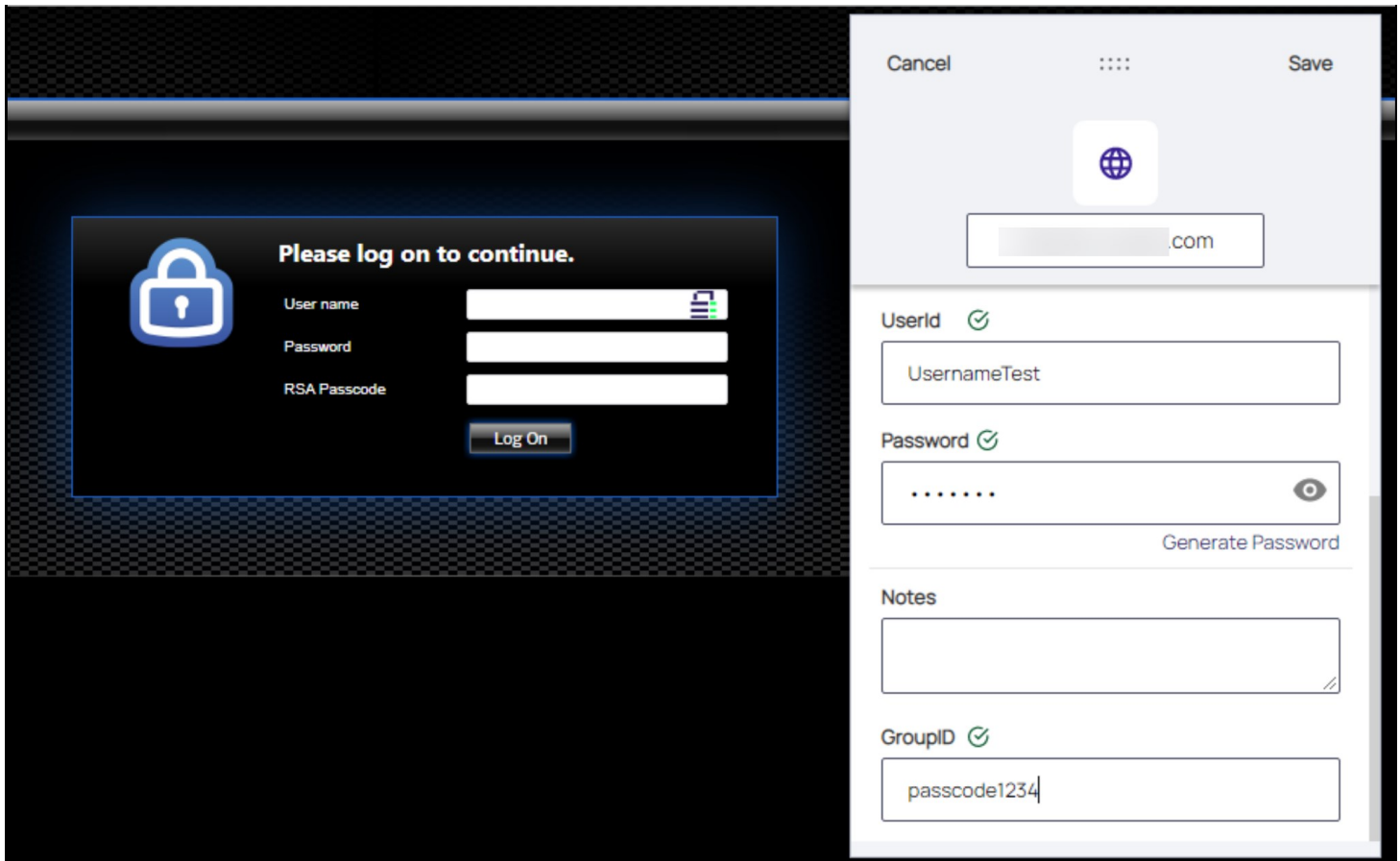
5. Drag the third field template to the web login's third field
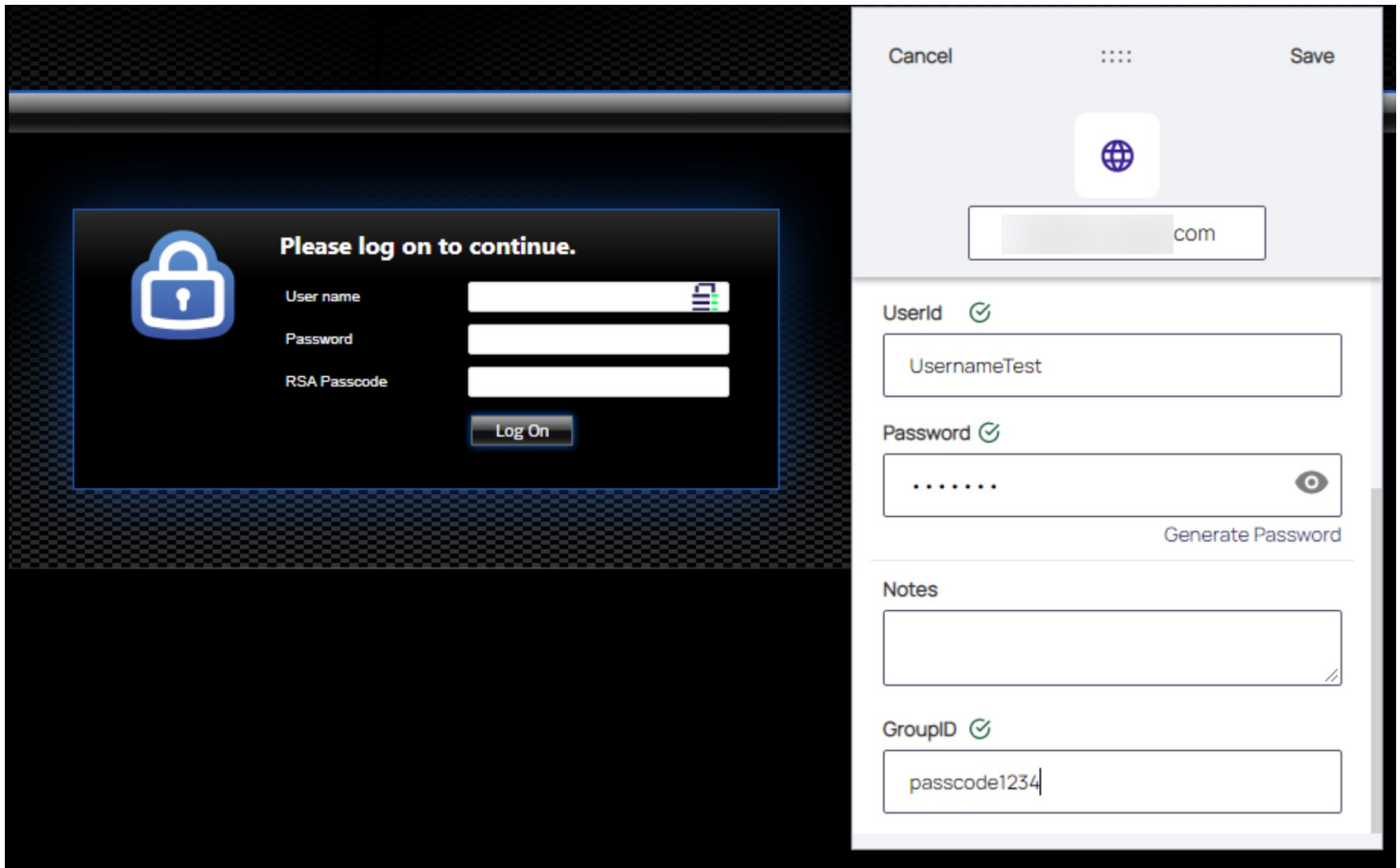
6. Click **Save**

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

Session Recording for web sessions is supported in the Web Password Filler. For a web session to be recorded, the Secret (in Secret Server) must have Session Recording enabled in the Security settings.

When you launch a Secret that has Session Recording enabled, or when you navigate to a web page and select a Secret that has Session Recording enabled, 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. On sites that allow it, the logo on the tab will alternate between the site logo and the recording icon.

When recording web sessions, the recording will be limited to the exact match for the domain/subdomain for the URL, which is everything between http(s):// and the next /. Anything *not* included in the exact URL will not be recorded. For example, if a Secret with session recording has the URL value set to https://delinea.company.com/ then only the browser tabs opened for that URL will be recorded. If the login page then redirects to https://company.com then the session will no longer be recorded since the subdomain has changed.

Likewise, you might be recording a session in a tab opened to https://delinea.company.com and 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 both secrets are being used, when the second session is selected, WPF will close the first session and tabs associated with the first Secret.

This is expected behavior, implemented to ensure that the only sessions recorded are those associated with Secrets that require session recording. Sites like microsoftonline allow only one login / active credential at a time. If you have session recording enabled for two secrets that do not contain a primary / secondary domain (such as .net, .com, .co) address, both sessions will be recorded independently. For instance red.local.something is not the same as blue.local.something because "something" is neither a primary domain nor 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**: Chrome versions 92 and newer throttle the number of screenshots per second and could impact the recording, including jumpy video or missed keystroke captures.

Session Recording Limits

The default maximum recording time for each session (start to end) regardless of how many tabs are open, is two hours. If a user starts session recording on red.delinea.com, and then opens a tab for blue.delinea.com, session recording will continue on blue.delinea.com when it is in focus. By default, session recording will stop after two hours, and both tabs will close. This session recording limit can be extended 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.

RegEx

RegEx is a sequence of patterns specified in Secret Server templates and provided to be specified as **OtherUrls** during account setup in Web Password Filler (WPF), allowing session recording on redirected websites.

When a user is logged into a website using a secret and session recording is enabled, WPF will record a session for that URL. If a user is redirected to another URL and session recording should continue for the redirected URL, those URLs can be added in the **OtherUrls** field when the account is added. Currently this field supports only URLs.
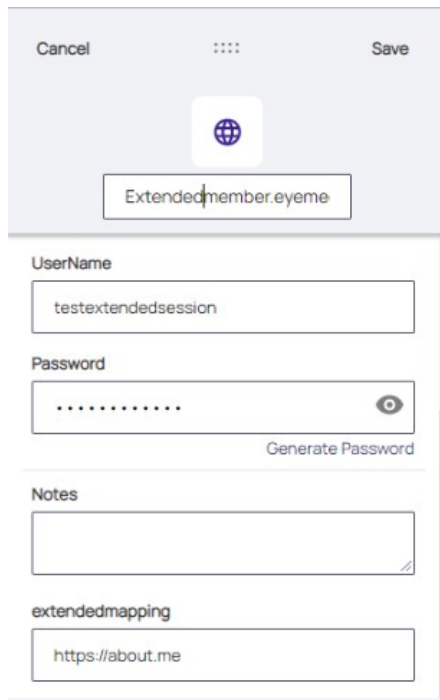
> **Note**: That as soon as a URL is accessed for a website and secret with session recording enabled, session recording will capture everything the user does, even if the user changes a password for that secret.

Using RegEx in WPF

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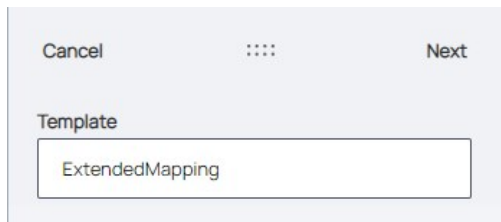
2. Click **OK**.

3. In the new Add Account to Secret Server dialog add the required details.
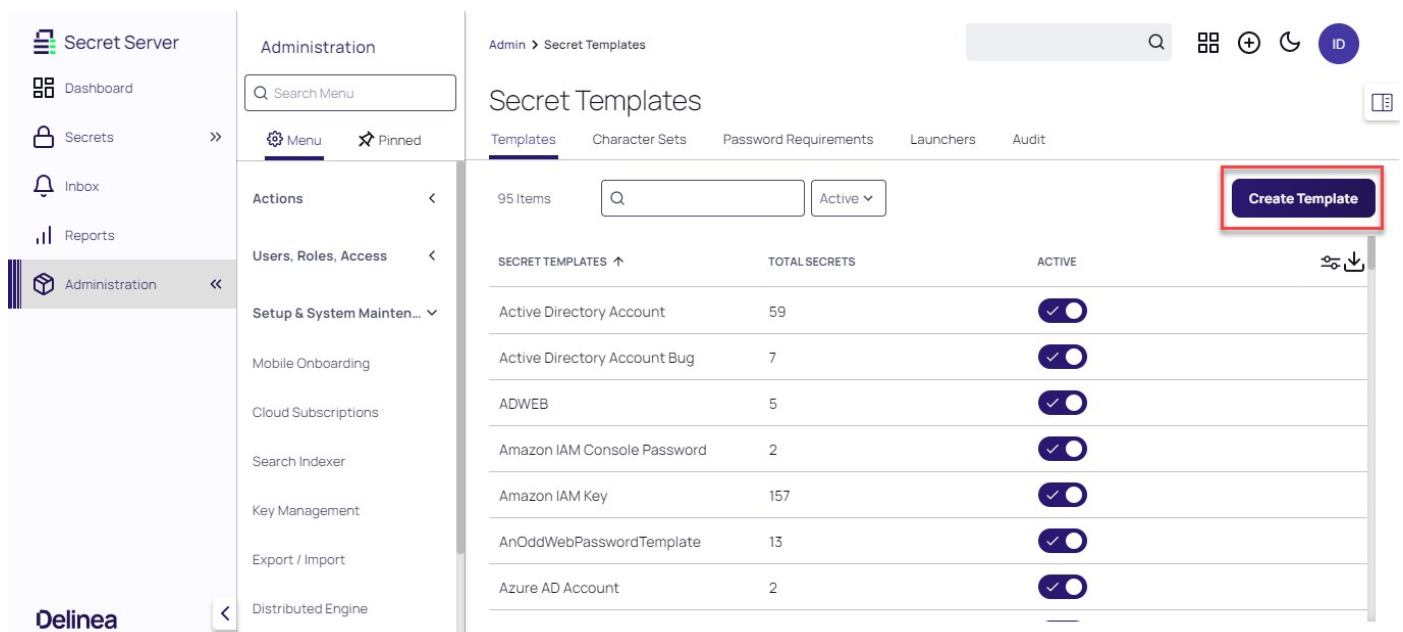
In the field **Extended Mapping**, enter any other URL for which session recording should enabled, in the event that the user is redirected to those URLs.

4. Click **Save**.

Setup in Secret Server

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

2. Click **Create Template**.

3. Name the new template and click **Save**.

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

5. In the **Mappings** page click **Add Mapping**.
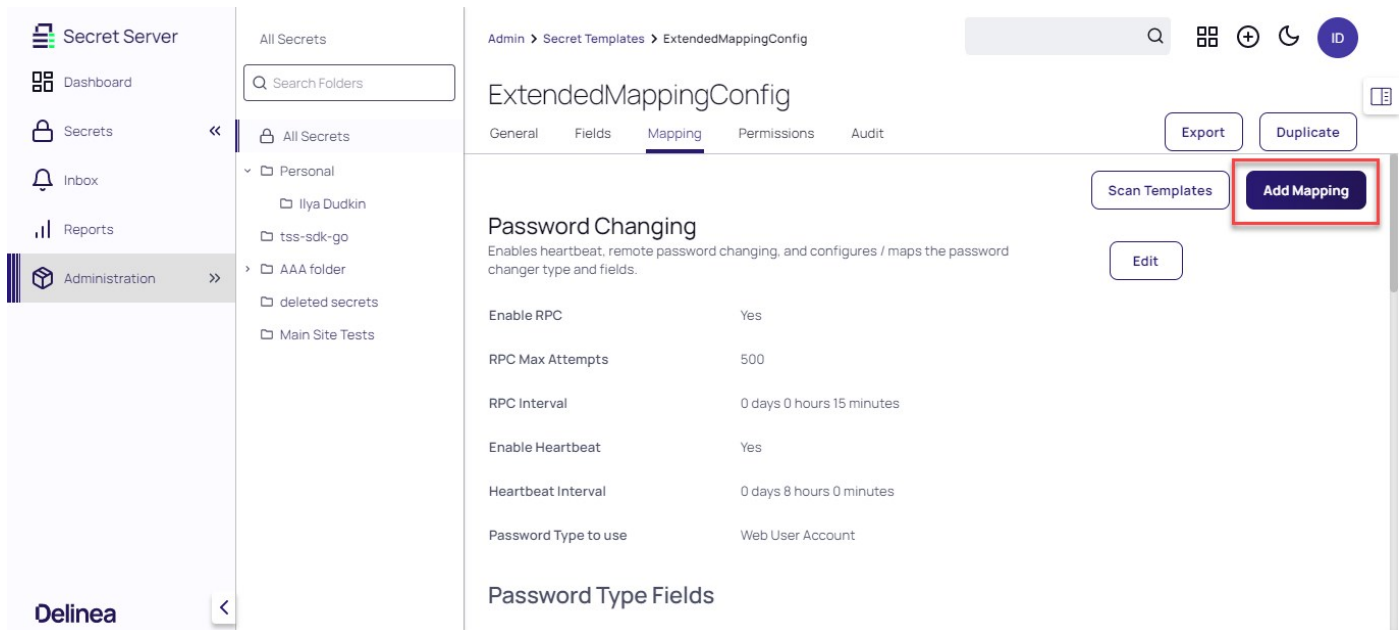
6. From the **Mapping Type** drop-down select **Regex List**
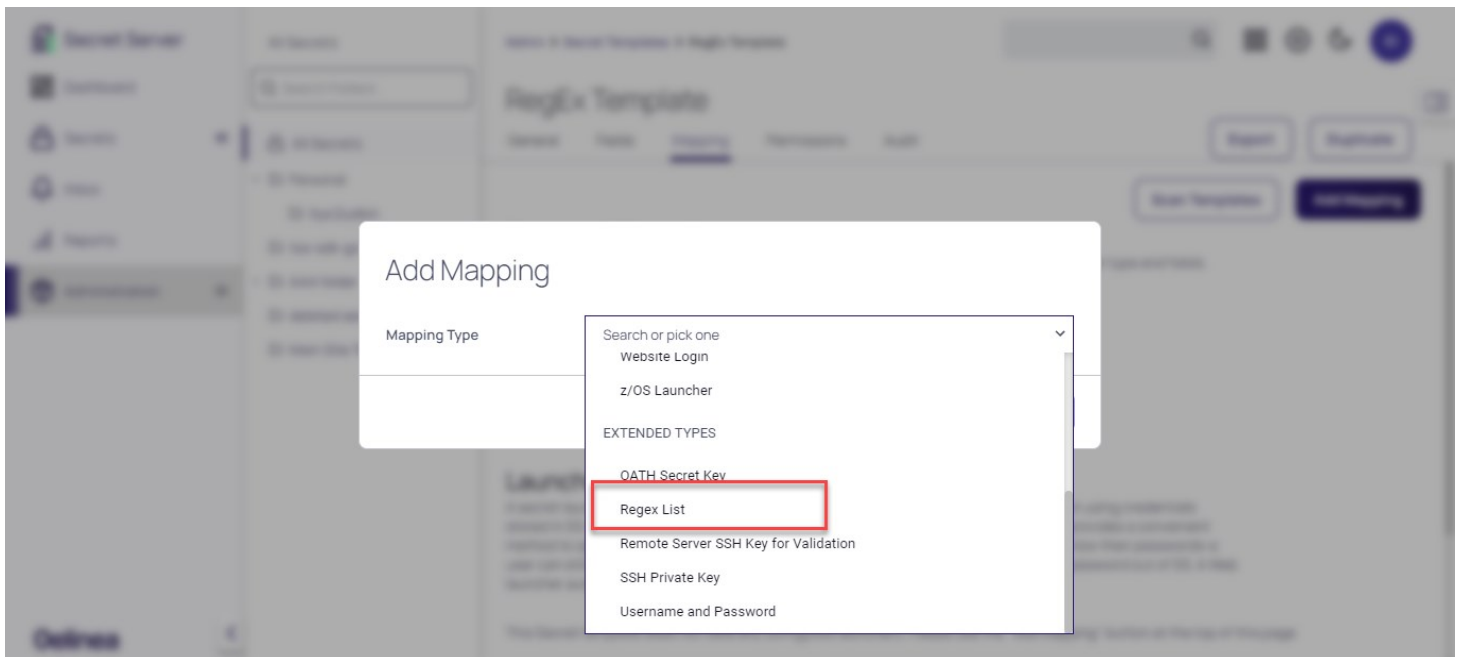
7. From the **Regex List Field** drop-down select the fields you would like to map.
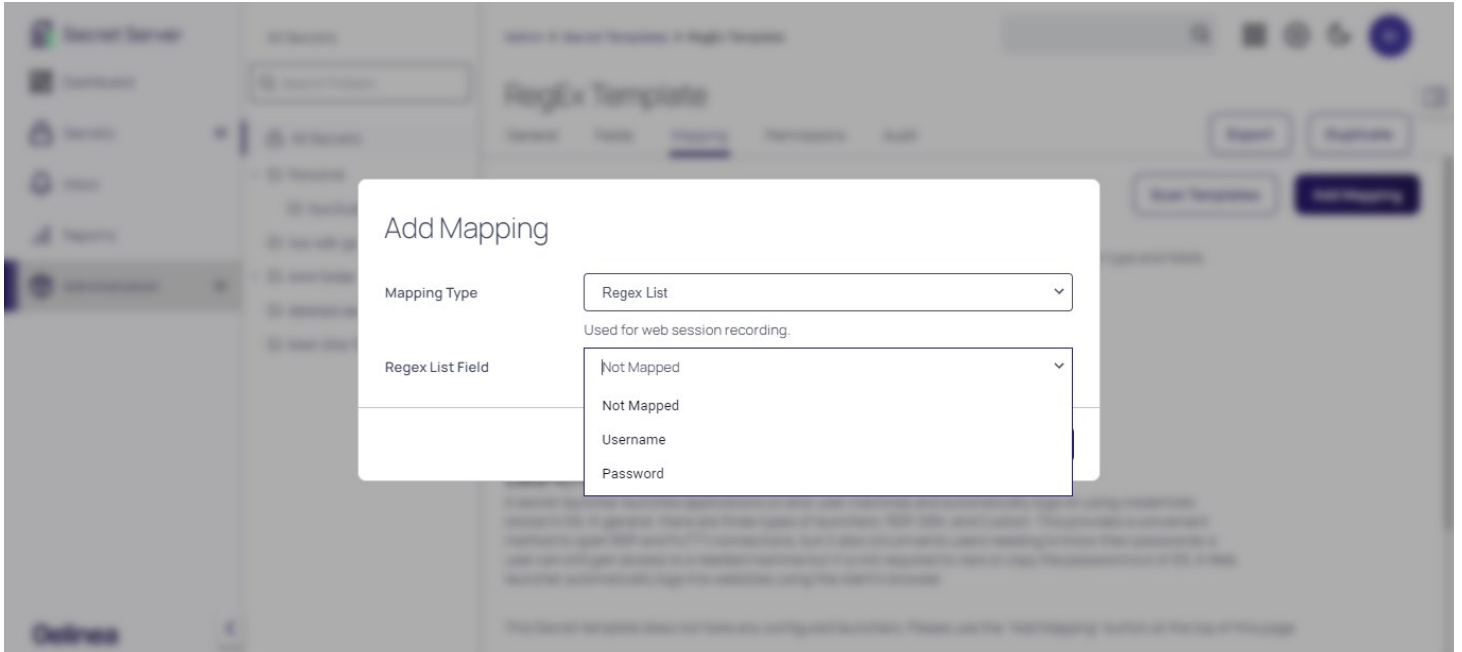
8. Click **Save**.

The template is now ready to be used in WPF.

If you have session recording enabled 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 both secrets are used, WPF will close the first session when the second session is selected, closing the tabs associated with the first secret. This is expected behavior, ensuring that the only sessions recorded are those associated with secrets that require session recording. Sites like *microsoftonline* 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 (e.g. .net, .com, .co.in) address, 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 was used to log into the Windows Admin Center directly. However, WPF **cannot** record RDP sessions logged into after that, because the main browser window still refers to the Windows Admin Center URL, and **not** to the RDP window nested inside the browser page.

In the sections below, users 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.

Supported Screen Resolution Sizes for Windows

		Chrome	Edge	Firefox
1920*1080	100	Yes	Yes	Yes
	125	Yes	Yes	Yes
	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
	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

Supported Screen Resolution Sizes for Mac

		Chrome
Monterey	1280*1024	Yes
	1024*768	Yes

BigSur	1024*768	Yes

Incognito Support

Follow these pre-requisite steps to ensure WPF 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/allow the following setting for:
    - Chrome: **Allow in incognito**
    - Edge: **Allow in InPrivate**
    - Firefox: **Run in Private Windows**
    - Opera: **Allow in incognito**
    - Safari: **Run in Private Window**
3. Login to WPF.

Port Numbers

Default ports (as defined by the browser) are stripped by the browser and treat URLs the same, this means basically that http://someurl is the same as http://someurl:80 and https://someurl.

When the domain is a non-primary / secondary domain, the port becomes part of the unique identifier and will be recorded independently.

- 10.0.0.61:55 is not the same as 10.0.0.61:555 or 10.0.0.61
- blue.local.something is not the same as blue.local.something:8080

List of Primary and Secondary Domains

.aaa.pro, .ab.ca, .abc.br, .abo.pa, .abogado, .abudhabi, .ac, .ac.cr, .ac.id, .ac.ke, .ac.mu, .ac.ni, .ac.nz, .ac.pa, .ac.th, .ac.vn, .aca.pro, .academy, .accountant, .accountant, .accountants, .acct.pro, .actor, .ad, .ads, .adult, .adult.ht, .ae, .ae.org, .aero, .af, .africa, .africa.com, .ag, .agency, .ai, .airforce, .al, .alsace, .am, .amsterdam, .analytics, .antivirus, .apartments, .app, .aq, .aquitaine, .ar.com, .arab, .archi, .architect, .architect, .army, .art, .art.do, .arts.nf, .arts.ve, .as, .asia, .asn.au, .asn.lv, .asso.km, .asso.mc, .associates, .at, .attorney, .auction, .audio, .author, .auto, .autos, .avocat.pro, .aw, .ax, .az, .ba, .baby, .band, .bank, .banque, .bar, .bar.pro, .barcelona, .bargains, .baseball, .basketball, .bayern, .bb, .bc.ca, .bcn, .be, .beauty, .beauty, .beer, .belem.br, .berlin, .best, .bet, .bg, .bh, .bi, .bib.ve, .bible, .bid, .bike, .bingo, .bio, .biz, .biz.az, .biz.bb, .biz.ck, .biz.cy, .biz.et, .biz.fj, .biz.ki, .biz.mv, .biz.ng, .biz.nr, .biz.om, .biz.pk, .biz.pl, .biz.pr, .biz.tj, .biz.tr, .biz.tt, .biz.vn, .bj, .black, .blackfriday, .blog, .blog.br, .blue, .bm, .bo, .boats, .bom, .bond, .boo, .book, .boston, .bot, .boutique, .br.com, .broadway, .broker, .brussels, .bs, .bt, .budapest, .build, .builders, .business, .buy, .buzz, .bw, .by, .bz, .bzh, .ca, .cab, .cafe, .cal, .call, .cam, .camera, .camp, .cancerresearch, .capetown, .capital, .car, .cards, .care, .career, .careers, .cars, .casa, .cash, .casino, .cat, .catering, .catholic, .cc, .cd, .center, .ceo, .cf, .cfa, .cfd, .cg, .ch, .channel, .charity, .chat, .cheap, .christmas, .church, .ci, .cin.kg, .circle, .city, .ck, .cl, .claims, .cleaning, .click, .clinic, .clothing, .cloud, .club, .club.tw, .cm, .cn, .cn.com, .cnidn, .cnregional, .co, .co.ae, .co.ag, .co.ao, .co.at, .co.az, .co.bb, .co.bi, .co.bw, .co.bz, .co.ci, .co.ck, .co.cm, .co.com, .co.cr, .co.de, .co.dm, .co.ee, .co.fk, .co.gg, .co.gl, .co.gy, .co.id, .co.il, .co.in, .co.ir, .co.je, .co.jp, .co.ke, .co.lc, .co.ls, .co.ma, .co.me, .co.mu, .co.mw, .co.mz, .co.na, .co.ni, .co.nl, .co.no, .co.nu, .co.nz, .co.om, .co.pn, .co.rs, .co.sh, .co.th, .co.tj, .co.tt, .co.tz, .co.ug, .co.uk, .co.ve, .co.vi, .co.za, .co.zm, .co.zw, .coach, .codes, .coffee, .college, .cologne, .com, .com.af, .com.ag, .com.al, .com.an, .com.aq, .com.ar, .com.au, .com.az, .com.ba, .com.bb, .com.bd, .com.bh, .com.bi, .com.bj, .com.bm, .com.bn, .com.bo, .com.br, .com.bs, .com.bt, .com.bw, .com.by, .com.bz, .com.ca, .com.ci, .com.cm, .com.cn, .com.co, .com.cu, .com.cv, .com.cy, .com.de, .com.do, .com.dz, .com.ec, .com.ee, .com.eg, .com.es, .com.et, .com.fj, .com.ge, .com.gh, .com.gi, .com.gl, .com.gn, .com.gp, .com.gt, .com.gu, .com.gy, .com.hn, .com.hr, .com.ht, .com.io, .com.jm, .com.jo, .com.kg, .com.kh, .com.ki, .com.km, .com.kn, .com.kw, .com.ky, .com.kz, .com.lb, .com.lc, .com.lk, .com.lr, .com.ls, .com.lv, .com.ly, .com.mk, .com.mm, .com.mo, .com.mt, .com.mu, .com.mv, .com.mw, .com.mx, .com.my, .com.na, .com.nf, .com.ng, .com.ni, .com.np, .com.nr, .com.om, .com.pa, .com.pe, .com.pf, .com.pg, .com.ph, .com.pk, .com.pl, .com.pn, .com.pr, .com.ps, .com.pt, .com.py, .com.qa, .com.sa, .com.sb, .com.sc, .com.sd, .com.se, .com.sg, .com.sh, .com.sl, .com.sn, .com.so, .com.sv, .com.tj, .com.tl, .com.tm, .com.tn, .com.tr, .com.tt, .com.tw, .com.ua, .com.ug, .com.uy, .com.vc, .com.ve, .com.vi, .com.vn, .com.ws, .com.ye, .community, .company, .compare, .computer, .condos, .conf.au, .conf.lv, .construction, .consulting, .contact, .contractors, .cooking, .cool, .coop, .coop.km, .corp, .corsica, .country, .coupon, .coupons, .courses, .cpa, .cpa.pro, .cr, .credit, .creditcard, .creditunion, .cricket, .cruise, .cruises, .cu, .cv, .cw, .cx, .cy, .cymru, .cz, .dad, .dance, .data, .date, .dating, .day, .dds, .de, .de.com, .deal, .dealer, .deals, .degree, .delivery, .democrat, .dental, .dentist, .desi, .design, .dev, .diamonds, .diet, .digital, .direct, .directory, .discount, .diy, .dj, .dk, .dm, .do, .docs, .doctor, .dog, .domains, .dot, .download, .drive, .dubai, .durban, .dz, .earth, .eat, .ebiz.tw, .ec, .eco, .ecom, .edu.bb, .edu.bi, .edu.bz, .edu.do, .edu.gl, .edu.gy, .edu.ki, .edu.km, .edu.lk, .edu.lv, .edu.mm, .edu.ni, .edu.np, .edu.pa, .edu.pl, .edu.pt, .edu.sl, .edu.sv, .edu.ve, .edu.vg, .edu.vn, .education, .ee, .eg, .email, .emp.br, .energy, .eng.pro, .engineer, .engineering, .enterprises, .equipment, .erotica.hu, .es, .esp.br, .esq, .estate, .et, .eu, .eu.com, .eus, .events, .exchange, .expert, .exposed, .express, .fail, .faith, .family, .fan, .fans, .far.br, .farm, .fashion, .fast, .feedback, .fi, .film, .fin.ec, .final, .finance, .financial, .financialaid, .finish, .fire, .firm.in, .firm.nf, .firm.ve, .fish, .fishing, .fit, .fitness, .flights, .floripa.br, .florist, .flowers, .fly, .fm, .fo, .foo, .food, .football, .forex, .forsale, .forum, .foundation, .fr, .free, .frl, .fun, .fund, .furniture, .furniture, .futbol, .fyi, .ga, .gal, .gallery, .game, .game.tw, .games, .garden, .gay, .gb.com, .gb.net, .gd, .gdn, .ge, .geek.nz, .gen.ck, .gen.in, .gen.nz, .gen.tr, .gent, .gf, .gg, .gh, .gi, .gift, .gifts, .gives, .giving, .gl, .glass, .global, .gm, .gmbh, .go.id, .gold, .golf, .gop, .got, .gouv.km, .gov.bb, .gov.gy, .gov.ki, .gov.mm, .gov.np, .gov.pt, .gov.sv, .gov.vn, .gp, .gq, .gr, .gr.com, .gr.jp, .graphics, .gratis, .green, .gripe, .grocery, .group, .gs, .gt, .guge, .guide, .guitars, .guru, .gy, .hair, .halal, .hamburg, .hangout, .haus, .health, .health.vn, .healthcare, .help, .helsinki, .here, .hiphop, .hiv, .hk, .hm, .hn, .hockey, .holdings, .holiday, .home, .homes, .horse, .hospital, .host, .hosting, .hot, .hoteis, .hotel, .hoteles, .hotels, .house, .how, .hr, .ht, .hu, .hu.com, .hu.net, .icu, .id, .id.au, .id.lv, .idn, .idv.tw, .ie, .im, .imamat, .immo, .immobilien, .in, .in.net, .in.th, .inc, .ind.br, .ind.gt, .ind.in, .industries, .info, .info.au, .info.az, .info.bb, .info.bi, .info.ck, .info.ec, .info.et, .info.fj, .info.ht, .info.hu, .info.ke, .info.ki, .info.mv, .info.nf, .info.nr, .info.pl, .info.pr, .info.tr, .info.tt, .info.ve, .info.vn, .ing, .ing.pa, .ink, .institute, .insurance, .insure, .int.ve, .int.vn, .international, .investments, .io, .iq, .ir, .irish, .is, .isla.pr, .islam, .ismaili, .ist, .istanbul, .it, .it.ao, .its.me, .jampa.br, .je, .jetzt, .jewelry, .jo, .jobs, .joburg, .jot, .joy, .jp, .jp.net, .jpn.com, .juegos, .jur.pro, .kaufen, .ke, .kg, .ki, .kid, .kids, .kiev.ua, .kim, .kitchen, .kiwi, .kiwi.nz, .km, .kn, .koeln, .kosher, .kr, .kr.com, .krd, .ky, .kyoto, .kz, .la, .land, .lat, .latino, .law, .law.pro, .lawyer, .lb, .lc, .lds, .lease, .legal, .lgbt, .li, .life, .lifeinsurance, .lifestyle, .lighting, .like, .limited, .limo, .link, .live, .living, .lk, .llc, .llp, .loan, .loans, .lol, .london, .lotto, .love, .lr, .ls, .lt, .ltd, .ltd.im, .ltd.uk, .ltda, .lu, .luxe, .luxury, .lv, .ly, .ma, .macapa.br, .madrid, .mail, .maison, .makeup, .man, .management, .maori.nz, .map, .market, .marketing, .markets, .mba, .mc, .md, .me, .me.ke, .me.uk, .med, .med.ec, .med.pa, .med.pro, .medecin.km, .media, .medical, .meet, .melbourne, .meme, .memorial, .men, .menu, .mex.com, .mg, .miami, .mil.id, .mil.km, .mil.mm, .mil.np, .minsk.by, .mk, .ml, .mls, .mn, .mo, .mo.bi, .mobi, .mobi.ke, .mobile, .moda, .moe, .moi, .mom, .money, .monster, .mormon, .mortgage, .moscow, .moto, .motorcycles, .mov, .movie, .mp, .mq, .mr, .ms, .mt, .mu, .museum, .music, .mutual, .mutualfunds, .mutuelle, .mv, .mw, .mx, .my, .my.tj,

.mz, .na, .nagoya, .name, .name.ae, .name.az, .name.cy, .name.eg, .name.et, .name.fj, .name.jo, .name.mv, .name.pr, .name.tr, .name.tt, .name.vn, .navy, .nc, .ne.jp, .ne.ke, .ne.tz, .ne.ug, .net, .net.ae, .net.af, .net.ag, .net.al, .net.ar, .net.au, .net.az, .net.ba, .net.bb, .net.bd, .net.bh, .net.bm, .net.bn, .net.bo, .net.br, .net.bs, .net.by, .net.bz, .net.ck, .net.cm, .net.cn, .net.co, .net.cv, .net.cy, .net.do, .net.dz, .net.ec, .net.eg, .net.et, .net.fj, .net.ge, .net.gg, .net.gl, .net.gn, .net.gp, .net.gr, .net.gt, .net.gu, .net.gy, .net.hn, .net.ht, .net.id, .net.il, .net.in, .net.io, .net.ir, .net.je, .net.jm, .net.jo, .net.kg, .net.kh, .net.ki, .net.kn, .net.kw, .net.ky, .net.kz, .net.lb, .net.lc, .net.lk, .net.lr, .net.ls, .net.lv, .net.ly, .net.ma, .net.me, .net.mm, .net.mo, .net.mt, .net.mu, .net.mv, .net.mw, .net.mx, .net.my, .net.nf, .net.ng, .net.ni, .net.np, .net.nr, .net.nz, .net.om, .net.pa, .net.pe, .net.pe, .net.pg, .net.ph, .net.pk, .net.pl, .net.pn, .net.pr, .net.ps, .net.py, .net.qa, .net.ru, .net.sa, .net.sb, .net.sc, .net.sg, .net.sh, .net.sl, .net.so, .net.th, .net.tj, .net.tl, .net.tn, .net.tr, .net.tt, .net.tw, .net.ua, .net.uk, .net.uy, .net.vc, .net.ve, .net.vi, .net.vn, .net.ws, .net.za, .network, .new, .news, .nf, .ng, .ngo, .ni, .nic.im, .ninja, .nl, .no, .no.com, .nom.ad, .nom.ag, .nom.br, .nom.co, .nom.es, .nom.fr, .nom.km, .nom.ni, .nom.pa, .nom.pe, .nom.ve, .notaires.km, .now, .nowruz, .nr, .nrw, .nu, .nuidn, .nyc, .nz, .observer, .off, .okinawa, .om, .one, .ong, .onl, .online, .ooo, .open, .or.at, .or.bi, .or.cr, .or.id, .or.jp, .or.ke, .or.th, .or.tz, .or.ug, .org, .org.ae, .org.af, .org.ag, .org.al, .org.ar, .org.au, .org.az, .org.ba, .org.bb, .org.bd, .org.bh, .org.bi, .org.bm, .org.bn, .org.bo, .org.br, .org.bs, .org.bw, .org.bz, .org.ck, .org.cn, .org.cv, .org.cy, .org.do, .org.dz, .org.ec, .org.eg, .org.es, .org.et, .org.fj, .org.ge, .org.gg, .org.gh, .org.gi, .org.gl, .org.gn, .org.gr, .org.gt, .org.gu, .org.gy, .org.hn, .org.ht, .org.hu, .org.il, .org.in, .org.io, .org.ir, .org.je, .org.jm, .org.jo, .org.kg, .org.kh, .org.ki, .org.kn, .org.ky, .org.kz, .org.lb, .org.lc, .org.lk, .org.lr, .org.ls, .org.lv, .org.ly, .org.ma, .org.me, .org.mm, .org.mo, .org.mt, .org.mu, .org.mv, .org.mw, .org.mx, .org.my, .org.mz, .org.na, .org.nf, .org.ng, .org.ni, .org.np, .org.nr, .org.nz, .org.om, .org.os, .org.pa, .org.pe, .org.pe, .org.pg, .org.ph, .org.pk, .org.pl, .org.pn, .org.pr, .org.ps, .org.pt, .org.py, .org.qa, .org.rs, .org.ru, .org.sa, .org.sb, .org.sc, .org.sh, .org.sl, .org.sn, .org.so, .org.sv, .org.tj, .org.tl, .org.to, .org.tr, .org.tt, .org.tw, .org.ua, .org.ug, .org.uk, .org.uy, .org.vc, .org.ve, .org.vi, .org.vn, .org.ws, .org.za, .organic, .osaka, .other.nf, .oz.au, .pa, .page, .paris, .pars, .partners, .parts, .party, .pay, .pe, .per.kh, .per.nf, .persiangulf, .pet, .pets, .pf, .ph, .pharmaciens.km, .pharmacy, .phd, .phone, .photo, .photography, .photos, .physio, .pics, .pictures, .pid, .pin, .ping, .pink, .pizza, .pk, .pl, .place, .play, .plc.im, .plc.uk, .plumbing, .plus, .pm, .pn, .poa.br, .poker, .porn, .pp.ru, .pr, .press, .presse.fr, .presse.km, .priv.me, .priv.no, .pro, .pro.ae, .pro.ec, .pro.fj, .pro.pr, .pro.vn, .prod, .productions, .prof, .promo, .properties, .property, .protection, .ps, .pt, .pub, .pvt.ge, .pw, .py, .qa, .qc.ca, .qc.com, .qpon, .quebec, .racing, .radio, .radio.am, .radio.fm, .re, .read, .realestate, .realtor, .realty, .rec.nf, .rec.ve, .recht.pro, .recife.br, .recipes, .red, .rehab, .reise, .reisen, .reit, .ren, .rent, .rentals, .repair, .report, .republican, .res.in, .rest, .restaurant, .retirement, .review, .reviews, .rich, .rio, .rio.br, .rip, .ro, .rocks, .rodeo, .room, .rs, .rsvp, .ru, .ru.com, .rugby, .ruhr, .run, .rw, .ryukyu, .sa, .sa.com, .saarland, .safe, .safety, .sale, .salon, .sarl, .sas, .save, .sb, .sc, .sc.ke, .sch.id, .scholarships, .school, .school.nz, .schule, .science, .scot, .sd, .se, .se.com, .se.net, .search, .secure, .security, .services, .sex, .sexy, .sg, .sh, .shiksha, .shoes, .shop, .shopping, .show, .si, .silk, .singles, .site, .sjc.br, .sk, .ski, .skin, .sl, .sld.pa, .sm, .smile, .sn, .so, .soccer, .social, .software, .solar, .solutions, .song, .soy, .spa, .space, .sport, .sports, .spot, .spreadbetting, .sr, .srl, .st, .stockholm, .storage, .store, .store.bb, .store.nf, .store.ve, .stream, .studio, .study, .style, .su, .sucks, .supplies, .supply, .support, .surf, .surgery, .sv, .swiss, .sx, .sy, .sydney, .systems, .taipei, .talk, .tatar, .tattoo, .tax, .taxi, .tc, .td, .team, .tech, .technology, .tel, .tennis, .tf, .tg, .th, .thai, .theater, .theatre, .tickets, .tienda, .tips, .tires, .tirol, .tj, .tk, .tl, .tm, .tm.cy, .tm.fr, .tm.km, .tm.mc, .tn, .to, .today, .tokyo, .tools, .top, .tour, .tours, .town, .toys, .toys, .trade, .trading, .training, .translations, .travel, .tt, .tube, .tunes, .tur.br, .tv, .tv.bb, .tv.br, .tw, .twidn, .ua, .ug, .uk, .uk.com, .uk.net, .um, .university, .uno, .us, .us.com, .us.org, .uy, .uy.com, .uz, .vacations, .vc, .ve, .vegas, .ventures, .versicherung, .vet, .veterinaire.km, .vg, .vi, .viajes, .video, .villas, .vin, .vip, .vision, .vix.br, .vlaanderen, .vn, .vodka, .vote, .voting, .voto, .voyage, .vu, .wales, .wang, .watch, .watches, .waw.pl, .weather, .web, .web.do, .web.id, .web.nf, .web.pk, .web.tj, .web.tr, .web.ve, .web.za, .webcam, .webs, .website, .wed, .wedding, .weibo, .wf, .whoswho, .wien, .wiki, .win, .wine, .winners, .work, .works, .world, .wow, .ws, .wtf, .xihuan, .xin, .xxx, .xyz, .yachts, .yachts, .ye, .yellowpages, .yoga, .yokohama, .you, .yt, .yun, .za.com, .zip, .zm, .zone, .zw
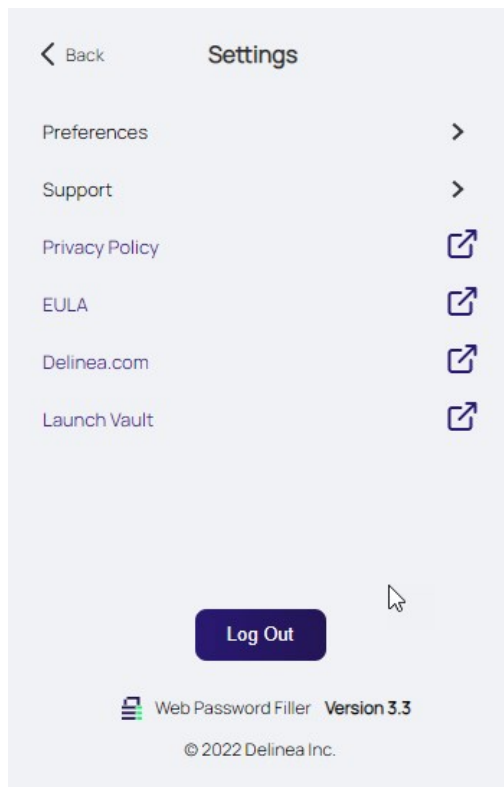
Logout of Secret Server

Use the WPF icon to logout:

1. On the upper-right of the browser, click the WPF icon:

2. The WPF logout modal opens.


   Click **Logout**.

3. The WPF icon changes to:

Windows Admin Center Support

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

- New user name will default/use a web password template only (Windows and AD templates are not supported)

- Using the "Connect" button in Windows Admin Center, will not show secrets associated with the selected machine

    - Work around: Select the machine link to retrieve the associated secrets

- Updating passwords will update the password in the current secret regardless of template

- How secrets are returned:

    - 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

- Session Recording of non-web password templates is not allowed. If an attempt to use a secret to log into an RDP session is made and the secret has session recording enabled, WPF will not allow the user to proceed and display the following message.
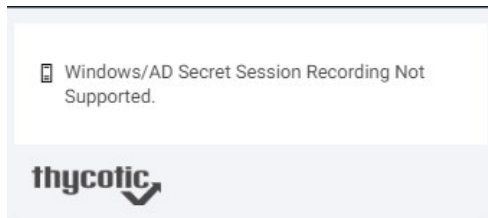
# Using Web Password Filler with Microsoft Online Services

This section guides users through using the Web browser extension to use Secret Server WPF to login to Microsoft Online. Launching Microsoft Online secrets with WPF takes a bit of extra configuration. This section explains the issue and suggests remedies.

> **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 SS. If Microsoft Online is your first site using WPF, we suggest first testing your installation on another site.

When you try to open a Microsoft Online secret with WPF, you might see
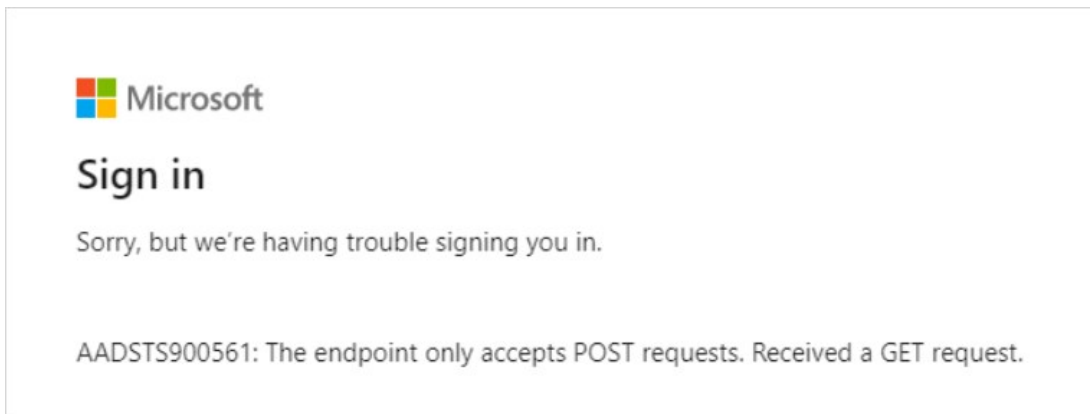
or
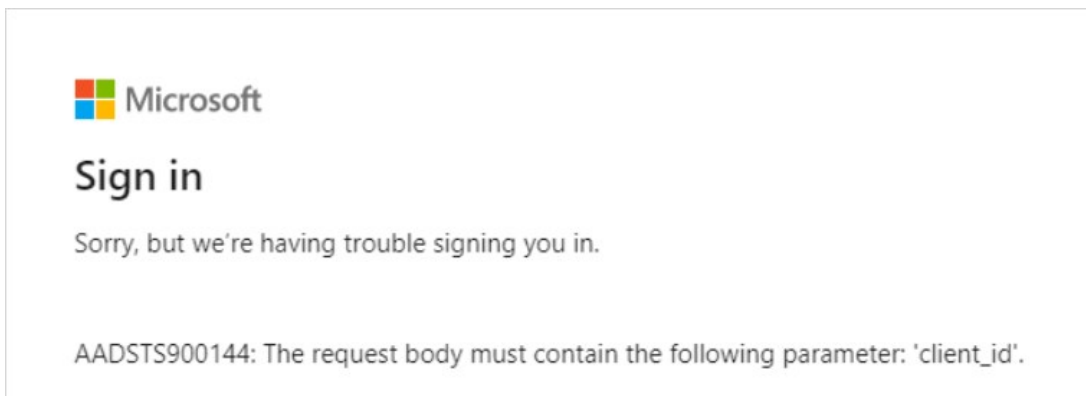
Neither of these errors provide a useful explanation. The real issue is simple with a very easy solution that you can implement yourself.

Normally, WPF captures the URL of the website you are on when it creates a secret, storing the 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 on with that secret, you get an error because the log on URL initially stored in the secret is for a redirected page that is no longer valid. Fortunately, WPF uses the URL stored in the secret, so once you adjust that URL, you never have to do it again.

The original (errant) stored URL is:

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

The permanent (real) URL is:

https://login.microsoftonline.com

So all that is needed is to ensure the secret stores the permanent URL, not the origin one.
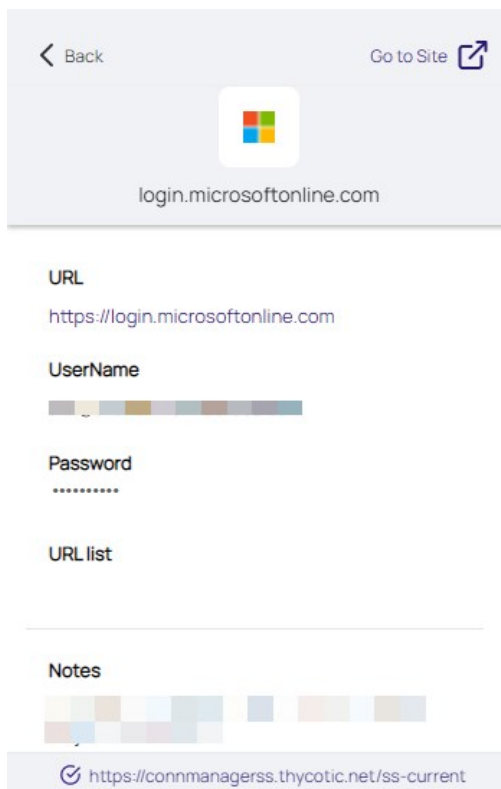
There are two ways to do this:

- **Before Saving the WPF Secret:** Change the URL when it is initially stored, right from WPF, *before* the secret is saved. This method is available 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:** Change the URL after the WPF secret is stored in SS. This method is the only option if the WPF secret has already been saved in Secret Server with the one-time redirected URL. This could happen because the WPF secret was created by an earlier WPF version or because you created the secret using the automatic secret creation feature, which captured the one-time redirected URL rather than the permanent one.

Important: Read this *entire* instruction before starting it.

If you have not yet created the secret, follow this method:

1. Go to the Microsoft Online log on (you already have an account and log on) or log-on setup page (you are setting up a new log on).

2. Follow the Creating Secrets procedure.

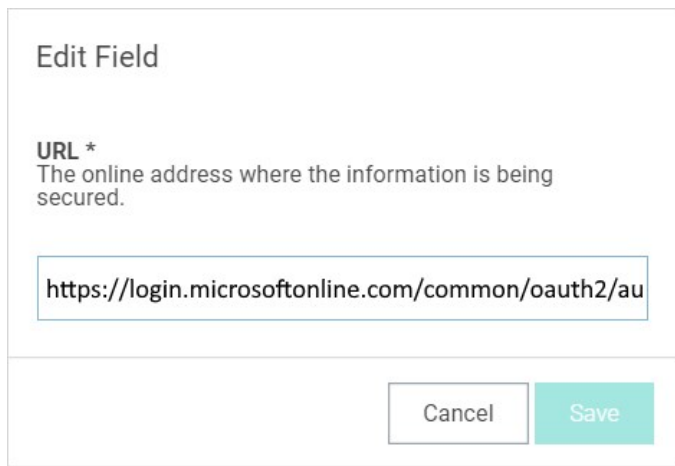3. When you get to the *second* "Add Account to Secret Server" popup, which looks like this:

You now see the website URL that WPF inferred, which is incorrect. The secret name was inferred too—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.

1. Login to SS.

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. Logout of SS.

7. Return to Microsoft Online to test the secret. You will need to login again.

Launching Comma-Separated URLs

In the event that a user has multiple URLs saved under the URL field, they will be able to see a dropdown list of all the saved URLs on a new row. They also have the ability to select and launch the desired URL with a click of a button through the custom web launcher.

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

1. In the *Secret Templates* tab inside Secret Server, find the secret template with comma separated URLs.

2. Click **Duplicate**

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

4. Inside the duplicate template, click the *Mapping* tab

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

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

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

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

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

To use the custom web launcher follow these simple steps:

1. Create a secret with the newly created template

Create New Secret

Personal/Ilya Dudkin   Change   Clear

Choose a Secret Template

Test Template

Test Template

Cancel   Create Secret

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

Create New Secret

Secret Template	Test Template **Change**
Folder	Personal/Ilya Dudkin ⊗
Secret Name *	
UserName	
Password	👁 Generate
Notes	
URL LIST	

Cancel   Create Secret

Unlimited Admin Mode

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

Create New Secret

Password	👁 Generate
Notes	
URL LIST	about.me,https://greenshadesonline.com/sso/admin/,https://www.tomorrow.do/
Site	Default ⌄

Cancel **Create Secret**

Unlimited Admin Mode

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

Secret Server

- 🔲 Dashboard
- 🔒 Secrets »
- 🔔 Inbox
- 📊 Reports
- 📦 Administration «

Delinea

Administration

🔍 secrets

← Back

Search Results

Export / Import

DevOps Secrets Vault

Discovery Secret Search Filt...

Secret Policies

Secret Templates

ℹ INFORMATION
Secret Server Cloud will be undergoing scheduled maintenance on February 4th 2023 between 2:00 PM and 6:00 PM ET, some features may be unavailable briefly during this window.   **Dismiss**

Secrets > Test-Comma-Separated-URL

Test-Comma-Separated-URL ☆

Options ⌄

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.

💻 Web Password Filler

No Active Sessions

Expiration and Heartbeat

Accessing Websites With Self-Signed Certificates on Chrome

In January 2024, Google will roll out Manifest V3, which means that you will no longer be able to use extensions that run Manifest V2. When this happens, there will be some changes in how Web Password Filler works with websites with self-signed certificates.

Below you will find some of the differences between how Web Password Filler handled websites with self-signed certificates on Manifest V2 and how they will be handled on Manifest V3.

With Secret Server URLs that had self-signed certificates, Web Password Filler would load the self-signed urls (e.g. local sites("https://localhost/somesite") and users would get an error and they would be redirected to that same URL in another tab. This other tab would display the following error: net::Err_CERT_COMMON_NAME_INVALID. If Web Password Filler accepted the certificate, the extension was allowed to proceed further. Below you can find the steps that reproduce this error:

1. Load local sites("https://localhost/somesite")
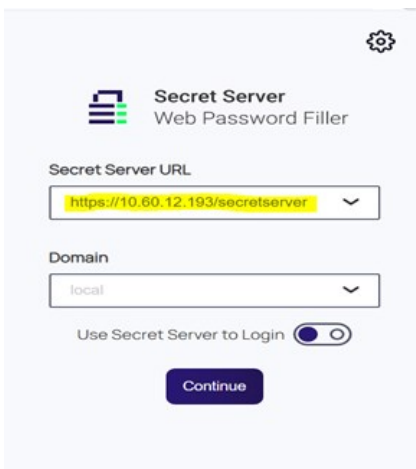
2. User would encounter the certificate error displayed below:
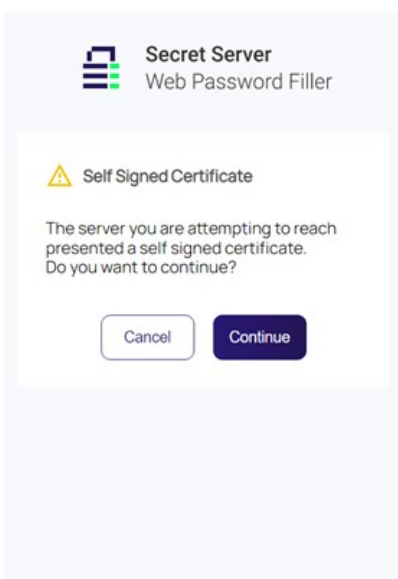
3. After clicking **Continue** users would be redirected to another tab where they would see the following error message: net::Err_CERT_COMMON_NAME_INVALID
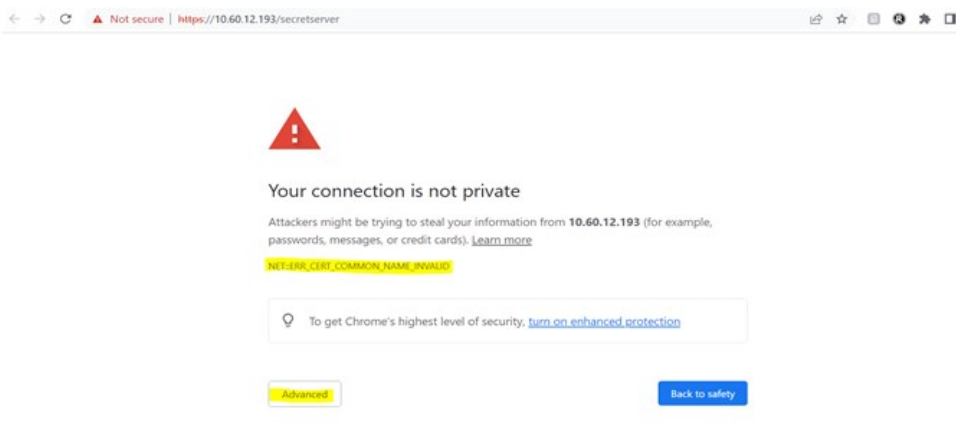
4. After clicking **Advanced** Web Password Filler is able to accept the self-singed certificate and the extension is allowed to proceed further.

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

1. Loads the self-signed urls e.g. local sites("https://localhost/somesite")
2. Users still get an error in the extension and are redirected to that same URL on another tab.
3. On the other tab users get the following error net::Err_CERT_COMMON_NAME_INVALID
4. If Web Password Filler accepts the certificate, the extension will continue to display the same error
5. Web Password Filler is not able to make any API calls to Secret Server
6. The extension is not allowed to proceed further

   Note: A workaround for a self-signed certificate issue in Manifest V3 is that the user needs to setup a local CA

Troubleshooting

The following Troubleshooting topics are available for the Web Password Filler:

- Enable Diagnostic Logging
- General questions to troubleshoot WPF issues
  - Version Compatibility
  - Login Issues
  - Problem Presentation/Behavior experienced by the user
  - Using Web Password Filler with Microsoft Online Services

Enable Diagnostic Logging

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

Items logged are:

- API methods trying to access Secret Server which are not supported and create error conditions.
- Secret Server URL.
- Date/Time stamp.
- Log download option via **View Log** access.

WPF offers functionality to print logs to a log file which includes details such as:

- Which API was called
- Which Secret Server the user is logged into
- 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 developer tools.

Investigating WPF Issues

When investigating issues with the Web Password Filler (WPF) the following questions should help narrow down the issue or provided needed information to troubleshoot.

Confirm that the issue is with the new Web Password Filler that was first released in Dec 2019 and in conjunction with Secret Serverv10.7.59.

Problems with other browser extensions/plugins (e.g. Login Assist, Clipboard Utility etc.) should not be deemed as WPF issues.

What browser is the issue occurring on?

- We currently support: Chrome, Firefox, Edge (Chromium) and Opera.

  General Chromium should work as well, but it is not officially supported.

- 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?

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, then we need the URL for the Facebook page that the browser is on when it fails.

- For issues of the WPF login failing, if you change the web page you are on when you try to login does it still occur?

- We will always want to know what **URL** you are on when an issue occurs, since some web pages might be trying to interfere with WPF.

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.

We don't list the version number in WPF directly, so you will need to go to the Extensions/Add-on page to get the version number. The location to get this value is roughly, but each browser does it slightly differently.

Basic steps to get this value are:

1. Go to the Settings menu in the browser. This it 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. The version number will be listed:

- ○ **Chrome** – At the top of the extension, in-line with the name.
- ○ **Firefox** – Click on the add-on to get the details and there will be a "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.

What type of action are you trying to perform?

There are a few basic action types that a user might be trying to take. They can include:

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.

What Secret template are they using?

The Web Password Filler is primarily designed to work with Secrets that use the Web Password template but can work for Secrets that use other templates.

In order to work with other Secret templates those templates need to have a URL field.

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

> **Note**: The URL field needs to be listed as "Searchable" in the Edit Templates screen in Secret Server.

WPF Login

Are you logged into WPF?

Currently you do need to log into WPF separately from SS. This is because we use the REST APIs to communicate back to SS. This design is also to allow users to log into WPF but NOT SS, which would let them go to a site and still access Secrets without using Secret Server directly.

You can tell at a glance if you are logged in or not by the icon in the browser.

1. Not Logged in

2. Logged in

There are two different methods for logging in:

1. Username and Password
2. SAML authentication through Secret Server. Refer to the Secret Server documentation on SAML

Are you experiencing issues logging in with Chrome or Edge?"

Customers using Web Password Filler version 3.2 or earlier may experience issues logging in on Chrome or Edge after these browsers made internal improvements. This issue was fixed in the 3.3 release.

Previous Products Compatibility

Is the old Login Assist or Secret Server Clipboard Utility installed?

If **either** of the old browser extensions are installed it is recommended that you **disable** them from the extensions page. Once they are disabled you should **refresh** your page (or if possible, completely close and re-open the browser but if they don't want to lose work in other tabs you should be able to just refresh).

After the old extensions are disabled, please refresh or close the browser and then try again. Does it still occur?

If it still reoccurs it might be worth seeing what other extensions might be installed to see if they are interfering.

We recommend **NOT** running the new WPF at the same time as the old Login Assist and Clipboard Utilities are enabled. Since they are all effectively trying to do the same thing, they can end up conflicting with each other and cause issues. As a result, they should not all be enabled at the same time.

Behavior/Problem Presentation

If reporting problems or asking for help with WPF, the more information that can be provided about the actual behavior experienced, the faster a resolution can be found.

All of previous troubleshooting topic help narrow things down. The more specific, the better.

Some examples:

1. Is the user not able to login to WPF?

   - Are they getting any error messages?
   - Are they logging in and then getting logged out again?
   - What authentication types are enabled and are they using them?
   - Is the "Login" button greyed out?
   - Is the Secret Server URL (and optional: Domain) entered in the "Configuration" tab?
   - Can they reach the Secret Server UI from the same machine/browser?

2. Is the Secret not being displayed on the site?

   - Is there only one Secret for the site?

     1. If Yes, then are all the Secret not being displayed? Or just some Secrets not displayed?

   - Does the logged in account have access to that Secret?

3. Are the credential fields populated correctly?

   - If No, what fields are being populated?

   - Is the green Delinea check logo displayed in the Username/email field?

     1. We ONLY display this in the Username or email fields, it is NOT displayed in the password field

   - Are the right-click options available in any of the login fields?

   - Which fields are not populated?

   - Are they populated and put in the wrong spot?

   - 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 log (like LinkedIn)?

4. Is it some kind of visual issue on the page?

   - Is the green Delinea log visible? Delinea
   - 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 a Secret is added in Secret Server or in WPF there are times when it might not appear immediately on the site. WPF relies on the Secret being indexed in SS, and it typically takes some time for that index to happen (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.

- In Release 1.1.0 of WPF a short-term caching option was introduced. This is indicated by 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. Is there some kind of other issue happening? If so, what?

Information on Security Scans

Periodically we run a security scan on the Web Password Filler. The results will be provided to our customers whenever available.

- [Checkmarx - scan on WPF 2.x](#)

Checkmarx Results

Based on the report results there are no Medium/High issues found, and nothing confirmed as valid issues.

    Note: The output file was edited to remove any unconfirmed and non-exploitable issues.

- Project Name: Thycotic.Integrations.WebPasswordFiller
- Scan Start: Tuesday, September 15, 2020 1:36:52 AM
- Preset: Checkmarx Default
- Scan Time: 00h:09m:34s
- Lines Of Code Scanned: 112606
- Files Scanned: 212
- Report Creation Time Tuesday, September 15, 2020 1:53:44 AM
- Online Results: No longer available
- Team: CxServer
- Checkmarx Version: 8.8.0.72 HF9
- Scan Type: Full
- Source Origin: GIT
- Density: 0/100 (Vulnerabilities/LOC)
- Visibility: Public

Filter Settings

Severity

- Included: High, Medium
- Excluded: Low, Information

Result State

- Included: Confirmed
- Excluded: Not Exploitable, To Verify, Urgent, Proposed Not Exploitable

Assigned to

- Included: All

Categories

- Included:

    - Uncategorized: All
    - Custom: All
    - PCI DSS v3.2: All
    - OWASP Top 10 2013: All
    - FISMA 2014: All
    - NIST SP 800-53: All

- OWASP Top 10 2017: All
- OWASP Mobile Top 10 2016: All

- Excluded:

  - Uncategorized: None
  - Custom: None
  - PCI DSS v3.2: None
  - OWASP Top 10 2013: None
  - FISMA 2014: None
  - NIST SP 800-53: None
  - OWASP Top 10 2017: None
  - OWASP Mobile Top 10 2016: None

Results Limit

Results limit per query was set to 500.

Selected Queries

Queries cannot be displayed because the report contains no results.

								[1]
A1-Injection [^2]	App. Specific	EASY	COMMON	EASY	SEVERE	App. Specific	0	0
A2-Broken Authentication [^2]	App. Specific	EASY	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A3-Sensitive Data Exposure [^2]	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	App. Specific	0	0
A4-XML External Entities (XXE)	App. Specific	AVERAGE	COMMON	EASY	SEVERE	App. Specific	0	0
A5-Broken Access Control [^2]	App. Specific	AVERAGE	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A6-Security Misconfiguration	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A7-Cross-Site Scripting (XSS) [^2]	App. Specific	EASY	WIDESPREAD	EASY	MODERATE	App. Specific	0	0
A8-Insecure Deserialization	App. Specific	DIFFICULT	COMMON	AVERAGE	SEVERE	App. Specific	0	0
A9-Using Components with Known Vulnerabilities [^2]	App. Specific	AVERAGE	WIDESPREAD	AVERAGE	MODERATE	App. Specific	0	0

							1	
A10-Insufficient Logging & Monitoring	App. Specific	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	App. Specific	0	0

[1] Best fix location values are absolute values derived from the entire vulnerabilities detected.

[^2] Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

							1	
A1-Injection [^2]	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	AVERAGE	SEVERE	ALL DATA	0	0
A2-Broken Authentication and Session Management [^2]	EXTERNAL, INTERNAL USERS	AVERAGE	WIDESPREAD	AVERAGE	SEVERE	AFFECTED DATA AND FUNCTIONS	0	0
A3-Cross-Site Scripting (XSS) [^2]	EXTERNAL, INTERNAL, ADMIN USERS	AVERAGE	VERY WIDESPREAD	EASY	MODERATE	AFFECTED DATA AND SYSTEM	0	0
A4-Insecure Direct Object References [^2]	SYSTEM USERS	EASY	COMMON	EASY	MODERATE	EXPOSED DATA	0	0
A5-Security Misconfiguration	EXTERNAL, INTERNAL, ADMIN USERS	EASY	COMMON	EASY	MODERATE	ALL DATA AND SYSTEM	0	0
A6-Sensitive Data Exposure [^2]	EXTERNAL, INTERNAL, ADMIN USERS, USERS BROWSERS	DIFFICULT	UNCOMMON	AVERAGE	SEVERE	EXPOSED DATA	0	0
A7-Missing Function Level Access Control	EXTERNAL, INTERNAL USERS	EASY	COMMON	AVERAGE	MODERATE	EXPOSED DATA AND FUNCTIONS	0	0
A8-Cross-Site Request Forgery (CSRF)	USERS BROWSERS	AVERAGE	COMMON	EASY	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0
A9-Using Components with	EXTERNAL USERS, AUTOMATED	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND	0	0

Known Vulnerabilities	TOOLS					FUNCTIONS	[1]	
A10-Unvalidated Redirects and Forwards	USERS BROWSERS	AVERAGE	WIDESPREAD	DIFFICULT	MODERATE	AFFECTED DATA AND FUNCTIONS	0	0

[1] Best fix location values are absolute values derived from the entire vulnerabilities detected.

[^2] Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

I Category I Issues Found I Best Fix Locations [1] I I ----- ----------------------I-------------I-------------------------I I PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection [^2] I 0 I 0 I I PCI DSS (3.2) - 6.5.2 - Buffer overflows I 0 I 0 I I PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage [^2] I 0 I 0 I I PCI DSS (3.2) - 6.5.4 - Insecure communications [^2] I 0 I 0 I I PCI DSS (3.2) - 6.5.5 - Improper error handling I 0 I 0 I I PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS) [^2] I 0 I 0 I I PCI DSS (3.2) - 6.5.8 - Improper access control I 0 I 0 I I PCI DSS (3.2) - 6.5.9 - Cross-site request forgery I 0 I 0 I I PCI DSS (3.2) - 6.5.10 - Broken authentication and session management [^2] I 0 I 0 I

- [1] Best fix location values are absolute values derived from the entire vulnerabilities detected.
- [^2] Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - FISMA 2014

		[1]	
Access Control [^2]	Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.	0	0
Audit And Accountability	Organizations must: (i) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and (ii) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.	0	0
Configuration Management [^2]	Organizations must: (i) establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and (ii) establish and enforce security configuration settings for information technology products employed in organizational information systems.	0	0
Identification And Authentication [^2]	Organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.	0	0

		[1]	
Media Protection [^2]	Organizations must: (i) protect information system media, both paper and digital; (ii) limit access to information on information system media to authorized users; and (iii) sanitize or destroy information system media before disposal or release for reuse.	0	0
System And Communications Protection [^2]	Organizations must: (i) monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems; and (ii) employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational information systems.	0	0
System And Information Integrity [^2]	Organizations must: (i) identify, report, and correct information and information system flaws in a timely manner; (ii) provide protection from malicious code at appropriate locations within organizational information systems; and (iii) monitor information system security alerts and advisories and take appropriate actions in response.	0	0

- [1] Best fix location values are absolute values derived from the entire vulnerabilities detected.
- [^2] Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - NIST SP 800-53

	[1]	
AC-12 Session Termination (P2)	0	0
AC-3 Access Enforcement (P1)	0	0
AC-4 Information Flow Enforcement (P1)	0	0
AC-6 Least Privilege (P1)	0	0
AU-9 Protection of Audit Information (P1)	0	0
CM-6 Configuration Settings (P2)	0	0
IA-5 Authenticator Management (P1)	0	0
IA-6 Authenticator Feedback (P2)	0	0
IA-8 Identification and Authentication (Non-Organizational Users) (P1)	0	0
SC-12 Cryptographic Key Establishment and Management (P1)	0	0
SC-13 Cryptographic Protection (P1)	0	0
SC-17 Public Key Infrastructure Certificates (P1)	0	0

		1
SC-18 Mobile Code (P2) [^2]	0	0
SC-23 Session Authenticity (P1)	0	0
SC-28 Protection of Information at Rest (P1) [^2]	0	0
SC-4 Information in Shared Resources (P1)	0	0
SC-5 Denial of Service Protection (P1)	0	0
SC-8 Transmission Confidentiality and Integrity (P1) [^2]	0	0
SI-10 Information Input Validation (P1) [^2]	0	0
SI-11 Error Handling (P2)	0	0
SI-15 Information Output Filtering (P0) [^2]	0	0
SI-16 Memory Protection (P1)	0	0

- [1] Best fix location values are absolute values derived from the entire vulnerabilities detected.
- [^2] Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - OWASP Mobile Top 10 2016

		1	
M1-Improper Platform Usage	This category covers misuse of a platform feature or failure to use platform security controls. It might include Android intents, platform permissions, misuse of TouchID, the Keychain, or some other security control that is part of the mobile operating system. There are several ways that mobile apps can experience this risk.	0	0
M2-Insecure Data Storage [^2]	This category covers insecure data storage and unintended data leakage.	0	0
M3-Insecure Communication	This category covers poor handshaking, incorrect SSL versions, weak negotiation, cleartext communication of sensitive assets, etc.	0	0
M4-Insecure Authentication [^2]	This category captures notions of authenticating the end user or bad session management. This can include: a. Failing to identify the user at all when that should be required, b. Failure to maintain the user's identity when it is required, c. Weaknesses in session management	0	0
M5-Insufficient Cryptography	The code applies cryptography to a sensitive information asset. However, the cryptography is insufficient in some way. Note that anything and everything related to TLS or SSL goes in M3. Also, if the app fails to use cryptography at all when it should, that probably belongs in M2. This category	0	0

			1
	is for issues where cryptography was attempted, but it wasn't done correctly.		
M6-Insecure Authorization	This is a category to capture any failures in authorization (e.g., authorization decisions in the client side, forced browsing, etc.). It is distinct from authentication issues (e.g., device enrolment, user identification, etc.). If the app does not authenticate users at all in a situation where it should (e.g., granting anonymous access to some resource or service when authenticated and authorized access is required), then that is an authentication failure not an authorization failure.	0	0
M7-Client Code Quality [^2]	This category is the catch-all for code-level implementation problems in the mobile client. That's distinct from server-side coding mistakes. This would capture things like buffer overflows, format string vulnerabilities, and various other code- level mistakes where the solution is to rewrite some code that's running on the mobile device.	0	0
M8-Code Tampering [^2]	This category covers binary patching, local resource modification, method hooking, method swizzling, and dynamic memory modification. Once the application is delivered to the mobile device, the code and data resources are resident there. An attacker can either directly modify the code, change the contents of memory dynamically, change or replace the system APIs that the application uses, or modify the application's data and resources. This can provide the attacker a direct method of subverting the intended use of the software for personal or monetary gain.	0	0
M9-Reverse Engineering [^2]	This category includes analysis of the final core binary to determine its source code, libraries, algorithms, and other assets. Software such as IDA Pro, Hopper, otool, and other binary inspection tools give the attacker insight into the inner workings of the application. This may be used to exploit other nascent vulnerabilities in the application, as well as revealing information about back end servers, cryptographic constants and ciphers, and intellectual property.	0	0
M10-Extraneous Functionality	Often, developers include hidden backdoor functionality or other internal development security controls that are not intended to be released into a production environment. For example, a developer may accidentally include a password as a comment in a hybrid app. Another example includes disabling of 2-factor authentication during testing.	0	0

- [1] Best fix location values are absolute values derived from the entire vulnerabilities detected.
- [^2] Project scan results do not include all relevant queries. Presets and\or Filters should be changed to include all relevant standard queries.

Scan Summary - Custom

		1
Must audit	0	0
Check	0	0
Optional	0	0

1. Best fix location values are absolute values derived from the entire vulnerabilities detected.

Release Notes

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

- 3.4.4 Release Notes

Previously released versions:

- 3.4.3 Release Notes
- 3.4.2 Release Notes
- 3.4.1 Release Notes
- 3.4.0 Release Notes
- 3.3.0 Release Notes
- 3.2.0 Release Notes
- 3.1.0 Release Notes
- 3.0.1 Release Notes
- 3.0.0 Release Notes
- 2.0.6 Release Notes
- 2.0.5 Release Notes
- 2.0.4 Release Notes
- 2.0.3 Release Notes
- 2.0.2 Release Notes
- 2.0.1 Release Notes
- 2.0.0 Release Notes
- 1.1.0 Release Notes
- 1.0.10 Release Notes
- 1.0.9 Release Notes
- 1.0.8 Release Notes - initial release

3.4.4 Release Notes

April 3rd, 2023

- 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.

Documentation Changelog

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

- [Release Notes](#)

- [Release Notes](#)

- [Release notes](#)

- [Release Notes](#)

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

- [Release Notes](#)
- [Refresh](#) option and hover.
- [Comment and Checkout](#) option.
- [View Logs and download](#) option.

- 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.

- [Release Notes](#)

- [Release Notes](#)

- [Release Notes](#)

- [Release Notes](#)

- [Release Notes](#)

- [Release Notes](#)

2.0.3 Release Updates

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

- Added [Security Scans](#) section.