



WebData Control Product Guide

Version 4.9



WEBDATA
CONTROL



Contents

About WebData Control.....	3
WebData Management.....	4
Browser Redirector.....	5
Favorites Synchronization	5
Resource Blocking.....	5
WebData Control Features	7
Browser Support	7
Operating System Support	7
WebData Management.....	8
Cookie Management	8
Browsing History Management.....	8
Temporary Internet Files	9
DOM Store Data	9
Compatibility Data.....	9
Enterprise Mode Data	10
Windows Store Applications.....	10
Data Optimization	10
Extension Management.....	11
Extension Locale Removal	11
Browser Redirector.....	12
URL Redirection	12
Setting the default browser	13
Enforcing use of a specific browser	13
Redirection to an external process.....	13
Launching with parameters.....	14
Favorites Synchronization	15
Resource Blocking.....	16
Ad Blocking	16
Automatic Updates	16
Network Service	17
Installing WebData Control.....	18
WebData Control Console	18



Installation	18
WebData Control Agent	21
Pre-Requisites	21
Manual Installation	21
Automated Installation	24
Configuring WebData Control	25
Console Layout and Navigation	25
File Menu	25
Global Settings	25
WebData Management Settings	27
Favorites Synchronization Settings	37
Browser Redirector Settings	42
Resource Blocking Settings	47
Configuration Deployment	48
Other Considerations	49
Microsoft Edge Chromium Startup Boost	49
Microsoft IEtoEdge BHO	49
The Microsoft Edge Chromium browser installs an IEtoEdge Browser Helper Object (BHO) in Internet Explorer when installed and this can cause issues with the WebData Control Browser Redirector feature.	49
Appendix A - Definitions	50
Appendix B – Temporary Internet and DOM data	51
Appendix C – Event Details	55
Appendix D – Data Report Format	56
Appendix E – Default Configuration	59



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. Internet Explorer and Microsoft Edge are present by default and the decision is often taken to provide Google Chrome or Mozilla Firefox as an alternative web browser for users.

There are various reasons for the delivery of multiple browsers, ranging from user choice 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.

With users accessing web resources on the internet browsers interact with web servers where web server administrators include tracking, advertising and analytical capabilities. The browsers arbitrarily executes web requests based on the browsers capabilities which often leads to browsers downloading additional content such as Ads. These requests require additional resources to process and display the content, increase the number of DNS requests and increases network utilization for little gain.

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

- WebData Management
- Browser Redirector
- Favorites Synchronization
- Resource Blocking



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.

Resource Blocking

Internet based websites often use tracking and advertising code that constitute the majority of the data downloaded by the browser and contributes to "web bloat". Advertising also increases the number of cookies served by websites, adds to the number of browser fingerprint requests and often increases behaviour tracking, all of which can have a negative impact on page load times. In addition to this there are security considerations in the form of malvertising and revenue generating activities which often lead to a diminished user experience.



WebData Control provides Resource Blocking capabilities which in the initial release provides an Ad Blocking capability. WebData Control can be used to enable Ad Blocking in Google Chrome and Microsoft Edge Chromium to improve the user experience, counter the negative points online advertising brings with it, and lowers resource wastage.

The WebData Control Resource Blocking feature will be enhanced in upcoming releases.



WebData Control Features

Browser Support

WebData Control provides support for the following browsers:

- Microsoft Internet Explorer 11
- Google Chrome
- Mozilla Firefox
- Microsoft Edge (Chromium)
- Microsoft Edge (Legacy)

***Note:** The Browser Redirector and Resource Blocking features work with Google Chrome 93+ and Edge Chromium 93+. Resource Blocking is only supported on Google Chrome and Microsoft Edge (Chromium)*

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 configuration 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 settings.

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 configuration settings. 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. 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. 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. 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 setting called **"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.



Resource Blocking

WebData Control's Resource Blocking feature can be enabled to provide Ad Blocking capabilities in the Google Chrome and Microsoft Edge (Chromium) browsers.

Ad Blocking

Ad Blocking capabilities are provided via a set of static and dynamic rules which are applied via browser extensions. These rules instruct the browser extension to block and allow web request based on a variety of patterns defined, and instruct the browser to modify web page CCS to hide/remove unwanted content.

The static rules are embedded into the bundled Resource Blocking extensions with dynamic rules being used to update the static rules as required.

For Resource Blocking to block Ads the following extensions need to be installed:

GOOGLE CHROME

To use WebData Control's Browser Redirector feature with Google Chrome an extension needs to be installed for each user. This extension is responsible for intercepting URL requests inside the Google Chrome 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. This extension is responsible for blocking web requests for Ads and manipulating CSS inside the Google Chrome browser.

Automatic Updates

Avanite manages an Azure hosted CDN which hosts the latest Ad Blocking definition files used by the Resource Blocking feature. The dynamic rules can be updated to use the latest definition files which is recommended to stay up to date with changes.



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 and the latest Resource Blocking Ad Blocking definition files.

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 and the Ad Blocking definition files used by Resource Blocking.



Installing WebData Control

WebData Control Console

With previous WebData Control releases configuration was done using a set of Group Policy ADMX templates. With this release the configuration is now done using the WebData Control Console which provides a simple user interface.

Installation

To install the WebData Control console, follow these steps:

1. As an administrator, run the WebDataControlConsole.msi. Click **Next** to continue the installation.

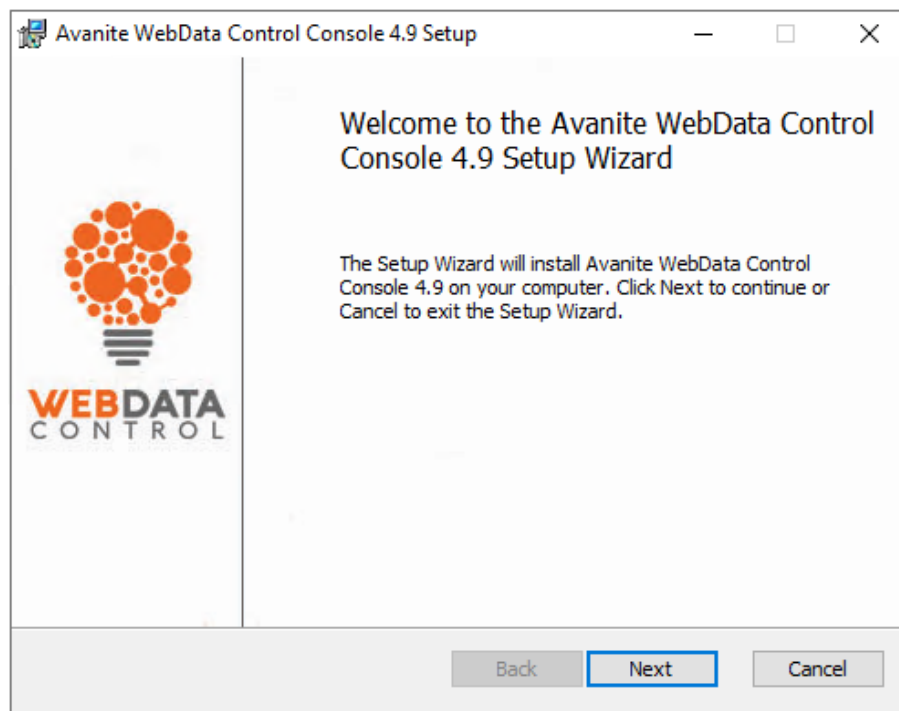


Figure 1 – Console Welcome screen

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

Keep the existing settings, 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.

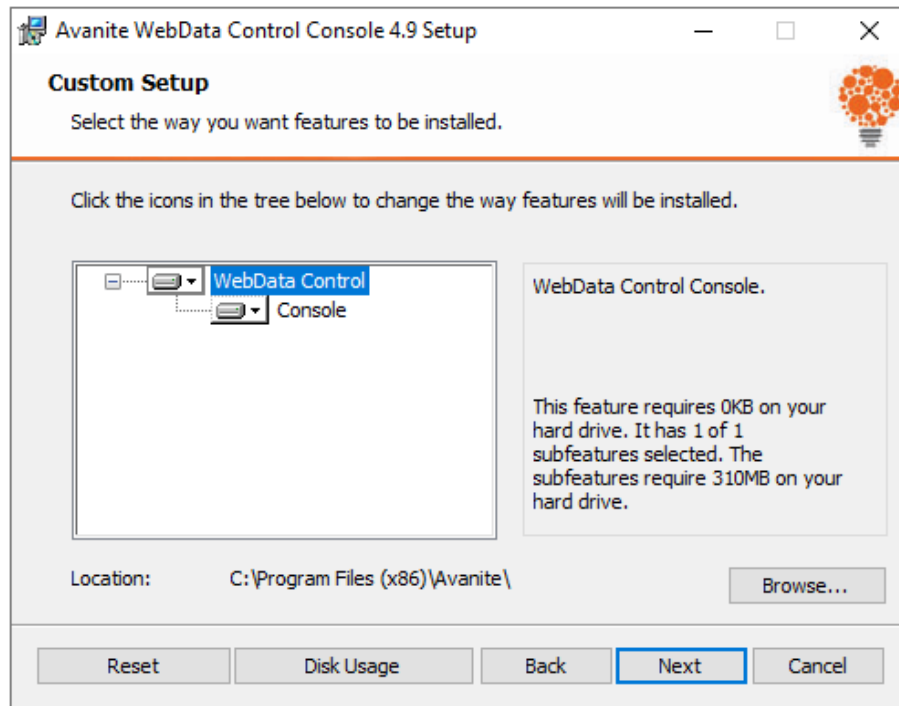


Figure 2 – Console Custom Setup options

3. Click **Install**.

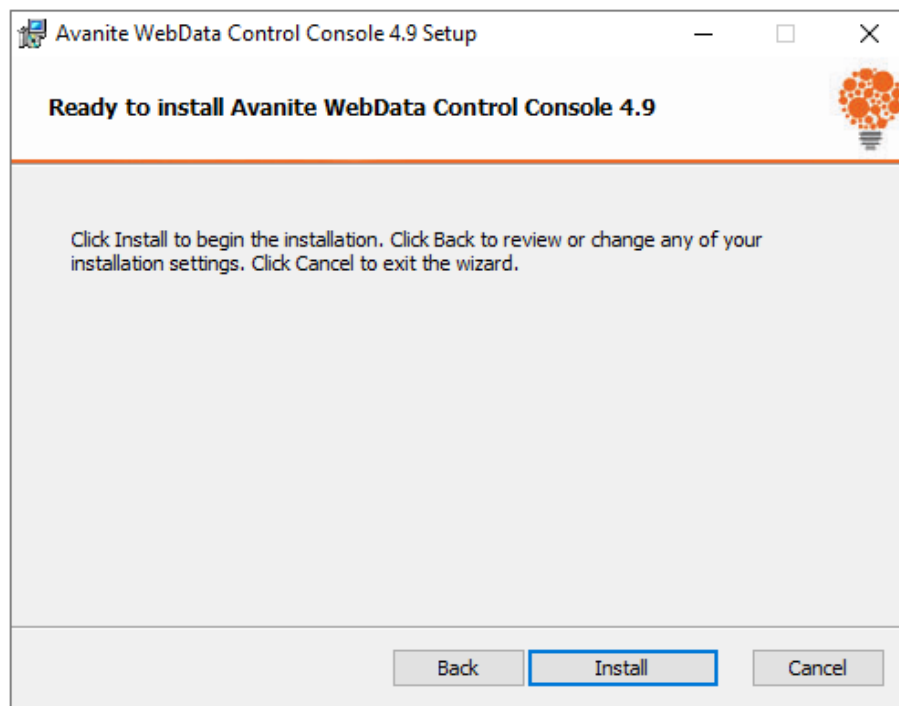


Figure 3 – Console Confirmation screen

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

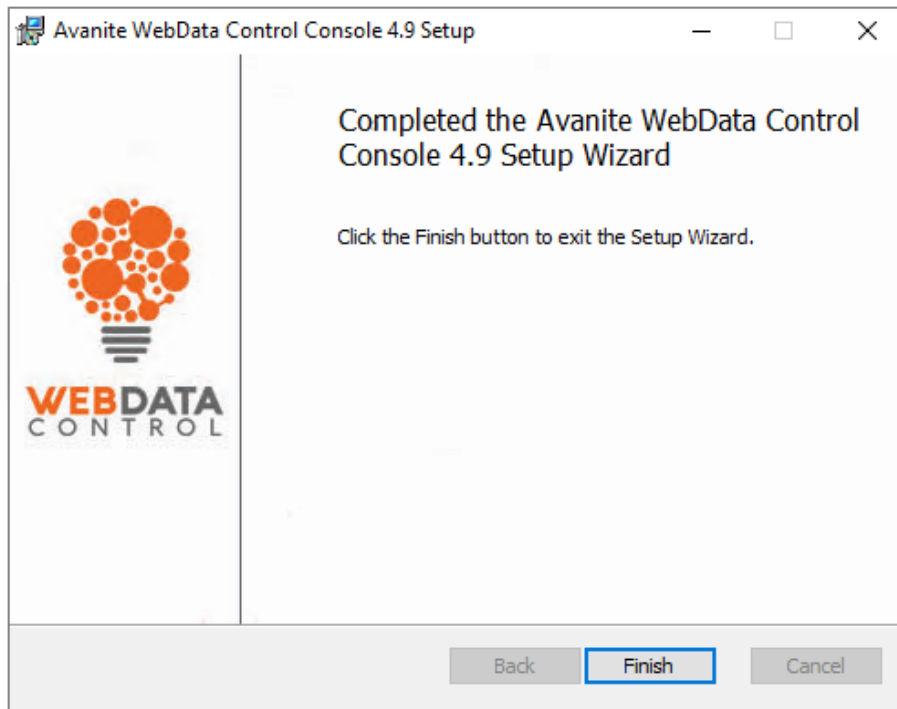


Figure 4 – Console Setup completion screen



WebData Control Agent

To use WebData Control the agent 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 the WebData Control agent is Microsoft .Net version 4.6 or greater. If not present, then the installation will prompt for the software and exit.

Manual Installation

To install the WebData Control agent, follow these steps:

1. As an administrator, run AvaWDC_x86.msi or AvaWDC_x64.msi depending on your system architecture. Click **Next** to continue the installation.

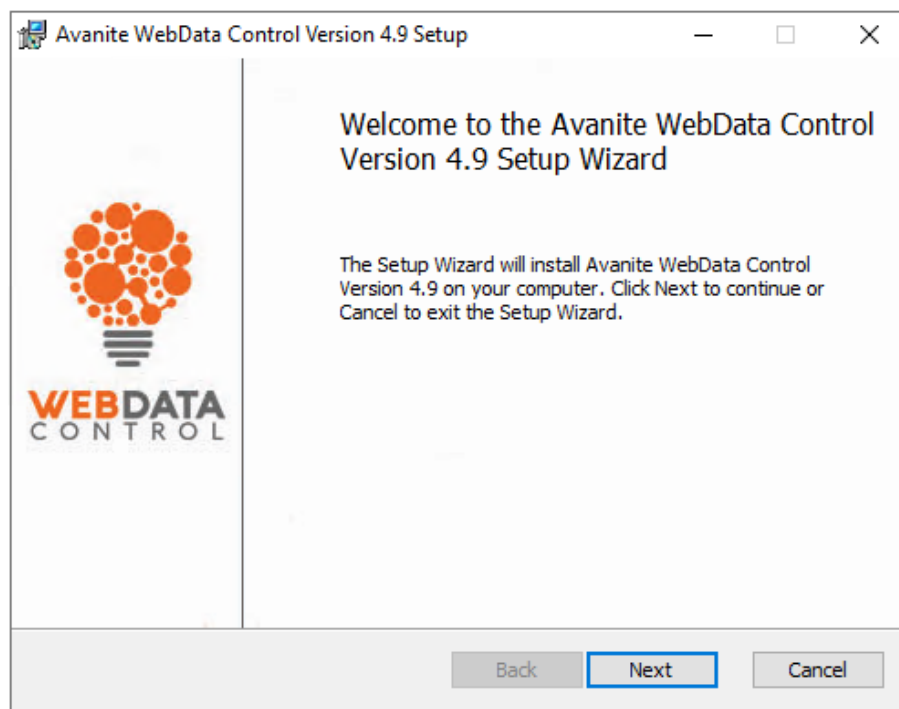


Figure 5 – Agent Welcome screen

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

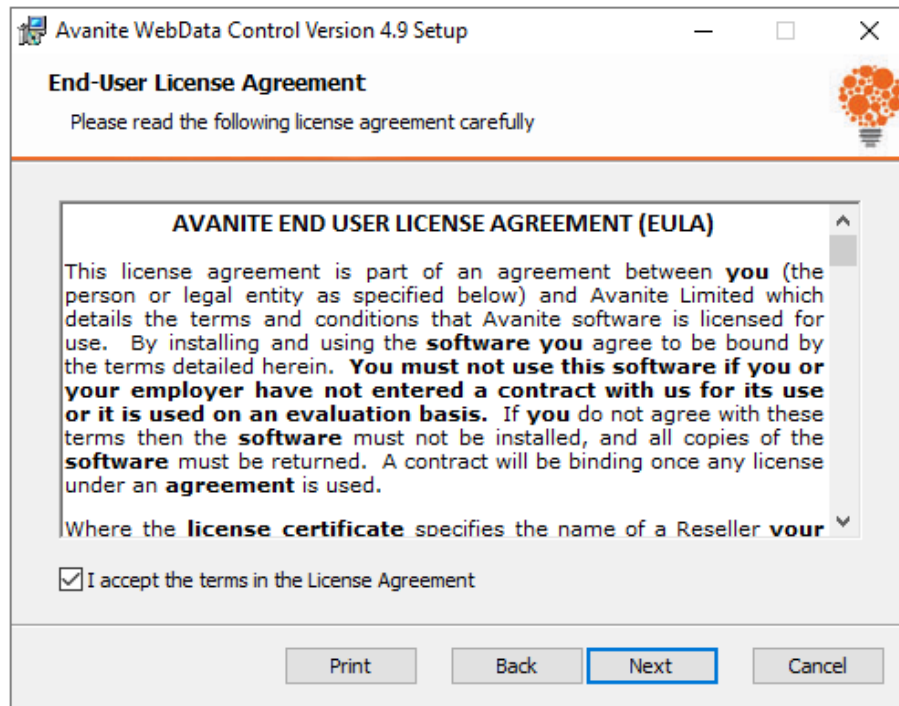


Figure 6 – Agent EULA Acceptance

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

By default, all WebData Control components are selected for installation and it is recommended this is not changed.

Click **Next** to continue.

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

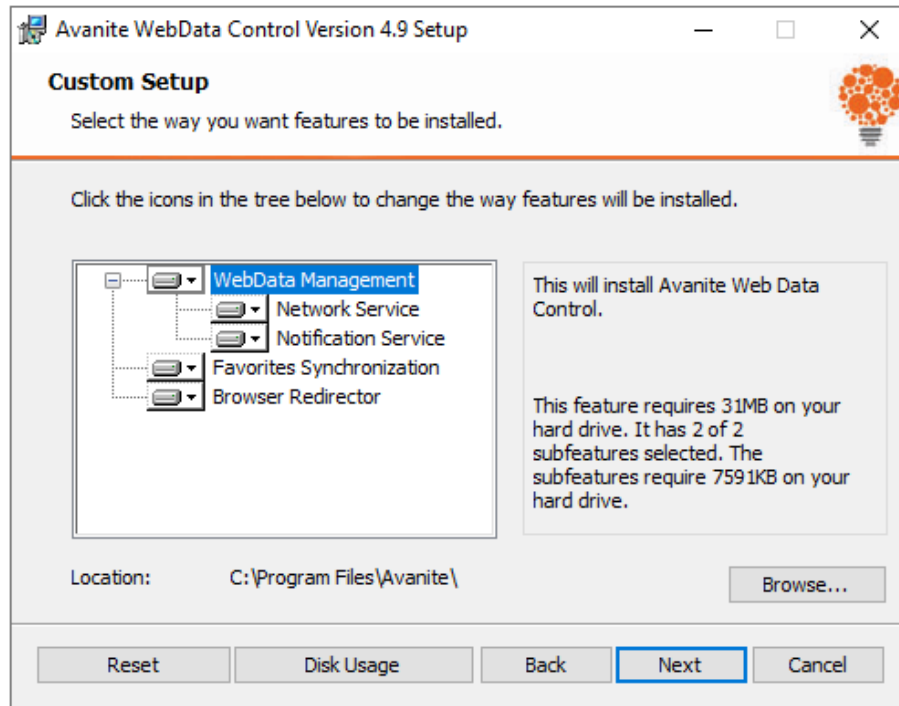


Figure 7 – Agent Custom Setup options

4. Click **Install**.

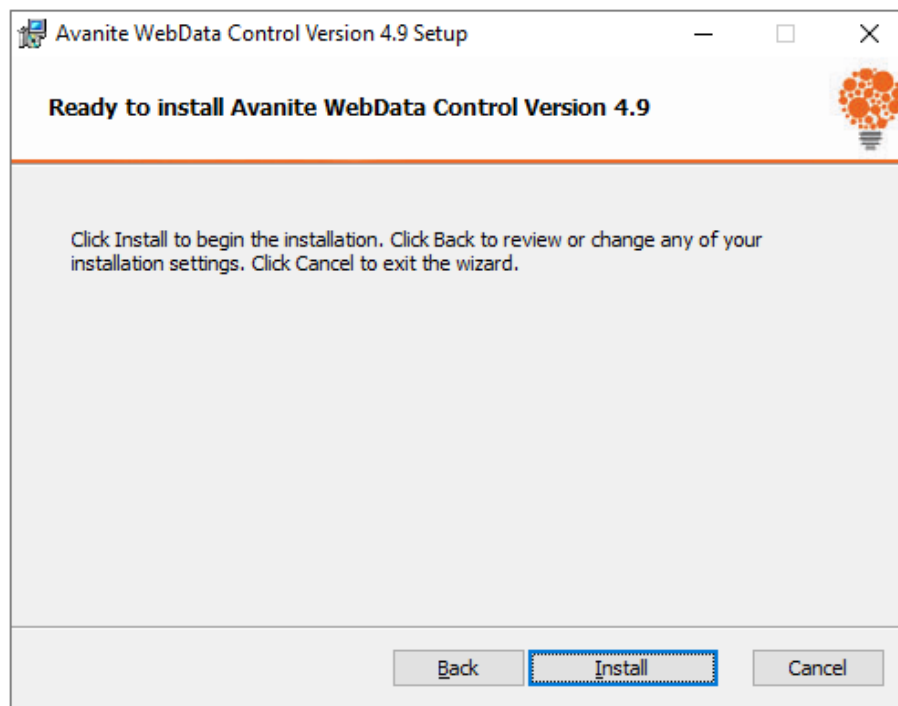


Figure 8 – Agent Confirmation screen



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

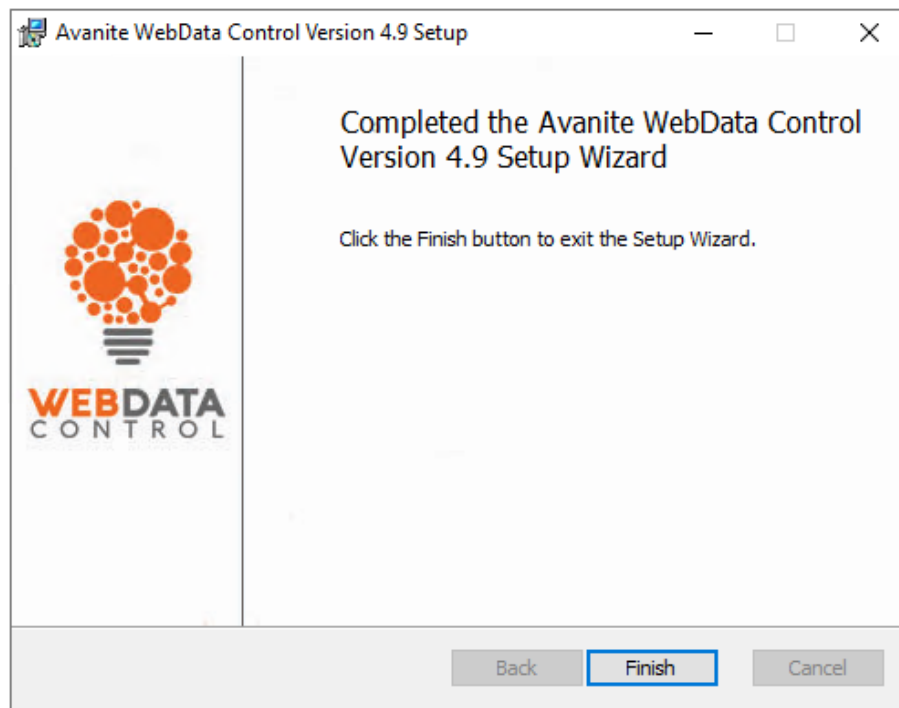


Figure 9 – Agent Setup completion screen

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 in the default installation directory:

```
MSIEXEC /qn /i <PathToMSI> /l*v <PathToLogFile>
```

<PathToMSI> needs to be updated to reference the location of the relevant installer MSI file
eg. C:\Install\Avanite\AvaWDC_x64.msi

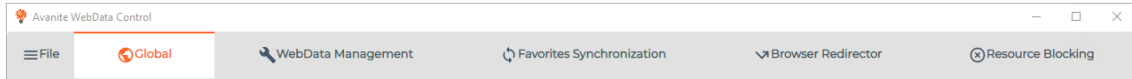
<PathToLogFile> needs to be updated to reference a path and filename to store the log file
eg. C:\Windows\Logs\Install.log



Configuring WebData Control

Console Layout and Navigation

The WebData Control Console has several different Menu's which can be used to create and save configurations.



File Menu

The File Menu provides options for managing configurations and includes options to create new, open existing and save.

- New – creates a new configuration.
- Open – opens an existing configuration file (.ava or .msi format).
- Save – saves the current open configuration to the same location it was opened from.
- Save As – saves the current configuration to a new file (.ava or .msi format).

Global Settings

The Global Tab allows for the following settings to be defined;

- Licenses
- Logging
- Event Logging
- Notifications

Licenses

This setting allows the WebData Control License to be distributed and must be configured.

In the Settings > Licenses field, enter the Avanite provided License key. Multiple License keys can be added if required.

Without a License, WebData Control will not function.

Note: Multiple licenses can be added if required.

A license key can be acquired by contacting support@avanite.com.



Logging

Logging

☐ Enable Diagnostic Logging

Path:

☐ Enable Debug Logging

Enabling this setting will enable logging by the WebData Control Agent.

It is recommended that Logging is enabled only when required.

When **Enable Diagnostic Logging** is selected you must 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.

When **Enable Debug Logging** is selected the log files will be encrypted and will only be readable by Avanite Support.

Event Logging

Event Logging

☐ Enable WebData Management Event Logging

☐ Enable Browser Redirector Event Logging

☐ Enable Favorites Synchronization Event Logging

WebData Control 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: **Enable WebData Management Event Logging**.

Events will be raised for Cookies, History, Browser Databases, Extensions and Extension Locales.

To generate events for the Browser Redirector feature, select the option: **Enable Browser Redirector Event Logging**.

Events will be raised when a URL redirection occurs.

To generate events for the Favorites Synchronization feature, select the option: **Enable Favorites Synchronization Event Logging**.

Events will be raised for creation of Default favorites and synchronization of user favorites.

For details of the events generated see Appendix C.



Toast Notifications

Toast Notifications

- ☐ Enable WebData Management Toast Notifications
- ☐ Enable Browser Redirector Toast Notifications
- ☐ Enable Favorites Synchronization Toast Notifications
- ☐ Custom Title for Toast Notifications
- ☐ Custom Icon for Toast Notifications (128x128 pixels)

No image file selected

This setting configures the features within WebData Control to display toast notifications to report on the various events that have occurred.

To enable notifications for the WebData Management feature, select the option: **Enable WebData Management Toast Notifications**.

To enable notifications for the Browser Redirector feature, select the option: **Enable Browser Redirector Toast Notifications**.

To enable notifications for the Favorites Synchronization feature, select the option: **Enable Favorites Synchronization Toast Notifications**.

Notifications can also be customized with a custom title and icon.

To enable a custom title for the Notifications select the option: **Custom Title for Toast Notifications**, and enter a new Title to be displayed.

To specify a custom icon select the option: **Custom Icon for Toast Notifications** and use the **Select Custom Toast Notification** button to provide a 128x128 .jpg to be used for the icon.

WebData Management Settings

WebData Management

WebData Management

- ☐ Enable WebData Management
 - ☐ WebData Management: Is Admin Condition
 - ☐ WebData Management: User Group Condition
- ☐ Disable WebData Management execution during logoff
- ☐ Google Chrome clean up on exit
- ☐ Microsoft Edge Chromium clean up on exit
- ☐ Mozilla Firefox clean up on exit
- ☐ Application Group Support



The options here relate to whether the WebData Management feature is enabled and how the WebData Control Agent behaves.

WebData Management Is Admin Condition

This setting is used to restrict the execution of WebData Management to non-administrative users.

Enabling this setting will stop the execution of WebData Management for users that are members of the Administrators group.

Note: *When WebData Management is enabled, by default it is enabled for all users.*

WebData Management User Group Condition

This setting is used to restrict the execution of WebData Management for users based on their Active Directory group membership.

Enabling this setting 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

Disable WebData Management execution during logoff

This setting allows WebData Management to be executed using a third-party application such as Ivanti Environment Manager.

If this setting is not configured, or set to Disabled, then WebData Management can be instigated via a third-party mechanism as required.

Google Chrome clean up on exit, Microsoft Edge Chromium clean up on exit, and Mozilla Firefox clean up on exit

By default, WebData Management executes at user log off, for all browsers. These options allow Firefox, Chrome, and Edge Chromium to perform data removal as device users exit these browsers.

Application Group Support



This setting changes the behavior of the Firefox, Chrome and Edge Chromium processing to be compatible with Ivanti Environment Manager Application Groups. When using Non Virtualized Application Groups (NVAG) to manage these browsers, this setting should be enabled.

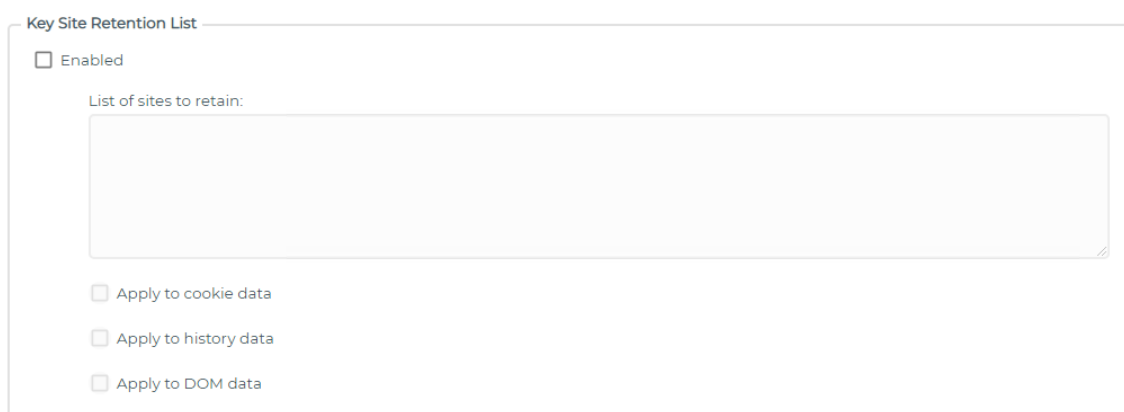
Advanced

AUTOMATIC UPDATES



Selecting the Automatic Updates for WebData Management option will instruct the WebData Control agent to download the latest cookie definition files from Avanite's Azure hosted Content Delivery Network (CDN).

KEY SITE RETENTION LIST



This setting allows you to specify sites where associated browsing data is retained. The setting will override any other settings you may have in place for all browser types except for those specified in the Key Site Purge List setting.

It is recommended that this setting 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.

To add sites to this setting specify the particular URLs 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:

Avanite.com/software

Retains data related to Avanite.com/software pages

Enable the **Apply to cookie data** option to retain all cookie data for sites matching the defined URL.



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.

Note: 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 PURGE LIST

Key Site Purge List

☐ Enabled

List of sites to remove:

☐ Apply to cookie data

☐ Apply to history data

☐ Apply to DOM data

This setting allows you to specify sites where associated browsing data is removed. The setting overrides any other settings you may have in place for all browser types without exception.

It is recommended that this setting is enabled only when required.

To add sites to this setting specify the particular URLs 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:

Avanite.com/software

Removes data related to Avanite.com/software pages

Enable the **Apply to cookie data** option to remove all cookie data for sites matching the defined URL.

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.



Note: 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.

LOGOFF SETTINGS

The screenshot shows a configuration panel titled "Logoff Settings". It contains a checkbox labeled "Enable Logoff Message" which is currently unchecked. Below the checkbox is a text input field labeled "Custom Logoff Message:".

This setting defines the logoff message for WebData Management.

When enabled, the **Enable Logoff Message** setting 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 no message is displayed during log off. The default Windows notifications are displayed.

Default Configuration

WEBDATA MANAGEMENT DEFAULT CONFIGURATION SETTINGS

The screenshot shows a configuration panel titled "WebData Management Default Configuration Settings". It contains a single orange button labeled "Enable Default Configuration Settings".

The WebData Management Default Configuration Settings automatically selects settings within the WebData Control console. The **Enable Default Configuration Settings** button can be used to quickly apply recommended settings to the basic configuration of WebData Management. The recommended settings will be applied in the WebData Management settings tabs in the Console.

For more details on the default WebData Management configuration see Appendix E.

Individual Browser Settings

Each of the **Google Chrome**, **Internet Explorer**, **Microsoft Edge**, **Microsoft Edge (Chromium)**, and **Mozilla Firefox** browsers have their own tabs for configuration of WebData Management policies specific to that particular browser. Each browser has similar settings with others only being applicable of specific browsers.



COOKIE SETTINGS

Cookie Settings

Not Configured

Days: 7

☐ Remove Expired Cookies

☐ Retain Only Secure Cookies

☐ Retain only HTTP Only Cookies

☐ Remove Third Party Cookies

These settings relate to how WebData Management handles cookies and are the same across all browsers.

The dropdown menu relates to the cookie retention setting and can be set various states and defaults to **Not Configured**:

To remove all cookie related 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 Calendar Days**, and specify a number of days.

To allow cookies to be retained for a specified number of active browsing days, select the option: **Retain Browsing Days**, and specify a number of days.

Note: This setting retains history data for the number of days selected where browsing activity has occurred. This excludes any days of inactivity.

In addition to the dropdown list, there are several checkboxes that can be applied:

To remove cookies that have expired, select 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 HTTP Only cookies**.

To remove third party cookies, enable the option: **Remove Third Party Cookies**.

For more details on cookies see Appendix A.

COOKIE REMOVAL BY TYPE

Cookie Removal by Type

☐ Remove known Advertising, Analytics and Tracking Cookies

Additional Cookie Types to Remove:



Enabling this setting 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, Analytics and Tracking Cookies**

Note: The WebData Control agent includes a pre-defined list of known advertising, analytics 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**.

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.

HISTORY SETTINGS

These settings relate to how WebData Management handles browsing history and are the same across all browsers.

The dropdown menu relates to the browsing history retention setting and can be set various states and defaults to **Not Configured**.

To remove all history-related data for the user, enable the option: **Clear All History**.

To allow for history to be retained for a specific number of days, enable the option: **Retain Calendar Days**.

To allow history data to be retained for a specified number of active browsing days, enable the option: **Retain Browsing Days**.

Note: This setting retains browsing history data for the number of days selected where browsing activity has occurred. This excludes any days of inactivity.



DATA REPORTING

The 'Data Reporting' settings panel contains the following elements:

- A checkbox labeled 'Enable Data Reporting'.
- A text input field labeled 'Path:'.
- A checkbox labeled 'Anonymize the exported data'.

When enabled, the **Enable Data Reporting** setting generates data exports of the WebData Management activity. 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. See Appendix D for details of the report format.

When enabled a folder path is required to specify the report location.

Example:

C:\Temp

To remove user references from the exported data, enable the option: **Anonymize the exported data**.

EXTENSION SETTINGS (GOOGLE CHROME AND MICROSOFT EDGE CHROMIUM ONLY)

The 'Extension Settings' panel contains the following elements:

- A dropdown menu labeled 'Extension Removal:' with the value 'Not Configured'.
- A text area labeled 'List of Extension:'.
- A checkbox labeled 'Enable Extension Locale Removal'.
- A text area labeled 'List of Extension Locales to Retain:'.

These settings manage specific browser extensions, removing them according to the options selected.

To explicitly remove all extensions listed, enable the option: **Extensions to be removed**.

To explicitly retain specific extensions, enable the option: **Extensions to be retained**.

To remove all 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 whose name start with Avanite.

Locale data may be present for each browser extension with locale information being present for each supported language.

When enabled, the **Enable Extension Locale Removal** setting manages locale data installed as part of any extensions.

The list specified is used for an exact text match (case insensitive). Wildcards are also supported.

Example:

en* retains all locales that contain en

In addition, the default locale for the extension and the user session will always be retained.

OTHER SETTINGS (INTERNET EXPLORER AND MICROSOFT EDGE ONLY)

Other Settings

DOM Settings Not Configured

Temporary Settings Not Configured

☐ Enterprise Mode Data Removal

☐ Compatibility Data Removal

When enabled, the **DOM Settings** setting removes 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 references to DOM data in the webcache database and all DOM data from the file system, enable the option: **Delete all files**.
- To remove references to 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**.

For more information, see Appendix B.

When enabled, the **Temporary Settings** setting removes temporary internet files data. The recommended setting for this setting 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 temporary internet files data from the file system enable the option: **Delete all files**.
- To remove references to 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**.

When enabled, the **Enterprise Mode Data Removal** setting removes any 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 article - <https://docs.microsoft.com/en-us/internet-explorer/ie11-deploy-guide/check-for-new-enterprise-mode-site-list-xml-file>.

When enabled, the **Compatibility Data Removal** setting removes related Compatibility data from the webcache database.

Compatibility mode data is updated dynamically by the browser and does not need to be retained.

OTHER SETTINGS (MICROSOFT EDGE CHROMIUM ONLY)

The screenshot shows the 'Other Settings' section of the Microsoft Edge Chromium settings. It contains three checkboxes: 'DOM Settings', 'Enterprise Mode Data Removal', and 'Temporary Settings'. All three checkboxes are currently unchecked.

When enabled, the **DOM Settings** setting removes 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.

When enabled, the **Temporary Settings** setting removes Edge Chromium temporary internet data.

For more information on DOM/Temporary Settings, see Appendix B.

When enabled, the **Enterprise Mode Data Removal** setting removes any Edge Chromium related Enterprise Mode data. 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 article - <https://docs.microsoft.com/en-us/internet-explorer/ie11-deploy-guide/check-for-new-enterprise-mode-site-list-xml-file>.

OTHER SETTINGS (GOOGLE CHROME AND MOZILLA FIREFOX ONLY)



When enabled, the **DOM Settings** setting removes 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.

When enabled, the **Temporary Settings** setting removes Edge Chromium temporary internet data.

For more information on DOM/Temporary Settings, see Appendix B.

Windows Store Apps

This setting 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.

When this setting is **Enabled**, the WebData Control Agent will remove all Windows Store Application data.

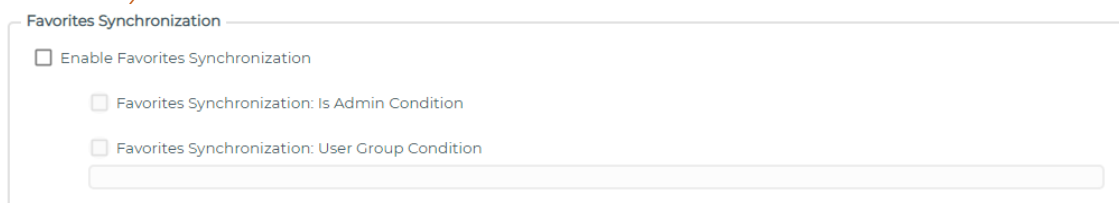
The **Windows Store Apps to Exclude** option allow the retention of data for Windows Store applications. Specify the data to be kept by defining the application name to match.

Example:

Microsoft.Office.OneNote

Favorites Synchronization Settings

Favorites Synchronization





The options here relate to whether the Favorites Synchronization feature is enabled and how the WebData Control Agent behaves.

Favorites Synchronization Is Admin Condition

This setting is used to restrict the execution of Favorites Synchronization to non-administrative users.

Enabling this setting will stop the execution of Favorites Synchronization for users that are members of the Administrators group.

Note: *When Favorites Synchronization is enabled, by default it is enabled for all users.*

Favorites Synchronization User Group Condition

This setting is used to restrict the execution of Favorites Synchronization for users based on their Active Directory group membership.

Enabling this setting 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

Global Settings

SYNCHRONIZE FAVORITES BETWEEN THE FOLLOWING BROWSERS

Synchronize Favorites Between the Following Browsers

- ☐ Google Chrome
- ☐ Internet Explorer
- ☐ Microsoft Edge Chromium
- ☐ Mozilla Firefox

This setting defines which browsers will be enabled for synchronization of Favorites.

Selecting a browser will enable it for synchronization and browser bookmarks/favorites will be shared between browsers that have been enabled.



Note: Multiple browsers need to be selected for this setting to have any effect.

GENERAL SETTINGS

General Settings
☐ Force Internet Explorer to Close
☐ Alternative Storage Folder
 Path:
☐ Read Only Mode

It is recommended that the **Force Internet Explorer to Close** setting is enabled to ensure Favorites are synchronized in a timely manner.

By default, within Internet Explorer, the iexplore.exe process remains running 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 setting adds the following registry values for each user session:

HKCU\Software\Microsoft\Internet Explorer\Main

TabShutdownDelay=dword: 00000000

HKCU\Software\Wow6432Node\Microsoft\Internet Explorer\Main

TabShutdownDelay=dword: 00000000

The relevant keys are added based on system architecture.

When enabled, the **Alternative Storage Folder** setting 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 icons from each browser 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 specified.

When enabled, the **Read Only Mode** setting defines whether Favorites Synchronization operates in read-only mode.



In read-only mode, device user Favorites are not synchronized between browsers, but the file and database which holds device user Favorites data are still populated. This can be used for migration purposes if required.

To allow the collection of device user Favorites data requires one or more browsers to be selected within the ***Synchronize Favorites between the following Browsers*** setting.

<BROWSER> DEFAULT FAVORITES

Each of the **Google Chrome, Internet Explorer, Microsoft Edge (Chromium)** and **Mozilla Firefox** browsers have their own tabs for configuration of Default Favorites specific to that particular browser. Each browser has the same options.

For Example, for **Google Chrome**:

<input type="checkbox"/>	Favorite Name	URL
No favorite entries found for Google Chrome		

<< < > >> Page 0 of 0 Show 10

Add Edit Delete [Rows Selected: 0]

The table can be used to add Default Favorites which will be provisioned to the appropriate browser on launch and de-provisioned on the exit of the browser.

To add an entry click the **Add** button which will prompt for an input as follows:



Favorites Synchronization

Add Name

Example Favorite\Example

Add URL

https://www.example.com/

Save

Cancel

Example:

Name: Avanite

URL: https://www.avanite.com/

This would create a shortcut called Avanite pointing to https://www.avanite.com/

When a default Favorite is created it is automatically excluded from synchronization to other browsers.

Note, a default Favorite can be added to a folder by including it as part of the *Value Name*.

Example:

Name: Avanite Favorites\Avanite Home Page

This would create the folder Avanite Favorites with a bookmark named Avanite Home Page.

To list the Favorite within the Other Bookmarks folder, begin the value name with other\.

Example:

Name: other\Avanite Favorites\Avanite Home Page

This would create the folder Avanite Favorites with a bookmark named Avanite Home Page. under the Other Bookmarks section within Chrome.

If other\ is not specified then the Favorite will be placed on the toolbar.

Entries can be added, removed and edited via the Table controls.



Browser Redirector Settings

Browser Redirector

The options here relate to whether the Browser Redirector feature is enabled and how the WebData Control Agent behaves.

Browser Redirector Is Admin Condition

This setting is used to restrict the execution of Browser Redirector to non-administrative users.

Enabling this setting will stop the execution of Browser Redirector for users that are members of the Administrators group.

Note: When Browser Redirector is enabled, by default it is enabled for all users.

Browser Redirector User Group Condition

This setting is used to restrict the execution of Browser Redirector for users based on their Active Directory group membership.

Enabling this setting 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 ;

Example:

Avanite \ User Group 1

Avanite \ User Group 1;Avanite \ User Group 2

Disable Automatic Installation of Extensions



By default, the WebData Control Agent will install the Browser Redirector browser extensions when the Browser Redirector feature is enabled for a user. Selecting this option disables the automatic installation of the Browser Redirector browser extensions.

Note: *Without the Browser Redirector extensions in-browser redirection will not work. Extensions can be manually or policy installed if required.*

For details of how to install extensions manually, please contact Avanite Support for guidance.

Disable Automatic Removal of Extensions During Logoff

By default, the Browser Manager Agent will remove the Browser Redirector browser extensions during logoff of a user session. Selecting this option disables the automatic removal of the Browser Redirector browser extensions.

Default and Launch Settings

DEFAULT BROWSER

Default Browser

☐ Specify Default Browser

Browser: Not Configured

☐ Enforce Administrator Defined Browser

☐ Enable User Defined Default Browser

When enabled, the **Specify Default Browser** setting 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 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 this option will force Browser Redirector to always use this browser unless a redirection match is found.

When enabled, the **Enable User Defined Default Browser** setting 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.



DEFAULT FAVORITES TO REDIRECT

Default Favorites to Redirect

☐ Enable Default Favorites to Redirect

☐ Google Chrome Favorites

☐ Internet Explorer Favorites

☐ Microsoft Edge Chromium Favorites

☐ Mozilla Firefox Favorites

When enabled, the **Enable Default Favorites to Redirect** setting 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.

BROWSER LAUNCH PARAMETERS

Browser Launch Parameters

☐ Enable Google Chrome Launch Parameters
Google Chrome Parameter List

☐ Enable Internet Explorer Launch Parameters
Internet Explorer Parameter List

☐ Enable Microsoft Edge Chromium Launch Parameters
Microsoft Edge Chromium Parameter List

☐ Enable Mozilla Firefox Launch Parameters
Mozilla Firefox Parameter List

These settings allow a set of pre-determined parameters to be specified which will be applied to browsers launched by Browser Redirector.

To apply launch parameters for Google Chrome select: **Enable Google Chrome Launch Parameters** option, and enter the parameters in the text box.

Example:

--disable-sync

To apply launch parameters for Internet Explorer select: **Enable Internet Explorer Launch Parameters** option, and enter the parameters in the text box.

Example:



-k

To apply launch parameters for Microsoft Edge Chromium select: **Enable Microsoft Edge Chromium Launch Parameters** option, and enter the parameters in the text box.

Example:

--disable-notifications

To apply launch parameters for Mozilla Firefox select: **Enable Mozilla Firefox Launch Parameters** option, and enter the parameters in the text box.

Example:

-foreground

OTHER SETTINGS

Other Settings

☐ Internet Explorer Enhanced Protected Mode Support

Selecting the option: **Internet Explorer Enhanced Protected Mode Support** allows Browser Redirector to support Internet Explorer's Enhanced Protected Mode. When this setting is enabled an Enhanced Protected Mode Browser Helper Object (BHO) is used.

URLs to Redirect

URLs to Redirect

<input type="checkbox"/>	URL	Google ...	Microso...	Mozilla ...	Internet...	Internet...	Alternat...
No URL entries found							

<< < > >>

Page 0 of 0

Show 10 ▾

Add Edit Delete

[Rows Selected: 0]



The **URLs to Redirect** table can be used to add URLs that will be redirected to the selected browser or external process.

To add an entry click the **Add** button which will prompt for an input as follows:

Browser Redirector

URL

Browser

☐ Google Chrome ☐ Microsoft Edge Chromium ☐ Mozilla Firefox ☐ Internet Explorer

☐ Internet Explorer (New Window) ☐ Alternative Process

Path for Alternative Process

Notes

URLs can be added and a selection can be made as to where to redirect to. Browser Redirector will intercept URLs being launched via links and from inside each Browser. The rule will be honored as entered here.

To ensure the best match, when you specify a URL enter the path to the web resource as fully as possible.

Example entries:

https://www.website.com

http://www.website.com

website.com

website.com/page

To redirect the specified URL to:

- Google Chrome select the **Google Chrome** option.
- Microsoft Edge Chromium select the **Microsoft Edge Chromium** option.
- Mozilla Firefox select the **Mozilla Firefox** option.
- Internet Explorer select the **Internet Explorer** option.
- A new instance of Internet Explorer select the **Internet Explorer (New Window)** option.
- An Alternative process select the **Alternative Process** option, then enter the command line for the process in the Path for Alternative Process field.

For each entry that is added notes can be stored for future reference as needed.



Resource Blocking Settings

Resource Blocking

The options here relate to whether the Resource Blocking feature is enabled and how the WebData Control Agent behaves.

Resource Blocking Is Admin Condition

This setting is used to restrict the execution of Resource Blocking to non-administrative users.

Enabling this setting will stop the execution of Resource Blocking for users that are members of the Administrators group.

Note: When Resource Blocking is enabled, by default it is enabled for all users.

Resource Blocking User Group Condition

This setting is used to restrict the execution of Resource Blocking for users based on their Active Directory group membership.

Enabling this setting will ensure that Resource Blocking 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 ;

Example:

Avanite\User Group 1

Avanite\User Group 1;Avanite\User Group 2

Disable Automatic Installation of Extensions



By default, the WebData Control Agent will install the Resource Blocking browser extensions when the Resource Blocking feature is enabled for a user. Selecting this option disables the automatic installation of the Resource Blocking browser extensions.

Note: *Without the Resource Blocking extensions in-browser redirection and Resource Blocking will not work. Extensions can be manually or policy installed if required.*

For details of how to install extensions manually, please contact Avanite Support for guidance.

Disable Automatic Removal of Extensions During Logoff

By default, the Browser Manager Agent will remove the Resource Blocking browser extensions during logoff of a user session. Selecting this option disables the automatic removal of the Resource Blocking browser extensions.

Ad Blocking

Ad Blocking

☐ Enable Automatic Updates for Resource Blocking

Selecting the **Enable Automatic Updates for Resource Blocking** option will instruct the WebData Control agent to download the latest Ad Blocking definition files from Avanite's Azure hosted Content Delivery Network (CDN).

Configuration Deployment

Once a configuration has been created via the WebData Control Console it can be saved as an .ava or .msi based configuration file which can be used to provide the configuration to the WebData Control Agent.

The installation of an .msi based configuration can also be done using an existing Software Deployment solution, such as Microsoft System Center Configuration Manager (SCCM). The .msi file will install the configuration to the C:\ProgramData\Avanite\WebData Control folder as a configuration.ava file where the WebData Control Agent will use it from.

Configurations can also be saved as .ava files. Saving the configuration as a configuration.ava file, and distributing this file to each endpoint where the WebData Control Agent is installed, is also an option. Copy the configuration.ava file to the C:\ProgramData\Avanite\WebData Control folder.

When the configuration.ava file is changed the WebData Control Agent will automatically update to use the new configuration the next time a user logs on to the endpoint.



Other Considerations

Microsoft Edge Chromium Startup Boost

The Microsoft Edge Chromium browser (version 88 or above) may use a feature called Startup Boost which can cause issues with WebData Management and Favorites Synchronization features of WebData Control as the browser runs continuously.

It is recommended that the Startup Boost feature is disabled which can be done by configuring the following Group Policy:

Policy:

Computer\Microsoft Edge\Performance

Setting:

Enable startup boost: Disabled

Further details on the Startup Boost feature can be found here -

<https://techcommunity.microsoft.com/t5/articles/startup-boost-faq/m-p/1810423>.

Microsoft IEtoEdge BHO

The Microsoft Edge Chromium browser installs an IEtoEdge Browser Helper Object (BHO) in Internet Explorer when installed and this can cause issues with the WebData Control Browser Redirector feature.

To disable the IEtoEdge BHO alter the following registry setting:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Ext\CLSID

{1FD49718-1D00-4B19-AF5F-070AF6D5D54C}=reg_sz: 0



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 – Event Details

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



Appendix D – 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:

<i>Field Name</i>	<i>Description</i>
<i>Version</i>	Defines a version number for the schema of the data
<i>Data Type</i>	Defines the entry as a cookie item
<i>Browser</i>	Defines which Browser the data was reported from
<i>Time Stamp</i>	Date and Time stamp of when the entry was written
<i>User</i>	Defines the user to which the data applies
<i>Domain</i>	Defines the domain of the user
<i>Machine</i>	Defines the machine on which the data was generated
<i>Action</i>	Defines what action was taken by WebData Control as the data was processed. Valid actions are: <ul style="list-style-type: none">• Remaining• Removed• RemovedType• Removed3rdParty• OrphanedInDB• Expired
<i>Base URL</i>	Defines the complete URL of the website
<i>Processed URL</i>	Defines the URL which was processed by WebData Control
<i>Type</i>	Defines the cookie type for the entry
<i>Secured</i>	Defines whether the entry was from a secure website (true/false)
<i>Last Accessed Date</i>	Defines the last access date for the entry
<i>Modified Date</i>	Defines the last modified date for the entry
<i>Expiry Date</i>	Defines the expiry date for the entry



History Report Format

The History report contains the following data fields:

<i>Field Name</i>	<i>Description</i>
<i>Version</i>	Defines a version number for the schema of the data
<i>Data Type</i>	Defines the entry as a history item
<i>Browser</i>	Defines which Browser the data was reported from
<i>Time Stamp</i>	Date and Time stamp of when the entry was written
<i>User</i>	Defines the user to which the data applies
<i>Domain</i>	Defines the domain of the user
<i>Machine</i>	Defines the machine on which the data was generated
<i>Action</i>	Defines what action was taken by WebData Control as the data was processed. Valid actions are: <ul style="list-style-type: none">• Remaining• Removed
<i>Base URL</i>	Defines the complete URL of the website
<i>Processed URL</i>	Defines the URL which was processed by WebData Control
<i>Secured</i>	Defines whether the entry was from a secure website (true/false)
<i>Last Accessed Date</i>	Defines the last access date for the entry
<i>Modified Date</i>	Defines the last modified date for the entry
<i>Expiry Date</i>	Defines the expiry date for the entry



Appendix E – Default Configuration

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

<i>Setting</i>	<i>Description</i>
<i>Google Chrome</i>	Cookie Settings: Retain Calendar Days: 7 Remove Expired Cookies: Enabled Remove Third Party Cookies: Enabled Cookie Removal by Type Settings: Remove Known Advertising, Analytics and Tracking Cookies: Enabled History Settings: Retain Calendar Days: 7 Other Settings: DOM Settings: Enabled Temporary Settings: Enabled
<i>Internet Explorer</i>	Cookie Settings: Retain Calendar Days: 7 Remove Expired Cookies: Enabled Remove Third Party Cookies: Enabled Cookie Removal by Type Settings: Remove Known Advertising, Analytics and Tracking Cookies: Enabled History Settings: Retain Calendar Days: 7 Other Settings: DOM Settings: Remove all files Temporary Settings: Remove all files Enterprise Mode Data Removal: Enabled Compatibility Data Removal: Enabled
<i>Microsoft Edge</i>	Cookie Settings: Retain Calendar Days: 7 Remove Expired Cookies: Enabled Remove Third Party Cookies: Enabled Cookie Removal by Type Settings: Remove Known Advertising, Analytics and Tracking Cookies: Enabled History Settings: Retain Calendar Days: 7 Other Settings:



	DOM Settings: Remove all files Temporary Settings: Remove all files Enterprise Mode Data Removal: Enabled Compatibility Data Removal: Enabled
<i>Edge Chromium</i>	Cookie Settings: Retain Calendar Days: 7 Remove Expired Cookies: Enabled Remove Third Party Cookies: Enabled Cookie Removal by Type Settings: Remove Known Advertising, Analytics and Tracking Cookies: Enabled History Settings: Retain Calendar Days: 7 Other Settings: DOM Settings: Enabled Temporary Settings: Enabled Enterprise Mode Data Removal: Enabled
<i>Mozilla Firefox</i>	Cookie Settings: Retain Calendar Days: 7 Remove Expired Cookies: Enabled Remove Third Party Cookies: Enabled Cookie Removal by Type Settings: Remove Known Advertising, Analytics and Tracking Cookies: Enabled History Settings: Retain Calendar Days: 7 Other Settings: DOM Settings: Enabled Temporary Settings: Enabled
<i>Windows Store Apps</i>	Windows Store Apps Data Removal: Enabled