Delinea

Web Password Filler

Administrator Guide

Version: 3.11.x

Publication Date: 5/15/2026

© Delinea, 2026

Web Password Filler Administrator Guide

Version: 3.11.x, Publication Date: 5/15/2026

© Delinea, 2026

Warranty Disclaimer

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

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

Disclaimer of Liability

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

Table of Contents

Web Password Filler 1

Getting Started 1

- Enabling Web Services in Secret Server 1
- Connecting to the Delinea Platform and Secret Server 1
  - Connecting to the Delinea Platform 2
  - Connecting to Secret Server 4
  - Logging in Locally 6
  - Specifying Default Protocols 7
  - Redirecting to Secret Server via Hyperlink 8
- Reviewing Terminology 9
  - Using Web Password Filler with Secret Server 9
- Installing Browser Extensions 11
- Navigating the Preferences Menu 11

Deploying Web Password Filler in Air-Gapped Environments 14

- Download the Extension 14
- Prepare for Deployment 14
- Deploying Extensions with Group Policy 14
- Configure Permissions and Restrictions (Optional) 14

Using WPF 15

- Logging in to a Website 15
- Accessing Secrets Guarded by MFA 16
- Autofilling OTP 17
- Recording Web Sessions 18
  - Session Recording Disconnecting Warning 19
  - Managing Session Recording Limits 21
    - Using RegEx 21
- Launching Comma-Separated URLs 25
  - Creating a Secret Template 25
  - Using the Custom Web Launcher 29
- Setting Comment Requirements 31
  - Requiring Comments When Enabling the 'Hide Secret Server Version Number' Setting 31
- Creating a Secret for a Website 32
  - Selecting a Folder 34
  - Adding Accounts 34
  - Syncing Recent and Favorite Lists with Secret Server 36
  - Refreshing the Recent and Favorites List 36
- Mapping Login Fields 38
  - Mapping Web Page Form Fields to Secret Fields 39
  - Enabling Field Mapping with Metadata 40
- Supporting Incognito Mode 40

Logging Out of Secret Server 41
Using Web Password Filler with Microsoft Online Services 42
Identifying the Problem 42
Understanding the Issue 43
Fixing the Issue When Creating the WPF Secret 43
Fixing the Issue After Having Saved the WPF Secret 44
Managing Port Numbers 45
Certificate Requirements for Web Password Filler in Chrome 45
Supporting Windows Admin Center 46

Securing Web Password Filler 47

Setting Up the Native Messaging Host 47
Downloading the Native Messaging Host 47
Software Requirements 47
Supported Browsers 47
Installing and Registering the Native Messaging Host 47
Uninstalling the Native Messaging Host 48
Configuring Web Password Filler Settings 48
Establishing Default Settings and Browser-Specific Overrides 48
Example settings.json File 49
Configuring Boolean and Session Settings 51
Settings Reference 51
Excluding Sites and Making Exceptions 55
Setting UI Behavior Based on Preferences 55
Managing Error Messages 57
Preventing Users from Disabling Session Recording 58

Troubleshooting 59

Addressing Usability Issues 59
Logging in with Web Password Filler 60
Choosing a Login Method 60
Troubleshooting Login Issues in Chrome or Edge 60
Enabling Diagnostic Logging 60
Managing Compatibility with Previous Products 61
Presenting Behaviors and Problems 61
Investigating WPF Issues 62
Confirming WPF Version 62
Identifying the Problematic Browser 63
Identifying the Affected Sites 63
Determining Site Access 63
Identifying the WPF Version with the Issue 63
Performing the Action 64
Using Templates 64

Release Notes 64

2025 Release Notes 64

3.11.9 Release Notes ... 64
Improvements ... 65
Fixed Issues ... 65
3.11.8 Release Notes ... 65
Fixed Issues ... 65
3.11.7 Release Notes ... 65
Improvements ... 65
Fixed Issues ... 65
3.11.6 Release Notes ... 66
Fixed Issues ... 66
3.11.5 Release Notes ... 66
Improvements ... 66
Fixed Issues ... 66
3.11.4 Release Notes ... 66
Fixed Issues ... 67
3.11.3 Release Notes ... 67
Improvements ... 67
Fixed Issues ... 67
3.11.2 Release Notes ... 67
Improvements ... 68
Fixed Issues ... 68
2024 Release Notes ... 68
3.11.1 Release Notes ... 68
Improvements ... 68
Fixed Issues ... 68
3.11.0 Release Notes ... 68
Improvements ... 69
Fixed Issues ... 69
3.10.3 Release Notes ... 69
Fixed Issues ... 69
3.10.2 Release Notes ... 69
Bug Fixes ... 69
3.10.1 Release Notes ... 70
Bug Fixes ... 70
3.10.0 Release Notes ... 70
Improvements ... 70
Bug Fixes ... 70
3.9.6 Release Notes ... 70
Enhancements ... 70
Bug Fixes ... 70
3.9.5 Release Notes ... 71
Bug Fixes ... 71
3.9.4 Release Notes ... 71
Improvements ... 71

Bug Fixes ... 71
3.9.3 Release Notes ... 72
Bug Fixes ... 72
3.9.0 Release Notes ... 72
Improvements ... 72
Bug Fixes ... 72
3.8.0 Release Notes ... 73
Improvements ... 73
Bug Fixes ... 73
Known Issues ... 74
2023 Release Notes ... 74
3.7.1 Release Notes ... 74
Bug Fixes ... 74
3.7.0 Release Notes ... 74
Features ... 74
Improvements ... 75
Bug Fixes ... 75
3.6.1 Release Notes ... 75
Bug Fixes ... 76
3.6.0 Release Notes ... 76
Features ... 76
General Improvements ... 76
Security Improvements ... 76
Bug Fixes ... 76
Known Issues ... 76
3.5.4 Release Notes ... 76
Improvements ... 77
Bug Fixes ... 77
3.5.3 Release Notes ... 77
Features ... 77
Bug Fixes ... 77
3.5.2 Release Notes ... 77
Features ... 77
Bug Fixes ... 77
Known Issues ... 78
3.5.1 Release Notes ... 78
Bug Fixes ... 78
Known Issues ... 78
3.5.0 Release Notes ... 78
Features ... 78
Bug Fixes ... 78
Known Issues ... 78
3.4.4 Release Notes ... 78
Bug Fixes ... 78

3.4.3 Release Notes 79
Features 79
Security Improvements 79
Bug Fixes 79
2022 Release Notes 79
3.4.2 Release Notes 79
Features 79
General Maintenance 79
Bug Fixes 79
Known Issues 80
3.4.1 Release Notes 80
Bug Fixes 80
3.4.0 Release Notes 80
Features 80
Product Enhancements 81
Bug Fixes 81
3.3.0 Release Notes 81
Features 81
Bug Fixes 81
3.2.0 Release Notes 82
Product Enhancements 82
Bug Fixes 82
Known Issues 83
2021 Release Notes 83
3.1.0 Release Notes 83
Product Enhancements 83
Known Issues 84
Bug Fixes 84
3.0.1 Hot Fix Release Notes 84
Product Improvement 84
Bug Fix 84
3.0.0 Release Notes 85
Improvements 85
Bug Fixes 85
Known Issues 85
2.0.6 Release Notes 86
Improvements 86
Bug Fixes 86
Known Issues/Limitations 87
2.0.5 Release Notes 87
Features 87
Bug Fixes 88
Known Issues and Limitations 89
Answers to FAQs 89

2020 Release Notes 90
2.0.4 Release Notes 90
Enhancements 90
Bug Fixes 90
Known Limitations 90
2.0.3 Release Notes 91
Enhancements 91
Security 91
Bug Fixes 91
Known Issues 92
2.0.2 Release Notes 92
Enhancements 92
Bug Fixes 93
Known Issues 94
2.0.1 Release Notes 95
Enhancements 95
Bug Fixes 95
2.0.0 Release Notes 96
Enhancements 96
Bug Fixes 96
1.1.0 Release Notes 97
Enhancements 97
Bug Fixes 97
1.0.9 Release Notes 97
Bug Fixes 97
1.0.8 Release Notes 98
1.0.10 Release Notes 98
Enhancements 98

Web Password Filler

Web Password Filler provides easy password autofill and lifecycle management services for web applications and web sites. It finds and enters credentials when a Delinea Platform or Secret Server instance stores secrets for that website.

The Delinea Platform and Secret Server store credential, as secrets for different URLs. When WPF identifies an autofill eligible field, it fetches the available secrets for that URL. You can then select the appropriate credential.

Note: The browser's own autofill or password manager may also trigger alongside WPF. To prevent overlapping suggestions, users can disable the browser's built-in autofill in their settings, or administrators can push browser policies (such as Chrome policies) to turn it off.

In addition to autofill, you can add a new secret, update an existing one, or generate a strong password—all through the context menu.

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

You can view and download early availability builds of Web Password Filler using the new beta link available here: Web Password Filler Beta Downloads.

Getting Started

Set up Web Password Filler in this order:

1. Verify your login access to Secret Server, and confirm that Web Services are enabled.
2. If needed, create a folder in Secret Server where WPF secrets reside.
3. In Secret Server, enable Web Services.
4. Install the WPF browser extension. See "Installing Browser Extensions" on page 11
5. Configure WPF to point to the Delinea Platform and Secret Server. See Delinea Platform and Secret Server Connection.

Note: WPF requires Web Services in Secret Server to work correctly. Enable them before installing the extension.

Enabling Web Services in Secret Server

To enable Web Services in Secret Server:

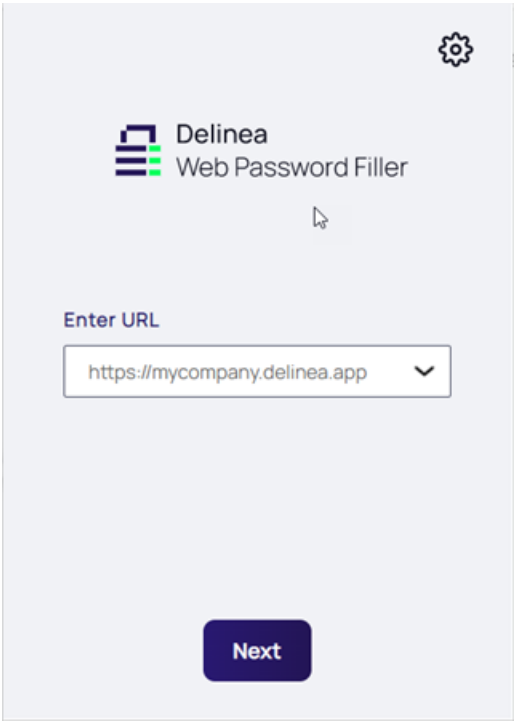
1. Navigate to **Admin** > **Configuration** > **Application Settings**.
2. Under the **View Web Services** section, set the **Enable Web Services** option to **Yes**.

Connecting to the Delinea Platform and Secret Server

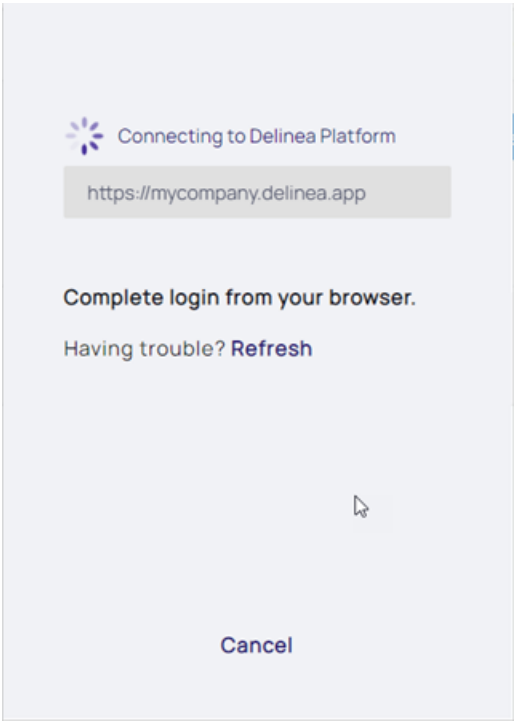
After installation, configure Web Password Filler to connect to the Delinea Platform or Secret Server vault by entering the vault URL in the WPF window.

Connecting to the Delinea Platform

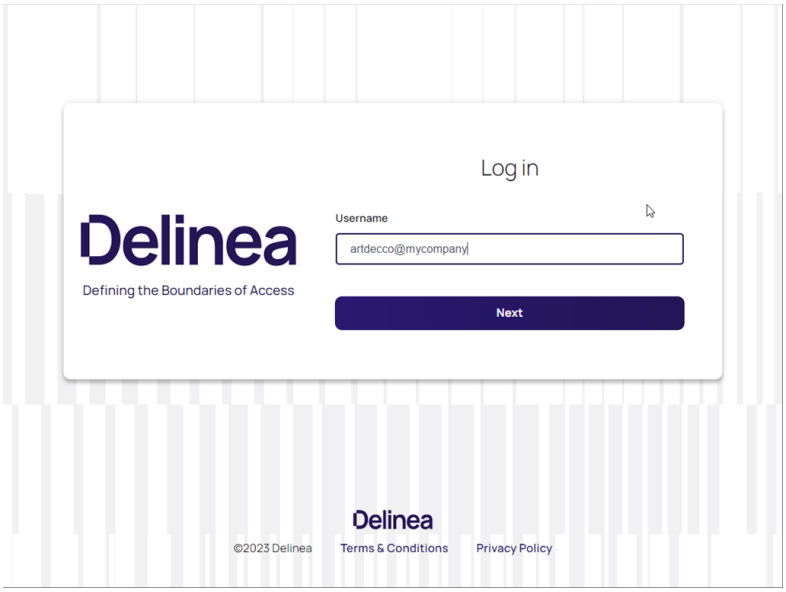
1. Open the browser in where Web Password Filler is installed.
2. Click the  icon. The WPF login window appears.
3. Enter the Delinea Platform URL and click **Next**



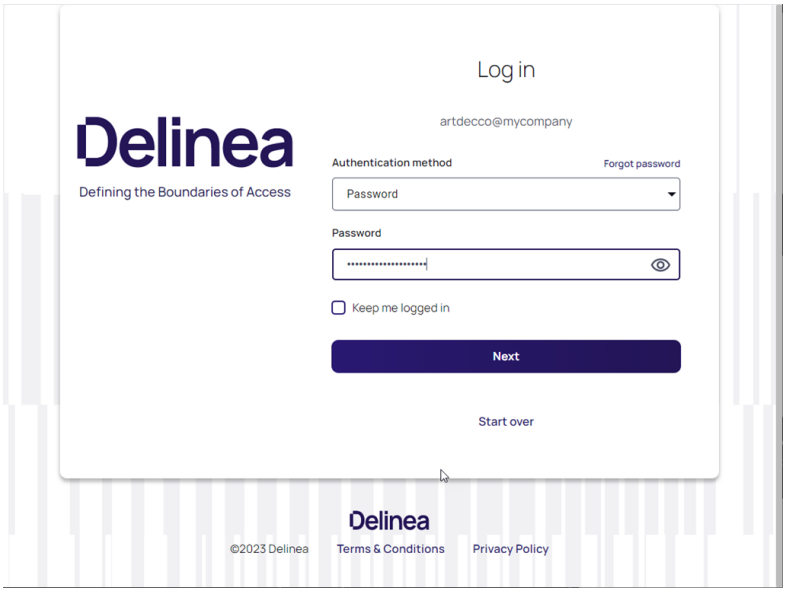
4. Complete login in the browser.



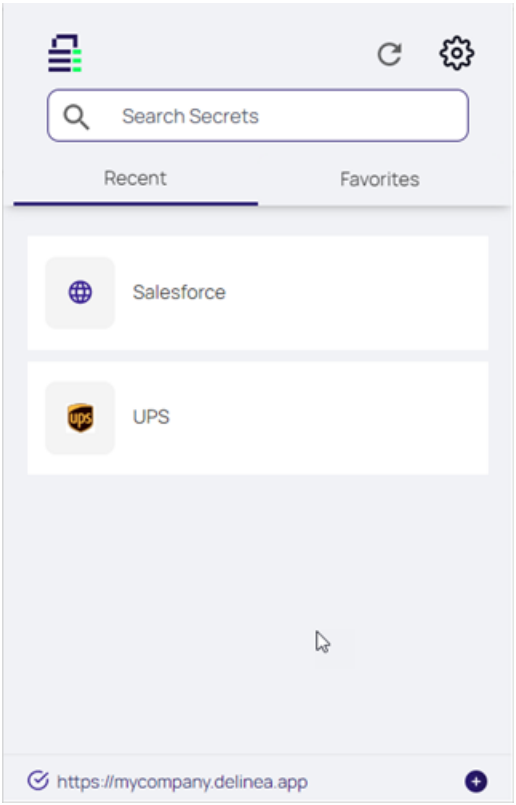
5. If prompted, enter your username and click **Next**



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



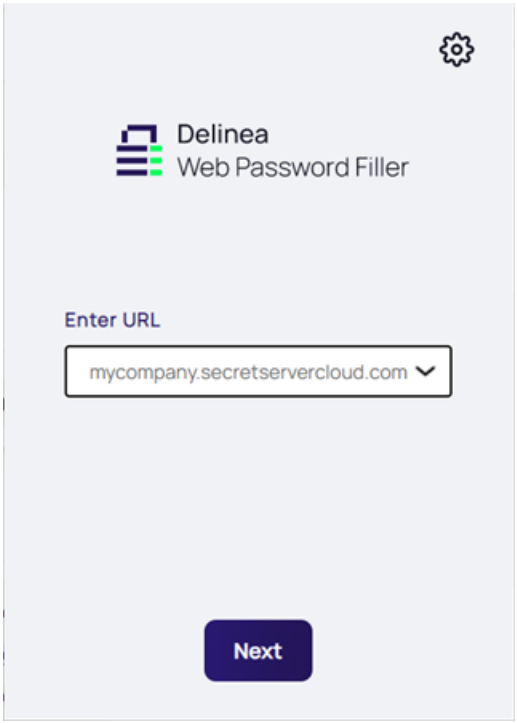
7. You are now logged in



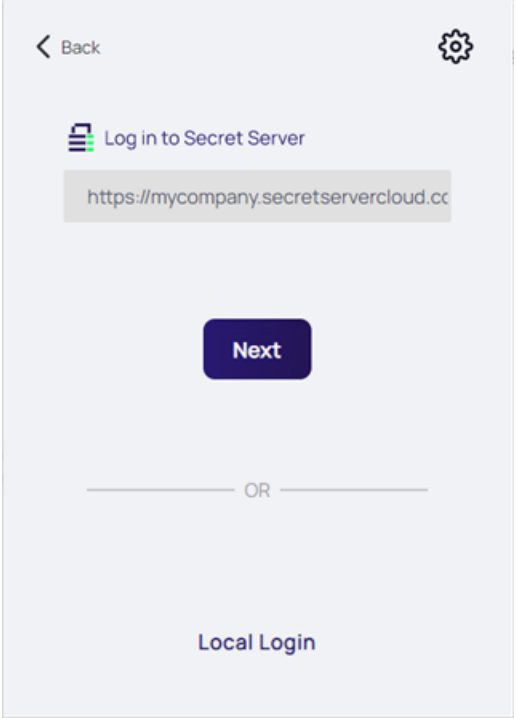
Connecting to Secret Server

To connect WPF with Secret Server:

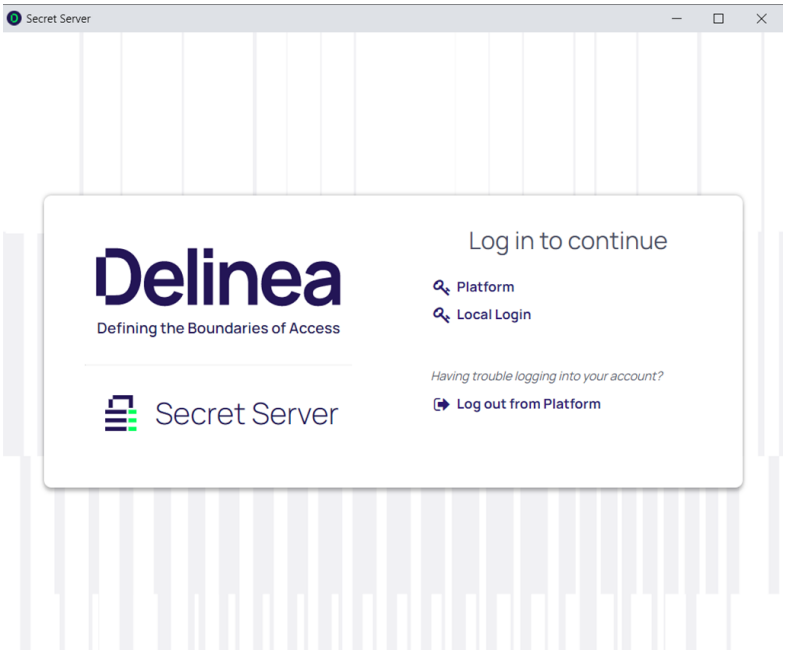
1. Open the browser where Web Password Filler is installed.
2. Click the **Web Password Filler** icon to open Web Password Filler.



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

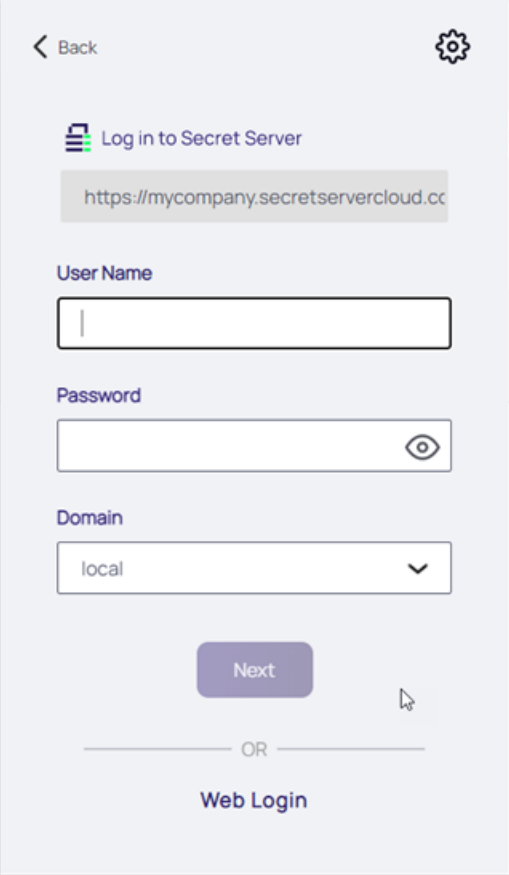


5. Proceed to the browser to complete the login



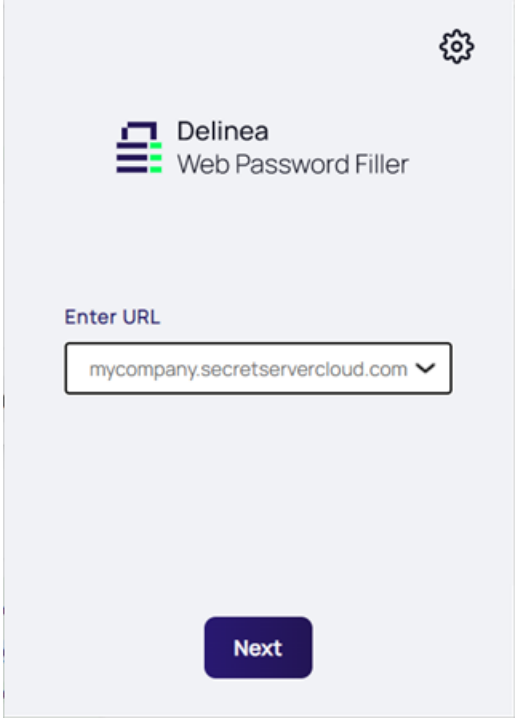
Logging in Locally

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



Specifying Default Protocols

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

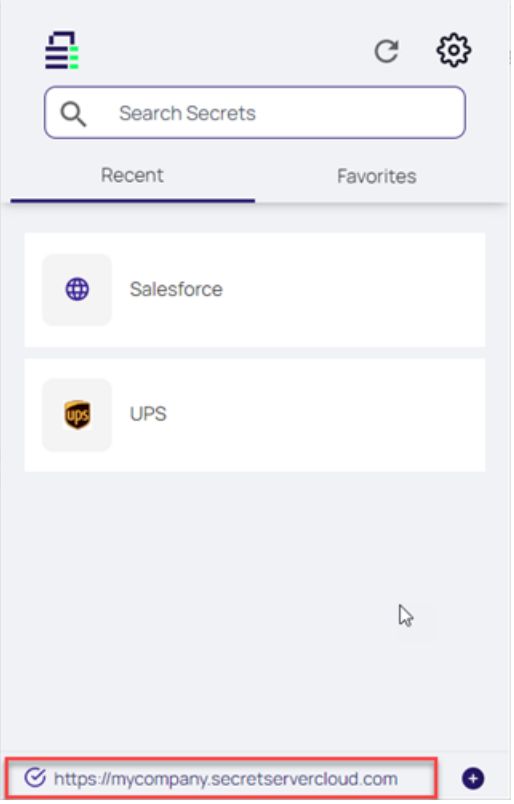


If you click **Next**, Web Password Filler assumes *https://* is the correct protocol and proceeds as if you had prefixed *https://*.

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

Redirecting to Secret Server via Hyperlink

When connected to the Delinea Platform or Secret Server, Web Password Filler displays the vault URL at the bottom of the window. Click this link to open the Delinea Platform or Secret Server vault site directly in your browser.



Reviewing Terminology

This section clarifies the terms used for the Web Password Filler browser extension to help eliminate confusion.

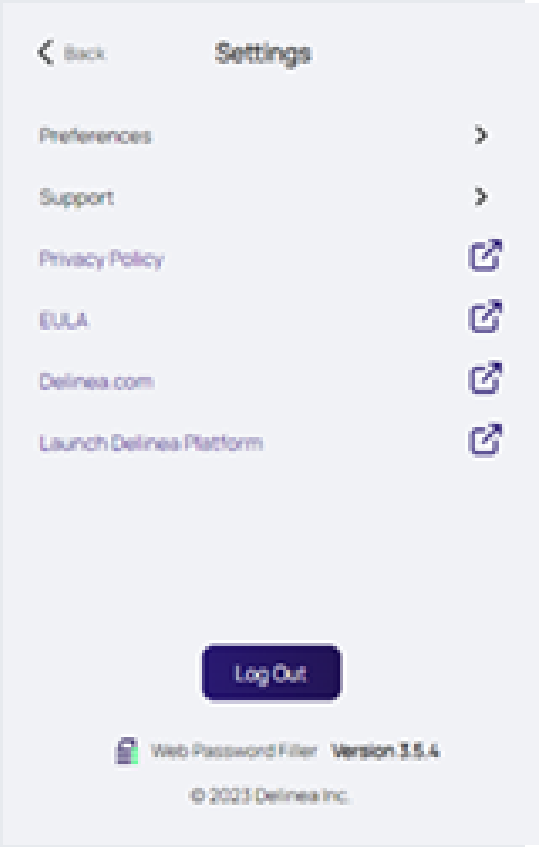
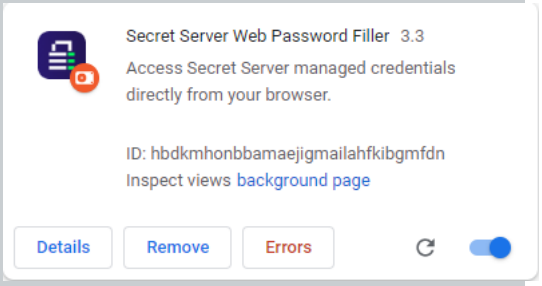
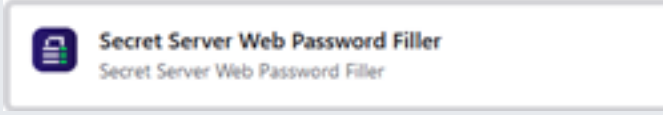
Using Web Password Filler with Secret Server

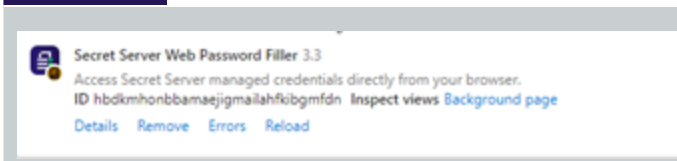
The new Web Password Filler browser extension is included in Secret Server version 10.7.59 and later. Typically, this is referred to as one of the following:

- WPF
- Web Password Filler
- Password Filler

In a browser, you will see the following:

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

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

State	Location/Browser	Example
	Edge (chromium version)	

Installing Browser Extensions

Install a supported browser extension to use Web Password Filler:

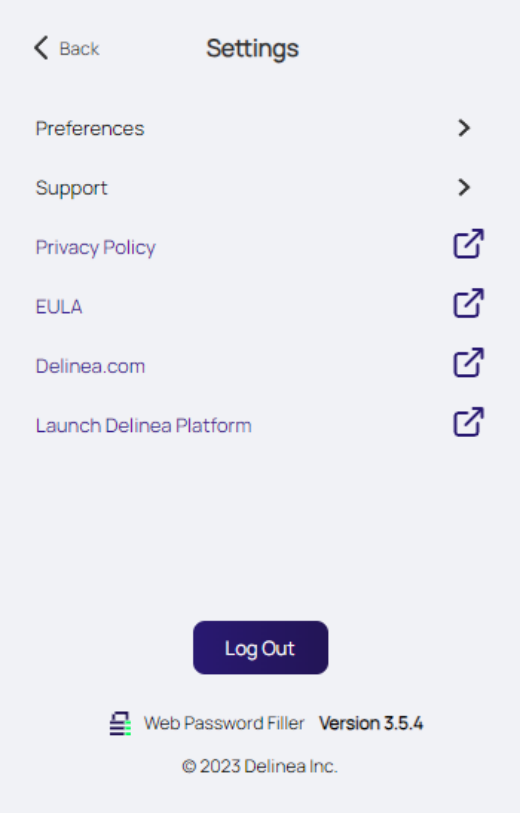
- **Chrome:** Install the extension in one of the following ways:
  - Click the Web launcher icon in a Web Password secret.
  - Download the extension from the Chrome Web Store.

    See Managing Extensions in Your Enterprise.
- **Edge Chromium:** Install the extension by downloading it from Microsoft Add-ons.
- **Firefox:** Install the extension by clicking the Web launcher icon in a Web Password secret, or by downloading it from the Firefox Browser Add-ons .
- **Safari:** Download the extension from the Apple support page for Safari Extensions on your Mac. For more information, see the notes in the list below:
  - WPF supports Safari running on macOS Monterey and Big Sur 11.1.0, 11.2.1 and later.
  - WPF does not support the Native Messaging Host configuration in Safari browsers.
  - The Safari browser extension does not support Windows Admin Center.
  - Safari 15 and above do not support session recording.

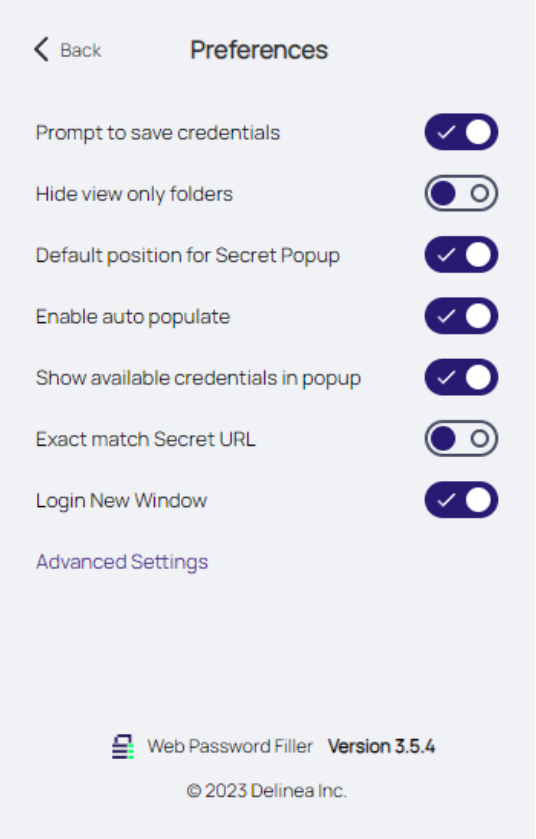
Navigating the Preferences Menu

1. Log in to Web Password Filler and click the WPF icon. 

   The **Settings** screen appears.



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



- **Prompt to save credentials**: Enable this setting to have WPF prompt you to save login credentials for future logins. Not recommended for shared systems. The prompt appears only when an existing secret is updated or when you enter credentials for a site with no associated secret.
- **Hide view only folders**: Enable this setting to hide folders for which you have read-only access.
- **Show available credentials in popup**: Enable this setting to display available credentials in a pop-up dialog.
- **Default position for Secret Popup**: Enable this setting to display the Secret pop-up in the top-right corner of the screen. When disabled, the pop-up appears below the Delinea check symbol.
- **Enable auto populate**: Enable this setting to have WPF automatically populate page fields when a secret is available for that site.
- **Exact Match Secret URL**: Enable this setting to restrict WPF to populating fields only when the URL exactly matches the URL stored in the secret. WPF will not populate fields on variations of the URL, including sub-pages.
- **Secret Server Login New Window**: Enable this setting to open the Secret Server login window in a new browser tab. When disabled, the login window opens in the current tab.
- **Advanced Settings > Session Recording Limit**: Enable this setting to configure session recording time limits through the UI. Limits can be set in one-hour increments, from one to eight hours. The default is two hours.
- **Advanced Settings > Input Threshold**: Input Threshold limits the number of input fields WPF checks on a page, which helps prevent performance issues on complex sites. By default, WPF checks up to 10 input fields. If

a page has more than 10 fields, WPF stops checking to avoid slowing down the site. Increasing this value may reduce performance on some sites.

- **Match Sessions by URL Host** : Controls how session recording identifies sites. When enabled (default), recording is scoped to the specific subdomain – for example, launching mail.google.com records only that subdomain, not other google.com tabs. When disabled, WPF records based on the base domain, so launching mail.google.com would record any tab on google.com.

Deploying Web Password Filler in Air-Gapped Environments

In air-gapped environments, administrators can deploy the Web Password Filler (WPF) browser extension by downloading the extension package and distributing it through internal infrastructure. This topic covers how to download, deploy, and configure WPF using Group Policy.

Download the Extension

Download the latest version of WPF for Chrome and Edge: WebPasswordFiller_current.zip

Prepare for Deployment

To prepare for deployment:

1. Extract the zip file.
2. Copy the extracted folder to a network location accessible to all target computers.
3. Ensure that share permissions grant 'read access' to all accounts or users that will receive the extension

Deploying Extensions with Group Policy

1. Follow Google's guide, Force-install apps and extensions, to deploy a Chrome extension using Group Policy.

   Note: The same process applies to Microsoft Edge, which is Chromium-based and supports Chrome extensions.

2. In the **Define the extension download location** section of the Google article, set the path to your internal network location where the extension files are stored.
3. Use the following extension ID when configuring Group Policy:

   mfpddejbpnbjkjoaicfedaljnfeollkh

Configure Permissions and Restrictions (Optional)

The Google Support article describes additional permissions administrators can enforce. For example:

- Prevent WPF from autofilling or prompting to save credentials for specific sites.
- Restrict WPF to run only on specific sites.

For instructions, see the **Prevent apps and extensions from altering webpages** section of the Google article.

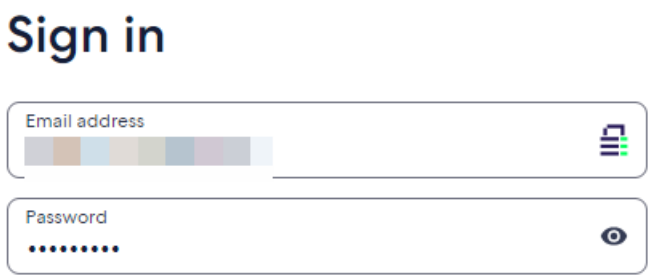
Using WPF

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

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

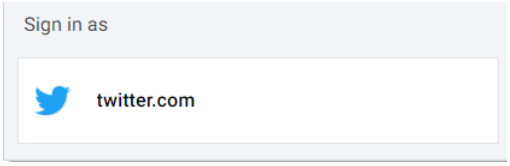
Logging in to a Website

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

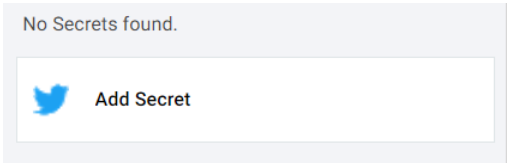


Note: If you are signed into Web Password Filler and do not see the purple and green lock in the username text box, try refreshing the web page to make it appear.

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



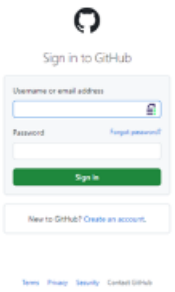
   - If you have no secrets related to the site, then a pop-up will open to give you the option to add a new secret:



   If you see the second possibility, you need to set up a secret for that website. See Creating a Secret for a Website.
4. Click the button for the desired secret, and you are signed in.

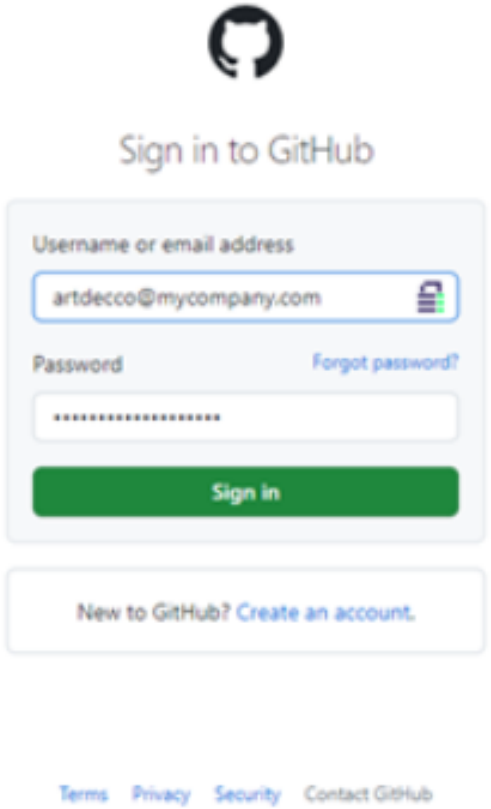
Accessing Secrets Guarded by MFA

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



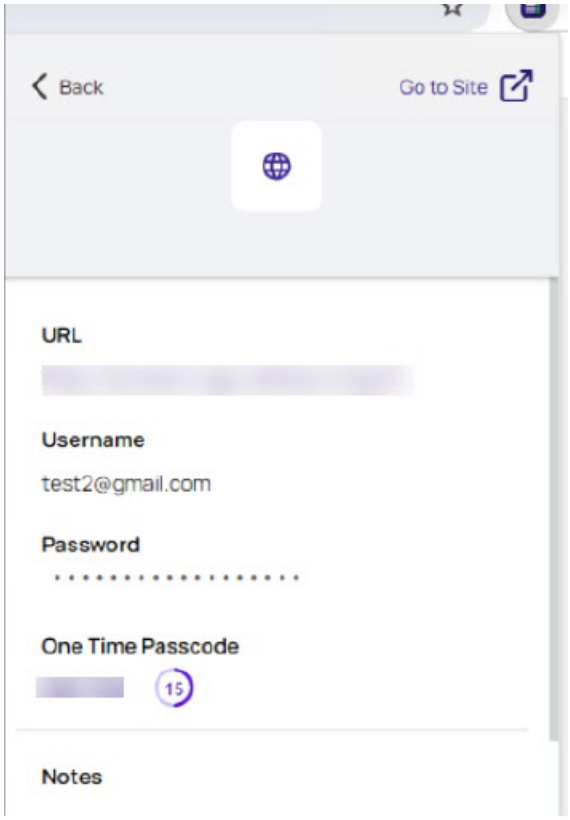


After clicking **Challenge**, you will be redirected to the Delinea Platform portal to complete the MFA challenge. When you have successfully completed the MFA challenge, you can return back to Web Password Filler to view or launch the secret.



Autofilling OTP

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



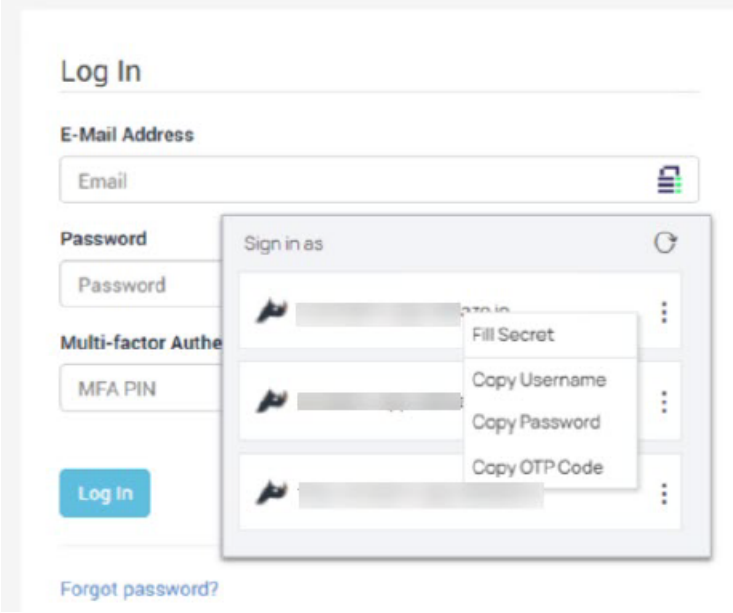
If you do not see Web Password Filler automatically identify an OTP field, you have the option to manually copy and paste the OTP from the secret.

To copy the OTP, complete the following steps:

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

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

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



For more information on how to set up OTP on secret templates, see Enabling OTPs for Launchers.

Recording Web Sessions

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

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

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

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

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

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

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

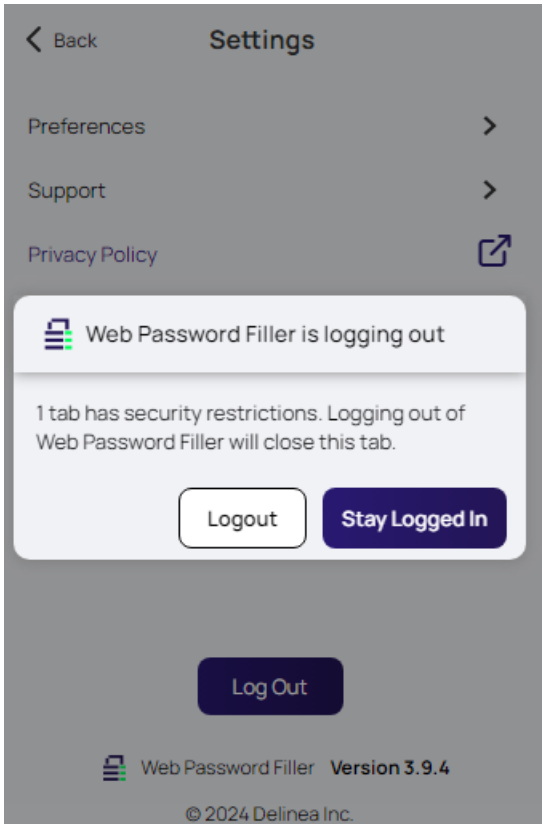
This expected behavior ensures that the system only records sessions associated with Secrets that require session recording. Sites like *microsoftonline* allow only one login / active credential at a time. If you enable session recording for two secrets that do not contain a primary / secondary domain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

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

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

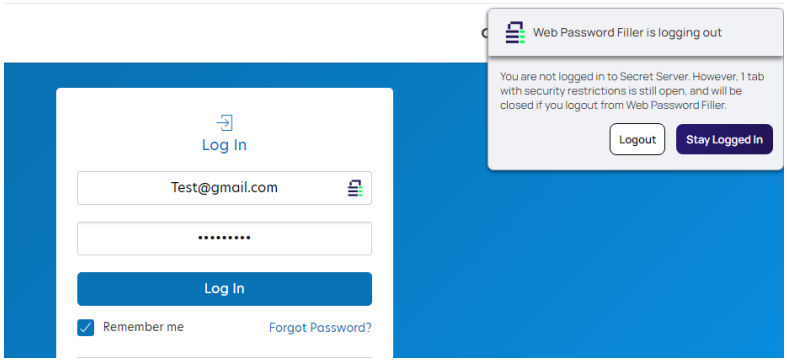
Session Recording Disconnecting Warning

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



This warning can occur in the following circumstances:

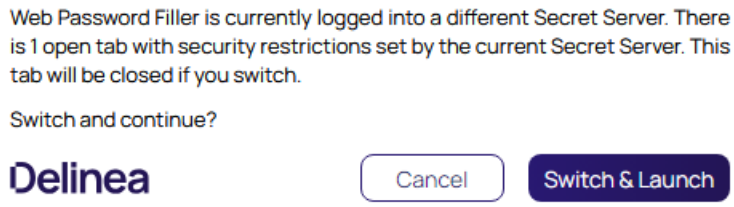
- The user logs out of Web Password Filler.
- The user has a tab open to the same Secret Server or platform that Web Password Filler is currently logged into. They then log out of the web tab.



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

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

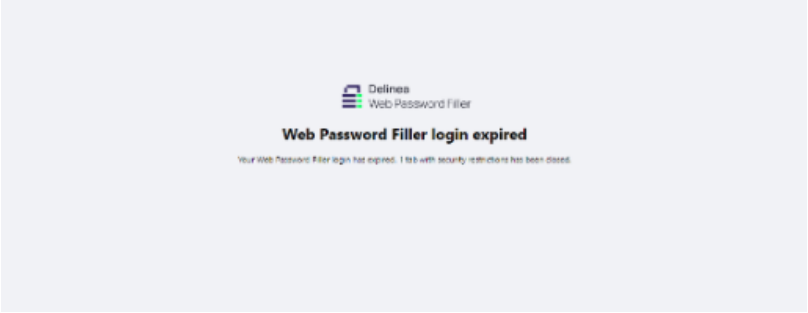
- The user launches a web session from a different Secret Server or platform instance, requiring Web Password Filler to switch login context to the new server. In this case, the system must end recorded sessions to the old server.



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

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

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



Managing Session Recording Limits

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

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

Using RegEx

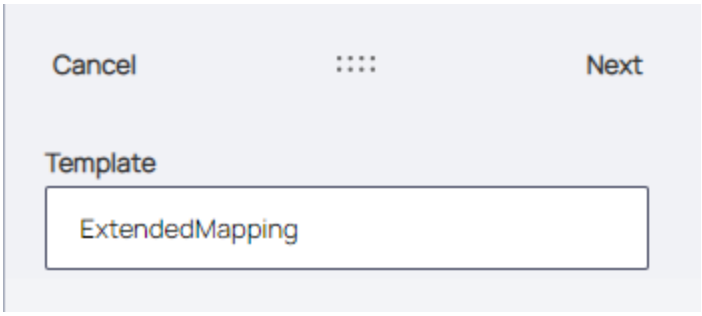
RegEx provides a sequence of patterns that Secret Server templates specify and that you can enter as **OtherUrls** during account setup in Web Password Filler. This allows you to record sessions on redirected websites.

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

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

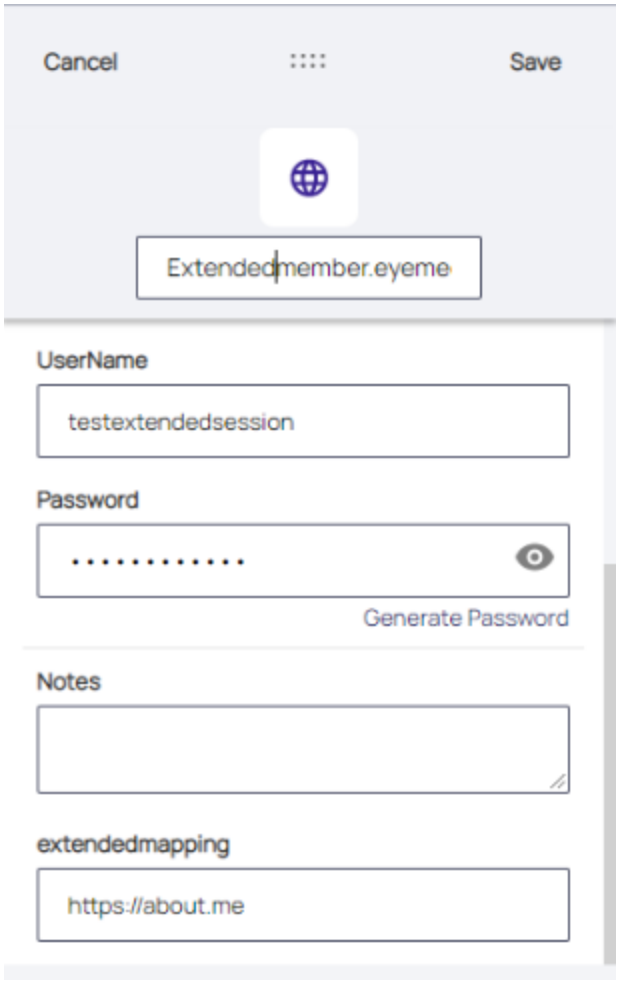
Using RegEx in WPF

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



2. Click **OK**.

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

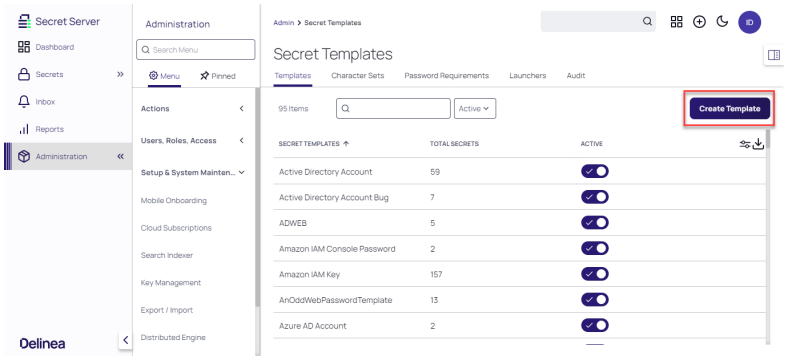


   Enter any other URL in the **Extended Mapping** field for which you should enable session recording, in case the user gets redirected to those URLs.

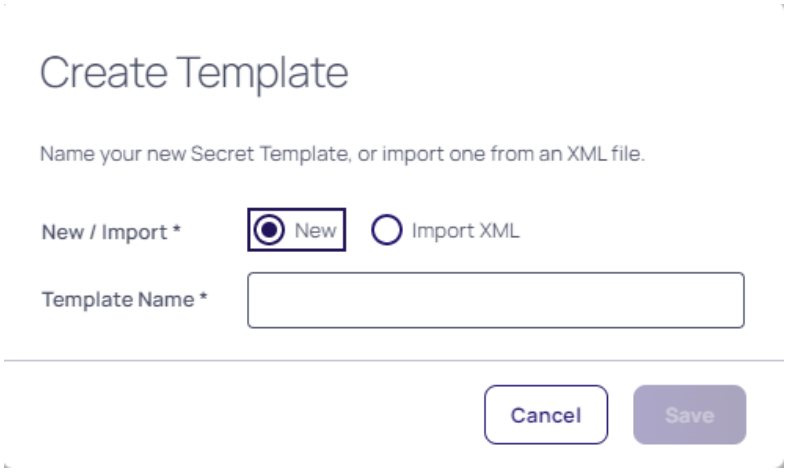
4. Click **Save**.

Setting Up Templates in Secret Server

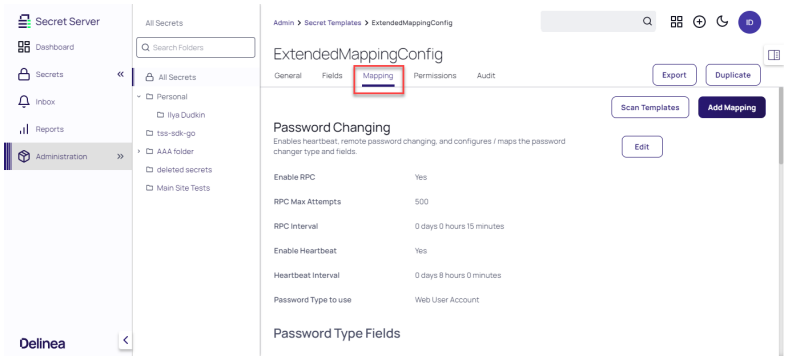
1. Sign into Secret Server and navigate to **Admin** > **Secret Templates**.



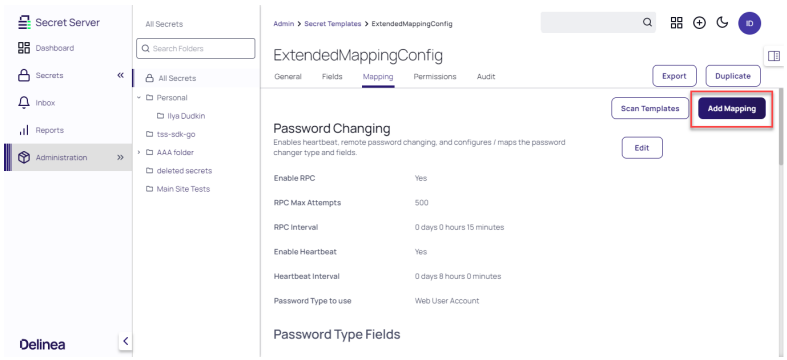
2. Click **Create Template**.
3. Name the new template and click **Save**.



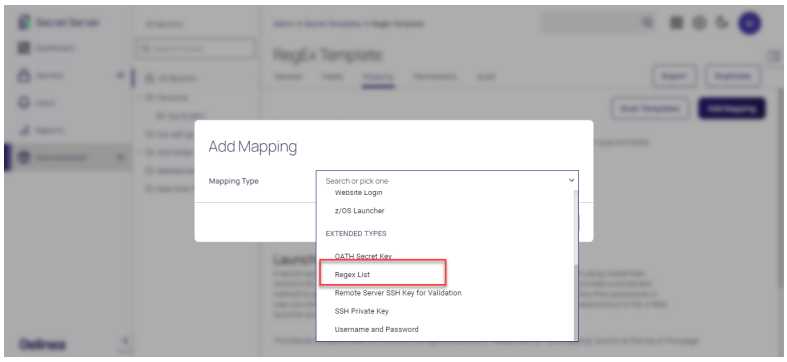
4. Inside the secret template, click **Mapping**.



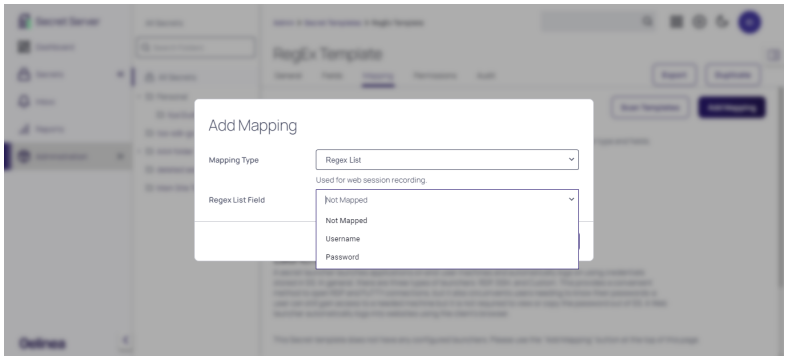
5. In the **Mappings** page, click **Add Mapping**.



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



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



8. Click **Save**.

You can now use the template in WPF.

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

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

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

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

Launching Comma-Separated URLs

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

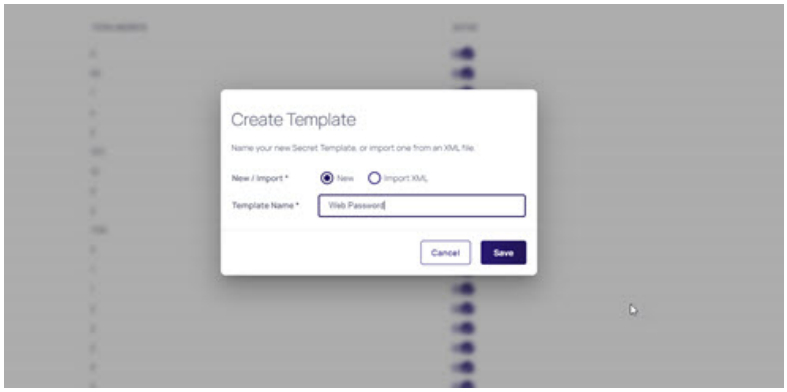
Creating a Secret Template

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

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

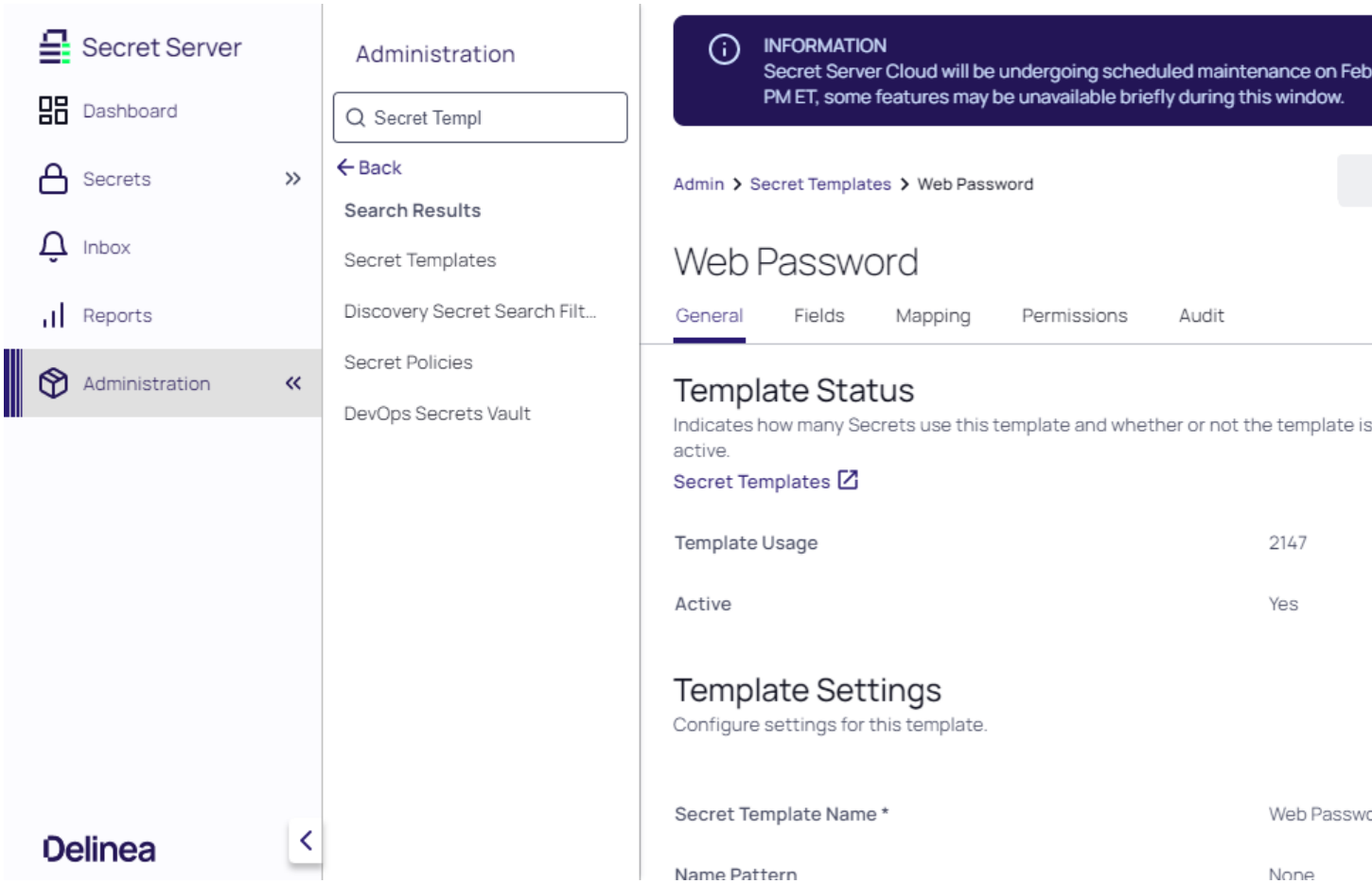


2. Give the new template a name and click **Save**.

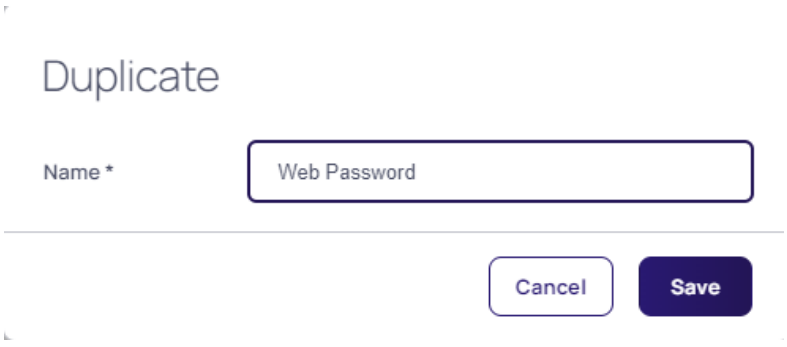


3. In the **Secret Templates** tab inside Secret Server, find the secret template you just created and click **Duplicate**.

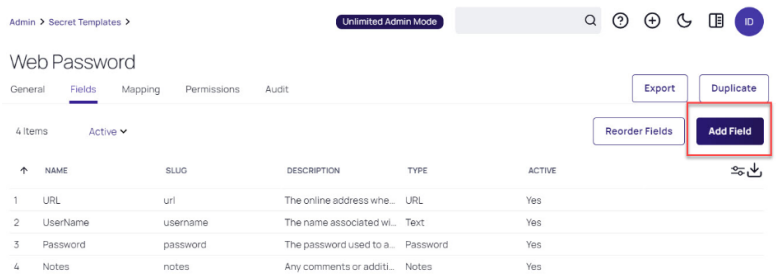
.



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

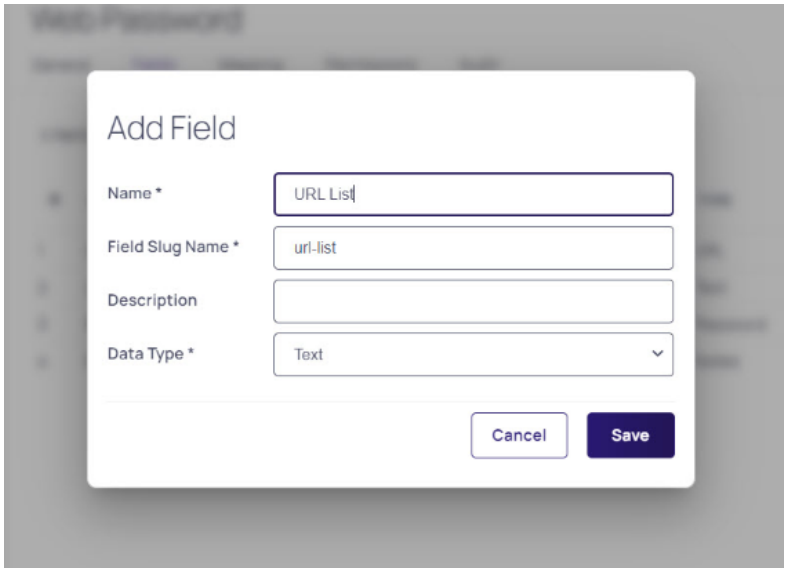


5. Inside the duplicate template, navigate to the **Fields** tab and click **Add Field**.

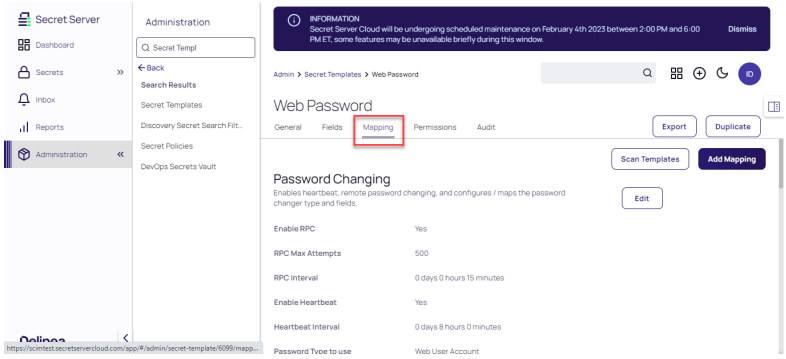


6. Create a new field with the name '*URL List*'. Click **Save**.

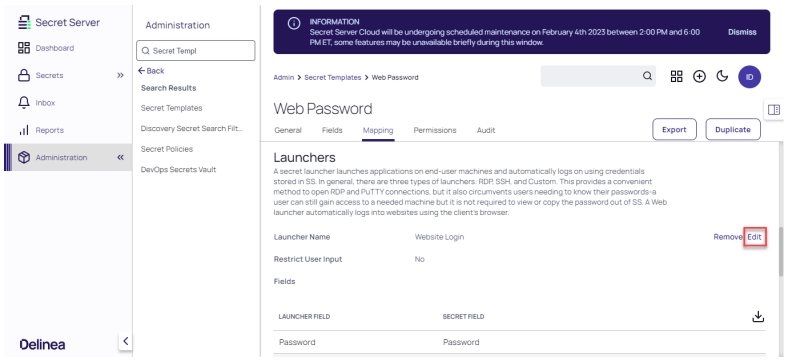
   Note: You can choose any *Data Type* except *URL List*, *List* or *URL*.



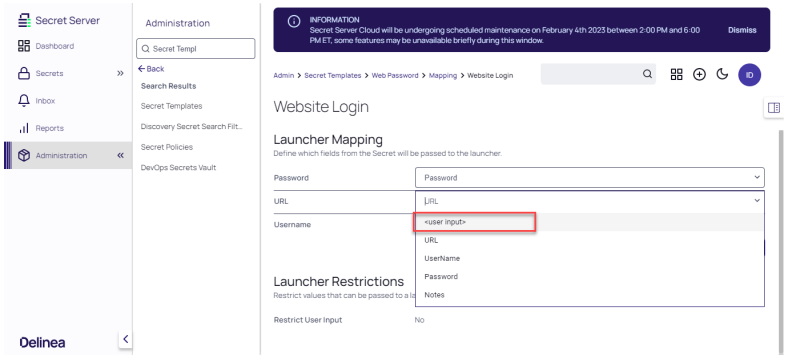
7. Click the **Mapping** tab.



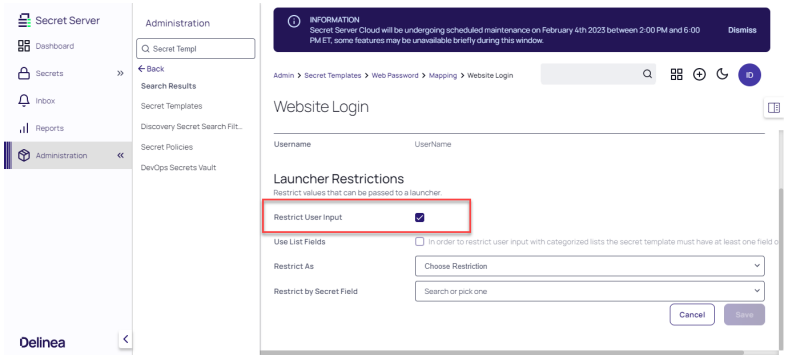
8. In the **Launcher Mapping** section, click **Edit**.



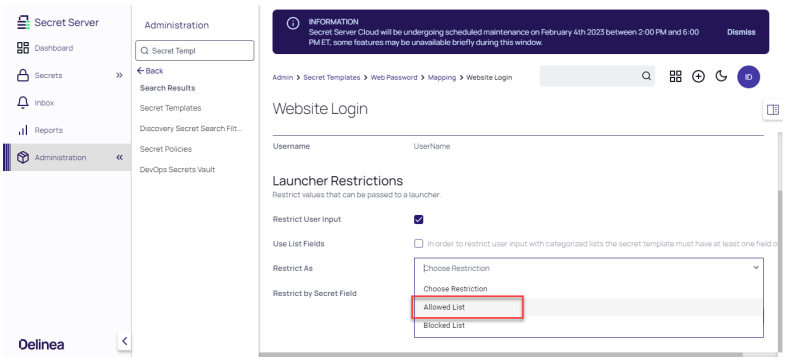
9. In the **URL** dropdown menu, select **user input** and click **Save**.



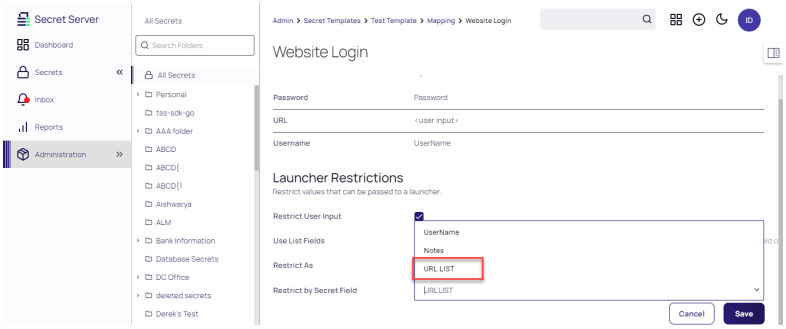
10. In the **Launcher Restriction** section, enable **Restrict User Input**.



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



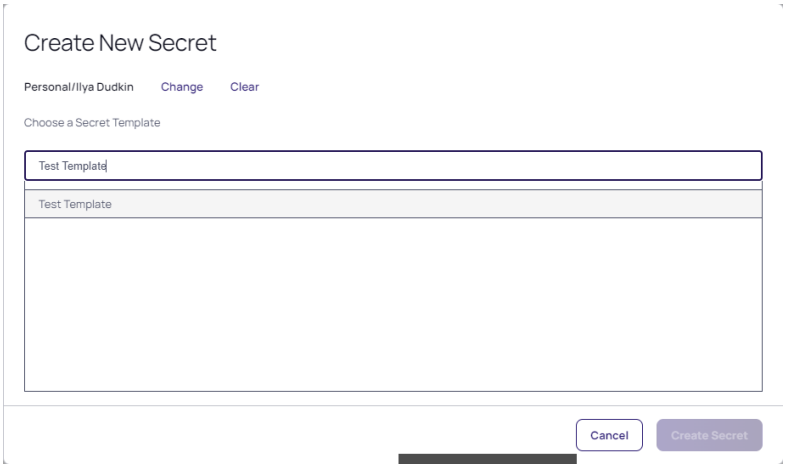
12. In the **Restrict by Secret Field** dropdown menu, select **URL List** and click **Save**.



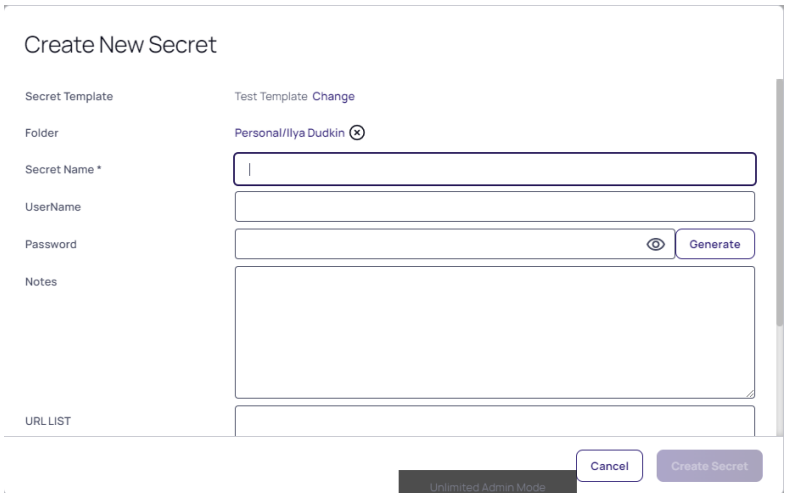
Using the Custom Web Launcher

To use the custom web launcher, follow these steps:

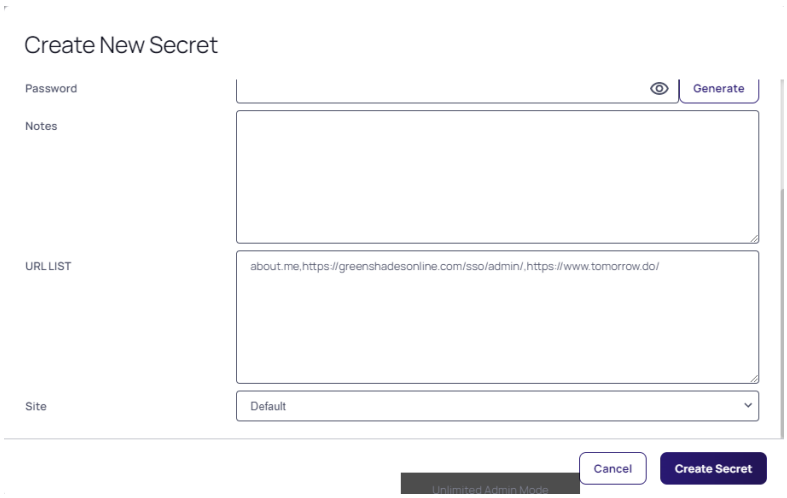
1. Create a secret with the newly created template.



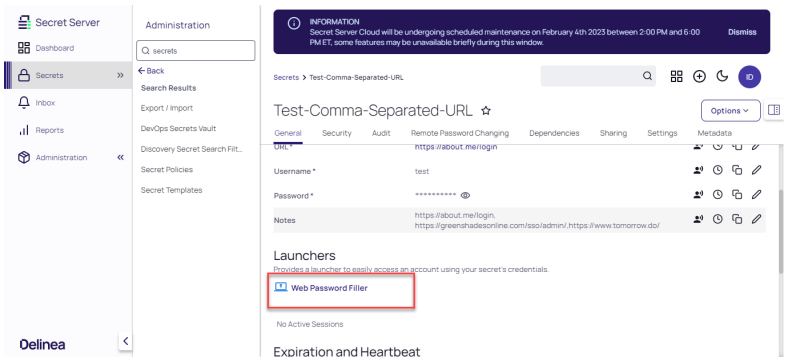
2. Input the *Secret Name*, *URL*, *Username* and *Password*.



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



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

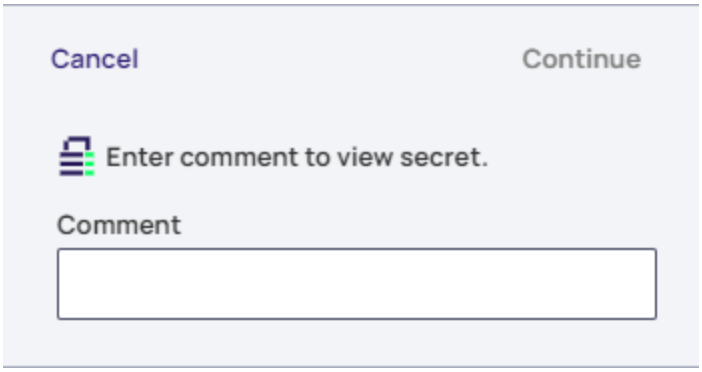


Setting Comment Requirements

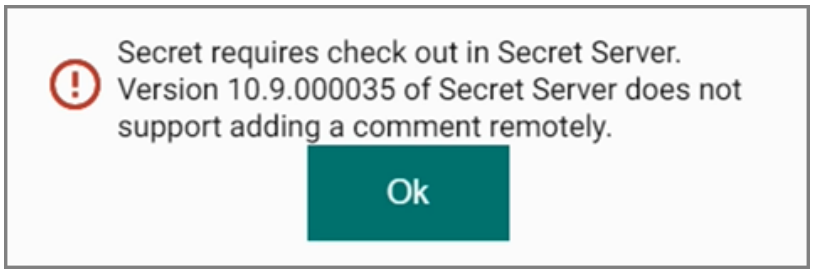
When a Secret in Secret Server requires a comment for checkout, you can supply that comment via the **Enter Comment** pop-up. Once you enter and submit the comment, WPF will populate the fields and give you access.

There are two levels of support for access to Secrets:

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



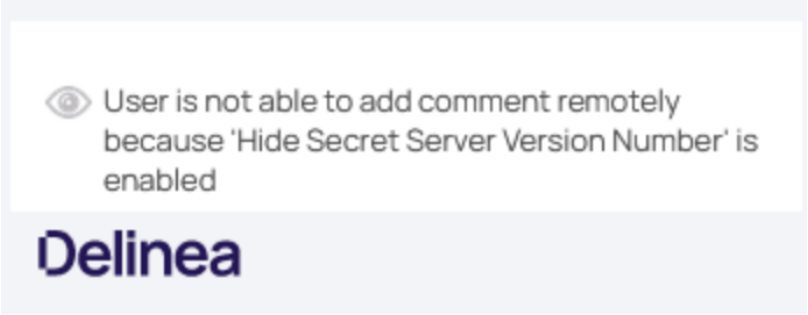
Note: Secret Server versions above 11.1.000004 support this feature. If you use it on version 11.1.000004 or earlier, you will see the following message:



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

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

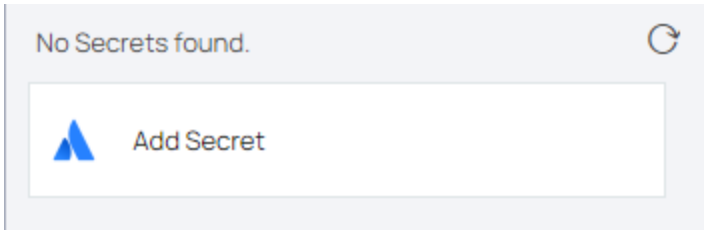
In this case, you will see a pop-up informing you that you cannot add a comment remotely because you have enabled 'Hide Secret Server Version Number'.



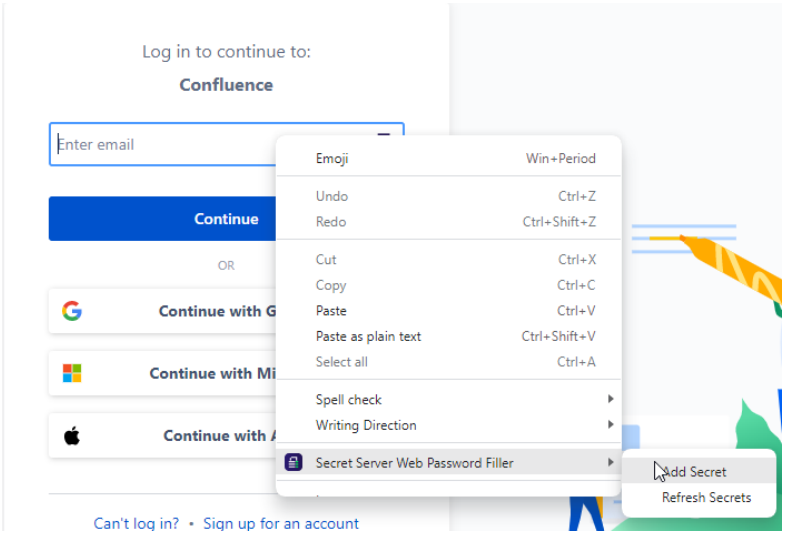
Creating a Secret for a Website

To create a new secret:

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

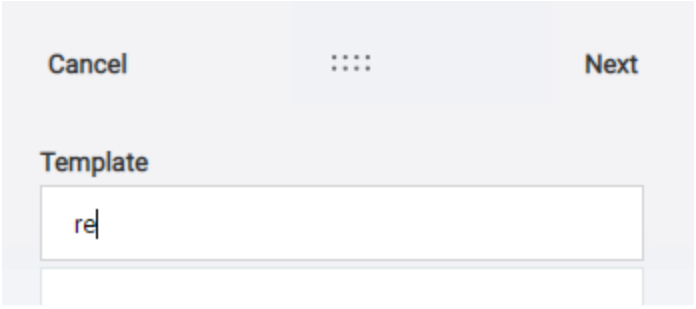


You can also right-click in the username or password field and select **Secret Server Web Password Filler | Add Secret**.

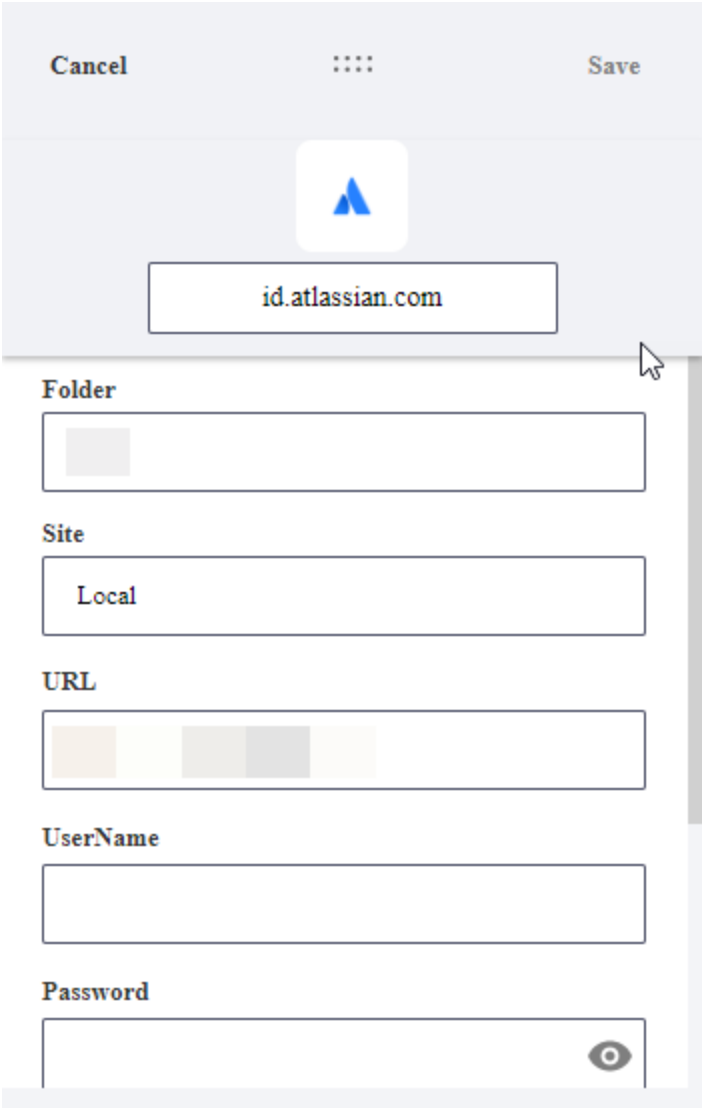


3. Select a **Template** for the newly added Secret. The default entry for the Choose a Secret Template field is **Web Template** because users choose that template most frequently. You can leave the default entry or click into the

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



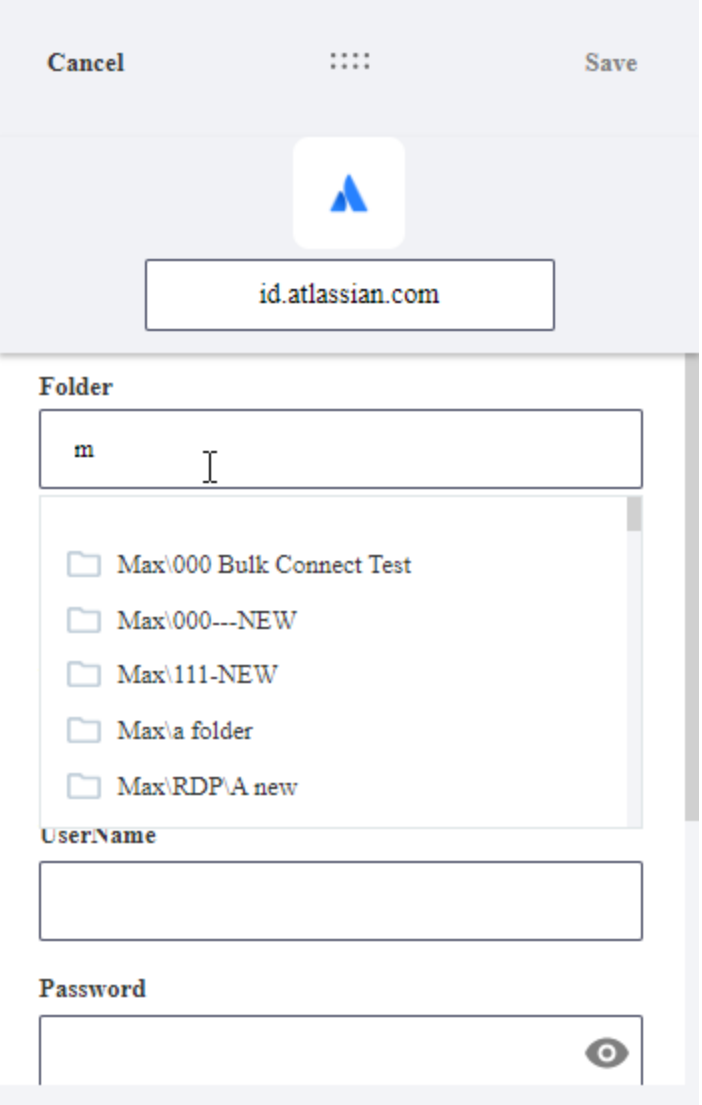
4. The **Add Account to Secret Server** pop-up appears:



Selecting a Folder

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

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



Adding Accounts

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

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



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

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

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

Syncing Recent and Favorite Lists with Secret Server

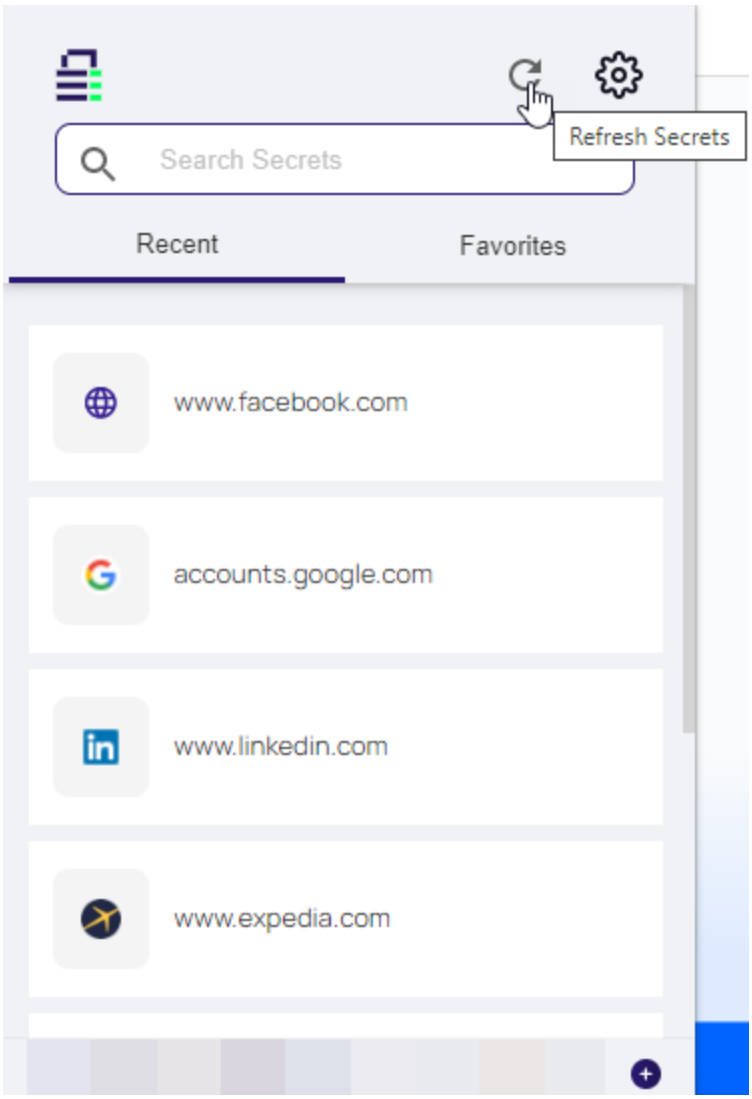
Users' Recent lists are synced between Web Password Filler and Secret Server. WPF currently displays all secrets in the Recents tab as there currently is no 'All Secrets' tab. Secrets are ordered from most-recent to least-recent where the least-recent would include web-based secrets that have never been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

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

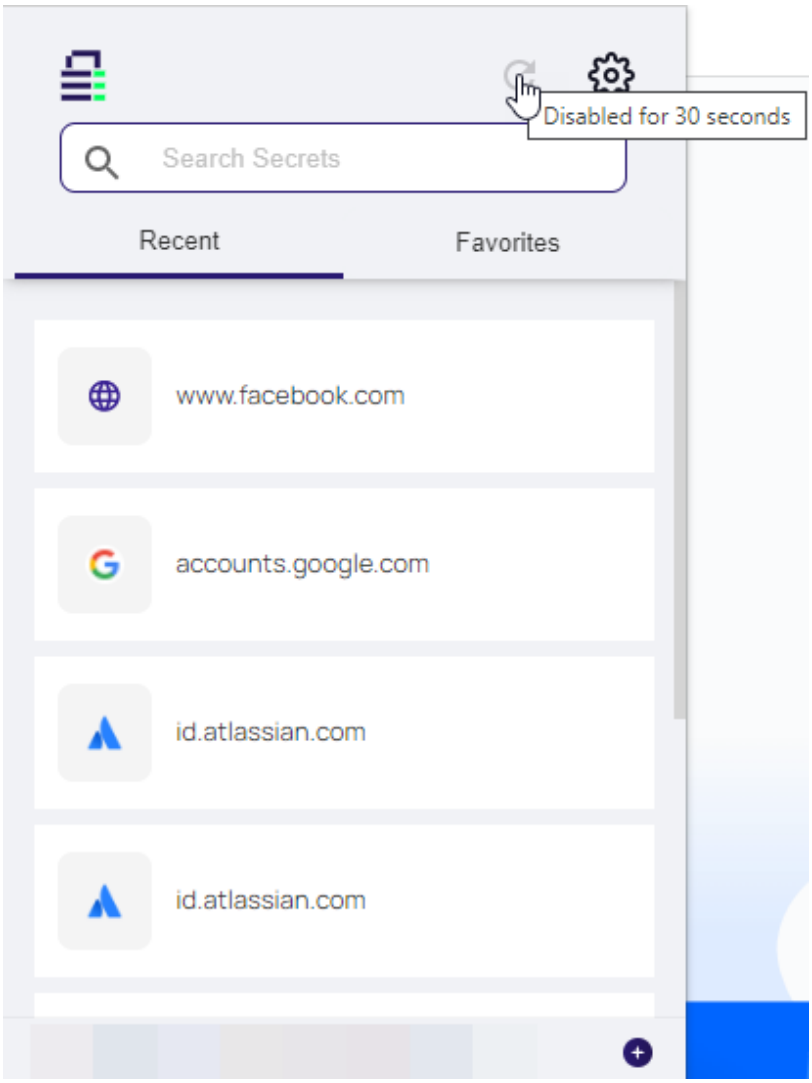
Web Password Filler also syncs the Favorite list between the browser extension and Secret Server.

Refreshing the Recent and Favorites List

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



After refreshing the refresh button is deactivated for 30 seconds.



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

Mapping Login Fields

Mapping login fields is the process of manually connecting fields in your secret to corresponding fields on a web page using drag-and-drop. This allows Web Password Filler to autofill login information on websites that use unconventional labels for username, password, and other login fields.

Important: Only map fields that Web Password Filler cannot identify, or fields for which automatic mapping is not working. Do not map fields that are already autofilling correctly, as this can interfere with the autofill functionality.

Important: Do not manually map a field whose value you cannot see in the Secret. For security reasons, Web Password Filler cannot retrieve hidden field values for autofill because doing so would risk exposing that value to the user.

Mapping Web Page Form Fields to Secret Fields

To map web page form fields when creating a secret:

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

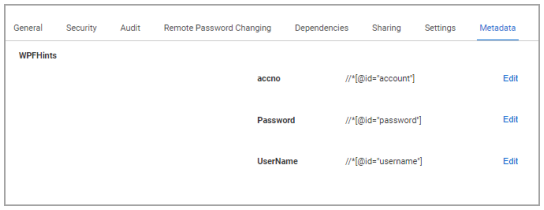


2. Drag the highlighted field to the corresponding field on the web page form.

Enabling Field Mapping with Metadata

Before end users can map fields, an administrator must configure the WPFHints metadata section. This section defines which template fields users can map and specifies the XPath values for web page form fields.

In the example below, the Metadata tab displays the WPFHints section with mappable template fields (accno, Password, and Username) and their corresponding XPath string values.



To configure the WPFHints section:

1. Select a secret and click the **Metadata** tab.
2. Click the **Section name** dropdown and select **Add new section**.
3. In **New section name**, enter **WPFHints**.
4. Click the **Metadata field** dropdown and select **Add new field**.
5. Enter a **Metadata field name**, **Field type**, and **Value**.

   Note: The initial field values aren't used for field mapping but are required to create the section.

6. Click **Save**.

There is no way to delete a metadata section. If you want to disable the ability to add field mappings, you can rename WPFHints to something else. Renaming the section will rename it globally across all secrets. Credential Manager and WPF no longer recognize the section as containing field mappings.

To rename the WPFHints section:

1. Select a mapped secret and click the **Metadata** tab.
2. In the **WPFHints** section, click **Edit**.
3. Rename the section and click **Save**.

Supporting Incognito Mode

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

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

- Firefox: **Run in Private Windows**
- Safari: **Run in Private Window.** You only need to enable extensions on macOS Sonoma (14) or higher. Safari automatically enables extensions on older macOS versions. To enable this setting. complete the following steps:

a. Choose **Safari** > **Settings**.

b. Click **Extensions**

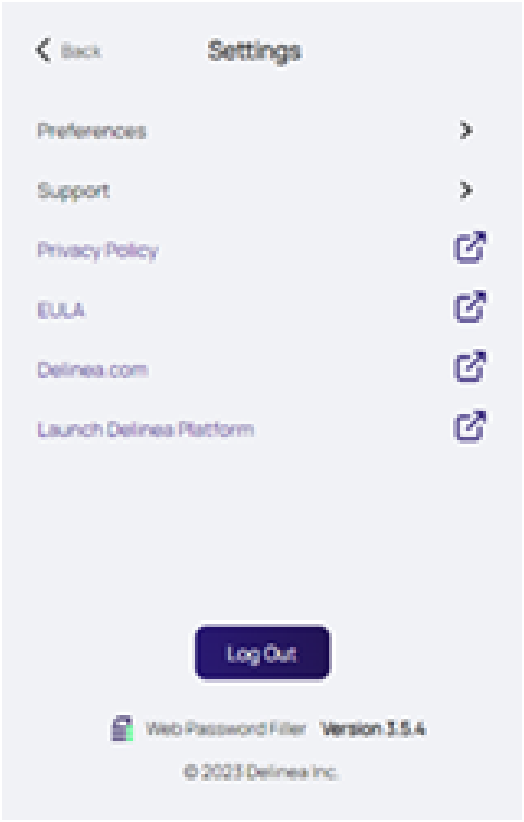
c. Select the extension in the sidebar, then select **Allow in Private Browsing** on the right.

3. Login to WPF.

Logging Out of Secret Server

Use the Web Password Filler icon to logout:

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



Click **Logout**.

3. The WPF icon changes to: 

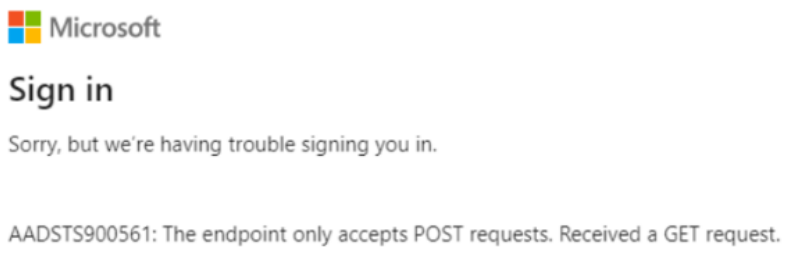
Using Web Password Filler with Microsoft Online Services

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

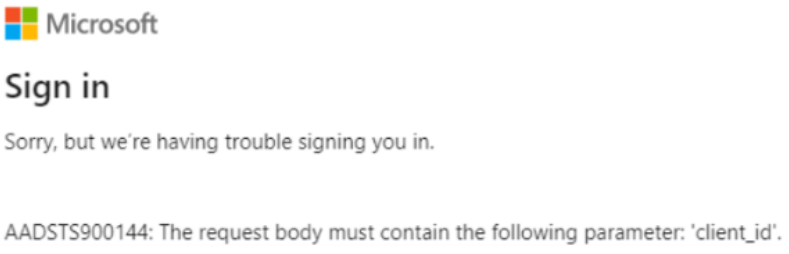
Note: This version of WPF is available in Secret Server release 10.7.59 and later. These instructions assume you have WPF installed correctly and are connected to Secret Server. If you're using WPF With Microsoft Online for the first time, we recommend you test your installation on another site first.

Identifying the Problem

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



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



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

Understanding the Issue

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

Web Password Filler initially stores this errant URL:

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

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

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

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

Choose between these two methods to update the URL:

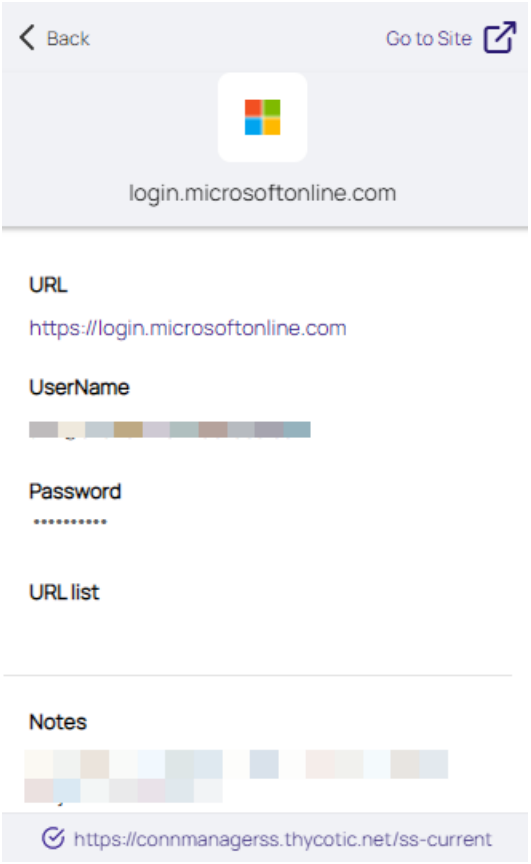
- **Before Saving the WPF Secret:**: You can change the URL when WPF initially stores it, right from WPF, *before* saving the secret. You can use this method if you create a new WPF secret using the WPF **Add Secret** button or the browser's context (right-click) menu.
- **After Saving the WPF Secret:**: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

Fixing the Issue When Creating the WPF Secret

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

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

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

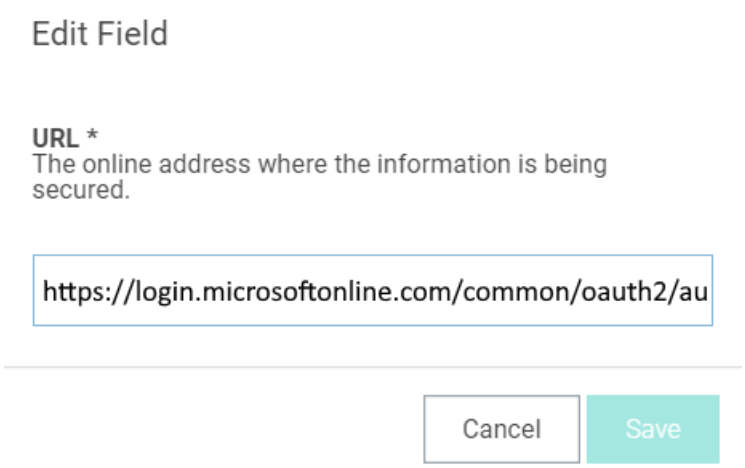


You now see the website URL that WPF inferred, which is incorrect. WPF also inferred the secret name–you can leave it as is or change it to whatever you like.

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

Fixing the Issue After Having Saved the WPF Secret

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



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

Managing Port Numbers

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

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

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

- 10.0.0.61:55 is different from10.0.0.61:555 or 10.0.0.61
- *blue.local.something* is different from *blue.local.something:8080*

Certificate Requirements for Web Password Filler in Chrome

Web Password Filler requires properly signed certificates to connect to on-premises Secret Server installations. Because Chrome's Manifest V3 implementation does not support self-signed certificates, you must use certificates signed by a Certificate Authority (CA).

To set up CA-signed certificates:

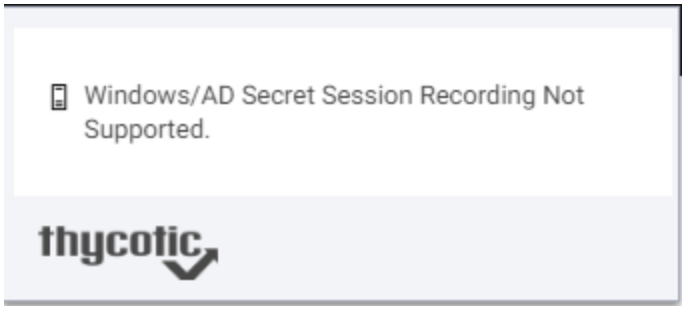
1. Set up a local CA if your organization does not already have one.
2. Install the CA root certificate as a trusted certificate authority on the computers where Web Password Filler will be used.
3. Create a certificate signed by your CA.
4. Install the CA-signed certificate on your Secret Server nodes.

Web Password Filler can now connect to Secret Server.

Supporting Windows Admin Center

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

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



Securing Web Password Filler

The following Securing Web Password Filler topics are available:

- "Setting Up the Native Messaging Host" below
- "Preventing Users from Disabling Session Recording" on page 58

Setting Up the Native Messaging Host

The Delinea Native Messaging Host provides a reliable method for storing settings, so that when the browser cache is deleted, the settings are not affected.

Without the Native Messaging Host, Web Password Filler runs normally, but the user must supply the Secret Server URL and modify other settings as needed.

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

You can prevent Web Password Filler from functioning on specific URLs by adding those URLs to an exclusion list. Web Password Filler does not access Secrets for URLs on the exclusion list, and it does not fill or auto-populate credentials or other information for those URLs.

Note: To use an exclusion list with Web Password Filler, you must have the Native Messaging Host installed.

Downloading the Native Messaging Host

You can download the Native Messaging Host installer here.

Software Requirements

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

Supported Browsers

- Chrome
- Edge Chromium
- Firefox

For more information about Native Messaging, see:

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

Installing and Registering the Native Messaging Host

To install and register the Native Messaging Host:

1. Copy the `ThycoticMessagingHost.exe` and `settings.json` files into an accessible directory, such as `C:\Thycotic\Web Password Filler\`.
2. Open a command window and enter the following command to register the Native Messaging Host with your browsers:
   `C:\Thycotic\Web Password Filler\ThycoticMessagingHost.exe --register`

   Note: The Native Messaging Host cannot interact with Web Password Filler until you complete this registration. If you register using the `EnableForAllUsers = true` option, you must run the registration as an administrator.

During registration, the Native Messaging Host creates a folder for each browser (Chrome, Edge, Firefox, and Opera) that contains the native messaging host configuration required by each browser. The Native Messaging Host also creates registry entries for each browser, either in the current user or local machine registry.

For example, you find `HKEY_CURRENT_USER\Software\Google\Chrome\NativeMessagingHosts\com.thycotic.wpf.host` with a default value that is the path to the native messaging host configuration file.

After you successfully register the Native Messaging Host, it automatically checks the configuration file for updates each time you launch your browser. You do not need to unregister or re-register when you change other settings in `settings.json`; the changes take effect the next time you launch your browser.

Uninstalling the Native Messaging Host

The Native Messaging Host no longer communicates with your browser extension once you uninstall it. This helps maintain system security and performance.

To uninstall the Native Messaging Host:

1. Open a command window.
2. Run the following command:
   `C:\Program Files\Thycotic\Web Password Filler\ThycoticMessagingHost.exe --unregister`

Configuring Web Password Filler Settings

The Native Messaging Host manages Web Password Filler settings by modifying the *settings.json* file. Each time you launch your browser, the Native Messaging Host reads the default configurations and settings from the JSON file and sends them to Web Password Filler. WPF then updates the local storage with the new settings and configurations.

Establishing Default Settings and Browser-Specific Overrides

To customize how the Native Messaging Host manages settings for different browsers, edit the `settings.json` file. Modify this file to set default options and create browser-specific overrides, ensuring each browser behaves according to your preferences.

To edit the `settings.json` file:

1. Launch a text editor and open the `settings.json` file where you downloaded it earlier in Step 1 of "Installing and Registering the Native Messaging Host" on the previous page.

2. At the beginning of the `settings.json` file, write one line for each browser, and in that line enter the browser's identification code.

   Label these initial lines as **Browser IDs**.

   Note: For a list of IDs, see "Settings Reference" on page 51.

3. Add the next set of lines to define the default settings for the Native Messaging Host and label these lines as **Default Settings**.
4. Apply the default settings to all browsers in the `settings.json` file and create a new section for each browser that requires settings different from the default.

   Label each new section as **Default Overrides per Browser**, then begin each override section with the browser's identification code.

   List the settings in the same order as the default settings.

   Enter a new value for each setting that differs from the default.

   The browser-specific value overrides the default value for that browser.

5. Save your changes.

Example settings.json File

The following example `settings.json` file sets the Secret Server base URL to `https://<your-secretserver-domain>/SecretServer`, where `<your-secretserver-domain>` should be replaced with your actual Secret Server domain name. It assigns the domain as 'local' and enables additional options for Web Password Filler.

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

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

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

Configuring Boolean and Session Settings

Customize your `settings.json` file to control Web Password Filler's behavior. Use Boolean options and session durations to adjust menu placement, URL matching, and how long sessions are recorded.

To configure Boolean and session settings:

1. Open the `settings.json` file in your text editor.
2. Set the Boolean setting for the menu position:
   - Set it to **true** to place the menu in the upper right corner.
   - Set it to **false** to display the pop-up below the credentials field.
3. Set the Boolean setting for URL matching:
   - Set it to **true** to accept only URLs that match the specified pattern.
   - Set it to **false** to allow partial URL matches.
4. Enter a session recording duration.

   Note: The default value is 120 minutes, and the maximum is 480 minutes.

5. Scroll to the section labeled with the browser's identification code and enter a different session recording duration value to override the default for that browser.
6. Save the `settings.json` file.

Settings Reference

Parameter	Default	Description
chromeExtensionID	"mfpddejbpnbjkjoaicfedaljnfeollkh"	This is the ID required for the Chrome browser registration.
edgeExtensionId	"kjldmpkefedgljefehmmfifbhnjngmbh"	This is the ID required for the Edge browser registration.
operaExtensionId	"eemnnadjdifcpkcnpalolohpepihhbbo"	This is the ID required for the Opera browser registration.
firefoxExtensionId	"dd1e31d5-3623-45cb-b1ad-64074d36b360@thycotic.com"	This is the ID required for the Firefox browser registration.

Parameter	Default	Description
ConfigSSUrl	"https://SomeURL/SecretServer"	This is the URL for your Secret Server instance.
ConfigDomain	"local"	This is the domain identification either local or your corporate network domain.
SettingUserSSLogin	true	Boolean that sets the checkbox to enable the Secret Server Login option.
SettingPrompToSave	true	Boolean that sets the checkbox to enable the Prompt to Save option.
SettingShowPopUp	true	Boolean that enables login credentials to pop up automatically. If false you just need to click the Delinea checkmark.
SettingEnableAutoPopulate	true	Boolean that sets the checkbox to enable the Auto Populate option for secrets and passwords.

Parameter	Default	Description
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

Parameter	Default	Description
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 Excluding Sites and Making Exceptions below. Does NOT accept wildcards.
SecretServerLoginWindo	false	If disabled then login window used to open in new tab in same browser.
matchSessionByHost	true	If enabled us host/origin instead of base domain to determine if two tabs record to the same session. If disabled use the base domain. By Default, it's enabled that is by host/origin.

Parameter	Default	Description
PerExtensionOverride	Contains a section for each browser type, with custom values for the 15 settings described in this table (ConfigSSUrl, ConfigDomain, HideConfigPage, etc.).	If a value in this section differs from the default value established at the top of the JSON file, the value here takes precedence for that browser, and overrides the default value.

Excluding Sites and Making Exceptions

You configure exclusions and exceptions in Web Password Filler to control which websites the extension interacts with, ensuring it fills credentials only on authorized login pages. This prevents the extension from interfering with registration forms or other non-login pages.

To exclude sites and make exceptions:

1. Open the `settings.json` file for the Native Messaging Host using a text editor.
2. In the **Exclude** section, enter a wildcard such as `https://*` or `http://*` to exclude all sites.
3. In the **ExcludeException** section, add the exact URL of each login page you want WPF to interact with, omitting any query strings.

   For example, https://MyCompanySite.com/login.aspx

Note: Use wildcards only in the Exclude section, and always use the precise URL in the ExcludeException section.

Setting UI Behavior Based on Preferences

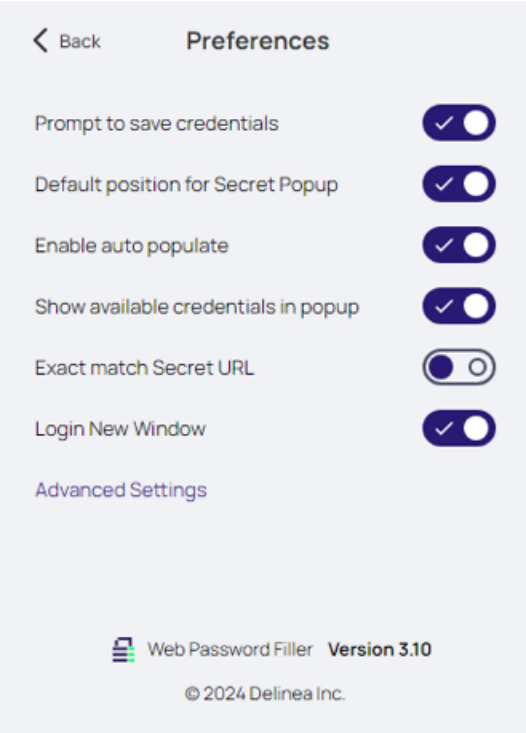
You can update UI behavior settings to control user access and tailor the application's configuration to your organization's needs. These settings are controlled by editing the `settings.json` file, which the application reads to determine which preferences and server details you can see or change in the UI.

To set your UI behavior settings:

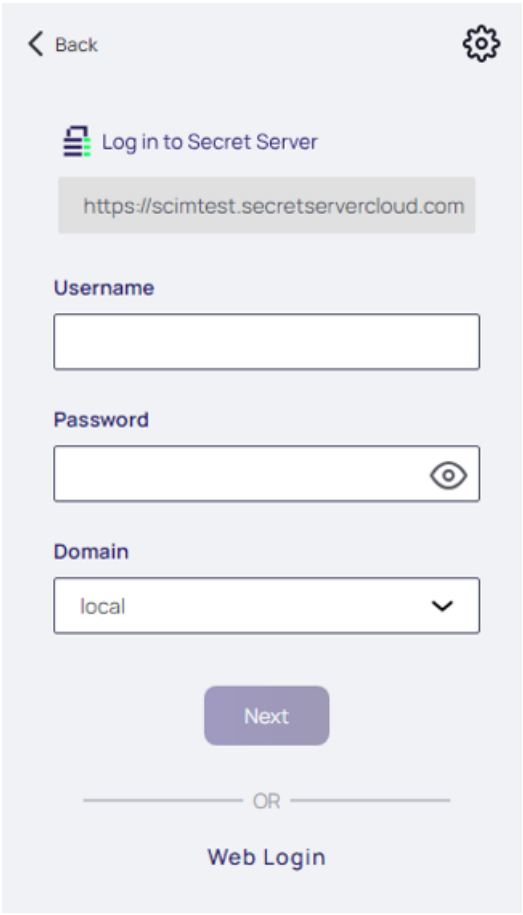
1. Open the `settings.json` file in a text editor.
2. Set each preference on the **Preferences** page to **true** or **false**.

   The following image shows what the **Preferences** dialog looks like to a Native Messaging Host user, based on

the `settings.json` file.



3. Enter the Secret Server URL and Domain as strings (text surrounded by quotation marks).



Note: You can choose to hide the preferences and configuration pages from end users by setting the appropriate flags in this file, preventing unauthorized changes.

Managing Error Messages

The `native-messaging.txt` file records error messages and stores them in the same folder where you install the Native Messaging Host. Use the error messages in this file to troubleshoot issues or provide details when you contact Delinea support services.

Error Message	Meaning	Resolution
There are elements missing from *settings.json*. Review the documentation and update *settings.json* with the missing attributes.	*settings.json* is missing required elements.	Review the *settings.json* format, ensure all elements are present, and verify the file is well formatted.

Error Message	Meaning	Resolution
This application must be run as an administrator when registering for All Users.	The 'EnableForAllUsers' setting is true, but the user lacks administrator permissions to update the registry key.	Run the application as an administrator to register the Native Messaging Host for all users.
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.	ThycoticMessagingHost.exe was executed without a required command line option.	Use `--register` or `--unregister` as a command line argument when running ThycoticMessagingHost.exe.
Incorrect command line. Review the documentation to register or unregister this application.	Only `--register` and `--unregister` are valid command line options.	Review the documentation and use only the supported command line options to register or unregister.

Preventing Users from Disabling Session Recording

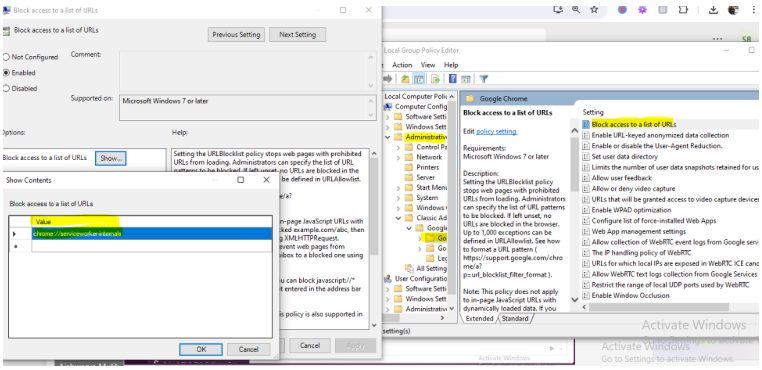
Session Recording now uses a new background system called *service workers* instead of the old background page. Service workers help run your web apps even when you're not actively using them. Users can accidentally stop service workers through a Chrome settings page (chrome://serviceworker-internals),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

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

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

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

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



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

Troubleshooting

The following Troubleshooting topics are available for Web Password Filler:

- "Enabling Diagnostic Logging" on the next page
- WPF Issue Investigation
  - "Managing Compatibility with Previous Products" on page 61
  - "Logging in with Web Password Filler" on the next page
  - "Presenting Behaviors and Problems" on page 61
  - Using Web Password Filler with Microsoft Online Services

Addressing Usability Issues

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

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

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

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

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

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

Logging in with Web Password Filler

Check if you're logged into Web Password Filler.

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

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

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

- Not logged in: 
- Logged in: 

Choosing a Login Method

You can log in using two different methods:

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

For more information on SAML, refer to the Secret Server documentation on SAML.

Troubleshooting Login Issues in Chrome or Edge

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

Enabling Diagnostic Logging

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

Logged items include:

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

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

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

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

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

Managing Compatibility with Previous Products

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

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

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

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

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

Presenting Behaviors and Problems

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

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

Some examples:

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

- Does the site have only one Secret?
  a. If no, can you see all the Secrets? Or can you only see some Secrets?
- Does your logged-in account have access to that Secret?

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

Investigating WPF Issues

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

Confirming WPF Version

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

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

Identifying the Problematic Browser

What browser is the issue occurring on?

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

  General Chromium should work as well, but we do not officially support it.
- Does the issue only occur on one browser? Or does it reproduce for multiple/all browsers?
- If it only reproduces on one browser, which one?

Identifying the Affected Sites

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

- If the issue only happens on one site, what is the URL for that site?

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

Determining Site Access

How are you accessing the site to use WPF?

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

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

Identifying the WPF Version with the Issue

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

Follow these basic steps to find the version number:

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

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

Performing the Action

What type of action are you trying to perform?

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

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

This includes filling credentials for a site

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

Using Templates

What Secret template are you using?

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

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

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

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

Release Notes

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

2025 Release Notes

This section includes the 2025 Web Password Filler Release Notes.

3.11.9 Release Notes

Release Date: November 18, 2025

Improvements

- Added protection against clickjacking attacks that use invisible or hidden layers, as demonstrated at Def Con 33. Added an optional warning (disabled by default) when any page layer covers Web Password Filler; this may trigger on harmless site changes, but existing protections block all known attack versions. (ref: 673136)

Fixed Issues

- Fixed an issue where a field on a non-login form was getting autofilled. (ref: 660330)
- Resolved an autofill issue on https://q2console.okta.com. (ref: 671995)
- Resolved an issue where the error message “Unable to autofill secret from selected secret” appeared when launching a URL list. (ref: 673235)
- Fixed an issue where checking all user input fields on some pages with thousands of fields led to performance issues. (ref: 678140)

3.11.8 Release Notes

Release Date: August 18, 2025

Fixed Issues

- Fixed an issue with Connection Manager integration when the logged-in user in Connection Manager was not the same as the logged-in user in Web Password Filler. (648770)
- Additional checks have been added so that secrets autofill in the proper fields. (654043)
- Improved OTP detection so it autofills correctly. (662918)
- Resolved an autofill issue that stopped working in release 3.11.7 for some sites. (663133, 669883)
- Resolved an issue where the message “Unable to autofill secret from selected secret” appeared when launching a session-recorded secret for the first time after WPF installation. (666721)
- Fixed an issue where a site with mapped fields would not autofill after launch. (668120)

3.11.7 Release Notes

Release Date: July 28, 2025

Improvements

- Improved the handling of launch actions from Connection Manager.
- Clarified the messages displayed to users when a launch or autofill cannot occur due to the secret requiring Incognito mode.

Fixed Issues

- The secret check-in was not logging out users on some Microsoft sites.
- Added a check to determine whether a form is a login form.
- WPF no longer detects the username field of the Add Person form on the Okta portal as a login field.

- Fixed an issue where users were unable to add a secret if required fields were left blank.
- The TOTP was not autofilling on some sites.
- Fixed an issue with autofilling on AWS Identity Center login.
- Only visible input fields were being checked before comparing against the threshold value for login form detection.
- Passwords were not autofilling on some sites.
- The password field now correctly autofills with the user's password instead of being treated as a TOTP field on the Okta Admin Console login.

3.11.6 Release Notes

Release Date: June 06, 2025

Fixed Issues

- Fixed an issue where passwords were immediately cleared after being autofilled on certain Microsoft SSO sites.

3.11.5 Release Notes

Release Date: May 07, 2025

Improvements

- Added support for launching web sessions from Connection Manager 2.7 planned for release in June 2025.

Fixed Issues

- An issue with password generation from the context menu has been resolved.
- When launching from an allow list, the audit log now shows the URL selected from the list.
- WPF now includes 'Sign In' text near fields as an indicator signal for login form detection.
- Fixed a conflict between Web Password Filler and Menlo Remote Browser Isolation that caused usernames and passwords to be populated incorrectly.
- Input threshold now properly prevents autofilling if a page contains more fields than the threshold value.
- WPF is now able to autofill TOTP for the Okta site.
- WPF now correctly autofills TOTP during platform login.
- Fixed an issue where the WPF login window would minimize in Firefox 136 on MacOS Sequoia.

3.11.4 Release Notes

Release Date: March 17, 2025

Fixed Issues

- The 'Update and Save' pop-up did not appear on some sites.
- Fixed an issue where, if the Native Messaging Host was configured, users could only select domains registered in the settings.json file.
- The password was not being autofilled correctly on some Safari browsers.
- Web Password Filler would prevent the login pop-up from appearing when idle.
- A 'Log in and continue' pop-up has been added if WPF is not configured with any sites, or has not been logged in.
- If a user attempts to autofill using a secret that does not have a web launcher mapped, the system now displays 'Unable to autofill from the selected Secret ' instead of silently failing.
- WPF now automatically populates the username field and displays the Delinea WPF icon during logins on Data Domain System Manager (DD2) DELL EMC devices.
- Fixed an issue where the username would not autofill properly on Sophos.

3.11.3 Release Notes

Release Date: February 2, 2025

Improvements

- The Delinea icon is now visible on the username field on any site when Exact Match is enabled, and there are no matching secrets, while prompts to save credentials work properly in this scenario.

Fixed Issues

- The password field was not getting auto-filled on some sites.
- On some sites, the Secret list appeared in the right corner of the site when the Delinea icon was clicked in the username field.
- The Save and Update Password pop-ups were not working properly on some sites.
- Web Password Filler was not submitting tickets according to the configured settings.
- Fixed the security pop-up, which now displays and aligns properly on the Screenrant site.
- The Delinea icon was not visible on the Supermicro device management login page.
- Two error messages were being displayed instead of one when entering the ticket number for a Service Now ticketing system on a secret that requires comment to view.
- The TOTP was not autofilling on AWS logins.

3.11.2 Release Notes

Release Date: January 7, 2025

Improvements

- Improved security of password handling when adding new secrets.
- The prompt to add new secrets now automatically closes after 3 minutes.

Fixed Issues

- For some login pages, the WPF icon was not clickable and users could not display the autofill suggestions.
- After closing recorded sessions for myapps.microsoft.com Web Password Filler was unable to force the site to log out.
- WPF did not autofill the TOTP code on the AWS console login page.
- Prevent scripts on pages that clear login fields from automatically clearing fields after WPF autofills.
- Web Password Filler did not autofill credentials on VMware vRealize.
- The secret URL overlapped with the secret name in the autofill suggestions list on some sites.
- Fixed issues where the WPF icon was incorrectly appearing on input fields within Secret Server and Delinea Platform.

2024 Release Notes

This section includes the 2024 Web Password Filler Release Notes.

3.11.1 Release Notes

Release Date: December 9, 2024

Improvements

- Web Password Filler now auto-fills credentials on the Secret Server and Delinea Platform login pages.
- WPF no longer automatically logs out when a Secret Server or Platform tab is logged out or expires due to inactivity.

Fixed Issues

- Web Password Filler would automatically save a secret if there was only one active template with a URL field. It now displays the Add Secret dialog so users can switch the folder before saving.
- The WPF icon was not appearing on the Verint login page.
- The token refresh interval in WPF has been changed to prevent issues caused by the refresh occurring after the access token has expired.
- WPF automatically filled the username into the MFA field on the Jira Service Management login page.

3.11.0 Release Notes

Release Date: October 30, 2024

Improvements

- Web Password Filler has enhanced how it prioritizes and sorts autofill suggestions:
  - Prioritizes exact matches of the URL first, with favorites that match the URL appearing first.
  - Sorts secrets based on their URL hierarchy.
- Fixed a potential XSS vulnerability when rendering field names during a new secret creation.

Fixed Issues

- Web Password Filler displayed an error message when users added a secret using a secret template where two fields have the same name.
- Changed how Web Password Filler sets the value of TOTP fields to fix an issue where some websites did not detect that a value was entered.
- WPF failed to log users out of the site when secret checkout expired in incognito mode.
- WPF incorrectly identified another field on the site as a login field and auto-populated the credentials into that field.
- WPF failed to log out users from the site when checkout expired or when forcefully checked in.

3.10.3 Release Notes

October 22, 2024

Fixed Issues

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

3.10.2 Release Notes

October 14, 2024

Bug Fixes

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

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

3.10.1 Release Notes

October 04, 2024

Bug Fixes

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

3.10.0 Release Notes

September 30, 2024

Improvements

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

Bug Fixes

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

3.9.6 Release Notes

August 27th, 2024

Enhancements

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

Bug Fixes

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

logged in.

- Fixed an issue with detecting the username field on some Cisco login pages.
- Fixed an issue affecting platform logins using Microsoft SSO when Native Messaging Host is installed.

3.9.5 Release Notes

July 26th, 2024

Bug Fixes

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

3.9.4 Release Notes

June 10th, 2024

Improvements

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

Bug Fixes

- A bug in the caching logic caused some secrets to not show up in the autofill match list.
- The refresh icon appeared in the popup if the user did not have the 'Add Secret' permission and no secrets were present for that site.
- Web Password Filler would sometimes display the 'Add Secret' dialog in the wrong browser window when adding a secret.
- When working in Mimecast, the Web Password Filler icon was displayed for some email fields, even though those fields were not valid for autofill.
- https://sso.cloud.com would not autofill in Web Password Filler.
- Fixed an issue that caused visual corruption in some recorded sessions.
- When using the Web Password Filler popup window to generate a password, the generated password contained duplicate letters. The passwords generated did not follow the Secret Server password policy.
- The system sometimes displayed 404 errors to the user when making background network calls to check the validity of login URLs.
- Updated the autofill field detection logic to handle login forms in Italian.

- Web Password Filler did not close launched Chrome sessions upon secret check in or when the secret timeout limit was reached.
- Web Password Filler reloaded the username page after the user submitted the username on some sites.
- An OTP API call occurred every 30 seconds, even if the user did not have the secret information page open.

3.9.3 Release Notes

May 6th, 2024

Bug Fixes

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

3.9.0 Release Notes

April 8th, 2024

Improvements

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

Bug Fixes

- Secret Servers with 5000+ folders would encounter performance issues during the addition of secrets and folder filtering processes.
- A "Bad Request" error has been resolved when "Exact Match URL" is disabled, autofilling using a secret with a categorized list, and the URL of the current page only partially matches the URL selected from the categorized list.
- Fixed the issue of the Delinea icon not displaying on the username field on some websites.
- The Delinea icon was not visible on the username field for some sites.
- When launching an incognito tab in Safari 17.1, it did not show a warning when the extension was not allowed in private browsing mode.
- When using autofill on secrets, Web Password Filler would remove the first character in both the password and username fields on some sites.
- The dropdown list on Web Password Filler's ticketing system was not aligned properly with other input methods.

- In Safari, certain images failed to display when the <img> tag provided the path '`webkit-masked-url://hidden/`'. To address this issue, it has been converted into SVG.
- The username and password was not being autofilled on some sites.
- If a secret was selected from the secret list, the password was not being autofilled.
- Fixed an issue where the secret list wouldn't load when 50 or more templates contained a URL field. This fix also requires upgrading to Secret Server 11.6 or higher.
- The Web Password Filler icon appeared on the wrong input element on some sites.
- Web Password Filler was trimming the 'www' from URLs when launching secrets.
- Previously, Web Password Filler only checked if the site URL contained the Secret Server domain, resulting in the exclusion of sites where the site URL domain was a substring of the Secret Server domain. Now, Web Password Filler verifies that the site URL domain precisely matches the Secret Server domain.

3.8.0 Release Notes

January 31st, 2024

Improvements

- When the Web Password Filler token expires and cannot be renewed, and the active recordings are still ongoing, the system will redirect the user to the session timeout page. This page will inform the user that the ongoing recording has been terminated.
- When a user attempts to log out from Secret Server or the Platform portal while a session recording is ongoing, they will see a confirmation dialog. This dialog will give the user the choice to either remain logged in or proceed with logging out.
- Web Password Filler now displays the folder name under Secret Details instead of the folder ID. When a user hovers the mouse over folders, the folder path is revealed as a tooltip. Shared secrets with restricted access will show the folder name as 'Restricted Folder'. Root folders will display the folder name as 'None', and when hovering the mouse over a root folder, it will display as 'No Folder'.
- When a user attempts to launch from a different server than the one currently logged into in Web Password Filler and there are active recordings, a confirmation dialog will appear. This dialog will give the user the choice to either launch and close the existing recordings or cancel the launch and keep recording.

Bug Fixes

- Web Password Filler would continuously open new tabs if users turned off the 'Secret Server Login New Window' setting through the Native Messaging Host.
- When users selected the '+' button on the Web Password Filler pop-up to add a secret, it would close the pop-up and not display the 'Add Secret' dialog.
- The Web Password Filler pop-up displayed an invalid logo when saving updated user inputs for username or password.
- Corrected an issue where the Web Password Filler required the 'Session Recording Limit' and 'Input Threshold' drop-down values to be the same number.

- Previously, when Web Password Filler encountered an error logging in it displayed a continually connecting window. In this release, Web Password Filler shows a connecting window with an error message.
- Web Password Filler sometimes automatically logged in when a user logged into Secret Server or Platform in the browser, even though the current URL in Web Password Filler did not match.
- Previously, if the platform user had clicked the 'Cancel' button during a challenge, logged out, then attempted to log in again while the Web Password Filler pop-up was open, the user encountered a challenge pop-up instead of logging in.
- When using Safari 17 the Web Password Filler pop-up would close once the MFA challenge was completed.
- When Safari 17.1 was used, it displayed font weights incorrectly for field labels.
- In Safari 17.1, it did not show a warning when a user launched an incognito tab and the extension was not allowed in private browsing mode.
- In Safari 17.1, certain images in Web Password Filler failed to display.

Known Issues

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

2023 Release Notes

This section includes the 2023 Web Password Filler Release Notes.

3.7.1 Release Notes

December 13th, 2023

Bug Fixes

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

3.7.0 Release Notes

November 7th, 2023

Features

- Users will now see a list of Recent web secrets that is consistent with the Recent secrets list they see in their Secret Server web portal view.

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

Improvements

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

Bug Fixes

- Fixed an issue where the Save button was getting enabled after filling in mandatory fields in the *Add Secret* window.
- Fixed an issue where Web Password Filler displayed an "Platform Identity Authentication has failed" error message when logged into the Delinea Platform.
- Fixed an issue with slow page performance when Web Password Filler is enabled.
- Fixed an issue where Web Password Filler was accepting a "0" value in numerical dropdown fields.
- Fixed an issue where Web Password Filler was displaying improper styling on certain sites.
- Fixed an issue where keyboard shortcuts were note working correctly.
- Fixed an issue where Web Password Filler failed to launch a secret for users who did not have the *Add Secret* permissions.
- Fixed an issue where users were unable to click the *Login* button.
- Fixed an issue where Web Password Filler was not auto-filling BitBucket login pages and for a few other sites.
- Fixed an issue where session recordings missed a few seconds at the beginning.
- Fixed an issue where the *Add Secret* button was not disabled on blank pages.
- Fixed an issue where *Save* and *Update* features were not working on some sites.
- Fixed an issue where Web Password Filler displayed an "Invalid URL" error message while refreshing secret.
- Fixed an issue where Web Password Filler was adding extra spaces when copying the username to the clipboard.
- Fixed an issue where Web Password Filler was not displaying a "Bad Request" message if a user entered an invalid URL.
- Fixed an issue where the copy button was causing URL text or usernames to be overridden.

3.6.1 Release Notes

August 22nd, 2023

Bug Fixes

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

3.6.0 Release Notes

August 21st, 2023

Features

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

General Improvements

- Improved session recording stability.

Security Improvements

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

Bug Fixes

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

Known Issues

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

3.5.4 Release Notes

July 20th, 2023

Improvements

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

Bug Fixes

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

3.5.3 Release Notes

June 20th, 2023

Features

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

Bug Fixes

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

3.5.2 Release Notes

May 30th, 2023

Features

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

Bug Fixes

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

Known Issues

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

3.5.1 Release Notes

May 12th, 2023

Bug Fixes

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

Known Issues

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

3.5.0 Release Notes

May 8th, 2023

Features

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

Bug Fixes

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

Known Issues

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

3.4.4 Release Notes

April 3rd, 2023

Bug Fixes

- Fixed an issue where Web Password Filler was not filling out user credentials for certain sites.
- Fixed an issue where the *Add Secret* window remained open after logging out of Web Password Filler.

- Fixed an issue where Web Password Filler was not autofilling secrets enabled to work only in incognito mode.

3.4.3 Release Notes

March 15th, 2023

Features

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

Security Improvements

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

Bug Fixes

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

2022 Release Notes

This section includes the 2022 Web Password Filler Release Notes.

3.4.2 Release Notes

December 5th, 2022

Features

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

General Maintenance

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

Bug Fixes

- Fixed an issue where nothing would happen when the user clicked "+" to add a secret in Chrome on a Mac
- Fixed an issue where Web Password Filler would not auto-populate when using URL lists
- Fixed an issue where users with *View Only* permissions were unable to use URL lists
- Fixed an issue where Web Password Filler was not properly handling special characters when adding a secret
- Fixed an issue where the *Copy Generated Password* functionality was not working

- Fixed an issue where Web Password Filler was not filling in passwords for some sites
- Fixed an issue where session processing would take too long for sites mentioned in extended mapping
- Fixed an issue where Web Password Filler was overwriting other mapped fields if the input type was "password"
- Fixed an issue where the *Comment Required* popup was not appearing when the "Hide Secret Server Version Number" setting was enabled
- Fixed an issue where the silent login window was not disappearing once the user disabled the *Use Secret Server To Login* toggle
- Fixed an issue where the Secret Server configuration URL field remained clickable when native messaging host was configured
- Fixed an issue where Web Password Filler would display an error message when redirecting from *http://* to *https://*
- Fixed an issue where the session recording icon continued to appear even after the user logged out from Web Password Filler.

Known Issues

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

3.4.1 Release Notes

September 23rd, 2022

Bug Fixes

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

3.4.0 Release Notes

August 18th, 2022

Features

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

Product Enhancements

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

Bug Fixes

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

3.3.0 Release Notes

June 21th, 2022

Features

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

Bug Fixes

- Fixed an issue where Web Password Filler intermittently shows an error popup after populating secret for https://www.portal.azure.com or https://portal.office.com
- Fixed an issue where an add comments popup appears on the Current Active tab instead of launching the URL in another tab if a Requires Comment-enabled secret launches from the Recent/Favorite tab.
- Fixed an issue where Web Password Filler was not showing a popup message when the connection with Secret Server was lost while session recording was in progress.
- Fixed an issue where the Thycotic icon would appear while creating a new user in Secret Server version 11.1.6.
- Fixed an issue where the Secret list was not appearing and the Web launcher was not working for SSO sites.
- Fixed an issue where an update password popup would appear after a user updates the username of a secret.
- Fixed an issue where the user would need to manually reload Secret Server webpages opened in the browser.
- Fixed an issue where the Customized Web Launcher UI Popup was not displaying properly.
- Fixed an issue where the secret name was overlapping with other secrets in the Recent tab if the name was very long.
- Fixed an issue where the Metadata (xpath) for Web Password Filler was not working.

- Fixed an issue where the Add Secret "+" button was enabled when a user, who does not have permission to add a secret, logged into Web Password Filler.
- Fixed an issue where Web Password Filler was displaying an error popup when updating a password.
- Fixed an issue where Web Password Filler was not refreshing secrets properly.
- Fixed an issue where UI elements on the Configuration page were not properly aligned when Web Password Filler was displaying an error.
- Fixed an issue where Web Password Filler closed launched tabs when left idle for 5 - 25 minutes and caused Google Chrome to freeze.
- Fixed an issue where Web Password Filler was showing a blank secret information page.

iOS Specific

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

3.2.0 Release Notes

February 9th, 2022

Product Enhancements

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

Bug Fixes

- Support was added for the web launcher, mapping, and session recording to correctly work with https://dcwebc.farelogix.com/sprk-lhg/
- Secret policy didn't apply when the was secret added via WPF.
- Fixed an issue which caused a 400 error when launching Secrets, despite the users being logged in.
- WPF with recording - Crowdstrike Falcon agent on MacOS causes Chrome thread high CPU and unresponsive browser when launching to myapps.microsoft.com.
- Resolved an issue when after an URL change the session recording stopped.
- Resolved issues with the Recent and Favorites tab in version 3.1.
- Infinite loop issue with WPF 3.1 with Microsoft Edge when logging in with the option "Secret Server - Login New Window disabled".
- Fixed problems with multiple URL fields not being recognized as URLs and as such not being auto-populated.

- Issues with auto population of username and password in WPF 3.1.
- WPF does not autofill passwords for sites with SSO.
- WPF 3.1 does not populate fields on secrets with Incognito Mode and Hide Launcher Password set to Yes.
- Resolved an issue with WPF secrets being opened in new Window, which left users on the last tab following the token generation.
- Resolved permission issues for "portal.azure.com" and subsequent sites.
- Resolved an MSFT Edge issue with unused secrets.
- Improved error messaging with Password Validation on Create relating to specific templates.

Known Issues

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

Browser Related

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

2021 Release Notes

This section includes the 2021 Web Password Filler Release Notes.

3.1.0 Release Notes

October 21, 2021

Product Enhancements

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

- The main WPF window, which opens when you click the active Web Password Filler icon in the upper right corner of your browser, displays two new tabs. One tab lists Recently-used secrets and the other lists secrets the user has marked as Favorites, for quick access.
- The footer of the main WPF window now indicates the URL of the Secret Server the user is logged into.
- When a user hovers their cursor over a Secret in the main WPF window, a Fill icon appears. If the URL in the secret matches the URL of the active browser tab, clicking the icon fills in the user's credentials on the page. If the URL in the Secret does not match the active browser tab, clicking the icon brings the user to the page

matching the URL in the Secret, where credentials can be filled in.

- When a user clicks anywhere on a Secret panel in the main WPF window, the Secret Details view opens. When a user hovers their cursor over the URL, Username, or Password fields, a new Copy icon appears that the user can click to copy the content of that field. The user receives a Toaster confirmation when the information is copied. If the user attempts to copy a password that they lack permissions to view, a popup explains that they cannot copy it.
- Web Password Filler can now be configured to have the Secret Server Login Window open in a new browser tab when the user disables or turns off the setting "Secret Server Login New Window."
- When a user is accessing a website with a checked-out secret and the maximum checkout time has passed, WPF closes the associated path and deletes the cookies, ending the user's logged-in session for improved security. The user then needs to check out the secret again to re-access the site through the Web Password Filler.

Known Issues

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

Bug Fixes

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

3.0.1 Hot Fix Release Notes

August 3, 2021

Product Improvement

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

Bug Fix

In some situations, the Web Password Filler 3.0.0 extension populated the password field with ***Not Valid For Display*** instead of the real password. This happened when the user did not have permission to view the password

due to a newer method used in that release. This issue has been resolved in this hot fix.

Please refer to 3.0.0 Release Notes for more updates.

3.0.0 Release Notes

July 16, 2021

Improvements

- **New User Interface Elements**: New UI design elements have been added to several pages including the home page, login experience, preferences with toggle switches, and a link to launch Secret Server via WPF.
- **Session Recording**: Previously when a session recording was active on a Chrome browser tab but the user was inactive in the browser/tab for more than five minutes, Secret Server assumed the session had ended. Now a "heartbeat" is sent every two minutes to let Secret Server know that the session is still alive even though the user is not interacting with it.
- **Field Mapping**: Some websites use unconventional labels to internally identify their username, password, and other login fields, and the Web Password Filler cannot automatically identify these fields. Users can map the fields on the Web page to the fields in the Secret using intuitive drag-and-drop functionality. To enable the field mapping function in the Web Password Filler, an administrator must add a new metadata section in Secret Server named WPFHints, which saves the field tag mapping information on the Secret.
- **Safari Support**: The Safari Web Password Filler extension now supports all functionality available in the other supported browser extensions.
- **Switch to the logged-in Secret Server**: When a Web Password Filler user launches a Secret from an instance of Secret Server that is not configured for WPF, WPF now prompts the user with the message, "Do you want to switch to the logged in Secret Server?" The user can then switch to the appropriate instance of Secret Server to complete their web login process.
- **Performance**: Fixed performance issues users were experiencing when installing or re-enabling the WPF extension for their browser.

Bug Fixes

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

Known Issues

Issue

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

Issue

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

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

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

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

Choose one of these three work-arounds:

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

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

Choose one of these three work-arounds:

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

2.0.6 Release Notes

May 25, 2021

Improvements

Web Password Filler now provides improved performance for session recording.

Bug Fixes

- Resolved issues where WPF was not working on some sites; `massmutual.okta.com`, `hitachi IAM`, `idp.secureworks.com`, `online.adp.com`, `photovisi.com`, `oracle weblogic server`, and `greenshadesonline.com`.
- Resolved an issue of WPF failing to exclude very long URLs that were on the Native Messaging Host (NMH) exclusion list. Web Password Filler now optimizes the query string and evaluates it for exclusion before sending the URL to the NMH.

- Resolved an issue of the Time-based One Time Password (TOTP) function failing in Web Password Filler when the browser language was not set to English. Web Password Filler now includes the localized TOTP messages that ship with Secret Server.
- Resolved an issue of session recording failing on sites that contained iframe or frame sets if the SRC value was in both the parent and child. WPF now ensures that it does not attempt to record the same tab twice regardless of child window source.
- Resolved an issue of Web Password Filler incorrectly displaying the **Login with Secret Server** window on some high resolution screens not being positioned optimally or appearing minimized.
- Web Password Filler now correctly identifies a username field when the element type is a textarea.
- "USER_IDENT" is used on some websites to identify the username field, and is now included in the Web Password Filler criteria for identifying a username field.

Known Issues/Limitations

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

2.0.5 Release Notes

March 30, 2021

Features

- When you are signing into Secret Server through WPF, a token is automatically generated for you. A window opens briefly showing the Generate Token button being pushed automatically, then the window closes.
- When you are logged into both Secret Server and Web Password Filler and you then log out of Secret Server, you are now automatically logged out of Web Password Filler.
- When you are logged into Secret Server and you click on a URL where you have a Secret configured, you will now be automatically logged into WPF, have a token generated for you, and have your credentials populated into the sign-in fields for the website.
- You can now specify the position for your pop-up Secrets list to appear: in the upper right corner of your window (default) or just below the username field, using the Native Messaging Host configuration file.
- When you are connected to WPF and you close your browser window without logging out, you will remain connected to WPF when you re-open your browser. You will still be logged into WPF for the duration of your web session timeout specified in Secret Server. In enable this feature, you must use the Native Messaging Host configuration file.
- When you are recording a session in an incognito window and the session recording ends due to a recording timeout limit (default 2 hours), WPF will close only those tabs where the session recording ended due to a timeout limit.
- Users and administrators can now extend the default recording time of two hours for a session to a maximum of eight hours, using the Native Messaging Host configuration file.

- You can now choose to have WPF require exact URL matches. If you choose this setting and the URL you browse to is not an exact match for the URL stored in the Secret, WPF will not display the Delinea checkmark logo and will not automatically populate your credentials into the website's username/password fields. See Native Messaging Host.
- In Safari, WPF now prompts the user with a message when using a secret that requires check out.
- When WPF encounters errors in the Native Messaging Host JSON file, it now logs those errors in the native-messaging.log file.
- You can now manually refresh your list of available Secrets by right-clicking the Delinea checkmark logo in a credentials field, clicking Secret Server Web Password Filler, and clicking Refresh Secrets. See Native Messaging Host.

Bug Fixes

- Resolved an issue of WPF automatically populating values on some websites even when auto populate was deselected.
- For security reasons when you log out of Secret Server, you will be logged out of WPF as well, even if you were logged in as two different users. This is expected behavior.
- Resolved an issue of WPF not adding some alphabet characters to fields when adding a Secret using “Add Account to Secret Server.”
- Resolved an issue of WPF generating an error related to Secrets with Checkout enabled.
- Resolved an issue of WPF generating a 400 Error when launching Secrets from Secret Server via WPF.
- Resolved an issue of WPF not detecting Secret Server login when using Duo MFA.
- Resolved an issue of WPF opening an extra blank tab when launching a webpage in Incognito mode.
- Resolved an issue of WPF filling the username field on the Microsoft authentication TOTP page.
- Resolved an issue of the Login button being grayed out when the WPF launcher populates credentials or launches a Secret.
- Resolved an issue of WPF being unable to find username controls on the Oracle WebLogic Console login page.
- Added logic to retry and stop when pages became unresponsive attempting to overwrite WPF changes to the background image.
- Resolved an issue of WPF prompting the user to enter credentials on a new page after they have already logged into that website.
- Resolved an issue with service now incident time logs page being auto filled by secret credentials
- Resolved an issue in the Safari browser after the user clicks “Show All,” of WPF displaying only the window in focus while leaving the non-focused windows in the background.
- Resolved an issue in the Safari browser of WPF not closing the About popup window.
- Resolved an issue in the Safari browser of WPF not correctly identifying a username field named “usr.”
- Resolved issues of WPF filling undesired form fields on multiple websites, including the following:

- IBM Storewize V7000
- Imperva Securesphere Management
- Kaseya VSA, Daffron Customer Information Systems
- Oracle netsuite and slm.saas.services
- Various sites reported by IH Mississippi Valley Credit Union
- Various internally-developed Web apps
- `http://isupportsvr1/rep`
- `http://premieragent.zillow.com/crm/agentlogin`
- `https://cmpame.cmpa.org`
- `https://comp.makonetworks.com`
- `https://hqprrsa02.cmpa.org:7004/console-ims`
- `https://nystateofhealth.ny.gov/`
- `https://prtg.centergrid.com/`
- `https://secure.trust-provider.com/`
- `www.logicmonitor.com`

Known Issues and Limitations

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

Answers to FAQs

- On macOS Big Sur 11.0.1 and 11.2.0, some WPF tabs can appear distorted. To correct this issue, please upgrade your macOS OS to the newest version.
- WPF now supports Safari running on the following macOS versions: Catalina, Mojave, Big Sur 11.1.0, 11.2.1 and later.
- Live Session Monitoring is not supported for sessions recorded by WPF.
- The Diagnostic button is visible when you are on a website. It is not visible when you open a blank tab or a new window.
- If you are logged into Secret Server and WPF as the same user or as different users, when you log out of Secret Server you will be logged out of WPF also. This is expected behavior because, for security reasons all cookies are cleared for the instance when you log out of Secret Server.
- accounts.booking.com, 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.

2020 Release Notes

This section includes the 2020 Web Password Filler Release Notes.

2.0.4 Release Notes

December 23, 2020

Enhancements

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

Bug Fixes

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

Known Limitations

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

2.0.3 Release Notes

Enhancements

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

    Note: The user story is that the exclusion list is set to exclude a site at URL `Company1.site1.com` but has an exclusion exception for `Company1.site1.com/login.aspx`. In this case if they navigate to the login page then the secret will auto-populate in the login fields (if users only have 1 secret). After users login and go to any other page on the site that also has fields which are detected as username/password type fields, the Web Password Filler will not do anything unless directed by the user. This is to prevent the Web Password Filler from auto filling values in fields, when the auto fill action is unwanted.
- Added a new “Site” drop down option to the “Add Secret” dialog in the Web Password Filler, to allow users to select which Secret Server Distributed Engine site a Secret should be saved to (defaults to “Local” value)

Security

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

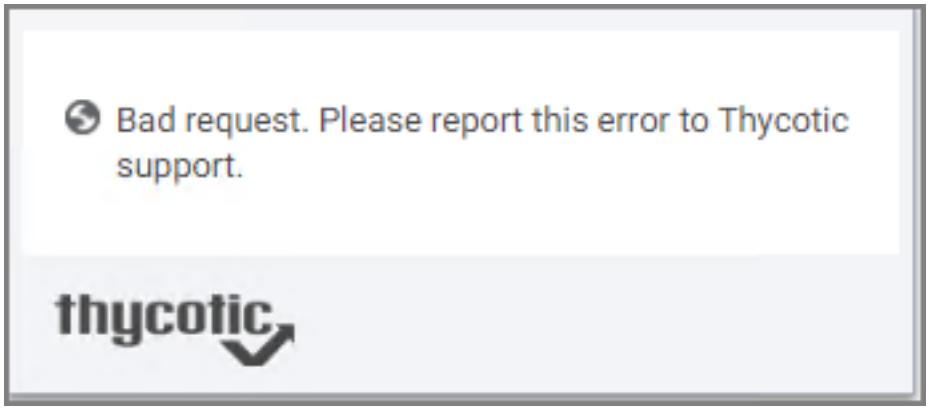
Bug Fixes

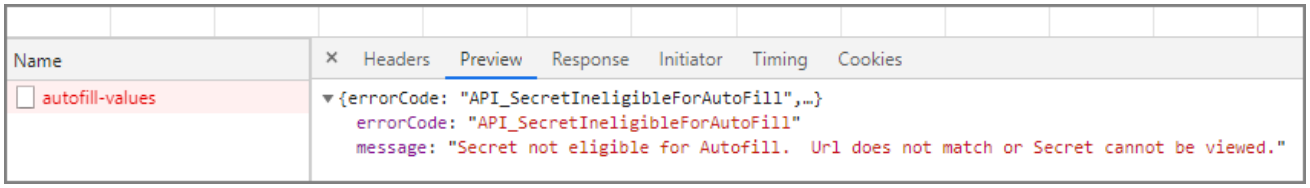
- Resolved an issue with a PaloAltoNetwork site that prevented the Password from auto filling after selecting the Secret.
- Resolved an issue with the Cisco APIC console returning a “Token Error” message after the login fields were populated and the user tried to log in.
- Resolved an issue for a Wells Fargo site login (https://wellsoffice.ceo.wellsfargo.com) where the “Login” button was still disabled by the site after the login fields were populated with valid values.
- Resolved an issue with the Delinea Force Customer portal login that prevented the site from reading valid values in the login fields when the “Log in” button is clicked.
- Resolved an issue that returned the message “Enter a value in the User Name field” even when a value was entered by the Web Password Filler on https://delinea.force.com/support/s/login.
- Resolved an issue that displayed a deleted Secret in the Secret list for a site, if the user deleted the secret in Secret Server after they logged into the Web Password Filler, but before the WPF refreshed its list.

- Resolved an issue for DUO login sites that prevented the page URL from being captured in the “URL” field when adding a new Secret on the “Add Account to Secret Server” dialog.
- Resolved an issue that prevented users from logging into the Web Password Filler with multiple Identity Providers configured and the Secret Server URL ending with a double slash (for example, https://Domain.Company/SecretServer//”)
- Resolved issue for sites that prevented the username or password for an existing Secret from being updated:
  - https://adobeid-na1.services.adobe.com, https://secureb.eyefinity.com, https://admin.zscaler.net, https://app.zipbooks.com, https://mibank.com, https://www.economist.com, https://www.internic.ca, https://www.svbconnect.com, https://id.getharvest.com, https://login.bnymellonwealth.com, https://www.sumopaint.com

Known Issues

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





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

2.0.2 Release Notes

Enhancements

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

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

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

Bug Fixes

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

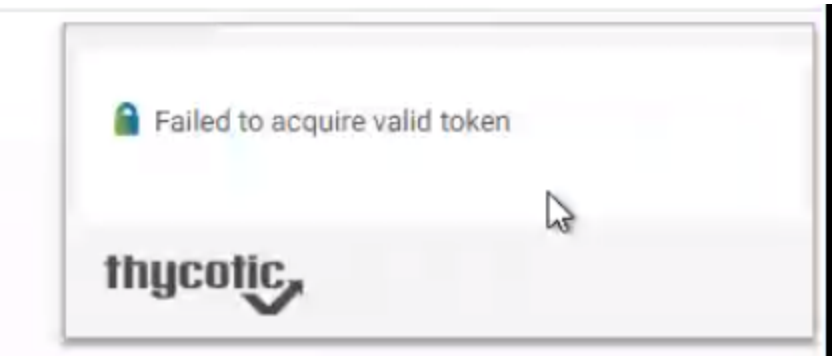
- Resolved an issue where logging into a Microsoft Online account with a username that is in all capital letters results in the password field being cleared (by the site) when it redirects to the password page.
- Resolved an issue for browser tabs being closed when multiple Secrets (with session recording)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

Known Issues

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



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



  This is expected behavior. The first log in will be successful and the user will be logged into WPF. There is no reason to have the additional tabs open and the user can simply close the additional tabs.
- If WPF Secret Server configuration has two back slashes at the end of the URL, the generated token does not appear to work. Resolution, remove one of the back slashes:
  - incorrect -> `https://mysecretServer//`
  - correct -> `https://mysecretServer/` OR `https://mysecretServer`

2.0.1 Release Notes

Enhancements

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

Bug Fixes

- Security: Fixed a JavaScript code injection issue.
- Fixed an issue where the “Refresh” icon is not displayed on the Secret list intermittently.
- Fixed styling issues for “Save your password” dialog for “Launchpad” site.
- Improved error handling and error message when no folders are found on “Add Secret” action.
- Fixed and 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

Enhancements

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

  Example, https://*Company.Sub.Primary.Domain*/subsite
- Improved support for sites that have multi-part top level domains, or parent domains in the URL. For example, this would include sites that have ".co.uk" or ".online.com", etc.

Bug Fixes

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

1.1.0 Release Notes

Enhancements

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

Bug Fixes

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

Firefox Specific

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

1.0.9 Release Notes

Bug Fixes

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

1.0.8 Release Notes

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

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

1.0.10 Release Notes

Enhancements

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