WebData Control Product Guide

Version 4.5

WEBDATA CONTROL

Contents

About WebData Control

With web-based applications and internet browsing being the norm today, the data generated by modern web browsers is increasingly causing system administrators issues. As ever, system administrators want to provide better controls, more security and minimize costs, whilst end users expect a great user experience, a fast logon and the same consistent experience in every session and on each machine, they use.

When delivering modern workspaces IT departments are often faced with the reality of having to provide and support multiple web browsers. With Windows 10, Internet Explorer and Microsoft Edge are present by default and the decision is often taken to provide Google Chrome or Mozilla Firefox as an alternative web browser for users on all operating systems.

The reason for the delivery of multiple browsers often relates to website compatibility with some websites only working correctly in a certain browser. An example of this would be websites which leverage ActiveX controls which only function in Internet Explorer. Other websites may not render correctly in certain browsers but work perfectly in others which makes things more complicated.

WebData Control provides a set of tools to assist with tackling these challenges in the form of three main features:

- WebData Management
- Browser Redirector
- Favorites Synchronization

WebData Management

Browser Redirector

Favorites Synchronization

WebData Management

Internet Explorer (IE), Google Chrome, Mozilla Firefox, and more recently Microsoft Edge are often provided as the standard mechanisms for browsing the internet and accessing web-based applications. These browsers all have proprietary mechanisms for storing cookies, browsing history, temporary internet files and document object model (DOM) information. This data needs managing to provide users with an optimal and consistent user experience.

WebData Control has been designed to allow for the granular management of this browser generated data to sanitize and optimize it based on the needs of the IT department, facilitating the ability to provide end users a great user experience.

Looking at Internet Explorer 11 and Microsoft Edge, much of the data corresponding to web browsing is now indexed and held within a central database, the webcachev01.dat. This database is in %UserProfile%\AppData\Local\Microsoft\Windows\WebCache. To identify data such as cookies and browsing history, you need the actual files on disk, the associated registry data, and the webcache database. If any one of these are not present, then the data is redundant, affecting the user experience.

This webcache database brings in major issues when we look at users roaming between devices. The webcache database starts at 26-32MB (dependent on OS version) and rapidly grows as users use the system. Things such as Universal Apps available from the Windows store, and simple browsing of the local network writes data into the database. This means that webcache files can rapidly grow to 100's of Megabytes.

For Google Chrome and Mozilla Firefox, the story is much the same with databases being used to store cookies, browsing history and supporting data. The file system is also used to store temporary internet files, browser cache information and other data such as frequently visited sites. These databases rapidly grow as users interact with the browsers and storing and restoring this data between sessions leads to increased storage costs, greater network utilization, and often, significantly longer logon and logoff times.

WebData Control is unique and provides a fresh solution to the problem. The conventional way is to allow the dataset to grow and increase centralized storage or make the decision to no longer manage this data. With WebData Control, the administrator can define which data is kept, and which data is removed. It seamlessly manages the contents of the browser databases, the relevant files on disk and relevant registry entries for a complete all-in-one solution.

Browser Redirector

With businesses now using browser-based applications more than ever before, this can present challenges for IT departments and users alike. Certain browser-based applications work best in a certain web browser, so IT departments need to provide multiple browsers to allow users to access different websites in different browsers for compatibility reasons. Some web-based applications work best in Google Chrome for example, but older line of business web-based applications require Internet Explorer for example.

WebData Control's Browser Redirection feature can help overcome these challenges by allowing administrators to define policies to ensure certain URLs are always launched in a certain browser. When a user clicks a URL link or types a URL to the browser address bar, WebData Control intercepts the request and routes it to the correct browser based on the rules that have been defined.

Favorites Synchronization

With users having access to multiple browsers, the management of browser bookmarks and favorites can be an issue. When users add a bookmark or favorite in a browser, they can then struggle to remember which browser they added it to. Users may also add a favorite in a browser which does not render the website or webpage correctly, causing users frustration and loss of productivity.

To assist with these challenges, WebData Control provides capabilities around the management of browser bookmarks and favorites. Using WebData Control favorites synchronization feature, administrators can provision default bookmarks/favorites to specific browsers and synchronize all non-default bookmarks/favorites between the different browsers based on their requirements.

WebData Control Features

Browser Support

The WebData Management. Browser Redirector and Favorites Synchronization features of WebData Control are supported for the following web browsers:

- Microsoft Internet Explorer 10/11
- Google Chrome
- Mozilla Firefox
- Microsoft Edge

Operating System Support

WebData Control is supported for use on the following operating systems:

- Windows 7
- Windows Server 2008 R2
- Windows 8
- Windows 8.1
- Windows Server 2012 R2
- Windows 10 (1703 and above)
- Windows Server 2016
- Windows Server 2019

WebData Management

Cookie Management

Cookies are essential to enable a rich browsing experience for users. Cookies enhance browsing for users by allowing websites to keep track of user information and preferences. Although many cookies are useful, there are also cookies that are used for other purposes such as tracking and targeting people/computers with adverts.

WebData Control allows you to define which cookies you want to keep and which you want to remove via advanced policies which provide granular control over the management of cookies. Cookies can be managed across all the common browsers that are supported.

WebData Control will remove cookies, cookie files and associated cookie data in the following ways:

- Remove cookie data associated with cookies not created, modified or access in the last x number of days
- Remove cookie data relating to the third-party cookies
- Remove cookie data relating to specific cookie types including known tracking and advertising cookies
- Remove cookie data for expired cookies or cookies which are no longer relevant
- Remove cookie data for defined sites
- Always retain cookie data for defined sites

Note: *For an explanation of cookie terms see Appendix A*

Browsing History Management

Information relating to a user's browsing history is stored by each of the supported web browsers in different ways. WebData Control gives a consistent method for an administrator to configure WebData Control to manage the browsing history retained for users:

- Define how long to keep browsing history
- Remove browsing history data for defined sites
- Always retain browsing history data for defined sites

Temporary Internet Files

Temporary Internet Files are designed to provide a faster web experience by placing much of the data within a webpage locally on the machine. The sheer amount of data stored means that this has long been more of a burden than a useful technology and is historically discarded between sessions. WebData Control provides a fresh approach to the

management of temporary internet files as it is now possible to manage temporary internet files on a per site basis.

DOM Store Data

Document Object Model (DOM) data is stored as websites are visited by users. This DOM data is used to store web page structures and speed up browsing and navigation. The DOM data is often stored in the form of XML, HTML or JScript files. These become large and cumbersome as users browse multiple websites. WebData Control provides the ability to granularly manage the DOM data stored by each browser allowing only required DOM data to be retained.

Compatibility Data

For Internet Explorer and Microsoft Edge, the webcache database holds compatibility information ensuring that older websites are rendered correctly in newer browsers. This is comprised of a default set of URLs provided by Microsoft. WebData Control allows for the default list of sites to be deleted to help reduce the size of the webcache database as much as possible.

Enterprise Mode Data

Internet Explorer and Microsoft Edge both have Enterprise Mode capabilities built in which allow administrators to define how websites are rendered for compatibility. Regardless of whether Enterprise Mode is used, the webcache database contains data related to Enterprise Mode. WebData Control allows for this data to be deleted from webcache to keep the size of the file down to the minimum required.

An additional benefit of removing the Enterprise Mode data from the webcache file is that the data is immediately populated from the EMIE Site list XML file when it is needed overcoming the need to wait for 65 seconds after the browser is launched for a refresh to occur.

Windows Store Applications

With Windows 8 and above, Windows Store Applications were introduced. These applications known as Store Apps, Universal Web Platform apps, Modern UI apps or Metro apps also store web data in both the file system and the webcache database. Much of the data is redundant and not user facing. WebData Control allows for Universal App data to be removed from the webcache database ensuring only relevant data for the user is retained.

Data Optimization

Once all data has been managed as per the defined configuration, WebData Control optimizes the web browser databases ensuring all redundant data is cleared and all residual space is reclaimed. This ensures the databases such as the Internet Explorer and Microsoft Edge webcache database size are kept to an absolute minimum, this will minimize the impact on the supporting infrastructure and ensure better logon/logoff times for the users. Chrome and Firefox databases are also optimized providing the same functionality across all supported browsers. Which databases are optimized depends on the browser and options selected when configuring WebData Control.

Note: *Some white space in the webcache data is marked as reserved and therefore cannot be reclaimed*

Google Chrome Extension Locale Removal

For organizations using Google Chrome there is an option to help manage the data related to extensions that have been installed. Often Chrome extensions come with support for over 40 different locales which are not required by most users.

WebData Control provides a mechanism to remove any locales which are not required, which reduces the size and complexity of the data that is stored by each extension. Locales can be defined for retention as needed, with all other locales being removed.

Google Chrome Extension Removal

Another feature provided in WebData Control is the ability to selectively choose which Google Chrome extensions should be retained and which should be removed. WebData Control can be configured to whitelist, or blacklist extensions based on requirements and any extensions which do not match the policy will be removed or retained as required.

Browser Redirector

WebData Control's Browser Redirector feature can be enabled to allow requests from websites to be intercepted and redirected to a different web browser based on a set of defined policies.

Browser Redirector can be specified as the default browser for each user and will intercept http and https URL requests and redirect them as required. Browser Redirector runs in each user session and acts as a proxy, directing web requests on a per request basis. When a user clicks on a URL in an application the request is intercepted by the Browser Redirector process and launches either Internet Explorer, Google Chrome, Mozilla Firefox or Microsoft Edge depending on the configured policy set. Where a request does not match a defined rule, the default specified "default" browser is used.

When a user types in a URL to a browser the Browser Redirector extensions intercept the request and again act as a proxy, directing web requests on a per request basis. When a matching rule is found the current tab is closed and the request is then launched in the alternative web browser. For example, if a user navigates to https://intranet in Google Chrome but this URL has been defined as an Internet Explorer only URL, the tab in Chrome is closed and the URL is loaded in a new instance/tab in Internet Explorer.

For browser redirector to work the following extensions need to be installed:

Internet Explorer

When WebData Control's Browser Redirector feature is installed an Internet Explorer Browser Helper Object (BHO) is automatically installed. This BHO is responsible for intercepting URL requests inside the Internet Explorer browser.

Google Chrome

To use WebData Control's Browser Redirector feature with Google Chrome an extension needs to be installed for each user. The extension is available from the Google Chrome store - https://chrome.google.com/webstore/detail/avanite-chrome-browser-re/efdgmiheichfaofhdhnkholekmhlcobm and can be installed for users by configuring the appropriate Chrome browser policies.

Mozilla Firefox

To use WebData Control's Browser Redirector feature with Mozilla Firefox an extension needs to be installed for each user. The extension is available from here - https://addons.mozilla.org/en-US/firefox/addon/avanite-browser-redirector/ and can be installed for users by configuring the appropriate Firefox browser policies.

Microsoft Edge

WebData Control's Browser Redirector feature can be used with Microsoft Edge by enabling the "Enable Edge UWP Application" policy. This policy forces the AvaniteBrowserRedirector.appxbundle to be installed which also installs an extension for Microsoft Edge.

Favorites Synchronization

The Internet Explorer, Microsoft Edge, Google Chrome and Mozilla Firefox browsers store bookmarks/favorites in different ways which results in users having a different set of bookmarks/favorites in each of the browsers they use, leading to a less than ideal user experience.

WebData Control allows for all bookmarks/favorites to be synchronized between browsers so that all browsers present the same set of bookmarks/favorites for the user.

In addition, WebData Control allows for a set of default favorites/bookmarks to be provisioned to each browser. These defaults will not synchronize to other browsers allowing for defined favorites/bookmarks to be provided for websites and resources which only work correctly with a specific browser.

The Favorites Synchronization feature also has a "read only" mode where by favorites from all browsers can be stored to a central location. These centrally stored favorites can then be deployed to a new environment to assist with migrations.

Notification Service

The Avanite Notification Service is an option which can be selected as part of the installation. The notification service serves multiple purposes:

- Provide a simple installation and execution mechanism - the service will ensure that the WebData Management component applies to any browser data prior to any profile management solutions and before the user profile is unloaded during the logoff of a user session.
- Enables the Browser Redirector feature to receive notifications for new sessions and ensures that browser requests are intercepted and redirected as required.
- Provides a session-based mechanism to allow the synchronization of Favorites/bookmarks to take place. The service handles all notifications for new sessions and ensures that the Favorites Synchronization is completed for any specified users.

The notification service is not required for the WebData Management feature but is required for Browser Redirector and Favorites Synchronization. The behavior of the notification service can be managed by policies as required.

Installing and Configuring WebData Control

Installation

To use WebData Control it must be installed on each Windows Desktop, Virtual Desktop or Terminal Server where you wish to manage user web data. Both manual and automated installations are possible, and the software is available in both x64 and x86 architectures.

Pre-Requisites

The only pre-requisite for the installation of WebData Control is Microsoft .Net version 4.5 or greater. If not present, then the installation will prompt for the software and exit.

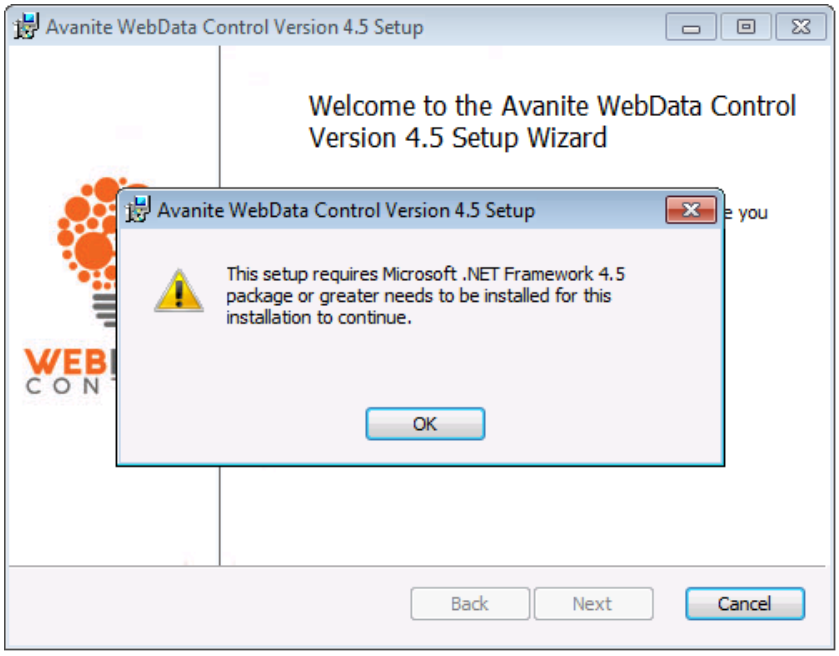

Figure 1 – Required pre-requisite missing

Interactive Installation

To install WebData Control, follow these steps:

1. As an administrator, run AvaWDCx86.msi or AvaWDCx64.msi depending on your system architecture. Click **Next** to continue the installation.

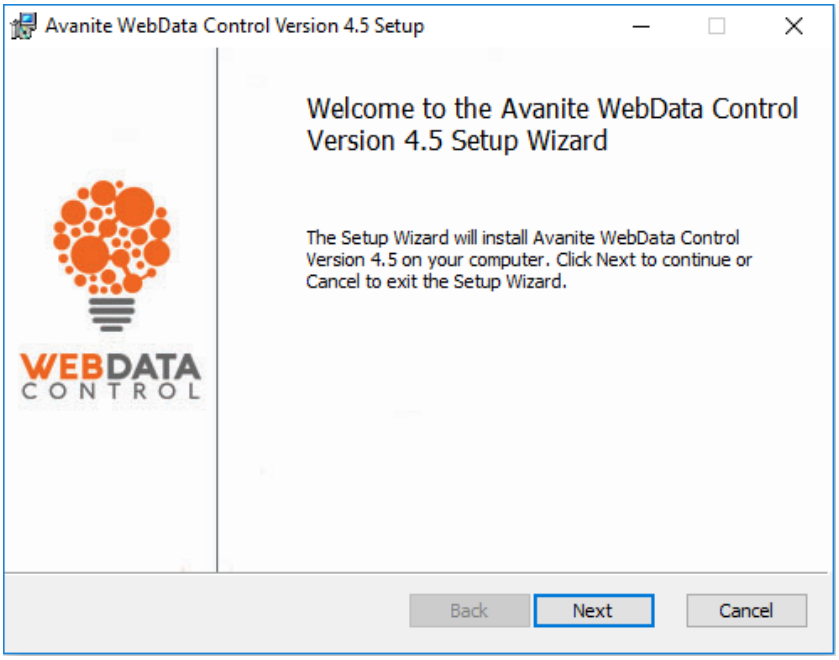

Figure 2 - Welcome screen

2. Read the EULA and if you accept the agreement check the box and click **Next**.

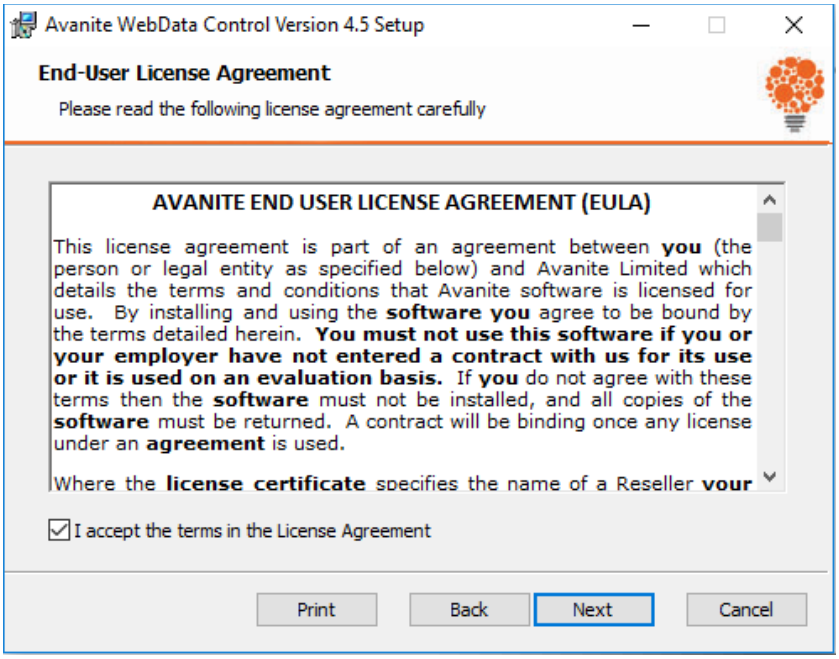

Figure 3 – EULA Acceptance

3. The Custom Setup provides the options to select components to be installed.

   By default, only the WebData Management component is installed.

   Select each component that is required as part of the installation, choosing the relevant options, then click **Next**.

   The installation directory can be changed by selecting the browse button, however it is recommended that the default is kept where possible.

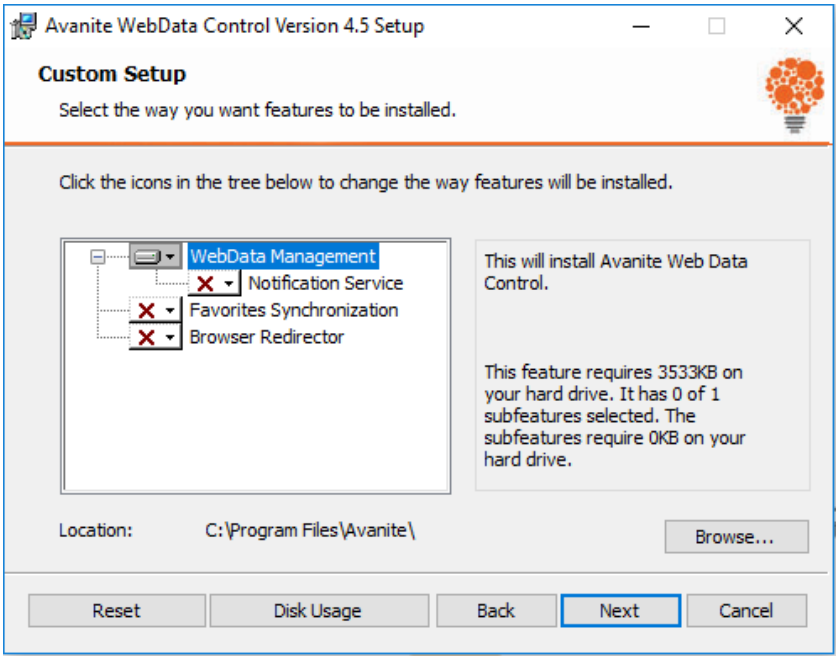

Figure 4 - Custom Setup options

4. Click **Install**.

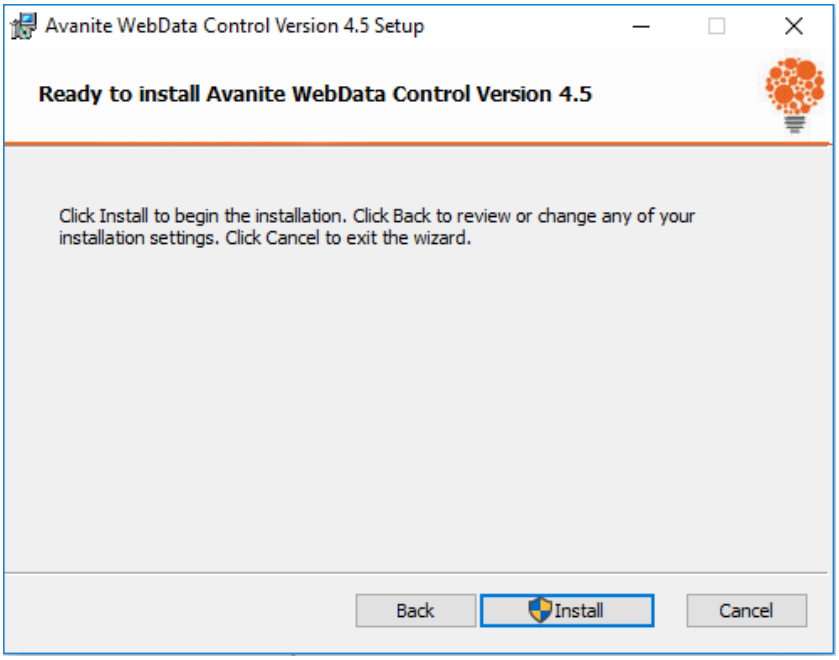

Figure 5 - Confirmation screen

5. After the installation is complete, click **Finish**.

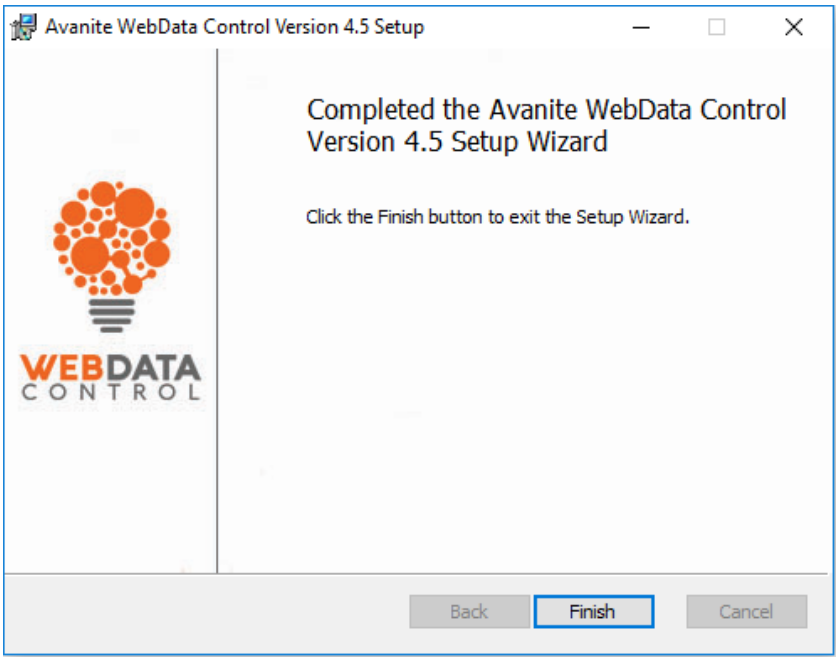

Figure 6 - Setup completion screen

Automated Installation

The installation can also be done using an existing Software Deployment solution, such as Microsoft System Center Configuration Manager (SCCM).

The following is an example of a command line for unattended installation that installs WebData Control and the Notification Service in the default installation directory:

MSIEXEC /qn /i <PathToMSI> /l*v <PathToLogFile> ADDLOCAL="InstallWDM, UseNotificationService, InstallFS,InstallBR"

<PathToMSI> needs to be updated to reference the location of the relevant installer MSI file eg. C:\Install\Avanite\AvaWDC64.msi

<PathToLogFile> needs to be updated to reference a path and filename to store the log file eg. C:\Windows\Logs\Install.log

Each component can be installed by selecting the relevant entry and adding to the ADDLOCAL options list:

InstallWDM – Install the WebData Management component
UseNotificationService – Use the Notification Service to execute WebData Management
InstallFS – Install the Favorites Synchronization component
InstallBR – Install the Browser Redirector component

Licensing

For WebData Control to run it requires the presence of a valid License key. To deploy the license string to the target devices, enable the GPO policy "License" with the Key Licence value from the license file being specified as the value.

```
<?xml version="1.0" encoding="utf-8"?>
<Avanite Version="3.0.1.0">
  <CRCChecks KeyEncryptCRC="5787" KeyCRC="11140" />
  <Licence ClientName="Sample" ExpiryDate="2019-02-11" Perpetual="False" WebDataControl="True">
    <Key Licence="L+YqR75wGHLtiVtSmJOLCnW9Fen6CK/M2rTJ4YUgGYJP1nuzX7/UjyJP+4bgyuawwa/2d3i0BiT121By0TpXig==" />
  </Licence>
</Avanite>
```

Figure 7 - License File

Note: *The License is the text between the quotes in the Key Licence section of the file as shown above*

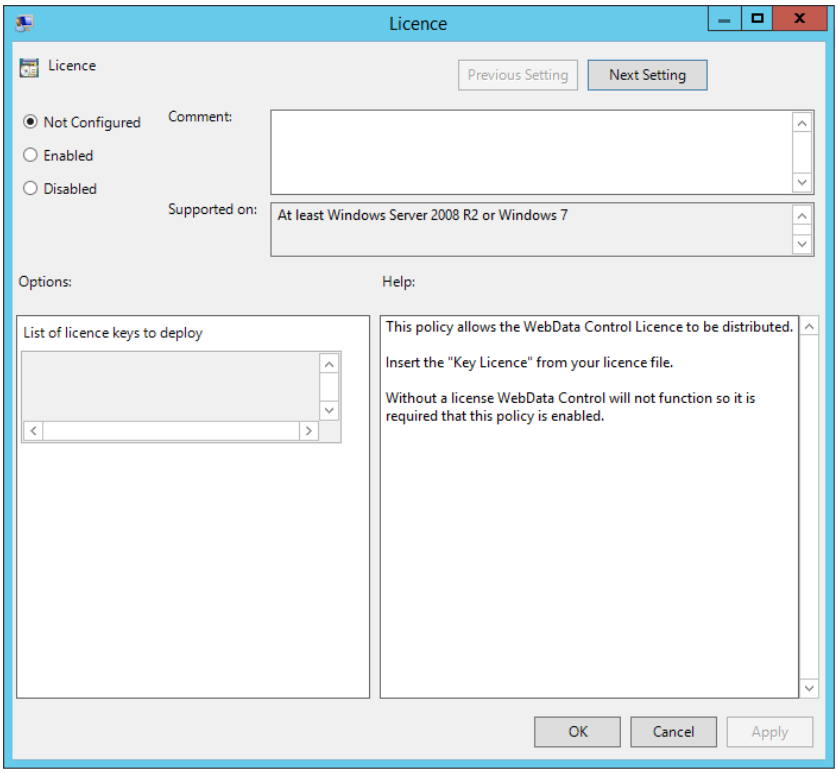

Figure 8 - License Policy

Configuring WebData Control

WebData Management

To use the WebData Management feature of WebData Control, the WebData Management option must be selected for installation.

The WebData Management component can be installed on its own and can be executed using a third-party mechanism. In some circumstances this may be beneficial, as with this approach no system level service will be installed.

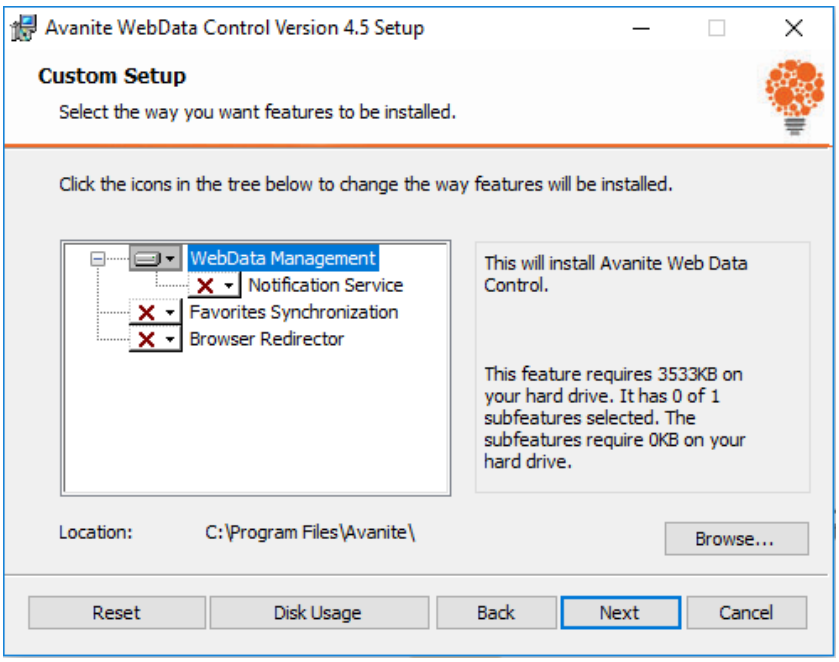

Figure 9 – Install only WebData Management

For guidance around using a third-party mechanism to initiate WebData Management please speak with Avanite Support.

The WebData Management component can also be installed with the Notification Service option selected. When the Notification Service component is selected the "Avanite Notification Service" is installed and will automatically execute WebData Management during the logoff phase of each user session.

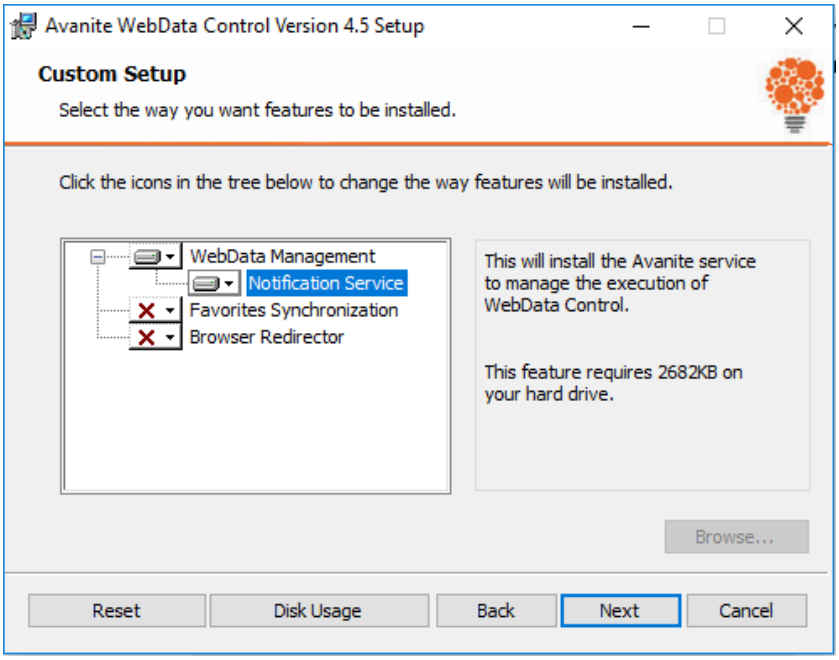

Figure 10 – Install WebData Management and Notification Service

Once the WebData Management component has been installed it needs to be configured using the provided ADMX templates. A recommended set of policies is outlined below to start working with WebData Management when the Notification Service has been installed.

Policy	*Recommended Setting*
Computer\WebData Control\Global	License: ***Enabled***, Value: ***<Enter License Key>***
Computer\WebData Control\Notification Service	Enable WebData Management: ***Enabled***
Computer\WebData Control\WebData Management	Default Configuration: ***Enabled***

Note: *For details of the Default Configuration see Appendix D*

Favorites Synchronization

To use the Favorites Synchronization feature of WebData Control the Favorites Synchronization option must be selected for installation.

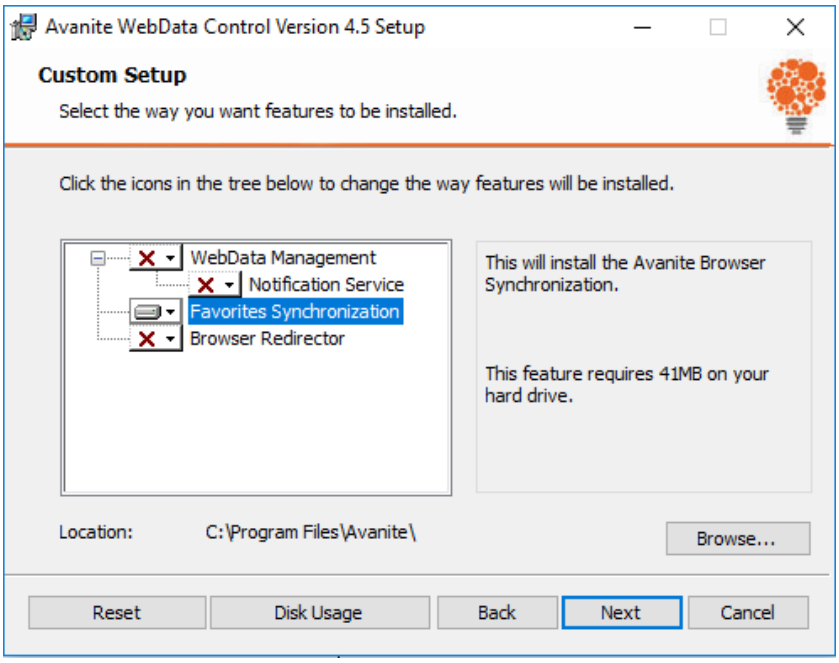

Figure 11 – Install only Favorites Synchronization

The Notification Service is automatically installed when the Favorites Synchronization component is selected for installation as it is required for this feature.

Once the Favorites Synchronization component has been installed it needs to be configured using the provided ADMX templates. A recommended set of policies is outlined below to start working with Favorites Synchronization.

Note: *Only enable the browser specific policies for browsers that are installed/in use)*

Policy	*Recommended Setting*
Computer\WebData Control\Global	License: ***Enabled***, Value: ***<Enter License Key>***
Computer\WebData Control\Notification Service	Enable Favorites Synchronization: ***Enabled***
Computer\WebData Control\Favorites Synchronization	Favorites Browser Selection: ***Enabled***, Values: ***Chrome Synchronization, Edge Synchronization, Firefox Synchronization, Internet Explorer Synchronization*** Force Internet Explorer to close: ***Enabled*** Favorites Storage Location: Enabled, Value: ***<A suitable share\folder path>***

If you are using Windows 10 1809 or above, in addition to the above settings, it is required that the following policies are configured for Microsoft Edge - https://docs.microsoft.com/en-us/microsoft-edge/deploy/group-policies/prelaunch-preload-gp. Without these policies Microsoft Edge runs continuously and stops synchronization from occurring.

Policy	*Recommended Setting*
Computer\Windows Components\Microsoft Edge	Allow Microsoft Edge to pre-launch at Windows start-up, when the system is idle, and each time Microsoft Edge is closed: ***Enabled***, Value: ***Prevent Pre-Launching*** Allow Microsoft Edge to load the Start and New Tab page at Windows startup and each time Microsoft Edge is closed: ***Enabled***, Value: ***Prevent tab preloading***

Browser Redirector

To use the Browser Redirector feature of WebData Control the Browser Redirector option must be selected for installation.

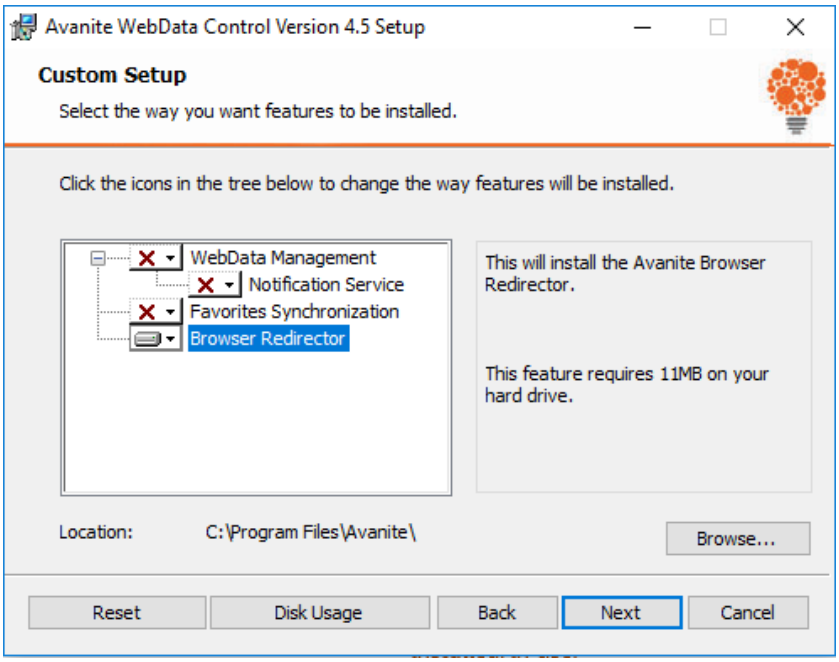

Figure 12 – Install only Browser Redirector

The Notification Service is automatically installed when the Browser Redirector component is selected for installation as it is required for this feature.

Once the Browser Redirector component has been installed it needs to be configured using the provided ADMX templates. A recommended set of policies is outlined below to start working with Browser Redirector.

Note: *Only enable the browser specific policies for browsers that are installed/in use)*

Policy	*Recommended Setting*
Computer\WebData Control\Global	License: ***Enabled***, Value: ***<Enter License Key>***
Computer\WebData Control\Notification Service	Enable Browser Redirector: ***Enabled***
Computer\WebData Control\Browser Redirector	Specify Default Browser: ***Enabled***, Value: ***<Browser of choice>*** Set Browser Redirector as default browser: ***Enabled*** URLs to redirect to Chrome: ***Enabled***, Values: ***<User defined>*** URLs to redirect to Edge: ***Enabled***, Values: ***<User defined>*** URLs to redirect to Firefox: ***Enabled***, Values: ***<User defined>*** URLs to redirect to Internet Explorer: ***Enabled***, Values: ***<User defined>*** Enable Edge UWP Application: ***Enabled***

If using Windows 10 it is required that the following policies are configured for Microsoft Edge. This allows the Avanite Microsoft Edge UWP application to be installed with the required Microsoft Edge extension:

Policy	*Recommended Setting*
Computer\Windows Components\App Package Deployment	Allow all trusted apps to install: ***Enabled***

For Google Chrome the following policy is required to allow the Avanite Chrome Browser Redirector extension to be installed for all users.

Policy	*Recommended Setting*
Computer\Google Chrome\Extensions	Configure the list of force-installed apps and extensions: ***Enabled***, Value: ***efdgmiheichfaofhdhnkholekmhlcobm***

For Mozilla Firefox the following policy is required to allow the Avanite Firefox Browser Redirector extension to be installed for all users.

Policy	*Recommended Setting*
Computer\Mozilla\Firefox\Extensions	Extensions to Install: ***Enabled***, Value: ***https://addons.mozilla.org/firefox/downloads/file/3058337/avanite_browser_redirector_extension-1.5-fx.xpi?src=dp-btn-primary***

It is also recommended that the following policies are reviewed and implemented to ensure the best possible experience for users. These policies disable default browser checks and stop unwanted warnings and messages from being presented to users.

Policy	*Recommended Setting*
Computer\Windows Components\Internet Explorer	Automatically activate newly installed add-ons: ***Enabled*** Turn off add-on performance notifications: ***Enabled***
Computer\Google Chrome	Set Google Chrome as Default Browser: ***Disabled***
Computer\Mozilla\Firefox	Don't Check Default Browser: ***Enabled***
User\Windows Components\Internet Explorer	Notify users if Internet Explorer is not the default web browser: ***Disabled***

WebData Control Policy Settings

Once the Group Policy template has been added, all options can be configured via the Group Policy Management Console.

WebData Control can be configured at the Computer level:

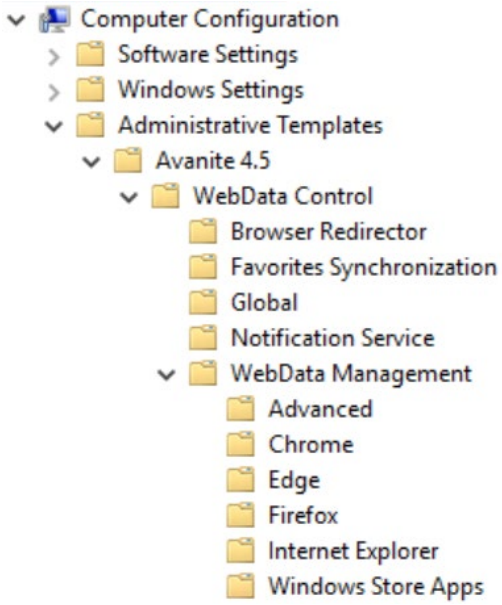

Figure 13 - ADMX Computer Level

WebData Control can also be configured at the User Level:

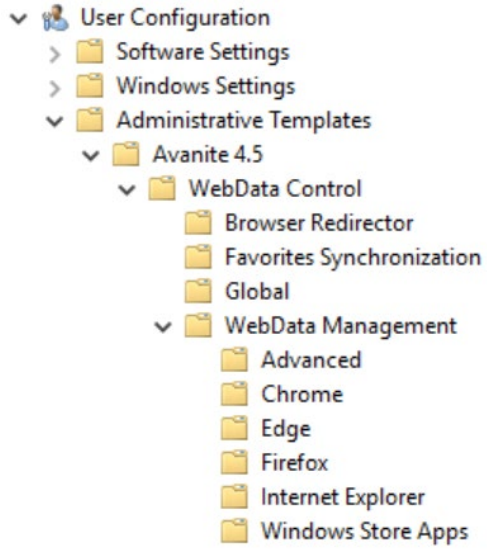

Figure 14 - ADMX User Level

Where policies are configured at both the Computer and User level the User level policies are used.

WebData Control Policy Reference

The following table outlines all the policy options available in the AvaWDCv4-5.admx:

WebData Control\Browser Redirector

Policy	*Description*
Specify Default Browser	This policy configures the default web browser to be used for the environment when the Browser Redirector feature is enabled. When the Browser Redirector component of WebData Control does not have a matching rule configured for redirecting a URL it will be opened in the browser defined here. Where a URL match is found Browser Redirector will launch the specified browser. When no browser is specified the default browser will be set to Internet Explorer. When the specified browser is not installed Internet Explorer will be used. It is recommended that this policy is enabled only when required.
Set Browser Redirector as default browser	This policy configures the Avanite Browser Redirector process as the default browser for each user session. Http and Https protocol requests will be handled by Browser Redirector. If this policy is not enabled, then clicking on URLs will not be supported as the Browser Redirector process needs to be defined as the default browser. The traditional method for setting the default browser can also be used as per https://docs.microsoft.com/en-us/internet-explorer/ie11-deploy-guide/set-the-default-browser-using-group-policy. It is recommended that this policy is enabled only when required.
URLs to redirect to Chrome	This policy configures a set of URLs that will be forced to open in the Chrome browser. The policy accepts inputs in a wildcard format and will directly match any part of a URL being accessed. Example inputs would be: https://www.website.com http://www.website.com website.com website.com/page It is recommended to enter the fullest path possible to ensure the best match. It is recommended that this policy is enabled only when required.

URLs to redirect to Edge	This policy configures a set of URLs that will be forced to open in the Edge browser. The policy accepts inputs in a wildcard format and will directly match any part of a URL being accessed. Example inputs would be: https://www.website.com http://www.website.com website.com website.com/page It is recommended to enter the fullest path possible to ensure the best match. It is recommended that this policy is enabled only when required.
URLs to redirect to Firefox	This policy configures a set of URLs that will be forced to open in the Firefox browser. The policy accepts inputs in a wildcard format and will directly match any part of a URL being accessed. Example inputs would be: https://www.website.com http://www.website.com website.com website.com/page It is recommended to enter the fullest path possible to ensure the best match. It is recommended that this policy is enabled only when required.
URLs to redirect to Internet Explorer	This policy configures a set of URLs that will be forced to open in the Internet Explorer browser. The policy accepts inputs in a wildcard format and will directly match any part of a URL being accessed. Example inputs would be: https://www.website.com http://www.website.com website.com website.com/page It is recommended to enter the fullest path possible to ensure the best match. It is recommended that this policy is enabled only when required.
Chrome Launch Parameters	This policy configures Chrome to launch with a set of specified parameters when redirected to using Browser Redirector. Additional parameters defined here will be passed to Chrome when it is launched via Browser Redirector.

	An example input for Chrome would be: -start-maximised It is recommended that this policy is only enabled when required.
Firefox Launch Parameters	This policy configures Firefox to launch with a set of specified parameters when redirected to using Browser Redirector. Additional parameters defined here will be passed to Firefox when it is launched via Browser Redirector. An example input for Firefox would be: -foreground It is recommended that this policy is only enabled when required.
Internet Explorer Launch Parameters	This policy configures Internet Explorer to launch with a set of specified parameters when redirected to using Browser Redirector. Additional parameters defined here will be passed to Internet Explorer when it is launched via Browser Redirector. An example input for Internet Explorer would be: -k It is recommended that this policy is only enabled when required.
Enable Edge UWP Application	This policy configures the Avanite Browser Redirector UWP application to be installed for users. Enabling this policy will force the Avanite Browser Redirector UWP Application to be installed for each user. This is required to redirect URLs from Edge via the Browser Redirector extension. It is required that this policy be enabled to use Browser Redirector with Edge.
Enable user defined default browser	This policy configures the Avanite Browser Redirector to enable users to select a default browser. Enabling this policy will force the Avanite Browser Redirector to use the user's choice of browser as the default. When a user chooses their own default browser this choice is stored in the HKCU\Software\Avanite key. It is recommended that this policy is enabled only when required.
Enforce default favorites to redirect	This policy forces all URLs specified in the Favorites Synchronization policies to be redirected. Where default favorites have been specified, this policy enforces the URLs for the default favorites are honored with Browser Redirector launching in the relevant browser where the favorite has been created. It is recommended that this policy is enabled only when required.

WebData Control\Favorites Synchronization

Policy	*Description*
Favorites Browser Selection	This policy defines which browsers will be enabled for favorites synchronization. Selecting a browser will enable it for synchronization and favorites will be shared between the browsers that have been enabled. Note: Multiple browsers need to be selected for this policy to have any effect. It is recommended that this policy is enabled only when required.
Force Internet Explorer to close	By default, Internet Explorer keeps the iexplore.exe process alive for 30 seconds after a user closes the browser. Enabling this policy adds the following registry values for each user session to ensure Internet Explorer is not kept alive after the user closes the browser. [HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main] "TabShutdownDelay"=dword:00000000 [HKEY_CURRENT_USER\Software\Wow6432Node\Microsoft\Internet Explorer\Main] "TabShutdownDelay"=dword:00000000 The relevant keys are added based on system architecture. It is recommended that this policy is enabled to ensure Favorites are synchronized in a timely manner.
Favorites Storage Folder	This policy allows an alternative folder to be defined to store the file which holds the user favorites. The file stores all details about the favorites/bookmarks from each of the browsers that are enabled for synchronization. The default location is "%AppData%\Avanite\BrowserFavorites". Enter the path as a literal path or as a UNC path as desired. The folder will be accessed as the user so must have read/write access to the folder specified. It is recommended that this policy is enabled only when required.
Default Chrome Favorites	This policy configures a default set of favorites to be available in Chrome. Enter the name for the favorites and the URL of the favorite to have it created in Chrome automatically. An example would be: Value Name: "Avanite" Value: "https://www.avanite.com/" This would create a shortcut called "Avanite" pointing to "https://www.avanite.com/"

	When a default favorite is created it is automatically excluded from synchronization to other browsers. * A default favorite can be added to a folder by including it as part of the "Value Name". For example "Avanite Favorites\Avanite Home Page" would create a folder called "Avanite Favorites" with a favorite named "Avanite Home Page". * If you want to move the favorite to be under the "Other Bookmarks" folder start the "Value Name" with "other\". For example, "other\Avanite Favorites\Avanite Home Page" would create a folder called "Avanite Favorites" with a favorite named "Avanite Home Page" under the other bookmarks section of Chrome. * If other is not specified then the favorite will be placed on the toolbar. It is recommended that this policy is only enabled when required.
Default Edge Favorites	This policy configures a default set of favorites to be available in Edge. Enter the name for the favorites and the URL of the favorite to have it created in Edge automatically. An example would be: Value Name: "Avanite" Value: "https://www.avanite.com/" This would create a shortcut called "Avanite" pointing to "https://www.avanite.com/" When a default favorites is created it is automatically excluded from synchronization to other browsers. * A default favorite can be added to a folder by including it as part of the "Value Name". For example, "Avanite Favorites\Avanite Home Page" would create a folder called "Avanite Favorites" with a favorite named "Avanite Home Page". * If you want to move the favorite to be under the "Other Bookmarks" folder start the "Value Name" with "other\". For example, "other\Avanite Favorites\Avanite Home Page" would create a folder called "Avanite Favorites" with a favorite named "Avanite Home Page" under the other bookmarks section of Edge. * If other is not specified then the favorite will be placed on the toolbar. It is recommended that this policy is only enabled when required.
Default Firefox Favorites	This policy configures a default set of favorites to be available in Firefox. Enter the name for the favorites and the URL of the favorite to have it created in Firefox automatically. An example would be: Value Name: "Avanite" Value: "https://www.avanite.com/"

	This would create a shortcut called "Avanite" pointing to "https://www.avanite.com/" When a default favorites is created it is automatically excluded from synchronization to other browsers. * A default favorite can be added to a folder by including it as part of the "Value Name". For example, "Avanite Favorites\Avanite Home Page" would create a folder called "Avanite Favorites" with a favorite named "Avanite Home Page". * If you want to move the favorite to be under the "Other Bookmarks" folder start the "Value Name" with "other\". For example, "other\Avanite Favorites\Avanite Home Page" would create a folder called "Avanite Favorites" with a favorite named "Avanite Home Page" under the other bookmarks section of Firefox. * If you want to move the favorite to be under the "Menu Bookmarks" folder start the "Value Name" with "menu\". For example, "menu\Avanite Favorites\Avanite Home Page" would create a folder called "Avanite Favorites" with a favorite named "Avanite Home Page" under the menu bookmarks section of Firefox. * If menu/other is not specified then the favorite will be placed on the toolbar. It is recommended that this policy is only enabled when required.
Default Internet Explorer Favorites	This policy configures a default set of favorites to be available in Internet Explorer. Enter the name for the favorites and the URL of the favorite to have it created in Internet Explorer automatically. An example would be: Value Name: "Avanite" Value: "https://www.avanite.com/" This would create a shortcut called "Avanite" pointing to "https://www.avanite.com/" When a default favorites is created it is automatically excluded from synchronization to other browsers. * A default favorite can be added to a folder by including it as part of the "Value Name". For example, "Avanite Favorites\Avanite Home Page" would create a folder called "Avanite Favorites" with a favorite named "Avanite Home Page". * If you want to move the favorite to be under the "Other Bookmarks" folder start the "Value Name" with "other\". For example, "other\Avanite Favorites\Avanite Home Page" would create a folder called "Avanite Favorites" with a favorite named "Avanite Home Page" under the other bookmarks section of Internet Explorer. * If other is not specified then the favorite will be placed on the toolbar. It is recommended that this policy is only enabled when required.

Read Only Mode	This policy defines whether favorites synchronization operates in read only mode. Enabling this policy enables a "read only" mode where favorites are not synchronized between browsers but the Avanite file which holds the user favorites is still populated. It is recommended that this policy is enabled only when required.

WebData Control\Global

Policy	*Description*
License	This policy allows the WebData Control License to be distributed. Insert the "Key Licence" from your license file. Without a license WebData Control will not function so it is required that this policy is enabled.
Diagnostic Logging	This policy defines whether WebData Control diagnostic logging is enabled or not. Enabling this policy will enable WebData Control logging. Entering "Log path" will define the location of the log files. This only requires a directory as the filename will be generated by the WebData Control E.g. "C:\Temp". It is recommended that this policy is enabled only when required.

WebData Control\Notification Service

Policy	*Description*
Browser Redirector Is Admin Condition	This policy is used to restrict the execution of Browser Redirector to non-administrative users. Enabling this policy will stop the execution of Browser Redirector for users that are members of the local administrators' group. By default, when Browser Redirector is enabled it will be enabled for all users.
Browser Redirector User Group Condition	This policy is used to restrict the execution of Browser Redirector for users based on their Active Directory group membership. Enabling this policy will ensure that Browser Redirector only executes for users that are a member of the specified group. When this policy is enabled Active Directory groups can be specified. Enter in the format {Domain Netbios Name}\{Group Name} separating each entry with a ';' Example: Avanite\User Group 1 or, Avanite\User Group 1;Avanite\User Group 2
Enable Browser Redirector	This policy enables the Browser Redirector feature. Enabling this policy will ensure that Browser Redirector is run by the Avanite Notification Service. Enabling this policy is required if you require Browser Redirector functionality.
Favorites Synchronization Is Admin Condition	This policy is used to restrict the execution of Favorites Synchronization to non-administrative users. Enabling this policy will stop the execution of Favorites Synchronization for users that are members of the local administrators' group. By default, when Favorites Synchronization is enabled it will be enabled for all users.
Favorites Synchronization User Group Condition	This policy is used to restrict the execution of Favorites Synchronization for users based on their Active Directory group membership. Enabling this policy will ensure that Favorites Synchronization only executes for users that are a member of the specified group. When this policy is enabled Active Directory groups can be specified. Enter in the format '{Domain Netbios Name}\{Group Name}' separating each entry with a ';' Example: Avanite\User Group 1 or, Avanite\User Group 1;Avanite\User Group 2
Enable Favorites Synchronization	This policy enables the Favorites Synchronization feature. Enabling this policy will ensure that Favorites Synchronization is run by the Avanite Notification Service. Enabling this policy is required if you require Favorites Synchronization functionality.

WebData Management Is Admin Condition	This policy is used to restrict the execution of WebData Management to non-administrative users. Enabling this policy will stop the execution of WebData Management for users that are members of the local administrators' group. By default, when the Avanite Notification Service is used WebData Control will be executed during the logoff phase of a user session for all users.
WebData Management User Group Condition	This policy is used to restrict the execution of WebData Management for users based on their Active Directory group membership. Enabling this policy will ensure that WebData Management only executes for users that are a member of the specified group. When this policy is enabled Active Directory groups can be specified. Enter in the format {Domain Netbios Name}\{Group Name} separating each entry with a ';' Example: Avanite\User Group 1 or, Avanite\User Group 1;Avanite\User Group 2
Enable WebData Management	This policy enables the WebData Management feature. This policy enables the Avanite notification service to handle the WebData Management features of WebData Control. If this policy is not configured, or set to disabled, then WebData Management can be instigated via a third-party mechanism as required.
WebData Control Logoff Message	This policy defines the logoff message for WebData Control. Enabling this policy allows for a custom logoff message to be displayed when WebData Control is executed during the logoff phase of a user session. By default, when the Avanite Notification Service is used, WebData Control will display a message during logoff.

WebData Control\WebData Management

Policy	*Description*
Default Configuration	This policy defines a default configuration for Avanite's WebData Management. Enabling this policy will setup WebData Management using Avanite's recommended settings. Note: If additional policies are enabled, they will override the Avanite default options. It is recommended that this policy is enabled only when required.

WebData Control\WebData Management\Advanced

Policy	*Description*
URL Whitelisting	This policy specifies retention of data for defined sites. This will override the selected policy settings for all browser types with the exception of the URL Blacklist. Sites specified in the "List of sites to retain" option will have their data retained. Specify data to be retained by defining the part of URL to match. E.g. Entering "Avanite.com/software" would retain data related to "Avanite.com/software" pages. Enabling the "Apply to cookie data" option will retain all cookie data for sites matching the defined URLs. Enabling the "Apply to history data" option will retain all history data for sites matching the defined URLs. Enabling the "Apply to DOM data" option will retain the DOM data for sites matching the defined URLs. DOM data here refers to the Document Object Model data which is used by browsers to store a variety of data required by web browsing and is retained for caching purposes. This option only applies to Internet Explorer and Edge. It is recommended that this policy is enabled, and entries added for intranet websites, internal web applications and line of business websites to ensure that cookies are always retained for these sites.
URL Blacklisting	This policy specifies the removal of data for defined sites. This will override the selected policy settings for all browser types without exception. Sites specified in the "List of sites to remove" option will have their data removed. Specify data to be removed by defining the part of URL to match. E.g. Entering "Avanite.com/software" would remove data related to "Avanite.com/software" pages. Enabling the "Apply to cookie data" option will remove all cookie data for sites matching the defined URLs.

	Enabling the "Apply to history data" option will remove all history data for sites matching the defined URLs. Enabling the "Apply to DOM data" option will remove the DOM data for sites matching the defined URLs. DOM data here refers to the Document Object Model data which is used by browsers to store a variety of data required by web browsing and is retained for caching purposes. This option only applies to Internet Explorer and Edge. It is recommended that this policy is enabled only when required.
Event Logging	This policy adds statistical data to the application event log. Enabling this policy will ensure overall statistics are collected in the application event log. The data will be collected for each execution of the WebData Management and will record data including: WebData Management start/end time, execution time, username, user domain, machine name and operating system. In addition, detailed counts will be recorded, listing what the WebData Control agent has actioned. It is recommended that this policy is enabled only when required.
File Deletion Throttling	This policy allows the option for the number of file deletions to be restricted. Enabling the option allows WebData Management to limit the number of files and folders to be removed from the system during each execution. It is recommended that this policy is enabled only when required.
Data Optimization	This policy allows the option for user web database optimization to be enabled. Enabling this option allows WebData Management to optimize and compact the various web databases to ensure they use a minimum amount of disk space. This applies to the relevant databases including: webcachev01.dat and the databases used by Chrome and Firefox. It is recommended that this policy is enabled.

WebData Control\WebData Management\Chrome

Policy	*Description*
Chrome DOM Data Removal	This policy will remove Chrome DOM data. DOM data here refers to Document Object Model data which is used by browsers to store a variety of data required by web browsing and is retained for caching purposes. Enabling this policy option will cause Chrome DOM data to be removed. It is recommended that this setting is enabled.
Chrome Data Report	This policy will generate data exports of the WebData Management activity for Chrome. There will be a separate file for cookies and history. The report will contain all entries and the action performed upon each item. The cookie report will contain all cookie types for all URLs. When enabled a folder path needs to be specified for the reports to be saved to. E.g. C:\Temp. The option to anonymize the data will remove the user references from the exported data. It is recommended that this policy is enabled only when required.
Chrome Extension Removal	This policy manages the locales that are installed as part of Chrome extensions. A locale is essentially a language used and supported by the extension. Note: The list provided will be used for an exact text match (case insensitive). However wild card use is supported to do a contains check. For example: 'en*' will keep all locales that contain 'en'. In addition, the default locale for the extension will always be retained. It is recommended that this policy is enabled only when required.
Chrome Extension Removal	This policy manages Chrome extensions Enabling the "Blacklisted Extensions" option will remove all Chrome extensions that are part of the blacklist specified. Enabling the "Whitelisted Extensions" option will remove all Chrome extensions that are not part of the whitelist specified. Enabling the "Remove All Extensions" option will remove all Chrome extensions. Note: The blacklist and whitelist verification will use an exact text match (case insensitive). However wild card use is supported to do a contains check. For example: 'Avanite*' will remove or keep all extensions that contain 'Avanite'. It is recommended that this policy is enabled only when required.
Chrome Cookie Retention	This policy allows for management of Chrome cookie data. Enabling this policy allows for cookies to be retained for a specific number of days.

	"Clear all Cookies" option removes all cookie related web data for the user. "Retain specified number of calendar days" option allows cookies to be retained for a specific number of days. This allows cookies to be retained for the previous number of calendar days and any days of inactivity will be included. "Retain specified number of browsing days" option retains cookies for days where browsing has occurred. This allows the cookies to be retained for the specified number of days where the user has been actively browsing and any days of inactivity will be ignored. Enabling the "Remove expired cookies" option removes cookie data for cookies that have expired. The recommended setting for this policy is to select "Retain specified number of browsing days" and set it to 7 days. It is also recommended that the "Remove expired cookies" option is enabled.
Chrome History Retention	This policy allows management of Chrome history data. Enabling this policy option allows for history data to be retained for a specific number of days. "Clear all history" option removes all history related web data for the user. "Retain specified number of calendar days" option allows for history to be retained for a specific number of days. This allows history to be retained for the previous number of calendar days. "Retain specified number of browsing days" option retains history for days where browsing has occurred. This allows the history to be retained for the specified number of days where the user has been actively browsing and any days of inactivity will be ignored. The recommended setting for this policy is to select "Retain specified number of browsing days" and set this to 7 days.
Chrome Temporary Internet Data Removal	This policy will remove Chrome temporary internet data. Enabling this policy option will cause Chrome temporary internet data to be removed. Including temporary and crash dump files, Pepper Flash, PNACL and caches files. It is recommended that this setting is enabled.
Chrome Cookie Type Removal	This policy will remove cookies of specified types within Chrome. An example of a cookie type is "_ga" which is used to gather data about website activity by Google Analytics. Providing the ability to remove cookies based on type allows granular control over which cookies are retained. The "Remove known advertising and tracking cookies" option enables functionality to remove cookie types identified as being used for advertising or tracking purposes that will not affect the usability of websites.

	The WebData Control agent includes a pre-defined list of known advertising and tracking cookie types which is used when this option is enabled. "List of Cookie types" allows for user specified cookie types to be removed. When entering a cookie type, the entries are treated as an exact match including the case. When the "Remove known advertising and tracking cookies" and a "List of Cookies types" options are both specified the list of cookie types to be removed are cumulative. The recommended setting for this policy is to enable the policy and check the "Remove known advertising and tracking cookies" option.
Chrome Third Party Cookie Removal	This policy will remove Chrome third party cookies. Third party cookies are cookies generated from domains which do not match that of the primary website browsed. It is recommended that this setting is enabled.

WebData Control\WebData Management\Edge

Policy	*Description*
Edge Compatibility Data Removal	This policy will remove the Edge related compatibility mode data stored in the webcache database. Compatibility mode data will be dynamically updated as needed by the browser and the data does not need to be retained in the webcache database. It is recommended that this setting is enabled.
Edge DOM Data Removal	This policy will remove Edge DOM data. DOM data here refers to Document Object Model data which is used by browsers to store a variety of data required by web browsing and is retained for caching purposes. Enabling this policy option will cause Edge DOM data to be removed. All DOM data references within the webcache database will be removed when this policy is enabled. Enabling the "Delete all files" option will remove all Edge DOM data referenced data from the file system. Enabling the "Do not remove files on disk" option only removes references to Edge DOM data from the webcache and the file system is left untouched. The recommended setting for this policy will depend on how the environment is configured. When a persistent profile is being used it is recommended to use the “Delete all files” setting, and when a non-persistent profile is being used it is recommended to use the "Do not remove files on disk" option.
Edge Data Report	This policy will generate data exports of the WebData Management activity for Edge. There will be a separate file for cookies and history. The report will contain all entries and the action performed upon each item. The cookie report contains all cookie types for all URLs. When enabled a folder path needs to be specified for the reports to be saved to. E.g. C:\Temp. The option to anonymize the data will remove the user references from the exported data. It is recommended that this policy is enabled only when required.
Edge Enterprise Mode Data Removal	This policy will remove any Edge related Enterprise Mode data stored in the webcache database. Enterprise Mode data will be dynamically updated by the browser and the data does not need to be retained within the webcache database. It is recommended that this setting is enabled.
Edge Cookie Retention	This policy allows for management of Edge cookie data.

	Enabling this policy allows for cookies to be retained for a specific number of days. "Clear all Cookies" option removes all cookie related web data for the user. "Retain specified number of calendar days" option allows cookies to be retained for a specific number of days. This allows cookies to be retained for the previous number of calendar days and any days of inactivity will be included. "Retain specified number of browsing days" option retains cookies for days where browsing has occurred. This allows the cookies to be retained for the specified number of days where the user has been actively browsing and any days of inactivity will be ignored. Enabling the "Remove expired cookies" option removes cookie data for cookies that have expired. The recommended setting for this policy is to select "Retain specified number of browsing days" and set it to 7 days. It is also recommended that the "Remove expired cookies" option is enabled.
Edge History Retention	This policy allows management of Edge history data. Enabling this policy option allows for history data to be retained for a specific number of days. "Clear all history" option removes all history related web data for the user. "Retain specified number of calendar days" option allows for history to be retained for a specific number of days. This allows history to be retained for the previous number of calendar days. "Retain specified number of browsing days" option retains history for days where browsing has occurred. This allows the history to be retained for the specified number of days where the user has been actively browsing and any days of inactivity will be ignored. The recommended setting for this policy is to select "Retain specified number of browsing days" and set this to 7 days.
Edge Temporary Internet Files Data Removal	This policy will remove Edge temporary internet files data. Enabling this policy option will cause Edge temporary internet files data to be removed. All temporary internet files data references in the webcache database will be removed when this policy is enabled. Enabling the "Delete all files" option will remove all Edge temporary internet files data from the file system. Enabling the "Do not remove files on disk" option only removes references to Edge temporary internet files data from the webcache database and the file system is left untouched. The recommended setting for this policy will depend on how the environment is configured. When a persistent profile is being used it is recommended to use the "Delete all files" setting, and when a non-

	persistent profile is being used it is recommended to use the "Do not remove files on disk" option.
Edge Cookie Type Removal	This policy will remove cookies of specified types within Edge. An example of a cookie type is "_ga" which is used to gather data about website activity by Google Analytics. Providing the ability to remove cookies based on type allows granular control over which cookies are retained. The "Remove known advertising and tracking cookies" option enables functionality to remove cookie types identified as being used for advertising or tracking purposes that will not affect the usability of websites. The WebData Control agent includes a pre-defined list of known advertising and tracking cookie types which is used when this option is enabled. "List of Cookie types" allows for user specified cookie types to be removed. When entering a cookie type, the entries are treated as an exact match including the case. When the "Remove known advertising and tracking cookies" and a "List of Cookies types" options are both specified the list of cookie types to be removed are cumulative. The recommended setting for this policy is to enable the policy and check the "Remove known advertising and tracking cookies" option.
Edge Third Party Cookie Removal	This policy will remove Edge third party cookies. Third party cookies are cookies generated from domains which do not match that of the primary website browsed. It is recommended that this setting is enabled.

WebData Control\WebData Management\Firefox

Policy	*Description*
Firefox DOM Data Removal	This policy will remove Firefox DOM data. DOM data here refers to Document Object Model data which is used by browsers to store a variety of data required by web browsing and is retained for caching purposes. Enabling this policy option will cause Firefox DOM data to be removed. It is recommended that this setting is enabled.
Firefox Data Report	This policy will generate data exports of the WebData Management activity for Firefox. There will be a separate file for cookies and history. The report will contain all entries and the action performed upon each item. The cookie report will contain all cookie types for all URLs. When enabled, a folder path needs to be specified for the reports to be saved to eg. C:\Temp. The option to anonymize the data will remove the user references from the exported data. It is recommended that this policy is enabled only when required.
Firefox Cookie Retention	This policy allows for management of Firefox cookie data. Enabling this policy allows for cookies to be retained for a specific number of days. "Clear all Cookies" option removes all cookie related web data for the user. "Retain specified number of calendar days" option allows cookies to be retained for a specific number of days. This allows cookies to be retained for the previous number of calendar days and any days of inactivity will be included. "Retain specified number of browsing days" option retains cookies for days where browsing has occurred. This allows the cookies to be retained for the specified number of days where the user has been actively browsing and any days of inactivity will be ignored. Enabling the "Remove expired cookies" option removes cookie data for cookies that have expired. The recommended setting for this policy is to select “Retain specified number of browsing days” and set it to 7 days. It is also recommended that the “Remove expired cookies” option is enabled.
Firefox History Retention	This policy allows management of Firefox history data. Enabling this policy option allows for history data to be retained for a specific number of days. "Clear all history" option removes all history related web data for the user.

	"Retain specified number of calendar days" option allows for history to be retained for a specific number of days. This allows history to be retained for the previous number of calendar days. "Retain specified number of browsing days" option retains history for days where browsing has occurred. This allows the history to be retained for the specified number of days where the user has been actively browsing and any days of inactivity will be ignored. The recommended setting for this policy is to select "Retain specified number of browsing days" and set this to 7 days.
Firefox Temporary Internet Data Removal	This policy will remove Firefox temporary internet files data. Enabling this policy option will cause Firefox Temporary Internet data to be removed. It is recommended that this setting is enabled.
Firefox Cookie Type Removal	This policy will remove cookies of specified types within Firefox. An example of a cookie type is "_ga" which is used to gather data about website activity by Google Analytics. Providing the ability to remove cookies based on type allows granular control over which cookies are retained. The "Remove known advertising and tracking cookies" option enables functionality to remove cookie types identified as being used for advertising or tracking purposes that will not affect the usability of websites. The WebData Control agent includes a pre-defined list of known advertising and tracking cookie types which is used when this option is enabled. "List of Cookie types" allows for user specified cookie types to be removed. When entering a cookie type, the entries are treated as an exact match including the case. When the "Remove known advertising and tracking cookies" and a "List of Cookies types" options are both specified the list of cookie types to be removed are cumulative. The recommended setting for this policy is to enable the policy and check the "Remove known advertising and tracking cookies" option.
Firefox Third Party Cookie Removal	This policy will remove Firefox third party cookies. Third party cookies are cookies generated from domains which do not match that of the primary website browsed. It is recommended that this setting is enabled.

WebData Control\WebData Management\Internet Explorer

Policy	*Description*
Internet Explorer Compatibility Data Removal	This policy will remove the Internet Explorer related compatibility mode data stored in the webcache database. Compatibility mode data will be dynamically updated as needed by the browser and the data does not need to be retained in the webcache database. It is recommended that this setting is enabled.
Internet Explorer DOM Data Removal	This policy will remove Internet Explorer DOM data. DOM data here refers to Document Object Model data which is used by browsers to store a variety of data required by web browsing and is retained for caching purposes. Enabling this policy option will cause Internet Explorer DOM data to be removed. All DOM data references within the webcache database will be removed when this policy is enabled. Enabling the "Delete all files" option will remove all Internet Explorer DOM data referenced data from the file system. Enabling the "Do not remove files on disk" option only removes references to Internet Explorer DOM data from the webcache database and the file system is left untouched. The recommended setting for this policy will depend on how the environment is configured. When a persistent profile is being used it is recommended to use the "Delete all files" setting, and when a non-persistent profile is being used it is recommended to use the "Do not remove files on disk" option.
Internet Explorer Data Report	This policy will generate data exports of the WebData Management activity for Internet Explorer. There will be a separate file for cookies and history. The report will contain all entries and the action performed upon each item. The cookie report contains all cookie types for all URLs. When enabled a folder path needs to be specified for the reports to be saved to eg. C:\Temp. The option to anonymize the data will remove the user references from the exported data. It is recommended that this policy is enabled only when required.
Internet Explorer Enterprise Mode Data Removal	This policy will remove any Internet Explorer related Enterprise Mode data stored in the webcache database. Enterprise Mode data will be dynamically updated by the browser and the data does not need to be retained within the webcache database. This setting overcomes the need to wait 65 seconds at browser launch as per the following article - https://docs.microsoft.com/en-us/internet-explorer/ie11-deploy-guide/check-for-new-enterprise-mode-site-list-xml-file.

	It is recommended that this setting is enabled.
Internet Explorer Cookie Retention	This policy allows for management of Internet Explorer cookie data in Internet Explorer version 10 and above. Enabling this policy allows for cookies to be retained for a specific number of days. "Clear all Cookies" option removes all cookie related web data for the user. "Retain specified number of calendar days" option allows cookies to be retained for a specific number of days. This allows cookies to be retained for the previous number of calendar days and any days of inactivity will be included. "Retain specified number of browsing days" option retains cookies for days where browsing has occurred. This allows the cookies to be retained for the specified number of days where the user has been actively browsing and any days of inactivity will be ignored. Enabling the "Remove expired cookies" option removes cookie data for cookies that have expired. The recommended setting for this policy is to select "Retain specified number of browsing days" and set it to 7 days. It is also recommended that the "Remove expired cookies" option is enabled.
Internet Explorer History Retention	This policy allows management of Internet Explorer history data in Internet Explorer version 10 and above. Enabling this policy option allows for history data to be retained for a specific number of days. "Clear all history" option removes all history related web data for the user. "Retain specified number of calendar days" options allows for history to be retained for a specific number of days. This allows history to be retained for the previous number of calendar days. "Retain specified number of browsing days" option retains history for days where browsing has occurred. This allows the history to be retained for the specified number of days where the user has been actively browsing and any days of inactivity will be ignored. The recommended setting for this policy is to select "Retain specified number of browsing days" and set this to 7 days.
Internet Explorer Temporary Internet Files Data Removal	This policy will remove Internet Explorer temporary internet files data. Enabling this policy option will cause Internet Explorer temporary internet files data to be removed. All temporary internet files data referenced in the webcache database will be removed when this policy is enabled. Enabling the "Delete all files" option will remove all Internet Explorer temporary internet files data from the file system.

	Enabling the "Do not remove files on disk" option only removes references to Internet Explorer temporary internet files data from the webcache and the file system is left untouched. The recommended setting for this policy will depend on how the environment is configured. When a persistent profile is being used it is recommended to use the "Delete all files" setting, and when a non-persistent profile is being used it is recommended to use the "Do not remove files on disk" option.
Internet Explorer Cookie Type Removal	This policy will remove cookies of specified types within Internet Explorer. An example of a cookie type is "_ga" which is used to gather data about website activity by Google Analytics. Providing the ability to remove cookies based on type allows granular control over which cookies are retained. The "Remove known advertising and tracking cookies" option enables functionality to remove cookie types identified as being used for advertising or tracking purposes that will not affect the usability of websites. The WebData Control agent includes a pre-defined list of known advertising and tracking cookie types which is used when this option is enabled. "List of Cookie types" allows for user specified cookie types to be removed. When entering a cookie type, the entries are treated as an exact match including the case. When the "Remove known advertising and tracking cookies" and a "List of Cookies types" options are both specified the list of cookie types to be removed are cumulative. The recommended setting for this policy is to enable the policy and check the "Remove known advertising and tracking cookies" option.
Internet Explorer Third Party Cookie Removal	This policy will remove Internet Explorer third party cookies. Third party cookies are cookies generated from domains which do not match that of the primary website browsed. It is recommended that this setting is enabled.

WebData Control\WebData Management\Windows Store Apps

Policy	*Description*
Windows Store Apps Data Removal	This policy allows the removal of data related to Windows Store Applications from the webcache database. Windows Store Applications that access the internet store data inside the webcache database. Enabling this policy removes all Windows Store Application data.

	The exclusion option allows important Windows Store applications to have their web data retained. Specify which data to be kept by defining the application name to match. E.g. "Microsoft.Office.OneNote". It is recommended that this setting is enabled.

Using WebData Management via Third-Party

WebData Management needs to be completed before any profile management solution captures the browser related profile data.

If the Avanite Notification Service is not used, this can also be done via a Group Policy Logoff action as shown below:

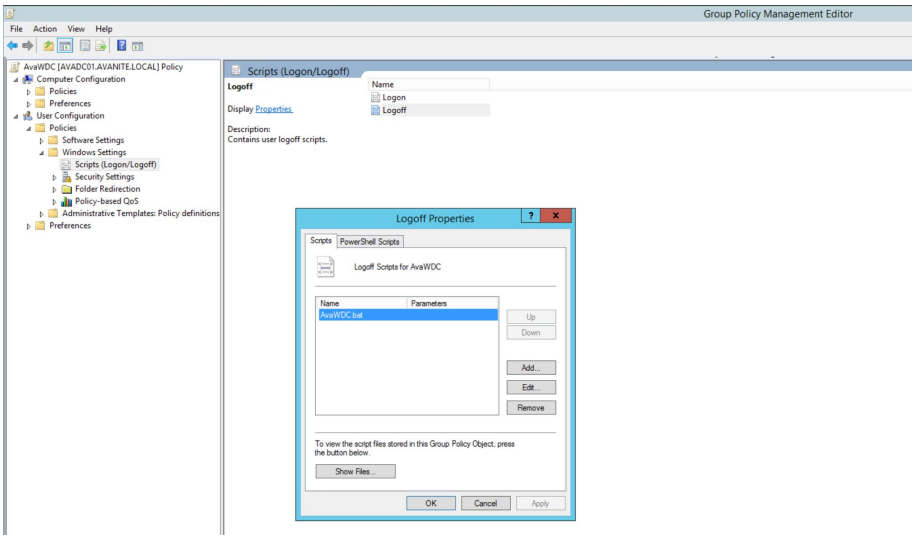

Figure 15 – Logoff Trigger

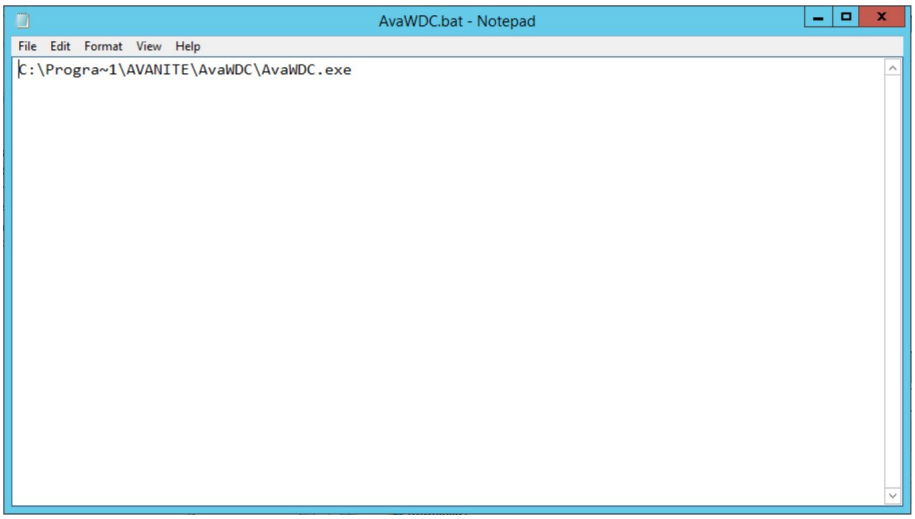

Figure 16 – Launch batch file

Note: WebData Control can be launched by any 3rd party profile solution, the group policy logoff script is an example of its implementation.

Appendix A - Definitions

First-Party Cookie

A first-party cookie is data stored on a user's computer that is created by a website with a domain name matching that of the one the user is currently visiting. First-party cookies are used for shopping baskets, storing user's website preferences and tracking user behavior.

Third-Party Cookie

A third-party cookie is data stored on a user's computer that is created by a website with a domain name other than the one the user is currently visiting. Third-party cookies are often used for tracking and advertising purposes to build up a picture of a user's habits and activities on a particular device.

Cookie Type

An example of a cookie type is "_ga" which is a cookie provided by Google Analytics. The "_ga" cookie is provided from a large number of websites in the world and gives a website administrator data about the traffic the website receives via the Google Analytics platform. As the cookie is provided directly from a website a user is visiting, this is a first-party cookie. Each cookie stored for a user on their computer has a type which is defined by the company that hosts the website. Cookie types can be used to identify a cookie regardless of whether it is a first-party or third-party cookie.

Appendix B - Roaming Profile Support

WebData Control actively supports management of Internet Explorer cookies in a roaming profile scenario. As per https://docs.microsoft.com/en-us/internet-explorer/ie11-deploy-guide/browser-cache-changes-and-roaming-profiles, when the "Delete cached copies of roaming profiles" Group Policy setting is enabled and the profile is of a Roaming type, when WebData Control executes it automatically manages cookies in the AppData\Roaming section of the user profile.

When using this mechanism only cookie information is retained between sessions with .dat or .rcookie files being generated in the AppData\Roaming part of the user profile. When Internet Explorer launches in each new session the .dat/.rcookie files are used to recreate the webcachev01.dat file. WebData Control's WebData Management feature understands this inter-relationship and manages the cookies as expected.

Appendix C – Data Report Format

The Data Report feature which is available for each of the supported browsers will output 2 files per user per browser when configured.

The filename of the output files will be as follows:

- N_<BrowserName>_Cookies_<GUID>.txt
- N_<BrowserName>_History_<GUID>.txt

<BrowserName> represents the name of the browser being used ie. IE, Edge, Chrome or Firefox.

<GUID> represents a unique identifier generated automatically for each execution for WebData Control.

Report files are | delimited text files which can easily be viewed by a text editor or imported into Microsoft Excel or similar for analysis.

Cookie Report Format

The Cookie report contains the following data fields:

Field Name	*Description*
Version	Defines a version number for the schema of the data
Data Type	Defines the entry as a cookie item
Browser	Defines which Browser the data was reported from
Time Stamp	Date and Time stamp of when the entry was written
User	Defines the user to which the data applies
Domain	Defines the domain of the user
Machine	Defines the machine on which the data was generated
Action	Defines what action was taken by WebData Control as the data was processed. Valid actions are: • Remaining • Removed • RemovedType • Removed3rdParty • OrphanedInDB • Expired
Base URL	Defines the complete URL of the website
Processed URL	Defines the URL which was processed by WebData Control
Type	Defines the cookie type for the entry
Secured	Defines whether the entry was from a secure website (true/false)
Last Accessed Date	Defines the last access date for the entry
Modified Date	Defines the last modified date for the entry
Expiry Date	Defines the expiry date for the entry

History Report Format

The History report contains the following data fields:

Field Name	*Description*
Version	Defines a version number for the schema of the data
Data Type	Defines the entry as a cookie item
Browser	Defines which Browser the data was reported from
Time Stamp	Date and Time stamp of when the entry was written
User	Defines the user to which the data applies
Domain	Defines the domain of the user
Machine	Defines the machine on which the data was generated
Action	Defines what action was taken by WebData Control as the data was processed. Valid actions are: • Remaining • Removed
Base URL	Defines the complete URL of the website
Processed URL	Defines the URL which was processed by WebData Control
Secured	Defines whether the entry was from a secure website (true/false)
Last Accessed Date	Defines the last access date for the entry
Modified Date	Defines the last modified date for the entry
Expiry Date	Defines the expiry date for the entry

Appendix D – Default Configuration

The following table sets out the policy settings defined in the Default Configuration:

Policy	*Description*
WebData Control\WebData Management\Advanced	Data Optimization: ***Enabled*** Event Logging: ***Enabled***
WebData Control\WebData Management\Chrome	Chrome Cookie Retention: Enabled, Values: ***Retain Specified number of browsing days, 7 days, Remove expired cookies*** Chrome Cookie Type Removal: ***Enabled***, Value: ***Remove known advertising and tracking cookies*** Chrome DOM Data Removal: ***Enabled*** Chrome History Retention: ***Enabled***, Values: ***Retain Specified number of browsing days, 7 days*** Chrome Temporary Internet Data Removal: ***Enabled*** Chrome Third Party Cookie Removal: ***Enabled***
WebData Control\WebData Management\Edge	Edge Compatibility Date Removal: ***Enabled*** Edge Cookie Retention: ***Enabled***, Values: ***Retain Specified number of browsing days, 7 days, Remove expired cookies*** Edge Cookie Type Removal: ***Enabled***, Value: ***Remove known advertising and tracking cookies*** Edge DOM Data Removal: ***Enabled***, Value: ***Delete all files*** Edge Enterprise Mode Data Removal: ***Enabled*** Edge History Retention: ***Enabled***, Values: ***Retain Specified number of browsing days, 7 days*** Edge Temporary Internet Files Data Removal: ***Enabled***, Value: ***Delete all files*** Edge Third Party Cookie Removal: ***Enabled***
WebData Control\WebData Management\Firefox	Firefox Cookie Retention: ***Enabled***, Values: ***Retain Specified number of browsing days, 7 days, Remove expired cookies*** Firefox Cookie Type Removal: ***Enabled***, Value: ***Remove known advertising and tracking cookies*** Firefox DOM Data Removal: ***Enabled*** Firefox History Retention: ***Enabled***, Values: ***Retain Specified number of browsing days, 7 days*** Firefox Temporary Internet Data Removal: ***Enabled*** Firefox Third Party Cookie Removal: ***Enabled***
WebData Control\WebData	Internet Explorer Compatibility Date Removal: ***Enabled***

Management\Internet Explorer	Internet Explorer Cookie Retention: ***Enabled***, Values: ***Retain Specified number of browsing days, 7 days, Remove expired cookies*** Internet Explorer Cookie Type Removal: ***Enabled***, Value: ***Remove known advertising and tracking cookies*** Internet Explorer DOM Data Removal: ***Enabled***, Value: ***Delete all files*** Internet Explorer Enterprise Mode Data Removal: ***Enabled*** Internet Explorer History Retention: ***Enabled***, Values: ***Retain Specified number of browsing days, 7 days*** Internet Explorer Temporary Internet Files Data Removal: ***Enabled***, Value: ***Delete all files*** Internet Explorer Third Party Cookie Removal: ***Enabled***
WebData Control\WebData Management\Windows Store Apps	Windows Store Apps Data Removal: ***Enabled***