WebData Control Product Guide

Version 4.8 SP1

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 (Chromium) 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.

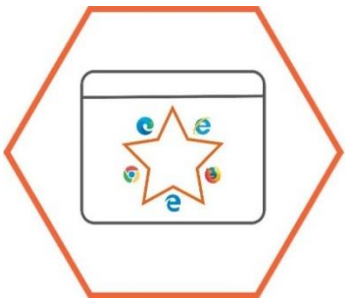
The reason for the delivery of multiple browsers often relates to website compatibility with specific websites only working correctly in a certain browser. An example of this would be websites which leverage ActiveX controls which only function in Internet Explorer. Other websites may not render correctly 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 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.

The WebData Management feature 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 (Legacy), much of the data corresponding to web browsing is now indexed and held within a central database, the webcachev01.dat. This database is located under %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 Microsoft Edge (Chromium), 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. Using the WebData Management feature, 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 may require Internet Explorer.

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, Browser Redirector 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/favorites 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's Favorites Synchronization feature, administrators can provision default bookmarks/favorites to only display in specific browsers and synchronize all non-default bookmarks/favorites between the different browsers based on their requirements.

User created bookmarks/favorites preferences are also retained. Properties such as "Icon Only" options and the relevant bookmarks/favorites icons are also synchronized to give users a consistent browsing experience.

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 (Chromium)

Note: *The WebData Management feature also supports the Microsoft Edge (Legacy) browser to ensure redundant data related to this browser can still be managed.*

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
- Windows 11
- Windows Server 2022

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

- Remove cookie data associated with cookies not created, modified or accessed 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 cookies which do not contain the "Secure" flag
- Remove cookie data for cookies which do not contain the "HttpOnly" flag
- 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 Management gives a consistent method for an administrator to manage the browsing history retained for users across all browsers:

- Define how long to keep browsing history
- Retain browsing history based on the number of calendar days or browsing days
- 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 Management 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.

WebData Control has a set of pre-configured temporary internet data removal rules built in which can be modified if required to ensure that control is maintained over this aspect of browser generated data.

Note: *For further details on options for managing temporary internet files see Appendix B*

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 Management provides the ability to granularly manage the DOM data stored by each browser allowing only required DOM data to be retained.

Similar to the temporary internet files, WebData Control has a set of pre-configured DOM Store data removal rules built in which can be modified to ensure control is maintained over this browser generated data.

Note: *For further details on options for managing DOM data see Appendix B*

Compatibility Data

For Internet Explorer and Microsoft Edge (Legacy), 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 Management 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 (Legacy) 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 Management allows for this data to be deleted from webcache to keep the size of the file down to the minimum required.

With Microsoft Edge (Chromium) being used in IE Mode the Internet Explorer browser is used to provide the website compatibility. Internet Explorer stores additional data in the webcache when used in this manner which is also managed by WebData Management.

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 Management 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 Management 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 (Legacy) 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 users. Microsoft Edge (Chromium), Google Chrome and Mozilla 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 Management.

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

Extension Management

Another feature provided in WebData Management is the ability to selectively choose which Microsoft Edge (Chromium) or Google Chrome extensions should be retained, and which should be removed. WebData Management can be configured to explicitly remove or explicitly retain extensions based on requirements and any extensions which do not match the policy will be removed or retained as required.

Extension Locale Removal

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

WebData Management 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.

> ***Note:*** *The default locale for extensions is always retained*

Browser Redirector

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

URL Redirection

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 Browser Redirector and launches either Internet Explorer, Google Chrome, Mozilla Firefox or Microsoft Edge (Chromium) depending on the configured policy set. Where a request does not match a defined rule, the default browser is used.

When a user types in a URL into a browser the Browser Redirector extensions intercept the request and direct 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 Google Chrome is closed and the URL is loaded in a new instance/tab in Internet Explorer.

For browser redirector to redirect URLs from inside the browser the following extensions need to be installed:

Internet Explorer

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

Where Internet Explorer is configured to use Enhanced Protected Mode a separate BHO can be enabled which is compatible with Enhanced Protected Mode operations.

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 Google Chrome browser policies. This extension is responsible for intercepting URL requests inside the Google Chrome browser.

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 Mozilla Firefox browser policies. This extension is responsible for intercepting URL requests inside the Mozilla Firefox browser.

Microsoft Edge (Chromium)

To use WebData Control's Browser Redirector feature with Microsoft Edge (Chromium) an extension needs to be installed for each user. The extension is available from the Microsoft Edge store – https://microsoftedge.microsoft.com/addons/detail/jennlkhphjkepfjmocknbgpagnkiiknk and can be installed for users by configuring the appropriate Microsoft Edge (Chromium) browser policies. This extension is responsible for intercepting URL requests inside the Microsoft Edge (Chromium) browser.

Setting the default browser

Browser Redirector allows for the default browser to be configured via a policy "*Specify Default Browser*" or via a standalone executable which can be executed in the user context. Both methods will configure the appropriate associations to ensure the selected browser is used as the default browser.

The standalone executable can be run inside a user session with standard user permissions or it can be executed using a logon script for example. The executable is located by default in the C:\Program Files\Avanite\AvaWDC folder and is called AvaniteDefaultBrowserUtility.exe.

The executable accepts the following parameters:

- Edge
- Chrome
- IE
- Firefox

Example command line: C:\Program Files\Avanite\AvaWDC\AvaniteDefaultBrowserUtility.exe Edge

This will set the default browser to Edge Chromium.

Enforcing use of a specific browser

Browser Redirector also supports enforcing the use of a specific browser for use cases such as kiosk machines. Where a default browser is specified and chosen to be enforced, Browser

Redirector will always launch the enforced browser, unless a rule exists for the URL to be redirected to an alternate browser.

Redirection to an external process

It is also possible to use Browser Redirector to redirect specific URLs to an external process. Browser Redirector enables the administrator to define a set of policies which redirect specific URLs to an external process. For example, when accessing a specific URL Browser Redirector can be configured to launch an App-V or ThinApp package or an alternative browser such as Safari or Opera.

Launching with parameters

When Browser Redirector is used, any redirected browser request can be configured to launch the browser with a defined set of parameters enabling administrators to meet any specific requirements they may have regards browser parameters. The parameters can also be used in conjunction with the enforcing a default browser option to ensure a certain browser is always used and is launched with a specific set of parameters on each launch.

Favorites Synchronization

The Internet Explorer, Microsoft Edge (Chromium), Google Chrome and Mozilla Firefox browsers store bookmarks/favorites in different ways which end up with users having a different set of bookmarks/favorites in each of the browsers they use, leading to a poor user experience.

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

Browser favorites are stored independently of the browsers. All user created bookmarks/favorites and their associated icons are stored by Avanite in the %AppData%\Avanite\BrowserFavorites folder by default, although this location can be changed to another location or network location as required.

In addition, Favorites Synchronization 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. In conjunction with the Browser Redirector capabilities these can also be redirected to the defined browser.

The Favorites Synchronization feature also has a "read only" mode whereby favorites/bookmarks from all browsers can be stored to a central location. These centrally stored favorites/bookmarks 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.

When the Notification Service is selected for use with the WebData Management feature, additional options are available for executing the data cleanup for the Google Chrome, Mozilla Firefox and Microsoft Edge (Chromium) browsers. WebData Management can be configured to perform the data management on the exit of the browser as well as during the logoff of a user session. If required, the automatic execution of WebData Management at logoff can be disabled so only the on browser exit processing is enabled.

Network Service

The Avanite Network Service is an option which can be selected as part of the installation. The network service will ensure that the latest Avanite definition files are downloaded automatically.

Avanite host a Content Delivery Network hosted in Microsoft Azure which contains the latest definition files for which tracking, advertising and analytics cookies are to be removed by WebData Management.

The Network Service is not required for any of the other features to function and is only used to update the files which store the definitions for which tracking, advertising and analytics cookies are to be removed by WebData Management.

Global Options

WebData Control provides some global options which include enabling the following:

- Diagnostic Logging
- Notifications
- Event Logging

Diagnostic Logging

Diagnostic Logging can be enabled via the "Diagnostic Logging" policy. When this policy is enabled the WebData Management, Browser Redirector and Favorites Synchronization feature will output log files containing information about actions completed by the agent.

When enabling this policy, a path must be provided where the log files can be created.

Notifications

Notifications can be enabled for the WebData Management, Browser Redirector and Favorites Synchronization features of WebData Control. The notifications utilize the Windows toast notification system and provide feedback inside a user session when a relevant event occurs.

Notifications are supported on Windows Server 2016, Windows Server 2019, Windows Server 2022 and all Windows 10/11 operating systems.

The "Enable Notifications" policy can be enabled and configured to provide notifications on a per-feature basis.

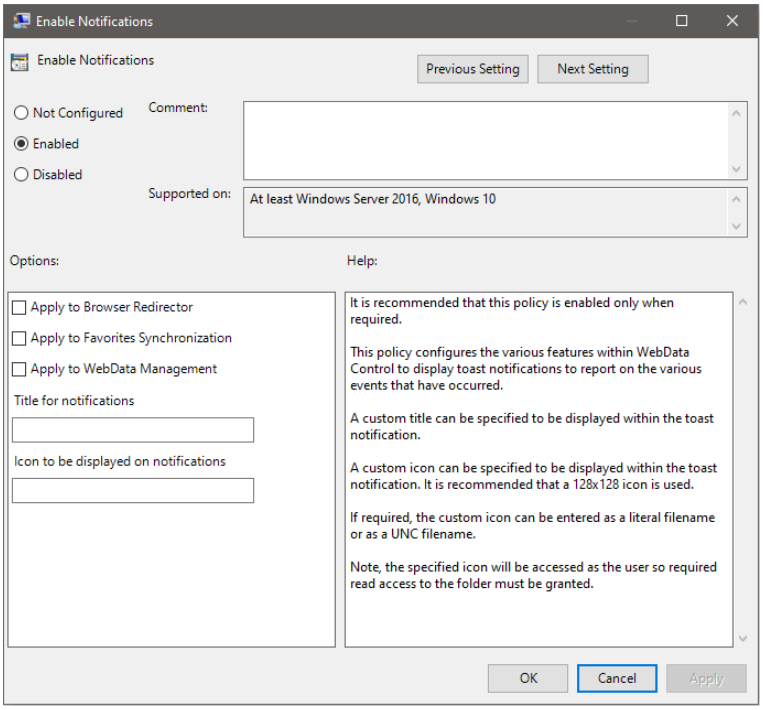


Figure 1 – Enable Notifications Policy

By default, the notifications are displayed with the WebData Control icon and title. If required a new title and icon can be specified to customize the experience inside the user session.

Event Logging

WebData Control can output details of a variety of actions that have been completed by the agent to the Windows Application Event log.

The "Event Logging" policy can be enabled and configured to provide events on a per-feature basis.

For details of the events generated please see Appendix C.

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.

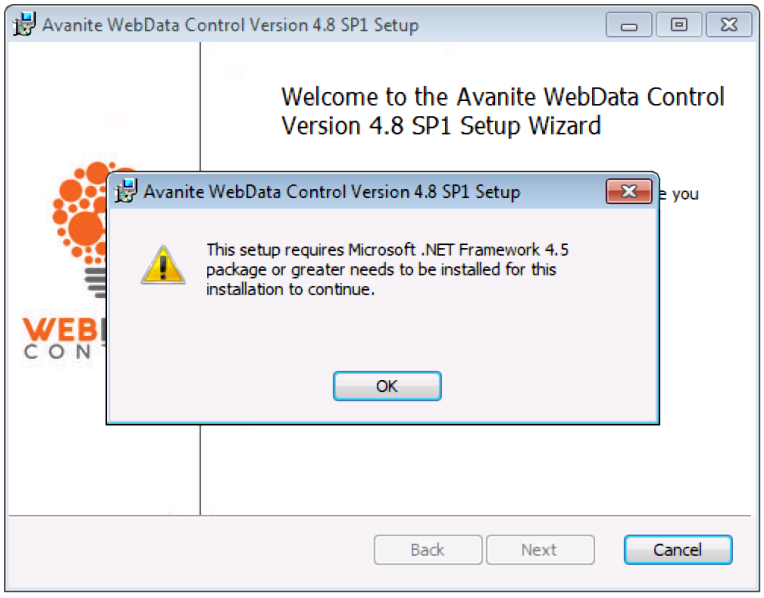


Figure 2 – Required pre-requisite missing

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.

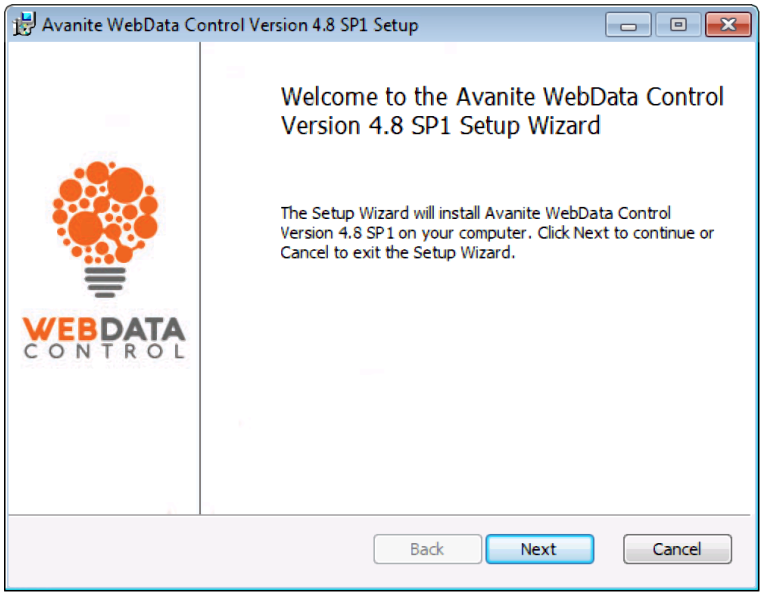


Figure 3 - Welcome screen

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

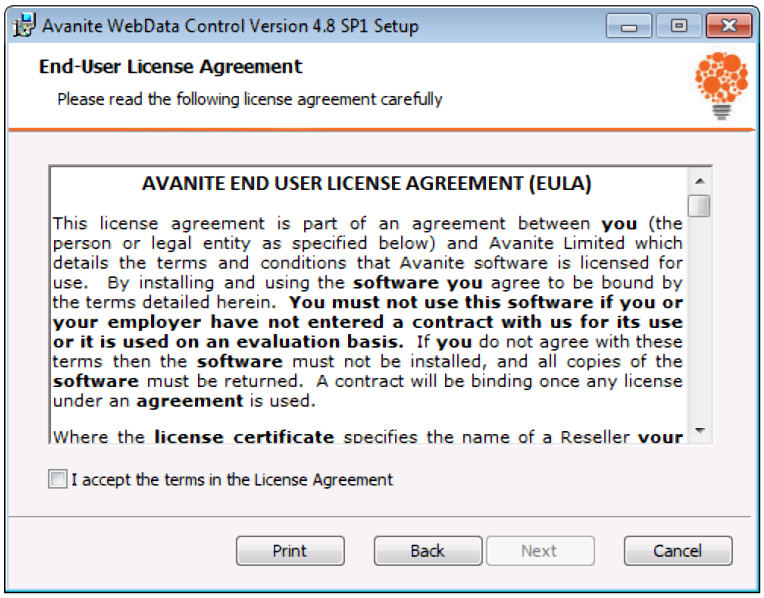


Figure 4 – EULA Acceptance

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.

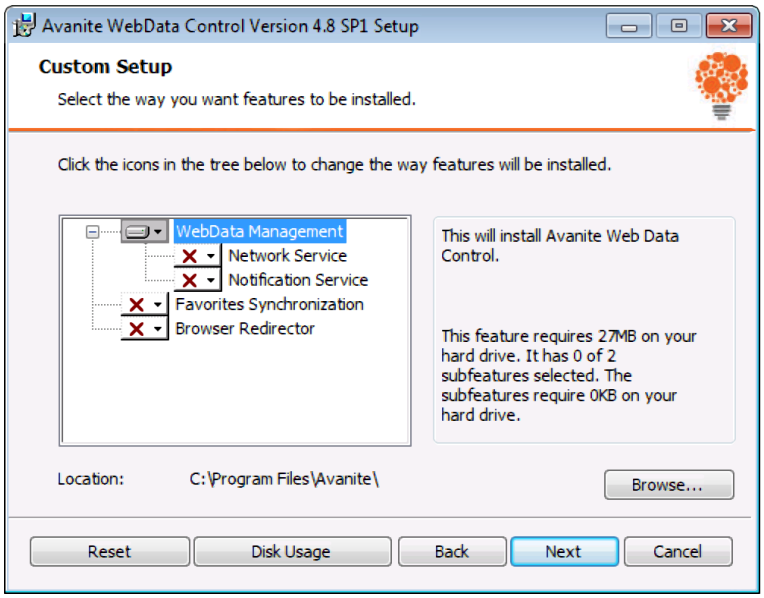


Figure 5 - Custom Setup options

4. Click **Install**.

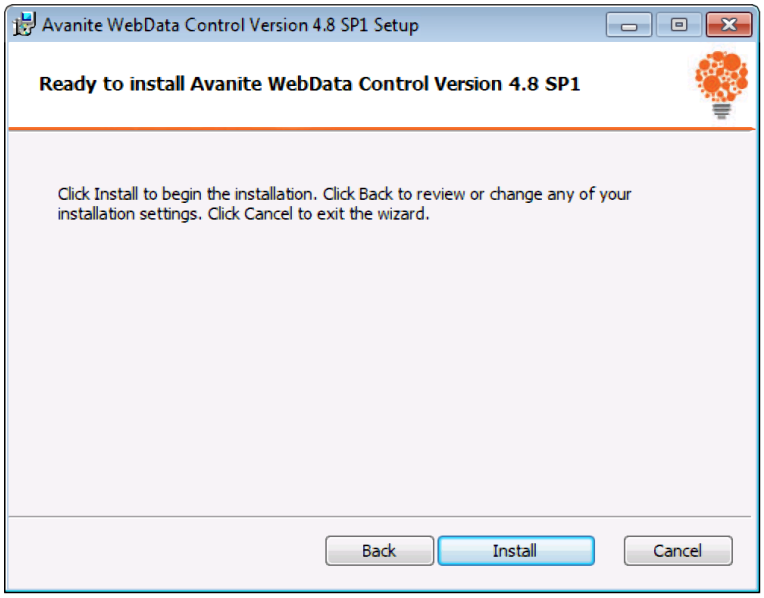


Figure 6 - Confirmation screen

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

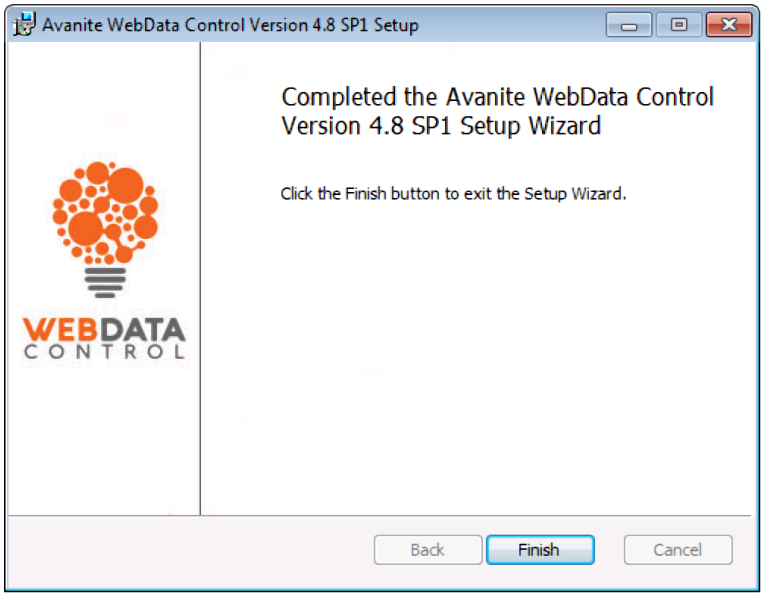


Figure 7 - Setup completion screen

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,UseNetworkService,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
UseNetworkService – Install the Network Service component
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 to the target devices, enable the policy "License" with supplied license key. A license key can be acquired by contacting support@avanite.com.

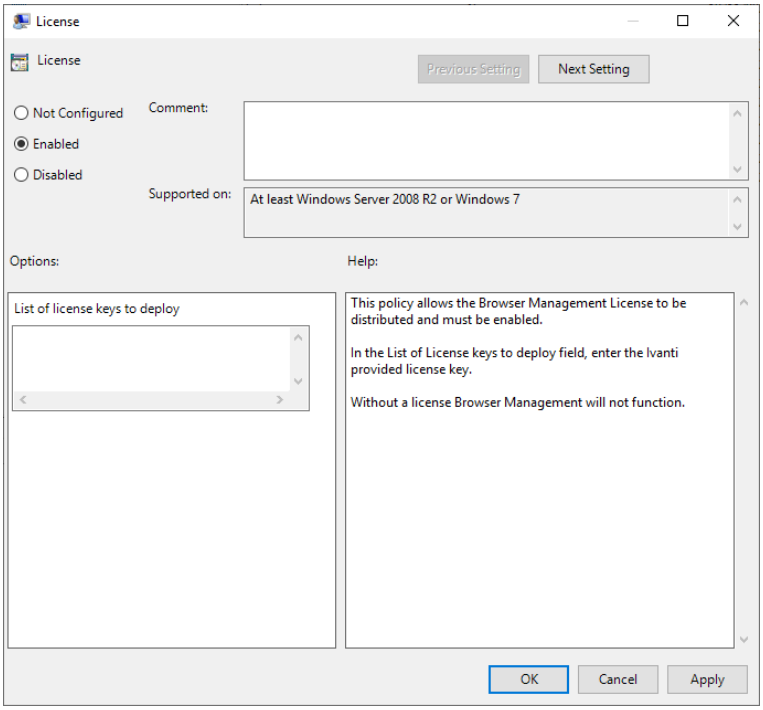


Figure 8 - License Policy

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.

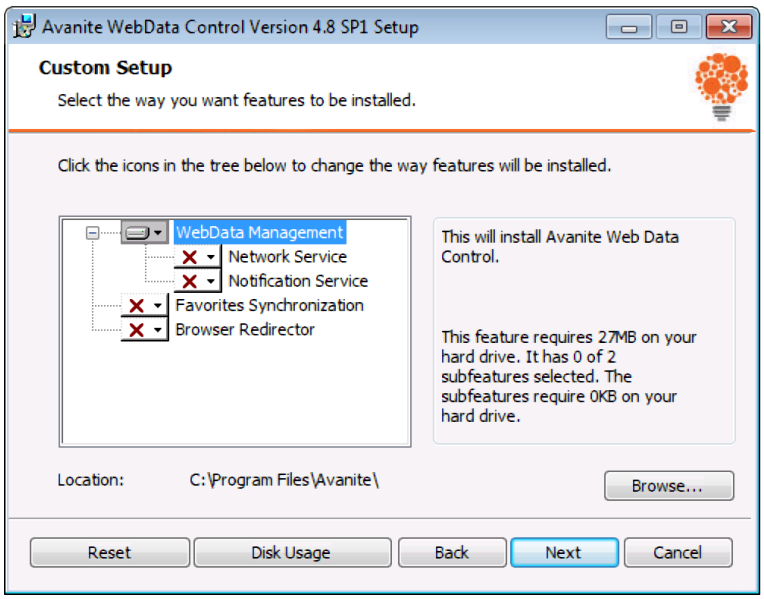


Figure 9 – Install only WebData Management

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

The WebData Management component can also be installed with the Network Service option selected. When the Network Service component is selected the "Avanite Network Service" is installed and will automatically check for updates to the definition files on the Avanite Content Delivery Network and download them as required.

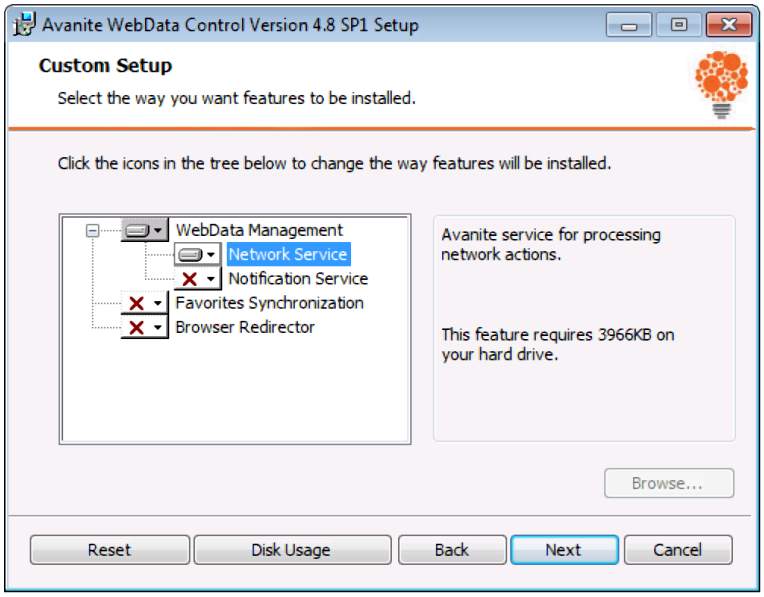


Figure 10 – Install WebData Management and Network Service

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.

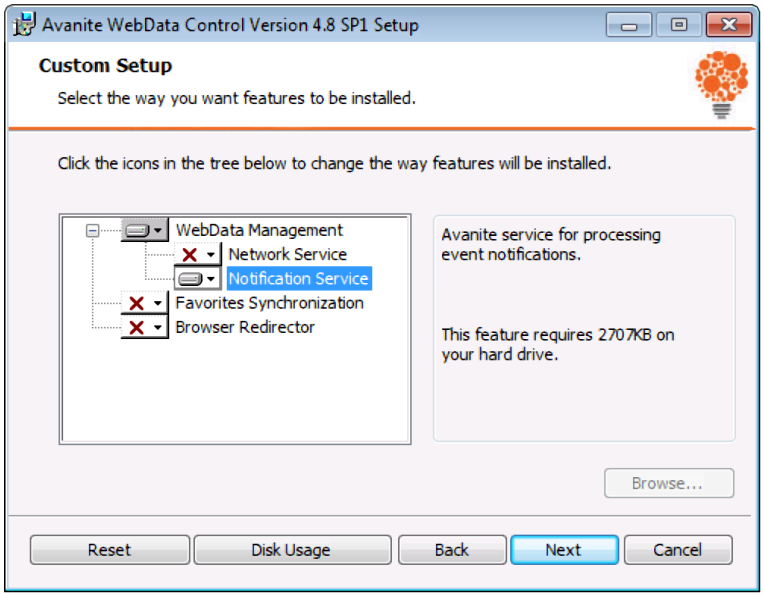


Figure 11 – Install WebData Management and Notification Service

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 and Network Service has been chosen to be 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\Network Service	Enable Automatic Updates: ***Enabled***
Computer\WebData Control\WebData Management	Default Configuration: ***Enabled***

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

Favorites Synchronization

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

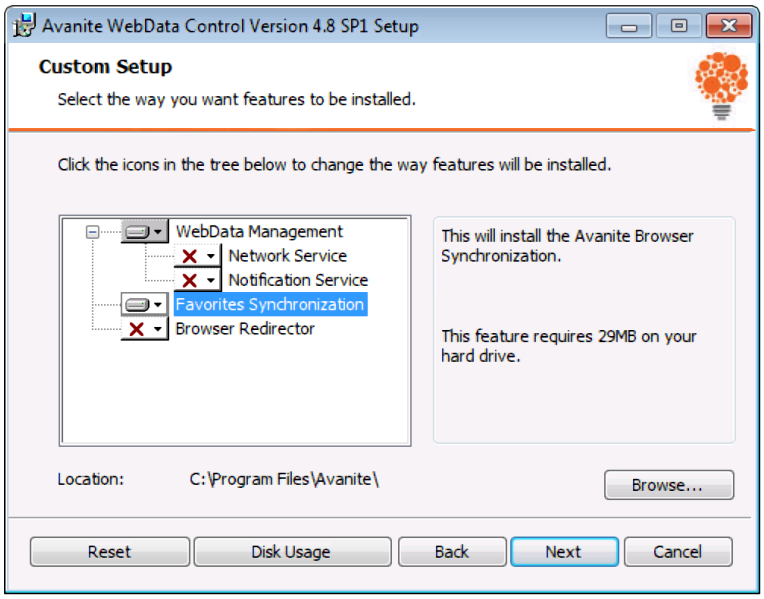


Figure 12 – Install only Favorites Synchronization

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.

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	Force Internet Explorer to close: ***Enabled***
Computer\WebData Control\Favorites Synchronization	Favorites Browser Selection: ***Enabled***, Values: ***Chrome Synchronization, Firefox Synchronization, Internet Explorer Synchronization, Edge Chromium Synchronization*** Favorites Storage Folder: Enabled, Value: ***<A suitable share\folder path>***

Note: Only enable the Favorites Browser Selection policy for browsers that are installed/in use)

If you are using Edge Chromium (version 88 or above), in addition to the above settings, the following policy should be configured for Microsoft Edge Chromium. Without these policies Microsoft Edge Chromium runs continuously and stops synchronization from occurring.

Policy	*Recommended Setting*
Computer\Microsoft Edge\Performance	Enable startup boost: ***Disabled***

Browser Redirector

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

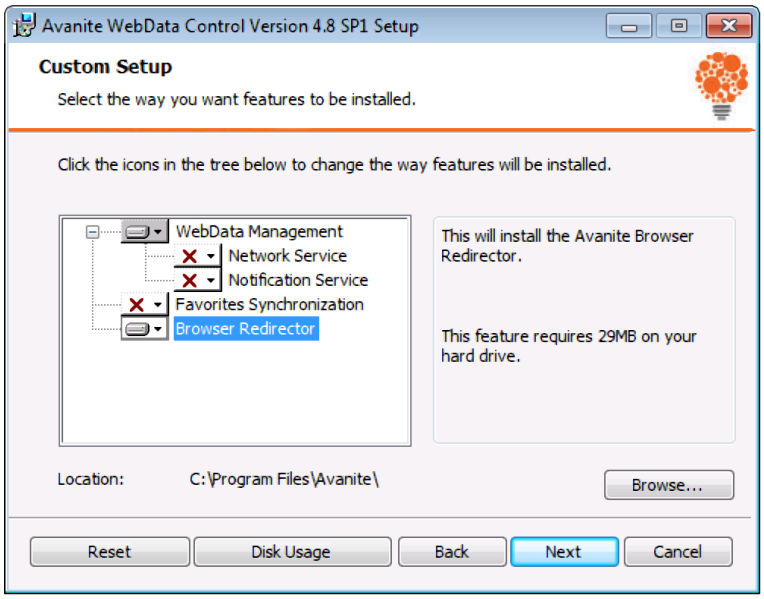


Figure 13 – Install only Browser Redirector

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.

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>*** URLs to redirect to Chrome: ***Enabled***, Values: ***<User defined>*** URLs to redirect to Firefox: ***Enabled***, Values: ***<User defined>*** URLs to redirect to Internet Explorer: ***Enabled***, Values: ***<User defined>*** URLs to redirect to Edge Chromium: ***Enabled***, Values: ***<User defined>***

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

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***

For Microsoft Edge (Chromium) the following policy is required to allow the Avanite Edge Browser Redirector extension to be installed for all users.

Policy	*Recommended Setting*
Computer\Microsoft Edge\Extensions	Control which extensions are installed silently: ***Enabled***, Value: ***jennlkhphjkepfjmocknbgpagnkiiknk***

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***
Computer\Microsoft Edge	Set Microsoft Edge as Default Browser: ***Disabled***
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:

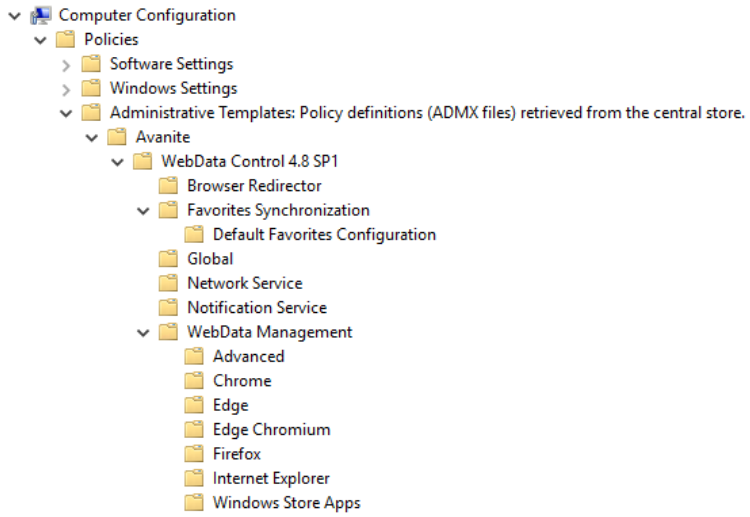


Figure 14 - ADMX Computer Level

WebData Control can also be configured at the User Level:

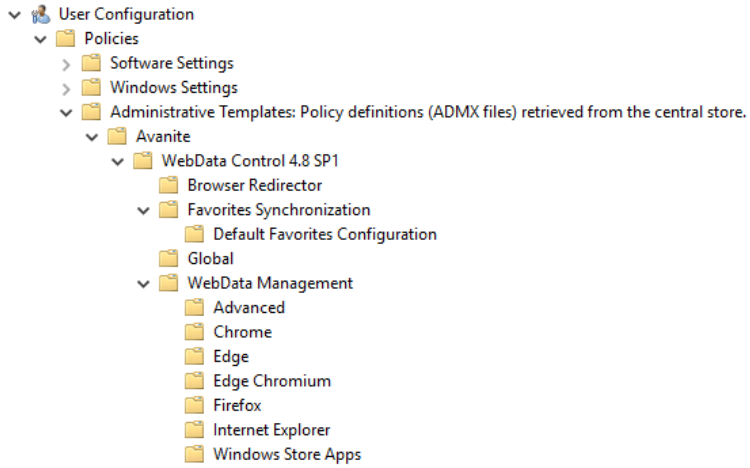


Figure 15 - ADMX User Level

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

> ***Note:*** *The Notification Service policies are only available at the Computer level and are required to enable the various product features*

WebData Control Policy Reference

The following table outlines all the policy options available in the AvaWDCv4-8 SP1.admx:

Avanite\WebData Control 4.8 SP1\Browser Redirector

Policy	*Description*
Chrome Launch Parameters	It is recommended that this policy is enabled only when required. The policy allows you to set pre-determined parameters which Chrome will use when launched via Browser Redirector. Any additional parameters will be removed. Example: --start-maximized
Edge Chromium Launch Parameters	It is recommended that this policy is enabled only when required. The policy allows you to set pre-determined parameters which Edge Chromium will use when launched via Browser Redirector. Any additional parameters will be removed. Example: --start-maximized
Enable user defined Default browser	It is recommended that this policy is enabled only when required. When enabled this policy allows the user to select a default browser and configures Browser Redirector to use this choice as the default. The user's preferred browser value is stored in the key: HKCU\Software\Avanite\WebData Control.
Enforce default favorites to redirect	It is recommended that this policy is enabled only when required. This policy enables URL redirection for any default favorites that have been configured. When enabled, any browser specific default favorites which have been specified will have their URLs redirected to the browser where the default favorite was defined.
Firefox Launch Parameters	It is recommended that this policy is enabled only when required. The policy allows you to set pre-determined parameters which Firefox will use when launched via Browser Redirector. Any additional parameters will be removed. Example: -foreground
Internet Explorer Enhanced Protected Mode Support	It is recommended that this policy is enabled only when required. When enabled this policy enables Browser Redirector to support Internet Explorer's Enhanced Protected Mode.
Internet Explorer Launch Parameters	It is recommended that this policy is enabled only when required. The policy allows you to set pre-determined parameters which Internet Explorer will use when launched via Browser Redirector. Any additional parameters will be removed.

	Example: -k
Specify Default Browser	It is recommended that this policy is enabled only when required. When this policy is enabled, it sets the default browser in the user session. Where no redirection policies apply, this will be the default browser used to open any URLs. Where a redirection policy URL match is found, Browser Redirector will launch the specified browser or alternative process. Where it is required that a specific browser needs to be enforced for use, select the option: Enforce Administrator Defined Browser. Selecting the Enforce Administrator Defined Browser will force Browser Redirector to always use this browser unless a redirection policy match is found.
URLs to redirect to an Alternative Process	It is recommended that this policy is enabled only when required. When enabled, this policy allows you to configure a set of URLs that will be forced to open in an alternative process. To ensure the best match, when you specify a URL enter the fullest path to the web resource as possible. The URL should be entered into the Value Name field. The Value field should contain the full path to the executable that the URL will be redirected to. The URL is not passed as a parameter by default. Example inputs would be: Value Name: "https://www.website.com/" Value: "%ProgramFiles%\AlternativeProcess.exe" https://www.website.com
URLs to redirect to Chrome	It is recommended that this policy is enabled only when required. When enabled, this policy allows you to configure a list of URLs that will always open in the Chrome browser. To ensure the best match, when you specify a URL enter the fullest path to the web resource as possible. By default the policy uses a "contains" check and will directly match any part of a URL being accessed. Example entries: https://www.website.com http://www.website.com website.com website.com/page
URLs to redirect to Edge Chromium	It is recommended that this policy is enabled only when required. When enabled, this policy allows you to configure a list of URLs that will always open in the Edge Chromium browser.

	To ensure the best match, when you specify a URL enter the fullest path to the web resource as possible. By default the policy uses a "contains" check and will directly match any part of a URL being accessed. Example entries: https://www.website.com http://www.website.com website.com website.com/page
URLs to redirect to Firefox	It is recommended that this policy is enabled only when required. When enabled, this policy allows you to configure a list of URLs that will always open in the Firefox browser. To ensure the best match, when you specify a URL enter the fullest path to the web resource as possible. By default the policy uses a "contains" check and will directly match any part of a URL being accessed. Example entries: https://www.website.com http://www.website.com website.com website.com/page
URLs to redirect to Internet Explorer	It is recommended that this policy is enabled only when required. When enabled, this policy allows you to configure a list of URLs that will always open in the Internet Explorer browser. If the Internet Explorer browser is already running a new tab will be opened. To ensure the best match, when you specify a URL enter the fullest path to the web resource as possible. By default the policy uses a "contains" check and will directly match any part of a URL being accessed. Example entries: https://www.website.com http://www.website.com website.com website.com/page
URLs to redirect to Internet Explorer (New Instance)	It is recommended that this policy is enabled only when required. When enabled, this policy allows you to configure a list of URLs that will always open in a new instance of the Internet Explorer browser. To ensure the best match, when you specify a URL enter the fullest path to the web resource as possible.

	By default the policy uses a "contains" check and will directly match any part of a URL being accessed. Example entries: https://www.website.com http://www.website.com website.com website.com/page

Avanite\WebData Control 4.8 SP1\Favorites Synchronization

Policy	*Description*
Favorites Browser Selection	It is recommended that this policy is enabled only when required. This policy defines which browsers will be enabled for synchronization of Favorites. Selecting a browser will enable it for synchronization and browser bookmarks (or Favorites) will be shared between browsers that have been enabled. Note: Multiple browsers need to be selected for this policy to have any effect.
Favorites Storage Folder	It is recommended that this policy is enabled only when required. This policy allows an alternative folder to be specified for storage of the file and database holding user Favorites. The file stores details about the Favorites/bookmarks. The database holds the associated favorites icons from each browser that is enabled for synchronization. The default location is %AppData%\Avanite\BrowserFavorites If required, enter your preferred location as a literal path or as a UNC path. Note, the folder specified will be accessed as the user so required read/write access to the folder must be granted.
Force Internet Explorer to close	It is recommended that this policy is enabled to ensure Favorites are synchronized in a timely manner. By default, within Internet Explorer, the iexplore.exe process remains alive for 30 seconds after a user closes the browser. This policy ensures the iexplore.exe process is ended as soon as the user closes the browser. Enabling this policy adds the following registry values for each user session: [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.
Read Only Mode	It is recommended that this policy is enabled only when required. This policy defines whether user Favorite synchronization operates in read-only mode. In read-only mode user Favorites are not synchronized between browsers, but the file and database which holds user Favorites data are still populated. This can be used for migration purposes if required.

	To allow the collection of the Favorites data, this policy requires one or more browsers to be selected within the Favorites Browser Selection policy.

Avanite\WebData Control 4.8 SP1\Favorites Synchronization\Default Favorites Configuration

Policy	*Description*
Default Chrome Favorites	It is recommended that this policy is enabled only when required. This policy configures a default set of bookmarks (or Favorites) for Chrome. To create this in Chrome, enter the name and the URL required. Example: Value Name: Example Value: https://www.example.com/ This would create a shortcut called Example pointing to https://www.example.com/ When a default Favorite is created it is automatically excluded from synchronization to other browsers. Note, a default Favorite can be added to a folder by including it as part of the Value Name. Example: Value Name: Example Favorites\Example Value: https://www.example.com/ This would create the folder Example Favorites with a bookmark named Example. To list the Favorite within the Other Bookmarks folder, begin the Value Name with other\. Example: Value Name: other\Example Favorites\Example Value: https://www.example.com/ This would create the folder Example Favorites with a bookmark named Example under the Other Bookmarks section within Chrome. If other\ is not specified then the Favorite will be placed on the toolbar.
Default Edge Chromium Favorites	It is recommended that this policy is enabled only when required. This policy configures a default set of bookmarks (or Favorites) for Edge Chromium. To create this in Edge Chromium, enter the name and the URL required. Example:

	Value Name: Example Value: https://www.example.com/ This would create a shortcut called Example pointing to https://www.example.com/ When a default Favorite is created it is automatically excluded from synchronization to other browsers. Note, a default Favorite can be added to a folder by including it as part of the Value Name. Example: Value Name: Example Favorites\Example Value: https://www.example.com/ This would create the folder Example Favorites with a bookmark named Example. To list the Favorite within the Other Bookmarks folder, begin the Value Name with other\. Example: Value Name: other\Example Favorites\Example Value: https://www.example.com/ This would create the folder Example Favorites with a bookmark named Example under the Other Bookmarks section within Edge Chromium. If other\ is not specified then the Favorite will be placed on the toolbar.
Default Firefox Favorites	It is recommended that this policy is enabled only when required. This policy configures a default set of bookmarks (or Favorites) for Firefox. To create this in Firefox, enter the name and the URL required. Example: Value Name: Example Value: https://www.example.com/ This would create a shortcut called Example pointing to https://www.example.com/ When a default Favorite is created it is automatically excluded from synchronization to other browsers. Note, a default Favorite can be added to a folder by including it as part of the Value Name. Example: Value Name: Example Favorites\Example Value: https://www.example.com/ This would create the folder Example Favorites with a bookmark named Example.

	To list the Favorite within the Other Bookmarks folder, begin the Value Name with other\. Example: Value Name: other\Example Favorites\Example Value: https://www.example.com/ This would create the folder Example Favorites with a bookmark named Example under the Other Bookmarks section within Firefox. If other\ is not specified then the Favorite will be placed on the toolbar.
Default Internet Explorer Favorites	It is recommended that this policy is enabled only when required. This policy configures a default set of bookmarks (or Favorites) for Internet Explorer. To create this in Internet Explorer, enter the name and the URL required. Example: Value Name: Example Value: https://www.example.com/ This would create a shortcut called Example pointing to https://www.example.com/ When a default Favorite is created it is automatically excluded from synchronization to other browsers. Note, a default Favorite can be added to a folder by including it as part of the Value Name. Example: Value Name: Example Favorites\Example Value: https://www.example.com/ This would create the folder Example Favorites with a bookmark named Example. To list the Favorite within the Other Bookmarks folder, begin the Value Name with other\. Example: Value Name: other\Example Favorites\Example Value: https://www.example.com/ This would create the folder Example Favorites with a bookmark named Example under the Other Bookmarks section within Internet Explorer. If other\ is not specified then the Favorite will be placed on the toolbar.

Avanite\WebData Control 4.8 SP1\Global

Policy	*Description*
Diagnostic Logging	It is recommended that this policy is enabled only when required. This policy defines whether WebData Control diagnostic logging is enabled or not. Enabling this policy will enable WebData Control logging. Enter a value for the Log path to define the location of the log files. Example: C:\Temp The entry requires a directory path only. The file name is generated automatically by WebData Control.
Enable Notifications	It is recommended that this policy is enabled only when required. This policy configures the various features within WebData Control to display toast notifications to report on the various events that have occurred. A custom title can be specified to be displayed within the toast notification. A custom icon can be specified to be displayed within the toast notification. It is recommended that a 128x128 icon is used. If required, the custom icon can be entered as a literal filename or as a UNC filename. Note, the specified icon will be accessed as the user so required read access to the folder must be granted.
Event Logging	It is recommended that this policy is enabled only when required. When enabled this policy allows for events to be raised to the Application event log for the WebData Management, Browser Redirector and Favorites Synchronization features. To generate events for the WebData Management feature, select the option: WebData Management Events. Events will be raised for Cookies, History, Browser Databases, Extensions and Extension Locales. To generate events for the Favorites Synchronization feature, select the option: Favorites Synchronization Events. Events will be raised for creation of Default favorites and synchronization of user favorites. To generate events for the Browser Redirector feature, select the option: Browser Redirector Events. Events will be raised when redirection occurs.
License	This policy allows the WebData Control License to be distributed and must be enabled. In the List of License keys to deploy field, enter the Avanite provided license key.

	Without a license WebData Control will not function.

Avanite\WebData Control 4.8 SP1\Network Service

Policy	*Description*
Enable Automatic Updates	Enabling this policy is recommended if you are using the WebData Management feature with the Network Service installed and the Remove known advertising and tracking cookies policy is enabled. This policy enables the Automatic Update feature. Enabling this policy will ensure that the data files used to define advertising and tracking cookies are automatically updated. This will ensure the latest definitions file for advertising and tracking cookies can be used by WebData Management.

Avanite\WebData Control 4.8 SP1\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 Administrators group. Note that when Browser Redirector is enabled, by default it is 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 executes only for users belonging to specified Active Directory groups. Active Directory groups are specified as follows: {Domain Netbios Name}\{Group Name} Where each entry is separated using a semi-colon ; Examples: Avanite\User Group 1 Avanite\User Group 1;Avanite\User Group 2
Enable Browser Redirector	Enabling this policy is required if you require Browser Redirector functionality. This policy enables the Browser Redirector feature. Enabling this policy will ensure that Browser Redirector is run by the Avanite WebData Control Notification Service.
Enable Favorites Synchronization	Enabling this policy is required if you require Favorites Synchronization functionality. This policy enables the Favorites Synchronization feature.

	Enabling this policy will ensure that Favorites Synchronization is run by the Avanite WebData Control Notification Service.
Enable WebData Management	This policy enables the WebData Management feature. Enabling this policy allows the Avanite WebData Control Notification Service to handle the WebData Management features of WebData Control. This policy will execute at user log off for all browsers. Options are available for Firefox, Chrome and Edge Chromium to perform data removal as users exit these browsers. Another option can be enabled: "Enable Application Group Support". This policy changes the behaviour of the Firefox, Chrome and Edge Chromium processing to ensure compatibility with Ivanti Environment Manager Personalization Groups. An additional option can be Enabled: Disable WebData Management execution during logoff. This policy allows WebData Management to be executed using a third-party application such as Ivanti Environment Manager. If this policy is not configured, or set to disabled, then WebData Management can be instigated via a third-party mechanism as required.
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 Administrators group. Note that when Favorites Synchronization is enabled, by default it is 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 executes only for users belonging to specified Active Directory groups. Active Directory groups are specified as follows: {Domain Netbios Name}\{Group Name} Where each entry is separated using a semi-colon ; Examples: Avanite\User Group 1 Avanite\User Group 1;Avanite\User Group 2
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 Administrators group. Note that when the WebData Management is enabled, by default it is enabled for all users.

WebData Control Logoff Message	This policy defines the log off message for WebData Management. Enabling this policy allows for a custom log off message to be displayed when WebData Management is executed during the log off phase of a user session. By default, when the WebData Management is enabled, no message is displayed during log off.
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 executes only for users belonging to specified Active Directory groups. Active Directory groups are specified as follows: {Domain Netbios Name}\{Group Name} Where each entry is separated using a semi-colon ; Examples: Avanite\User Group 1 Avanite\User Group 1;Avanite\User Group 2

Avanite\WebData Control 4.8 SP1\WebData Management

Policy	*Description*
Default Configuration	It is recommended that this policy is enabled only when required. This policy defines a default configuration for WebData Management. Enabling this policy will apply recommended settings and a basic configuration for WebData Management. Note: If additional policies are enabled they will override the settings in the default configuration.

Avanite\WebData Control 4.8 SP1\WebData Management\Advanced

Policy	*Description*
Data Optimization	This policy allows the option for user web database optimization to be enabled. Enabling this policy allows WebData Management to optimize and compact the various web databases to ensure they use a minimum amount of disk space. This applies to a number of relevant databases including: webcachev01.dat and the databases used by Chrome, Edge Chromium and Firefox.
Key Site Purge List	It is recommended that this policy is enabled only when required. This policy allows you to specify sites where associated browsing data is removed. This policy overrides any other policy settings you may have in place for all browser types without exception. To add sites to this policy specify the particular URL required. The URL should be specific to the data you wish to remove. Add any required URL in the List of sites to remove field. Example: website.com/software Removes data related to website.com/software pages Enable the Apply to cookie data option to remove all cookie data for sites matching the defined URLs. Enable the Apply to history data option to 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.

Key Site Retention List	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. This policy allows you to specify sites where associated browsing data is retained. This policy will override any other settings you may have in place for all browser types except for those specified in the Key Site Purge List policy. To add sites to this policy specify the particular URL required. The URL should be specific to the data you wish to retain. Add any required URL in the List of sites to retain field. Example: website.com/software Retains data related to website.com/software pages Enable the Apply to cookie data option to retain all cookie data for sites matching the defined URLs. Enable the Apply to history data option to retain all history data for sites matching the defined URLs. Enable the Apply to DOM data option to 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.

Avanite\WebData Control 4.8 SP1\WebData Management\Chrome

Policy	*Description*
Chrome Cookie Retention	It is recommended that this setting is enabled with specific options configured. The recommended settings for this policy are: Retain specified number of browsing days: Enabled and value set to 7 days Remove expired cookies: Enabled Enabling this policy allows for management of Chrome cookie data, and retains the data for a specific number of days. To remove all cookie related web data for the user, select the option: Clear all Cookies To allow cookies to be retained for a specified number of days, select the option: Retain specified number of calendar days To allow cookies to be retained for a specified number of active browsing days, select the option: Retain specified number of browsing days Note this setting retains cookie data for the number of days selected where browsing activity has occurred. This excludes any days of inactivity. To remove cookies which have expired, enable the option: Remove expired cookies To remove cookies which do not have the Secure flag, enable the option: Retain only secure cookies To remove cookies that do not have the HttpOnly flag, enable the option: Retain only HttpOnly cookies
Chrome Cookie Type Removal	It is recommended this policy is enabled with specific options configured. Recommended settings for this policy: Remove known advertising and tracking cookies: Enabled The policy allows granular control over which cookie types are retained. Enabling the policy allows you to remove cookies based on their type. For example, _ga cookies are used to gather data about website activity by Google Analytics and you may choose to remove them. To remove cookie types identified as being used for advertising or tracking purposes enable the option: Remove known advertising and tracking cookies Note, the WebData Control agent includes a pre-defined list of known advertising and tracking cookie types which is used when this option is enabled. Removal of these cookies will not affect the usability of websites.

	To define specific cookie types to be removed enter the cookie type in the field: List of Cookie types Note that when you add a cookie type to the list an exact match is required - including case. When both options are enabled the List of Cookie types is appended to the Remove known advertising and tracking cookies list.
Chrome Data Report	It is recommended that this policy is enabled only when required. When enabled, this policy generates data exports of the WebData Management activity for Chrome. The report contains all entries and the action performed upon each item. Separate files are generated for cookie and history data. The cookie report contains all cookie types for all URLs. When enabled a folder path is required to specify the report location. For example, C:\Temp To remove user references from the exported data, enable the option: Anonymize the exported data
Chrome DOM Data Removal	It is recommended that this setting is enabled. When enabled, this policy removes Chrome Document Object Model (DOM) data. DOM data is used by browsers to store a variety of data required by web browsing. The data is retained for caching purposes.
Chrome Extension Locale Removal	It is recommended that this policy is enabled only when required. Locale data may be present for each Chrome extension with locale information being present for each supported language. When enabled, this policy manages locale data installed as part of Chrome extensions. Note: The list specified is used for an exact text match (case insensitive). Wildcards are also supported. Example: en* retains all locales that start with en. The default locale for each extension will always be retained.
Chrome Extension Removal	It is recommended that this policy is enabled only when required. This policy manages Chrome extensions, removing them according to the options selected. To explicitly remove all Chrome extensions listed, enable the option: Extensions to be removed To explicitly retain specific Chrome extensions, enable the option: Extensions to be retained To remove all Chrome extensions, enable the option: Remove All Extensions

	Note: For the Extensions to be removed and Extensions to be retained options the verification will use an exact text match (case insensitive). However wildcard use is supported to perform a contains check. Example: Avanite* removes all extensions that start with Avanite.
Chrome History Retention	It is recommended that this setting is enabled. The recommended setting for this policy is: Retain specified number of browsing days: Enabled and value set to 7 days Enabling this policy option allows for history data to be retained for a specific number of days. To remove all history related web data for the user, enable the option: Clear all history To allow history to be retained for a specific number of days, enable the option: Retain specified number of calendar days To allow history data to be retained for a specified number of active browsing days, enable the option: Retain specified number of browsing days Note this setting retains history data for the number of days selected where browsing activity has occurred. This excludes any days of inactivity.
Chrome Temporary Internet Data Removal	It is recommended that this setting is enabled. When enabled this policy removes Chrome temporary internet data.
Chrome Third Party Cookie Removal	It is recommended that this setting is enabled. When enabled this policy removes Chrome third party cookies. Third party cookies are generated from domains which do not match that of the primary website browsed.

Avanite\WebData Control 4.8 SP1\WebData Management\Edge

Policy	*Description*
Edge Compatibility Data Removal	It is recommended that this setting is enabled. When enabled, this policy removes Edge related compatibility mode data from the webcache database. Compatibility mode data is updated dynamically by the browser and does not need to be retained.
Edge Cookie Retention	It is recommended that this setting is enabled with specific options configured. The recommended settings for this policy are: Retain specified number of browsing days: Enabled and value set to 7 days Remove expired cookies: Enabled Enabling this policy allows for management of Edge cookie data, and retains the data for a specific number of days. To remove all cookie related web data for the user, select the option: Clear all Cookies To allow cookies to be retained for a specified number of days, select the option: Retain specified number of calendar days To allow cookies to be retained for a specified number of active browsing days, select the option: Retain specified number of browsing days Note this setting retains cookie data for the number of days selected where browsing activity has occurred. This excludes any days of inactivity. To remove cookies which have expired, enable the option: Remove expired cookies To remove cookies which do not have the Secure flag, enable the option: Retain only secure cookies To remove cookies that do not have the HttpOnly flag, enable the option: Retain only HttpOnly cookies
Edge Cookie Type Removal	It is recommended this policy is enabled with specific options configured. Recommended settings for this policy: Remove known advertising and tracking cookies: Enabled The policy allows granular control over which cookie types are retained. Enabling the policy allows you to remove cookies based on their type. For example, _ga cookies are used to gather data about website activity by Google Analytics and you may choose to remove them.

	To remove cookie types identified as being used for advertising or tracking purposes enable the option: Remove known advertising and tracking cookies Note, the WebData Control agent includes a pre-defined list of known advertising and tracking cookie types which is used when this option is enabled. Removal of these cookies will not affect the usability of websites. To define specific cookie types to be removed enter the cookie type in the field: List of Cookie types Note that when you add a cookie type to the list an exact match is required - including case. When both options are enabled the List of Cookie types is appended to the Remove known advertising and tracking cookies list.
Edge Data Report	It is recommended that this policy is enabled only when required. When enabled, this policy generates data exports of the WebData Management activity for Edge. The report contains all entries and the action performed upon each item. Separate files are generated for cookie and history data. The cookie report contains all cookie types for all URLs. When enabled a folder path is required to specify the report location. For example, C:\Temp To remove user references from the exported data, enable the option: Anonymize the exported data
Edge DOM Data Removal	It is recommended that this setting is enabled. Settings will depend on how the environment is configured. When enabled, this policy removes Edge Document Object Model (DOM) data. DOM data is used by browsers to store a variety of data required by web browsing. The data is retained for caching purposes. To remove all Edge DOM data referenced in the webcache from the file system enable the option: Delete all files To remove all references to Edge DOM data from the webcache database, enable the option: Do not remove files on disk When a persistent profile is being used the recommendation is to enable: Delete all files When a non-persistent profile is being used the recommendation is to enable: Do not remove files on disk
Edge Enterprise Mode Data Removal	It is recommended that this setting is enabled. This policy removes any Edge related Enterprise Mode data stored in the webcache database. Enterprise Mode data is dynamically updated by the browser and the data does not need to be retained within the webcache database.

Edge History Retention	It is recommended that this setting is enabled. The recommended setting for this policy is: Retain specified number of browsing days: Enabled and value set to 7 days Enabling this policy option allows for history data to be retained for a specific number of days. To remove all history related web data for the user, enable the option: Clear all history To allow history to be retained for a specific number of days, enable the option: Retain specified number of calendar days To allow history data to be retained for a specified number of active browsing days, enable the option: Retain specified number of browsing days Note this setting retains history data for the number of days selected where browsing activity has occurred. This excludes any days of inactivity.
Edge Temporary Internet Files Data Removal	This policy removes Edge temporary internet files data. The recommended setting for this policy will depend on how the environment is configured. When enabled all temporary internet files data references in the webcache database will be removed. To remove all Edge temporary internet files data from the file system enable the option: Delete all files To remove references to Edge temporary internet files data from the webcache database whilst leaving the file system untouched, enable the option: Do not remove files on disk When a persistent profile is being used the recommended setting to enable is: Delete all files When a non-persistent profile is being used the recommended setting to enable is: Do not remove files on disk
Edge Third Party Cookie Removal	It is recommended that this setting is enabled. When enabled this policy removes Edge third party cookies. Third party cookies are generated from domains which do not match that of the primary website browsed.

Avanite\WebData Control 4.8 SP1\WebData Management\Edge Chromium

Policy	*Description*
Edge Chromium Cookie Retention	It is recommended that this setting is enabled with specific options configured. The recommended settings for this policy are: Retain specified number of browsing days: Enabled and value set to 7 days Remove expired cookies: Enabled Enabling this policy allows for management of Edge Chromium cookie data, and retains the data for a specific number of days. To remove all cookie related web data for the user, select the option: Clear all Cookies. To allow cookies to be retained for a specified number of days, select the option: Retain specified number of calendar days To allow cookies to be retained for a specified number of active browsing days, select the option: Retain specified number of browsing days Note this setting retains cookie data for the number of days selected where browsing activity has occurred. This excludes any days of inactivity. To remove cookies which have expired, enable the option: Remove expired cookies To remove cookies which do not have the Secure flag, enable the option: Retain only secure cookies To remove cookies that do not have the HttpOnly flag, enable the option: Retain only HttpOnly cookies
Edge Chromium Cookie Type Removal	It is recommended this policy is enabled with specific options configured. Recommended settings for this policy: Remove known advertising and tracking cookies: Enabled The policy allows granular control over which cookie types are retained. Enabling the policy allows you to remove cookies based on their type. For example, _ga cookies are used to gather data about website activity by Google Analytics and you may choose to remove them. To remove cookie types identified as being used for advertising or tracking purposes enable the option: Remove known advertising and tracking cookies Note, the WebData Control agent includes a pre-defined list of known advertising and tracking cookie types which is used when this option is enabled. Removal of these cookies will not affect the usability of websites.

	To define specific cookie types to be removed enter the cookie type in the field: List of Cookie types Note that when you add a cookie type to the list an exact match is required - including case. When both options are enabled the List of Cookie types is appended to the Remove known advertising and tracking cookies list.
Edge Chromium Data Report	It is recommended that this policy is enabled only when required. When enabled, this policy generates data exports of the WebData Management activity for Edge Chromium. The report contains all entries and the action performed upon each item. Separate files are generated for cookie and history data. The cookie report contains all cookie types for all URLs. When enabled a folder path is required to specify the report location. For example, C:\Temp To remove user references from the exported data, enable the option: Anonymize the exported data
Edge Chromium DOM Data Removal	It is recommended that this setting is enabled. When enabled, this policy removes Edge Chromium Document Object Model (DOM) data. DOM data is used by browsers to store a variety of data required by web browsing. The data is retained for caching purposes.
Edge Chromium Enterprise Mode Data Removal	It is recommended that this setting is enabled. This policy removes any Edge Chromium related Enterprise Mode data stored in the webcache database. Enterprise Mode data is dynamically updated by the browser and the data does not need to be retained within the webcache database. Note, this setting overcomes the need to wait 65 seconds at browser launch as referenced int the following Microsoft article - https://docs.microsoft.com/en-us/internet-explorer/ie11-deploy-guide/check-fornew-enterprise-mode-site-list-xml-file.
Edge Chromium Extension Locale Removal	It is recommended that this policy is enabled only when required. Locale data may be present for each Edge Chromium extension with locale information being present for each supported language. When enabled, this policy manages locale data installed as part of Edge Chromium extensions. Note: The list specified is used for an exact text match (case insensitive). Wildcards are also supported. Example: en* retains all locales that start with en. The default locale for each extension will always be retained.
Edge Chromium Extension Removal	It is recommended that this policy is enabled only when required.

	This policy manages Edge Chromium extensions, removing them according to the options selected. To explicitly remove all Edge Chromium extensions listed, enable the option: Extensions to be removed. To explicitly retain specific Edge Chromium extensions, enable the option: Extensions to be retained. To remove all Edge Chromium extensions, enable the option: Remove All Extensions Note: For the Extensions to be removed and Extensions to be retained options the verification will use an exact text match (case insensitive). However wildcard use is supported to perform a contains check. Example: Avanite* removes all extensions that start with Avanite.
Edge Chromium History Retention	It is recommended that this setting is enabled. The recommended setting for this policy is: Retain specified number of browsing days: Enabled and value set to 7 days Enabling this policy option allows for history data to be retained for a specific number of days. To remove all history related web data for the user, enable the option: Clear all history To allow history to be retained for a specific number of days, enable the option: Retain specified number of calendar days To allow history data to be retained for a specified number of active browsing days, enable the option: Retain specified number of browsing days Note this setting retains history data for the number of days selected where browsing activity has occurred. This excludes any days of inactivity.
Edge Chromium Temporary Internet Data Removal	It is recommended that this setting is enabled. When enabled this policy removes Edge Chromium temporary internet data.
Edge Chromium Third Party Cookie Removal	It is recommended that this setting is enabled. When enabled this policy removes Edge Chromium third party cookies. Third party cookies are generated from domains which do not match that of the primary website browsed.

Avanite\WebData Control 4.8 SP1\WebData Management\Firefox

Policy	*Description*
Firefox Cookie Retention	It is recommended that this setting is enabled with specific options configured. The recommended settings for this policy are: Retain specified number of browsing days: Enabled and value set to 7 days Remove expired cookies: Enabled Enabling this policy allows for management of Firefox cookie data, and retains the data for a specific number of days. To remove all cookie related web data for the user, select the option: Clear all Cookies To allow cookies to be retained for a specified number of days, select the option: Retain specified number of calendar days To allow cookies to be retained for a specified number of active browsing days, select the option: Retain specified number of browsing days Note this setting retains cookie data for the number of days selected where browsing activity has occurred. This excludes any days of inactivity. To remove cookies which have expired, enable the option: Remove expired cookies To remove cookies which do not have the Secure flag, enable the option: Retain only secure cookies To remove cookies that do not have the HttpOnly flag, enable the option: Retain only HttpOnly cookies
Firefox Cookie Type Removal	It is recommended this policy is enabled with specific options configured. Recommended settings for this policy: Remove known advertising and tracking cookies: Enabled The policy allows granular control over which cookie types are retained. Enabling the policy allows you to remove cookies based on their type. For example, _ga cookies are used to gather data about website activity by Google Analytics and you may choose to remove them. To remove cookie types identified as being used for advertising or tracking purposes enable the option: Remove known advertising and tracking cookies Note, the WebData Control agent includes a pre-defined list of known advertising and tracking cookie types which is used when this option is enabled. Removal of these cookies will not affect the usability of websites.

	To define specific cookie types to be removed enter the cookie type in the field: List of Cookie types Note that when you add a cookie type to the list an exact match is required - including case. When both options are enabled the List of Cookie types is appended to the Remove known advertising and tracking cookies list.
Firefox Data Report	It is recommended that this policy is enabled only when required. When enabled, this policy generates data exports of the WebData Management activity for Firefox. The report contains all entries and the action performed upon each item. Separate files are generated for cookie and history data. The cookie report contains all cookie types for all URLs. When enabled a folder path is required to specify the report location. For example, C:\Temp To remove user references from the exported data, enable the option: Anonymize the exported data
Firefox DOM Data Removal	It is recommended that this setting is enabled. When enabled, this policy removes Firefox Document Object Model (DOM) data. DOM data is used by browsers to store a variety of data required by web browsing. The data is retained for caching purposes.
Firefox History Retention	It is recommended that this setting is enabled. The recommended setting for this policy is: Retain specified number of browsing days: Enabled and value set to 7 days Enabling this policy option allows for history data to be retained for a specific number of days. To remove all history related web data for the user, enable the option: Clear all history To allow history to be retained for a specific number of days, enable the option: Retain specified number of calendar days To allow history data to be retained for a specified number of active browsing days, enable the option: Retain specified number of browsing days Note this setting retains history data for the number of days selected where browsing activity has occurred. This excludes any days of inactivity.
Firefox Temporary Internet Data Removal	It is recommended that this setting is enabled. When enabled this policy removes Firefox temporary internet data.
Firefox Third Party Cookie Removal	It is recommended that this setting is enabled. When enabled this policy removes Firefox third party cookies.

	Third party cookies are generated from domains which do not match that of the primary website browsed.

Avanite\WebData Control 4.8 SP1\WebData Management\Internet Explorer

Policy	*Description*
Internet Explorer Compatibility Data Removal	It is recommended that this setting is enabled. When enabled, this policy removes Internet Explorer related compatibility mode data from the webcache database. Compatibility mode data is updated dynamically by the browser and does not need to be retained.
Internet Explorer Cookie Retention	It is recommended that this setting is enabled with specific options configured. The recommended settings for this policy are: Retain specified number of browsing days: Enabled and value set to 7 days Remove expired cookies: Enabled Enabling this policy allows for management of Internet Explorer cookie data, and retains the data for a specific number of days. To remove all cookie related web data for the user, select the option: Clear all Cookies To allow cookies to be retained for a specified number of days, select the option: Retain specified number of calendar days To allow cookies to be retained for a specified number of active browsing days, select the option: Retain specified number of browsing days Note this setting retains cookie data for the number of days selected where browsing activity has occurred. This excludes any days of inactivity. To remove cookies which have expired, enable the option: Remove expired cookies To remove cookies which do not have the Secure flag, enable the option: Retain only secure cookies To remove cookies that do not have the HttpOnly flag, enable the option: Retain only HttpOnly cookies
Internet Explorer Cookie Type Removal	It is recommended this policy is enabled with specific options configured. Recommended settings for this policy: Remove known advertising and tracking cookies: Enabled The policy allows granular control over which cookie types are retained.

	Enabling the policy allows you to remove cookies based on their type. For example, _ga cookies are used to gather data about website activity by Google Analytics and you may choose to remove them. To remove cookie types identified as being used for advertising or tracking purposes enable the option: Remove known advertising and tracking cookies Note, the WebData Control agent includes a pre-defined list of known advertising and tracking cookie types which is used when this option is enabled. Removal of these cookies will not affect the usability of websites. To define specific cookie types to be removed enter the cookie type in the field: List of Cookie types Note that when you add a cookie type to the list an exact match is required - including case. When both options are enabled the List of Cookie types is appended to the Remove known advertising and tracking cookies list.
Internet Explorer Data Report	It is recommended that this policy is enabled only when required. When enabled, this policy generates data exports of the WebData Management activity for Internet Explorer. The report contains all entries and the action performed upon each item. Separate files are generated for cookie and history data. The cookie report contains all cookie types for all URLs. When enabled a folder path is required to specify the report location. For example, C:\Temp To remove user references from the exported data, enable the option: Anonymize the exported data
Internet Explorer DOM Data Removal	It is recommended that this setting is enabled. Settings will depend on how the environment is configured. When enabled, this policy removes Internet Explorer Document Object Model (DOM) data. DOM data is used by browsers to store a variety of data required by web browsing. The data is retained for caching purposes. To remove all Internet Explorer DOM data referenced in the webcache from the file system enable the option: Delete all files To remove all references to Internet Explorer DOM data from the webcache database, enable the option: Do not remove files on disk When a persistent profile is being used the recommendation is to enable: Delete all files When a non-persistent profile is being used the recommendation is to enable: Do not remove files on disk
Internet Explorer Enterprise Mode Data Removal	It is recommended that this setting is enabled. This policy removes any Internet Explorer related Enterprise Mode data stored in the webcache database.

	Enterprise Mode data is dynamically updated by the browser and the data does not need to be retained within the webcache database. Note, this setting overcomes the need to wait 65 seconds at browser launch as referenced in the following Microsoft article - https://docs.microsoft.com/en-us/internet-explorer/ie11-deploy-guide/check-fornew-enterprise-mode-site-list-xml-file.
Internet Explorer History Retention	It is recommended that this setting is enabled. The recommended setting for this policy is: Retain specified number of browsing days: Enabled and value set to 7 days Enabling this policy option allows for history data to be retained for a specific number of days. To remove all history related web data for the user, enable the option: Clear all history To allow history to be retained for a specific number of days, enable the option: Retain specified number of calendar days To allow history data to be retained for a specified number of active browsing days, enable the option: Retain specified number of browsing days Note this setting retains history data for the number of days selected where browsing activity has occurred. This excludes any days of inactivity.
Internet Explorer Temporary Internet Files Data Removal	This policy removes Internet Explorer temporary internet files data The recommended setting for this policy will depend on how the environment is configured. When enabled all temporary internet files data references in the webcache database will be removed. To remove all Internet Explorer temporary internet files data from the file system enable the option: Delete all files To remove references to Internet Explorer temporary internet files data from the webcache database whilst leaving the file system untouched, enable the option: Do not remove files on disk When a persistent profile is being used the recommended setting to enable is: Delete all files When a non-persistent profile is being used the recommended setting to enable is: Do not remove files on disk
Internet Explorer Third Party Cookie Removal	It is recommended that this setting is enabled. When enabled this policy removes Internet Explorer third party cookies. Third party cookies are generated from domains which do not match that of the primary website browsed.

Avanite\WebData Control 4.8 SP1\WebData Management\Windows Store Apps

Policy	*Description*
Windows Store Apps Data Removal	It is recommended that this setting is Enabled. This policy allows the removal of data related to Windows Store Applications from the webcache database. Windows Store Applications access the internet store data inside the webcache database. Enabling this policy removes all Windows Store Application data. The Exclusion option allows the retention of web data for Windows Store applications. Specify the data to be kept by defining the application name to match. Example: Microsoft.Office.OneNote

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, or the "Disable WebData Management execution during logoff" policy is configured this can also be done via a Group Policy Logoff action as shown below:

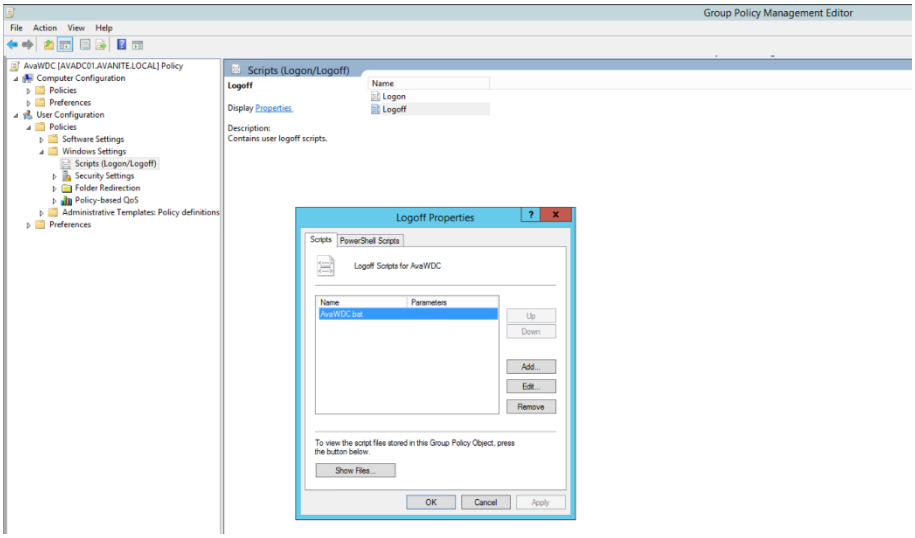


Figure 16 – Logoff Trigger

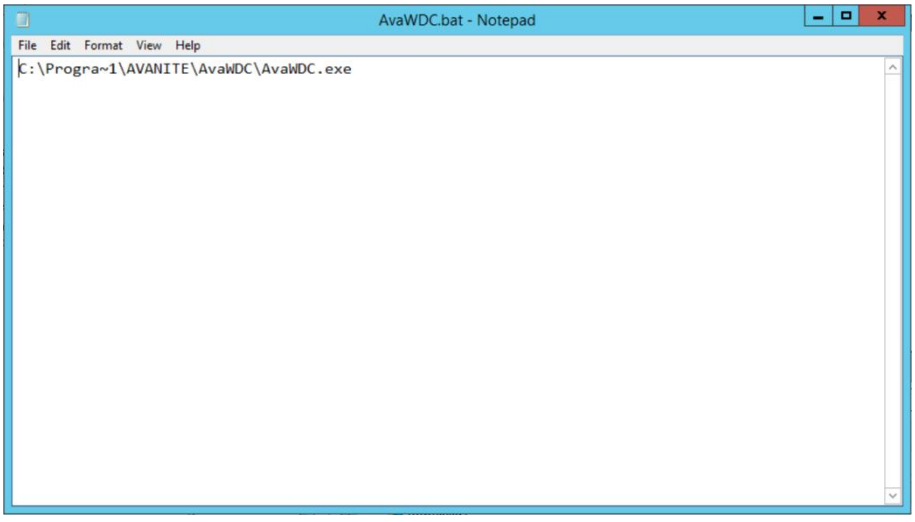


Figure 17 – Launch batch file

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.

Cookie Security Flags

Secure

Cookies can be set with a secure flag which forbids the cookie to be transmitted over simple HTTP. By default, cookies are not set with the secure flag.

HttpOnly

Cookies can be set with a HttpOnly flag which limits the scope of the cookie and prevents the use of the cookie on the client side. By default, cookies can be set and used over HTTP and directly by the browser via javascript. Setting the HttpOnly flag restricts access to cookies via javascript at the client side.

Appendix B – Temporary Internet and DOM data

WebData Control has a number of options for configuring retention and removal of browser cache information such as temporary internet files and DOM data.

For the Internet Explorer and Microsoft Edge (Legacy) browsers this is handled using the relevant WebData Management policies which have options related to removing the temporary internet files and DOM data from the webcachev01.dat database with options relating to whether the referenced files should be deleted from the filesystem or not.

For the Google Chrome, Microsoft Edge (Chromium) and Mozilla Firefox browsers the data that is deleted is managed via the AvaniteWDMSettings.ava file which is located in the C:\Program Files\Avanite\AvaWDC folder by default. When the relevant DOM Data removal or Temporary Internet Files Data Removal policies are enabled for these browsers the DOM and temporary internet files data will be removed according to the definitions contained in this file.

The file included by default is in JSON format and contains settings to remove the following items on a per browser basis:

- Folders related to Chrome Temporary Internet Files
- Files related to Chrome Temporary Internet Files
- Folders used to store temporary data
- Folders used to store DOM data

Each item can have a "retention" value specified (in seconds) which ensures that files and/or folders older than this are removed.

The settings for each browser are shown below:

Google Chrome

```
"ChromeFolderSettings": {
        "ProfileTempFolders": [
                {
                        "Name": "Application Cache"
                },                      {
                        "Name": "Cache"
                },                      {
                        "Name": "Code Cache"
                },                      {
                        "Name": "File System"
                },                      {
                        "Name": "Media Cache"
                },                      {
                        "Name": "Service Worker\\CacheStorage",
                        "Retention": "1209600"
                },
```

```
                {
                        "Name": "Service Worker\\ScriptCache",
                        "Retention": "1209600"
                },
                {
                        "Name": "Search Logos"
                }
        ],
        "ProfileTempFiles": [
                {
                        "Name": "*.old"
                },
                {
                        "Name": "*.dmp"
                },
                {
                        "Name": "*.tmp"
                }
        ],
        "TempFolders": [
                {
                        "Name": "SwReporter"
                },
                {
                        "Name": "PepperFlash"
                },
                {
                        "Name": "pnacl"
                },
                {
                        "Name": "PnaclTranslationCache"
                }
        ],
        "DOMFolders": [
                {
                        "Name": "Local Storage\\leveldb"
                }
        ]
}
```

Microsoft Edge (Chromium)

```
"EdgeChromiumFolderSettings": {
        "ProfileTempFolders": [
                {
                        "Name": "Application Cache"
                },
                {
                        "Name": "Cache"
                },
                {
                        "Name": "Code Cache"
                },
                {
                        "Name": "File System"
                },
                {
                        "Name": "Media Cache"
                },
                {
                        "Name": "Service Worker\\CacheStorage",
                        "Retention": "1209600"
                },
                {
                        "Name": "Service Worker\\ScriptCache",
                        "Retention": "1209600"
                },
                {
                        "Name": "Search Logos"
                }
        ],
        "ProfileTempFiles": [
                {
                        "Name": "*.old"
                },
                {
                        "Name": "*.dmp"
                },
                {
                        "Name": "*.tmp"
                }
        ],
        "TempFolders": [
                {
                        "Name": "PepperFlash"
                },
                {
```

```
                "Name": "pnacl"
            },
            {
                "Name": "PnaclTranslationCache"
            }
        ],
        "DOMFolders": [
            {
                "Name": "Local Storage\\leveldb"
            }
        ]
}
```

Mozilla Firefox

```
"FirefoxFolderSettings": {
            "ProfileTempFolders": [
                {
                    "Name": "cache2"
                },
                {
                    "Name": "offlinecache"
                }
            ],
            "DOMFolders": [
                {
                    "Name": "storage\\default folder"
                },
                {
                    "Name": "storage\\default"
                }
            ],
            "DOMFiles": [
                {
                    "Name": "webappsstore.sqlite"
                }
            ]
        }
}
```

Appendix C - 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 D – Event Details

Event ID	*Event details*
10900	Webcache details – webcache folder sizes before/after, webcache files before/after, webcache database before/after
10901	WebData Management processing (Internet Explorer)
10902	Internet Explorer cookies details – cookies before/after, removed cookie details
10903	Internet Explorer cookie files – cookie files before/after, removed cookie file details
10904	Internet Explorer history – history before/after, removed history details
10910	Google Chrome databases – sizes before/after
10911	WebData Management processing (Google Chrome)
10912	Google Chrome cookies details – cookies before/after, removed cookie details
10913	Google Chrome history – history before/after, removed history details
10915	Google Chrome extensions – extension details, extension locale details, extension action details
10920	Microsoft Edge Chromium databases – sizes before/after
10921	WebData Management processing (Microsoft Edge Chromium)
10922	Microsoft Edge Chromium cookies details – cookies before/after, removed cookie details
10923	Microsoft Edge Chromium history – history before/after, removed history details
10925	Microsoft Edge Chromium extensions – extension details, extension locale details, extension action details
10930	Mozilla Firefox databases – sizes before/after
10931	WebData Management processing (Mozilla Firefox)
10932	Mozilla Firefox cookies details – cookies before/after, removed cookie details
10933	Mozilla Firefox history – history before/after, removed history details
10950	Browser Redirector – setting default browser
10951	Browser Redirector – direct Link URL redirection details
10952	Browser Redirector – browser extension URL redirection details
10960	Favorites Synchronization – synchronization completed
10961	Favorites Synchronization – browser default favorites details
10970	WebData Control – license valid/invalid and license expiry details
10990	WebData Control – features enabled/disabled details

Appendix E – 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 history 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 F – Default Configuration

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

Policy	*Description*
WebData Management\Advanced	Data Optimization: ***Enabled***
WebData Management\Chrome	Chrome Cookie Retention: Enabled, Values: ***Retain Specified number of calendar 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 calendar days, 7 days*** Chrome Temporary Internet Data Removal: ***Enabled*** Chrome Third Party Cookie Removal: ***Enabled***
WebData Management\Edge	Edge Compatibility Data Removal: ***Enabled*** Edge Cookie Retention: ***Enabled***, Values: ***Retain Specified number of calendar 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 calendar days, 7 days*** Edge Temporary Internet Files Data Removal: ***Enabled***, Value: ***Delete all files*** Edge Third Party Cookie Removal: ***Enabled***
WebData Management\Edge Chromium	Edge Chromium Cookie Retention: Enabled, Values: ***Retain Specified number of calendar days, 7 days, Remove expired cookies*** Edge Chromium Cookie Type Removal: ***Enabled***, Value: ***Remove known advertising and tracking cookies*** Edge Chromium DOM Data Removal: ***Enabled*** Edge Chromium History Retention: ***Enabled***, Values: ***Retain Specified number of calendar days, 7 days*** Edge Chromium Temporary Internet Data Removal: ***Enabled*** Edge Chromium Third Party Cookie Removal: ***Enabled***
WebData Management\Firefox	Firefox Cookie Retention: ***Enabled***, Values: ***Retain Specified number of calendar 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 calendar days, 7 days*** Firefox Temporary Internet Data Removal: ***Enabled*** Firefox Third Party Cookie Removal: ***Enabled***
WebData Management\Internet Explorer	Internet Explorer Compatibility Data Removal: ***Enabled*** Internet Explorer Cookie Retention: ***Enabled***, Values: ***Retain Specified number of calendar 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 calendar days, 7 days*** Internet Explorer Temporary Internet Files Data Removal: ***Enabled***, Value: ***Delete all files*** Internet Explorer Third Party Cookie Removal: ***Enabled***
WebData Management\Windows Store Apps	Windows Store Apps Data Removal: ***Enabled***