

# Browsium Catalyst 2.0 Administration Guide

A large, dark purple square containing the white text "Ct" in a serif font.

Bonding Browsers to Business  
[www.browsium.com](http://www.browsium.com)



# Administration Guide

---

This guide has been created for IT administrators to assist in installing, configuring, and deploying Browsium Catalyst. This version of the guide is designed for use with Browsium Catalyst 2.0.1.

For more information about Browsium Catalyst, other Browsium products, or to contact Browsium Support, please visit [www.browsium.com](http://www.browsium.com).



# Table of Contents

---

1. Introduction.....	5
1.1. Browsium Catalyst Explained .....	6
1.2. Browsium Catalyst Configuration Manager and Client.....	7
2. Installation.....	9
2.1. Catalyst Components.....	10
2.2. Software Requirements.....	11
2.3. Installing the Browsium Catalyst Client.....	12
2.4. Installing Browsium Catalyst Configuration Manager.....	17
2.5. Available Command Line Switches for the Installer .....	20
2.5.1. Installation Options .....	20
2.5.2. Display Options.....	20
2.5.3. Restart Options .....	20
2.5.4. Logging Options.....	21
2.5.5. Repair Options.....	21
2.5.6. Command Line Installation Examples.....	22
2.6. Upgrading from Evaluation to Licensed Version.....	22
3. Catalyst Configuration Manager Overview.....	25
3.1. Menu Bar .....	26
3.2. The Settings Node .....	27
3.3. The Browsers Node.....	28
3.4. The Rules Node.....	30

4. Rule Basics.....	32
4.1. How to Create a Rule.....	33
4.2. How to Remove a Rule.....	39
5. Managing the Catalyst Client software.....	41
5.1. Managing the Catalyst Extension for Internet Explorer.....	42
5.1.1. Enable the Catalyst Add-on for Internet Explorer via Group Policy.....	42
5.1.2. Disable Internet Explorer's Default Browser Check via Group Policy and the local Registry .....	46
5.2. Managing the Catalyst Extension for Google Chrome.....	47
5.2.1. Enable the Catalyst Extension for Chrome via Group Policy.....	47
5.2.2. Disable Chrome's Default Browser Check via Group Policy.....	49
5.2.3. Disable 'Predict network actions' in Google Chrome .....	50
5.3. Managing the Catalyst Extension for Mozilla Firefox.....	52
5.3.1. Disable Firefox's Default Browser Check via Group Policy .....	52
5.4. Readyng Windows 8 for Catalyst .....	53
5.4.1. Set Catalyst as Default Browser for Project Development and Testing.....	54
5.4.2. Set Catalyst as Default Browser for Enterprise Deployment.....	57
6. Configuration Deployment to End User PCs.....	60
6.1. Deploying via Flat Files.....	62
6.2. Deploying via Serialized Registry Keys.....	64
6.2.1. A Few Words About ADMX.....	67
6.3. Query the Active Configuration with WhichConfig.....	67
A. Troubleshooting.....	70
A.1. Catalyst Rule Fails To Engage.....	70
A.2. Browser Window Doesn't Get Focus Automatically .....	71
A.3. Catalyst Doesn't Take Over Default Browser on Windows 8.....	71
A.4. The Controller Becomes Unresponsive.....	71



## *Section One*

# Introduction

---

In this section you will learn:

- ✓ What is Browsium Catalyst
- ✓ The components which make up Browsium Catalyst
- ✓ What to expect from Browsium Catalyst

# 1. Introduction

As a rule, the IT department is responsible for determining the standard desktop configuration and web browser for the organization. In the past, most IT groups opted to use Internet Explorer for its flexibility in management as well as IE having been included with Windows. As the web has evolved, pressures have been put on the IT group to offer more browser choice to their users. The challenge of offering choice was complicated by the need for IT to properly manage the alternate browser offerings.

Browsium Catalyst ("Catalyst") is designed to help IT organizations to address these challenges and offer a selection of browser choice to end users – all without losing management functionality. Catalyst provides the ability to deliver browser change and still ensure business process remains uninterrupted.

Catalyst is more than just about controlling browser behavior. Catalyst is designed to solve IT challenges around legacy web application compatibility issues, challenges around embracing emerging technologies and reducing support costs. Lastly, Catalyst provides the bridge needed for IT to address consumerization in the workplace.

## 1.1. Browsium Catalyst Explained

Browsium Catalyst is the first multi-browser redirection and management tool of its kind. Unlike other browser redirection engine solutions which have been designed and implemented as part of a vendor specific solution, Catalyst is platform and browser agnostic. By removing any reliance on a specific vendor technology, Catalyst enables an IT organization to be in complete control regardless of how they want to implement the solution.

Catalyst provides the ability to safely deploy multiple browsers to end users and still control which browser can be used for a given website or web application. In delivering this level of control, IT organizations finally have a toolset to enable browser choice. Now IT can deliver a multi-browser solution in a manner that makes sense for the organization. Business needs and end user choice are decoupled from web application contingencies, giving IT the flexibility to meet multi-browser requests with confidence.

Catalyst makes sense to the user since they have to do nothing special or different; the add-ons do all the switching automatically. The solution is seamless. The end user can focus on doing their work and avoiding problems or downtime.

Catalyst is controlled by a hierarchical system of Rules, defined using the Catalyst Configuration Manager. Understanding this system is the key to understanding Catalyst. The Configuration Manager provides tools to define criteria by which web applications are loaded in a desired browser. In addition to simply specifying a website to open in a given browser, Catalyst offers the ability to control the user experience when being redirected.

For example, some web applications not only need to be opened in a specific browser, but the application requirements are to open each link in a new session. Catalyst can do that with ease. If the requirement is to open content in a new tab, no problem. Catalyst can even block requests entirely, helping provide an extra layer of immediate protection when a security advisory is issued for an exploit on a given browser.

Catalyst is designed to keep users where IT wants them to go – while not getting in the way when IT hasn't set a policy for a given location. Catalyst enables IT administrators to ensure the right browser is used for the right application, but undefined applications can be accessed with the browser of choice for the user.

Catalyst is built on an opt-in basis. In other words, Catalyst intervenes when – and only when – it is instructed to act.

## 1.2. Browsium Catalyst Configuration Manager and Client

The Catalyst Configuration Manager is the main interaction point for IT administrators using Catalyst. Catalyst has been designed to work in a traditional IT setting and deploy using existing technology systems in use at your organization.

The basic design of the Catalyst Configuration Manager is such that it easily matches the architecture and needs of your organization. Using a distributed solutions approach, web application owners, business units or the IT organization can use the Catalyst Configuration Manager to create Rules and configurations for their specific needs; alternatively, a single administrator can manage all the Rules, and Settings.

The Catalyst Client includes extensions for three browsers – the installed version of Internet Explorer, Google Chrome 22 (or later) and Firefox 15 (or later). Catalyst also supports the ability to define and configure additional custom browsers – either additional versions of Chrome or Firefox, or an arbitrary browser to set as a target for redirection. Once the Catalyst Client has been installed on a system, the Catalyst Controller process will load at user logon and read the configuration from the system.

Catalyst supports both local and Group Policy managed settings to provide the most flexibility and truly deliver an enterprise-ready solution. Once the configuration is loaded, the browser extensions monitor the navigation process for each browser and communicate with the Controller to ensure the correct Rule is followed and the appropriate browser is invoked.





*Section Two*

# Installation

---

In this section you will learn:

- ✓ About the Browsium Catalyst components
- ✓ Software requirements for Browsium Catalyst
- ✓ How to install Browsium Catalyst

## 2. Installation

It's easy to install Browsium Catalyst – the software includes two simple MSI packages containing the Catalyst Configuration Manager and the Catalyst Client. Administrators need both the Browsium Catalyst Configuration Manager and the Catalyst Client. End users only require the Catalyst Client.

Administrator credentials are required to install Browsium Catalyst, but everything will run using standard user permissions so system access remains tightly control and secure. This section provides details on the specific components of Catalyst.

## 2.1. Catalyst Components

The Catalyst system is comprised of two main parts, an administrative interface for defining Rules and configurations, browser client add-ons for Microsoft Internet Explorer, Google Chrome and Mozilla Firefox.

- **Catalyst Administration Tools (Catalyst-AdminSetup.exe)**

This application allows for the management and configuration of Catalyst settings for users and PCs. This application is not meant for end users so this package should not be installed broadly – installation of this package should be limited to System Administrators and Web Application/Business Unit owners.

- **Catalyst Configuration Manager**

The Catalyst Configuration Manager (**ManagerUI.exe**) is the single management interface for the Catalyst system. This application provides the central point for creating, configuring and managing Projects, Settings, Browsers and Rules.

- **Catalyst Client (Catalyst-ClientSetup.msi)**

The Catalyst Client is responsible for loading Catalyst configuration data and redirecting browser traffic based on that configuration. The client package should be installed on all PCs in your organization. The package consists of three core components:

- **Catalyst Controller**

The Catalyst Controller (**Controller.exe**) is the main part of the client add-on infrastructure used by Catalyst to handle Rules implementation and redirection. The Client Framework consists of a background process/listener service that must be running in order for the Catalyst system to operate. Without this component, the browser add-ons cannot communicate properly and redirection will fail to function properly.

- **Catalyst Client Extensions for Internet Explorer, Chrome and Firefox**

Catalyst installs extensions to each browser to enable communication between the browser and the Catalyst Controller.

## 2.2. Software Requirements

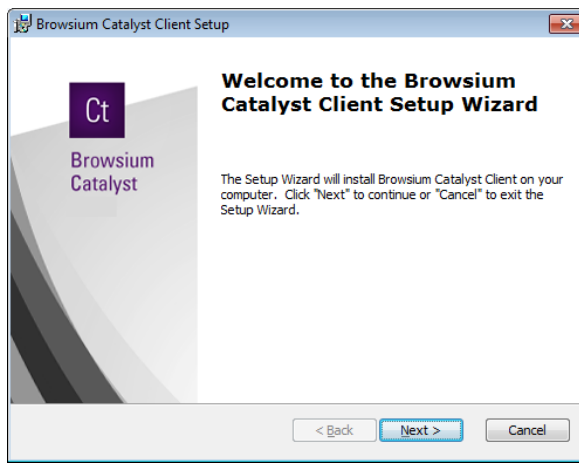
The following minimum system specifications are required to run Catalyst.

- Microsoft Windows
  - Windows XP SP3
  - Windows 7
  - Windows 8.1
  - Windows Server 2003
  - Windows Server 2008 R2
  - Windows Server 2012 R2
- Microsoft Internet Explorer 6, 7, 8, 9, 10, or 11
- Google Chrome 22 (or later)
- Mozilla Firefox 15 (or later)
- .NET Framework Version 3.5 SP1 for Catalyst Configuration Manager
- 512MB system memory
  - 1GB system memory when used on multi-user Windows Servers

## 2.3. Installing the Browsium Catalyst Client

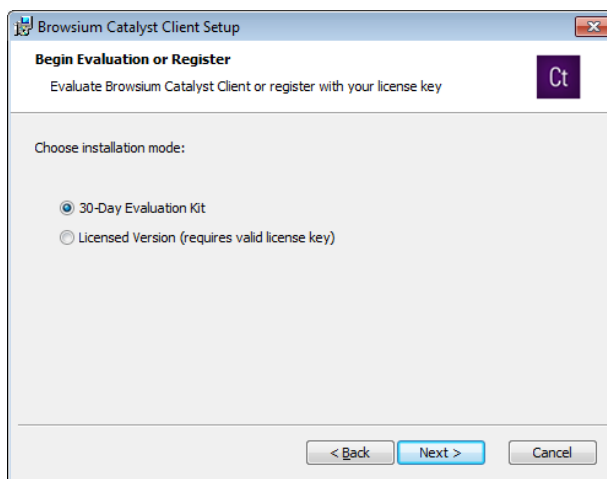
This section covers manual installation of the Browsium Catalyst Client. You will need Administrator rights to run the Client Installer. Once installed, the Catalyst Client can run under any user account and does not require special user permissions or elevation.

1. To start the Client Installer process, simply double-click on the Catalyst-ClientSetup.msi file provided by Browsium. The first screen provides a basic introduction. Click Next to get started.

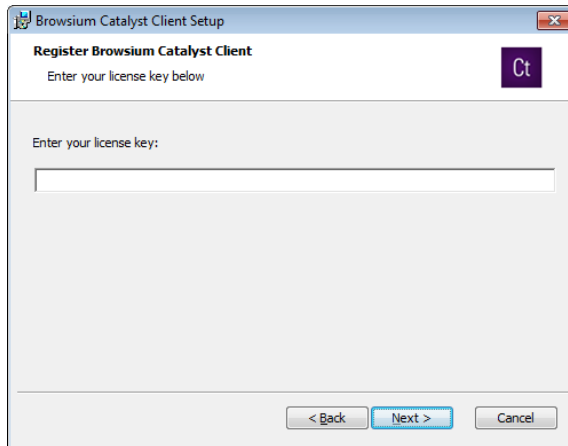


Once the installation process has begun, you will be presented with two installation mode choices. One installs the Catalyst Client software as a 30-Day Evaluation Kit. The second installs the fully licensed version, requiring a license key provided by Browsium.

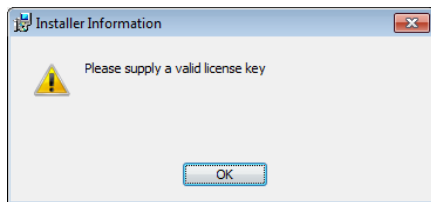
**When you have completed your 30-Day Evaluation of Catalyst and are ready to install the License, the process is defined in [section 2.5.5 Repair Options](#).**



If you have chosen the Licensed Version, you may now enter the license key that has been provided by Browsium and then click Next. The license key can be copied from your Browsium Catalyst Download Page and pasted into the empty box.

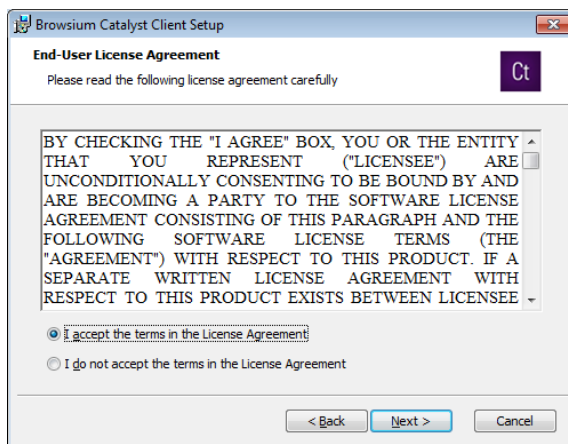


Your license key is then validated. An invalid license key will result in the following error:

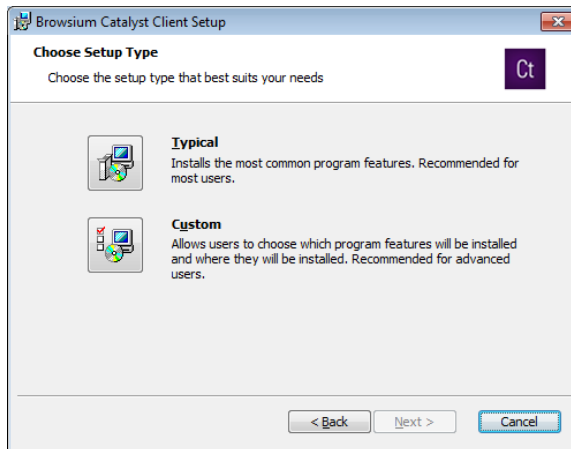


If you believe your key is valid, please contact Browsium Support. You may install the 30-day Evaluation Kit now and update the license key later. Be sure to delete the invalid key after clearing the error dialog before clicking Back to the previous screen.

2. The next screen contains the End User License Agreement (EULA) for Browsium Catalyst software. You will need to read and agree to the terms of the EULA in order to proceed.

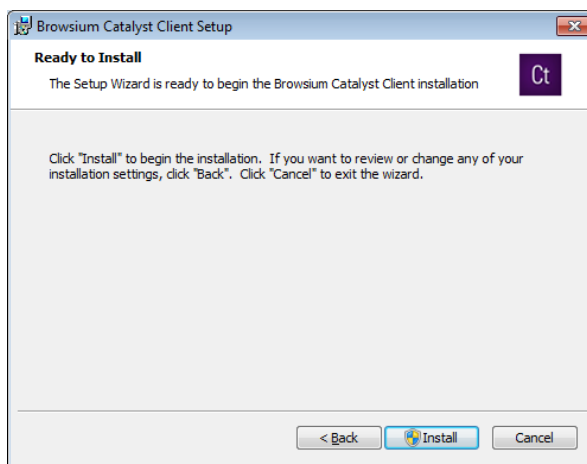


3. Select the installation option which best suits your organization.



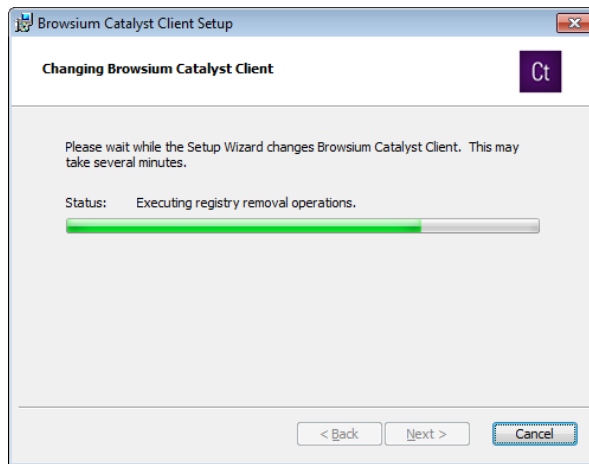
Selecting 'Typical' will install client files to "C:\Program Files\Browsium\Catalyst" (or C:\Program Files (x86)\Browsium\Catalyst on 64-bit systems).

4. Now you are ready to install the Catalyst Client. Simply click **Install** to proceed.

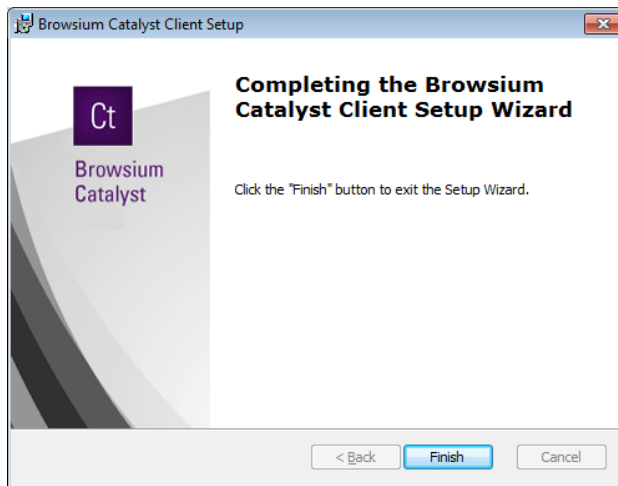


**The Catalyst Client requires Administrator rights for installation so the installer may generate a UAC prompt before installing. Once installed the Catalyst Client runs using standard user permissions.**

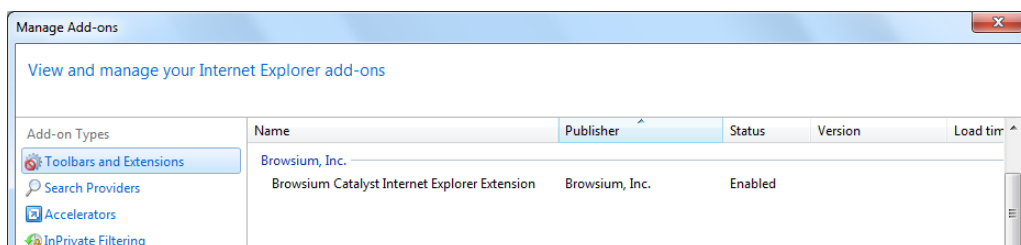
During the process you will see a progress bar:



When the Client installation process has finished, you will see the following screen indicating success.

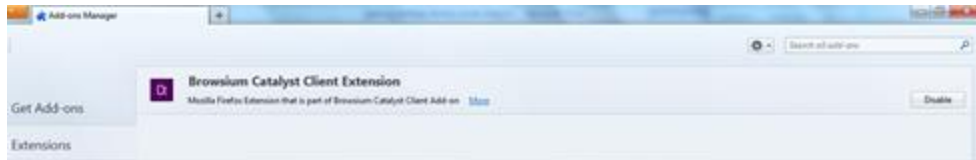
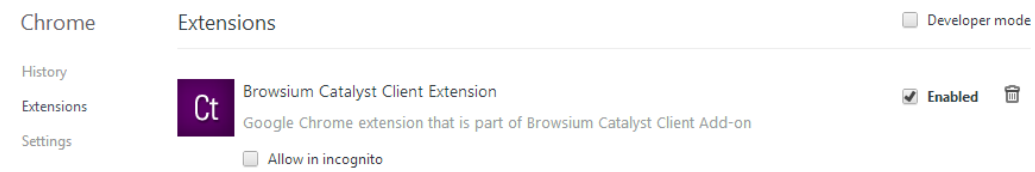


To confirm the Catalyst installation has completed properly, Launch Internet Explorer, and look under Tools->Manage Add-ons, and ensure the Catalyst extensions for each browser is listed and Enabled.





Do the same for Chrome and Firefox.

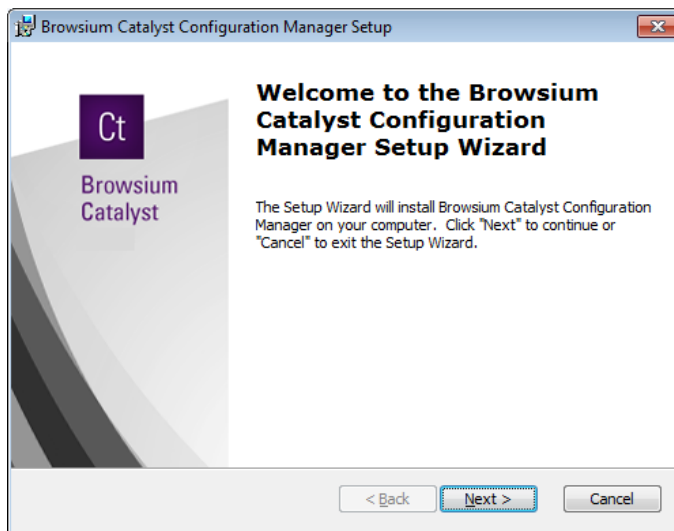


## 2.4. Installing Browsium Catalyst Configuration Manager

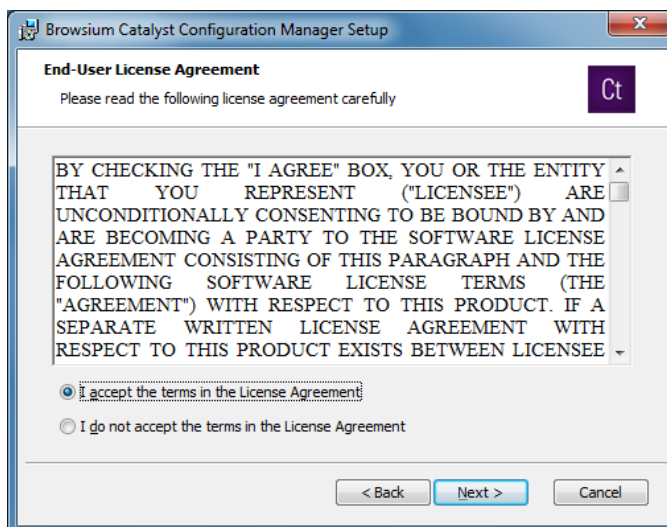
This section covers the installation process for the Browsium Catalyst Configuration Manager. The Browsium Catalyst Client should also be installed on the system for project development.

The steps for installing the Catalyst Configuration Manager are as follows:

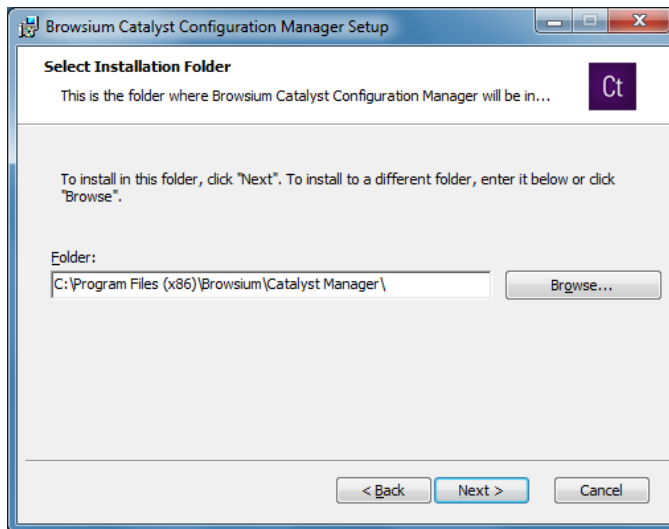
1. Locate the Catalyst Configuration Manager Installation file (**Catalyst-AdminSetup.msi**) and double click to run the program.



2. Confirm you have read and agreed to the End-User License Agreement (EULA) by clicking '**I agree to the terms in the License Agreement**' and **Next** to continue with installation.

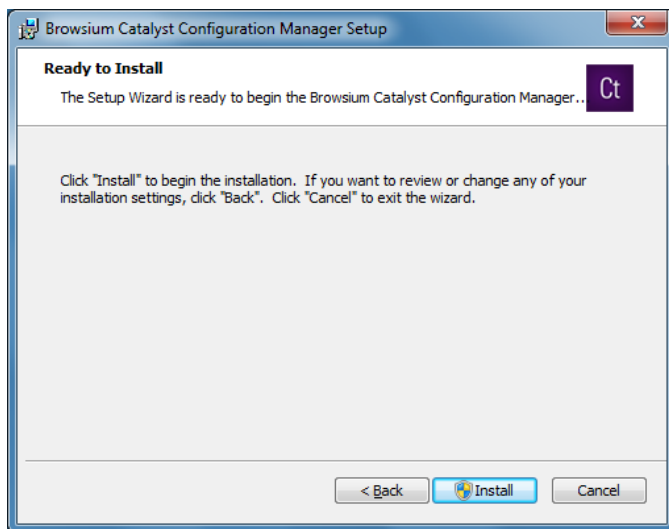


3. By default the installer places the required files in "\Program Files\Browsium\Catalyst Manager" (32-bit systems) or "\Program Files (x86)\Browsium\Catalyst Manager" (64-bit systems) on the system drive.



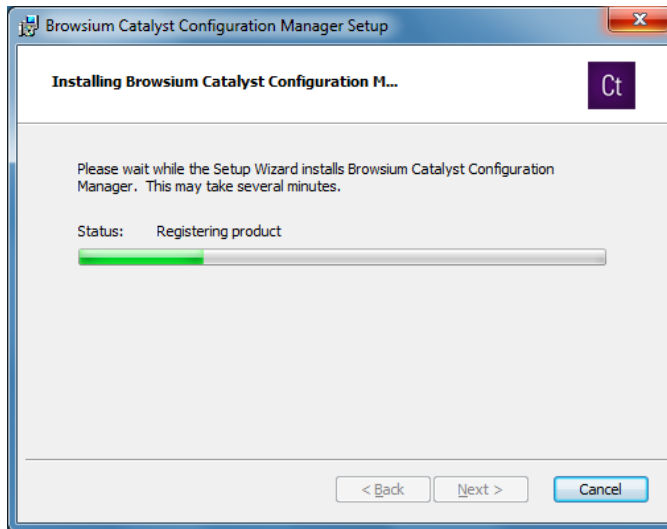
Select an installation location and click **Next**.

4. Now you're ready to install the Catalyst Configuration Manager. Click **Install**.

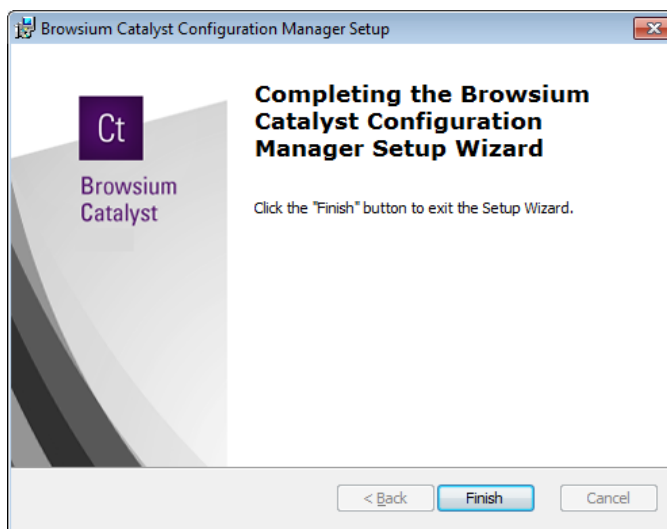


**The Catalyst Configuration Manager requires Administrator rights so the installer may generate a UAC prompt before installing.**

5. During the installation process you will see a progress window



6. This screen will be displayed when the installation is complete and all necessary files have been configured. Click **Finish** and you are ready to begin working with Catalyst.



## 2.5. Available Command Line Switches for the Installer

Catalyst supports network-based installations using Windows Installer (MSIEXEC.EXE) for organizations that use software distribution systems or want to deploy via installation scripts and logon applications. Ion provides for several options that are controlled by the following switches. Note: You must run Command Prompt as Administrator on Windows 7 and above.

### 2.5.1. Installation Options

Switch	Description
<code>/j&lt;u m&gt; &lt;Product.msi&gt; [/t &lt;Transform List&gt;] [/g &lt;Language ID&gt;]</code>	Advertises a product – ‘m’ to advertise to all users, ‘u’ to advertise to the current user
<code>&lt;/uninstall   /x&gt; &lt;Product.msi   ProductCode&gt;</code>	Uninstalls the product
<code>APPDIR=&lt;path&gt;</code>	Installs product to a specific directory, other than the default location
<code>OPT_PID=&lt;license key&gt;</code>	Installs with a Catalyst license key

### 2.5.2. Display Options

Switch	Description
<code>/quiet</code>	Quiet mode, no user interaction
<code>/passive</code>	Unattended mode - progress bar only
<code>/q[n b r f]</code>	Sets user interface level, where: n - No User Interface b - Basic User Interface r - Reduced User Interface f - Full User Interface (Default)
<code>/help</code>	Shows help information

### 2.5.3. Restart Options

Switch	Description
<code>/norestart</code>	Do not restart after the installation is complete
<code>/promptrestart</code>	Prompts the user for restart if necessary
<code>/forcerestart</code>	Always restart the computer after installation (the default if no other option is selected)

### 2.5.4. Logging Options

Switch	Description
<code>/l[i w e a r u c m o p v x + ! *] &lt;LogFile&gt;</code>	Install keeping a log file, where: i - Status messages w - Nonfatal warnings e - All error messages a - Start up actions r - Action-specific records u - User requests c - Initial UI parameters m - Out-of-memory or fatal exit information o - Out-of-disk-space messages p - Terminal properties v - Verbose output x - Extra debugging information + - Append to existing log file ! - Flush each line to the log * - Log all information, except for v and x options
<code>/log &lt;LogFile&gt;</code>	Equivalent of /!<LogFile>

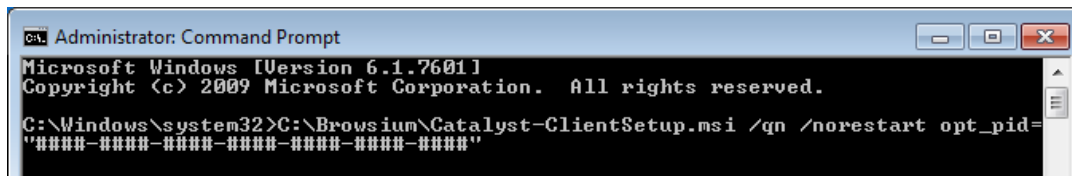
### 2.5.5. Repair Options

Switch	Description
<code>/f[p e c m s o d a u v] &lt;Product.msi   ProductCode&gt;</code>	Repairs a product

### 2.5.6. Command Line Installation Examples

The following example will install Catalyst-ClientSetup.msi with a Catalyst license key in Quiet Mode with No User Interface and will not automatically reboot the system. However, a restart or logoff/logon is required for proper installation and configuration of Catalyst.

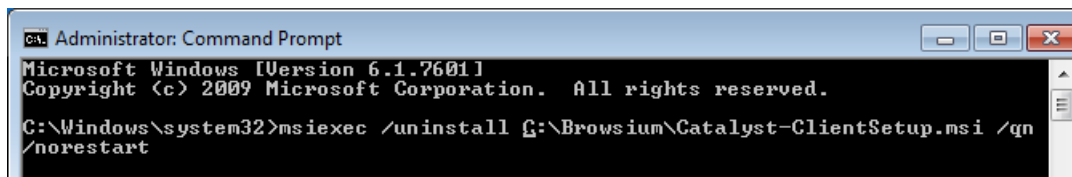
Launch the Command Prompt as Administrator, enter the path to Catalyst-ClientSetup.msi (located in C:\Browsium for this example), add the /qn and /norestart switches, and substitute the hash marks (#) with your Catalyst license key provided by Browsium.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>C:\Browsium\Catalyst-ClientSetup.msi /qn /norestart opt_pid=
"####-####-####-####-####-####-####"
```

The following example will uninstall Catalyst-ClientSetup.msi in Quiet Mode with No User Interface and will not automatically reboot the system. Launch the Command Prompt as Administrator, enter "msiexec /uninstall" followed by the path to Catalyst-ClientSetup.msi and add the /qn and /norestart switches.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Windows\system32>msiexec /uninstall C:\Browsium\Catalyst-ClientSetup.msi /qn
/norestart
```

More information on deploying the Catalyst Client to ensure all browser extensions are enabled by default can be found in [section 5](#).

## 2.6. Upgrading from Evaluation to Licensed Version

You have two options when your 30-Day Evaluation is complete and you wish to upgrade your Catalyst Client software to the fully licensed version:

The first is to enter the license key in the Windows registry utilizing a registry editing tool or command line script. You must have administrator rights to edit the registry.

For 32-bit systems, the registry key is as follows:

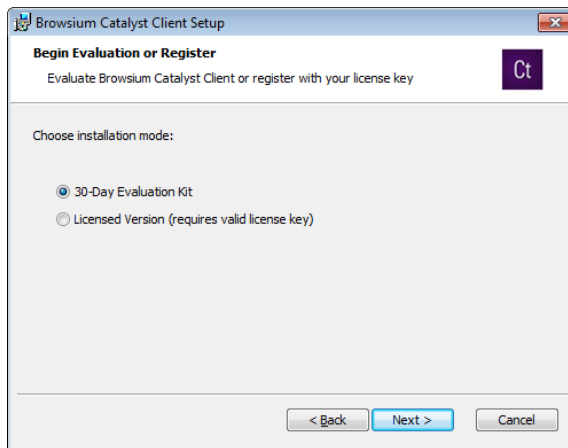
HKEY\_LOCAL\_MACHINE\SOFTWARE\Browsium\Catalyst\Full

For 64-bit systems, the registry key is as follows:

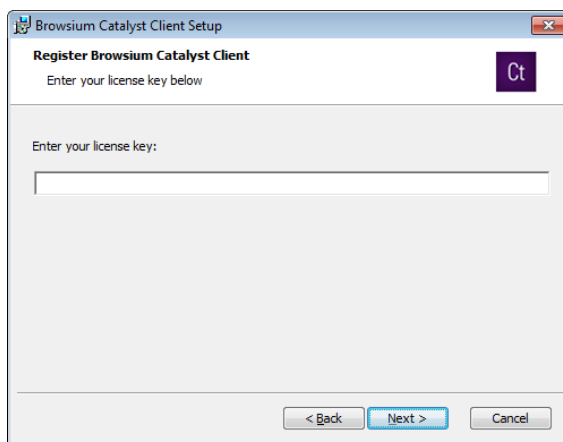
HKEY\_LOCAL\_MACHINE\SOFTWARE\Wow6432Node\Browsium\Catalyst\Full

The value is your license key: ####-####-####-####-####-####-####

The second option is to uninstall the client software with Windows Program and Features uninstall utility which can be found in Control Panel. Then reinstall Catalyst-ClientSetup.msi, select Licensed Version, click Next.



Then enter the license file provided by Browsium and continue with the install process as before.



You may also install the Catalyst Client from a command line using the OPT\_PID=<license key> switch documented in [section 2.5](#).





### *Section Three*

# Introduction to the Catalyst Configuration Manager

---

In this section you will learn:

- ✓ More about the Browsium Catalyst Configuration Manager
- ✓ Where to find settings in the Browsium Catalyst Configuration Manager

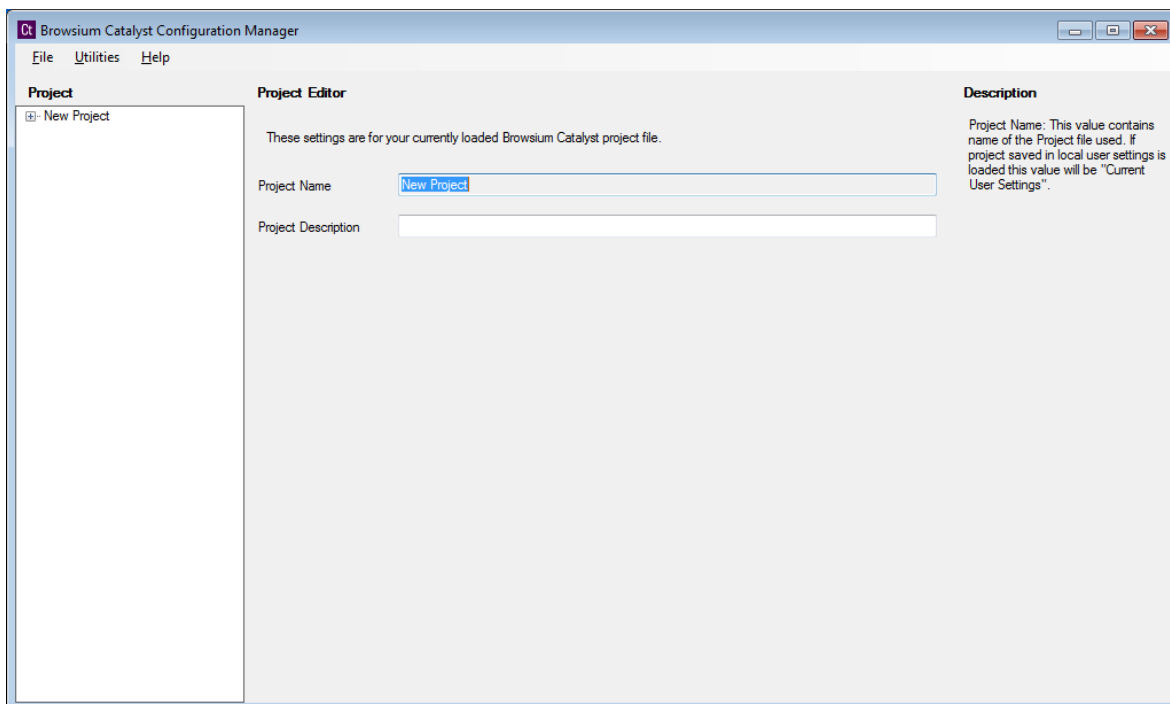
### 3. Catalyst Configuration Manager Overview

The Catalyst Configuration Manager enables you to create and manage Rules that define the websites you want to open using the Catalyst system. This section looks at the various elements of the Catalyst Configuration Manager. The Configuration Manager is designed with the look and feel of an MMC snap-in, with three main functional areas:

Objects Pane (Left) – Tree view containing Settings, Browsers and Rules

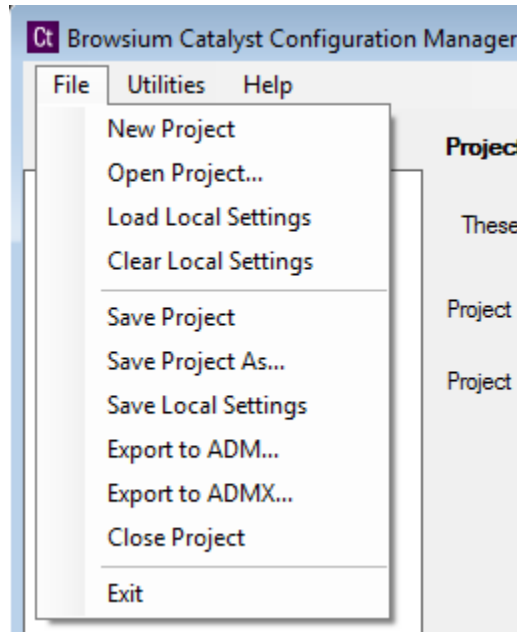
Content Pane (Center) – Main data and content window

Actions Pane (Right) – Contextual links and descriptions for common tasks and steps



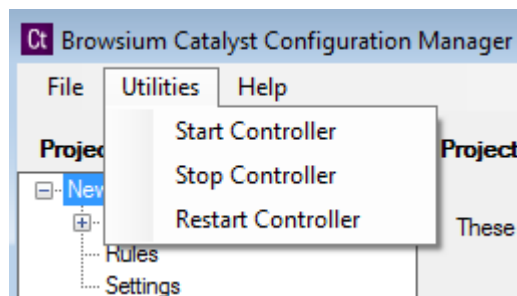
### 3.1. Menu Bar

The Catalyst Configuration Manager Menu Bar dynamically updates the list of available File menu items based on the active Node selected in the Objects Pane.



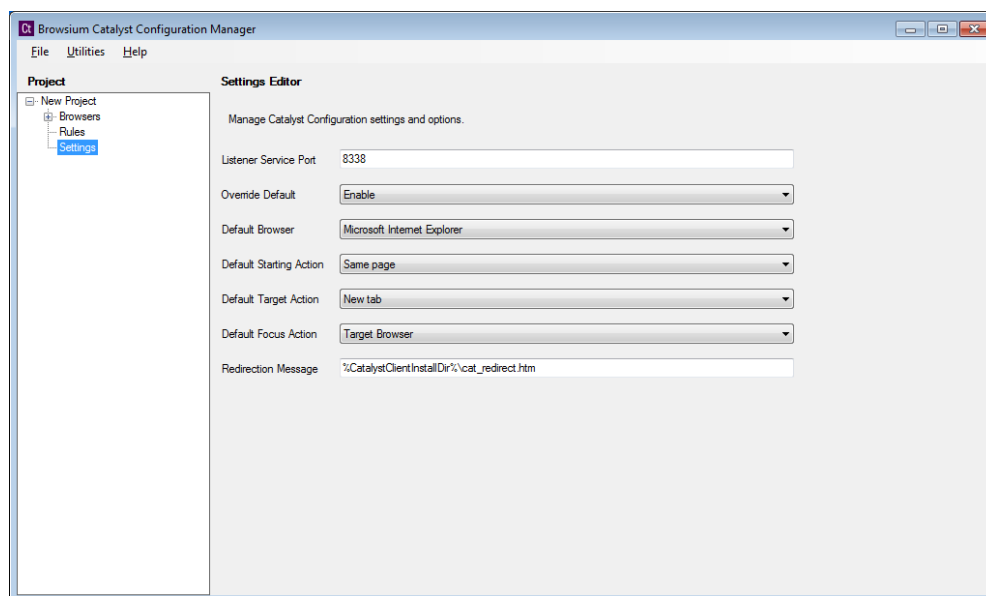
To aid in configuration testing and tuning, the Catalyst Configuration Manager allows Administrators to apply settings directly in the local system registry. Organizations should use the Save Local Settings option for rapid local testing. This option reduces delays and overhead of exporting the configuration to a Flat File or Serialized Registry Keys by applying those settings and restarting the Catalyst Controller to load configuration values.

You can use the Utilities menu to manage the Controller (Controller.exe) process. You may need to Start/Stop/Restart the Controller in order to load new configurations or reproduce troubleshooting steps.



## 3.2. The Settings Node

The Settings Node gives you the ability to edit global settings for Catalyst configurations that will be applied to the Catalyst system. These settings encompass features such as the Listener Service Port, Override Default, Default Browser and other future setting options.



**Listener Service Port** – This port is used by the Controller to communicate with the browser add-ons for the local machine. The default port value is 8338.

**Override Default** – Defines whether Catalyst should override the default browser setting on the system. It must be set to 'Enable' for the Catalyst system to operate.

**Default Browser** – Allows an administrator to define the default browser (as defined by Catalyst) to be used for loading web addresses when no Rule exists.

**Default Starting Action** – Determines the default Starting Action when a new Rule is created.

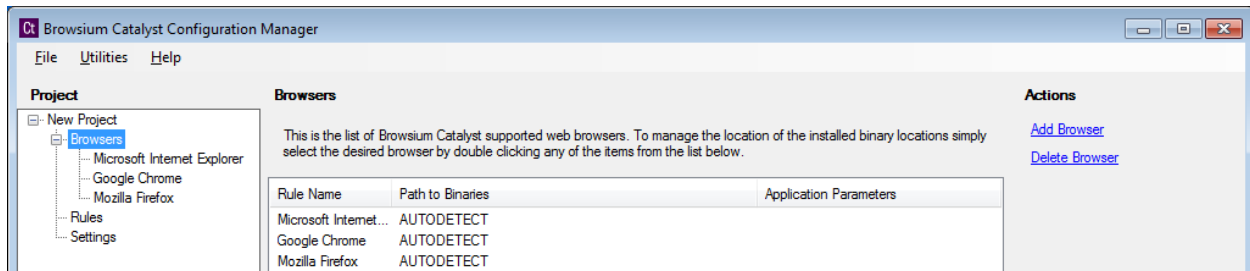
**Default Target Action** – Determines the default Target Action when a new Rule is created.

**Default Focus Action** – Determines the default Focus Action when a new Rule is created.

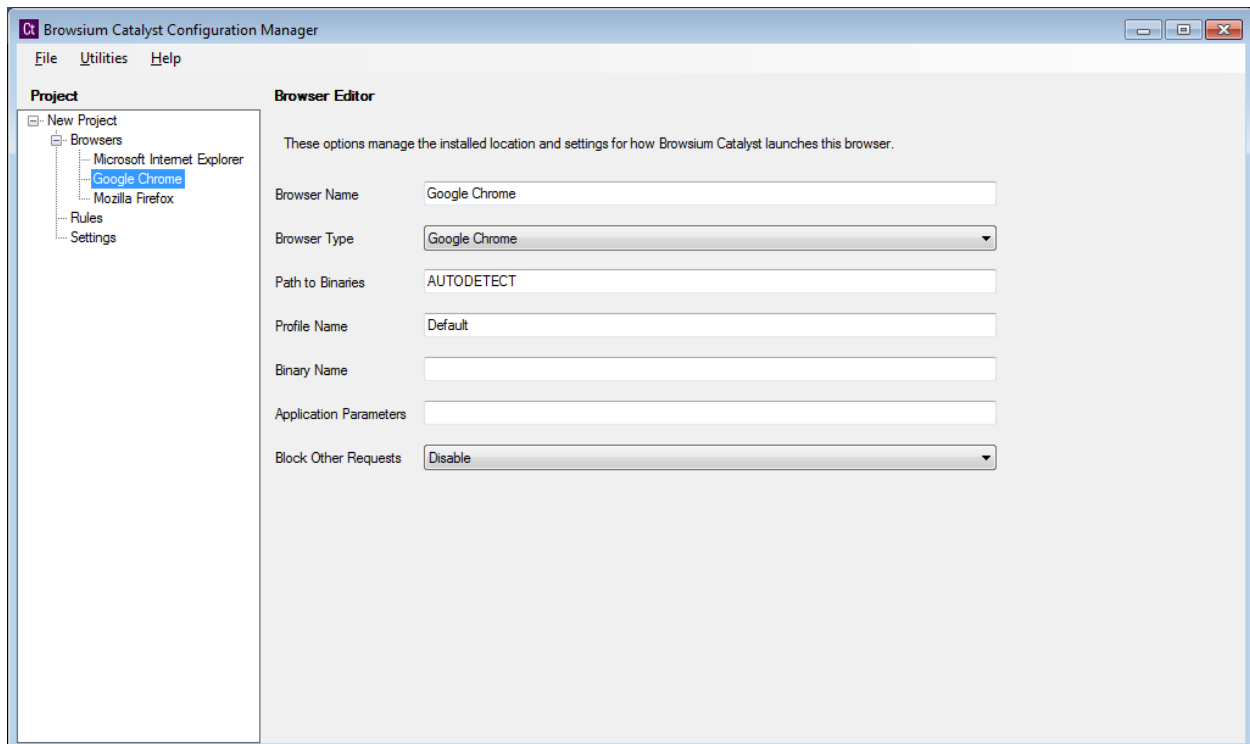
**Redirection Message** – Enables administrators to control the message displayed when Rules have a Starting Action setting of Redirect. Editing this location is supported, but administrators are encouraged to keep the location as-is and replace the file with one to match the design and branding for your organization.

### 3.3. The Browsers Node

The Browsers Node contains the list of defined browsers for a given system. Catalyst only supports the three preset browsers – Internet Explorer, Chrome and Firefox by default. The Catalyst Configuration Manager will attempt to automatically determine the installation path for each installed browser. If one of the browsers is not installed on the system running the Catalyst Configuration Manager, that entry will remain as an option, but the path will be blank and any attempt to use that browser will result in an error.



Clicking on one of the browser items brings up the edit options. Here you can modify the installation path and add application parameters to be used when launching the browser.



**Browser Name** – This is the name of the browser. Browser names can be modified to reflect naming relevant to your organization.

**Changing the Browser Name for a Firefox browser item will result in unexpected behavior. This is a design limitation of the Firefox product.**

**Browser Type** – The Browser Type value is used by Catalyst to identify which type of browser is defined by the setup. This value is required to support multiple browser instances and variations. Setting the Browser Type incorrectly may cause unexpected behaviors.

**Path to Binaries** – This is the path location containing the application binaries. The Catalyst system needs to have the accurate location of the binaries in order to properly load the defined browser when Rule conditions are met. Errors in the path location will cause the Catalyst system to fail to properly load a browser or web content.

**Profile Name** – This value is used to support multiple profile configurations for Google Chrome and Mozilla Firefox.

**Binary Name** – When Browser Type is set to 'Other', the binary name must be defined here.

**Application Parameters** – In addition to launching a desired browser, the Catalyst system can open the application using additional parameters specified here. Ensure any additional parameters are correct for the specific browser as incorrect items may cause the browser to stop loading.

**Block Other Requests** – By default the Catalyst system is designed to only intervene in content loading and redirection when explicitly defined by a Rule. Setting this option will prevent the user from loading any content in the specified browser **unless** the content matches a Rule.

**Use caution when setting to Enable, as users may become confused when the browser redirects any address entered that does match Rules targeted for that browser.**

## 3.4. The Rules Node

The Rules Node is the main interface for creating, editing and managing evaluation criteria for which Catalyst is to manage browser activity. This section contains details on the various elements and pieces of this interface.



The Rules Pane shows the hierarchical rules list that Catalyst uses to determine what (if any) action to take when a web address is entered. The heading for each column in this window refers to the specific rule element (e.g. Rule Name, Element, Operator, Value, etc.) for a given Rule. The Actions pane will display the 4 available options for managing Rules.



**Add Rule** – To create a new rule, click the Add Rule link in the Actions Pane to bring up the Rule Editor window. The next part of this section provides details on the options and values in the Rule Editor window. See the [How to Create a Rule Section](#) for details on creating rules.

**Delete Rule** – To delete a Rule, select it from the Rules Manager Window, then click the Delete Rule link in the Actions Pane.

**To disable a rule rather than remove it, double click the Rule to edit it and change the 'Set Rule' value to 'Disable'.**

**Move Rule Up/Move Rule Down** – By default, rules are ordered in the sequence they are added. Since rules are evaluated in the order they are stored, the sequence of rules can be critical to the proper functionality of your web application in Catalyst. To manually adjust the order of a Rule, simply highlight the Rule and use the Up and Down buttons to move it to the proper placement.



#### *Section Four*

## Creating Rules in Catalyst

---

In this section you will learn:

- ✓ How to create Rules
- ✓ How to test Rules
- ✓ How to remove Rules



## 4. Rule Basics

Once the Browsium Catalyst Configuration Manager installation is complete, you can begin configuring which sites to load in the desired browser. The Browsium Catalyst Configuration Manager is provided as a simple interface to create, delete and manage the Rules and Settings that govern Catalyst behavior.

**Systems must have the Browsium Catalyst Client for the appropriate browsers installed in order to use the Rules and configurations created in the Catalyst Configuration Manager.**

## 4.1. How to Create a Rule

Catalyst offers a few ways to deliver powerful options for rule matching in order to meet the specific needs of your environment. In this example we have identified a website, <http://www.yourang.us>, which must be opened using Internet Explorer – it will not work properly in any other browser.

To create the Rules needed for the YouRang site, use the following steps:

1. Click the Rules Node, click the '**Add Rule**' link in the Actions pane to bring up the Rule Editor screen.

Rule Editor		Description
Rules define the starting and target browser actions for a given set of conditions.		
Rule Name	<input type="text" value="New Rule 1"/>	<p>Rule Name: This field is used to name the specific Rule, and should be meaningful to your organization. Rule Names should be short and clear and may contain any characters. For example, the name 'HR - Benefits System' would be a great way to uniquely identify this Rule for a specific HR team application.</p> <p>Two Rules cannot contain the same name and care should be taken to use unique names.</p>
Rule Active	<input type="button" value="Enable"/>	
Element	<input type="button" value="Absolute URI"/>	
Operator	<input type="button" value="Includes"/>	
Value	<input type="text" value="http://www.example.com"/>	
Starting Browser	<input type="button" value="ANY"/>	
Starting Action	<input type="button" value="Same page"/>	
Target browser	<input type="button" value="Microsoft Internet Explorer"/>	
Target Action	<input type="button" value="New tab"/>	
Focus	<input type="button" value="Target Browser"/>	

Start by entering a name for the Rule. Rule names are friendly names for organizational and identification purposes only and have no effect on the behavior of a rule. For this example, we will choose "YouRang Portal".

2. Keep the 'Rule Active' value to 'Enable' to ensure the Rule is active and Catalyst will trigger when the proper conditions are met.

3. Select an Element type from the dropdown menu. For this example, we will choose the most common and granular type of rules used by customers, "Absolute URI". An Absolute URI is the exact text excluding any fragments you would see in the browser's address bar when you are at a site. The other Element options are included for many scenarios where they offer a better Rule matching basis.

Rule Editor		Description
Rules define the starting and target browser actions for a given set of conditions.		
Rule Name	<input type="text" value="YouRang Portal"/>	
Rule Active	<input type="button" value="Enable"/>	
Element	<input type="button" value="Absolute URI"/>	Element: Select the element on which the Rule is to act. The most common Element type is Absolute URI, which is the default option for this setting. Available options are:
Operator	<input type="button" value="Absolute URI"/>	Domain - The domain (including top level domain) only. Should not be used for Intranet sites, use other Element options instead.
Value	<input type="text"/>	Absolute URI - The entire canonical URI, including protocol scheme, username, password, hostname, domain, port, path, query, extension and fragment.
Starting Browser	<input type="button" value="ANY"/>	Zone - The Zone of the URI. E.g. Intranet, LocalMachine, Internet, etc.
Starting Action	<input type="button" value="Same page"/>	NOTE: Please note that machines with IE 6 installed won't be able to match the rules with "Domain" as the element. Catalyst client will ignore such rules on machines with IE 6 installed.
Target browser	<input type="button" value="Microsoft Internet Explorer"/>	
Target Action	<input type="button" value="New tab"/>	
Focus	<input type="button" value="Target Browser"/>	

4. Next, choose an Operator from the dropdown menu. For this example, we will choose "Includes". The operator "Includes" allows Catalyst to open the website if the value in the Rule matches the value anywhere in the browser's address bar. Since the Operator condition match is very broad, it will load pages from any website that includes the Value so care should be used when selecting the "Includes" Operator.

Rule Editor		Description
Rules define the starting and target browser actions for a given set of conditions.		
Rule Name	<input type="text" value="YouRang Portal"/>	
Rule Active	<input type="button" value="Enable"/>	
Element	<input type="button" value="Absolute URI"/>	
Operator	<input type="button" value="Includes"/>	Operator: Select the Operator value on which the Rule will evaluate. In addition to common Operator values, Rules can be triggered by complex Regular Expressions, providing the maximum flexibility for any scenario.
Value	<input type="text"/>	
Starting Browser	<input type="button" value="ANY"/>	
Starting Action	<input type="button" value="Includes"/>	
Target browser	<input type="button" value="Microsoft Internet Explorer"/>	
Target Action	<input type="button" value="New tab"/>	
Focus	<input type="button" value="Target Browser"/>	

- Enter a Value to check for Rule matching conditions. For this example we will use "yourang.us" to match our portal site.

Rule Editor		Description
Rules define the starting and target browser actions for a given set of conditions.		
Rule Name	<input type="text" value="YouRang Portal"/>	<p>Value: The Value field should be the string or integer that must be conditionally matched to instruct Browsium Catalyst to manage which browser will be used to load the content.</p> <p>Note: When Element is set to Zone, the Value field is used to define the Zone value. Legal Values would be 'LocalMachine', 'Intranet', 'Trusted', 'Internet' and 'Restricted'.</p> <p>The default value for all new Rules is 'http://www.example.com'.</p>
Rule Active	<input type="button" value="Enable"/>	
Element	<input type="button" value="Absolute URI"/>	
Operator	<input type="button" value="Includes"/>	
Value	<input type="text" value="yourang.us"/>	
Starting Browser	<input type="button" value="ANY"/>	
Starting Action	<input type="button" value="Same page"/>	
Target browser	<input type="button" value="Microsoft Internet Explorer"/>	
Target Action	<input type="button" value="New tab"/>	
Focus	<input type="button" value="Target Browser"/>	

- The 'Starting Browser' option allows administrators to define if the user must initiate a Rule action from a specific browser, or if the Rule should be triggered regardless of which browser is active at the time. The default value for this setting is 'ANY' to ensure the broadest rule coverage.

Rule Editor		Description
Rules define the starting and target browser actions for a given set of conditions.		
Rule Name	<input type="text" value="YouRang Portal"/>	<p>Starting Browser: Select which browser must be used to initiate Browsium Catalyst redirection. Select a browser if action should be taken only when users initiate requests from a specific browser.</p> <p>The default value – ANY – is recommended so users will be redirected regardless of which browser is being used.</p>
Rule Active	<input type="button" value="Enable"/>	
Element	<input type="button" value="Absolute URI"/>	
Operator	<input type="button" value="Includes"/>	
Value	<input type="text" value="yourang.us"/>	
Starting Browser	<input type="button" value="ANY"/> <input type="button" value="Microsoft Internet Explorer"/> <input type="button" value="Google Chrome"/> <input type="button" value="Mozilla Firefox"/> <input type="button" value="ANY"/>	
Starting Action	<input type="button" value="Same page"/>	
Target browser	<input type="button" value="Microsoft Internet Explorer"/>	
Target Action	<input type="button" value="New tab"/>	
Focus	<input type="button" value="Target Browser"/>	

7. Catalyst provides the ability for administrators to control the user experience behavior when a Rule is triggered. Administrators can set Catalyst to leave the user on the same page, redirect them (and display a redirection notice page) or close the active tab. By default the 'Starting Action' option is set to 'Same Page' to avoid interrupting the user activity and simply leaving the user at their last successful navigation.

Rule Editor	Description
Rules define the starting and target browser actions for a given set of conditions.	
Rule Name	YouRang Portal
Rule Active	Enable
Element	Absolute URI
Operator	Includes
Value	yourang.us
Starting Browser	ANY
Starting Action	Same page
Target browser	Same page Redirect Close tab
Target Action	New tab
Focus	Target Browser

**Description**

Starting Action: Define the Starting Browser navigation behavior. It can be one of the following options.

Same page - Instruct the Starting Browser to cancel the desired navigation and remain on the current page while opening the content in the Target Browser.

Redirect - Instruct the Starting Browser to cancel the desired navigation and redirect to a local webpage that tells the user that the content was opened in another browser.

Close tab - Instruct the Starting Browser to cancel the desired navigation and close the current tab while opening the content in the Target Browser.

NOTE: On machines where IE 6 is installed, "Close tab" option will be interpreted as "Same page".

8. The 'Target Browser' setting defines which browser is loaded when the Rule conditions are met. By default this value is set to the value listed in the 'Settings' pane – in this case 'Microsoft Internet Explorer'. Administrators should set this value to the desired browser. If the purpose of the Rule is to block navigation (e.g. for security purposes), simply set the value to 'NONE'. For this example we will load the YouRang portal in Microsoft Internet Explorer.

Rule Editor	Description
Rules define the starting and target browser actions for a given set of conditions.	
Rule Name	YouRang Portal
Rule Active	Enable
Element	Absolute URI
Operator	Includes
Value	yourang.us
Starting Browser	ANY
Starting Action	Same page
Target browser	Microsoft Internet Explorer Microsoft Internet Explorer Google Chrome Mozilla Firefox NONE
Target Action	Target Browser
Focus	Target Browser

**Description**

Target Browser: Select which browser is required/desired to load the content when the Rule is triggered by the user.

When set to 'NONE', navigation action will be aborted. Catalyst will also ignore Target Action and Focus values when Target browser is set to 'NONE'.

9. Catalyst offers the ability to granularly control browser behaviors when loading content, offering the ability to load sites in a New tab, New window or New session. By default the 'Target Action' value is set to 'New tab'. Select the option which works best for your organization.

Rule Editor		Description
Rules define the starting and target browser actions for a given set of conditions.		
Rule Name	<input type="text" value="YouRang Portal"/>	
Rule Active	<input type="button" value="Enable"/>	
Element	<input type="button" value="Absolute URI"/>	
Operator	<input type="button" value="Includes"/>	
Value	<input type="text" value="yourang.us"/>	
Starting Browser	<input type="button" value="ANY"/>	
Starting Action	<input type="button" value="Same page"/>	
Target browser	<input type="button" value="Microsoft Internet Explorer"/>	
Target Action	<input type="button" value="New tab"/> <input type="button" value="New tab"/> <input type="button" value="New window"/> <input type="button" value="New session"/>	<p>Target Action: Define the target browser navigation behavior. It can be one of the following options:</p> <p>New Tab – Open the content in the specified browser using a New Tab.</p> <p>New Window – Open the content in the specified browser using a New Window.</p> <p>New Session – Open the content in the specified browser using a New User Session.</p> <p>NOTE: On machines where IE 6 is installed, "New tab" will be interpreted as "New Window".</p>
Focus		

10. The final Rule option is Focus, offering control over which browser gets visual focus. The default setting for this option is 'Target Browser'.

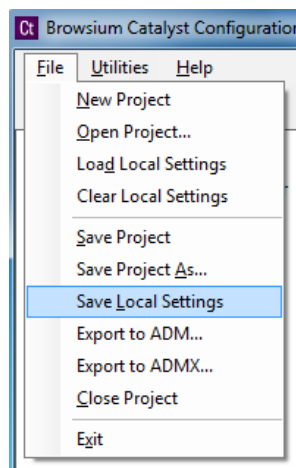
Rule Editor		Description
Rules define the starting and target browser actions for a given set of conditions.		
Rule Name	<input type="text" value="YouRang Portal"/>	
Rule Active	<input type="button" value="Enable"/>	
Element	<input type="button" value="Absolute URI"/>	
Operator	<input type="button" value="Includes"/>	
Value	<input type="text" value="yourang.us"/>	
Starting Browser	<input type="button" value="ANY"/>	
Starting Action	<input type="button" value="Same page"/>	
Target browser	<input type="button" value="Microsoft Internet Explorer"/>	
Target Action	<input type="button" value="New tab"/>	
Focus	<input type="button" value="Target Browser"/> <input type="button" value="Target Browser"/> <input type="button" value="Starting Browser"/>	<p>Focus: Assign which browser should obtain focus when the navigation is complete.</p> <p>When set to 'Starting Browser', the current browser will retain focus and the desired content will load in the alternate browser in the background.</p> <p>When set to 'Target Browser', the Target browser will take focus. 'Target Browser' is the default option.</p>

11. When you are done creating the Rule (or changing a setting), simply click back to the Rules label on the Objects pane to save the Rule. You must still save the Project itself or the configuration will be lost when the Catalyst Configuration Manager is closed.
12. You can continue to add Rules until you have completed all the desired entries.
13. Rules and settings can be saved either as Local Settings or Project files.

**Projects should be saved regularly to ensure work is not accidentally lost. Catalyst does not auto-save work in progress.**

Saving as Local Settings will apply the configuration to the PC instantly for testing, whereas saving the project file would not apply the configuration now, but enable you to load it later or deploy it to another system.

For this example, we'll use the Save Local Settings option under the File menu.



14. Once the settings are saved, simply open Chrome or Firefox and browse to the 'www.yourang.us' website and Catalyst will automatically stop the navigation in your current browser and open Internet Explorer to the YouRang site.

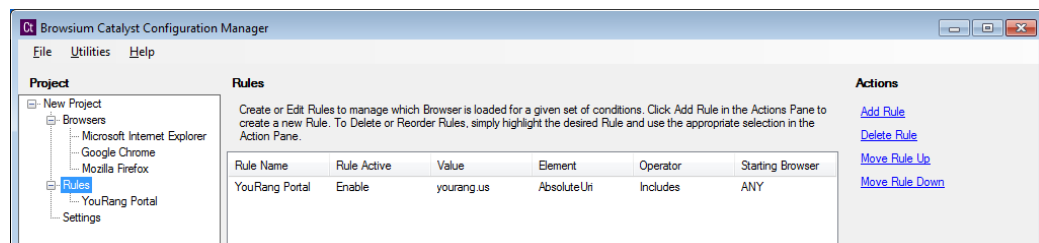


## 4.2. How to Remove a Rule

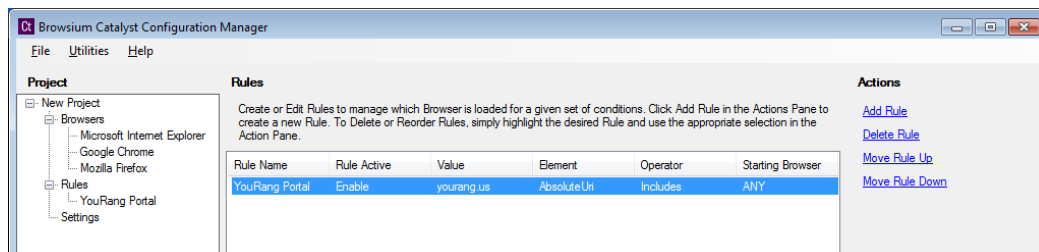
Rules are easily removed when they are no longer needed using the Browsium Catalyst Configuration Manager.

You can remove a rule by following these steps:

1. Open the Catalyst Configuration Manager and load the Project containing the Rules you want to remove (using either Load Local Settings or Open Project from the File menu). With the Project loaded, click the Rules node to bring up the ordered list of Rules.



2. Select the Rule you wish to remove from the list of Rules.



3. Click the Delete Rule in the Actions pane.

**Remember to save the configuration using the File menu (either as a Project File or Local Settings) before closing the Catalyst Configuration Manager to ensure the deleted Rule is actually removed from your configuration.**





### *Section Five*

## Catalyst Management Options

---

In this section you will learn:

- ✓ How to use Group Policy to manage Catalyst extension settings for each browser
- ✓ To automatically enable and lock down the Catalyst extensions on remote systems
- ✓ To configure other settings to improve the Catalyst experience for end users

## 5. Managing the Catalyst Client software

It is important develop a strategy to properly deploy and manage the Catalyst Client software on end user PCs. As part of your strategy, two important system configuration options should be considered.

The first is to ensure the Catalyst browser extensions are 'enabled' for all browsers on each client PC. It is recommended that you also block end users from disabling the Catalyst browser extensions once they've been enabled.

The second is to ensure that neither Internet Explorer, Chrome, nor Firefox are selected as the 'default browser' or set to prompt to become the default – Catalyst itself (actually the Catalyst Controller) must be the default so it can route all navigation to the appropriate browser. Catalyst will take over as the default browser automatically, every time the Controller starts.

Many organizations utilize Group Policy to enforce settings on end users PCs. The alternative method for managing the enforcement of the browser settings for Internet Explorer is by adding or changing registry settings manually.

To modify settings manually in the local PC registry, administrators will need to use a registry editor. The default Windows registry editor which must be launched from the Run command is regedit.exe. Administrative privileges are required to use the regedit.exe editor.

While these important system configuration options can be managed by Group Policy in both Internet Explorer and Google Chrome, Mozilla Firefox does not natively support Group Policy today.

## 5.1. Managing the Catalyst Extension for Internet Explorer

This section will guide you through the various settings for Internet Explorer that can be managed in a Catalyst deployment.

### 5.1.1. Enable the Catalyst Add-on for Internet Explorer via Group Policy

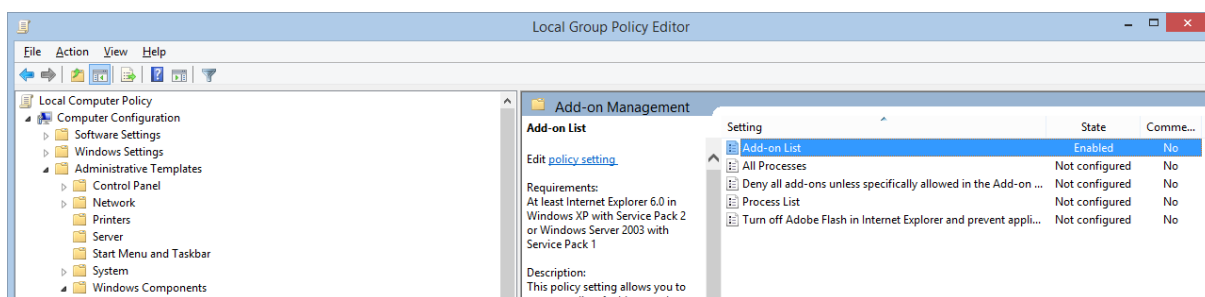
Recent versions of Internet Explorer require user confirmation before any new add-on (or extension) is enabled, unless that add-on is set to 'enabled' during the deployment process. The most common way to enable the Browsium Catalyst Internet Explorer extension during deployment is by utilizing Group Policy to make the necessary registry changes on client PCs. Alternative methods to modify the registry on client PCs, such as using a registry editing tool, a Visual Basic Script or making the changes to the registry with software distribution tools.

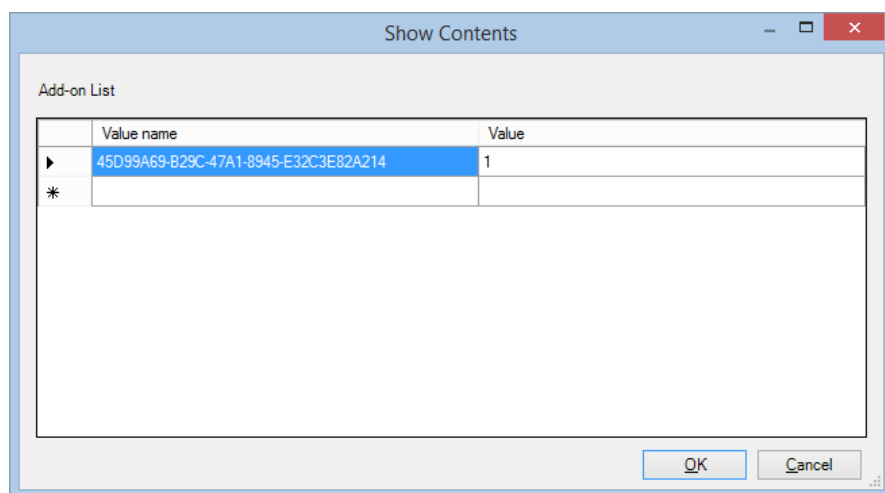
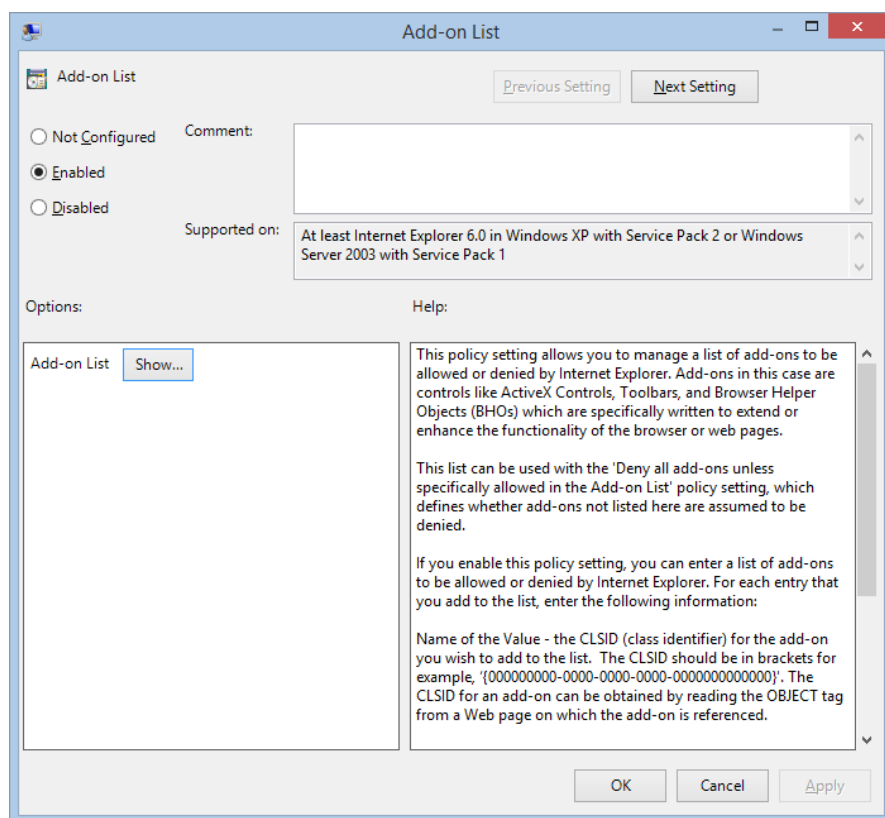
#### Group Policy - Understanding the 'Add-on List Policy'

Administrators can control the use of specific add-ons through the **add-on list** policy. Administrators can choose to enable or disable an add-on as well as allow a specific add-on to be managed by the user.

**Policy Name:** add-on list

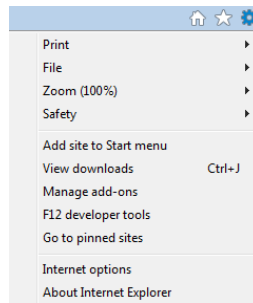
**Path:** User Configuration or Computer Configuration node; Administrative Templates\Windows Components\Internet Explorer\Security Features\Add-on Management. To set this policy, an administrator can enable the policy and enter the GUID/CLSID of the Catalyst add-on to the Add-on List and set the value to 1.



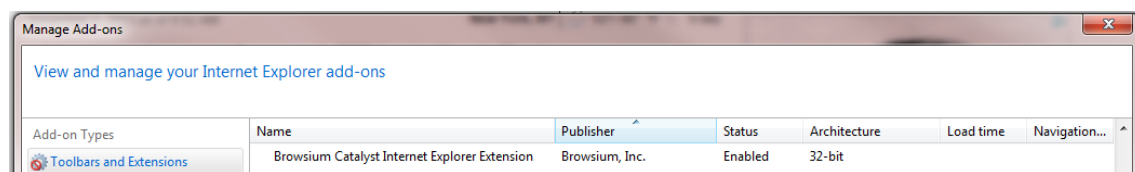


## Determining the GUID/CLSID of the Catalyst Internet Explorer Extension

After installing the Browsium Catalyst Client, go to the tools menu in Internet Explorer and choose Manage add-ons.

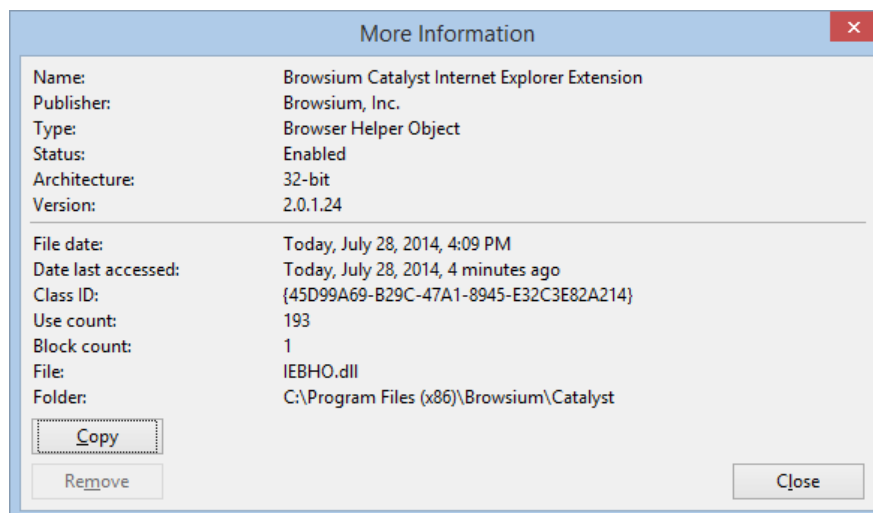


You'll then be presented with the Manage Add-ons interface where you should see Browsium Catalyst Internet Explorer Extension in the list among the Toolbars and Extensions that are currently loaded in Internet Explorer.



Right Click on the Browsium Catalyst Internet Explorer Extension and choose "More Information" from the dropdown menu.

The CLSID, (Class ID) will appear in the dialog box.



Click the "Copy" button and then paste the contents of this dialog box (including the Class ID) to Notepad for later reference and save the text file. When you make the registry changes documented above, you will need to use the Class ID to identify the add-on in the policy.

To set this policy with a manual or automated registry entry, an administrator can create a registry value based on the GUID/CLSID of the add-on in either of the following keys and then set the desired value:

HKEY\_CURRENT\_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Ext\CLSID

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Ext\CLSID

Each add-on is a value in this registry key with the following properties.

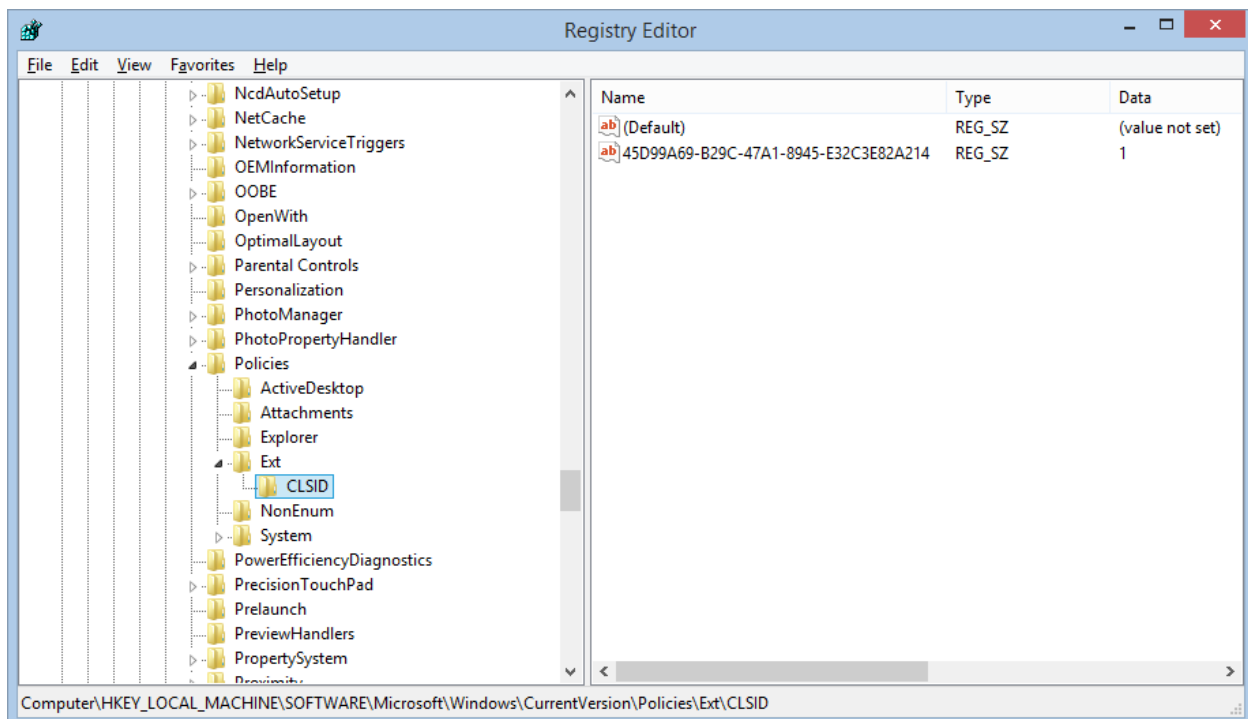
**Name:** *GUID* of add on which is {45D99A69-B29C-47A1-8945-E32C3E82A214}

**Type:** REG\_SZ

**Value:**

- 0 - Add-on is disabled and cannot be managed by the end user.
- 1 - Add-on is allowed and cannot be managed by the end user.
- 2 - Add-on is allowed and can be managed by the end user.

The Add-on (CLSID) lists are empty by default.



### 5.1.2. Disable Internet Explorer's Default Browser Check via Group Policy and the local Registry

By default, some versions of Internet Explorer will prompt the user to select it as the default browser. Since Catalyst becomes the default browser, you will want to prevent this behavior.

With Group Policy settings and local registry settings, you can remove the ability for end users to change the default browser to Internet Explorer. Depending on which Group Policy template is on the system, this policy will vary. This policy allows you to prevent Internet Explorer from checking to see whether it is the default browser and prevents the user from changing it.

Before you enable this policy, you will want to uncheck the box "Tell me if Internet Explorer is not the default browser". The check box is on the Program tab in the Internet Options dialog box. You can uncheck the box with a registry setting in the HKCU hive. The path to the registry key is below. The value for "Check Associations" should be "no".

```
[HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main]"Check_Associations"="no"
```

The Group Policy settings are listed below. All of them can be found at the following path:

**Path:** User Configuration\Administrative Templates\Windows Components\Internet Explorer

#### **For IE6 – IE9:**

**Policy Name:** Prevent changing default browser check

#### **For IE10:**

**Policy Name:** Disable changing default browser check

**Policy Name:** Notify users if Internet Explorer is not the default web browser

If you enable this policy, the **Internet Explorer Should Check to See Whether It Is the Default Browser**. Also, the check box on the **Programs** tab in the **Internet Options** dialog box appears dimmed and the user cannot change the default browser to IE. If you disable this policy or do not configure it, users can determine whether Internet Explorer will check to see if it is the default browser. When Internet Explorer performs this check, it prompts the user to specify which browser to use as the default.

## 5.2. Managing the Catalyst Extension for Google Chrome

To ease your Group Policy setup, several templates can guide you through the configurable options. The Group Policy templates, and associated guidance are provided by Google and can be found on [Google's support site](#). You may find additional settings (beyond those documented in this section) that you may wish to enforce or enable based upon your organization's preferences.

**Starting with Chrome 28, policies are loaded directly from the Group Policy API on Windows. Policies manually written to the Windows registry will be ignored. See <http://crbug.com/259236> for details.**

### 5.2.1. Enable the Catalyst Extension for Chrome via Group Policy

By default, Chrome automatically disables all extensions that are side-loaded (installed by a 3<sup>rd</sup> party program, like the Catalyst Client installation package), requiring users to enable them manually. The only way to centrally enable the Catalyst Extension for Chrome for enterprise deployment is via Group Policy for domain-joined systems.

The policy **Configure the list of force-installed extensions** (a.k.a. `ExtensionInstallForcelist`) allows you to specify a list of extensions that will be installed silently and enabled by default, without user interaction. This policy also works for side-loaded extensions, effectively overriding the default behavior in Chrome.

Each item of the list is a string that contains an extension ID and an update URL, separated by a semicolon (;). The extension ID is the 32-letter string found e.g. on `chrome://extensions` when in 'Developer mode'. The update URL must point to an Update Manifest XML document as described at <http://code.google.com/chrome/extensions/autoupdate.html>. Note that the update URL set in this policy is only used for the initial installation; subsequent updates of the extension will use the update URL indicated in the extension's manifest.

For each item, Google Chrome will retrieve the extension specified by the extension ID from the update service at the specified update URL and silently install it. Users will be unable to uninstall extensions that are specified by this policy. If you remove an extension from this list, it will be automatically uninstalled by Google Chrome. Extensions specified in this list are also automatically whitelisted for installation; the **Configure extension installation blacklist** (a.k.a. `ExtensionInstallBlackList`) does not affect them.



**A by-product of the `ExtensionInstallForceList` policy is that managed extensions are silently installed in Chrome, enabled by default, and block users from disabling or removing them. This is desired for enterprise deployment of Catalyst.**

**If this policy is 'Not Configured', users can delete any extension in Chrome, including Catalyst, from the Extensions page. This is undesirable, as side-loaded extensions that are deleted are automatically blacklisted and re-enabling them is tricky (but achievable). Contact [Browsium Support](#) if this happens.**

To force-enable the Catalyst Extension for Chrome, and lock it down so users can't disable or delete it, you will use the **Configure the list of force-installed extensions** policy. This process requires an XML Manifest, which references the Catalyst extension .crx file. Both must be available on a server or in the Chrome web store. Browsium is hosting these files for all customers on browsium.com.

Follow these steps to ensure that this method is properly configured using Group Policy for your domain-joined systems. These instructions assume you're using the ADM template. The Group Policy location will change if using ADMX.

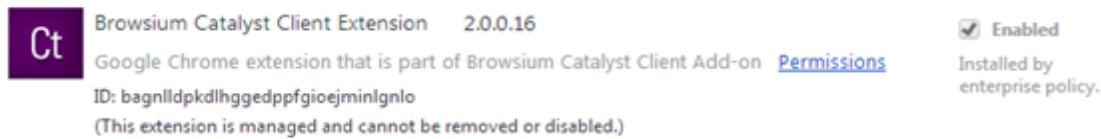
**As of Chrome 33, the `ExtensionInstallForceList` policy is only enforced for domain-joined systems. All client PCs in your environment must be joined to a Windows domain or you will not be able to centrally manage the Catalyst Chrome extension. Attempting to configure `ExtensionInstallForceList` via the Local Policy Editor will result in unpredictable behavior of the Catalyst Chrome extension.**

1. Download and install the [Google Chrome Standalone MSI](#).
2. Install Catalyst Client software.
3. Download the Group Policy templates for Chrome from the [Google support site](#).
4. Import the Google Chrome Group Policy template into your Group Policy editor.
5. Enable the policy **Configure the list of force-installed extensions**.
6. Enter the following value by selecting the 'Show...' button in the Options window and apply the setting.

(This is the Catalyst extension ID followed by the URL for the manifest XML document, with no spaces in the string.)

```
bagnlldpkdlhggedppfgioejminlgnlo;http://www.browsium.com/crx/catalyst-2.0.1/catalyst-chrome-2.0.1.xml
```

7. View the results on the Chrome Extensions page (<chrome://extensions>).

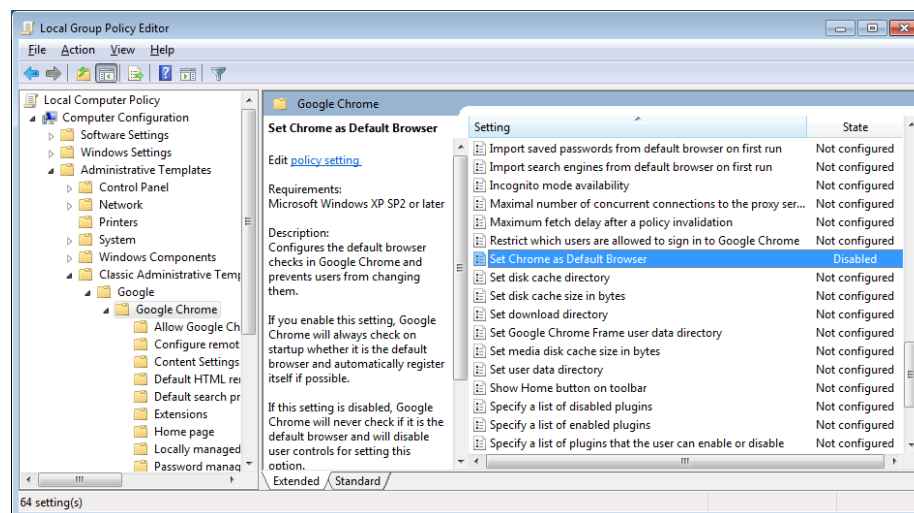


**The Catalyst Chrome extension will have a different version number from the other Catalyst components. For Catalyst 2.0.1, the Chrome extension has the version number 2.0.0.16 while all other components have the version number 2.0.1.24.**

### 5.2.2. Disable Chrome's Default Browser Check via Group Policy

Group policy can be used to configure the default browser checks in Google Chrome and prevent users from changing them. If you 'Enable' this setting, Chrome will always check on startup whether it is the default browser and automatically register itself if possible. If this setting is 'Disabled', Chrome will never check if it is the default browser and will disable user controls for setting this option (the desired state when using Catalyst). If this setting is 'Not Configured', Chrome will allow the user to control whether it is the default browser and whether user notifications should be shown when it isn't.

For all users running Catalyst, the **Set Chrome as Default Browser** setting (a.k.a. `DefaultBrowserSettingEnabled`) should be "Disabled" in your Group Policy editor. The path for this setting in the Local Group Policy Editor is Local Computer Policy\Administrative Templates\Classic Administrative Templates (ADM)\Google\Google Chrome.

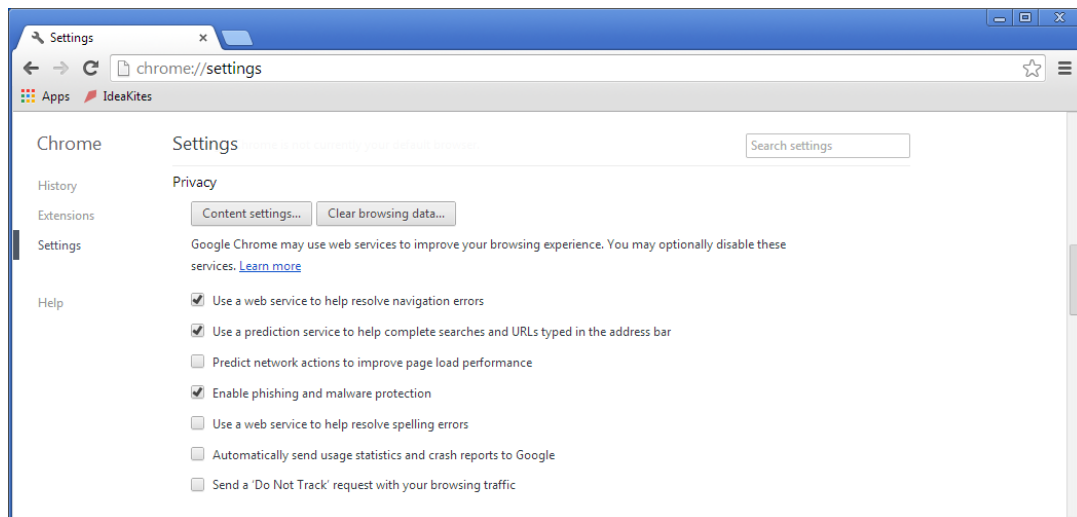


### 5.2.3. Disable 'Predict network actions' in Google Chrome

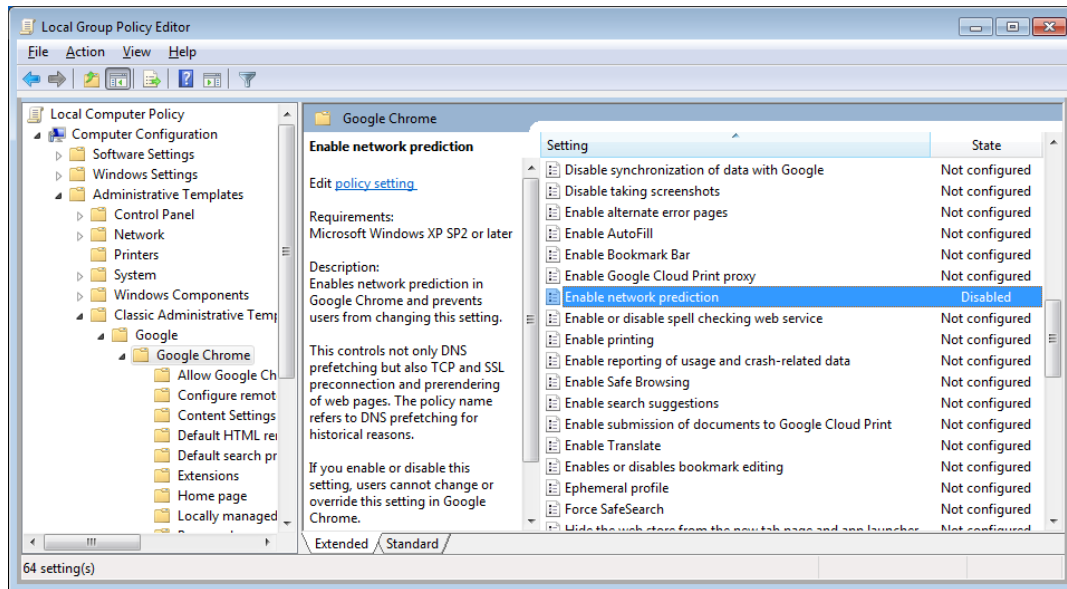
Google Chrome includes a 'predictive' network capability, called "predict network actions", and designed to improve page load performance. This feature pre-fetches pages based on URLs entered into the address bar by the user or instructions coded into a webpage by a website.

When enabled, the predict network actions feature instructs the Chrome browser to download the targeted pages on the user's behalf, without their explicit interaction or having instantiated a navigation event. As a result this feature may cause Catalyst to see 'phantom' navigation requests coming from Chrome for pages already in the Chrome history that match a Catalyst Rule. While these navigation requests may be valid, there is no way for Catalyst to determine which navigation events are issued 'silently' by the predictive feature or those issued intentionally by the user. The result is that a Catalyst navigation may occur while typing an address into the Chrome address bar, even if the ultimate URL would not match a Catalyst rule.

Users of Catalyst should disable the predict network actions feature to avoid false positives that cause Catalyst redirection when a rule would not ultimately be matched. This feature can be disabled manually from the Chrome Settings page, in the Advanced/Privacy section, by unchecking the box next to "Predict network actions to improve page load performance".



IT can centrally manage this setting across a large number of end user PCs, and prohibit users from changing the setting, by installing the Chrome Group Policy templates and disabling the '**Enable network prediction**' policy (a.k.a. `DnsPrefetchingEnabled`).



## 5.3. Managing the Catalyst Extension for Mozilla Firefox

To use Group Policy to manage Firefox, you must first download the GPO for Firefox add-on which can be found at <https://addons.mozilla.org/en-US/firefox/addon/gpo-for-firefox/>.

The next step is to download the ADM(X) template from <http://sourceforge.net/projects/gpofirefox/files/firefox.adm/download>. Once the templates are imported into your Group Policy Editor, you can disable the default browser check as well as other settings you may find useful.

### 5.3.1. Disable Firefox's Default Browser Check via Group Policy

This policy configures the default browser checks in Mozilla Firefox and prevents users from changing them. If you enable this setting, Firefox will not check on startup whether it is the default browser and also will not allow the user to change this setting.

For all users on a PC, the **Disable Firefox Default Browser Check** setting should be "enabled" in your Group Policy editor. The path for this setting is Local Computer Policy\Administrative Templates\Classic Administrative Templates (ADM)\Mozilla Firefox.

This setting will make the following changes to the PC's registry once the policy is propagated:

**Data type:** REG\_DWORD

**Windows registry location:**

HKEY\_LOCAL\_MACHINE\Software\Policies\Firefox\FirefoxCheckDefault

**Example value:** 0x00000001

The value in this case should set be "0"

**Data type:** REG\_SZ

**Windows registry location:**

HKEY\_LOCAL\_MACHINE\Software\Policies\Firefox\FirefoxCheckDefaultType

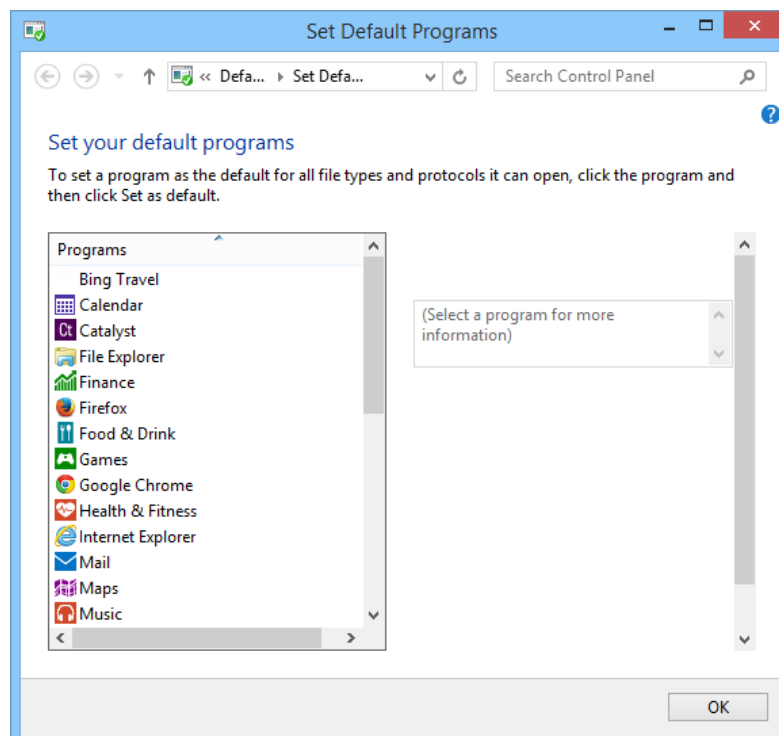
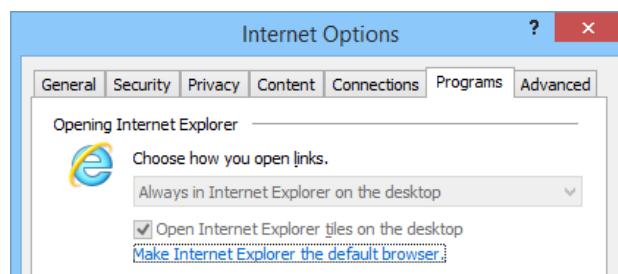
The value in this case should be "Locked"

## 5.4. Ready Windows 8 for Catalyst

Microsoft has made significant changes with Windows 8 that impact the way Catalyst handles certain navigation operations. For Catalyst to work properly in all scenarios, it must be the default browser in Windows.

Prior to Windows 8 (and Windows Server 2012), the Catalyst Controller automatically configured itself as the default browser, or more specifically, the default program for the HTTP, HTTPS and FTP protocols. This enabled Catalyst to direct traffic to the appropriate browser for desktop shortcuts and links to websites in applications, such as email programs.

With Windows 8, Microsoft has blocked applications from programmatically configuring the default browser. Only end users (or IT administrators via Group Policy) can set a default browser. This is even true of Internet Explorer, which can only invoke the Set Default Programs control panel to when selecting Make "Internet Explorer the default browser" from Internet Options.



Because of these new restrictions in Windows 8, default browser settings must be manually configured for Catalyst. The following sections will guide you through this process for two scenarios:

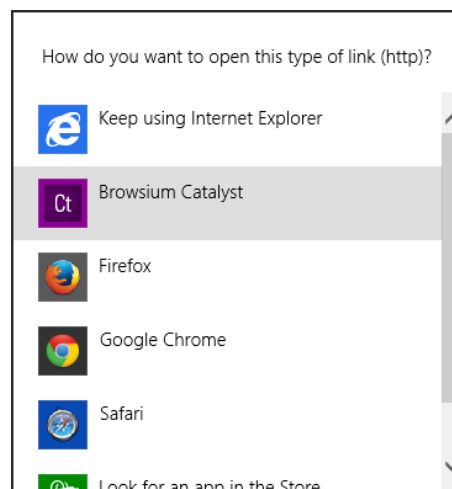
Catalyst Project Development, which includes evaluation and testing of Catalyst

Catalyst Enterprise Deployment, to control the default browser in a managed enterprise

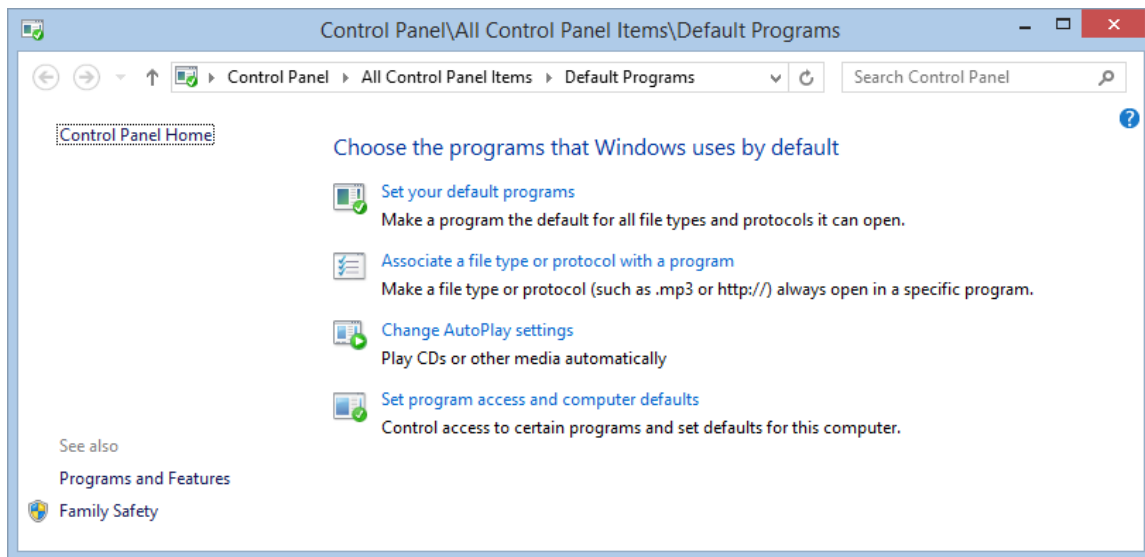
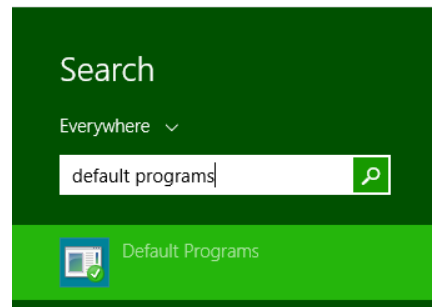
#### **5.4.1. Set Catalyst as Default Browser for Project Development and Testing**

When developing Catalyst projects (or configurations) or simply evaluating Catalyst for future purchase, it's not practical to configure Group Policy to set Catalyst as the default browser on Windows 8. Instead it's much easier to set the default browser using the Default Programs control panel in Windows.

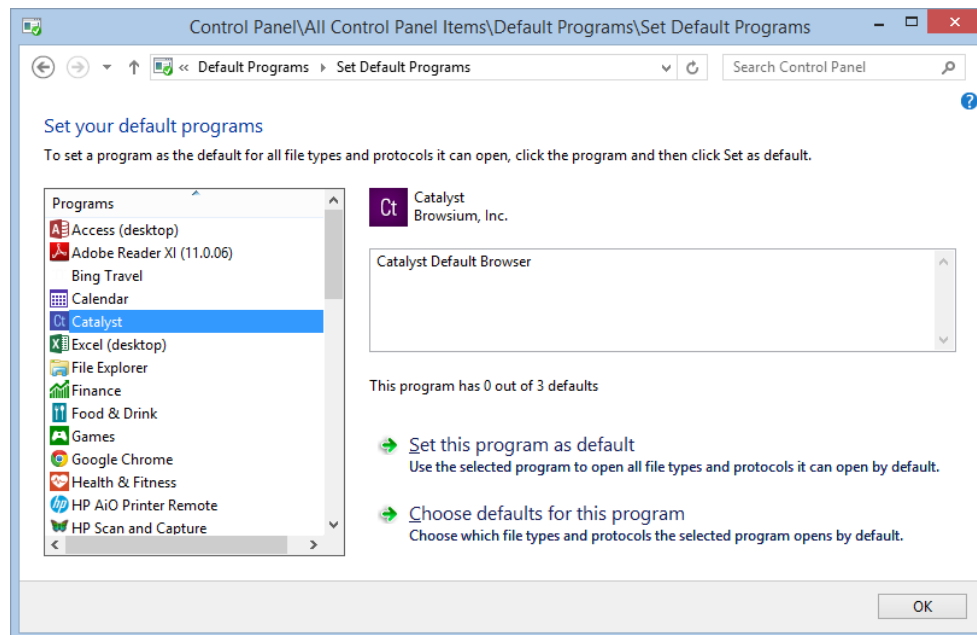
After creating a configuration in Catalyst Configuration Manager and Saving Local Settings for testing, Windows will prompt you to change the default browser. This works in much the same way as Internet Explorer, described in the prior section, but uses a different interface. Windows will directly prompt for a choice of default browser for HTTP (and HTTPS), followed by another prompt for FTP.



To avoid these prompts, and ensure that Catalyst has the defaults it needs, it's best to manually configure Catalyst as the default browser in the control panel. Launch the Default Programs control panel by pressing the Windows key, typing 'default programs' and then pressing enter. (There are many methods for invoking a control panel in Windows 8 – choose the option you're most comfortable with.)

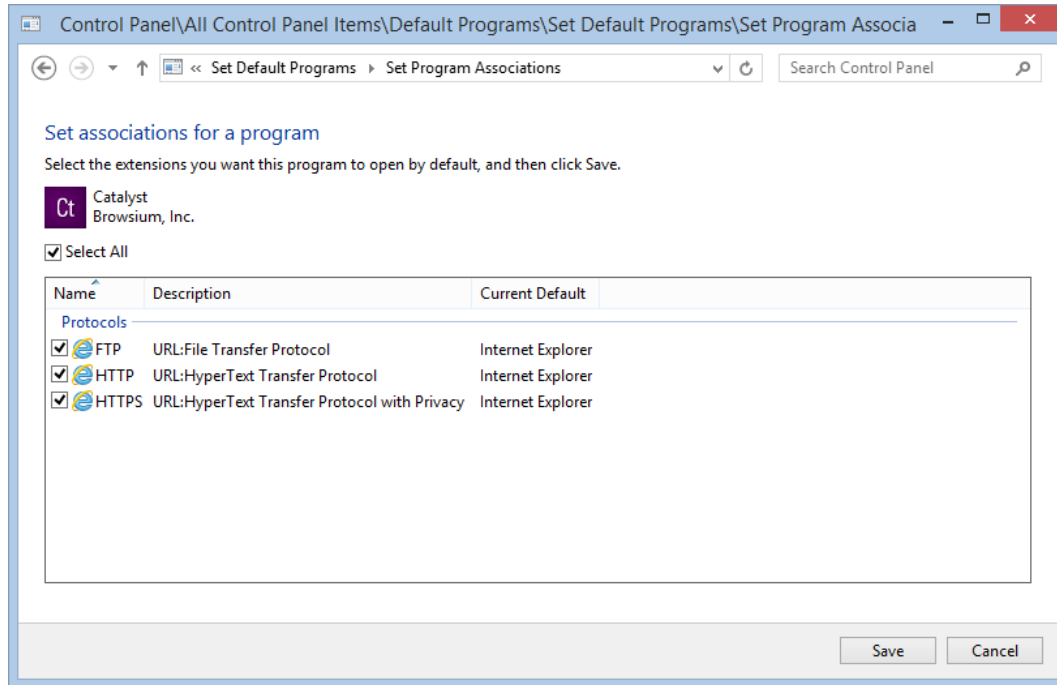


Choose 'Set your default programs' then navigate to the Catalyst Icon.





You'll notice that Catalyst has "0 out of 3 defaults" (if you had not already selected it as the default when starting the Catalyst Controller). You want it to have all 3 defaults – which correspond to HTTP, HTTPS, and FTP. Select the option 'Choose defaults for this program'. Check the box to 'Select all' then click 'Save'



Catalyst will hold these defaults until you change the settings by selecting another browser as the default if prompted. If you plan to continue to use Catalyst, you should not change the default browser, per the guidance earlier in section 5. Catalyst has a built-in fail-safe if the Controller is stopped, either manually or by the Clear Local Settings option in Catalyst Configuration Manager, where it will restore Internet Explorer as the default program for HTTP, HTTPS, and FTP even though the Default Programs control panel still shows Catalyst owning the setting for these protocols.

### 5.4.2. Set Catalyst as Default Browser for Enterprise Deployment

When deploying Catalyst across an enterprise running Windows 8, you will want to use enterprise-class management tools to set Catalyst as the default browser.

Prior to Windows 8, applications could set the default handler for a file type/protocol by manipulating the registry. This means IT could easily have a script or a Group Policy manipulating the registry. For example for the Mailto protocol, you just needed to change the "default" value under HKEY\_CLASSES\_ROOT\mailto\shell\open\command

With Windows 8, this method is no longer available. But Microsoft has introduced a new Group Policy mechanism for declaring these defaults in Windows 8 to accommodate this type of scenario. The basic idea is to have an XML file that maps programs to the file type/protocol that they should be the default for. The following steps provide guidance for configuring and deploying Catalyst as the default browser across an enterprise of Windows 8 systems.

**This guidance is not required for Windows 7 or Windows XP as the Catalyst Controller is able to programmatically take over as the default browser on those systems.**

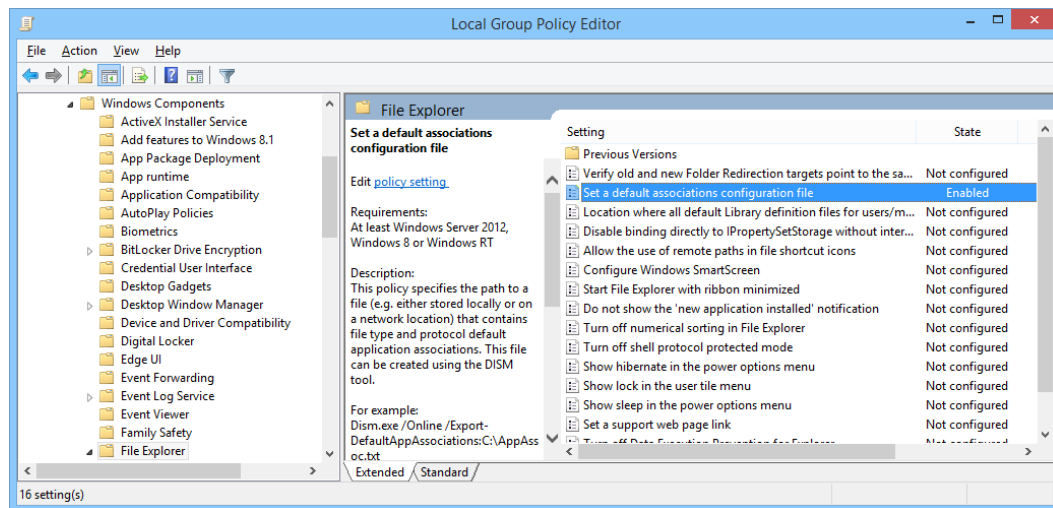
1. Create your XML file or export it from a system which has Catalyst as the default browser using DISM, per [Microsoft's guidance](#). Among the many entries in your XML file, the following association identifiers must point to Catalyst.

```
<?xml version="1.0" encoding="UTF-8"?>
<DefaultAssociations>
  <Association Identifier="FTP" ProgId="CatalystHTML" ApplicationName="Catalyst" />
  <Association Identifier="http" ProgId="CatalystHTML" ApplicationName="Catalyst" />
  <Association Identifier="https" ProgId="CatalystHTML" ApplicationName="Catalyst" />
</DefaultAssociations>
```

2. Use the new Windows 8 Group Policy that enables you to set the association for file types and protocols. Enable the policy "Set a default associations configuration file" found at "Computer configuration\administrative templates\Windows Components\File Explorer". This will set the following registry entry:

```
<HKLM\Software\Policies\Microsoft\Windows\System!DefaultAssociationsConfiguration>
```

This policy specifies the path for the XML file that can be either stored locally or on a network location.



**Using DISM to import the XML is not enough; you must still link it to the Group Policy Object.**

**In addition, the system needs to be domain-joined and the associations are applied at logon time.**



## *Section Six*

# Catalyst Deployment Options

---

In this section you will learn:

- ✓ How to export ADM and ADMX templates from Catalyst
- ✓ How to import Catalyst templates into your environment
- ✓ How to configure Catalyst to use Flat File settings

## 6. Configuration Deployment to End User PCs

Catalyst supports a variety of methods for deploying configurations (Catalyst Settings and Rules) to PCs in an enterprise. In this section, we'll examine these methods and provide recommendations and specific deployment guidance for typical enterprise scenarios.

Catalyst configurations can be deployed across an enterprise via two methods:

- 1) A **Flat File** which contains the entire configuration, formatted as XML, pushed out to a known location on end user PCs or a shared network location; or
- 2) **Serialized registry keys**, where the entire configuration is stored in a set of registry keys which are deployed to end users via Group Policy.

Though the Flat File option doesn't require Group Policy, it does require a pointer to the configuration file in the registry of all end user PCs. The registry preference extension for Group Policy is often the most efficient way to streamline the deployment of this registry key and value.

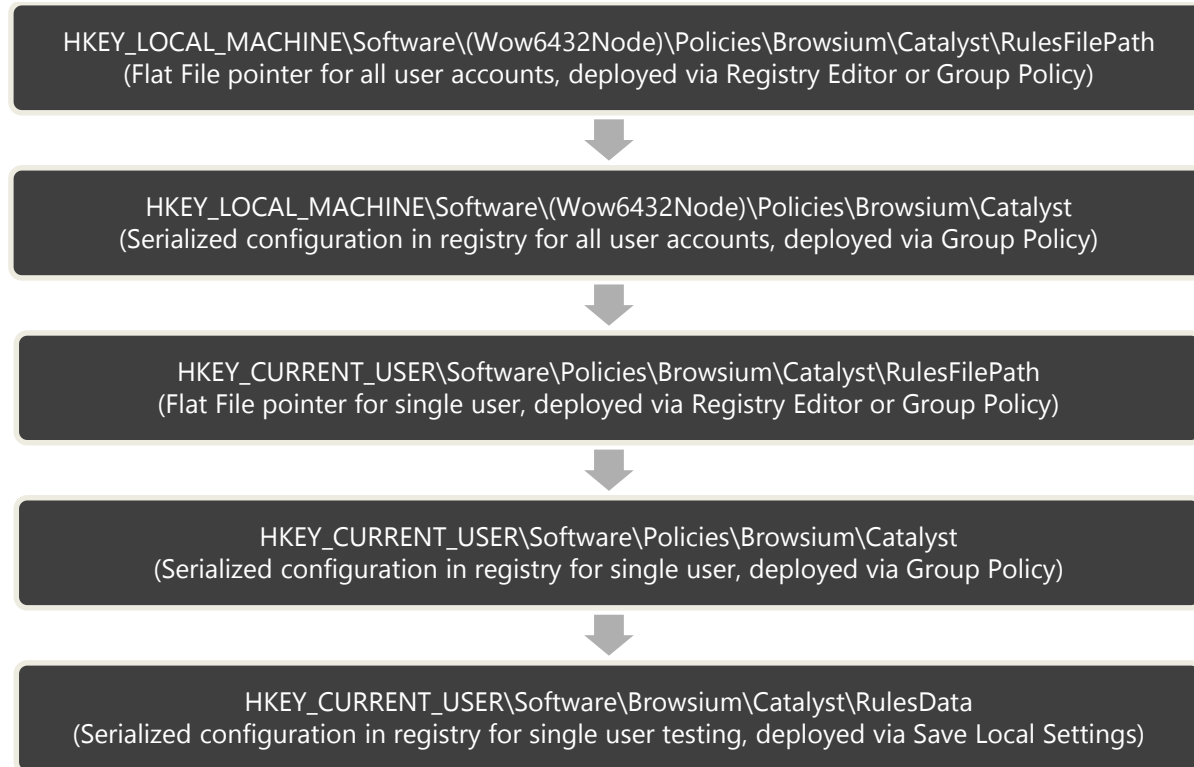
Before we look at Flat File and serialized registry deployments, it is important to understand methodologies for deploying configurations on test systems during configuration development. Catalyst makes it easy to test a configuration without requiring a centralized deployment methodology. This is done via the **Save Local Settings** option from the File menu of Catalyst Configuration Manager.

This option will deploy the configuration into the Windows registry in the HKEY\_CURRENT\_USER hive, immediately restart the Controller to read the configuration, and enable iterative testing of the Settings and Rules without a tedious enterprise deployment process. This method should only be used for testing as it requires manual operation of Catalyst Configuration Manager which should never be made available to end users.

The last concept that must be understood before embarking on a Catalyst deployment is the precedence hierarchy for the evaluation of configurations when multiple configurations are found on a system. Catalyst follows this hierarchy to load the configuration that will be used on a given end user system (and on test systems). Once a valid configuration is found, Catalyst will stop searching and that configuration will be used.

**Deploying different Catalyst configurations using multiple methodologies on a single PC may cause unpredictable results as only the configuration highest in the hierarchy will be in use.**

The following table provides the hierarchy of Catalyst configuration precedence. The string “(Wow6432Node)” in the registry path denotes the Wow6432Node registry key that will be included in the path on 64-bit Windows systems. 32-bit Windows systems do not contain this key, hence the use of parentheses in the example.



Two additional locations can reference Flat Files in RulesFilePath for Catalyst. These are HKEY\_CURRENT\_USER\\Software\\Browsium\\Catalyst\\RulesFilePath and HKEY\_LOCAL\_MACHINE\\Software\\(Wow6432Node)\\Browsium\\Catalyst\\RulesFilePath. However, these locations are not robust as they are deleted from the registry when Catalyst is uninstalled (which may occur during a version upgrade). Browsium recommends using the Policies key for Flat File deployments, whether via Group Policy or a registry script. More on this in [section 6.1](#).

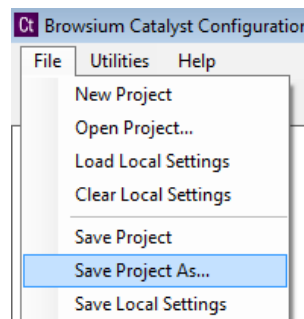
Given the options available for Catalyst configuration deployment, it's not uncommon to deploy multiple configurations and lose track of which configuration is active. To ease troubleshooting, the Catalyst Controller provides a command-line function to query the local system and identify the location of the configuration currently in use. The command "Controller.exe /WhichConfig" can be run from a standard Command Prompt. Details on its usage are [section 6.3](#).

## 6.1. Deploying via Flat Files

Browsium recommends that Catalyst configurations be deployed via Flat File. Configuration are standard XML documents, allowing you to take full advantage of this versatile and very compact format. Configurations are easy to update by simply replacing the Flat File on end user systems or a network share. This is in contrast to deploying configurations serialized in the registry via Group Policy (detailed in [section 6.2](#)) which adds unnecessary complexity and limitations to managing a Catalyst deployment.

However, Catalyst will not look for a Flat File configuration by default. You must configure each client system to look for a Flat File configuration. But this only needs to be done once, no matter how often the Flat File is updated – provided the file name and file location is not changed. The following steps provide guidance to enable Catalyst to read its configuration from a Flat File.

First, save your project as a .CAX file using the File / Save Project (or Save Project As...) menu in the Catalyst Configuration Manager.



Next, instruct Catalyst to load the configuration file you just saved using the Flat File method. To do this, you must edit the system registry manually (for local testing) or via a script or Group Policy (for remote deployment). Browsium recommends using the [registry preference extension for Group Policy](#) as the most efficient way to streamline deployment of this registry key/value.

The Catalyst project file (.cax) must be stored in a user-readable location on the local PC or a network share – local PC recommended as Catalyst will not start if the network is unavailable at user logon. You will enter that specific location in the RulesFilePath registry value. You must define the RulesFilePath value for either per-user settings (which will enable the configuration for a single user account on the system), or per-machine settings (which will enable the configuration for all user accounts on the system).

**Loading a configuration from a network location will cause the Catalyst Controller to not start if the network share is unavailable at user logon.**

The following registry keys and associated values must be created, depending on the system and user accounts being targeted:

For **per-user** settings on **32-bit and 64-bit** Windows systems, find or create:

HKEY\_CURRENT\_USER\Software\Policies\Browsium\Catalyst

For **per-machine** settings on **32-bit** Windows systems, find or create:

HKEY\_LOCAL\_MACHINE\Software\Policies\Browsium\Catalyst

For **per-machine** settings on **64-bit** Windows systems, find or create:

HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Policies\Browsium\Catalyst

Then create or populate the following String Value in the Catalyst key:

RulesFilePath (REG\_SZ) = C:\directory\... [the path to your Catalyst project file (.cax)]

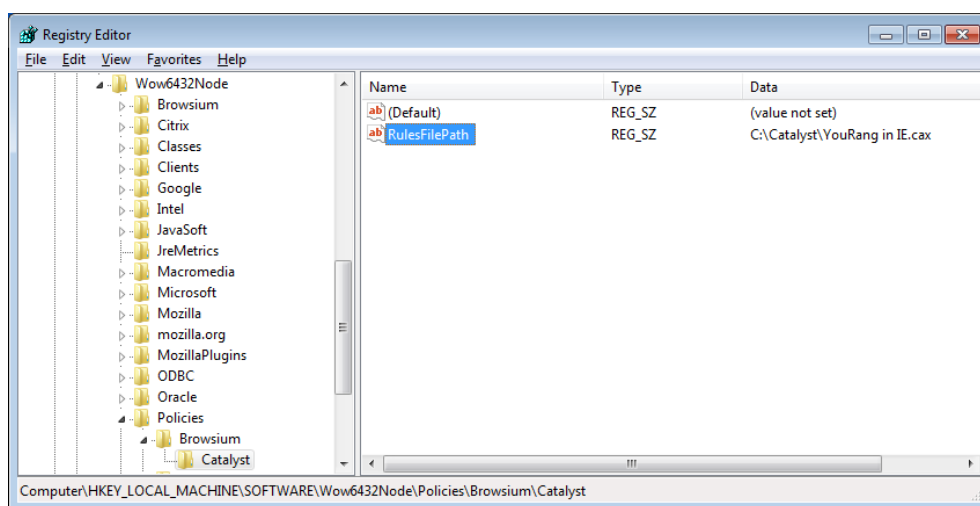
**Slashes in the file path must be escaped with a slash when invoking Regedit.exe via a .reg file. So c:\directory becomes c:\\directory in the registry value. Similarly, '\\server\share' becomes '\\\\server\\share'.**

In the following example, RulesFilePath has been configured to use the file "YouRang in IE.cax" in the C:\Catalyst directory for all users on a 64-bit Windows system. These entries can be scripted and delivered to the registry on remote clients via Registry Preference Extensions for Group Policy or via the following text in a .reg file.

Windows registry Editor Version 5.00

[HKEY\_LOCAL\_MACHINE\Software\Wow6432Node\Policies\Browsium\Catalyst]

"RulesFilePath"="C:\\Catalyst\\YouRang in IE.cax"



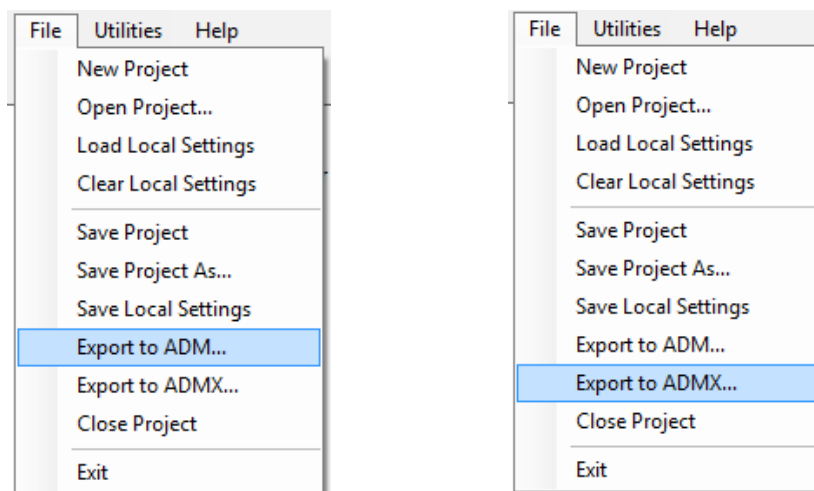


## 6.2. Deploying via Serialized Registry Keys

Using serialized registry keys to deploy Catalyst configurations requires the creation of ADM or ADMX files that contain the Catalyst Rules and Settings. These will then be used by your Group Policy infrastructure to push the configuration to end user PCs.

**Browsium recommends deploying Catalyst configurations using Flat Files and not serialized registry keys due to limitations and complexity of the ADM and ADMX architectures. This feature will be deprecated in an upcoming release of Catalyst.**

Creating the ADM or ADMX files containing the Catalyst configuration can be easily done within the Catalyst Configuration Manager. After creating and testing the Catalyst project, export the project by selecting “Export to ADM...” or “Export to ADMX...” from the File menu.



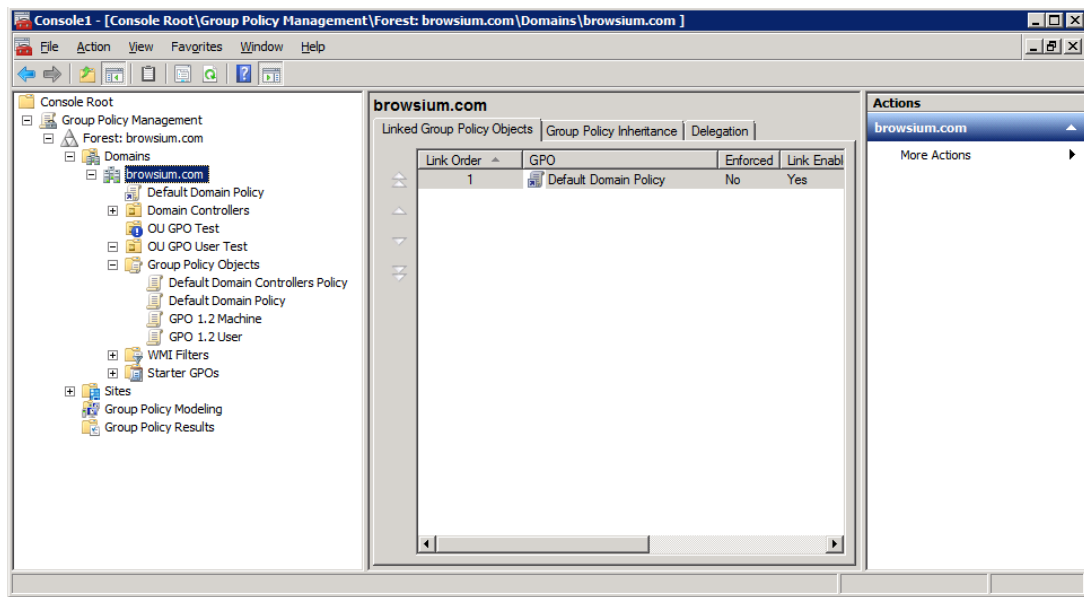
**You will choose between using ADM and ADMX depending on the Windows, Windows Server, and Active Directory environment within your organization. Microsoft has published detailed guidance to help you decide.**

**For the purposes of this guide, we will assume you have chosen ADM.**

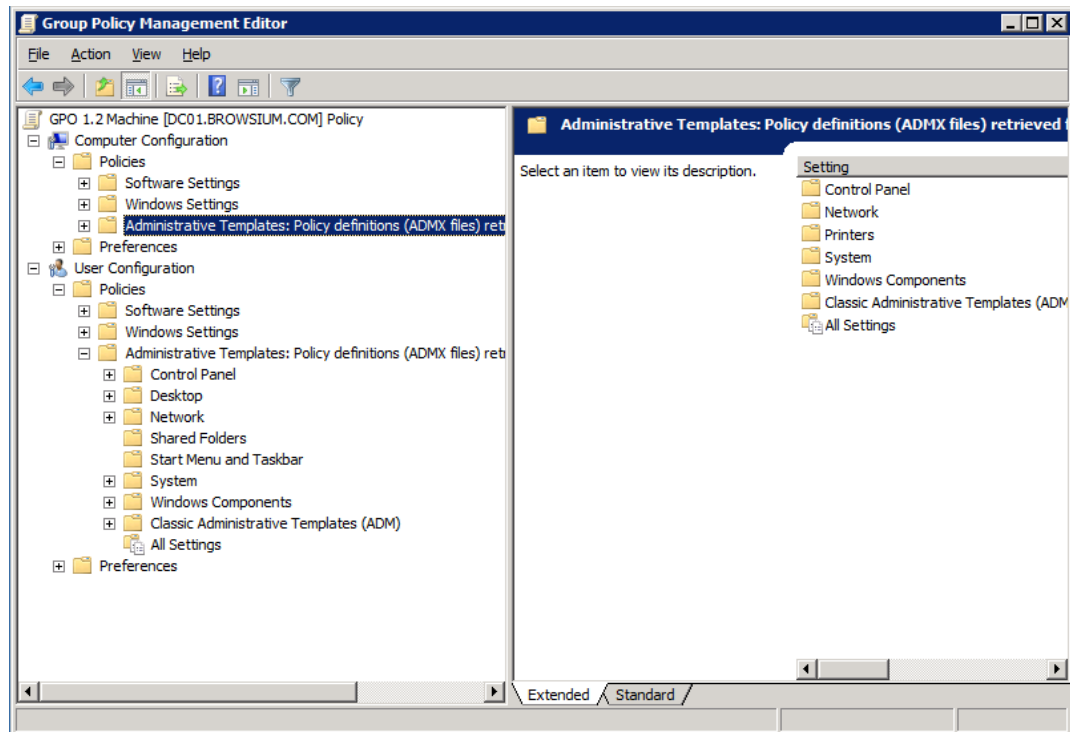
Once you have exported and named your ADM file, transfer the file to a Domain Controller or a system running Group Policy Manager.

**Catalyst Configuration Manager always exports the file as Catalyst.adm. If the target directory already contains a file of the same name, the export will silently overwrite the file. However, exporting to ADM or ADMX with configuration changes that have not yet been committed (by navigating to another screen in Catalyst Configuration Manager) are not written to the resulting ADM or ADMX files. Save Local Settings and Save Project both automatically commit all current changes before saving.**

Launch the Group Policy Manager, create a new Group Policy Object and set permissions to it.



Right click the newly created Group Policy Object, select 'edit' to launch the Group Policy Editor.



Open the Computer Configuration > Policies node, then right click on Administrative Templates item. Choose the Add/Remove Templates option and select the ADM file exported from the Catalyst Configuration Manager above.

Now expand the Classic Administrative Templates folders under Machine and User Configuration and expand the Catalyst Folder. You will see folders named *Settings and Rules*. Open up each item in these folders and Enable them.

**Catalyst Policies are not enabled by default. They must be 'Enabled' individually. Use the 'Not Configured' setting if you do not want to use one or more of the Settings or Rules.**

**In addition, always make changes to Rules and Settings in the Catalyst Configuration Manager and not in the Group Policy Editor.**

As soon as your policies are updated on client systems, and the Catalyst Controller is started, your Catalyst configuration will be in effect. It is possible to script the starting of the Catalyst Controller, but the script must run in User, not System, context. Browsium recommends restarting the systems or waiting until the next time users log into their systems. The Catalyst Controller starts automatically upon login, provided it finds a valid configuration within the hierarchy. See the opening of section 6 for a refresher on the Catalyst configuration hierarchy.

### 6.2.1. A Few Words About ADMX

If you've chosen to deploy with .ADMX files instead of .ADM files, you'll need to alter your deployment steps as follows:

Once you've completed the ADMX export, you will have two files – Catalyst.admx and Catalyst.adml. Rename these files for your needs and copy them to a Domain Controller.

**Catalyst Configuration Manager always exports the file as Catalyst.admx and Catalyst.adml. If the target directory already contains a file of the same name, the export will silently overwrite the file. However, exporting to ADM or ADMX with configuration changes that have not yet been committed (by navigating to another screen in Catalyst Configuration Manager) are not written to the resulting ADM or ADMX files. Save Local Settings and Save Project both automatically commit all current changes before saving.**

On the Domain Controller, place the ADMX file in C:\Windows\PolicyDefinitions. Place the ADML file in C:\Windows\PolicyDefinitions\en-US. Placing the files in these locations will automatically create a new template within your Group Policy Manager.

Launch the Group Policy Manager and locate the Catalyst folder within the Default Domain Policy under Administrative Templates: Policy Definitions (ADMX files). Open up each item in these folders and set them to 'Enabled'.

**Catalyst Policies are not enabled by default. They must be 'Enabled' individually. Use the 'Not Configured' setting if you do not want to use one or more of the Settings or Rules. Setting the value to Disabled may cause unexpected impacts on client load behavior.**

As with ADM, your policies will now be pushed out to end user systems and your Catalyst configuration will be in effect the next time the Catalyst Controller is started.

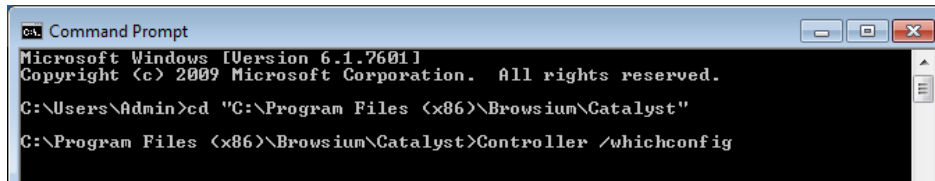
## 6.3. Query the Active Configuration with WhichConfig

The Catalyst Controller provides a command-line function to query the local system and identify the location of the configuration currently in use. The command is "Controller /WhichConfig" and can be run from a standard Command Prompt.

In the following example, a Flat File configuration has been deployed to HKEY\_LOCAL\_MACHINE\Policies\Wow6432Node\Browsium\Catalyst with the value "C:\Catalyst\YouRang in IE" stored in RulesFilePath.

**Note that the query uses registry reflection and therefore the result ignores the Wow6432Node key on 64-bit Windows systems although it is in the path of the registry key value containing the Flat File pointer.**

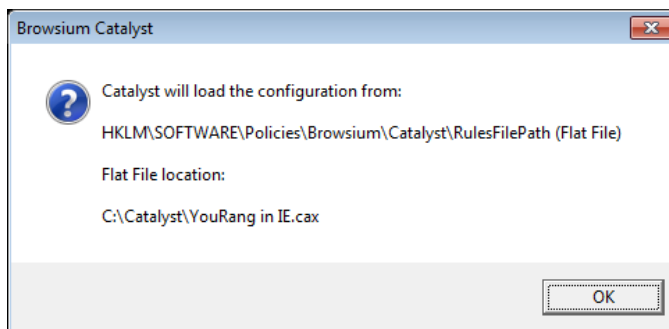
Executing this command ...



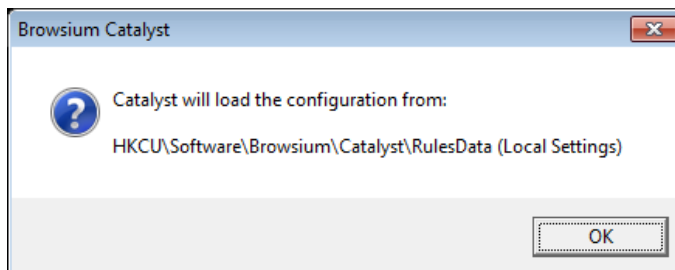
```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Admin>cd "C:\Program Files (x86)\Browsium\Catalyst"
C:\Program Files (x86)\Browsium\Catalyst>Controller /whichconfig
```

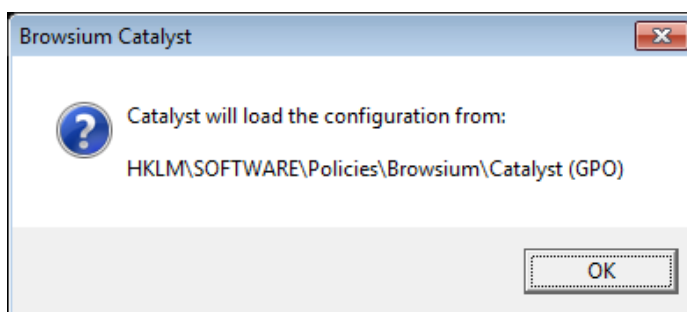
... results in the configuration acknowledge as:



Configurations serialized into the registry via Save Local Settings are acknowledged as:



Configurations serialized into the registry via ADM or ADMX and Group Policy are acknowledged as:





*Appendix A*

## Appendix A: Troubleshooting

---

In this section you will learn:

- ✓ How to Recognize Issues with a Catalyst Configuration
- ✓ What to do When Catalyst is Not Working as Expected

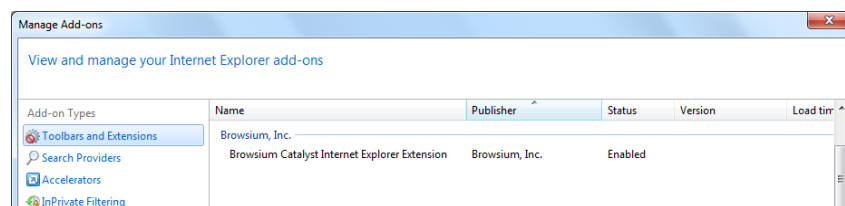
# A. Troubleshooting

## A.1. Catalyst Rule Fails To Engage

You may encounter a scenario in which Catalyst fails to engage on one or more websites based on rules you've created.

The following points may guide you to a resolution:

- **Review System Prerequisites**
  - Check to see that the target computer meets the performance and storage requirements to run Catalyst.
- **Confirm the Catalyst Executable Files are Running**
  - Check to see that the Catalyst Controller (**Controller.exe**) is running on the target machine.
- **Ensure the Catalyst Extensions are Enabled and Running**
  - Confirm the Browsium Catalyst Client extensions are seen and loaded by Internet Explorer, Chrome and Firefox
    - Open each browser and open the Manage Add-Ons/Extensions dialog. Do you see the Catalyst client extension installed? Is it enabled?
    - For example, An Internet Explorer instance that correctly loads the Catalyst Client extension will display the following information in the Manage Add-Ons dialog:



- **Visit the Knowledge Base or Contact Support**
  - If all of these steps fail, consider searching the [Browsium Catalyst Knowledge Base](#).
  - If you have a support contract, contact your systems integrator, or [Browsium Support](#) for one-on-one guidance.

## A.2. Browser Window Doesn't Get Focus Automatically

Some users may experience 'focus' issues where a web page or web application loads and the user is unable to interact with the browser window automatically. This issue is related to how Windows provides focus control (the ability to receive input). Users will need to click inside the browser tab window to ensure proper focus.

## A.3. Catalyst Doesn't Take Over Default Browser on Windows 8

Microsoft made a change in Windows 8, and no longer allows 3<sup>rd</sup> party software to programmatically take over as the default browser. As Catalyst must be the default browser to manage navigation through all entry points for HTTP, HTTPS, and FTP, it must be set as the default by end users or via Group Policy. See [section 5 of this guide](#) for details on how to control browser defaults on Windows 8.

## A.4. The Controller Becomes Unresponsive

Restart the Controller process ([Controller.exe](#)) by using the Utilities menu in the Catalyst Configuration Manager.