



Delinea

Web Password Filler

Documentation © 3.0.0



Table of Contents

Web Password Filler	6
Getting Started	7
Enable Web Services in Secret Server	7
Installing Browser Extensions	8
Connecting with Secret Server	9
Login to Secret Server	12
Manually Logging into Secret Server with WPF	12
Logging into Secret Server via the WPF Secret Server Button	13
Preferences Menu	14
Terminology	16
Secret Server Web Password Filler	16
Secret Server Login Assist	17
Secret Server Clipboard Utility	19
Native Messaging Host	20
Installing the Native Messaging Host	20
<i>Download Location</i>	20
<i>Requirements</i>	20
<i>Supported Browsers</i>	20
<i>Installation</i>	20
<i>Registration</i>	20
<i>Uninstalling the Thycotic Native Messaging Host</i>	21
Configuration Options	21
<i>Establishing Default Settings and Browser-Specific Overrides</i>	21
<i>Settings.json Format</i>	22
<i>Site Exclusions and Exceptions</i>	25
<i>UI Behavior Based on Preferences</i>	25
<i>Error Messages</i>	26
Using WPF	27
Log in to a Website	27
Creating a Secret for a Website	28
Mapping Login Fields	30
Map fields on a Web page form to the fields in a Secret	30
Enabling Field Mapping with Metadata	30
Session Recording	32
Session Recording Limits	32
RegEx	32

<i>Using RegEx in WPF</i>	33
<i>Setup in Secret Server</i>	33
Incognito Support	37
Port Numbers	38
List of Primary and Secondary Domains	39
Logout of Secret Server	41
Windows Admin Center Support	42
Using Web Password Filler with Microsoft Online Services	43
The Problem	43
What Is Going on?	43
Fixing the Issue When Creating the WPF Secret	44
Fixing the Issue After Having Saved the WPF Secret	44
Troubleshooting	46
Investigating WPF Issues	47
Confirm WPF Version	47
Identify the Browser	47
Site Information	47
Access to Site	47
What version of WPF are you encountering the issue on?	47
Action to be Performed	48
Templates Used	48
WPF Login	49
Login Method	49
Previous Products Compatibility	50
Behavior/Problem Presentation	51
Information on Security Scans	53
Checkmarx Results	54
Thycotic Integrations Web Password Filler Scan Report	54
<i>Filter Settings</i>	54
Severity	54
Result State	54
Assigned to	54
Categories	54
Results Limit	55
<i>Selected Queries</i>	55
<i>Scan Summary - FISMA 2014</i>	57
<i>Scan Summary - NIST SP 800-53</i>	58
<i>Scan Summary - OWASP Mobile Top 10 2016</i>	59
<i>Scan Summary - Custom</i>	60
Release Notes	62

3.0.1 Hot Fix Release Notes	63
Product Improvement	63
Bug Fix	63
3.0.0 Release Notes	64
Improvements	64
Bug Fixes	64
Known Issues	64
<i>Issue</i>	64
<i>Issue</i>	64
<i>The user does not have permissions to view the password in Secret Server because the</i>	64
<i>The secret (under the Security tab) has</i>	64
<i>The template used for the secret has</i>	65
2.0.6 Release Notes	66
Improvements	66
Bug Fixes	66
Known Issues/Limitations	66
2.0.5 Release Notes	67
Features	67
Bug Fixes	67
Known Issues/Limitations	68
Answers to FAQs	68
2.0.4 Release Notes	69
Enhancements	69
Bug Fixes	69
Known Limitations	69
2.0.3 Release Notes	70
Enhancements	70
Security	70
Bug Fixes	70
Known Issues	70
2.0.2 Release Notes	72
Enhancements	72
Bug Fixes	72
Known Issues	73
2.0.1 Release Notes	74
Enhancements	74
Bug Fixes	74
2.0.0. Release Notes	75
Enhancements	75
Bug Fixes	75

1.1.0. Release Notes	76
Enhancements	76
Bug Fixes	76
<i>Firefox Specific</i>	76
1.0.10 Release Notes	77
Enhancements	77
1.0.9 Release Notes	78
Bug Fixes	78
1.0.8 Release Notes	79
Documentation Changelog	80
August 2021	80
July 2021	80
May 2021	80
March 2021	80
December 2020	80
October 2020	80
September 2020	80

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

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

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

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

Getting Started

Please set up WPF in the following order:

1. Ensure you can log in to Secret Server the conventional way and that web services are enabled.
2. If necessary, create a folder in Secret Server where the WPF secrets will reside.
3. In Secret Server enable Web Services.
4. [Install the WPF browser extension.](#)
5. [Configure WPF to point to Secret Server.](#)
6. [Login to Secret Server via WPF.](#)

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

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

Installing Browser Extensions

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


- **Chrome:** Install the extension by clicking the Web launcher icon in a Web Password secret, or by downloading it from the Google [Chrome](#) add-ons site. Also see [Managing Extensions in Your Enterprise](#) on securely managing Chrome extensions at scale.
- **Edge Chromium:** Install the extension by downloading it from the Microsoft [Edge](#) add-ons site.
- **Firefox:** Install the extension by clicking the Web launcher icon in a Web Password secret, or by downloading it from the [Firefox](#) add-ons site.
- **Safari:** Install the extension by downloading it from [How to install Safari extensions on your Mac](#). See the notes in the list below:
 - WPF supports Safari running on macOS Catalina, Mojave, Big Sur 11.1.0, 11.2.1 and later.
 - WPF does not support the Native Messaging Host configuration in Safari browsers.
 - The Safari browser extension does not support Windows Admin Center.

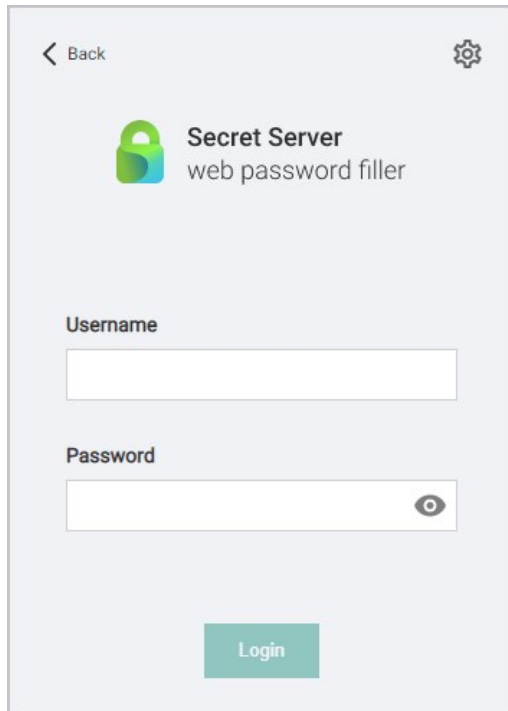
Note: WPF versions newer than 2.0.2 do not support Opera. If you are using WPF v 2.0.2 or older and you need to use Opera, you can download the extension from the [Opera](#) add-ons site.

Connecting with Secret Server


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

To connect WPF with Secret Server:

1. Open Google Chrome or any other supported browser.
2. In the upper-right corner of the browser, click the **Password Filler**  icon. The WPF login window appears:



Back

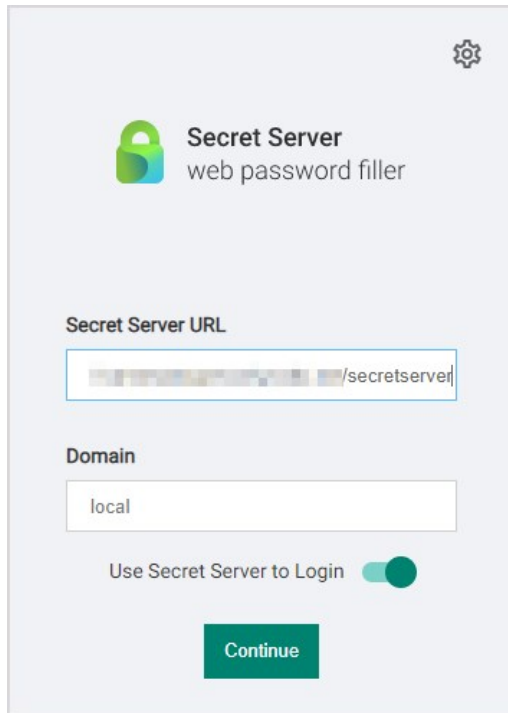
 **Secret Server**
web password filler

Username

Password

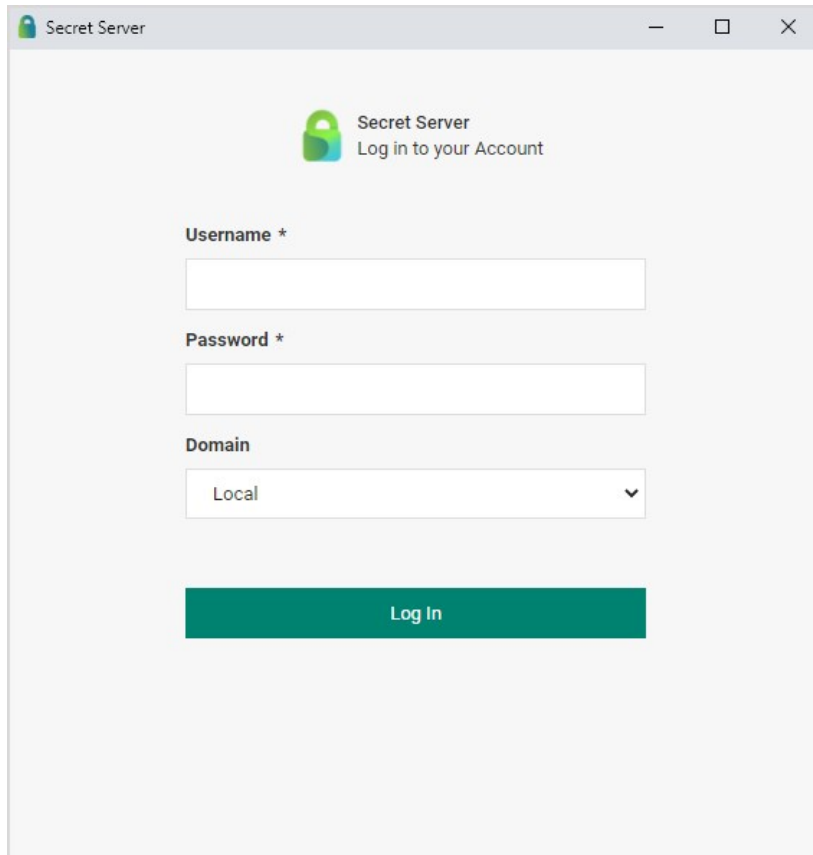
Login

3. Click **Back** in the upper left corner.



The screenshot shows a configuration window for the Secret Server web password filler. At the top left is a lock icon and the text "Secret Server web password filler". A gear icon is in the top right corner. Below the title is a text input field labeled "Secret Server URL" containing a masked URL ending in "/secretserver/". Below that is a text input field labeled "Domain" containing the word "local". At the bottom, there is a toggle switch labeled "Use Secret Server to Login" which is currently turned on (green). A green "Continue" button is at the bottom center.

4. In the **Secret Server URL** field, type your Secret Server URL. For example: <https://myserver/secretserver/>
5. In the **Domain** field, type the domain of Secret Server. This only applies if you set up Secret Server to use a domain otherwise it is Local by default. This should match the options configured in Secret Server for this sign in page:



The image shows a window titled "Secret Server" with a standard Windows title bar (minimize, maximize, close buttons). Inside the window, there is a logo of a green padlock with a white keyhole, followed by the text "Secret Server" and "Log in to your Account". Below this, there are three input fields: "Username *" (a text box), "Password *" (a text box), and "Domain" (a dropdown menu currently showing "Local"). At the bottom of the form is a large green button labeled "Log In".

6. Click the **Login** button.

Login to Secret Server

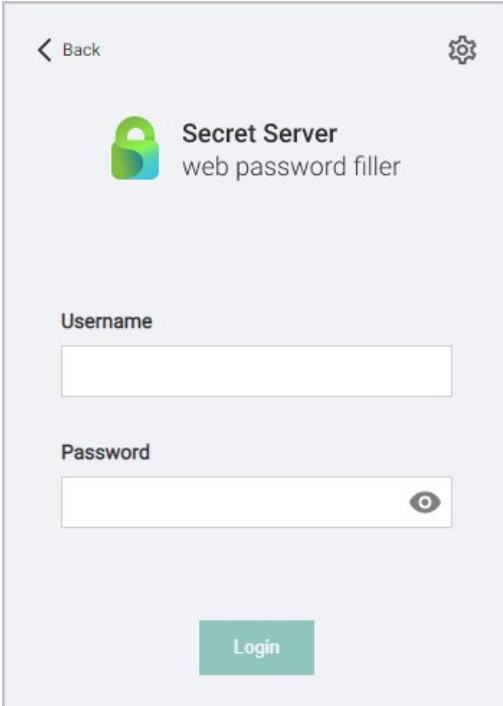
Before you have access to any secrets that apply to your websites, you must first log in and connect WPF to Secret Server. There are two ways to do this. The first is by entering your credentials into WPF and having it verify back with Secret Server. The second is by redirecting the login (through a new browser tab) back to Secret Server and using the Secret Server Web login to make the connection.

The examples below use Google Chrome and Duo. However other browsers and two-factor authentication applications are supported. Refer to information about [supported extensions](#) and Secret Server's list of two-factor applications that are supported.

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

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

1. Open, for example, **Google Chrome**.
2. In the upper-right corner of the browser, click the **Password Filler**  icon. The WPF login window appears:



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


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

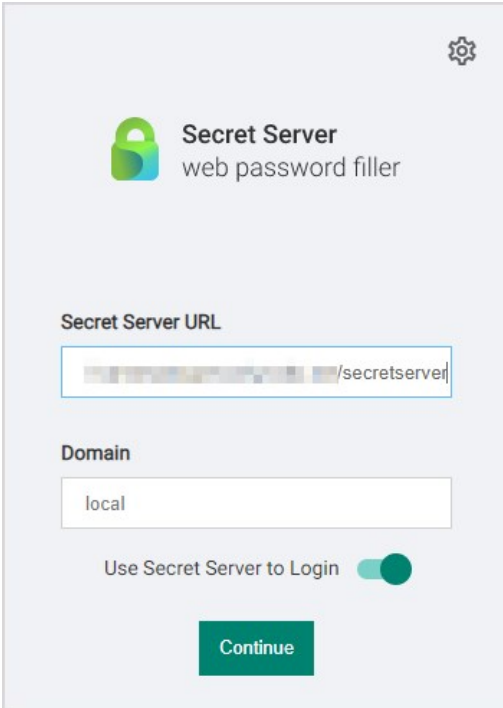
5. Click the **Login** button. If you do not have two-factor authentication enabled in Secret Server, you are now logged in.
6. If you have two-factor authentication enabled in Secret Server (and your login was authenticated), you are sent to the **Two Factor** screen to complete the second authentication. Click **Push Duo** to authenticate with your Duo app, or click **Phone** to receive an

authentication text message with a PIN code to enter in the **Pin Code** field, then click **Login**.

You are now logged in to Secret Server, and the WPF icon changes to 

The **Login with Secret Server** button allows you to log in to WPF using a redirect through the Secret Server log in, also known as SAML or single sign on. This replaces the User Name and Password text boxes on the Login tab in WPF.

1. Open, for example, **Google Chrome**.
2. In the upper-right corner of the browser, click the **Password Filler**  icon. If you already have enabled the **Use Secret Server to login** option, the Login screen will display fields for your Secret Server URL and Domain, as well as a **Login with Secret Server** toggle button.



Secret Server
web password filler

Secret Server URL
[redacted]/secretserver|


Domain
local

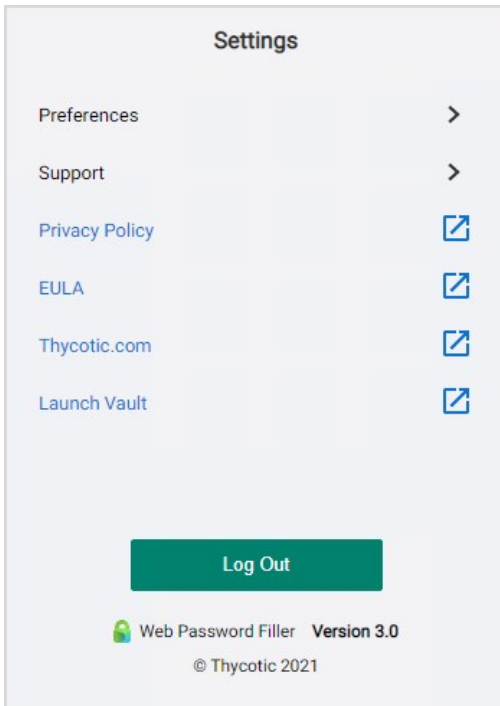
Use Secret Server to Login

Continue

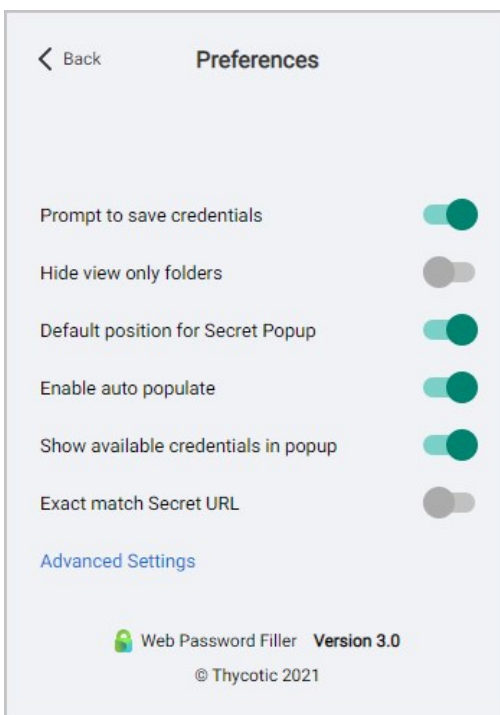
3. Click the **Login with Secret Server** toggle button. WPF opens a new tab for Secret Server in the browser, where you can log into Secret Server. After logging into Secret Server, a token is automatically generated for you. A window opens briefly showing the Generate Token button being pushed automatically, then the window quickly closes.

Preferences Menu

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



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



- **Prompt to save credentials:** Select this preference 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 thycotic check symbol.
- **Enable auto populate:** Select this preference so that when a Secret is available for a web page, WPF will automatically populate the fields on the page.
- **Exact match Secret URL Exact match.** Select this preference to ensure that WPF populates fields only if the URL exactly matches the URL specified in the Secret, and will not populate fields on variations of the URL, including sub-pages.
- **Advanced Settings / > Session Recording Limit** Select this preference to enable setting session recording limits through the UI in hourly increments, from one to eight hours. The default limit is two hours.



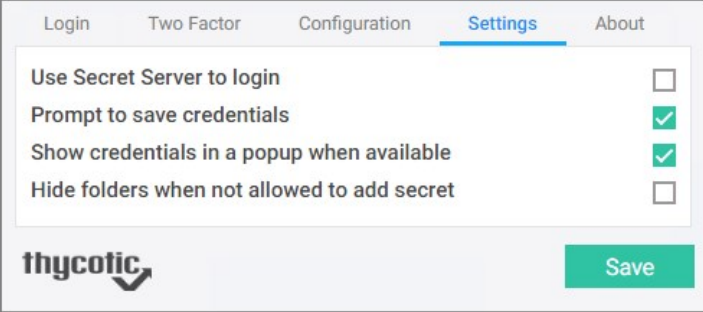
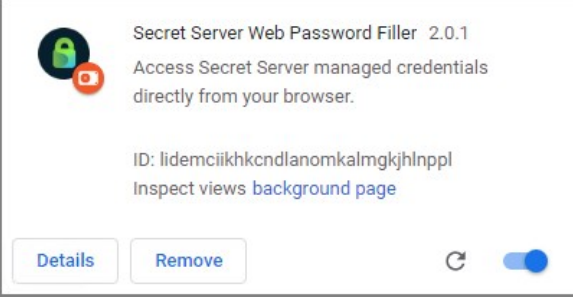
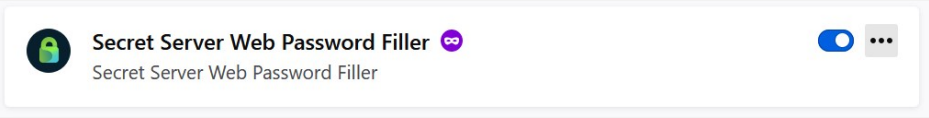
Terminology

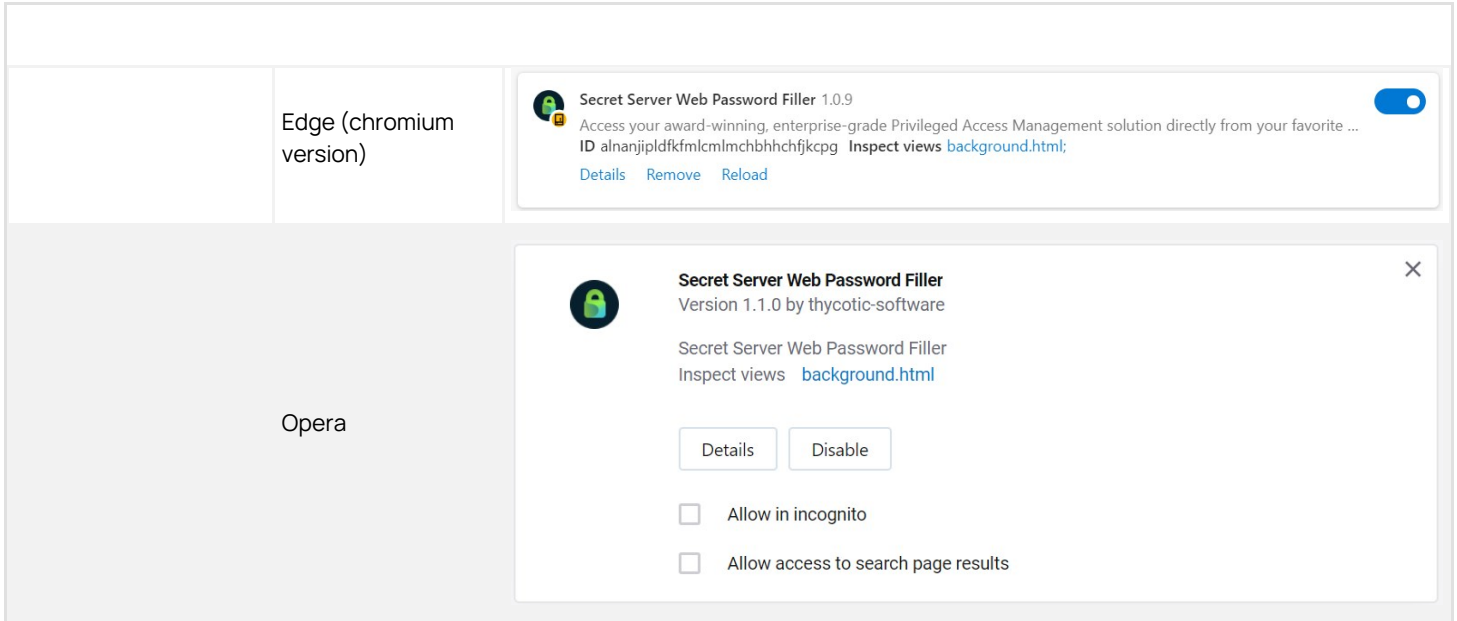
To help eliminate any potential confusion for terminology for the different browser add-ons, this section will review what terms were being used for each add-on and provide some visual points.

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

- WPF
- Web Password Filler
- Password Filler

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

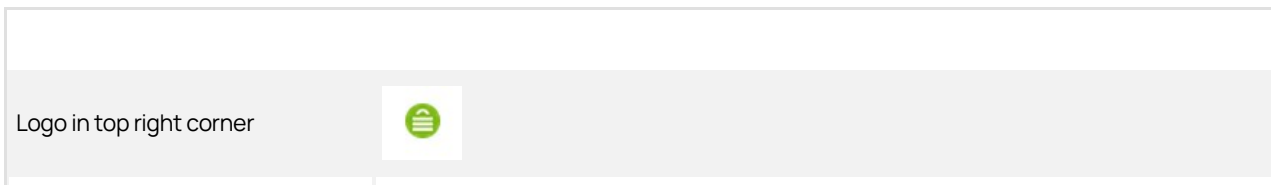
Logged Out	(In top right corner)	
Logged In	(In top right corner)	
Application in Browser (Settings Menu)		
Item on Extensions / Add-On page	Chrome	
	Firefox	









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:



Application in Browser	<div data-bbox="483 289 1323 1100"><h3>Secret Server Login Assist</h3><p>HAVE A SECRET FOR THIS URL?</p><p>All matching Secrets will be listed below the password field.</p></div>
Drop down option on field	<div data-bbox="483 1142 976 1297">  <p>No Matching Secrets found.</p></div>
Item on Extensions / Add-On page	<div data-bbox="483 1339 1339 1787"><p>Secret Server Login Assist 1.0.16</p><p>ID: pbemhiacephlgacdahceanbbiokmgldb Inspect views background.html</p><p>Details Remove </p></div>



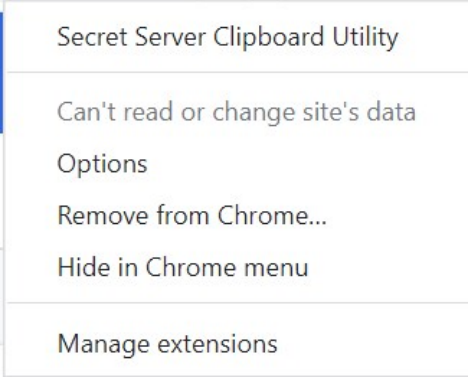
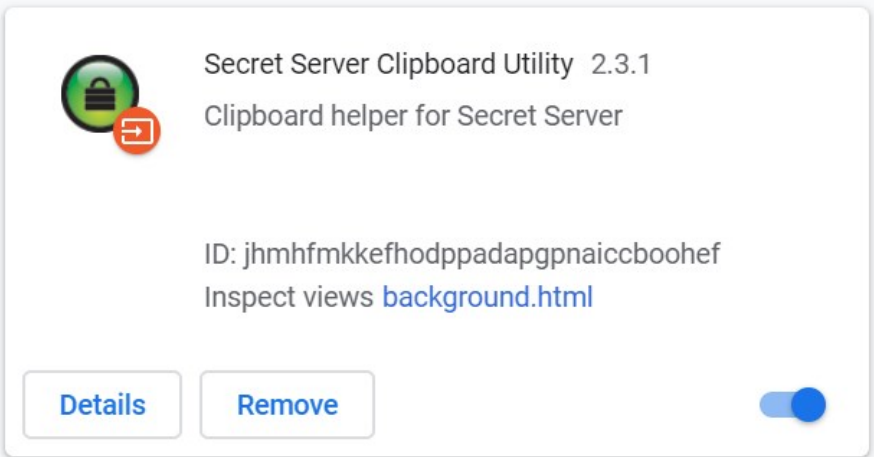

This is the Clipboard Utility that was available with previous versions of Secret Server. The options and functionality of this extension have NOT be added into the NEW Web Password Filler (as of Feb 28, 2020).

Also refer to [June 2020 - Bulletins and Technical Notes](#).

It is typically referred to as:

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

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

Logo in top right corner	
or	
Application in Browser	 <ul style="list-style-type: none">Secret Server Clipboard UtilityCan't read or change site's dataOptionsRemove from Chrome...Hide in Chrome menuManage extensions
Item on Extensions / Add-On page	 <p> Secret Server Clipboard Utility 2.3.1 Clipboard helper for Secret Server</p> <p>ID: jhmhfmkkefhodppadapgpnaiiccboohef Inspect views background.html</p> <p>Details Remove <input checked="" type="checkbox"/></p>

Native Messaging Host

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

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

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

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

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

Download Location

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

Requirements

- .NET version 4.5.2
- Thycotic Web Password Filler version 2.0.3 and later

Supported Browsers

- Chrome
- Edge Chromium
- FireFox
- Opera

Additional information regarding Native Messaging can be found at

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

Installation

The user installs the Thycotic 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 Thycotic Native Messaging Host

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

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

Establishing Default Settings and Browser-Specific Overrides

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

```

{
  Browser
  IDs {
    "chromeExtensionId": "mfpddejbpnbjckjoaicfedaljnfeollkh",
    "edgeExtensionId": "kjldmpkefedgljefehmmfifbhnjngmbh",
    "operaExtensionId": "eemnnaadjdfcpkcpalolohpepihhbbo",
    "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": [
      {
        Default
        Overrides
        per Browser {
          "id": "mfpddejbpnbjckjoaicfedaljnfeollkh",
          "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 Thycotic 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": "mfpddejbpnbjckjoaicfedaljnfeollkh",
  "edgeExtensionId": "kjldmpkefedgljefehmmfifbhnjngmbh",
  "operaExtensionId": "eemnnaadjdfcpkcpalolohpepihhbbo",
  "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": "mfpddejbpnbjkjoaicfedaljnfedllkh",
    "ConfigSSUrl": "https://SomeURL/SecretServer",
    "ConfigDomain": "",
    "HideConfigPage": true,
    "HideSettingPage": false,
    "SettingUserSSLogin": true,
    "SettingPrompToSave": true,
    "SettingShowPopup": true,
    "SettingHideReadOnlyFolders": true,
    "SettingEnableAutoPopulate": true,
    "EnableForAllUsers": false,
    "PopupDefaultPosition": false,
    "ExactMatchUrl": true,
    "maxSessionRecordingLimit": 120,
    "Exclude": [
      "http://*",
      "http://endoftheinternet.com",
      "https://www.MyCompanySite.com",
      "https://live.com/"
    ],
    "ExcludeException": [
      "https:// MyCompanySite.com/Login.html",
      "https://login.live.com/login.srf"
    ]
  },
  {
    "id": "kjldmpkefedgljefehmmfifbhjngmbh",
    "ConfigSSUrl": "https://localhost/SecretServer/",
    "ConfigDomain": "",
    "HideConfigPage": false,
    "HideSettingPage": false,
    "SettingUserSSLogin": false,
    "SettingPrompToSave": false,
    "SettingShowPopup": false,
    "SettingHideReadOnlyFolders": false,
    "SettingEnableAutoPopulate": false,
    "PopupDefaultPosition": false,
    "ExactMatchUrl": false,
    "maxSessionRecordingLimit": 120,
    "Exclude": [ "http://" ],
    "ExcludeException": []
  },
  {
    "id": "dd1e31d5-3623-45cb-b1ad-64074d36b360@thycotic.com",
    "HideConfigPage": false
  },
  {
    "id": "eemnadjdfcpkcnpalolohpepihbbo"
  }
]
}

```

Where:

chromeExtensionID	"mfpddejbpnbjkjoaicfedaljnfedllkh"	This is the ID required for the Chrome browser registration.
edgeExtensionId	"kjldmpkefedgljefehmmfifbhjngmbh"	This is the ID required for the Edge browser registration.
operaExtensionId	"eemnadjdfcpkcnpalolohpepihbbo"	This is the ID required for the Opera browser registration.
firefoxExtensionId	"dd1e31d5-3623-45cb-b1ad-64074d36b360@thycotic.com"	This is the ID required for the Firefox browser registration.

ConfigSSUrl	"https://SomeURL/SecretServer"	This is the URL for your Secret Server instance.
ConfigDomain	"local"	This is the domain identification either local or your corporate network domain.
HideConfigPage	false	Boolean that controls if the Configuration tab is visible or not.
HideSettingPage	false	Boolean that controls if the Settings tab is visible or not.
SettingUserSSLogin	true	Boolean that sets the checkbox to enable the Secret Server Login option.
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 Thycotic checkmark.
SettingHideReadOnlyFolders	true	Boolean that sets the checkbox to enable the Hide Read Only Folder option.
SettingEnableAutoPopulate	true	Boolean that sets the checkbox to enable the Auto Populate option for secrets and passwords.
EnableForAllUsers	false	Boolean specifying if the Native Messaging Host is available under the local user context only or made available for all users. If set to true, it allows all users on the machine to access the settings.json file as long as it's in a shared location. If set to false it only applies to the current logged in user no matter where the file is stored. Changes impacting the registry keys also require admin permissions if EnableForAllUsers is set to true.
PopupDefaultPosition	true	Boolean that positions the menu in the upper right corner of the screen. If false the popup appears below the credentials fields.
ExactMatchUrl	false	Boolean that configures WPF to recognize only exact URL matches
maxSessionRecordingLimit	120	The number of minutes allowed for a session recording. Default is 120 minutes and maximum allowed is 480 minutes.
Exclude	[list]	Refer to Site Exclusions and Exceptions below. Accepts wildcards.
ExcludeException	[list]	Refer to Site Exclusions and Exceptions below. Does NOT accept wildcards.
PerExtensionOverride	Contains a section for each browser type, with custom values for the 15 settings described in this table (ConfigSSUrl, ConfigDomain, HideConfigPage, etc.).	If a value in this section differs from the default value established at the top of the JSON file, the value here takes precedence for that browser, and overrides the default value.

Site Exclusions and Exceptions

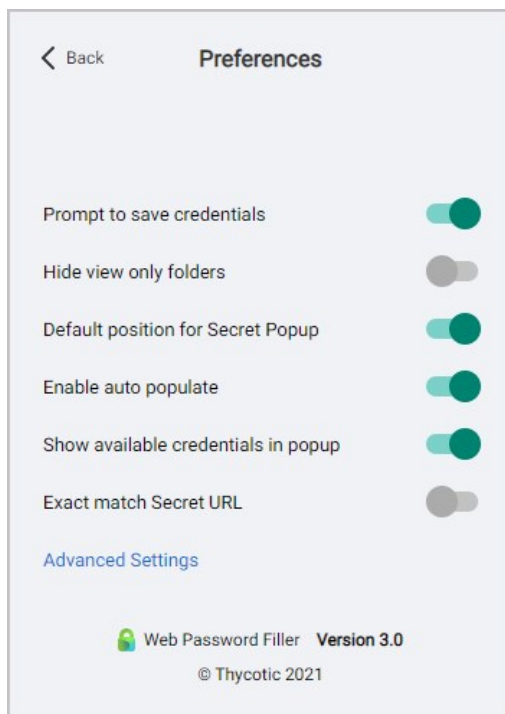
The Thycotic Web Password Filler is an “inclusive” extension. Any website that contains a username and password has the potential to have a secret retrieved from or stored in Secret Server. However, some sites are simple web forms that contain user name, password and a variety of other field types. Registration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

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

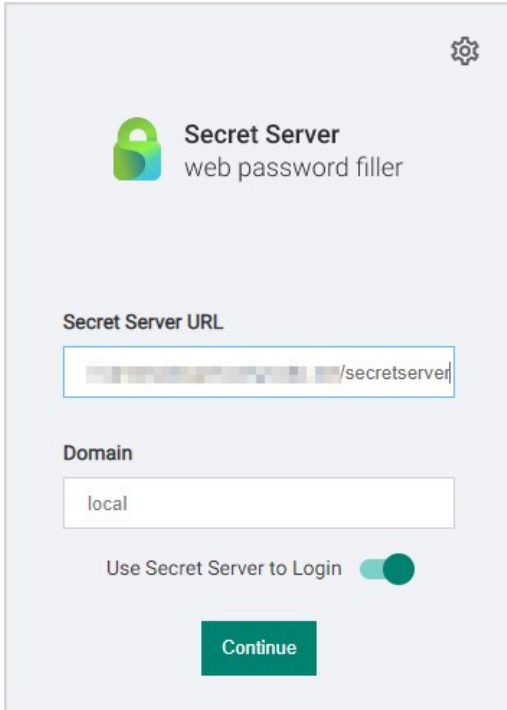
Note: Only the “Exclude” section accepts a wild card. The “ExcludeException” must be the exact URL without a query string.

UI Behavior Based on Preferences

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



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



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

Error Messages

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

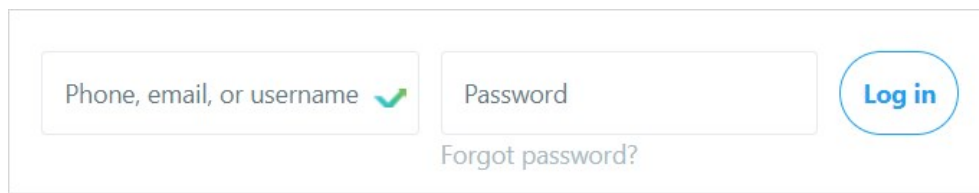
- The following error message indicates that there are missing elements in the `settings.json`.
There are elements missing from `settings.json`. Review the documentation and update `setting.json` with the missing attributes.
Review the `settings.json` format and ensure all elements are provided and the json is well formatted.
- The following message indicates that the setting "EnableForAllUsers" is set to true; however, the user attempting to register the Thycotic Native Messaging Host does not have administrator permissions and cannot update or create the hkey local machine registry key required for browser registration.
This application must be run as an administrator when registering for All Users
- The following error message indicates that 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.

Using WPF

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

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

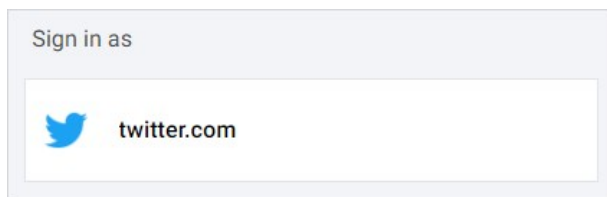
1. Take a quick look at your WPF button on your browser's button bar. If it is grayed out, you will need to sign into Secret Server and return here.
2. Navigate to the website you want to access. Note there is a green Thycotic logo in the site's account name text box:



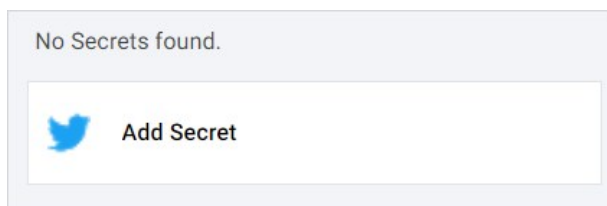
The screenshot shows a login form with two input fields: "Phone, email, or username" and "Password". A green checkmark is visible in the username field. To the right of the password field is a blue "Log in" button. Below the password field is a link that says "Forgot password?".

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

3. Click the Thycotic 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:

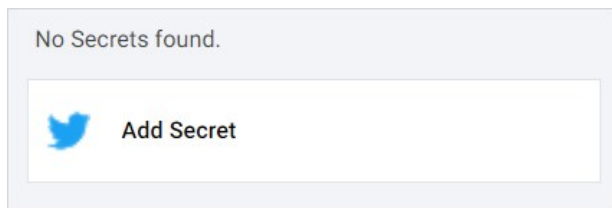


If you see the second possibility, you need to set up a secret for that website. See [Creating a Secret for a Website](#).

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

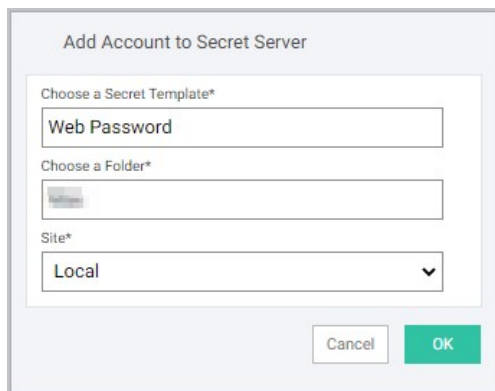
Creating a Secret for a Website

1. Navigate to the **create a new account** form on the website you want to create a secret for.
2. Click the Thycotic icon in the password text box. A modal appears:



You can also select the username or password fields and right-click and go to ___Password Filler | Add Secret___.

3. Click the **Add Secret** button. The **Add Account to Secret Server** modal appears:



4. Begin typing "web" in the **Choose a Secret Template** search box. The word Web Password will appear in a dropdown list. By default, WPF tries to add the standard Web Password template for you. You can search for a different template.
5. Click the **Web Password** suggestion. The search box is populated with it.
6. Type the name of the Secret Server folder in which you want the secret to reside. If you did not already set one up, by default, Secret Server creates a folder titled with your Secret Server username. Click to select the desired folder in the drop-down that appears. By default, WPF tries to select the personal folder for the username that you used for the login. If one does not exist, you will need to specify which folder to save it to.
7. Click **OK**. Another **Add Account to Secret Server** modal appears:

Add Account to Secret Server

Secret Template	Web Password	Change
Folder		Change
Site Name	Local	Change
Secret Name	login. .com	
URL	https://login. .com/gsp/static	
UserName	[blurred]	
Password	*****	Generate
Notes	[empty text area]	

[Cancel](#) [Add](#)

Secret Server fills in some of the text boxes for you based on the current website.

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

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

Mapping Login Fields

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

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

The screenshot shows a dialog box titled "Add Account to Secret Server". It contains several configuration fields: "Secret Template" (Web Password), "Folder" (Max), "Site Name" (Local), "Secret Name" (www. .com), "URL" (https://www. .com/Accour), "User Name" (empty), "Password" (empty), and "Notes" (empty). A "Generate" button is next to the Password field. A tooltip is visible over the Password field, stating "Drag this to the Password field on the page". At the bottom are "Cancel" and "Add" buttons.

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

The screenshot shows a web page form with a "Password" label above a text input field. The input field contains the text "Password" and has a "Show" button to its right.

The field mapping function in the Web Password Filler can be enabled by a user with Administer Metadata permissions. Field mapping can also be enabled on an existing secret if an administrator with access to the secret creates the metadata section, **WPFHints**. The user can then create any metadata field values (string values with the XPath to the field that should be populated) in the **WPFHints** section to populate the site.

Main Site Tests > commandcontroller.com ☆

General Sharing Settings Metadata

WPFHints

Password id("passwordField")

UserName id("userNameField")

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.

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://thycotic.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://thycotic.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.

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.thycotic.com`, and then opens a tab for `blue.thycotic.com`, session recording will continue on `blue.thycotic.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.

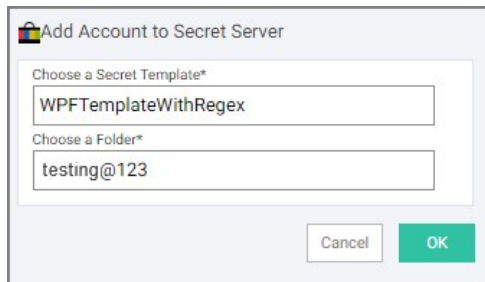
RegEx is a sequence of patterns specified in Secret Server templates and provided to be specified as **OtherUrls** during account setup in Web Password Filler (WPF), allowing session recording on redirected websites.

When a user is logged into a website using a secret and session recording is enabled, WPF will record a session for that URL. If a user is redirected to another URL and session recording should continue for the redirected URL, those URLs can be added in the **OtherUrls** field when the account is added. Currently this field supports only URLs.

Note: That as soon as a URL is accessed for a website and secret with session recording enabled, session recording will capture everything the user does, even if the user changes a password for that secret.

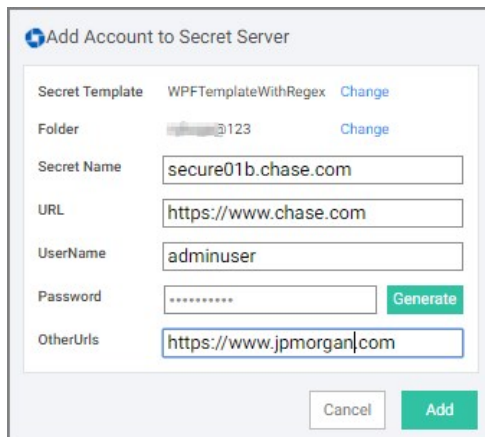
Using RegEx in WPF

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



The screenshot shows a dialog box titled "Add Account to Secret Server". It has two input fields: "Choose a Secret Template*" with the value "WPFTemplateWithRegex" and "Choose a Folder*" with the value "testing@123". At the bottom right, there are "Cancel" and "OK" buttons.

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



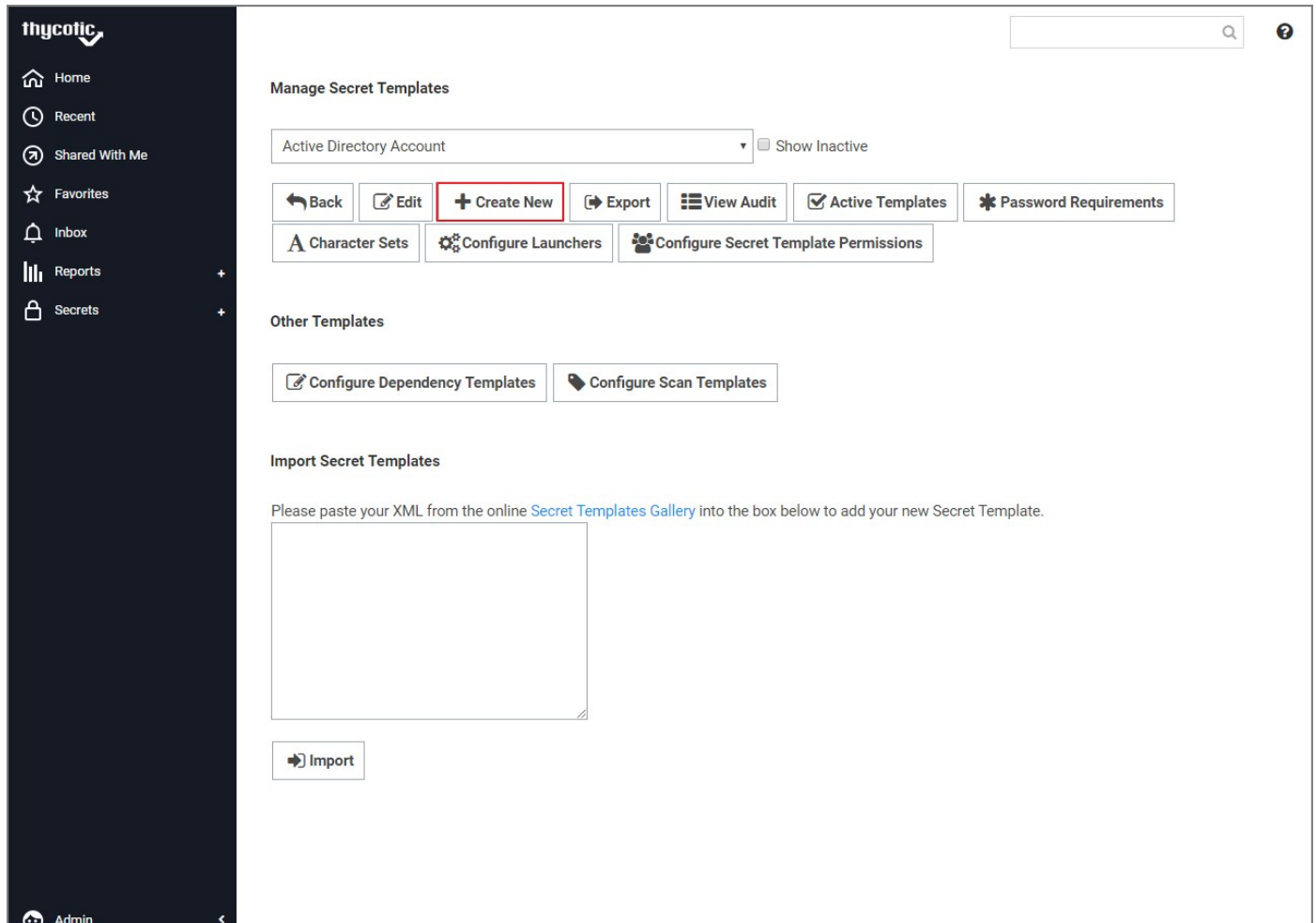
The screenshot shows the "Add Account to Secret Server" dialog box with the following fields and values: "Secret Template" (WPFTemplateWithRegex), "Folder" (testing@123), "Secret Name" (secure01b.chase.com), "URL" (https://www.chase.com), "UserName" (adminuser), "Password" (masked with asterisks), and "OtherUrls" (https://www.jpmorgan.com). There are "Cancel" and "Add" buttons at the bottom right.

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

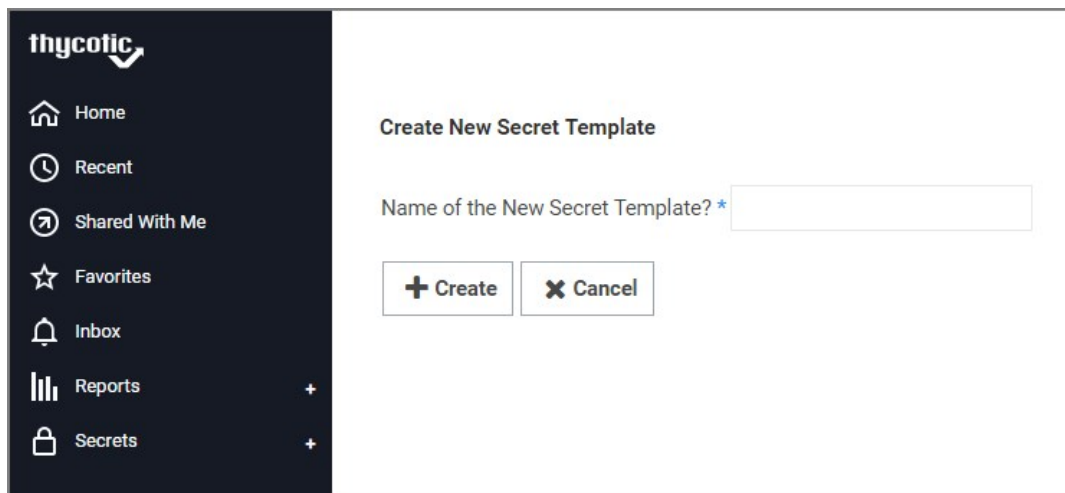
4. Click **Add**.

Setup in Secret Server

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



2. Click **Create New**.
3. Name the new secret and click **Create**.



4. On the **Settings** page, click **Configure Extended Mappings**.

FIELDS				
FIELD NAME	FIELD SLUG NAME	FIELD DESCRIPTION	FIELD TYPE	IS REQUIRED
userid	userid	userid	Text	✓
password	password	password	Text	✓
Url	url-	URL	Text	✓
Secretname	secretname	secret name	Text	✓
OtherUrls	otherurls	other urls for session recording	Text	✓

Text ▼

✖

Show Inactive Fields

← Back
⚙️ Configure Password Changing
🌐 Configure Launcher
🔗 Configure Extended Mappings
📄 View Audit

5. On the **Secret Template Extended Mappings** page click **Add New Mapping**.

Secret Template Extended Mappings

Extended Mapping to use Regex List ▼

Regex List Field OtherUrls ▼ *

Save

✖ Cancel

1. From the **Extended Mapping to use** drop-down select **Regex List**.
2. From the **Regex List Field** drop-down select **OtherUrls**.
3. Click **Save**.

The template is now ready to be used in WPF.

If you have session recording enabled for two secrets that contain the same primary or secondary domain (e.g. microsoftonline.com) and the same host name (e.g. microsoftonline.com) AND both secrets are used, WPF will close the first session when the second session is selected, closing the tabs associated with the first secret. This is expected behavior, ensuring that the only sessions recorded are those associated with secrets that require session recording. Sites like *microsoftonline* only allow one login / active credential at a time.

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

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

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

Incognito Support

Follow these pre-requisite steps to ensure WPF can launch secrets in incognito mode:

1. On the secret via the secret template in Secret Server enable the setting **Web Launcher required Incognito Mode**.
2. On the extension's management page, enable/allow the following setting for:
 - Chrome: **Allow in incognito**
 - Edge: **Allow in InPrivate**
 - Firefox: **Run in Private Windows**
 - Opera: **Allow in incognito**
 - Safari: **Run in Private Window**
3. Login to WPF.

Port Numbers

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

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

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

List of Primary and Secondary Domains

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

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

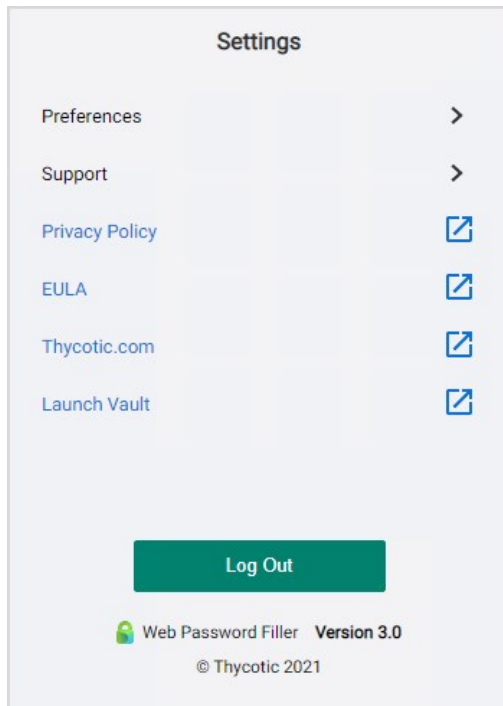
Logout of Secret Server

Use the WPF icon to logout:

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



2. The WPF logout modal opens.



Click **Logout**.

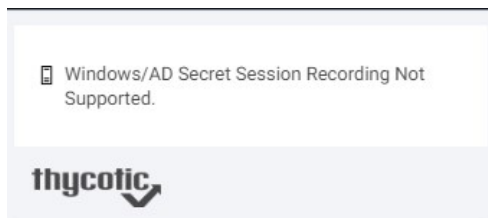
3. The WPF icon changes to:



Windows Admin Center Support

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

- New user name will default/use a web password template only (Windows and AD templates are not supported)
- Using the "Connect" button in Windows Admin Center, will not show secrets associated with the selected machine
 - Work around: Select the machine link to retrieve the associated secrets
- Updating passwords will update the password in the current secret regardless of template
- How secrets are returned:
 - Secrets with Host Name (As machine name)
 - link text --> IP (Host Name) --- Secrets will be returned
 - link text --> Host Name --- Secrets will be returned
 - link text --> IP Address --- Secrets will NOT be returned
 - Secrets with IP Address (As machine name)
 - link text --> IP(Host Name) --- Secrets will NOT be returned
 - link text --> Host Name --- Secrets will NOT be returned
 - link text --> IP Address --- Secrets will be returned
- Session Recording of non-web password templates is not allowed. If an attempt to use a secret to log into an RDP session is made and the secret has session recording enabled, WPF will not allow the user to proceed and display the following message.

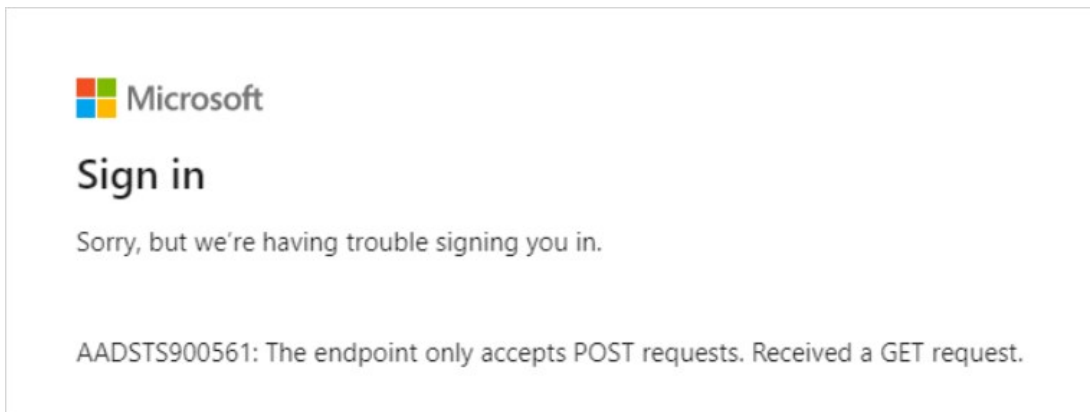


Using Web Password Filler with Microsoft Online Services

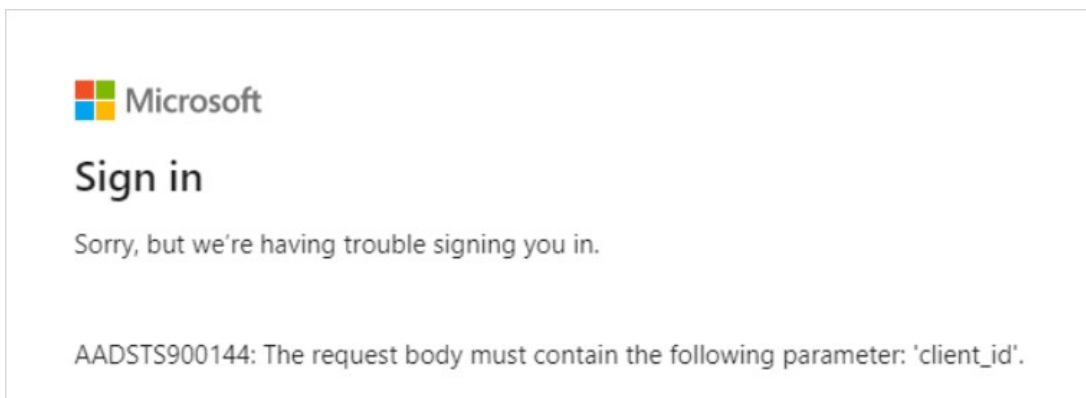
This section guides users through using the Web browser extension to use Secret Server WPF to login to Microsoft Online. Launching Microsoft Online secrets with WPF takes a bit of extra configuration. This section explains the issue and suggests remedies.

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

When you try to open a Microsoft Online secret with WPF, you might see



or



Neither of these errors provide a useful explanation. The real issue is simple with a very easy solution that you can implement yourself.

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

The original (errant) stored URL is:

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

The permanent (real) URL is:

<https://login.microsoftonline.com>

So all that is needed is to ensure the secret stores the permanent URL, not the origin one.

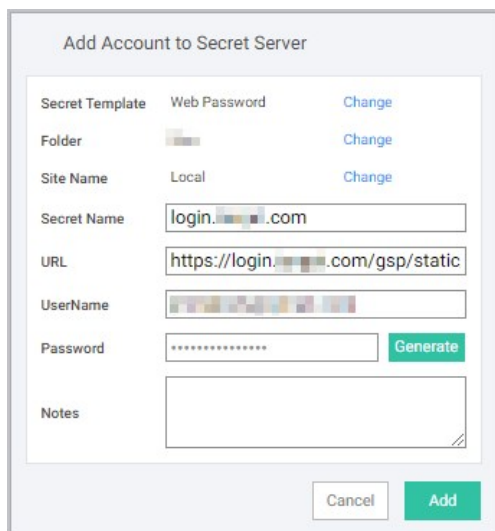
There are two ways to do this:

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

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

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

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



The screenshot shows a dialog box titled "Add Account to Secret Server". It contains several fields and buttons:

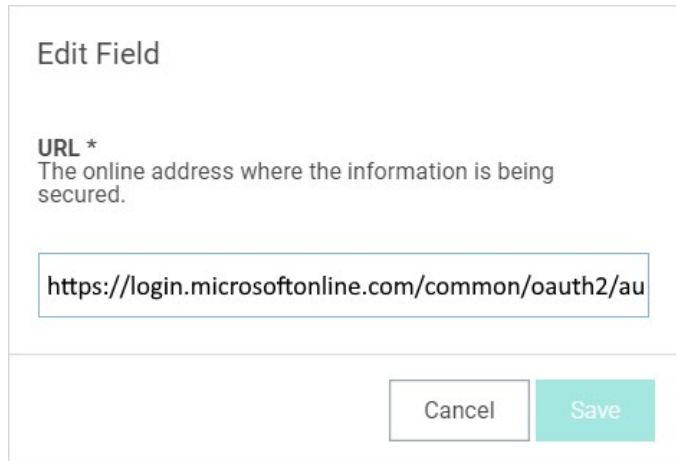
- Secret Template: Web Password (with a "Change" link)
- Folder: (with a "Change" link)
- Site Name: Local (with a "Change" link)
- Secret Name: login.microsoft.com
- URL: https://login.microsoft.com/gsp/static
- UserName: (with a masked input)
- Password: (with a masked input and a "Generate" button)
- Notes: (with a text area)
- Buttons: "Cancel" and "Add" at the bottom.

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

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

1. Login to SS.

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



Edit Field

URL *
The online address where the information is being secured.

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

Cancel Save

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

Troubleshooting

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

- [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](#)

Investigating WPF Issues

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

Confirm that the issue is with the new Web Password Filler that was first released in Dec 2019 and in conjunction with Secret Server v10.7.59.

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

What browser is the issue occurring on?

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

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

- If the issue only happens on one site, what is the URL for that site?
For example, if the issue only occurs on Facebook, then we need the URL for the Facebook page that the browser is on when it fails.
- For issues of the WPF login failing, if you change the web page you are on when you try to login does it still occur?
- We will always want to know what **URL** you are on when an issue occurs, since some web pages might be trying to interfere with WPF.

How are you accessing the site to use WPF?

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

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

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

Basic steps to get this value are:

1. Go to the Settings menu in the browser. This 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.

What type of action are you trying to perform?

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

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

This includes filling credentials for a site

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

What Secret template are they using?

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

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

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

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

WPF Login

Are you logged into WPF?

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

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

1. Not Logged in



2. Logged in



There are two different Login methods, which login method is being used?

1. The two login methods are Username/Password and Login through Secret Server (for SAML). Refer to the Secret Server documentation on [SAML](#).

Previous Products Compatibility

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

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

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

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

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

Behavior/Problem Presentation

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

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

Some examples:

1. Is the user not able to login to WPF?
 - Are they getting any error messages?
 - Are they logging in and then getting logged out again?
 - What authentication types are enabled and are they using them?
 - Is the "Login" button greyed out?
 - Is the Secret Server URL (and optional: Domain) entered in the "Configuration" tab?
 - Can they reach the Secret Server UI from the same machine/browser?
2. Is the Secret not being displayed on the site?
 - Is there only one Secret for the site?
 1. If Yes, then are all the Secret not being displayed? Or just some Secrets not displayed?
 - Does the logged in account have access to that Secret?
3. Are the credential fields populated correctly?
 - If No, what fields are being populated?
 - Is the green Thycotic check logo displayed in the Username/email field?
 1. We ONLY display this in the Username or email fields, it is NOT displayed in the password field
 - Are the right-click options available in any of the login fields?
 - Which fields are not populated?
 - Are they populated and put in the wrong spot?
 - Does the site require a drop-down or other action to be taken before the credential fields are available?
 - Does the site use a multi-page login (like O365)? Or single page log (like LinkedIn)?
4. Is it some kind of visual issue on the page?
 - Is the green Thycotic log visible?
 - Is the green Thycotic logo in the wrong place on the page?
 - Is the page displaying as blank?
 - Are the icons for the Secrets not showing up?
5. Is it a newly added Secret that is not showing up?
 - When a Secret is added in Secret Server or in WPF there are times when it might not appear immediately on the site. WPF relies on the Secret being indexed in SS, and it typically takes some time for that index to happen (depending on the size of the environment).
 - Usually if you wait a few minutes and refresh the page you should be able to see it appear.

- In Release 1.1.0 of WPF a short-term caching option was introduced. This is indicated by a refresh button on the drop down for the credentials. This caching means that we should keep the Secret in memory for that browser session so we don't have to wait for Secret Server to index it.

6. Is there some kind of other issue happening? If so, what?

Information on Security Scans

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

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

Checkmarx Results



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

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

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

Filter Settings

Severity

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

Result State

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

Assigned to

- Included: All

Categories

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

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

- Excluded:

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

Results Limit

Results limit per query was set to 500.

Selected Queries

Queries cannot be displayed because the report contains no results.

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

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

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

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

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

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

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

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

I Category | Issues Found | Best Fix Locations¹ | -----|-----|-----| PCI DSS (3.2) - 6.5.1 - Injection flaws - particularly SQL injection [^2] | 0 | 0 | PCI DSS (3.2) - 6.5.2 - Buffer overflows | 0 | 0 | PCI DSS (3.2) - 6.5.3 - Insecure cryptographic storage [^2] | 0 | 0 | PCI DSS (3.2) - 6.5.4 - Insecure communications [^2] | 0 | 0 | PCI DSS (3.2) - 6.5.5 - Improper error handling | 0 | 0 | PCI DSS (3.2) - 6.5.7 - Cross-site scripting (XSS) [^2] | 0 | 0 | PCI DSS (3.2) - 6.5.8 - Improper access control | 0 | 0 | PCI DSS (3.2) - 6.5.9 - Cross-site request forgery | 0 | 0 | PCI DSS (3.2) - 6.5.10 - Broken authentication and session management [^2] | 0 | 0 |

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

Scan Summary - FISMA 2014

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

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

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

Scan Summary - NIST SP 800-53

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

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

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

Scan Summary - OWASP Mobile Top 10 2016

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

is for issues where cryptography was attempted, but it wasn't done correctly.

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

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

Scan Summary - Custom

1		
Must audit	0	0
Check	0	0
Optional	0	0

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

Release Notes

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

- [3.0.1 Release Notes](#)
- [3.0.0 Release Notes](#)
- [2.0.6 Release Notes](#)
- [2.0.5 Release Notes](#)
- [2.0.4 Release Notes](#)
- [2.0.3 Release Notes](#)
- [2.0.2 Release Notes](#)
- [2.0.1 Release Notes](#)
- [2.0.0 Release Notes](#)
- [1.1.0 Release Notes](#)
- [1.0.10 Release Notes](#)
- [1.0.9 Release Notes](#)
- [1.0.8 Release Notes - initial release](#)

3.0.1 Hot Fix Release Notes

August 3, 2021

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.

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

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

3.0.0 Release Notes

July 16, 2021

- **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 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.
- **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.
- 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/>

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, Thycotic 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

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

The secret (under the Security tab) has

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

Choose one of these three work-arounds:

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

2.0.6 Release Notes

May 25, 2021

Web Password Filler now provides improved performance for session recording.

- 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.

- 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 Thycotic checkmark, then select the desired secret to populate.

2.0.5 Release Notes

March 30, 2021

- 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 Thycotic 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 Thycotic checkmark logo in a credentials field, clicking Secret Server Web Password Filler, and clicking Refresh Secrets. See [Native Messaging Host](#).
-
- 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 Storewise V7000
 - Imperva Securesphere Management

- Kaseya VSA, Daffron Customer Information Systems
- Oracle netsuite and slm.saas.services
- Various sites reported by IH Mississippi Valley Credit Union
- Various internally-developed Web apps
- <http://isupportsvr1/rep>
- <http://premieragent.zillow.com/crm/agentlogin>
- <https://cmpame.cmpa.org>
- <https://comp.makonetworks.com>
- <https://hqprsa02.cmpa.org:7004/console-ims>
- <https://nystateofhealth.ny.gov/>
- <https://prtg.centergrid.com/>
- <https://secure.trust-provider.com/>
- www.logicmonitor.com

- 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.

- 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.

2.0.4 Release Notes

December 23, 2020

- 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.

- 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>

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

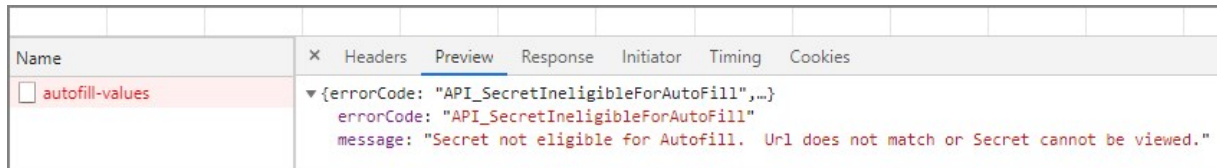
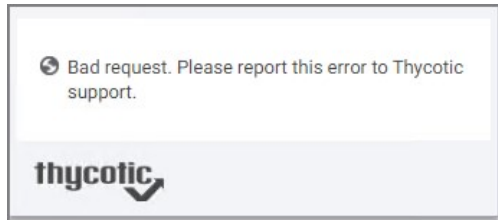
2.0.3 Release Notes

- 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)
- 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.
- 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 Thycotic 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://thycotic.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>
- A delay may occur and trigger an error message due to indexing on the Secret Server side after a URL change for Secrets that are setup

for an exact URL match. The error message will state that the exact domain doesn't exist.



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

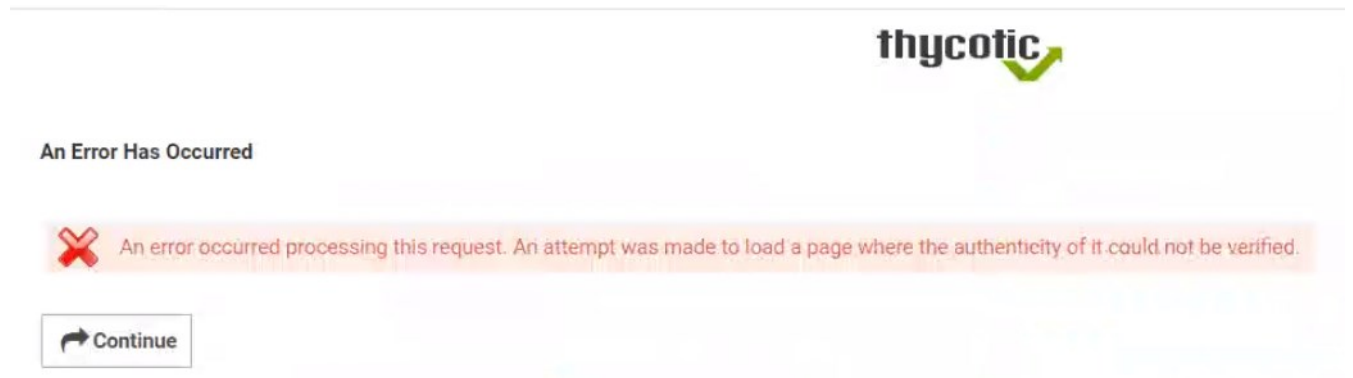
2.0.2 Release Notes

- 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.

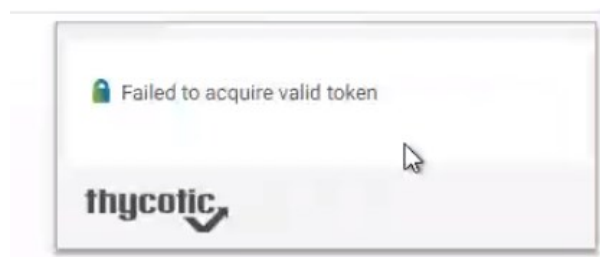
LAUNCHER SETTINGS	
Enable Launcher	Yes
Launcher Deployment Type	Protocol Handler
Enable Protocol Handler Auto-Update	Yes
Send Secret URL to Launcher	Yes
Allow Secret Server to Retrieve Website Content	Yes
Allow Web Launcher Mappings to be Downloaded	Yes
Allow Web Launcher Mappings to be Uploaded Off-site	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 Thycotic check logo in the field.
- Resolved an issue when a website used multi-page logins or page redirect during while launching a web password secret from Secret Server, resulting in Secret Server sending a different URL to Web Password Filler. This is resolved by the above Secret Server-side check and setting the launcher option in Secret Server.
- Resolved an issue that prevented the password from being filled for logins on sites:
 - www.businessdirect.att.com
 - login.tenable.com
- Resolved an issue where Secret Server instances that use Windows Authentication caused Web Password filler to prompt users to generate a new login token (for a second time) even if they had already generated a token.
- 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.
- If you have multiple identity providers and attempt to log in multiple times (for example, open WPF and click login, then open WPF again and click login a second time) an error is triggered after clicking the login button the second time, and one of the following messages can appear:
 - Secret Server displays an error that the authenticity of the page could not be verified.



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



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

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

2.0.1 Release Notes

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

2.0.0. Release Notes

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

1.1.0. Release Notes

- 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.

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

Firefox Specific

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

1.0.10 Release Notes

- 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.

1.0.9 Release Notes

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

1.0.8 Release Notes

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

- Authenticate back to the Secret Server instance without directly logging into the Secret ServerUI – via REST API
 - Support Username/Password style login
 - Support Secret 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

Documentation Changelog

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

- [Release Notes](#)

- [Release Notes](#)

- [Release Notes](#)

- [Release Notes](#)

- [Release Notes](#)

2.0.3 Release Updates

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

- Added [Security Scans](#) section.