

Web Password Filler

Administrator Guide

Version: 3.6.x

Publication Date: 11/6/2023

Web Password Filler Administrator Guide

Version: 3.6.x, Publication Date: 11/6/2023

© Delinea, 2023

Warranty Disclaimer

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

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

Disclaimer of Liability

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

Table of Contents

Web Password Filler	1
Getting Started	1
Enable Web Services in Secret Server	1
Connecting to the Delinea Platform and Secret Server	1
Connecting to the Delinea Platform	1
Connect to Secret Server	5
Local Login	9
Default Protocols	9
Redirecting to Secret Server via Hyperlink	10
Terminology	11
Secret Server Web Password Filler	11
Secret Server Login Assist	13
Secret Server Clipboard Utility	15
Installing Browser Extensions	16
Native Messaging Host	17
Installing the Native Messaging Host	17
Download Location	17
Requirements	17
Supported Browsers	17
Installation	18
Registration	18
Uninstalling the Delinea Native Messaging Host	18
Configuration Options	18
Establishing Default Settings and Browser-Specific Overrides	18
Settings.json Format	19
Site Exclusions and Exceptions	23
UI Behavior Based on Preferences	23
Error Messages	25
Preferences Menu	26
Using WPF	29
Log in to a Website	29
Accessing Secrets Guarded by MFA	30
Session Recording	31
Enabling Mouse Path Tracking On Recordings	32
Session Recording Limits	36
RegEx	36
Using RegEx in WPF	37
Setup in Secret Server	39
Resolutions	42
Supported Screen Resolution Sizes for Windows	42

Table of Contents

Supported Screen Resolution Sizes for Mac	44
Launching Comma-Separated URLs	44
Create a Secret Template	44
Using the Custom Web Launcher	54
Comment Required Option	58
Comment Required When the "Hide Secret Server Version Number" setting is Enabled	58
Creating a Secret for a Website	59
Choose a Secret Template	61
Choose a Folder	61
Site	62
Recent and Favorites - Refresh	64
Mapping Login Fields	65
Map fields on a Web page form to the fields in a Secret	65
Enabling Field Mapping with Metadata	67
Mapping Secrets With Three or More Login Fields	68
Incognito Support	72
Logout of Secret Server	72
Using Web Password Filler with Microsoft Online Services	73
The Problem	74
What Is Going on?	74
Fixing the Issue When Creating the WPF Secret	75
Fixing the Issue After Having Saved the WPF Secret	76
Port Numbers	77
Accessing Websites With Self-Signed Certificates on Chrome	77
Working With Self-Signed Certificates on Manifest V2	78
Working With Self-Signed Certificates on Manifest V3	80
Windows Admin Center Support	80
Troubleshooting	81
Enable Diagnostic Logging	81
Previous Products Compatibility	82
WPF Login	82
Login Method	82
Issues Logging In With Chrome or Edge	82
Behavior/Problem Presentation	83
Investigating WPF Issues	84
Confirm WPF Version	84
Identify the Browser	84
Site Information	84
Access to Site	84
What version of WPF are you encountering the issue on?	85
Action to be Performed	85
Templates Used	85

Table of Contents

Release Notes	86
1.0.10 Release Notes	87
Enhancements	87
1.0.8 Release Notes	87
1.0.9 Release Notes	88
Bug Fixes	88
1.1.0 Release Notes	88
Enhancements	88
Bug Fixes	88
Firefox Specific	88
2.0.0 Release Notes	89
Enhancements	89
Bug Fixes	89
2.0.1 Release Notes	89
Enhancements	89
Bug Fixes	90
2.0.2 Release Notes	91
Enhancements	91
Bug Fixes	91
Known Issues	92
2.0.3 Release Notes	93
Enhancements	93
Security	94
Bug Fixes	94
Known Issues	94
2.0.4 Release Notes	95
Enhancements	95
Bug Fixes	95
Known Limitations	96
2.0.5 Release Notes	96
Features	96
Bug Fixes	97
Known Issues/Limitations	98
Answers to FAQs	98
2.0.6 Release Notes	98
Improvements	98
Bug Fixes	99
Known Issues/Limitations	99
3.0.0 Release Notes	99
Improvements	99
Bug Fixes	100
Known Issues	100
Issue	100
Issue	100

Table of Contents

The user does not have permissions to view the password in Secret Server because the View Launcher Password permission is not assigned to their Role.	100
The secret (under the Security tab) has Viewing Password Requires Edit enabled and the user does not have Edit permissions (or in the older UI, Hide Launcher Password is set to Yes)	100
The template used for the secret has Viewing Requires Edit enabled for the password field and the user does not have Edit permissions	101
3.0.1 Hot Fix Release Notes	101
Product Improvement	101
Bug Fix	101
3.1.0 Release Notes	101
Product Enhancements	101
Known Issues	102
Bug Fixes	102
3.2.0 Release Notes	102
Product Enhancements	102
Bug Fixes	103
Known Issues	103
Browser Related	103
3.3.0 Release Notes	103
Features	104
Bug Fixes	104
iOS Specific	104
3.4.0 Release Notes	104
Features	105
Product Enhancements	105
Bug Fixes	105
3.4.1 Release Notes	105
Bug Fixes	105
3.4.2 Release Notes	105
Features	105
General Maintenance	105
Bug Fixes	106
Known Issues	106
3.4.3 Release Notes	106
Features	106
Security Improvements	106
Bug Fixes	107
3.4.4 Release Notes	107
Bug Fixes	107
3.5.0 Release Notes	107
Features	107
Bug Fixes	107
Known Issues	107
3.5.1 Release Notes	107
Bug Fixes	108

Table of Contents

Known Issues	108
3.5.2 Release Notes	108
Features	108
Bug Fixes	108
Known Issues	108
3.5.3 Release Notes	108
Features	108
Bug Fixes	108
3.5.4 Release Notes	108
Improvements	109
Bug Fixes	109
3.6.0 Release Notes	109
Features	109
General Improvements	109
Security Improvements	109
Bug Fixes	109
Known Issues	110
3.6.1 Release Notes	110
Bug Fixes	110
Documentation Changelog	110
August 2023	110
July 2023	110
June 2023	110
May 2023	110
April 2023	110
March 2023	110
December 2022	111
September 2022	111
June 2022	111
February 2022	111
November 2021	111
October 2021	111
August 2021	111
July 2021	111
May 2021	111
March 2021	111
December 2020	112
October 2020	112
September 2020	112

Web Password Filler

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

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


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

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

Getting Started

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 the Delinea Platform and Secret Server.](#)

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


Enable Web Services in Secret Server

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

Connecting to the Delinea Platform and Secret Server

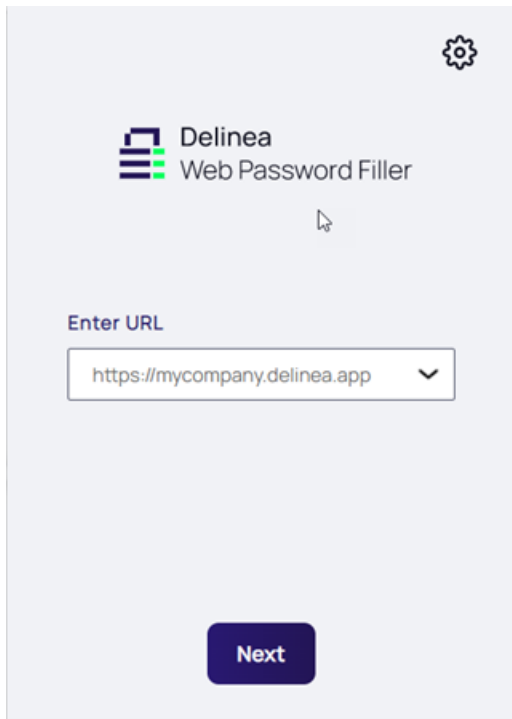
After installation, you must configure WPF to connect with the Delinea Platform or Secret Server vault of your choice by using the URL field in the WPF window.

Connecting to the Delinea Platform

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

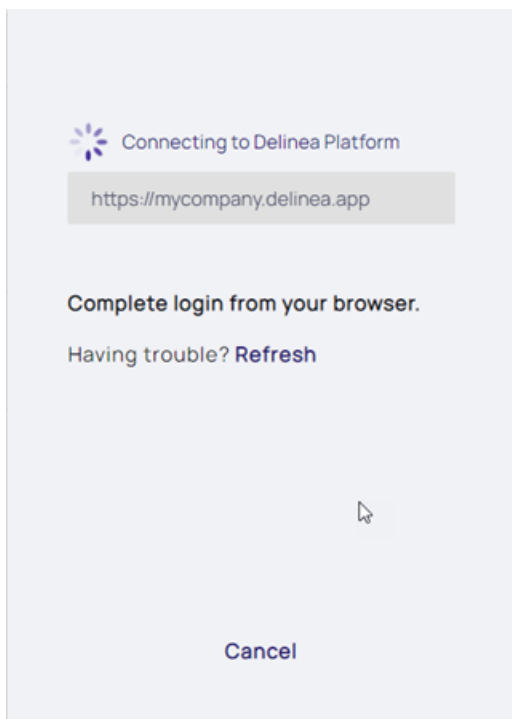
Getting Started

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



The screenshot shows the 'Delinea Web Password Filler' interface. At the top right is a gear icon. The Delinea logo and 'Web Password Filler' text are centered. Below is a text input field labeled 'Enter URL' containing the text 'https://mycompany.delinea.app'. A dark blue 'Next' button is positioned at the bottom center.

4. Proceed to your browser to complete login



The screenshot shows the 'Connecting to Delinea Platform' screen. It features a loading spinner icon and the text 'Connecting to Delinea Platform'. Below this is a grey box containing the URL 'https://mycompany.delinea.app'. The main instruction reads 'Complete login from your browser.' followed by 'Having trouble? Refresh'. A 'Cancel' button is located at the bottom center.

Getting Started

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

Delinea
Defining the Boundaries of Access

Log in

Username

Next

Delinea
©2023 Delinea [Terms & Conditions](#) [Privacy Policy](#)

Getting Started

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

Delinea
Defining the Boundaries of Access

Log in

artdecco@mycompany

Authentication method [Forgot password](#)

Password

Password

Keep me logged in

Next

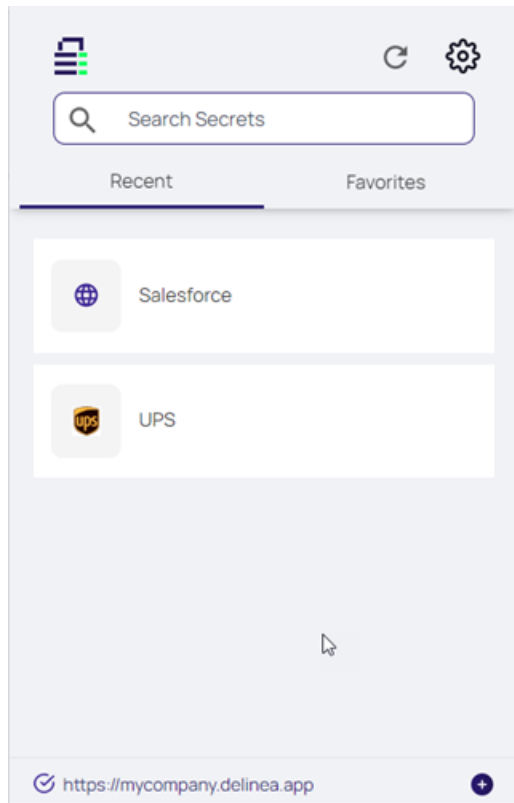
[Start over](#)

Delinea

©2023 Delinea [Terms & Conditions](#) [Privacy Policy](#)

Getting Started


7. You are now logged in

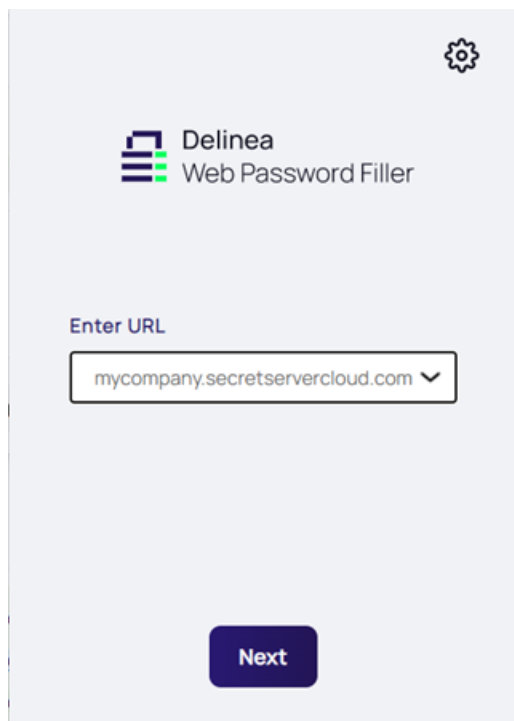


Connect to Secret Server

To connect WPF with Secret Server:

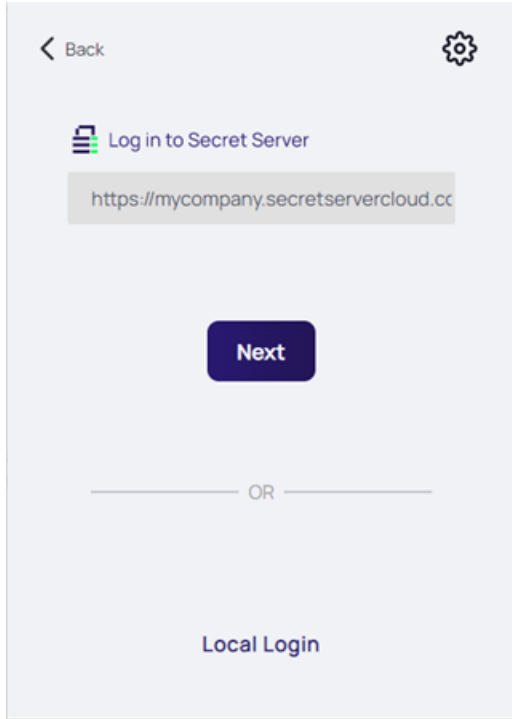
Getting Started

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



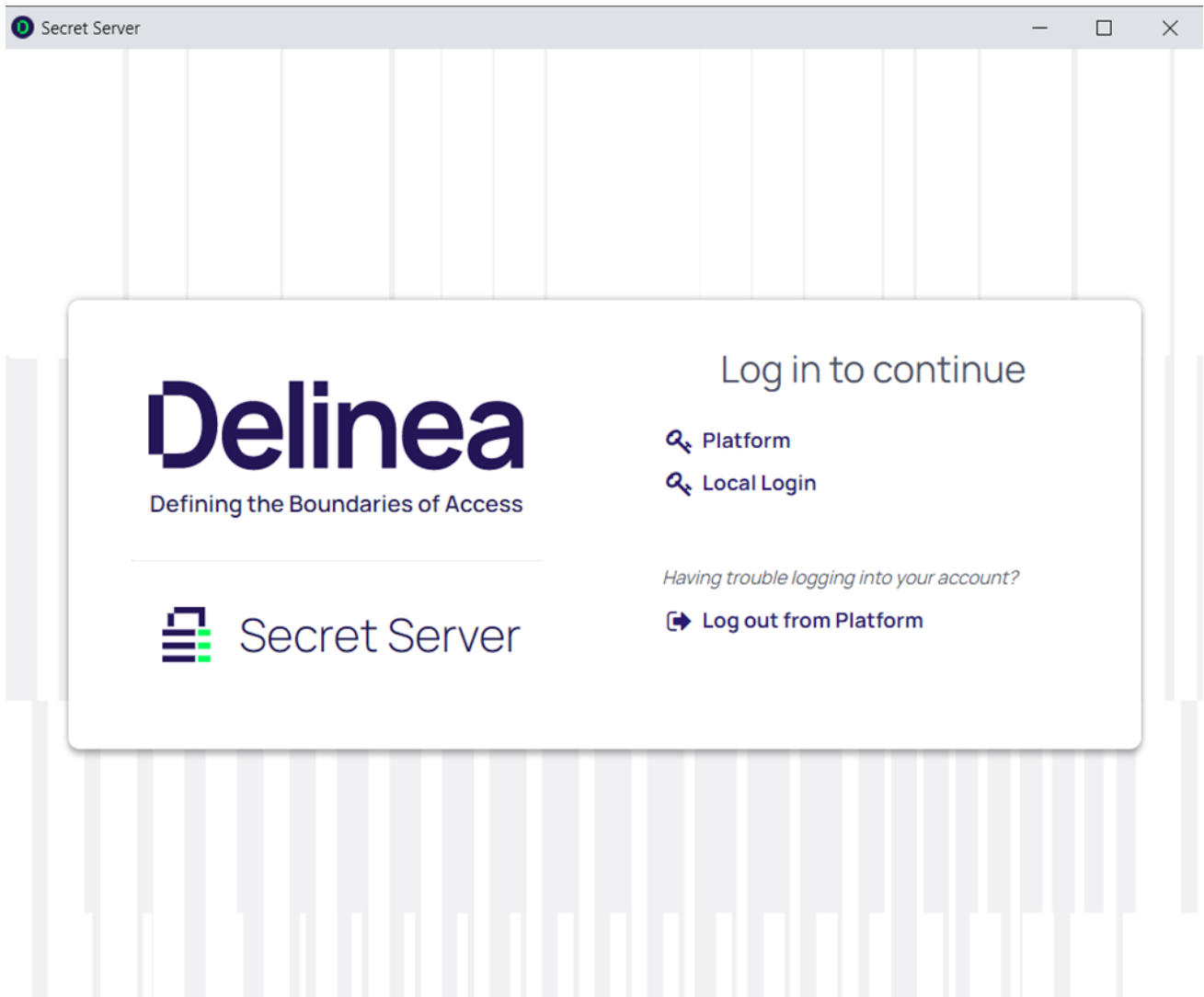
3. Enter your Secret server URL For example: `https://mycompany.secretservercloud.com` and click **Next**
4. You can sign in with any of your configured login methods. To use the web login, click **Next**

Getting Started

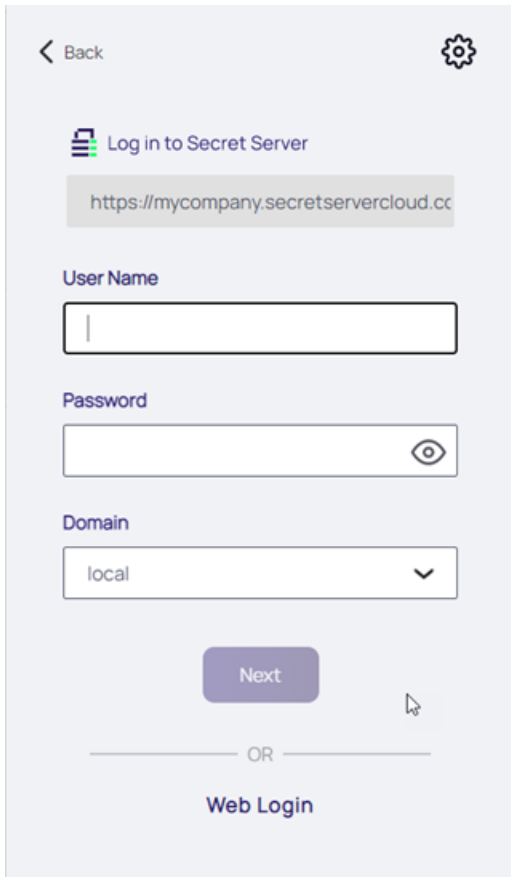


Getting Started

5. Proceed to browser to complete login



Local Login



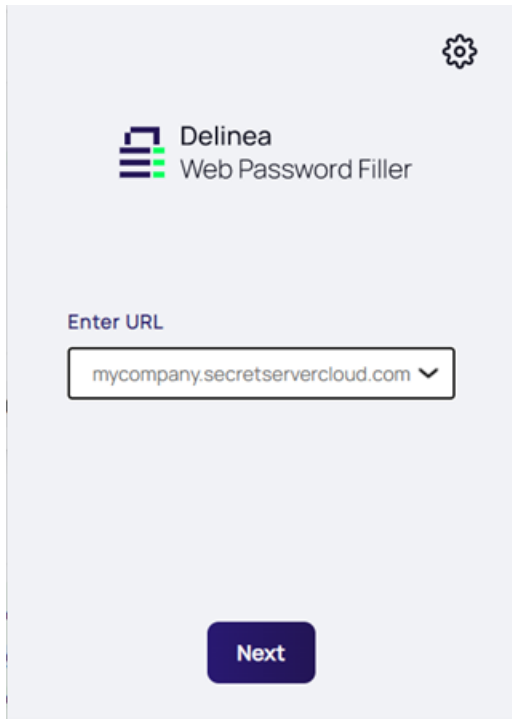
The screenshot shows a mobile application interface for logging into a Secret Server. At the top left is a back arrow and the text "Back". At the top right is a gear icon for settings. Below this is a header "Log in to Secret Server" with a server icon. A text field contains the URL "https://mycompany.secretservercloud.cc".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

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

Default Protocols

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

Getting Started



The screenshot displays the Delinea Web Password Filler interface. At the top right, there is a gear icon for settings. The Delinea logo and the text 'Delinea Web Password Filler' are centered. Below this, the text 'Enter URL' is positioned above a text input field. The input field contains the URL 'mycompany.secretservercloud.com' and a dropdown arrow. At the bottom center, there is a dark blue button labeled 'Next'.

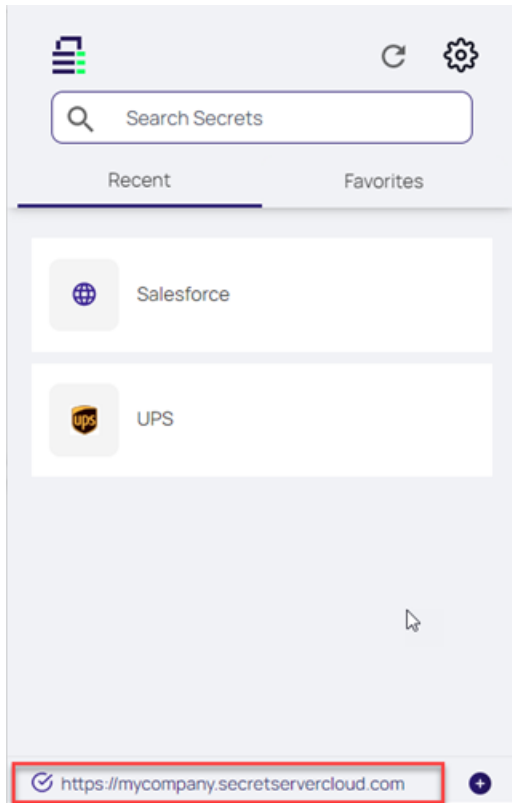
If you click **Next**, Web Password Filler assumes *https://* is the correct protocol and proceeds as if you had prefixed *https://* in the very beginning.

 **Note:** If you specify a protocol, Web Password Filler will use that protocol.

Redirecting to Secret Server via Hyperlink

When connected to the Delinea Platform or Secret Server vault, Web Password Filler will show the URL at the bottom. Clicking on this link will take you to the Platform or Secret Server vault site.

Getting Started



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.

Secret Server Web Password Filler


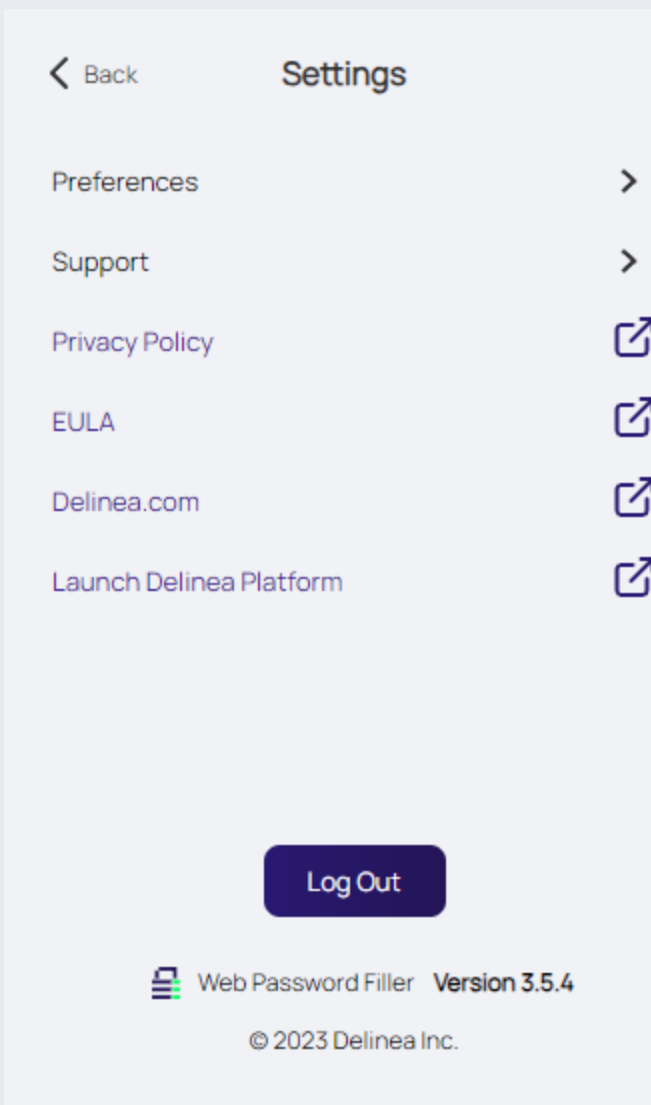
This is the new Web Password Filler browser extension that was released with Secret Server version 10.7.59 and later. Typically, this will be referred to as:

- WPF
- Web Password Filler
- Password Filler

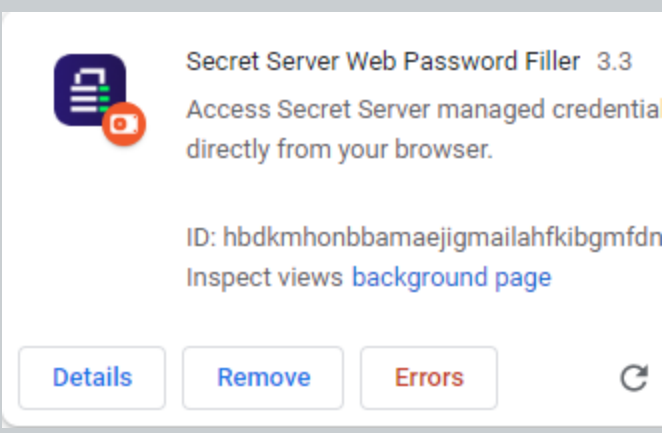
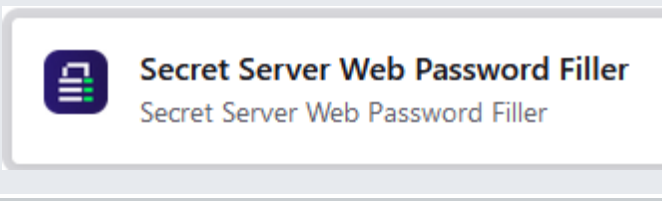
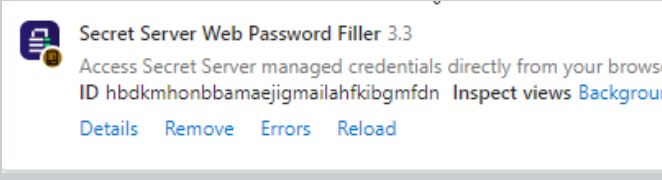
When looking in a browser this is represented by the following:

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

Getting Started

State	Location/Browser	Example
Logged In	(In top right corner)	
Application in Browser (Settings Menu)		

Getting Started


State	Location/Browser	Example
Item on Extensions / Add-On page	Chrome	 <p>Secret Server Web Password Filler 3.3 Access Secret Server managed credentials directly from your browser.</p> <p>ID: hbdkmhonbbamaejigmailahfkibgmfdn Inspect views background page</p> <p>Details Remove Errors</p>
	Firefox	 <p>Secret Server Web Password Filler Secret Server Web Password Filler</p>
	Edge (chromium version)	 <p>Secret Server Web Password Filler 3.3 Access Secret Server managed credentials directly from your browser. ID hbdkmhonbbamaejigmailahfkibgmfdn Inspect views Background</p> <p>Details Remove Errors Reload</p>

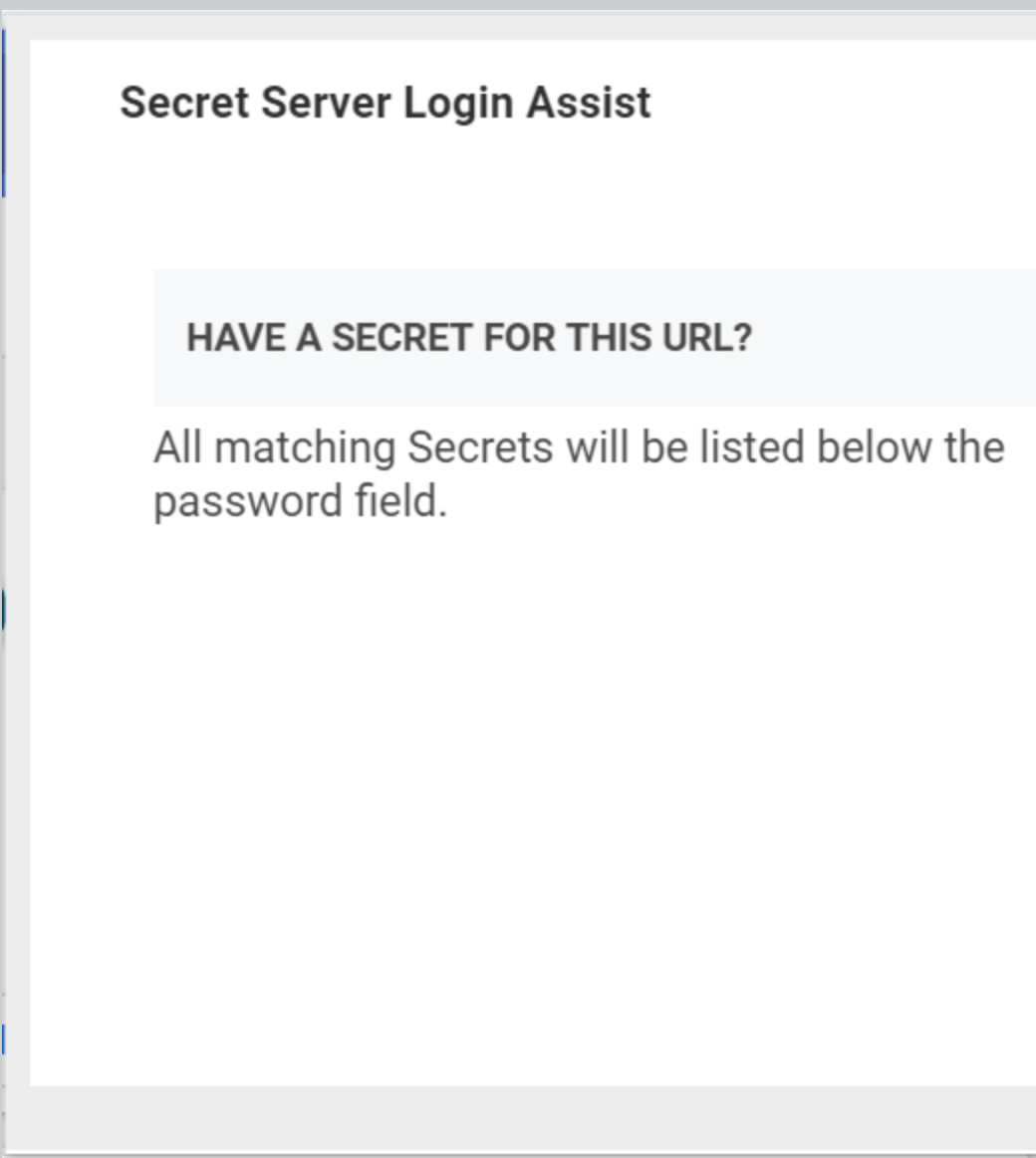
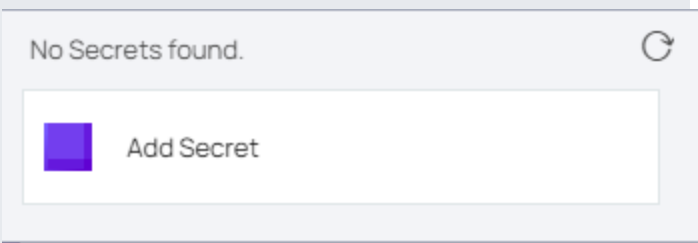
Secret Server Login Assist

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

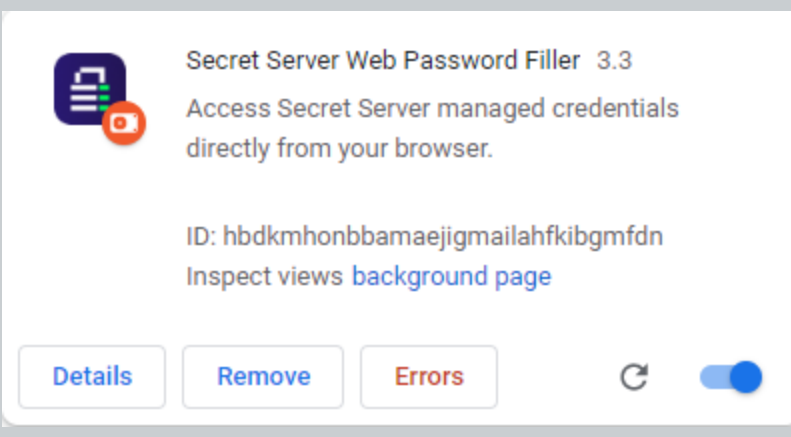
- WPF (Term No longer used in relation to this extension)
- Web Password Filler (Term No longer used in relation to this extension)
- Login Assist (Still used)

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

Location	Example
Logo in top right corner	

Location	Example
Application in Browser	
Drop down option on field	

Getting Started

Location	Example
Item on Extensions / Add-On page	



Secret Server Clipboard Utility

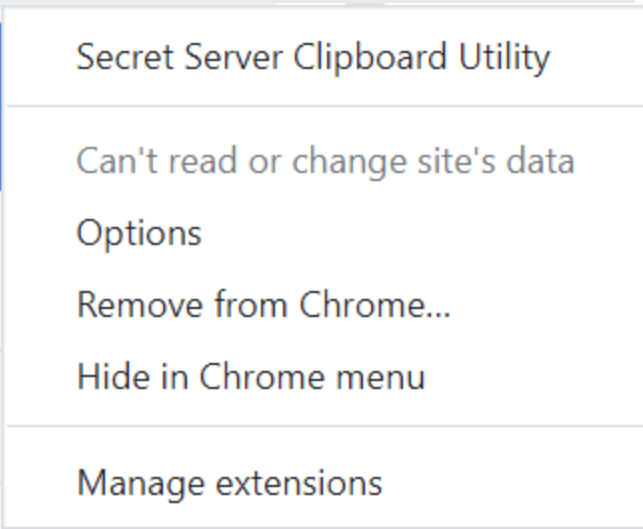
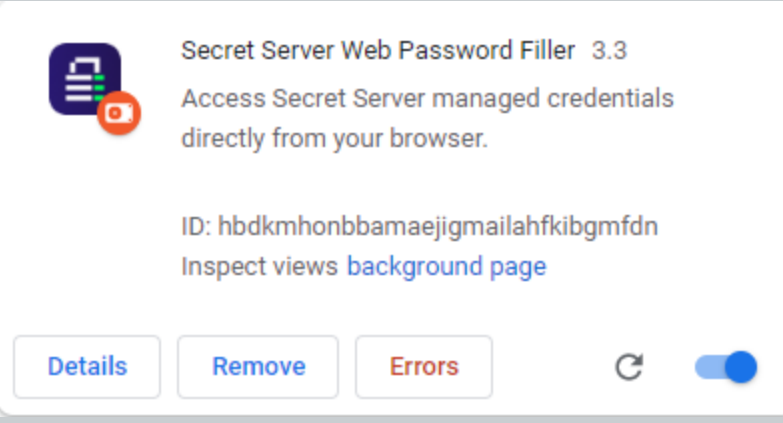


This is the Clipboard Utility that was available with previous versions of Secret Server. The options and functionality of this extension have NOT be added into the NEW Web Password Filler (as of Feb 28, 2020).

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:

Location	Example
Logo in top right corner	
or	

Location	Example
Application in Browser	 <p>Secret Server Clipboard Utility</p> <hr/> <p>Can't read or change site's data</p> <p>Options</p> <p>Remove from Chrome...</p> <p>Hide in Chrome menu</p> <hr/> <p>Manage extensions</p>
Item on Extensions / Add-On page	 <p> Secret Server Web Password Filler 3.3</p> <p>Access Secret Server managed credentials directly from your browser.</p> <p>ID: hbdkmhonbbamaejigmailahfkibgmfdn</p> <p>Inspect views background page</p> <p>Details Remove Errors  <input checked="" type="checkbox"/></p>

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:

Getting Started

- WPF supports Safari running on macOS Monterey and Big Sur 11.1.0, 11.2.1 and later.
- WPF does not support the Native Messaging Host configuration in Safari browsers.
- The Safari browser extension does not support Windows Admin Center.
- Session recording is not supported on Safari 15 and above

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.

Installing the Native Messaging Host

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

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

Getting Started

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.

Configuration Options

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

Getting Started

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
  IDs
  {
    "chromeExtensionId": "mfpddejbpbjnkjoaicfedaljnfeo11kh",
    "edgeExtensionId": "kjldmpkefedgljefehmmfifbhngmbh",
    "operaExtensionId": "eemnadjdifcpkcpalolohpepihbbo",
    "firefoxExtensionId": "dd1e31d5-3623-45cb-b1ad-64074d36b360@thycotic.com",
  }
  Default
  Settings
  {
    "ConfigSSUrl": "https://SomeURL/SecretServer",
    "ConfigDomain": "",
    "HideConfigPage": false,
    "HideSettingPage": false,
    "SettingUserSSLogin": true,
    "SettingPromptToSave": true,
    "SettingShowPopup": true,
    "SettingHideReadOnlyFolders": true,
    "SettingEnableAutoPopulate": true,
    "EnableForAllUsers": false,
    "PopupDefaultPosition": true,
    "ExactMatchUrl": false,
    "maxSessionRecordingLimit": 120,
    "Exclude": [ "http://*" ],
    "ExcludeException": [],
    "PerExtensionOverride": [
      {
        "id": "mfpddejbpbjnkjoaicfedaljnfeo11kh",
        "ConfigSSUrl": "https://SomeURL/SecretServer",
        "ConfigDomain": "",
        "HideConfigPage": true,
        "HideSettingPage": false,
        "SettingUserSSLogin": true,
        "SettingPromptToSave": true,
        "SettingShowPopup": true,
        "SettingHideReadOnlyFolders": true,
        "SettingEnableAutoPopulate": true,
        "EnableForAllUsers": false,
        "PopupDefaultPosition": false,
        "ExactMatchUrl": true,
        "maxSessionRecordingLimit": 120,
        "Exclude": [
          "http://*",
          "http://endoftheinternet.com",
          "https://www.MyCompanySite.com",
          "https://live.com/"
        ],
        "ExcludeException": [
          "https:// MyCompanySite.com/Login.html",
          "https://login.live.com/login.srf"
        ]
      }
    ]
  }
},
```

Settings.json Format

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

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

```
{
  "chromeExtensionId": "mfpddejbpbjnkjoaicfedaljnfeo11kh",
```

Getting Started

```
"edgeExtensionId": "kjldmpkefedgljefehmmfifbhnjngmbh",
"operaExtensionId": "eemnadjdifcpkcnpalolohpepihhbbo",
"firefoxExtensionId": "dd1e31d5-3623-45cb-b1ad-64074d36b360@thycotic.com",
"ConfigSSUrl": "https://SomeURL/SecretServer",
"ConfigDomain": "local",
"HideConfigPage": false,
"HideSettingPage": false,
"SettingUserSSLogin": true,
"SettingPromptToSave": true,
"SettingShowPopup": true,
"SettingHideReadOnlyFolders": true,
"SettingEnableAutoPopulate": true,
"EnableForAllUsers": false,
"PopupDefaultPosition": true,
"ExactMatchUrl": false,
"maxSessionRecordingLimit": 120,
"Exclude": [ "http://*" ],
"ExcludeException": [],
"PerExtensionOverride": [
  {
    "id": "mfpddejbpbjkbjkaicfedaljnfeollkh",
    "ConfigSSUrl": "https://SomeURL/SecretServer",
    "ConfigDomain": "",
    "HideConfigPage": true,
    "HideSettingPage": false,
    "SettingUserSSLogin": true,
    "SettingPromptToSave": true,
    "SettingShowPopup": true,
    "SettingHideReadOnlyFolders": true,
    "SettingEnableAutoPopulate": true,
    "EnableForAllUsers": false,
    "PopupDefaultPosition": false,
    "ExactMatchUrl": true,
    "maxSessionRecordingLimit": 120,
    "Exclude": [
      "http://*",
      "http://endoftheinternet.com",
      "https://www.MyCompanySite.com",
      "https://live.com/"
    ],
    "ExcludeException": [
      "https:// MyCompanySite.com/Login.html",
      "https://login.live.com/login.srf"
    ]
  },
  {
    "id": "kjldmpkefedgljefehmmfifbhnjngmbh",
    "ConfigSSUrl": "https://localhost/SecretServer/",
    "ConfigDomain": "",
    "HideConfigPage": false,
    "HideSettingPage": false,
    "SettingUserSSLogin": false,
    "SettingPromptToSave": false,
    "SettingShowPopup": false,
```

Getting Started

```
    "SettingHideReadOnlyFolders": false,
    "SettingEnableAutoPopulate": false,
    "PopupDefaultPosition": false,
    "ExactMatchUrl": false,
    "maxSessionRecordingLimit": 120,
    "Exclude": [ "http://*" ],
    "ExcludeException": []
  },
  {
    "id": "dd1e31d5-3623-45cb-b1ad-64074d36b360@thycotic.com",
    "HideConfigPage": false
  },
  {
    "id": "eemnadjdifcpcnpalolohpepihhbbo"
  }
]
}
```

Where:

Parameter	Default	Description
chromeExtensionID	"mfpddebpbnpjjoaicfedaljnfeollkh"	This is the ID required for the Chrome browser registration.
edgeExtensionId	"kjldmpkefedgljefehmmfifbhjnngmbh"	This is the ID required for the Edge browser registration.
operaExtensionId	"eemnadjdifcpcnpalolohpepihhbbo"	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.

Getting Started

Parameter	Default	Description
SettingUserSSLogin	true	Boolean that sets the checkbox to enable the Secret Server Login option.
SettingPromptToSave	true	Boolean that sets the checkbox to enable the Prompt to Save option.
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	
ExactMatchUrl	false	
maxSessionRecordingLimit	120	

Getting Started

Parameter	Default	Description
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.).	

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.

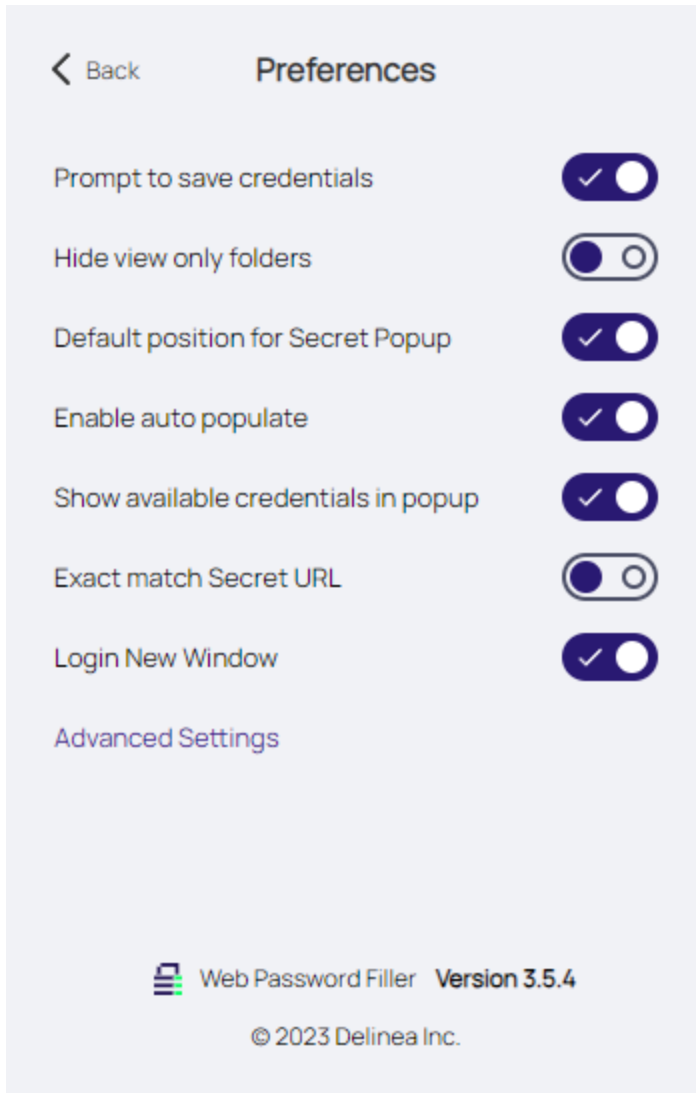
To exclude all sites, a wild card can be used (`https://*` and/or `http://*`) and then simply add the sites where secrets are available (<https://MyCompanySite.com/login.aspx>) to the exclusion exception list.

Note: Only the “Exclude” section accepts a wild card. The “ExcludeException” must be the exact URL without a query string.

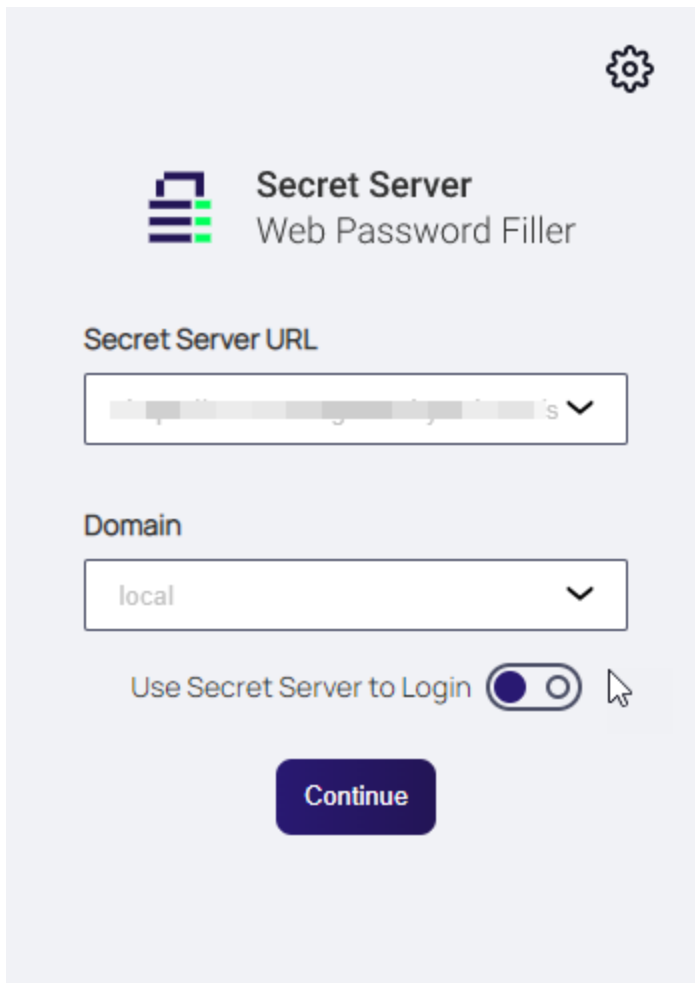
UI Behavior Based on Preferences

Each preference on the Preferences page can be set using “true” or “false” in the *settings.json*.

Getting Started



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



Secret Server
Web Password Filler

Secret Server URL

Domain

Use Secret Server to Login

Continue

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

Getting Started

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 the ThycoticMessagingHost.exe was executed without the required command line option.

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

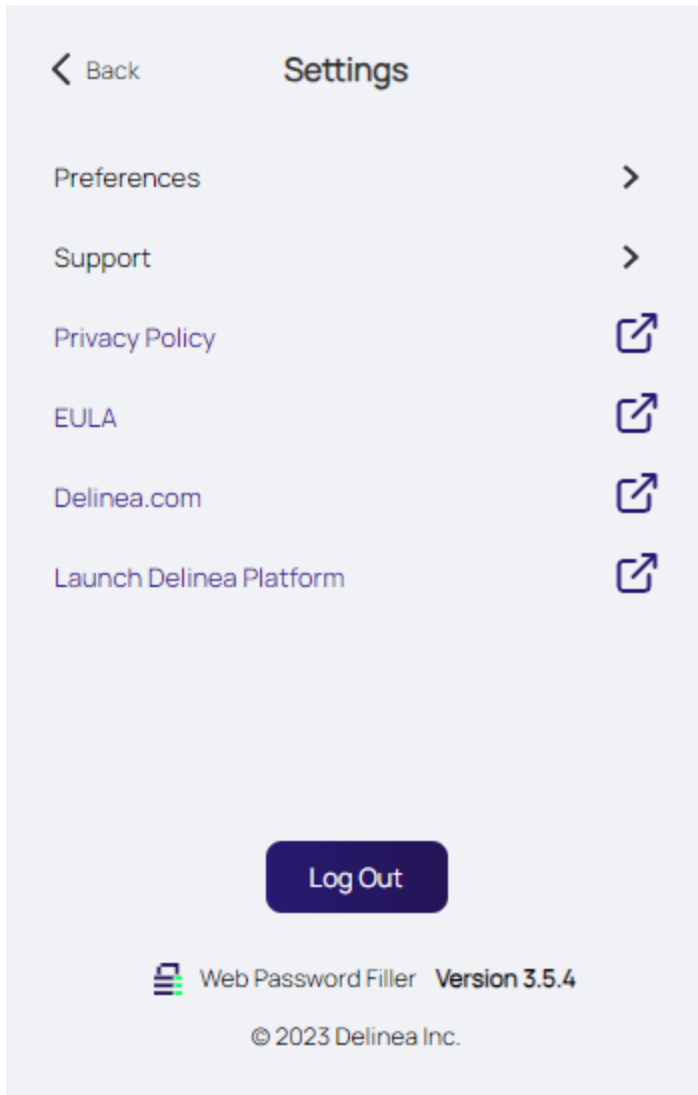
- The following message indicates that only --register and --unregister are valid command line options.

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

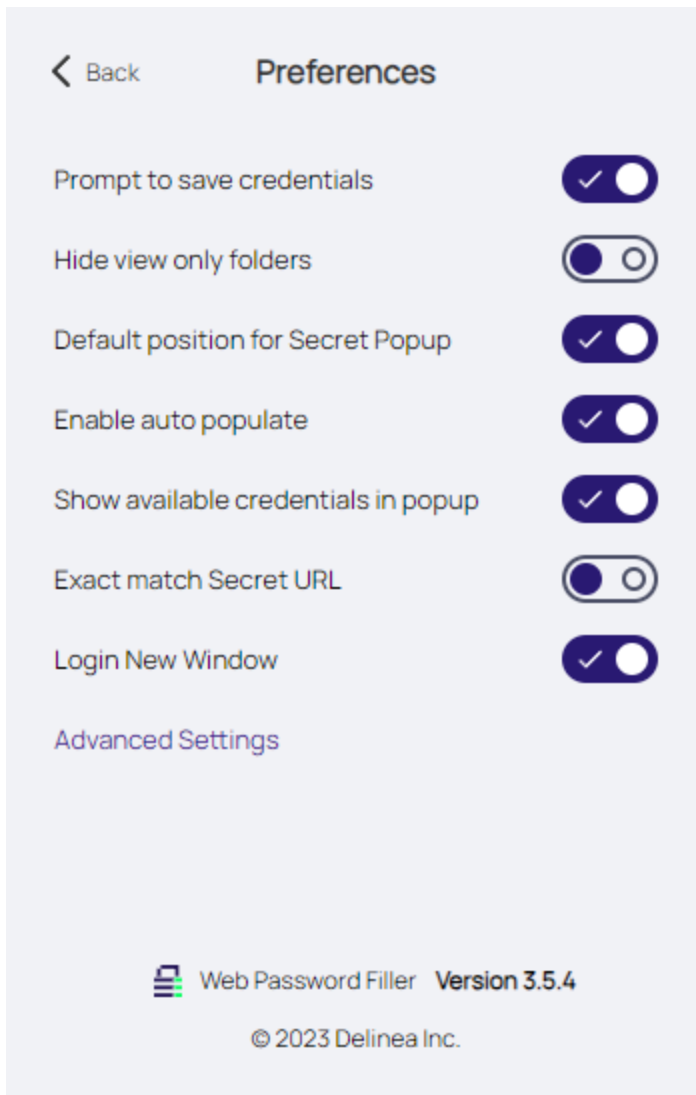
Preferences Menu

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

Getting Started



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



- **Prompt to save credentials:** Select this preference if you want WPF to prompt you to save your login credentials for future logins. Not recommended for shared systems. The prompt only appears if an existing secret is updated, or if a user enters credentials for a site and no Secret was used.
- **Hide view only folders:** Select this preference to prevent users from seeing folders to which they have read access only.
- **Show available credentials in popup:** Select this preference to have available credentials will be displayed in a pop-up dialog.
- **Default position for Secret Popup:** Select this preference to have the Secret popup appear at the top right of the screen. The non-default position is under the Delinea check symbol.
- **Enable auto populate:** Select this preference so that when a Secret is available for a web page, WPF will automatically populate the fields on the page.

Using WPF

- **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.

Using WPF

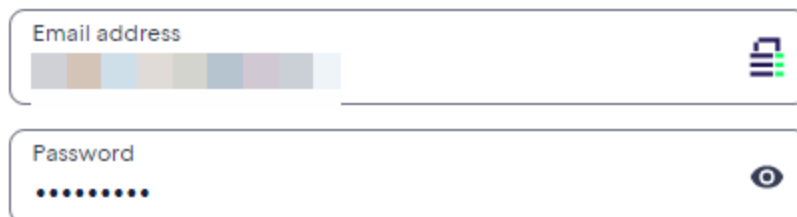
Once WPF is set up and you are logged into the Delinea Platform or Secret Server, you can use WPF to log in to websites for which Secrets are managed via the Delinea Platform or Secret Server.

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

Log in to a Website

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

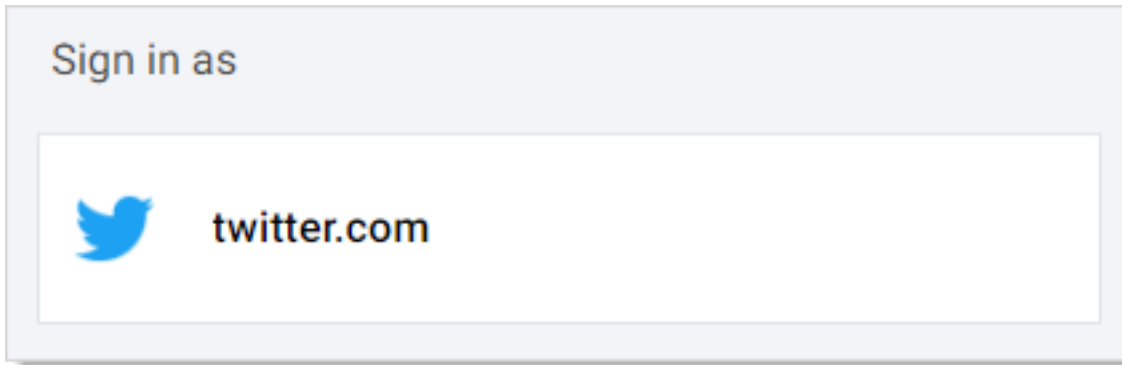
Sign in



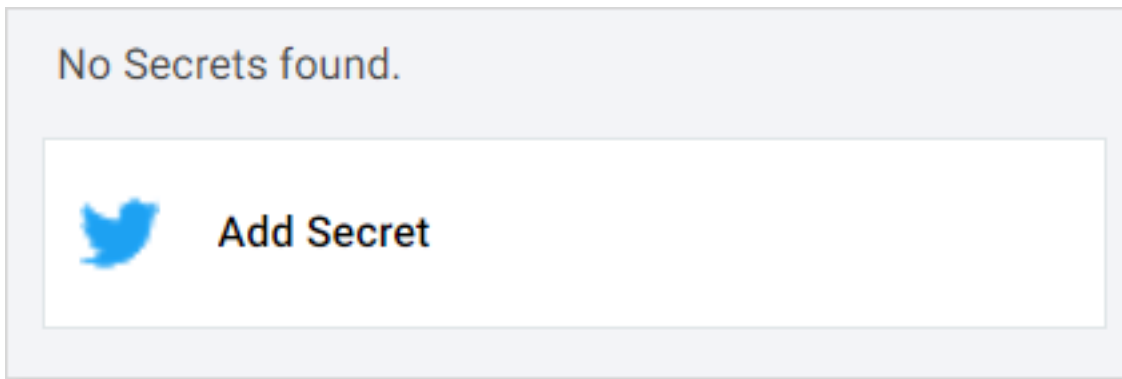
The image shows a sign-in form with two input fields. The top field is labeled "Email address" and contains a blurred placeholder. To the right of the field is a purple and green lock icon. The bottom field is labeled "Password" and contains a blurred placeholder. To the right of the field is an eye icon.

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:



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



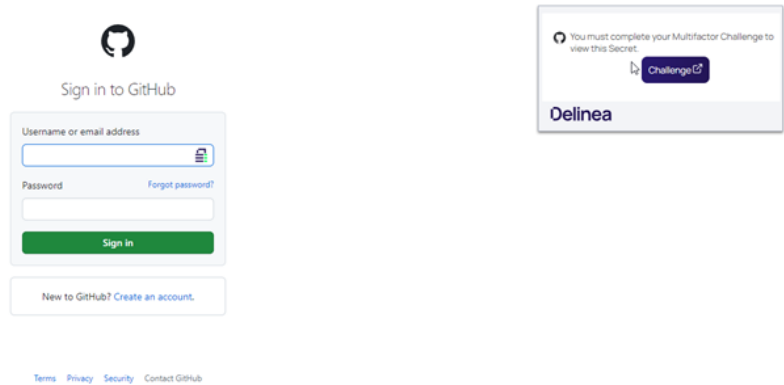
If you see the second possibility, you need to set up a secret for that website. See [Creating a Secret for a Website](#).

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

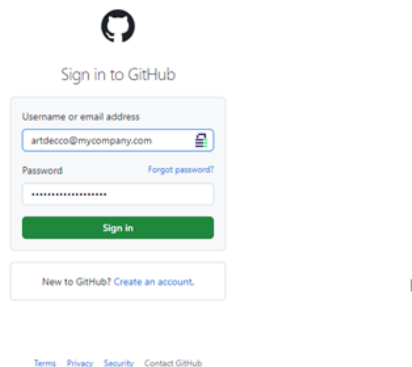
Accessing Secrets Guarded by MFA

Delinea Platform users can access secrets guarded by MFA through Web Password Filler. When a user attempts to login to a portal guarded by MFA, they will see a popup that they must complete and additional MFA challenge:

Using WPF



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



Session Recording

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.

Using WPF

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.



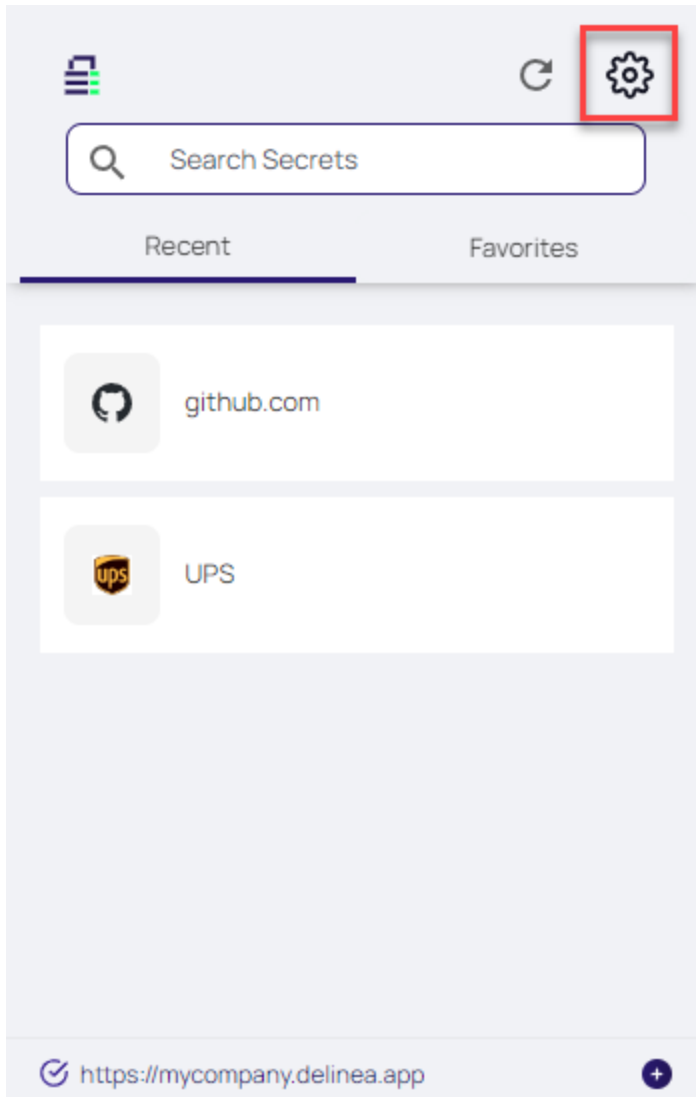
Note: Chrome versions 92 and newer throttle the number of screenshots per second and could impact the recording, including jumpy video or missed keystroke captures.

Enabling Mouse Path Tracking On Recordings

Users who wish to track mouse paths on session recordings can enable this feature by following these steps:

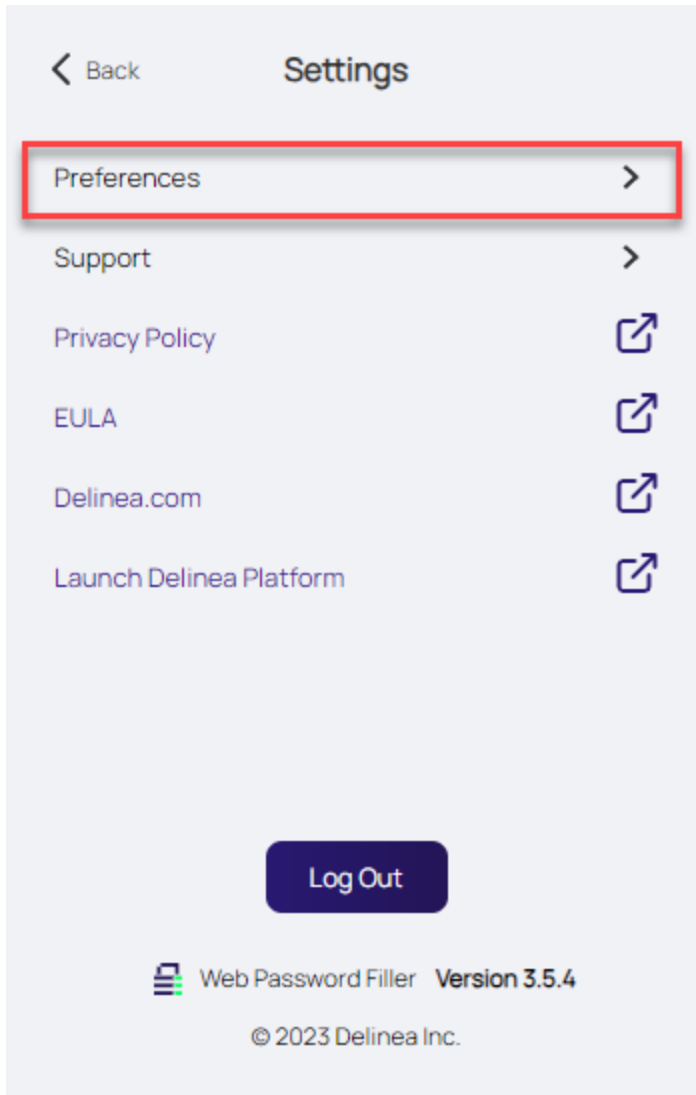
1. Click the **Settings** icon

Using WPF



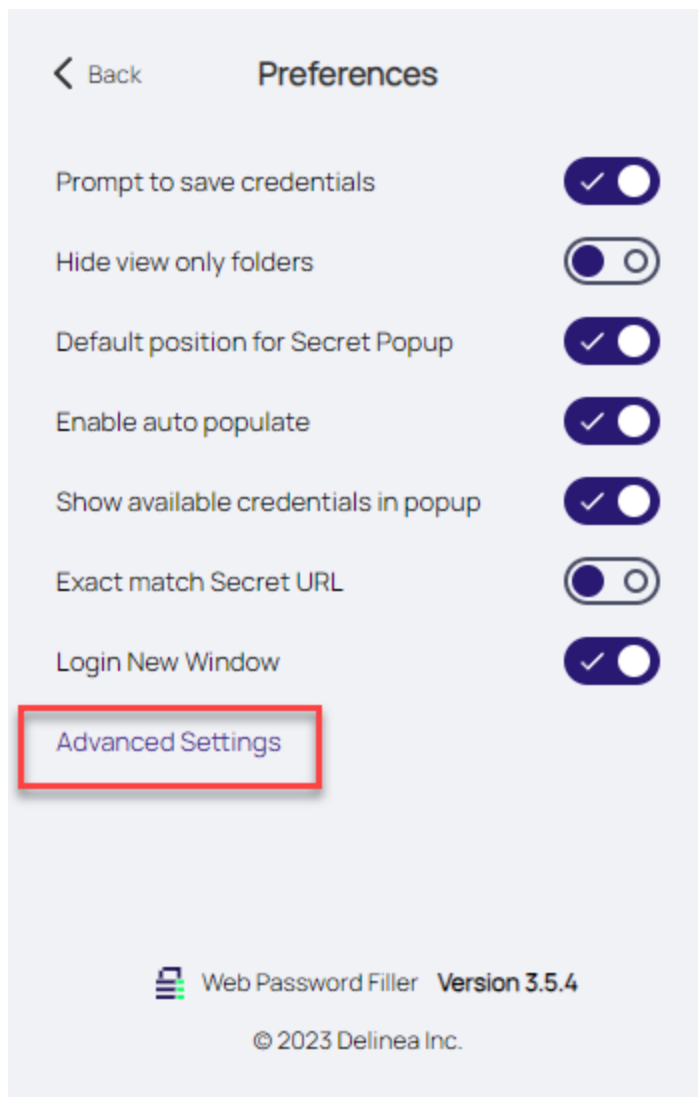
2. Click **Preferences**

Using WPF

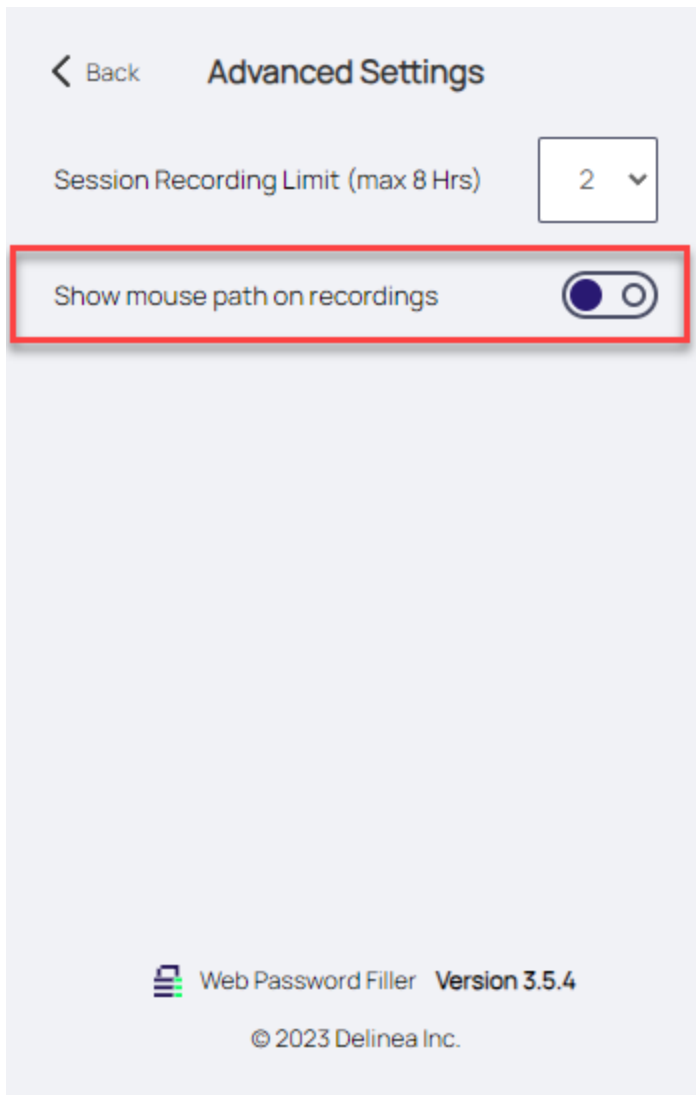


3. Click **Advanced Settings**

Using WPF



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



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.

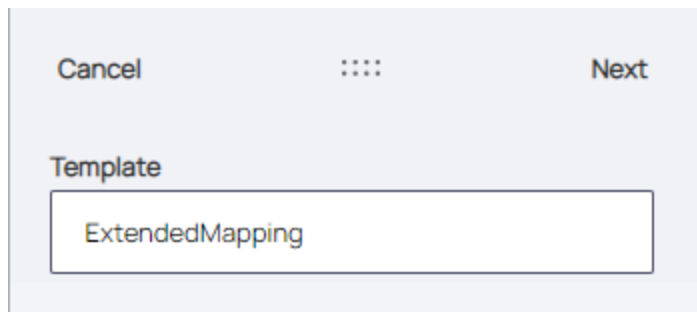
Using WPF

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.

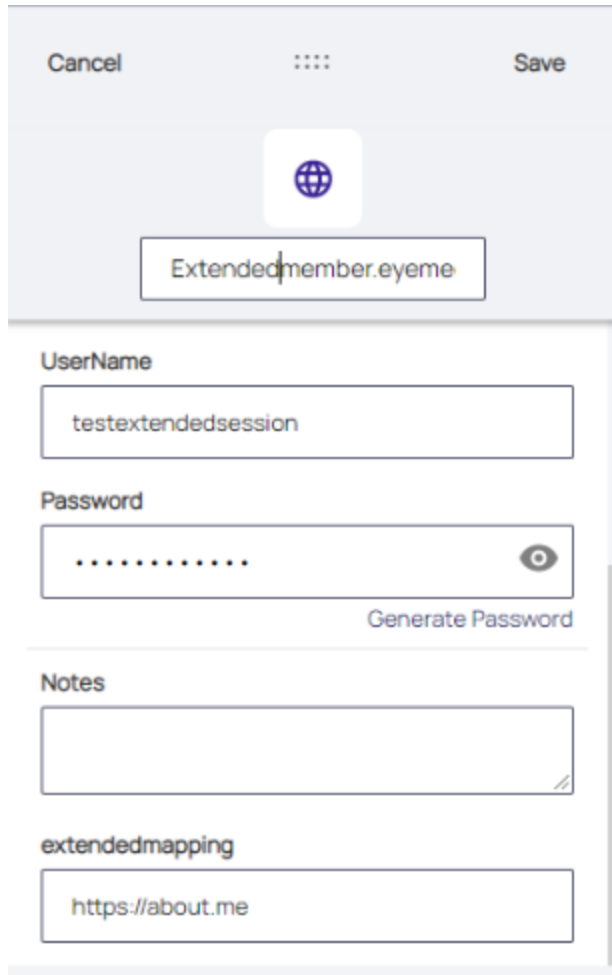
Using RegEx in WPF

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.

Using WPF



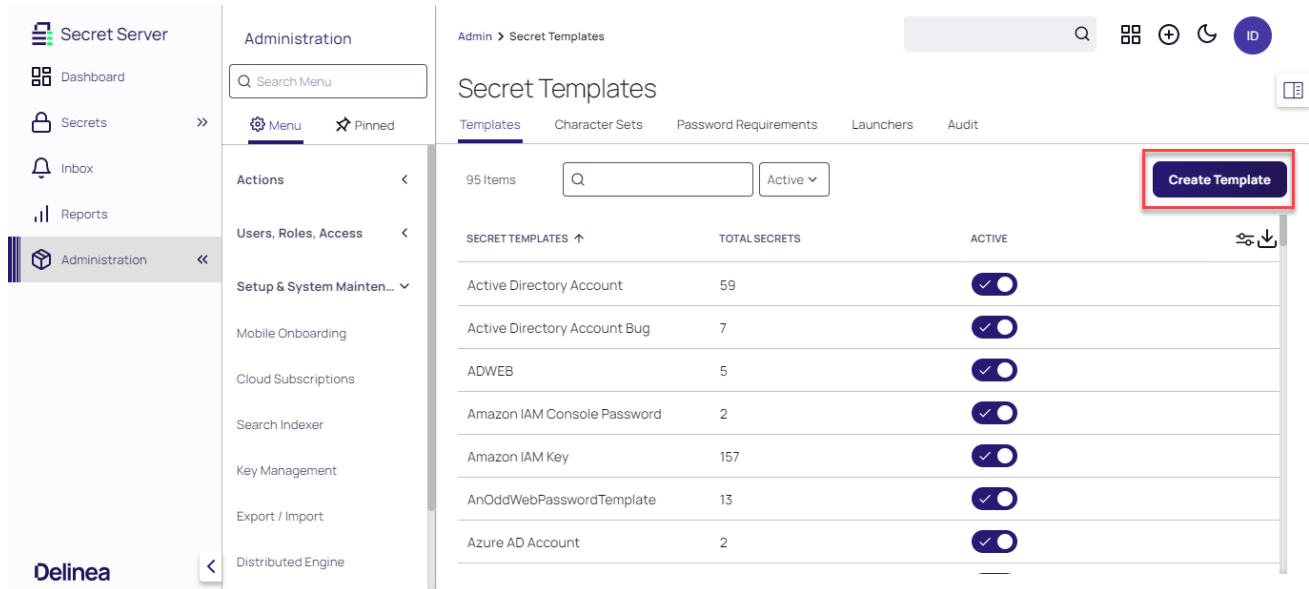
The screenshot shows a configuration window for WPF. At the top, there are buttons for 'Cancel', a menu icon (three dots), and 'Save'. Below this is a header area with a globe icon and a text field containing 'Extendedmember.eyeme'. The main content area has several sections: 'UserName' with a text field containing 'testextendedsession'; 'Password' with a masked text field (dots) and a 'Generate Password' button; 'Notes' with an empty text area; and 'extendedmapping' with a text field containing 'https://about.me'.

In the field **Extended Mapping**, enter any other URL for which session recording should be enabled, in the event that the user is redirected to those URLs.

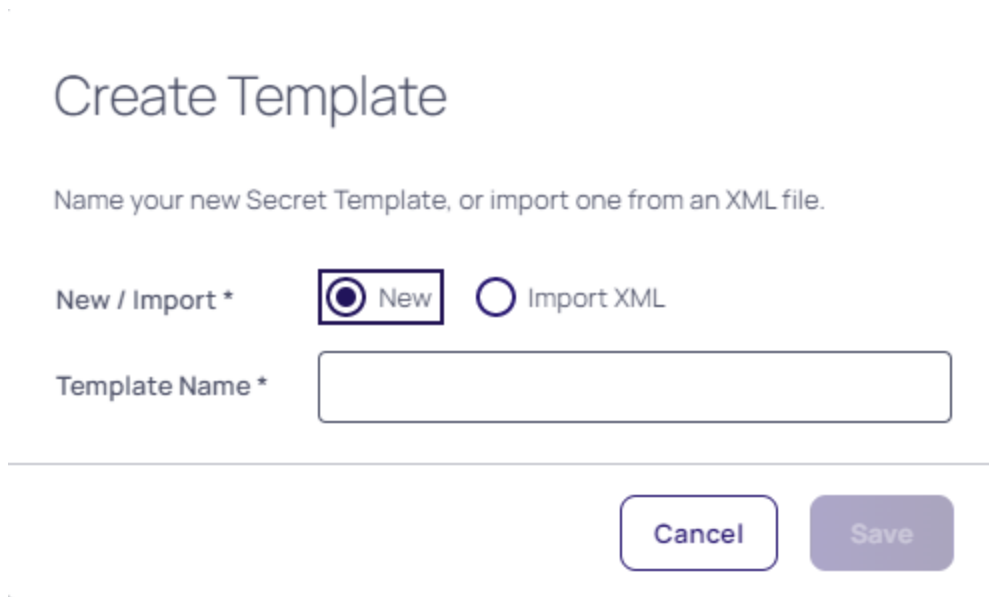
4. Click **Save**.

Setup in Secret Server

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



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



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

Using WPF

The screenshot shows the Secret Server Administration console. On the left is a navigation sidebar with 'Administration' selected. The main content area is titled 'ExtendedMappingConfig' and has tabs for 'General', 'Fields', 'Mapping', 'Permissions', and 'Audit'. The 'Mapping' tab is highlighted with a red box. Below the tabs, there are buttons for 'Export', 'Duplicate', 'Scan Templates', and 'Add Mapping'. The 'Add Mapping' button is highlighted with a red box. The main content area displays the 'Password Changing' section with a description and a table of settings.

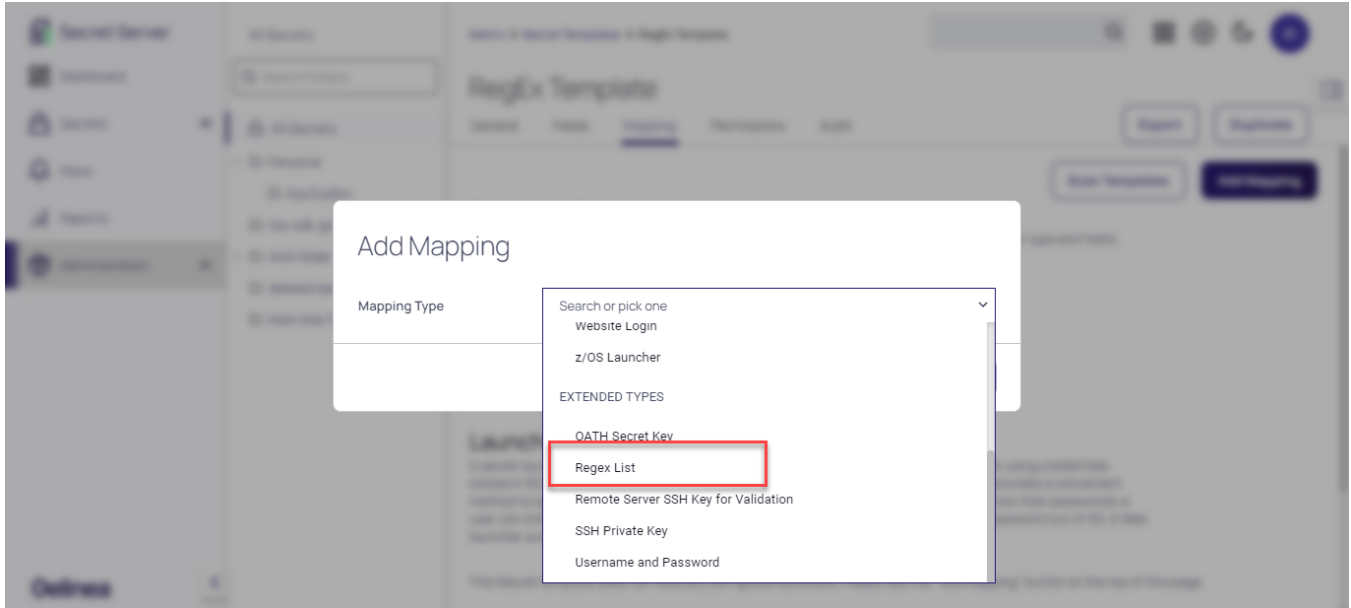
Setting	Value
Enable RPC	Yes
RPC Max Attempts	500
RPC Interval	0 days 0 hours 15 minutes
Enable Heartbeat	Yes
Heartbeat Interval	0 days 8 hours 0 minutes
Password Type to use	Web User Account

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

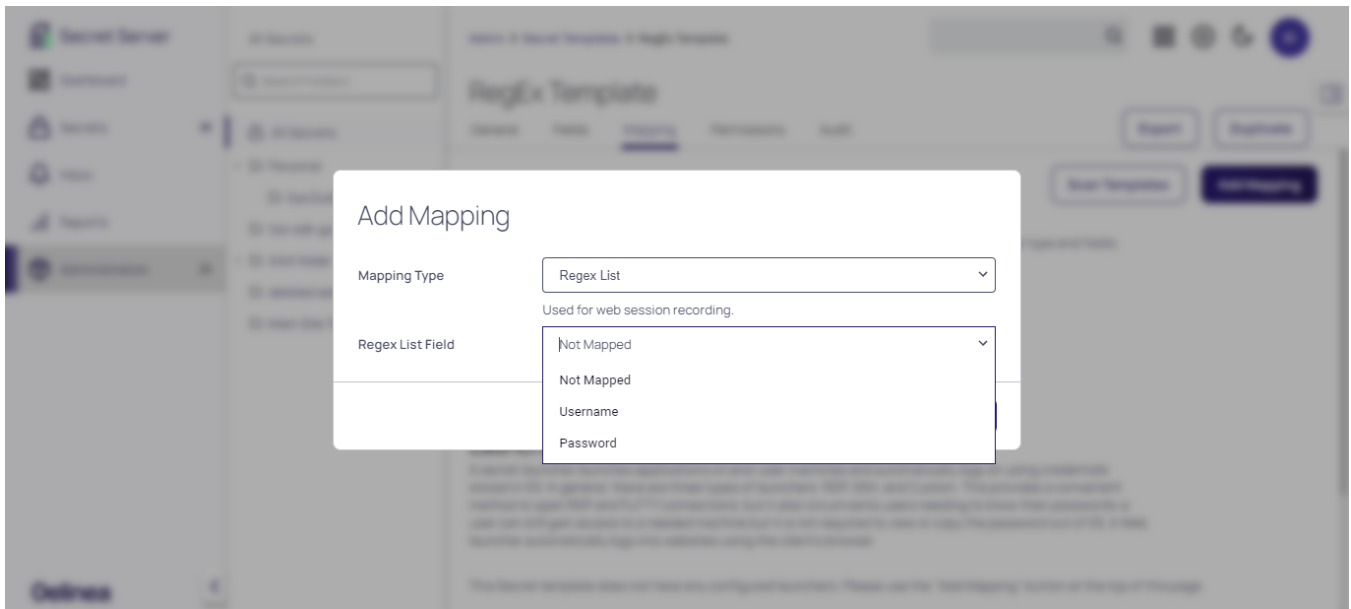
This screenshot is identical to the previous one, showing the 'ExtendedMappingConfig' page with the 'Mapping' tab selected. The 'Add Mapping' button is highlighted with a red box.

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

Using WPF



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.

Using WPF

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.

Resolutions

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

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

Using WPF

Display Resolution	Display Scaling in %	Does WPF support Session Recording on Browser		
	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

Using WPF

Display Resolution	Display Scaling in %	Does WPF support Session Recording on Browser		
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

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

Launching Comma-Separated URLs

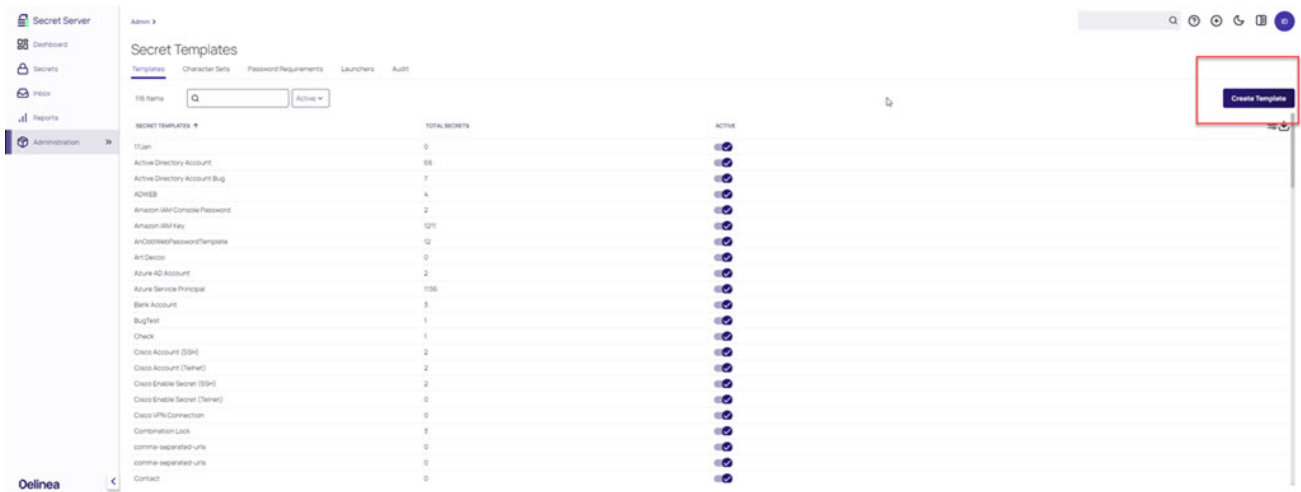
In the event that a secret has multiple URLs saved under the URL field, those URLs will appear in a dropdown list of all the saved URLs on a new row. Users also have the ability to select and launch the desired URL with a click of a button through the custom web launcher.

Create a Secret Template

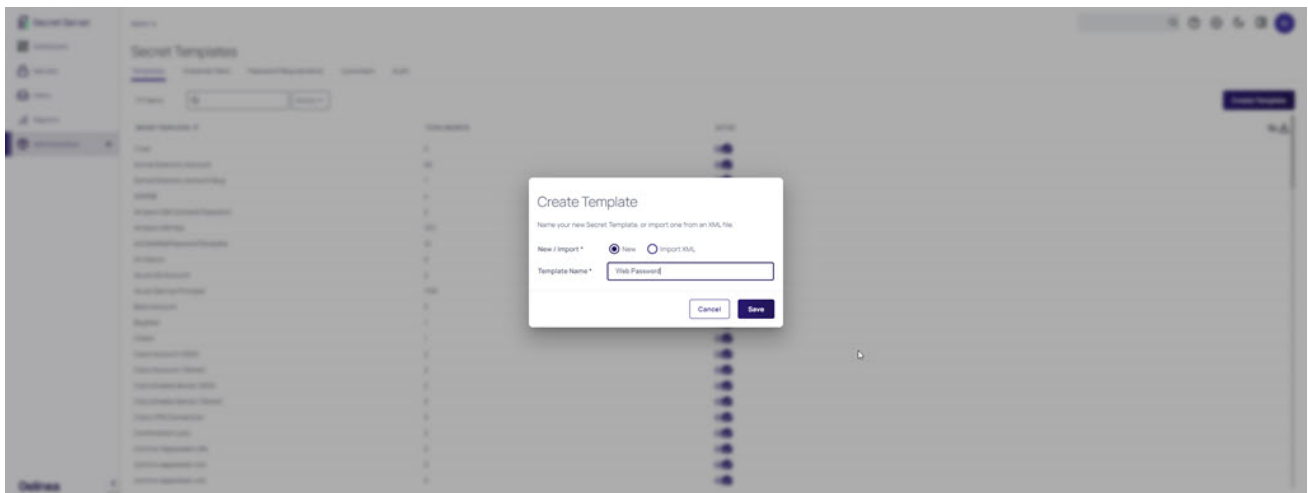
To use the custom web launcher, users will first need to create a secret template:

Using WPF

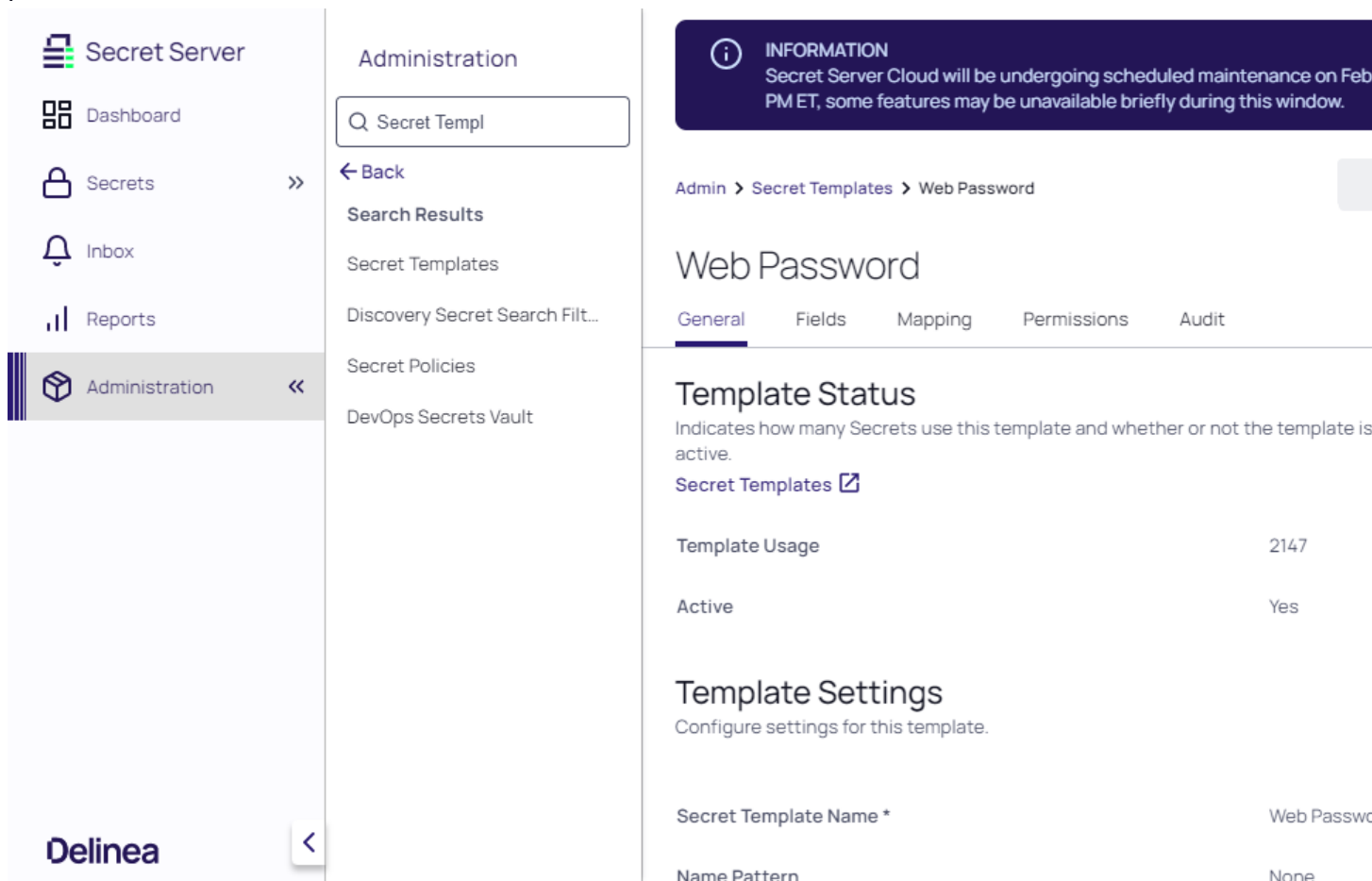
1. In the *Secret Templates* tab inside Secret Server, click **Create Template**.



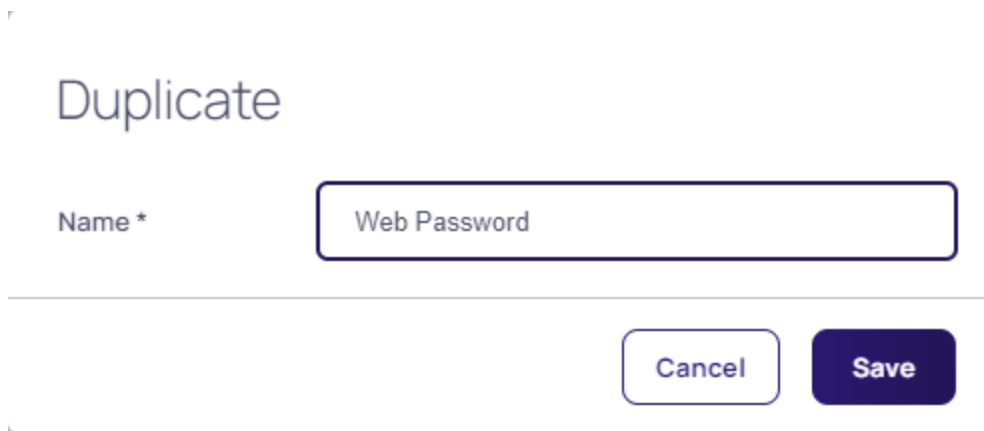
2. Give the new template a name and click **Save**



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



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




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

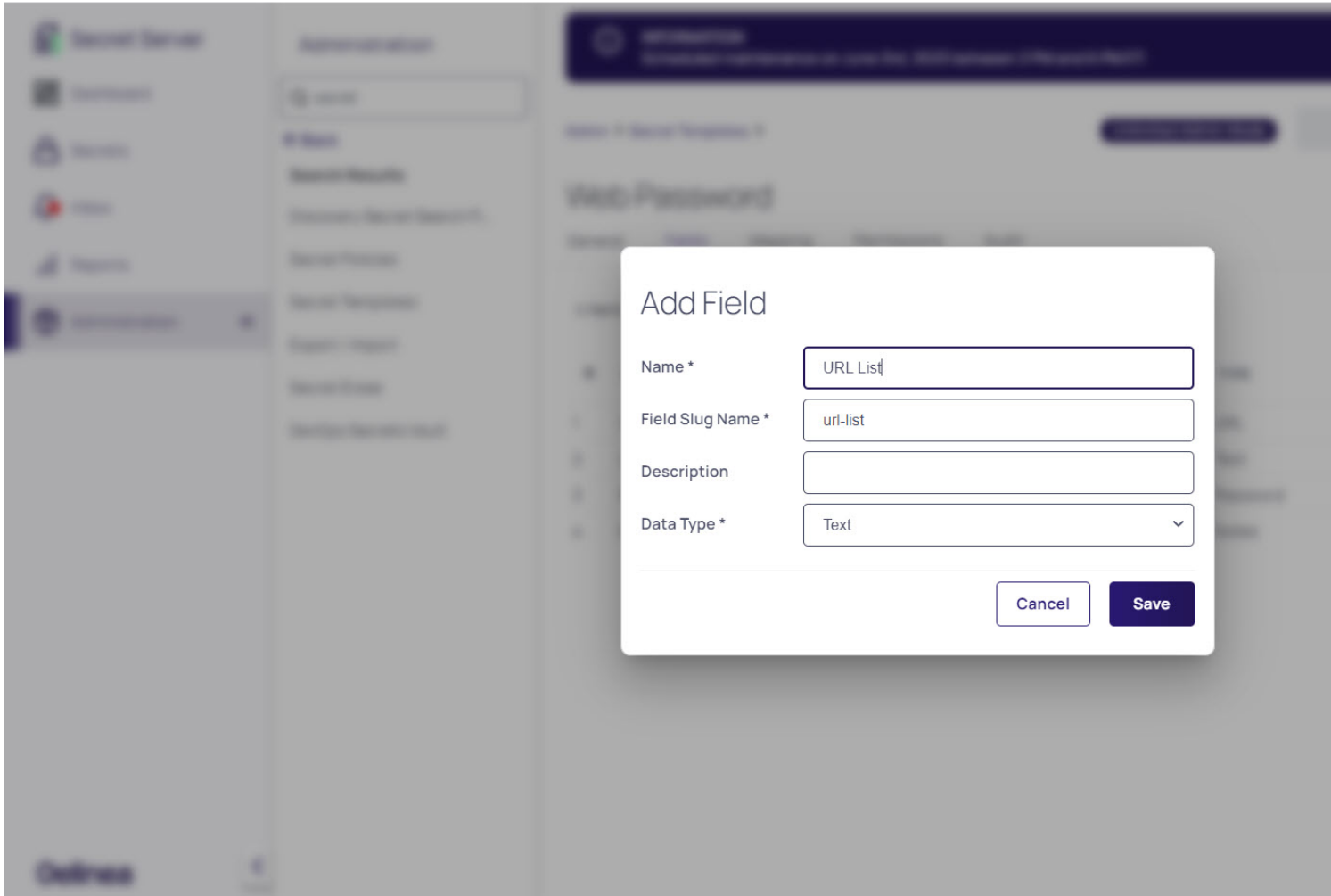
Using WPF

The screenshot shows the Delinea Secret Server Administration interface. On the left is a navigation sidebar with options: Secret Server, Dashboard, Secrets, Inbox, Reports, and Administration (selected). The main content area is titled 'Administration' and contains a search bar with 'secret' entered, a 'Back' button, and a 'Search Results' section. Below this are links for Discovery Secret Search Fi..., Secret Policies, Secret Templates, Export / Import, Secret Erase, and DevOps Secrets Vault. At the bottom left of the sidebar is the 'Delinea' logo. The right-hand pane shows a notification banner for 'INFORMATION' regarding scheduled maintenance on June 3rd, 2023. Below the notification is a breadcrumb trail 'Admin > Secret Templates >' and a 'Unlimited Admin Mode' button. The main heading is 'Web Password', with tabs for 'General', 'Fields' (selected), 'Mapping', 'Permissions', and 'Audit'. It shows '4 Items' and an 'Active' dropdown. A table lists the fields:

	NAME	SLUG	DESCRIPTION	TYPE
1	URL	url	The online address whe...	URL
2	UserName	username	The name associated wi...	Text
3	Password	password	The password used to a...	Password
4	Notes	notes	Any comments or additi...	Notes

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

 **Note:** The *Data Type* can be anything except *URL List*, *List* or *URL*



7. Click the *Mapping* tab

Using WPF

The screenshot displays the Secret Server Administration interface. On the left is a navigation sidebar with options: Secret Server, Dashboard, Secrets, Inbox, Reports, and Administration (selected). The main content area is titled 'Administration' and contains a search bar with 'Secret Templ' and a list of sub-panels: Back, Search Results, Secret Templates, Discovery Secret Search Filt..., Secret Policies, and DevOps Secrets Vault. At the top right, a dark blue information banner states: 'INFORMATION Secret Server Cloud will be undergoing scheduled maintenance on February 14, 2024 at 12:00 PM ET, some features may be unavailable briefly during this window.' Below this, the breadcrumb path is 'Admin > Secret Templates > Web Password'. The 'Web Password' section has tabs for 'General', 'Fields', 'Mapping' (highlighted with a red box), 'Permissions', and 'Audit'. Under the 'Mapping' tab, the 'Password Changing' section is visible, with a description: 'Enables heartbeat, remote password changing, and configures / maps the password changer type and fields.' Below this is a table of configuration items:

Enable RPC	Yes
RPC Max Attempts	500
RPC Interval	0 days 0 hours 15 minutes
Enable Heartbeat	Yes
Heartbeat Interval	0 days 8 hours 0 minutes
Password Type to use	Web User Account

The browser address bar at the bottom shows the URL: <https://scimtest.secretservercloud.com/app/#/admin/secret-template/6099/mapp...>

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

Using WPF

The screenshot displays the Delinea Secret Server Administration interface. On the left is a navigation sidebar with options: Secret Server, Dashboard, Secrets, Inbox, Reports, and Administration (selected). The main content area is titled 'Administration' and contains a search bar with 'Secret Templ' and a list of sub-items: Back, Search Results, Secret Templates, Discovery Secret Search Filt..., Secret Policies, and DevOps Secrets Vault. At the top right, a dark blue information banner states: 'INFORMATION Secret Server Cloud will be undergoing scheduled maintenance on February 14, 2024 at 12:00 PM ET, some features may be unavailable briefly during this window.' Below this, the breadcrumb 'Admin > Secret Templates > Web Password' is visible. The main heading is 'Web Password' with tabs for General, Fields, Mapping (active), Permissions, and Audit. The 'Launchers' section includes a descriptive paragraph and a configuration table.

Launcher Name	Website Login
Restrict User Input	No
Fields	
LAUNCHER FIELD	SECRET FIELD
Password	Password

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

The screenshot displays the Delinea Secret Server Administration interface. On the left is a navigation sidebar with options: Secret Server, Dashboard, Secrets, Inbox, Reports, and Administration (selected). The main content area is titled 'Administration' and contains a search bar with 'Secret Templ' and a list of sub-items: Back, Search Results, Secret Templates, Discovery Secret Search Fil..., Secret Policies, and DevOps Secrets Vault. At the top right, an information banner states: 'INFORMATION Secret Server Cloud will be undergoing scheduled maintenance on February 14, 2024, from 12:00 AM ET to 12:00 PM ET, some features may be unavailable briefly during this window.' Below this is a breadcrumb trail: Admin > Secret Templates > Web Password > Mapping > Website Login. The main heading is 'Website Login' followed by 'Launcher Mapping' and the instruction 'Define which fields from the Secret will be passed to the launcher.' A table lists fields: Password (mapped to Password), URL (mapped to |JRL), Username (mapped to <user input>), and Launcher Restrictions (mapped to Notes). The 'Restrict User Input' toggle is currently set to 'No'.

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

Using WPF

The screenshot shows the Delinea Secret Server Administration interface. On the left is a navigation sidebar with options: Secret Server, Dashboard, Secrets, Inbox, Reports, and Administration (selected). The main content area is titled 'Administration' and contains a search bar with 'Secret Templ' and a list of items: Back, Search Results, Secret Templates, Discovery Secret Search Fil..., Secret Policies, and DevOps Secrets Vault. At the top right, there is an information banner about scheduled maintenance. Below that is a breadcrumb trail: Admin > Secret Templates > Web Password > Mapping > Website Login. The main heading is 'Website Login'. Underneath, there is a 'Username' field with the value 'UserName'. The 'Launcher Restrictions' section is titled 'Restrict values that can be passed to a launcher.' and contains a table of settings:

Restrict User Input	<input checked="" type="checkbox"/>
Use List Fields	<input type="checkbox"/> In order to restrict user input with category
Restrict As	Choose Restriction
Restrict by Secret Field	Search or pick one

The 'Restrict User Input' row is highlighted with a red border. The 'Restrict As' dropdown menu is currently open, showing 'Choose Restriction'.

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

Using WPF

The screenshot shows the Delinea Secret Server Administration interface. On the left is a navigation sidebar with options: Secret Server, Dashboard, Secrets, Inbox, Reports, and Administration (highlighted). The main content area is titled 'Administration' and contains a search bar with 'Secret Templ' and a list of sub-panels: Back, Search Results, Secret Templates, Discovery Secret Search Fil..., Secret Policies, and DevOps Secrets Vault. At the top right, there is an information banner about scheduled maintenance. Below that is a breadcrumb trail: Admin > Secret Templates > Web Password > Mapping > Website Login. The main heading is 'Website Login'. Underneath, there are fields for 'Username' (containing 'UserName') and 'Restrict User Input' (checked). The 'Restrict As' dropdown is open, showing options: Choose Restriction, Choose Restriction, Allowed List (highlighted with a red box), and Blocked List. The 'Restrict by Secret Field' label is visible below the dropdown.

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

Using WPF

Secret Server

- Dashboard
- Secrets
- Inbox
- Reports
- Administration

All Secrets

Search Folders

- All Secrets
- Personal
- tss-sdk-go
- AAA folder
- ABCD
- ABCD{
- ABCD{1
- Aishwarya
- ALM
- Bank Information
- Database Secrets
- DC Office
- deleted secrets
- Derek's Test

Admin > Secret Templates > Test Template > Mapping > Website Login

Website Login

Password Password

URL <user input>

Username UserName

Launcher Restrictions

Restrict values that can be passed to a launcher.

Restrict User Input

Use List Fields

Restrict As

Restrict by Secret Field

- UserName
- Notes
- URL LIST
- JURLLIST

Using the Custom Web Launcher

To use the custom web launcher follow these simple steps:

Using WPF

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 (x)
Secret Name *	<input type="text"/>
UserName	<input type="text"/>
Password	<input type="password"/> <input type="button" value="Generate"/>
Notes	<input type="text"/>
URLLIST	<input type="text"/>

Unlimited Admin Mode

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

Create New Secret

Form for creating a new secret with fields for Password, Notes, URL LIST, and Site.

Password: [] [Generate]

Notes: []

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

Site: Default [v]

Cancel Create Secret

Unlimited Admin Mode

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

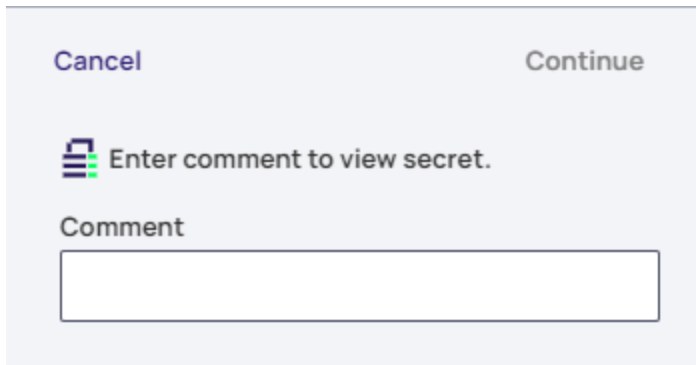
The screenshot shows the Secret Server interface. On the left is a navigation sidebar with 'Secrets' selected. The main content area shows the details for a secret named 'Test-Comma-Separated-URL'. At the top, there is an information banner about scheduled maintenance. Below that, the secret's details are shown, including the URL 'https://about.me/login', username 'test', and password '*****'. The 'Launchers' section is visible, with a red box highlighting the 'Web Password Filler' option. Below the launchers, it says 'No Active Sessions' and 'Expiration and Heartbeat'.


Comment Required Option

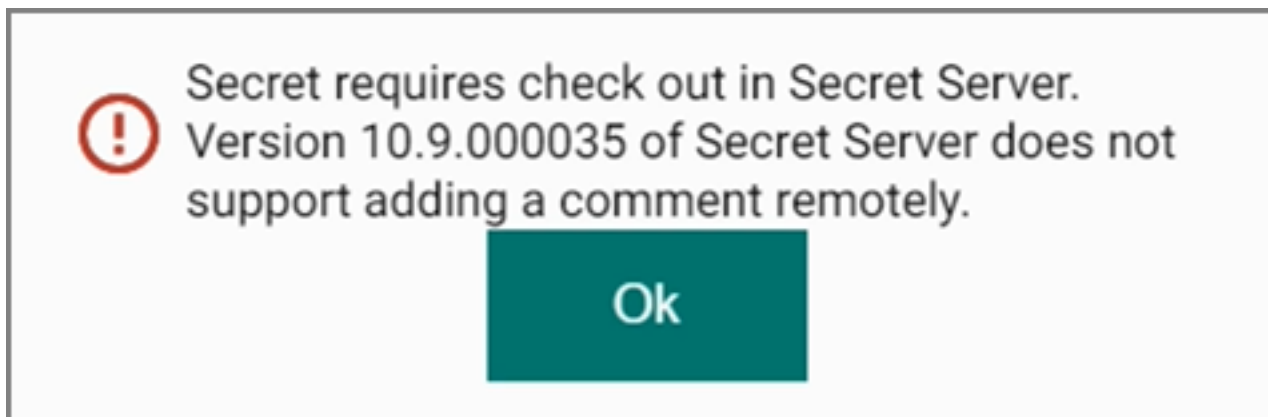
When a Secret in Secret Server requires that a comment for checkout, the user can supply that comment via the **Enter Comment** modal. Once the comment is entered and submitted WPF will populate the fields and access is given.

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 field and **Checkout**.



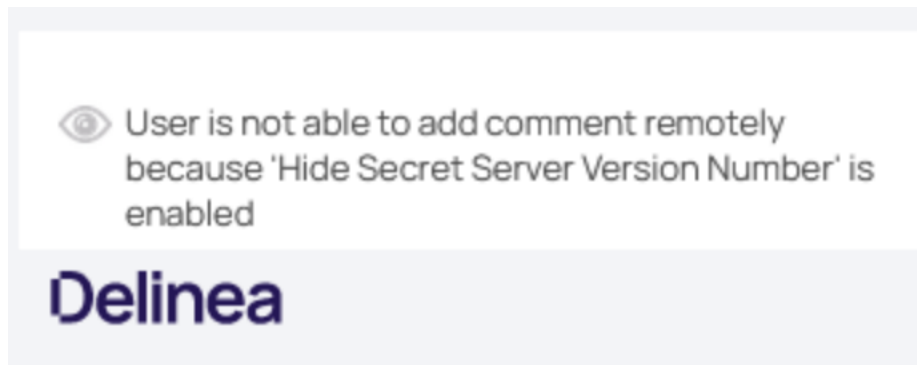
 **Note:** This feature is only supported with Secret Server versions above 11.1.000004. If used on version 11.1.000004 or earlier, the following message will be displayed.



Comment Required When the "Hide Secret Server Version Number" setting is Enabled

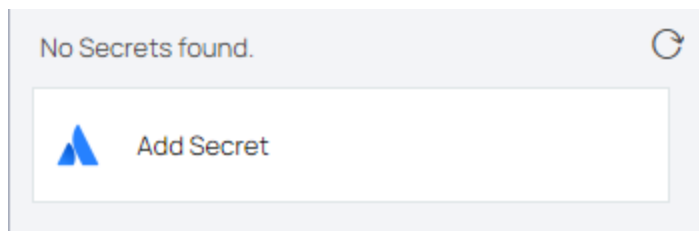
To add a comment to any secret, Web Password Filler requires the actual Secret Server version number. However, when the "Hide Secret Server Version Number" setting is enabled, the API calls will not return information about the Secret Server version.

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:

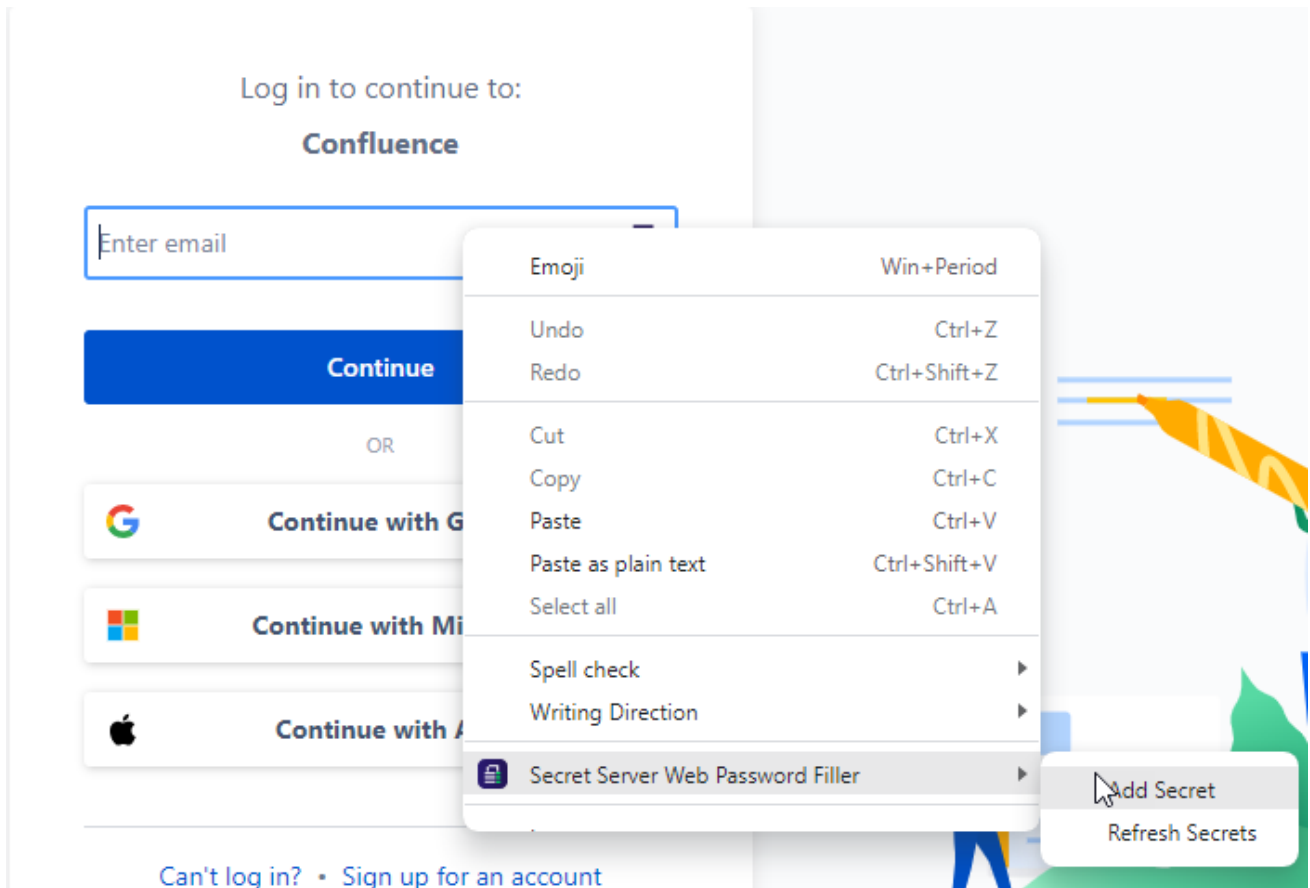


Creating a Secret for a Website

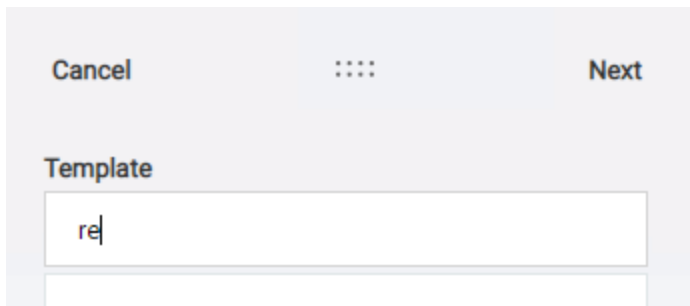
1. Navigate to the page to create a new account on a website.
2. Click the Delinea icon in the password text box. A modal appears:



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 screenshot shows a modal window titled 'Add Secret' with a header containing 'Cancel', a menu icon, and 'Save'. Below the header is the Atlassian logo and a text field containing 'id.atlassian.com'. The main form area contains several fields: 'Folder' with a small square icon, 'Site' with 'Local' selected, 'URL' with a color selection bar, 'UserName' with an empty text box, and 'Password' with an empty text box and an eye icon for visibility.

Choose a Secret Template

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.


Choose a Folder

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

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

Using WPF

Cancel ⋮ Save



id.atlassian.com

Folder

m

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

User.Name

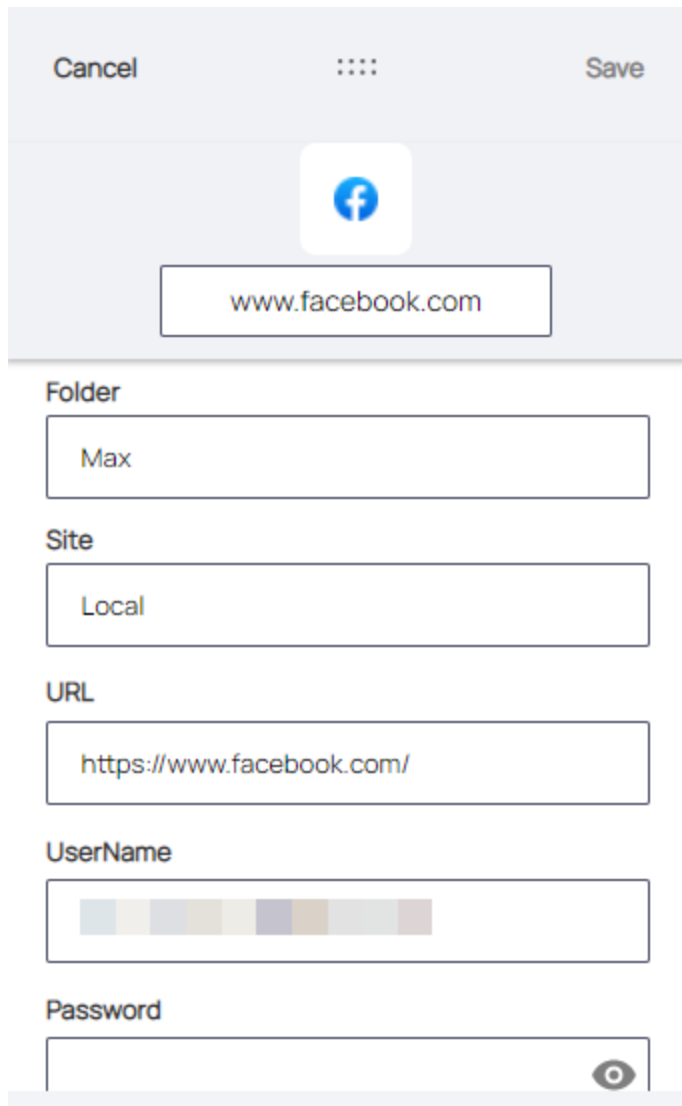
Password

Site


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,

Using WPF



Cancel ⋮ Save



www.facebook.com

Folder

Max

Site

Local


URL

https://www.facebook.com/

UserName


[Blurred]

Password

[Empty] 

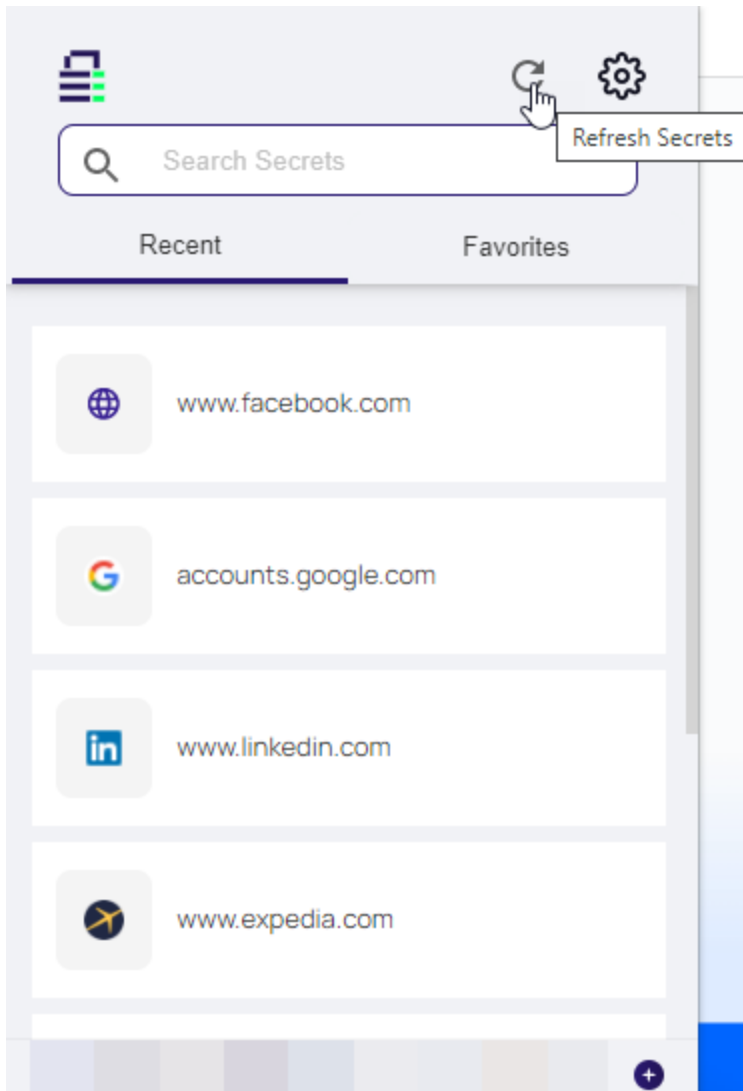
If you are setting up a secret for Microsoft Online, leave the modal as is (do not close it) and read [Using WPF with Microsoft Online Services](#) before continuing.

- 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.
- Type your username for the website for **User Name**.
- If this is a new account, click **Generate** to create a strong password for the site. Otherwise, use the existing password for the website.
- 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.

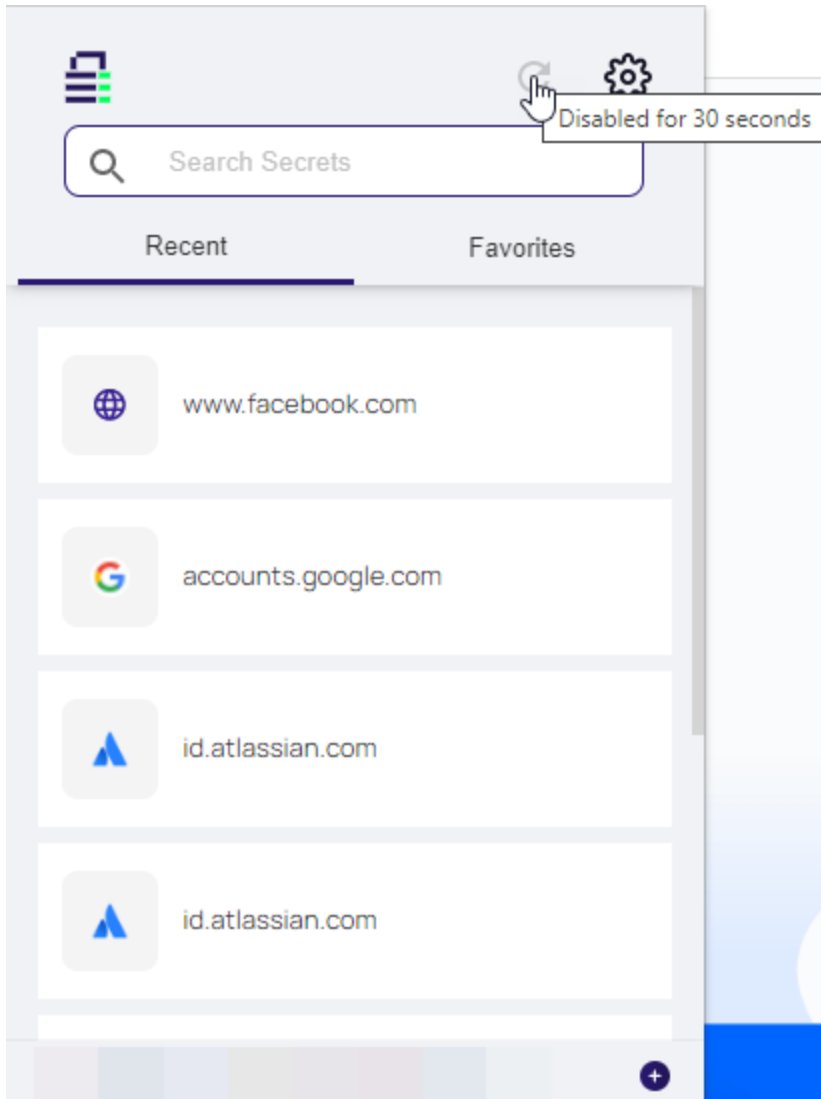
 **Note:** Not all websites work with WPF populating the "new account" information for you. There are ways around that, like creating the website account first outside of WPF, and then using those credentials.

Recent and Favorites - Refresh

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.

Map fields on a Web page form to the fields in a Secret

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.

Using WPF

The screenshot shows a mobile application interface with a light gray header containing 'Cancel', a menu icon (three dots), and 'Save'. Below the header is a blue logo and a text field containing 'id.atlassian.com'. The main form area has several sections: 'UserName' with a text field containing 'ilya.dudkin@softwarium.net'; 'Password' with a text field containing dots and an eye icon, and a 'Generate Password' button below it; 'Notes' with a large empty text area; and 'URL list' with an empty text area. A tooltip with a hand icon points to the 'Password' field, containing the text 'Drag this to the Password field on the page'.

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



Enabling Field Mapping with Metadata

To enable the field mapping function for Web Password Filler end users, a Secret Server administrator must create a metadata section named **WPFHints**. In the WPFHints section, the administrator must assign a name for each 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"]`.

Using WPF

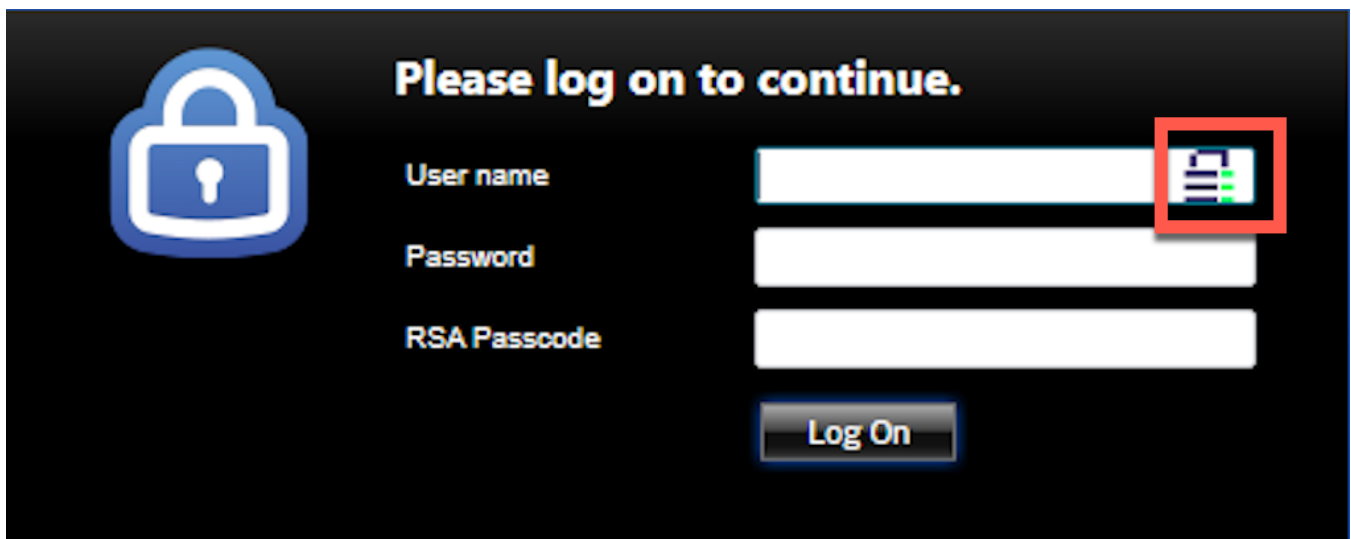
General	Security	Audit	Remote Password Changing	Dependencies	Sharing	Settings	Metadata
WPFHints							
				accno	//*[id="account"]		Edit
				Password	//*[id="password"]		Edit
				UserName	//*[id="username"]		Edit

Mapping Secrets With Three or More Login Fields

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 Password Filler needs to populate.

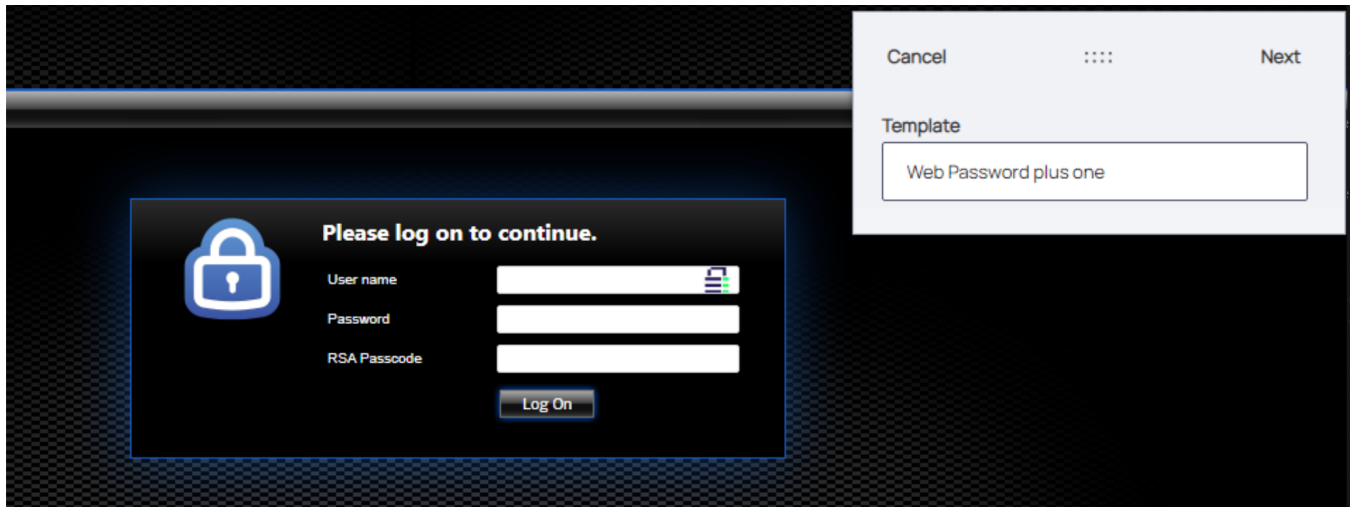
The steps listed below will guide users on how to map secrets with three or more fields:

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

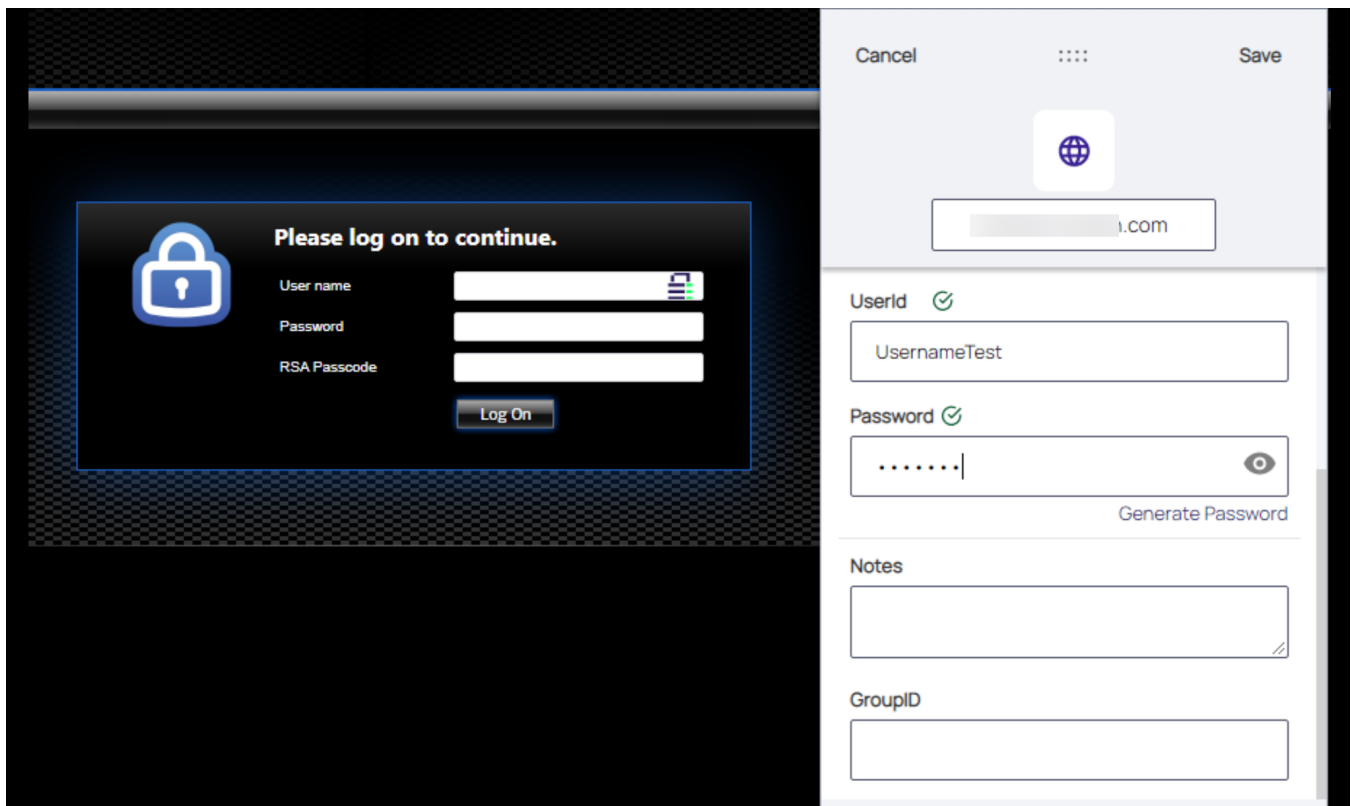


2. When adding a secret, select a customized template that has more fields than the standard web password template. In this case, there is one additional field.

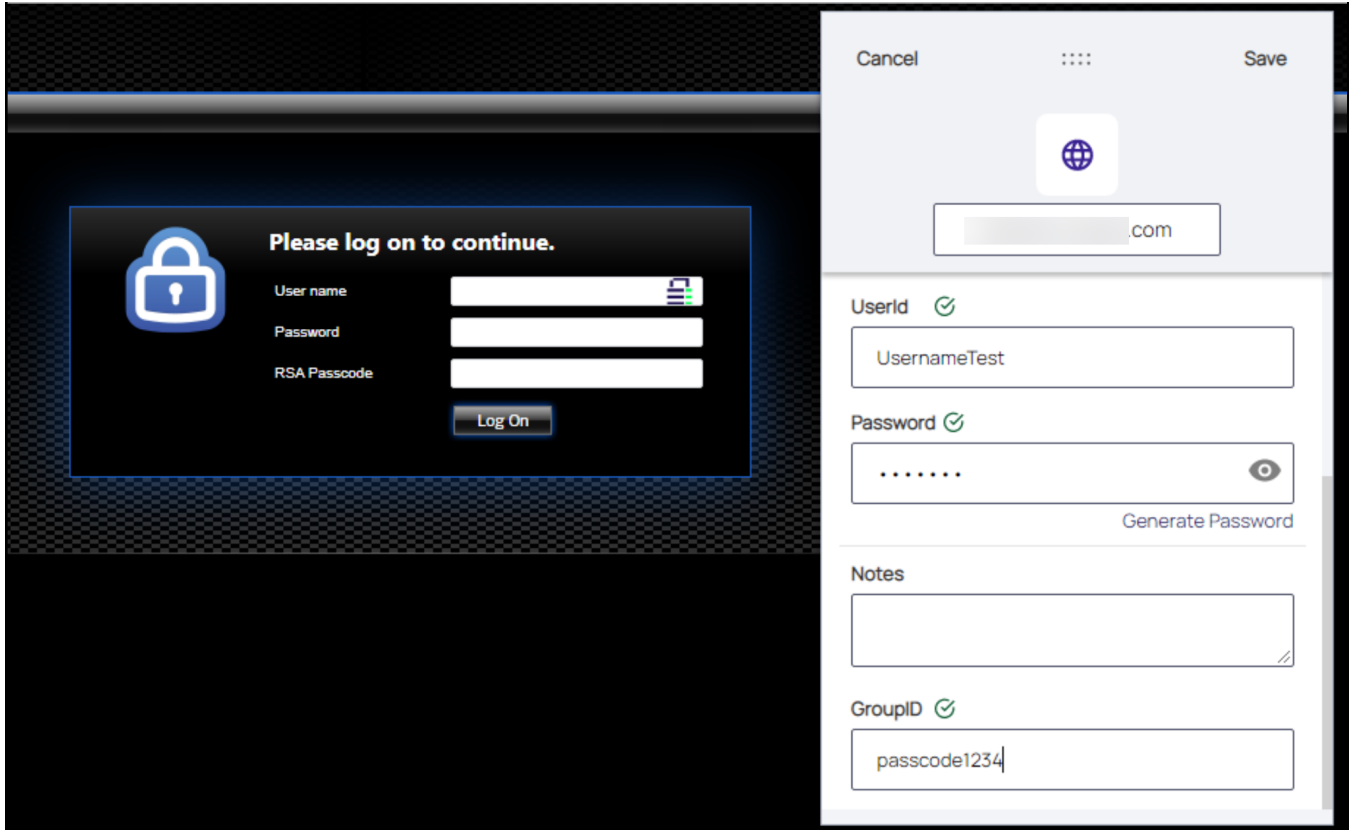
Using WPF



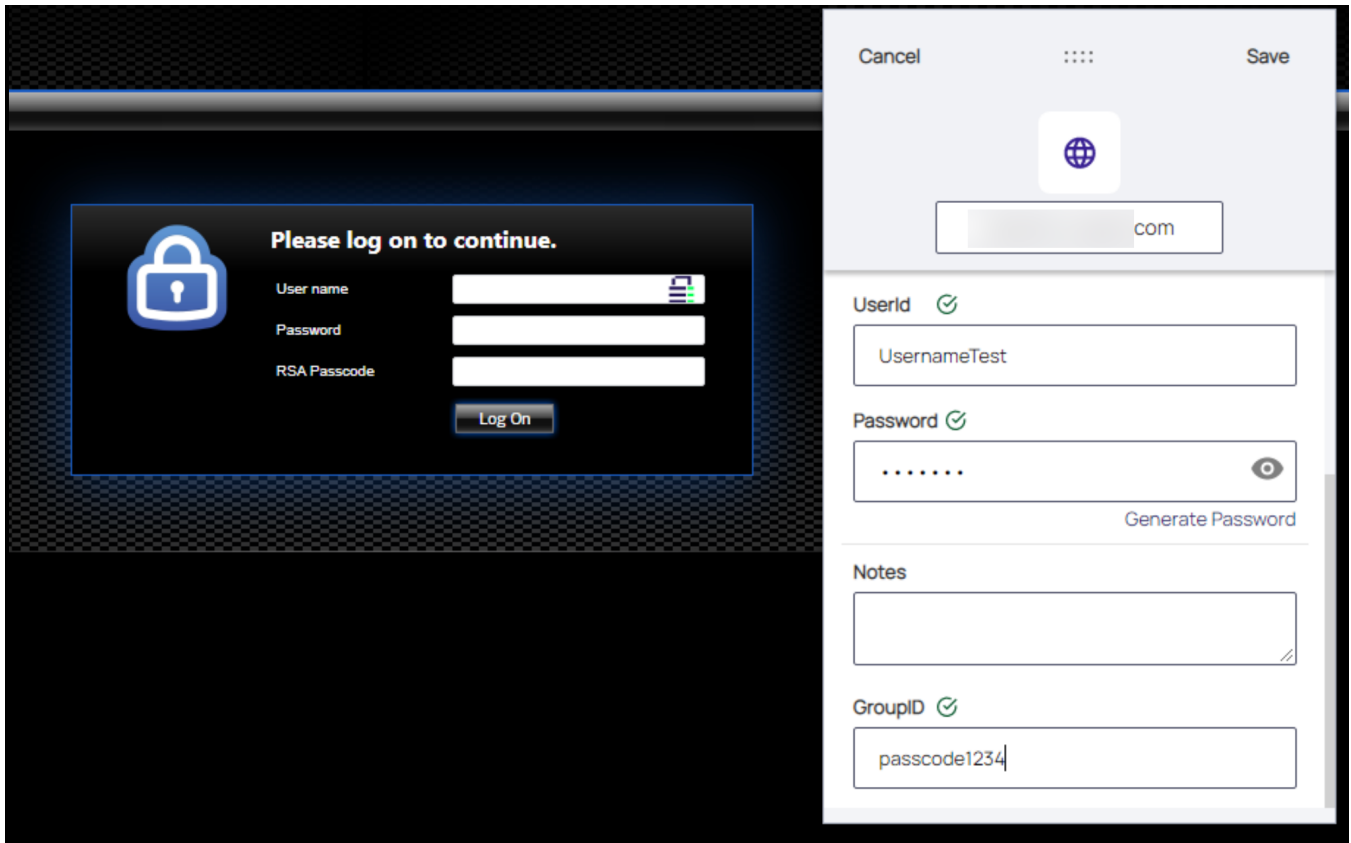
3. Drag the template User ID field to the web login Username



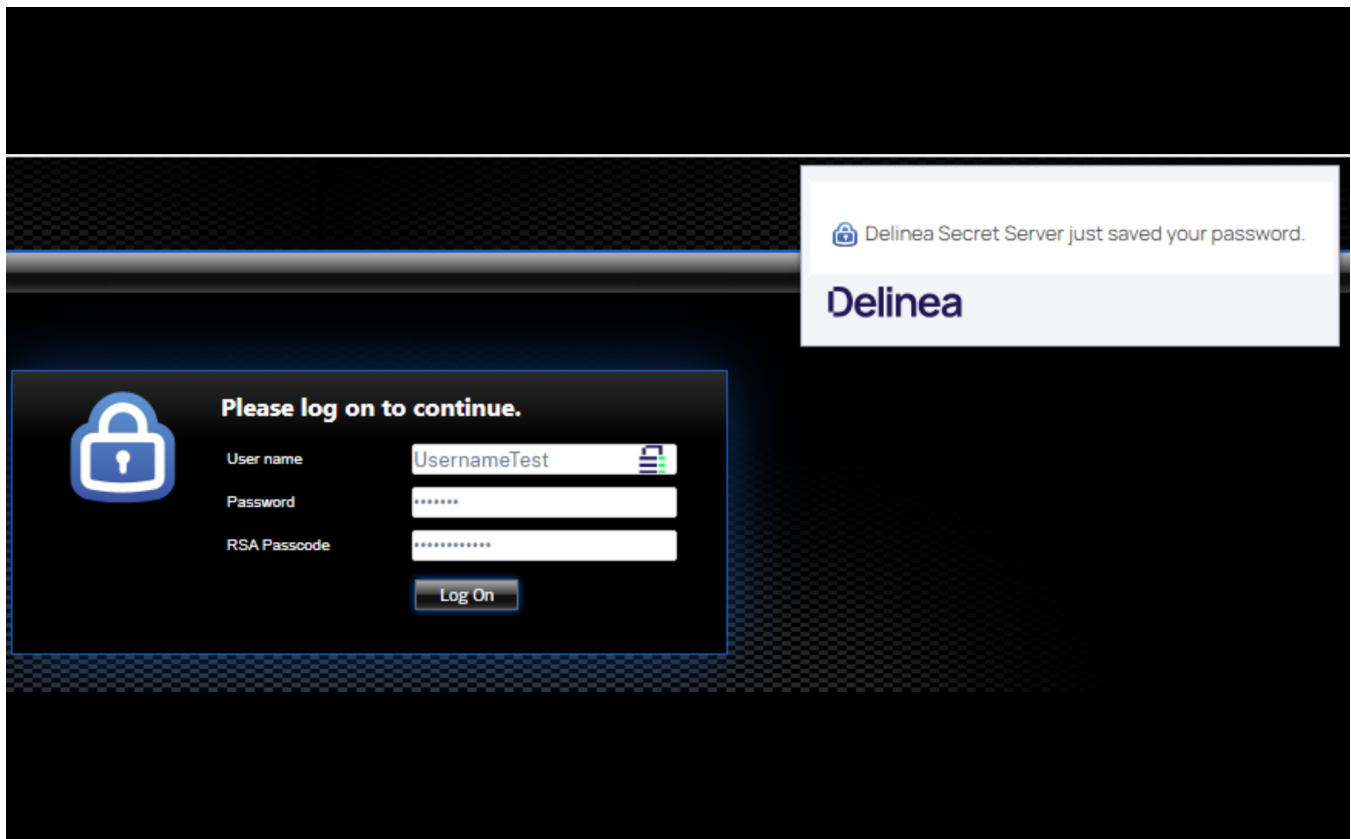
4. Drag the template password field to the web login's Password field




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.

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**
 - Safari: **Run in Private Window**
3. Login to WPF.

Logout of Secret Server

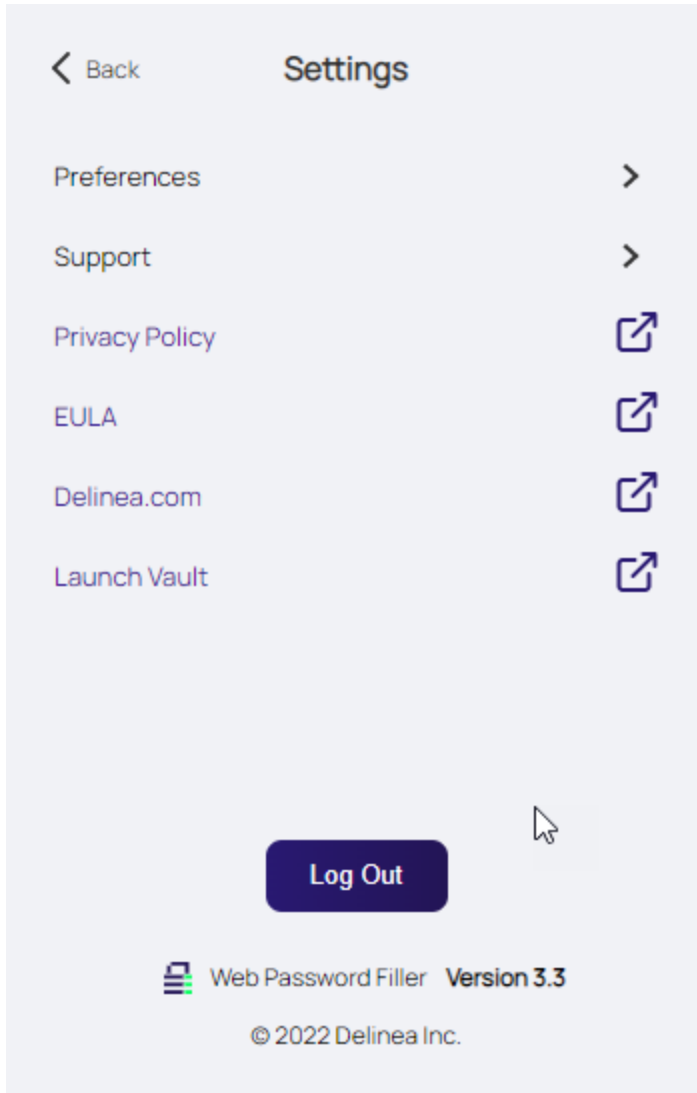
Use the WPF icon to logout:

Using WPF

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:



Using Web Password Filler with Microsoft Online Services

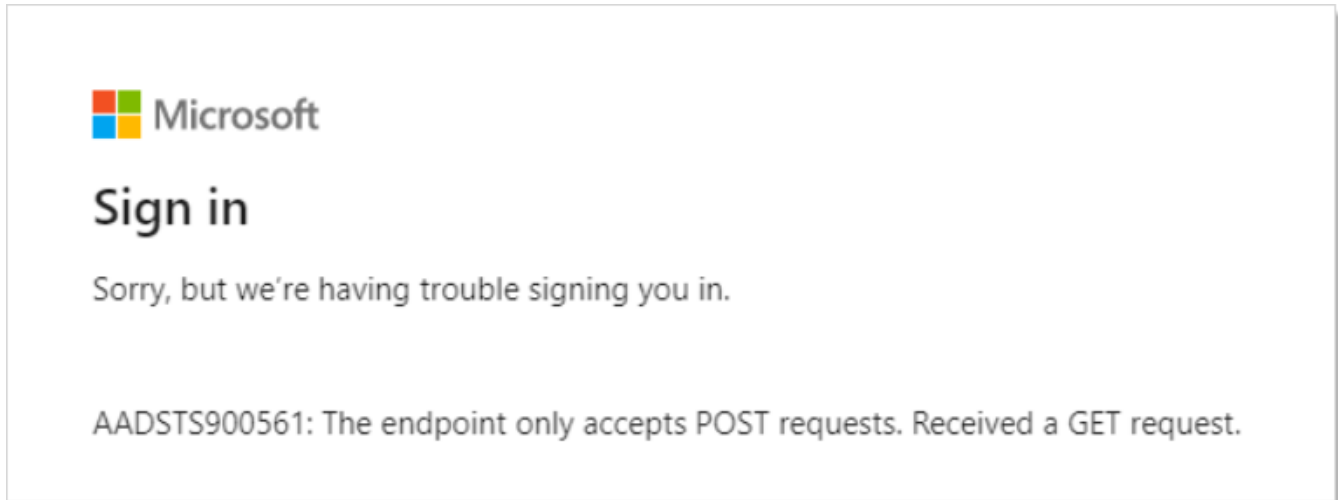
This section guides users through using the Web browser extension to use Secret Server WPF to login to Microsoft Online. Launching Microsoft Online secrets with WPF takes a bit of extra configuration. This section explains the issue and suggests remedies.

Using WPF

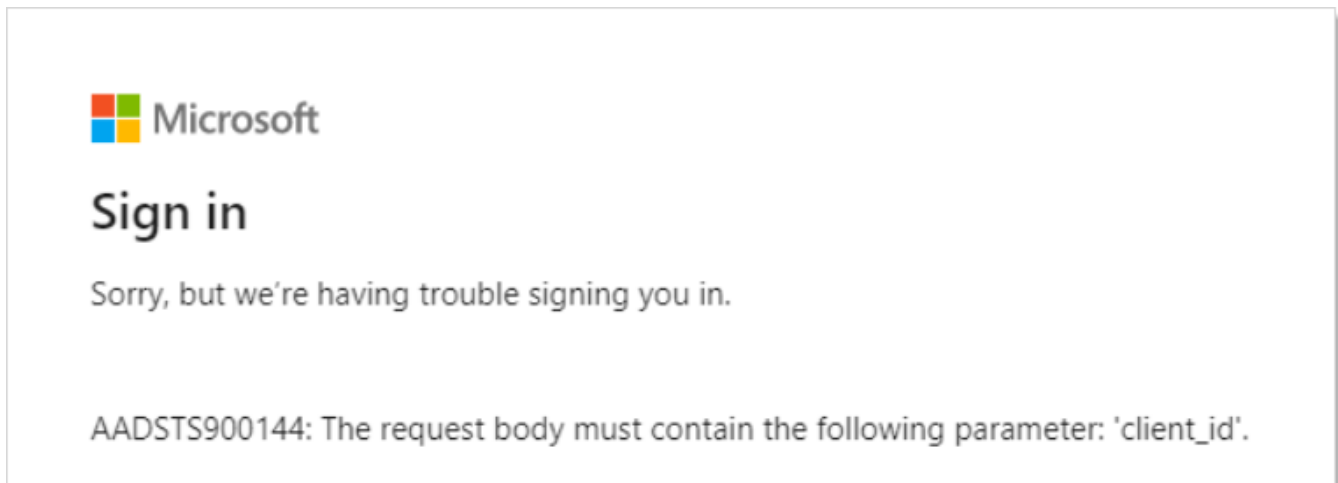
Note: This version of WPF is available in Secret Server release 10.7.59 and later. These instructions assume you have WPF installed correctly and are connected to SS. If Microsoft Online is your first site using WPF, we suggest first testing your installation on another site.

The Problem

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.

What Is Going on?

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

Using WPF

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:

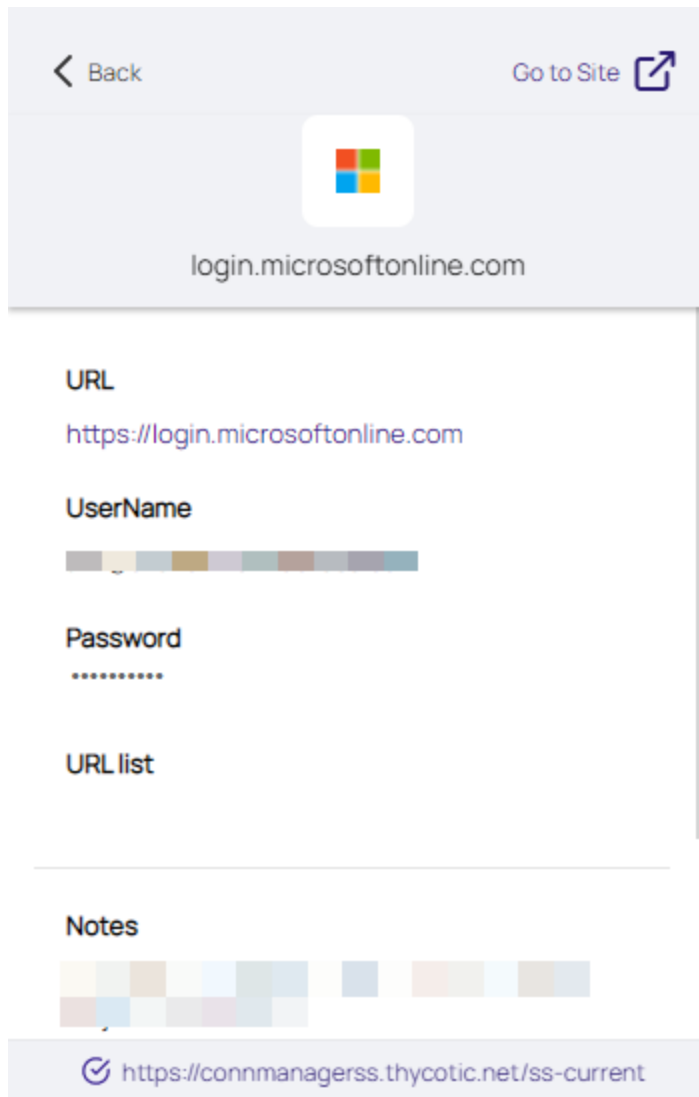
- **Before Saving the WPF Secret:** Change the URL when it is initially stored, right from WPF, *before* the secret is saved. This method is available if you create a new WPF secret using the WPF Add Secret button or the browser's context (right click) menu.
- **After Saving the WPF Secret:** Change 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.

Fixing the Issue When Creating the WPF Secret

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:

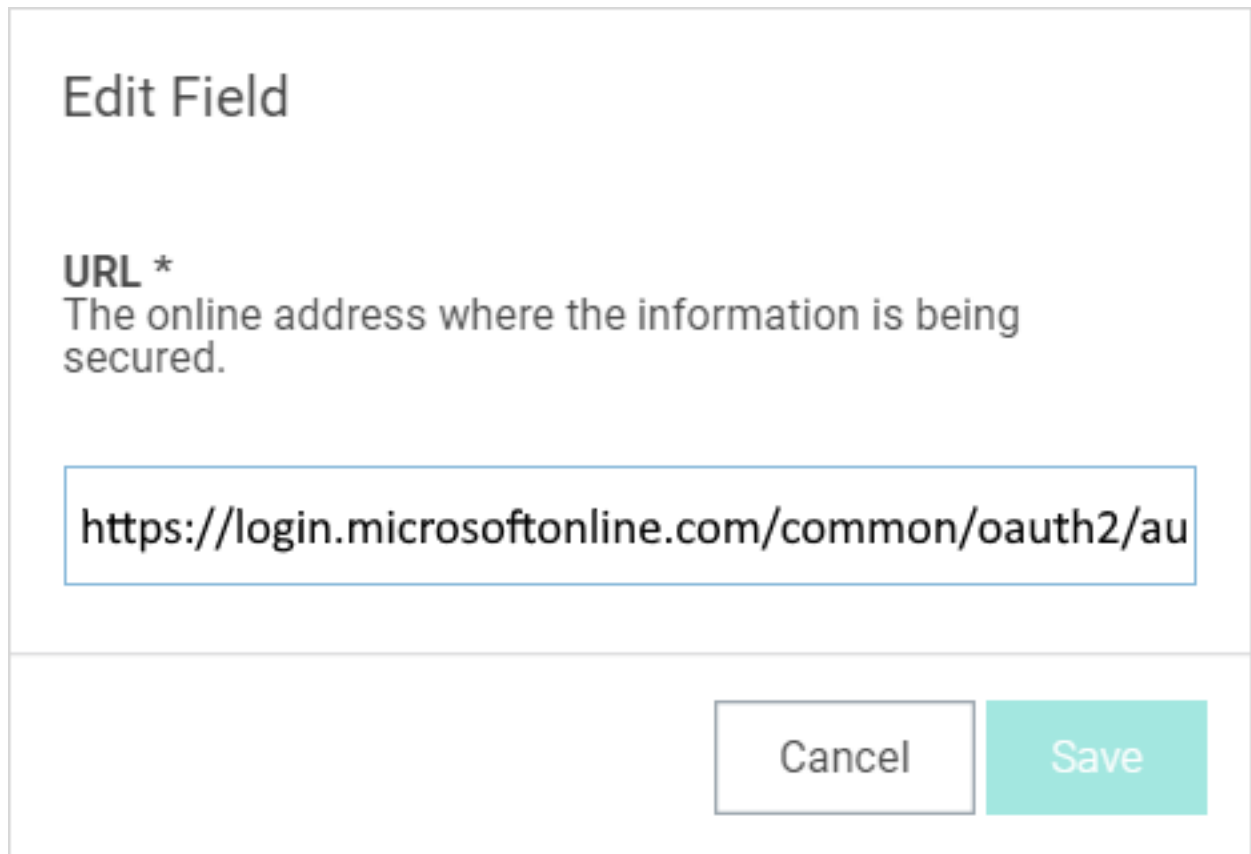


You now see the website URL that WPF inferred, which is incorrect. The secret name was inferred too—leave it as is or change it to whatever you like.

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.

Fixing the Issue After Having Saved the WPF Secret

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.

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

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.

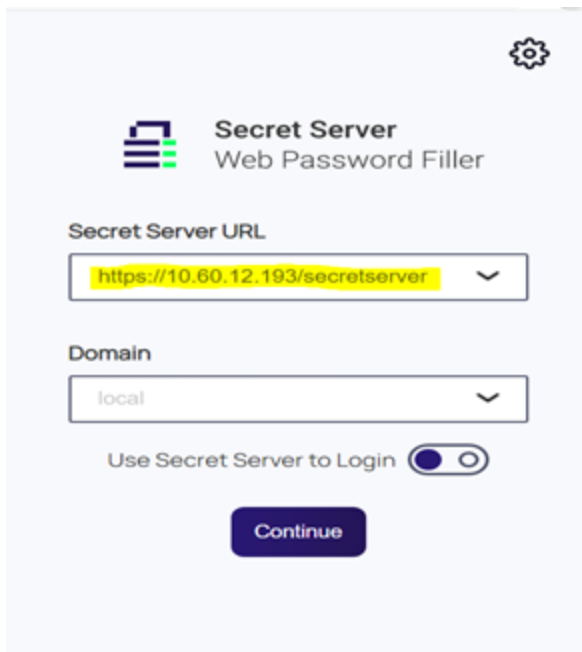
Using WPF

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.

Working With Self-Signed Certificates on Manifest V2

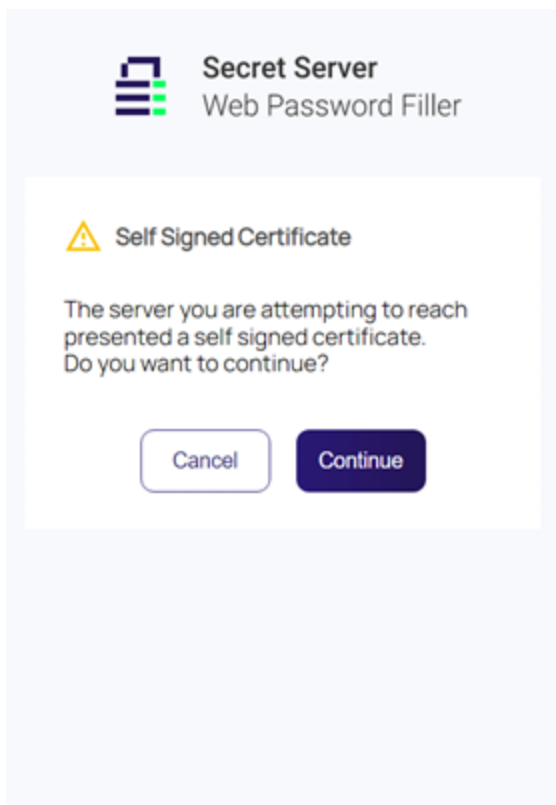
With Secret Server URLs that had self-signed certificates, Web Password Filler would load the self-signed urls (e.g. local sites("https://localhost/somesite")) and users would get an error and they would be redirected to that same URL in another tab. This other tab would display the following error: 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")

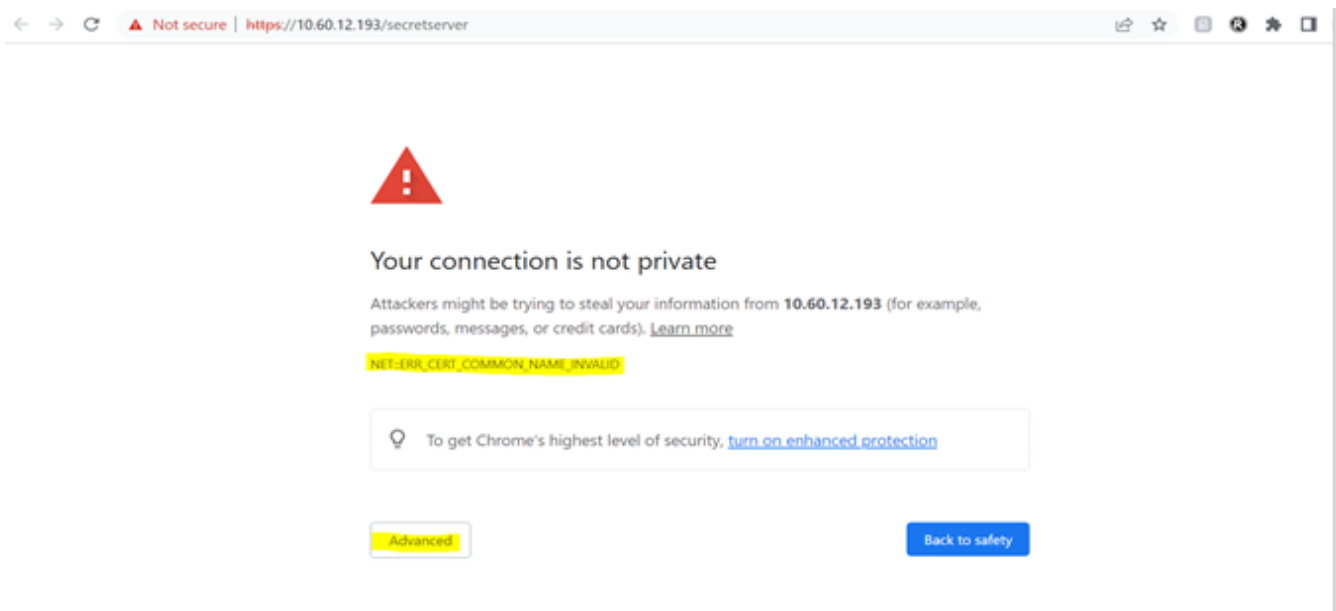


2. User would encounter the certificate error displayed below:

Using WPF



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-signed certificate and the extension is allowed to proceed further.

Working With Self-Signed Certificates on Manifest V3

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

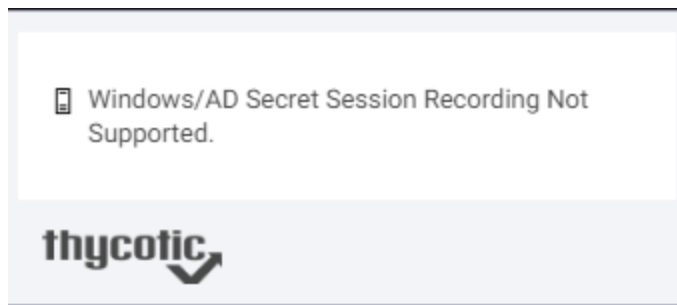
Windows Admin Center Support

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

Troubleshooting

display the following message.



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.

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.

WPF Login

Are you logged into WPF?

Users logging in to Secret Server via web login will automatically be logged in to Web Password Filler. Users who log in to Secret Server via local login will need to log in to Web Password Filler separately.



Note: For users to automatically be logged in to Web Password Filler after successfully logging in to Secret Server, the Secret Server site the user is logging into must match the URL currently in Web Password Filler.

Additionally, 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



Login Method

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](#)

Issues Logging In With Chrome or Edge

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.

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?
 - a. 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?
 - a. 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

Troubleshooting

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?

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 WPF Version

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.

Identify the Browser

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?

Site Information

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.

Access to Site

How are you accessing the site to use WPF?

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

Troubleshooting

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.

What version of WPF are you encountering the issue on?

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 is typically in the top right corner (and looks like a hamburger menu)
2. In the drop-down list select:
 - **Chrome** - More tools > Extensions
 - **Firefox** - Add-ons
 - **Edge (Chromium)** - Extensions
 - **Opera** - Extensions (in the left-hand menu).
3. 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.

Action to be Performed

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.

Templates Used

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.

Release Notes

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.

Release Notes

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

- ["3.6.1 Release Notes" on page 110](#)
- ["3.6.0 Release Notes " on page 109](#)
- [3.5.4 Release Notes](#)
- [3.5.3 Release Notes](#)
- [3.5.2 Release Notes](#)
- [3.5.1 Release Notes](#)
- [3.5.0 Release Notes](#)
- [3.4.4 Release Notes](#)
- [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](#)

Release Notes

- [1.0.9 Release Notes](#)
- [1.0.8 Release Notes - initial release](#)

1.0.10 Release Notes

Enhancements

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

1.0.8 Release Notes

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

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

1.0.9 Release Notes

Bug Fixes

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

1.1.0 Release Notes

Enhancements

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

Bug Fixes

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

Firefox Specific

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

2.0.0 Release Notes

Enhancements

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

Bug Fixes

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

2.0.1 Release Notes

Enhancements

- Added ability to check permissions for logged in users and only display options/folders based on those permissions.
 - Users only see the "Add Secret" option if they have permissions to add a Secret.
 - When adding a Secret, users see folders in the drop-down based on their permissions only and they won't

Release Notes

see folders with “Read” permissions.

- Secrets with "Read" access only have improved error messages.
- Improved support for Microsoft Online login sites that use multiple domains for Username/password logins on separate pages.
 - This applies for sites like login.live.com, microsoftonline.com, etc.
 - This is WPF side support for page “refer” links in page header.
- Added “alarm” notification for when users are reaching maximum session recording timeout of 2 hours.
- Modify back-end support for Refresh Tokens to use “alarm” based system.
 - This helps to prevent token read errors for the browser.
- Improved support for sites that force the username list to display on top of the Web Password Filler drop-down on the Username field (and prevent the overlap).
- Added additional “Remember for this site” options on WPF security pop-ups for sites with multiple domain logins.

Bug Fixes

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

2.0.2 Release Notes

Enhancements

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

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

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

Bug Fixes

- Resolved an issue when a website used multi-page logins or page redirect during while launching a web password secret from Secret Server, resulting in Secret Server sending a different URL to Web Password Filler.

Release Notes

This is resolved by the above Secret Server-side check and setting the launcher option in Secret Server.

- Resolved an issue that prevented the password from being filled for logins on sites:
 - www.businessdirect.att.com
 - login.tenable.com
- Resolved an issue where Secret Server instances that use Windows Authentication caused Web Password filler to prompt users to generate a new login token (for a second time) even if they had already generated a token.
- Resolved an issue where logging into a Microsoft Online account with a username that is in all capital letters results in the password field being cleared (by the site) when it redirects to the password page.
- Resolved an issue for browser tabs being closed when multiple Secrets (with session recording) are launched in the same browser for the same IP address (but with different port numbers). Resolution does require an additional IP address:port value pair to be added to the RegEx field in Secret Server.
- Resolved issue for a site where the auto-fill values from the secret were being entered into the fields and then cleared out by the site.

Known Issues

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



An Error Has Occurred

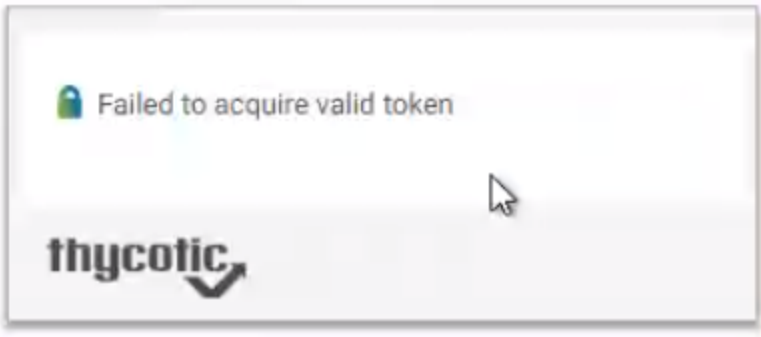


An error occurred processing this request. An attempt was made to load a page where the authenticity of it could not be verified.

 Continue

Release Notes

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




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

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

2.0.3 Release Notes

Enhancements

- Added ability to set an exclusion list for site URLs:
 - Sites listed in the exclusion list will not have Secrets populated into the Username/Password fields by default. Secrets can still be populated in these fields by clicking the Green check icon to autofill. This should help prevent none username/password fields from having values filled in them automatically even if they are identified as username/password type fields
 - An “Exclusion exception” list also exists so specific pages on the site domain will still auto-populate as normal.
 - This can be set per-user or generally on the machine and WPF reads the information from a [local Json file using the web browser’s native services](#). This does require an additional .NET 4.5.2 app to help roll out the local JSON file.

 **Note:** The user story is that the exclusion list is set to exclude a site at URL `Company1.site1.com` but has an exclusion exception for `Company1.site1.com/login.aspx`. In this case if they navigate to the login page then the secret will auto-populate in the login fields (if users only have 1 secret). After users login and go to any other page on the site that also has fields which are detected as username/password type fields, the Web Password Filler will not do anything unless directed by the user. This is to prevent the Web Password Filler from auto filling values in fields, when the auto fill action is unwanted.

- Added a new “Site” drop down option to the “Add Secret” dialog in the Web Password Filler, to allow users to select which Secret Server Distributed Engine site a Secret should be saved to (defaults to “Local” value)

Security

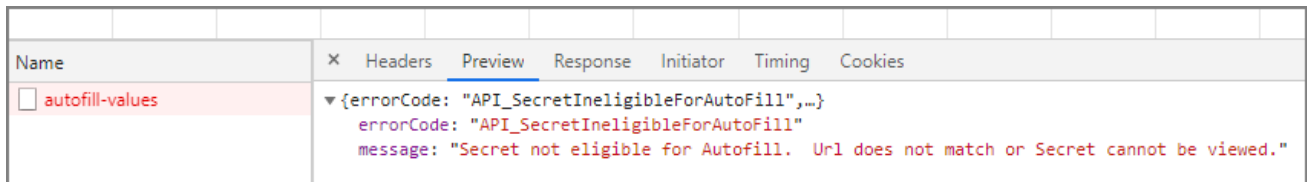
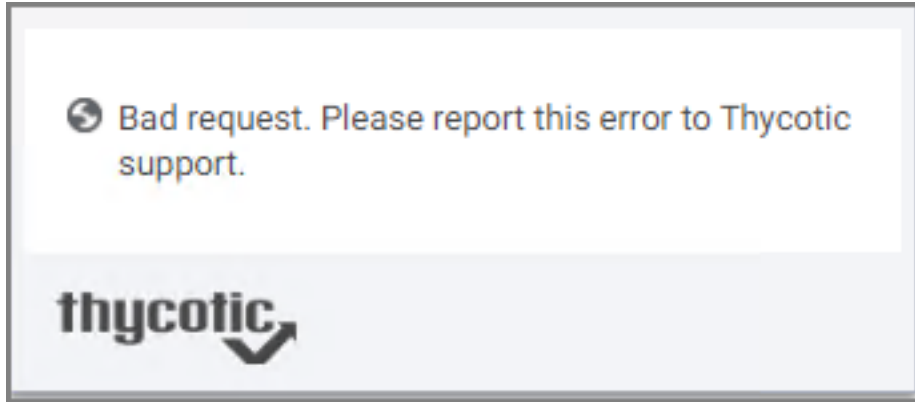
- Added sanitization on Secret Server Secret name on the pop-up display to prevent JavaScript code (using script code in the Secret name) from allowing the website to create an opening using the Secret name for access.

Bug Fixes

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

Known Issues

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



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

2.0.4 Release Notes

December 23, 2020

Enhancements

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

Bug Fixes

- Resolved issue with WPF icon not rendering correctly in login dialogs.
- Resolved issues for DUO login sites that prevented admin/owner tasks such as updates to the password:
 - Firefox: Solved duplicate drop-down entries.
 - Opera: Solved login issues.
- Resolved issue with misleading error message being returned upon unauthenticated secret launch.
- Resolved a redirect issue with SAML enable for Okta and One Login integration.
- Resolved issue for sites that prevented the username or password for an existing Secret from being updated/populated:
 - premieragent.zillow.com/crm/agentlogin, fx.tourfactory.com, https://telepizza-sso.awsapps.com/start/#, https://www.spectera.com/PWP/Landing

Known Limitations

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

2.0.5 Release Notes

March 30, 2021

Features

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

Bug Fixes

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

Release Notes

- <https://hqprrsa02.cmpa.org:7004/console-ims>
- <https://nystateofhealth.ny.gov/>
- <https://prtg.centergrid.com/>
- <https://secure.trust-provider.com/>
- www.logicmonitor.com

Known Issues/Limitations

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

Answers to FAQs

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

2.0.6 Release Notes

May 25, 2021

Improvements

Web Password Filler now provides improved performance for session recording.

Bug Fixes

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

Known Issues/Limitations

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

3.0.0 Release Notes

July 16, 2021

Improvements

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

Server named WPFHints, which saves the field tag mapping information on the Secret.

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

Bug Fixes

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

Known Issues

Issue

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

Issue

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

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

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

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

Choose one of these three work-arounds:

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

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

Choose one of these three work-arounds:

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

3.0.1 Hot Fix Release Notes

August 3, 2021

Product Improvement

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

Bug Fix

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

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

3.1.0 Release Notes

October 21, 2021

Product Enhancements

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

- The main WPF window, which opens when you click the active Web Password Filler icon in the upper right corner of your browser, displays two new tabs. One tab lists Recently-used secrets and the other lists secrets the user has marked as Favorites, for quick access.
- The footer of the main WPF window now indicates the URL of the Secret Server the user is logged into.
- When a user hovers their cursor over a Secret in the main WPF window, a Fill icon appears. If the URL in the secret matches the URL of the active browser tab, clicking the icon fills in the user's credentials on the page. If the URL in the Secret does not match the active browser tab, clicking the icon brings the user to the page matching the URL in the Secret, where credentials can be filled in.
- When a user clicks anywhere on a Secret panel in the main WPF window, the Secret Details view opens. When a user hovers their cursor over the URL, Username, or Password fields, a new Copy icon appears that the user can click to copy the content of that field. The user receives a Toaster confirmation when the information is copied. If the user attempts to copy a password that they lack permissions to view, a popup explains that they

Release Notes

cannot copy it.

- Web Password Filler can now be configured to have the Secret Server Login Window open in a new browser tab when the user disables or turns off the setting "Secret Server Login New Window."
- When a user is accessing a website with a checked-out secret and the maximum checkout time has passed, WPF closes the associated path and deletes the cookies, ending the user's logged-in session for improved security. The user then needs to check out the secret again to re-access the site through the Web Password Filler.

Known Issues

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

Bug Fixes

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

3.2.0 Release Notes

February 9th, 2022

Product Enhancements

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

Bug Fixes

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

Known Issues

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

Browser Related

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

3.3.0 Release Notes

June 21th, 2022

Features

- Web Password Filler has been updated to reflect Delinea Inc.'s rebranding along with our new company colors and icons.
- Web Password Filler now offers dropdown functionality for selecting domains fields on the configuration page.
- Web Password Filler now offers a dropdown list for logging on to more than one Secret Server.

Bug Fixes

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

iOS Specific

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

3.4.0 Release Notes

August 18th, 2022

Features

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

Product Enhancements

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

Bug Fixes

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

3.4.1 Release Notes

September 23rd, 2022

Bug Fixes

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

3.4.2 Release Notes

December 5th, 2022

Features

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

General Maintenance

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

Bug Fixes

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

Known Issues

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

3.4.3 Release Notes

March 15th, 2023

Features

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

Security Improvements

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

Bug Fixes

- Fixed an issue where Web Password Filler was cropping the session recording videos
- Fixed an issue where Web Password Filler was not filling out passwords for certain sites
- Fixed an issue where the *Add Secret* button was enabled for users who did not have permissions to add secrets

3.4.4 Release Notes

April 3rd, 2023

Bug Fixes

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

3.5.0 Release Notes

May 8th, 2023

Features

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

Bug Fixes

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

Known Issues

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

3.5.1 Release Notes

May 12th, 2023

Bug Fixes

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

Known Issues

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

3.5.2 Release Notes

May 30th, 2023

Features

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

Bug Fixes

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

Known Issues

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

3.5.3 Release Notes

June 20th, 2023

Features

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

Bug Fixes

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

3.5.4 Release Notes

July 20th, 2023

Improvements

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

Bug Fixes

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

3.6.0 Release Notes

August 21st, 2023

Features

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

General Improvements

- Improved session recording stability.

Security Improvements

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

Bug Fixes

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

Known Issues

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

3.6.1 Release Notes

August 22nd, 2023

Bug Fixes

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

Documentation Changelog

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

August 2023

- "3.6.1 Release Notes" above
- "3.6.0 Release Notes " on the previous page

July 2023

- [3.5.4 Release Notes](#)

June 2023

- [3.5.3 Release Notes](#)

May 2023

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

April 2023

- [Release Notes](#)

March 2023

- [Release Notes](#)

December 2022

- [Release Notes](#)

September 2022

- [Release Notes](#)

June 2022

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

February 2022

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

November 2021

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

October 2021

- [Release Notes](#)

August 2021

- [Release Notes](#)

July 2021

- [Release Notes](#)

May 2021

- [Release Notes](#)

March 2021

- [Release Notes](#)

Release Notes

December 2020

- [Release Notes](#)

October 2020

2.0.3 Release Updates

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

September 2020

- Added Security Scans section.