Browsium Catalyst 1.0
Administration Guide

browsium

Bonding Browsers to Business
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 1.0.3.

For more information about Browsium Catalyst, other Browsium products, or to contact Browsium Support, please visit www.browsium.com.

Table of Contents

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 Browser Extensions

The Catalyst Configuration Manager is the main interaction point for IT administrators using the Catalyst system. The Catalyst system 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 Browsium Catalyst system supports extensions for three browsers – the installed version of Internet Explorer, Google Chrome 22 (or later) and Firefox 15 (or later). This release supports the ability to define and configure additional versions of the browsers from these three vendors. Once the Catalyst Client has been installed on a system, the Catalyst Controller process will load at user logon and read the configuration information from the system.

Catalyst supports both local and group policy managed settings to provide the most flexibility and truly deliver an enterprise ready testable 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 loaded.

This is the power of Catalyst: You control which browser is allowed, and which are not. Only the sites you configure with the Catalyst Configuration Manager are displayed using the Catalyst redirection process. We invite you to put Catalyst through the paces, deploy to some end user test machines and validate support for exporting Rules and configurations settings via Group Policy, or distribute them as flat files (in an easy to read XML format) to ensure interoperability with virtually any software management infrastructure.

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 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

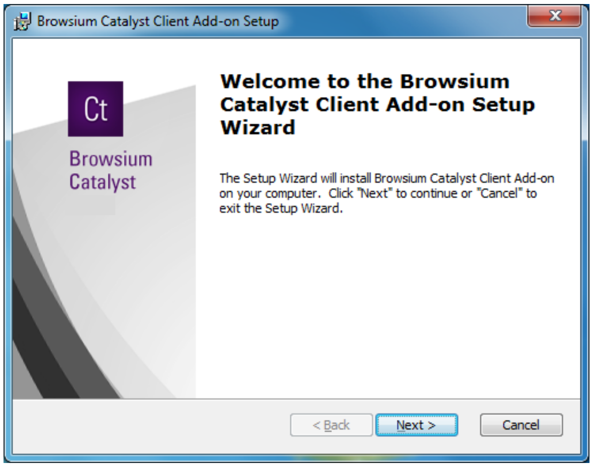
The following minimum system specifications are required to run the Catalyst system.

- Microsoft Windows System
    - Windows XP SP3 (32-bit only)
    - Windows 7 SP1 (32- and 64-bit systems are supported)
    - Windows Server 2003 (32- and 64-bit systems are supported)
    - Windows Server 2008 R2
- Microsoft Windows Internet Explorer 6, 7, 8, 9, or 10
- Google Chrome 22 (or later)
- Mozilla Firefox 15 (or later)
- .NET Framework Version 3.5 (or later)
- 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.

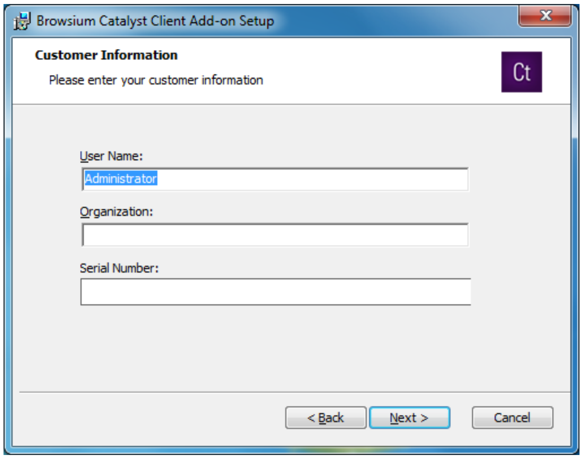
1. To start the Client Installer process, simply double-click on the Catalyst-ClientSetup.msi file provided by Browsium. To properly complete the installation process you will need an account with Administrator rights. The first screen provides a basic introduction. Click Next to get started.



Welcome to the Browsium Catalyst Client Add-on Setup Wizard

The Setup Wizard will install Browsium Catalyst Client Add-on on your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

2. Now enter your Name, Organization and License Key (Serial Number)



Customer Information

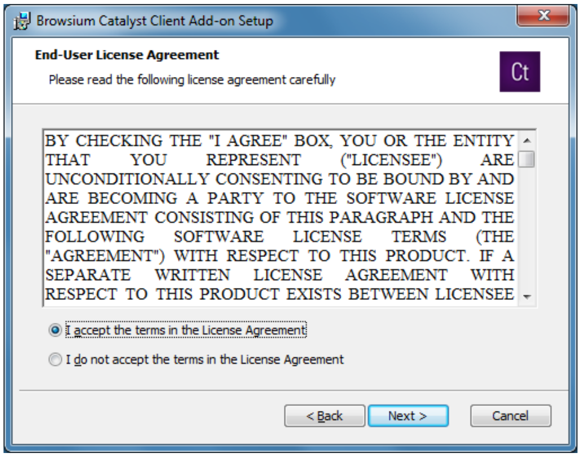
Please enter your customer information

User Name: Administrator

Organization:

Serial Number:

3. 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.



End-User License Agreement

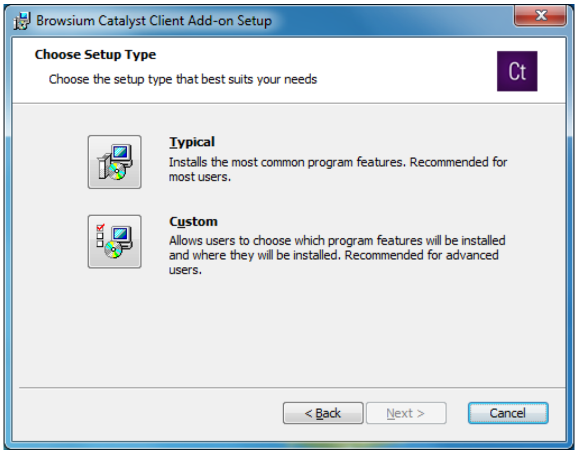
Please read the following license agreement carefully

BY CHECKING THE "I AGREE" BOX, YOU OR THE ENTITY THAT YOU REPRESENT ("LICENSEE") ARE UNCONDITIONALLY CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THE SOFTWARE LICENSE AGREEMENT CONSISTING OF THIS PARAGRAPH AND THE FOLLOWING SOFTWARE LICENSE TERMS (THE "AGREEMENT") WITH RESPECT TO THIS PRODUCT. IF A SEPARATE WRITTEN LICENSE AGREEMENT WITH RESPECT TO THIS PRODUCT EXISTS BETWEEN LICENSEE

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

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



Choose Setup Type

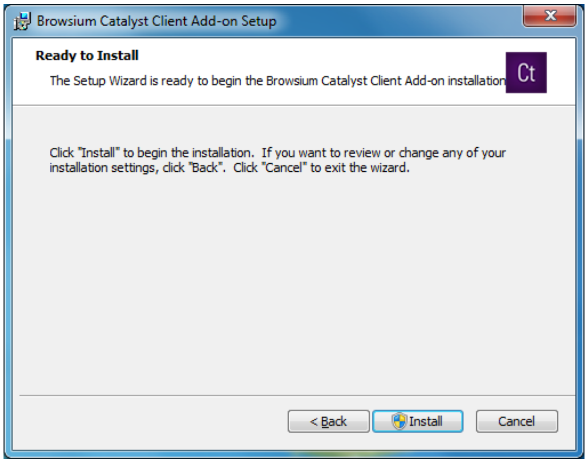
Choose the setup type that best suits your needs

Typical
Installs the most common program features. Recommended for most users.

Custom
Allows users to choose which program features will be installed and where they will be installed. Recommended for advanced users.

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

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



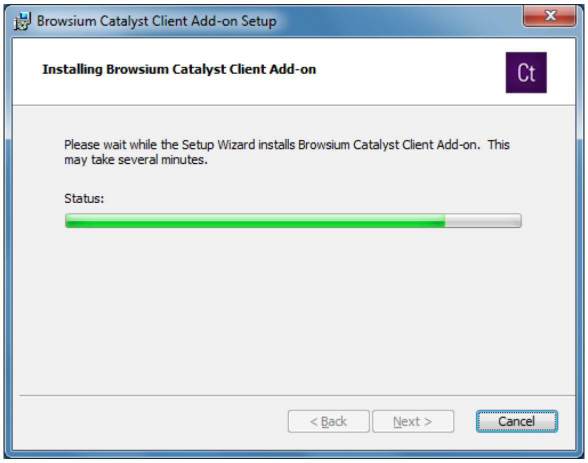
Ready to Install

The Setup Wizard is ready to begin the Browsium Catalyst Client Add-on installation

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

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.

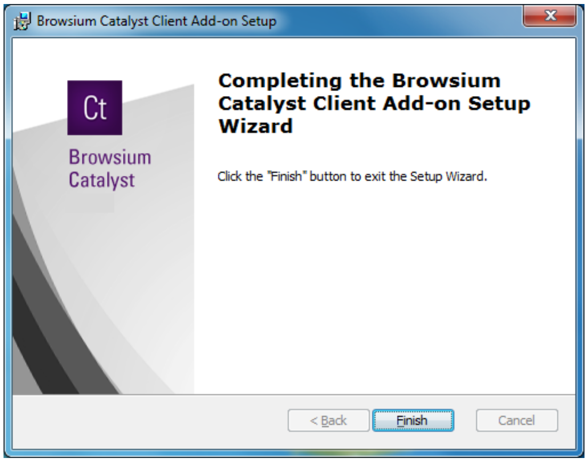
During the process you will see a progress bar:



Installing Browsium Catalyst Client Add-on

Please wait while the Setup Wizard installs Browsium Catalyst Client Add-on. This may take several minutes.

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

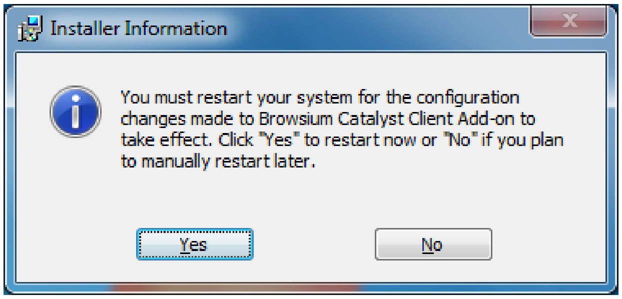


Completing the Browsium Catalyst Client Add-on Setup Wizard

Click the "Finish" button to exit the Setup Wizard.

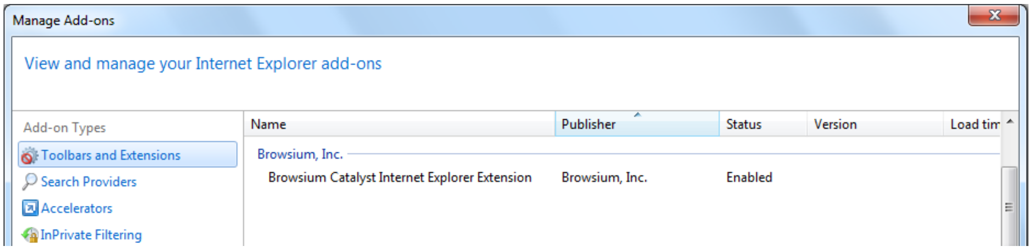
6. After clicking ‘Finish’ you will be prompted to restart the system.

   This step is required to ensure each browser is closed and properly restarted with the Catalyst add-on running. Attempting to install the Catalyst add-on without a restart may result in unexpected behavior.



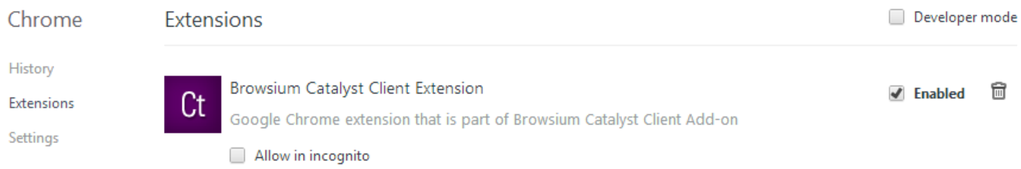
You must restart your system for the configuration changes made to Browsium Catalyst Client Add-on to take effect. Click "Yes" to restart now or "No" if you plan to manually restart later.

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.



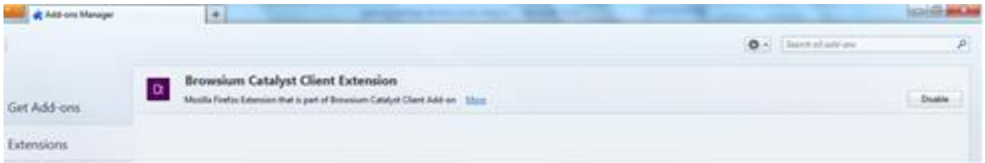
Name	Publisher	Status	Version	Load tim
Browsium, Inc.				
Browsium Catalyst Internet Explorer Extension	Browsium, Inc.	Enabled		

Do the same for Chrome and Firefox.



Browsium Catalyst Client Extension

Google Chrome extension that is part of Browsium Catalyst Client Add-on



Browsium Catalyst Client Extension

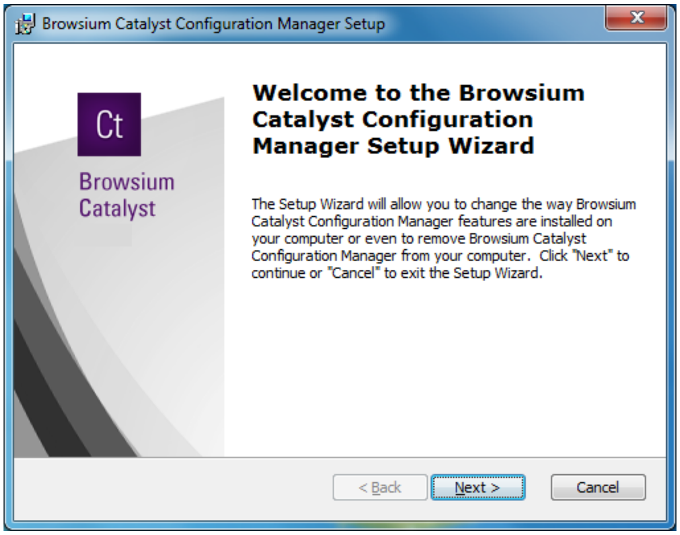
Mozilla Firefox Extension that is part of Browsium Catalyst Client Add-on More

2.4. Installing Browsium Catalyst Configuration Manager

This section covers the installation process for the Browsium Catalyst Configuration Manager. The Browsium Catalyst Client should be installed on the system in order to properly use the Catalyst Rules system.

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

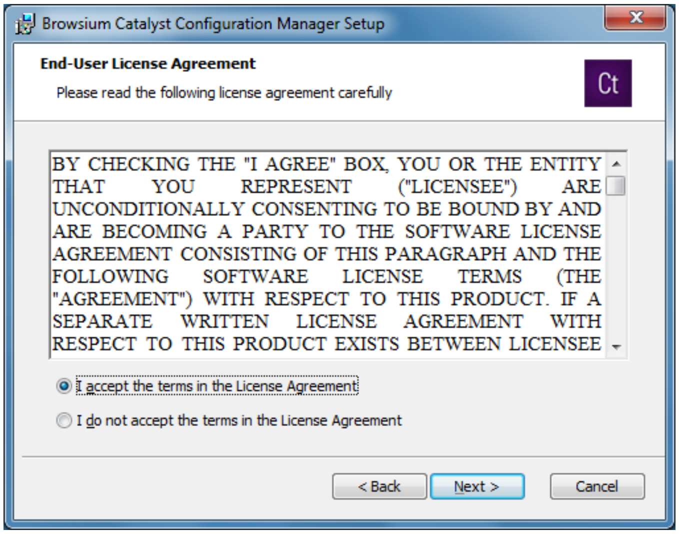
1. Locate the Catalyst Configuration Manager Installation file (***Catalyst-AdminSetup.exe***) and double click to run the program.



Welcome to the Browsium Catalyst Configuration Manager Setup Wizard

The Setup Wizard will allow you to change the way Browsium Catalyst Configuration Manager features are installed on your computer or even to remove Browsium Catalyst Configuration Manager from your computer. Click "Next" to continue or "Cancel" to exit the Setup Wizard.

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.



Browsium Catalyst Configuration Manager Setup

End-User License Agreement

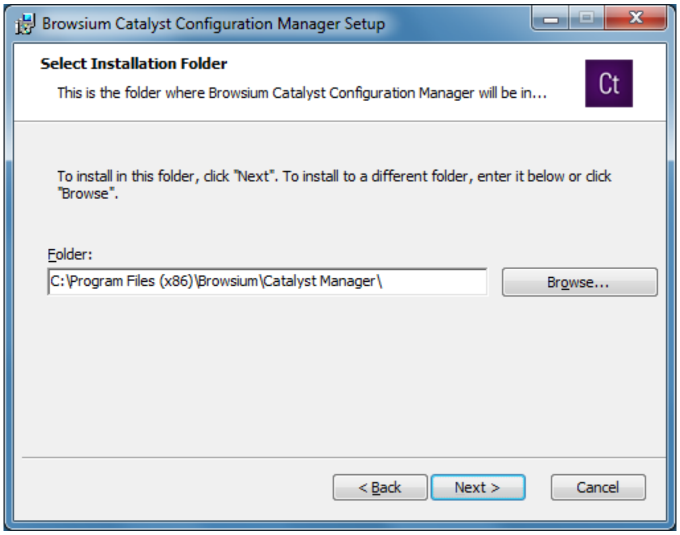
Please read the following license agreement carefully

BY CHECKING THE "I AGREE" BOX, YOU OR THE ENTITY THAT YOU REPRESENT ("LICENSEE") ARE UNCONDITIONALLY CONSENTING TO BE BOUND BY AND ARE BECOMING A PARTY TO THE SOFTWARE LICENSE AGREEMENT CONSISTING OF THIS PARAGRAPH AND THE FOLLOWING SOFTWARE LICENSE TERMS (THE "AGREEMENT") WITH RESPECT TO THIS PRODUCT. IF A SEPARATE WRITTEN LICENSE AGREEMENT WITH RESPECT TO THIS PRODUCT EXISTS BETWEEN LICENSEE

● I accept the terms in the License Agreement

○ I do not accept the terms in the License Agreement

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.



Browsium Catalyst Configuration Manager Setup

Select Installation Folder

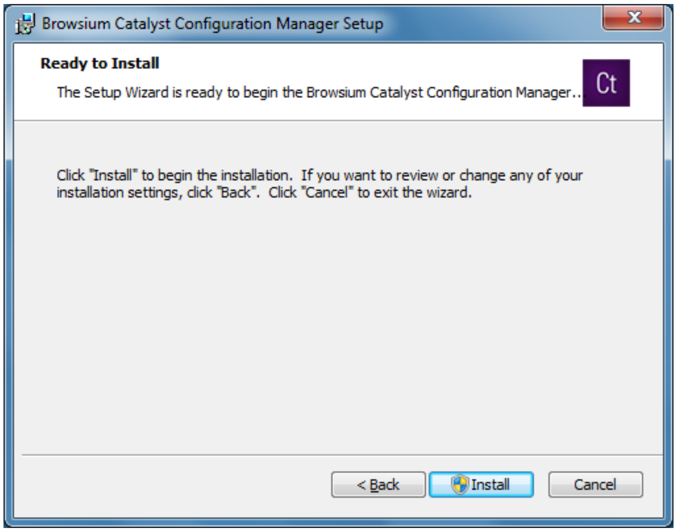
This is the folder where Browsium Catalyst Configuration Manager will be in...

To install in this folder, click "Next". To install to a different folder, enter it below or click "Browse".

Folder:
C:\Program Files (x86)\Browsium\Catalyst Manager\

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

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



Browsium Catalyst Configuration Manager Setup

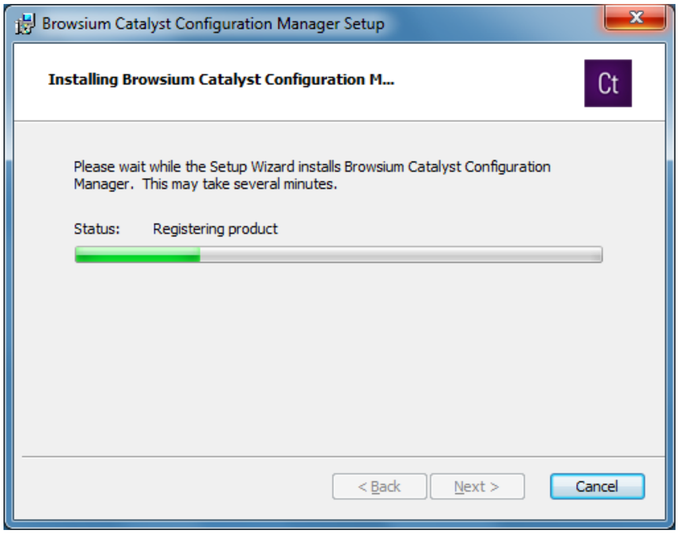
Ready to Install

The Setup Wizard is ready to begin the Browsium Catalyst Configuration Manager..

Click "Install" to begin the installation. If you want to review or change any of your installation settings, click "Back". Click "Cancel" to exit the wizard.

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



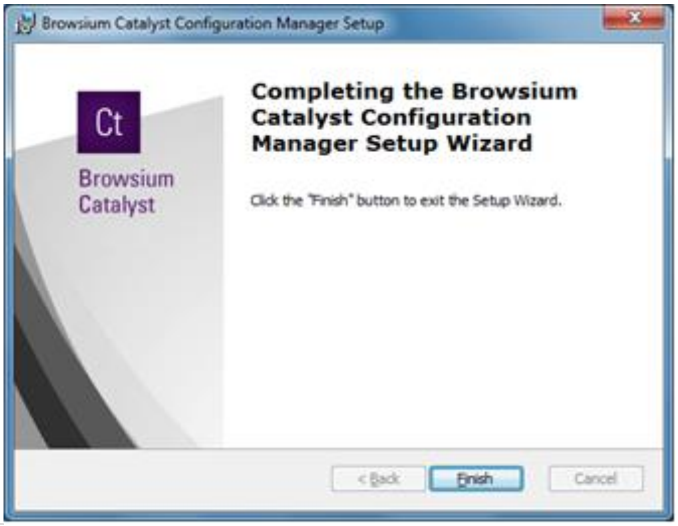
Browsium Catalyst Configuration Manager Setup

Installing Browsium Catalyst Configuration M...

Please wait while the Setup Wizard installs Browsium Catalyst Configuration Manager. This may take several minutes.

Status: Registering product

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 the Catalyst system.



Completing the Browsium Catalyst Configuration Manager Setup Wizard

Click the "Finish" button to exit the Setup Wizard.

Section Three

Introduction to the Catalyst Configuration Manager

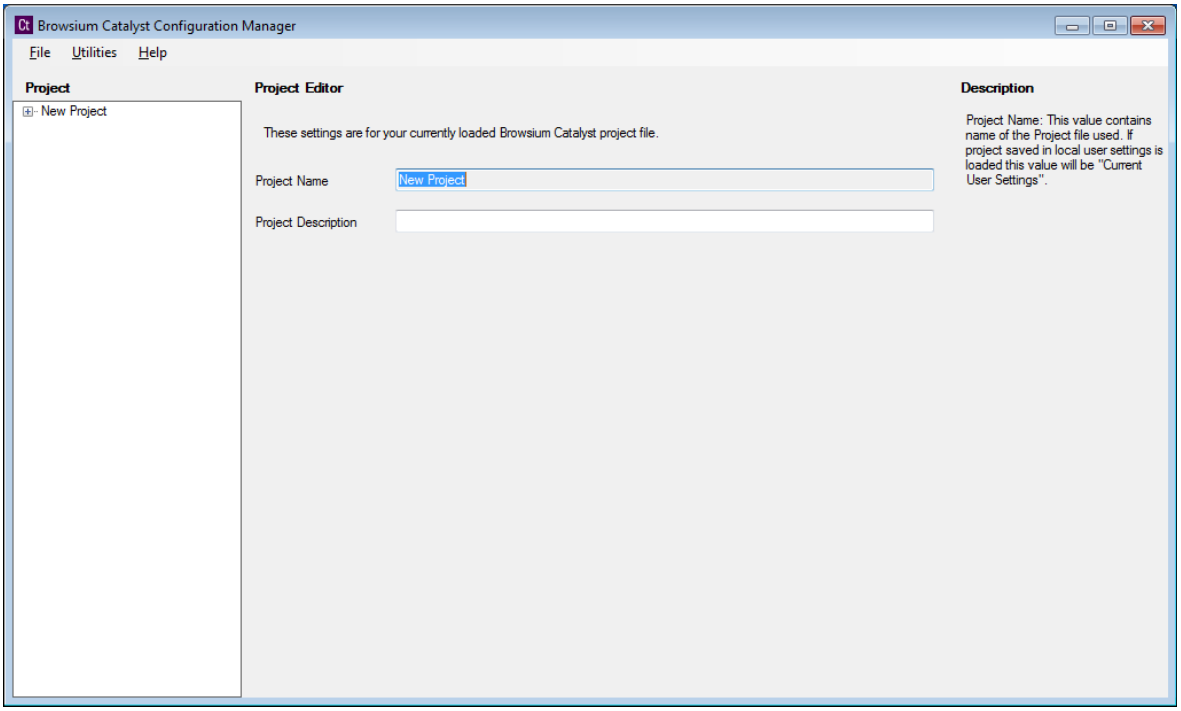
In this section you will learn:

✓ 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



These settings are for your currently loaded Browsium Catalyst project file.

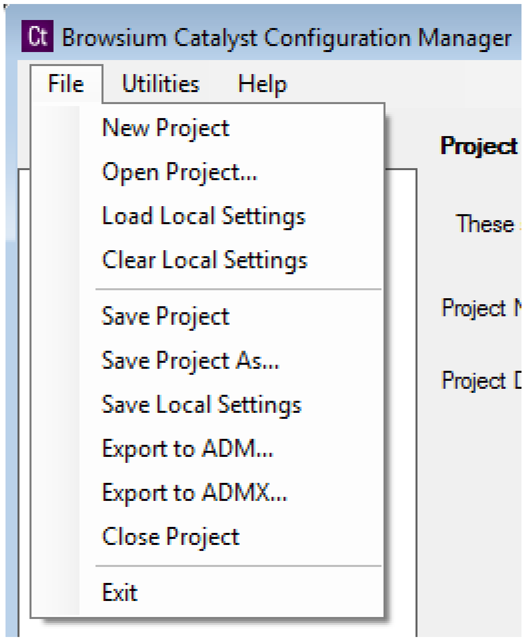
Project Name: New Project

Project Description:

Project Name: This value contains name of the Project file used. If project saved in local user settings is loaded this value will be "Current User Settings".

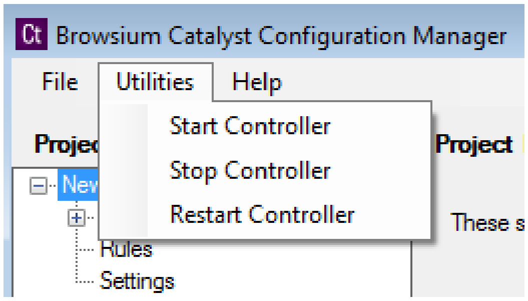
3.1. Menu Bar

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.



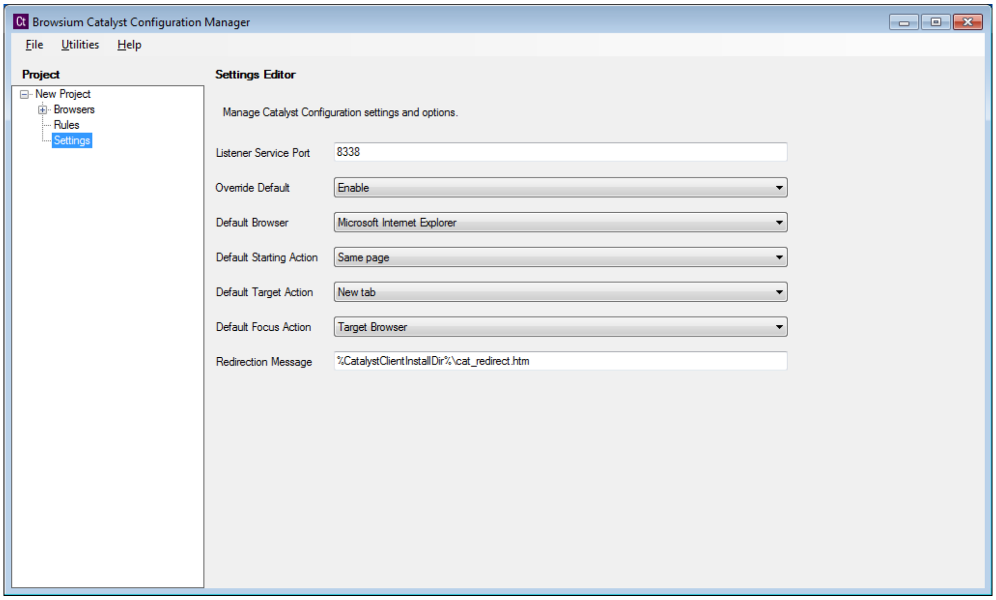
To aid in configuration testing and tuning, the Catalyst Configuration Manager allows Administrators to apply settings directly in the local system registry. Organizations should use the Save Local Settings option for rapid local testing. This option reduces delays and overhead of exporting settings to Group Policy by applying those settings and forcing the local machine to reload policy values. Catalyst will support saving settings to either the Current User (HKCU) or Local Machine (HKLM) based on the needs of your organization and whichever choice properly replicates the target client system settings for your organization.

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.



Settings Editor

Manage Catalyst Configuration settings and options.

Listener Service Port: 8338
Override Default: Enable
Default Browser: Microsoft Internet Explorer
Default Starting Action: Same page
Default Target Action: New tab
Default Focus Action: Target Browser
Redirection Message: %CatalystClientInstallDir%\cat_redirect.htm

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.

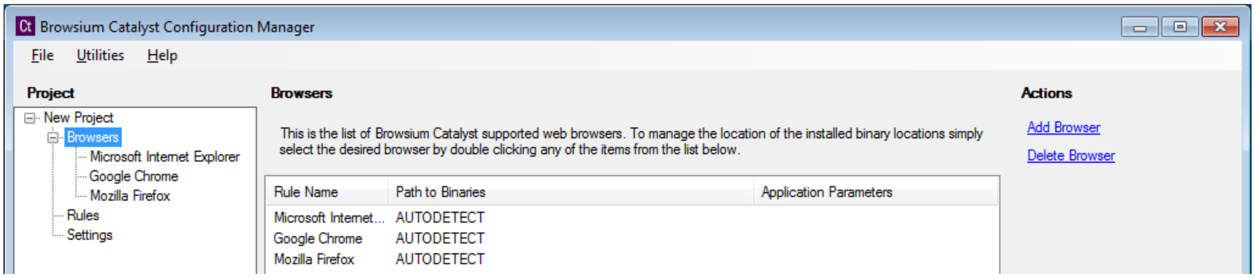
Default Target Action – Determines the default Target Action when a new Rule is created.

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

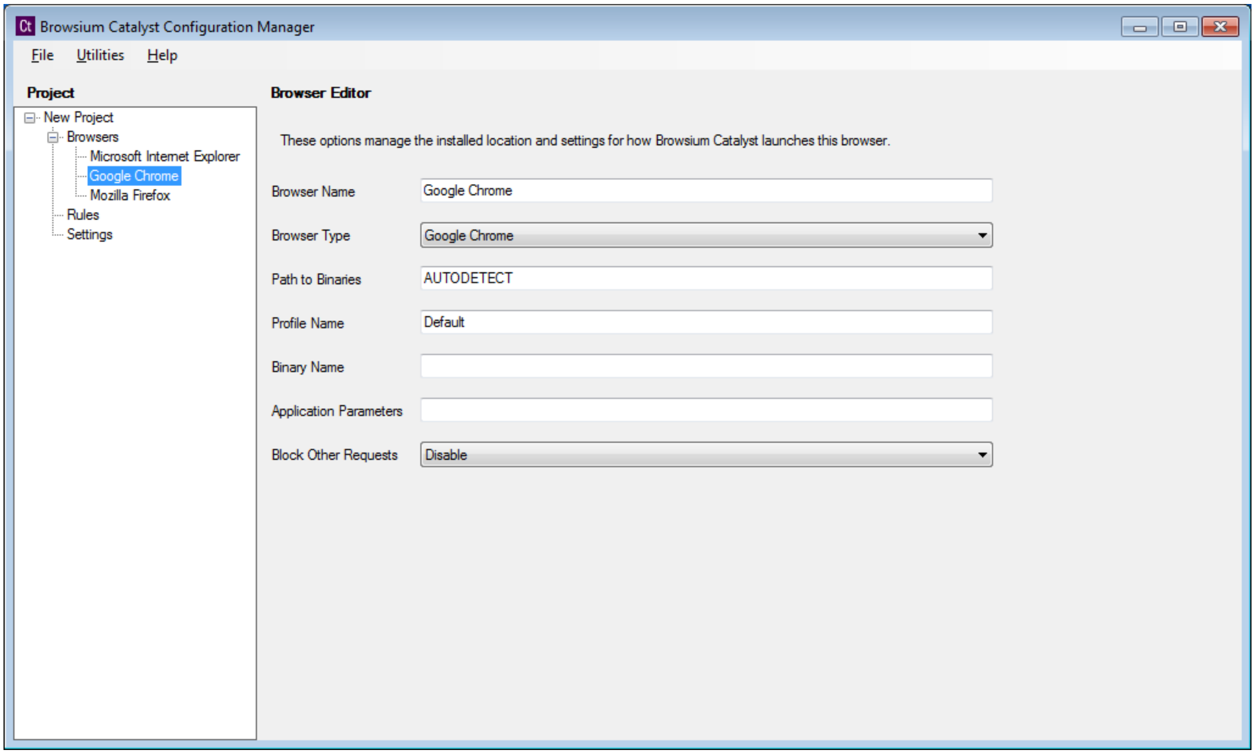
The Browsers Node contains the list of defined browsers for a given system. Catalyst only supports the three preset browsers – Internet Explorer, Chrome and Firefox. The Catalyst Configuration Manager will attempt to automatically determine the installation path for each installed browser. If one of 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.



This is the list of Browsium Catalyst supported web browsers. To manage the location of the installed binary locations simply select the desired browser by double clicking any of the items from the list below.

Rule Name	Path to Binaries	Application Parameters
Microsoft Internet...	AUTODETECT	
Google Chrome	AUTODETECT	
Mozilla Firefox	AUTODETECT	

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.



These options manage the installed location and settings for how Browsium Catalyst launches this browser.

Browser Name	Google Chrome
Browser Type	Google Chrome
Path to Binaries	AUTODETECT
Profile Name	Default
Binary Name	
Application Parameters	
Block Other Requests	Disable

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.

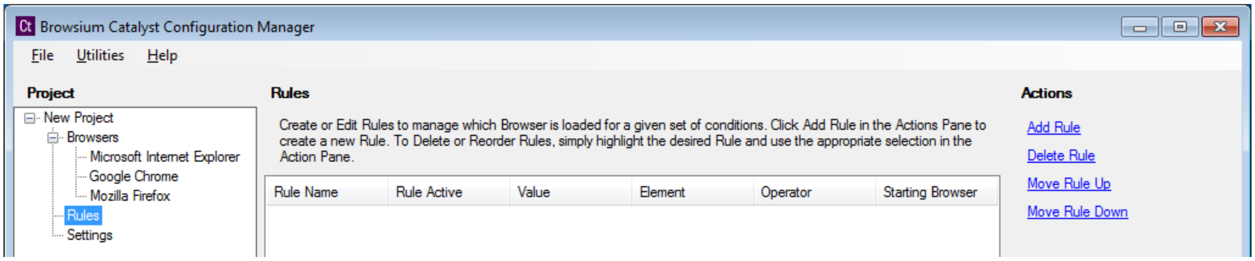
Application Parameters – In addition to launching a desired browser, the Catalyst system can open the application using additional parameters specified here. Ensure any additional parameters are correct for the specific browser as incorrect items may cause the browser to stop loading.

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 create support tickets when the browser no longer loads content and fails to load any address entered that does match Rules loaded on their system.**

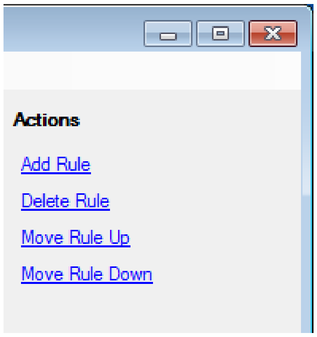
3.4. The Rules Node

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.



Create or Edit Rules to manage which Browser is loaded for a given set of conditions. Click Add Rule in the Actions Pane to create a new Rule. To Delete or Reorder Rules, simply highlight the desired Rule and use the appropriate selection in the Action Pane.

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 rest 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. By design, Browsium Catalyst only renders sites explicitly identified in the rule set, so you must create a Rule or series of Rules in order to effectively use Browsium Catalyst.

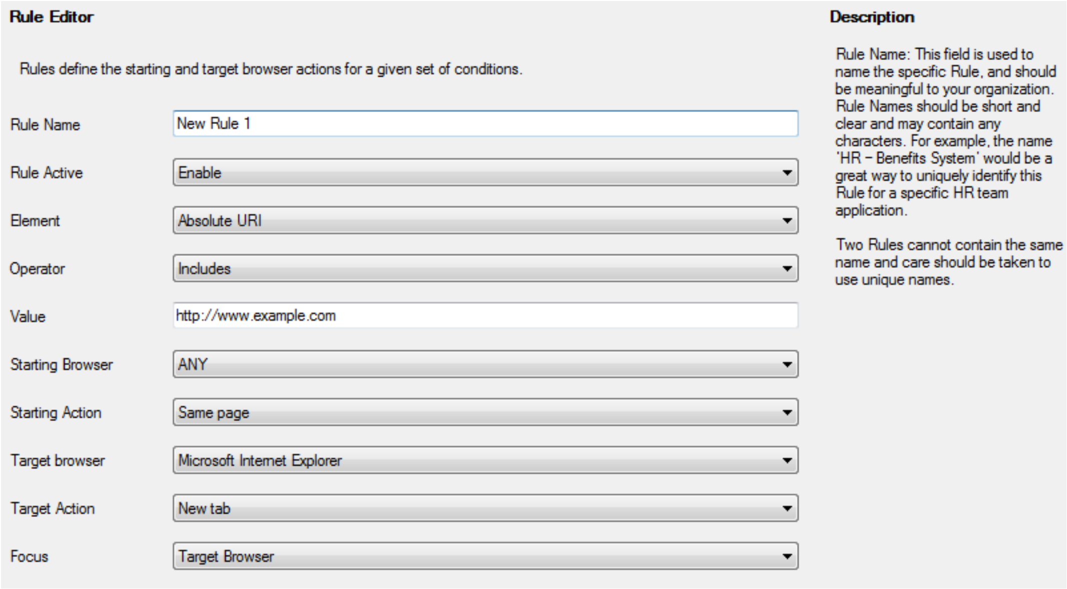
> **Systems must have the Browsium Catalyst Client for the appropriate browsers installed in order to use the Rules and configurations created in the Catalyst Configuration Manager.**

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

Rules define the starting and target browser actions for a given set of conditions.

Rule Name	New Rule 1
Rule Active	Enable
Element	Absolute URI
Operator	Includes
Value	http://www.example.com
Starting Browser	ANY
Starting Action	Same page
Target browser	Microsoft Internet Explorer
Target Action	New tab
Focus	Target Browser

Description

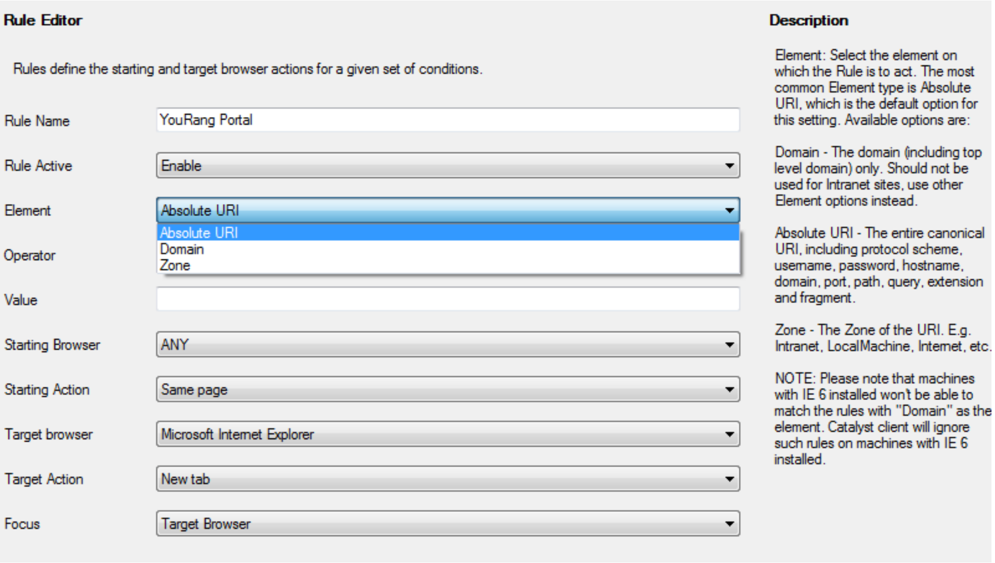
Rule Name: This field is used to name the specific Rule, and should be meaningful to your organization. Rule Names should be short and clear and may contain any characters. For example, the name 'HR – Benefits System' would be a great way to uniquely identify this Rule for a specific HR team application.

Two Rules cannot contain the same name and care should be taken to use unique names.

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

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	
Value	
Starting Browser	ANY
Starting Action	Same page
Target browser	Microsoft Internet Explorer
Target Action	New tab
Focus	Target Browser

Description

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:

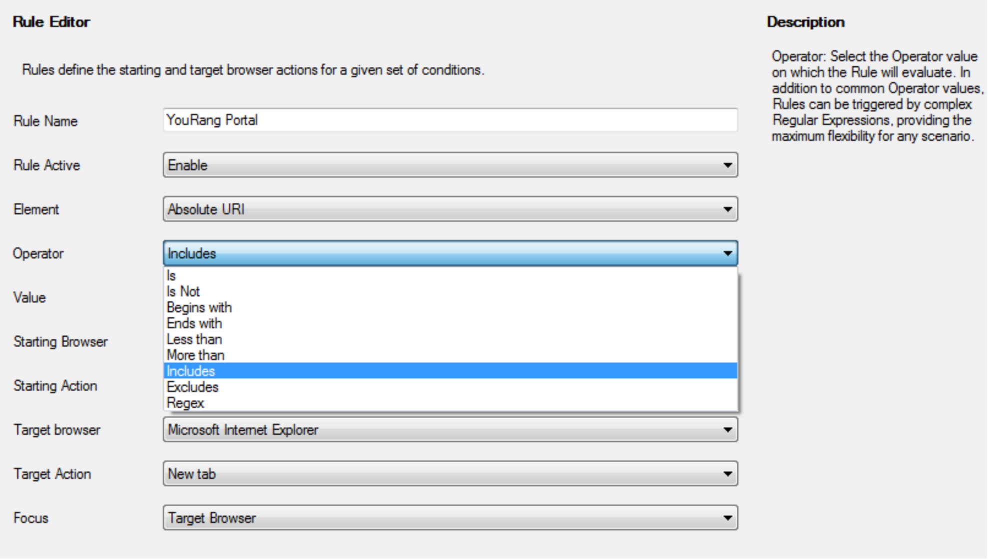
Domain - The domain (including top level domain) only. Should not be used for Intranet sites, use other Element options instead.

Absolute URI - The entire canonical URI, including protocol scheme, username, password, hostname, domain, port, path, query, extension and fragment.

Zone - The Zone of the URI. E.g. Intranet, LocalMachine, Internet, etc.

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.

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

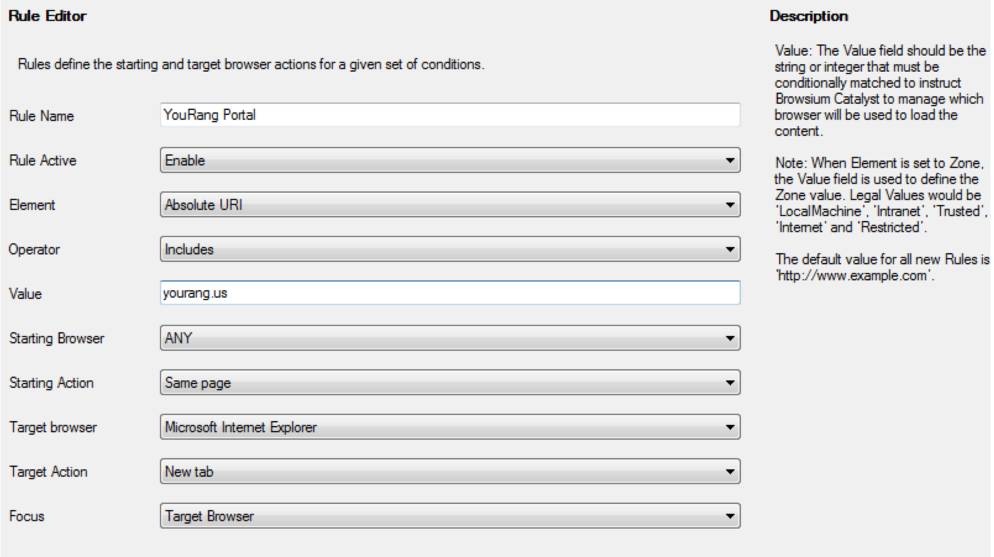
Rules define the starting and target browser actions for a given set of conditions.

Rule Name	YouRang Portal
Rule Active	Enable
Element	Absolute URI
Operator	Includes
Value	
Starting Browser	
Starting Action	
Target browser	Microsoft Internet Explorer
Target Action	New tab
Focus	Target Browser

Description

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.

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



Rule Editor

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
Target Action	New tab
Focus	Target Browser

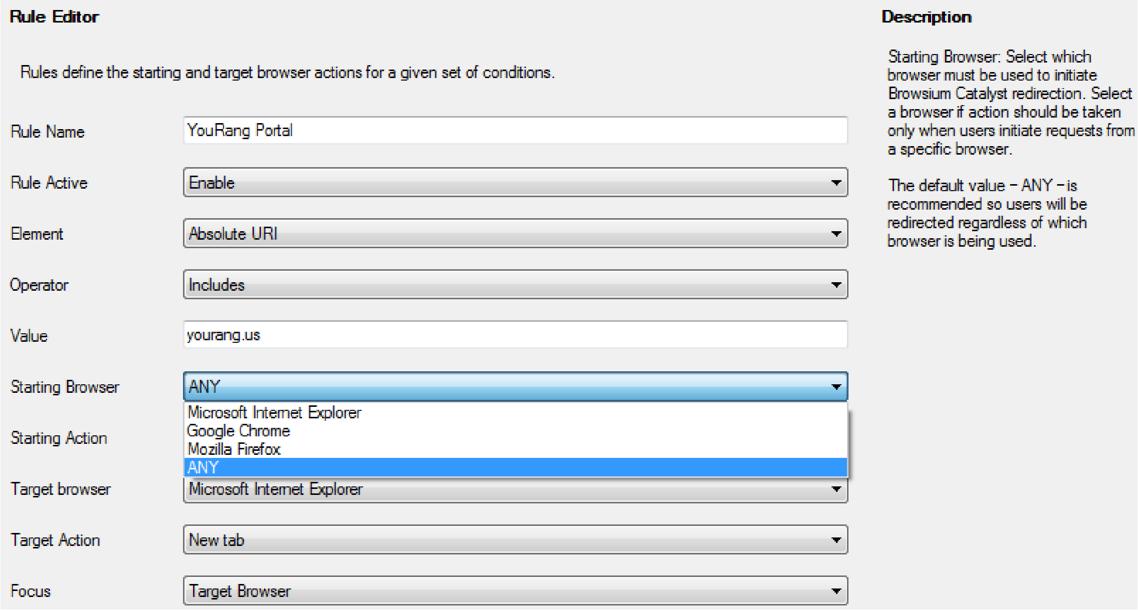
Description

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.

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'.

The default value for all new Rules is 'http://www.example.com'.

6. 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

Rules define the starting and target browser actions for a given set of conditions.

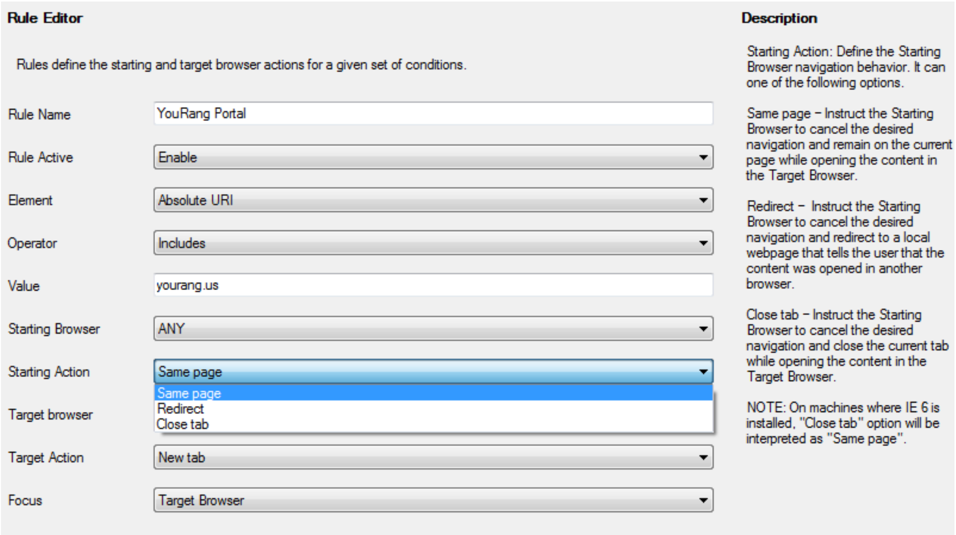
Rule Name	YouRang Portal
Rule Active	Enable
Element	Absolute URI
Operator	Includes
Value	yourang.us
Starting Browser	ANY
Starting Action	
Target browser	Microsoft Internet Explorer
Target Action	New tab
Focus	Target Browser

Description

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.

The default value – ANY – is recommended so users will be redirected regardless of which browser is being used.

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

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	
Target Action	New tab
Focus	Target Browser

Description

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

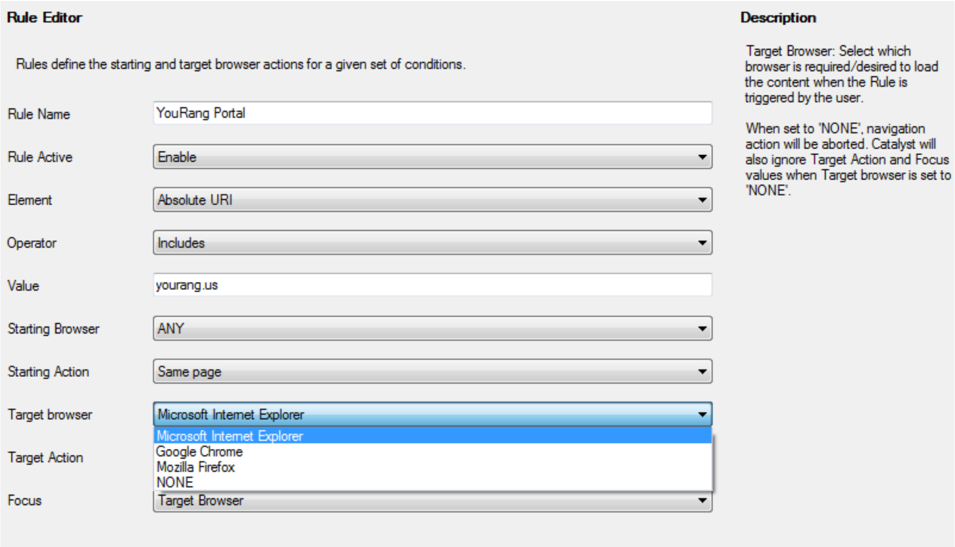
Same page – Instruct the Starting Browser to cancel the desired navigation and remain on the current page while opening the content in the Target Browser.

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

Rules define the starting and target browser actions for a given set of conditions.

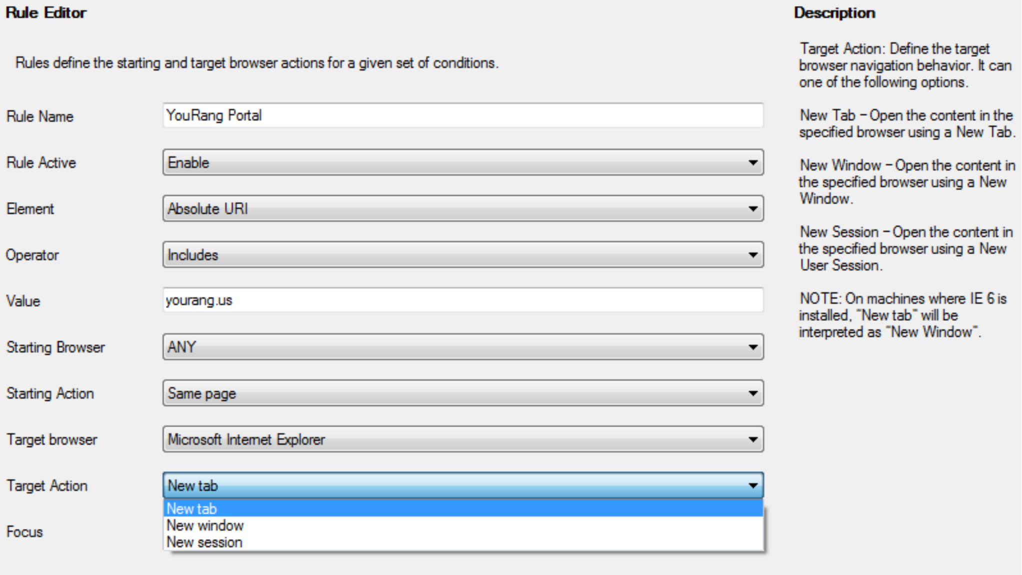
Rule Name	YouRang Portal
Rule Active	Enable
Element	Absolute URI
Operator	Includes
Value	yourang.us
Starting Browser	ANY
Starting Action	Same page
Target browser	Microsoft Internet Explorer
Target Action	
Focus	Target Browser

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

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
Target Action	New tab
Focus	

Description

Target Action: Define the target browser navigation behavior. It can one of the following options.

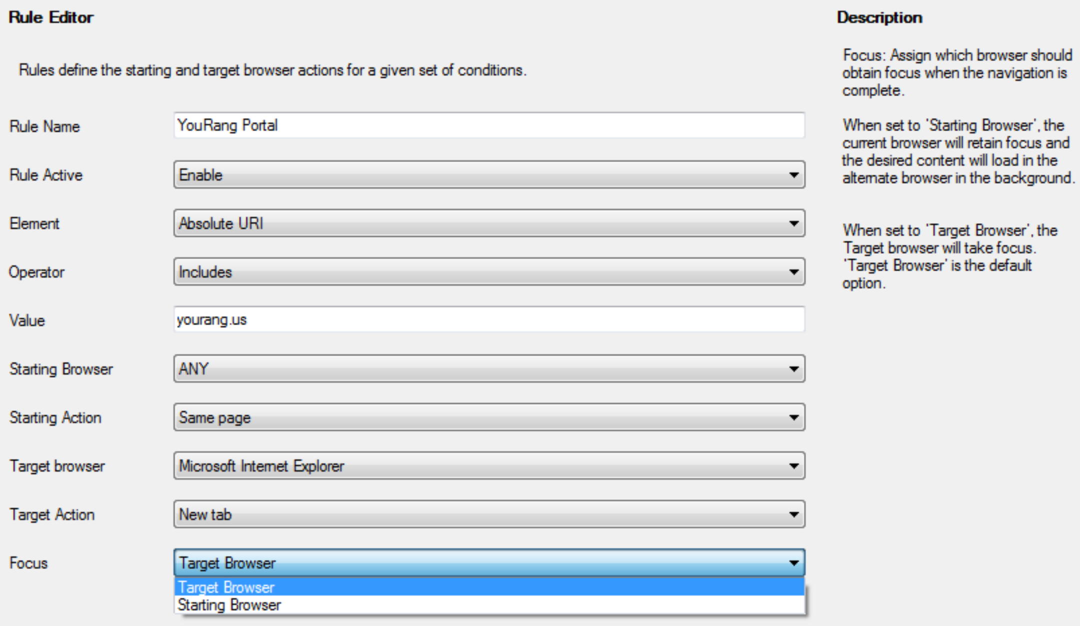
New Tab – Open the content in the specified browser using a New Tab.

New Window – Open the content in the specified browser using a New Window.

New Session – Open the content in the specified browser using a New User Session.

NOTE: On machines where IE 6 is installed, "New tab" will be interpreted as "New Window".

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

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
Target Action	New tab
Focus	Target Browser

Description

Focus: Assign which browser should obtain focus when the navigation is complete.

When set to 'Starting Browser', the current browser will retain focus and the desired content will load in the alternate browser in the background.

When set to 'Target Browser', the Target browser will take focus. 'Target Browser' is the default option.

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.

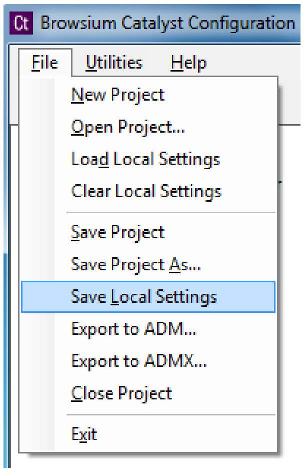
12. You can continue to add Rules until you have completed all the desired entries.

13. Rules and configurations can be saved either as Local Settings or Project files.

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

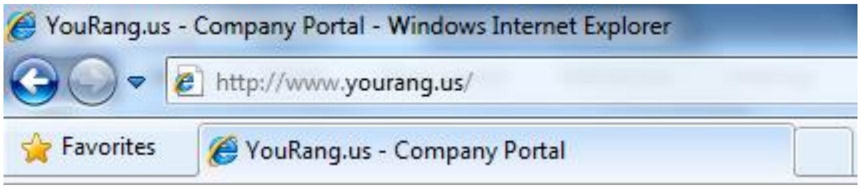
Saving as Local Settings will apply the rules and configuration to the PC instantly, whereas saving the Project file would not apply those rules now but enable you to load them later or pass them to another machine.

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



In order to save the Catalyst configuration files to the local system, you may need to click '**Allow**' on the process elevation request.

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.

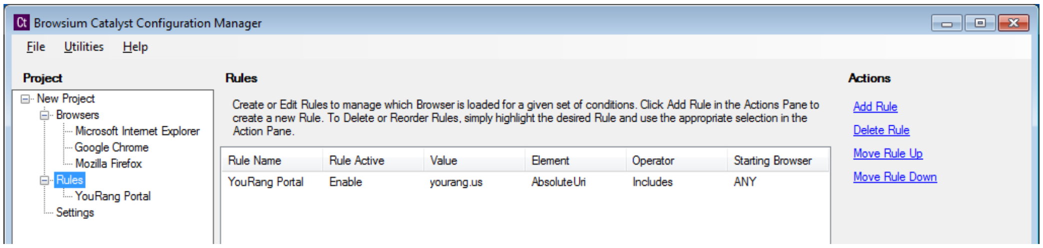

YouRang.us - Company Portal - Windows Internet Explorer
http://www.yourang.us/
Favorites
YouRang.us - Company Portal

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:

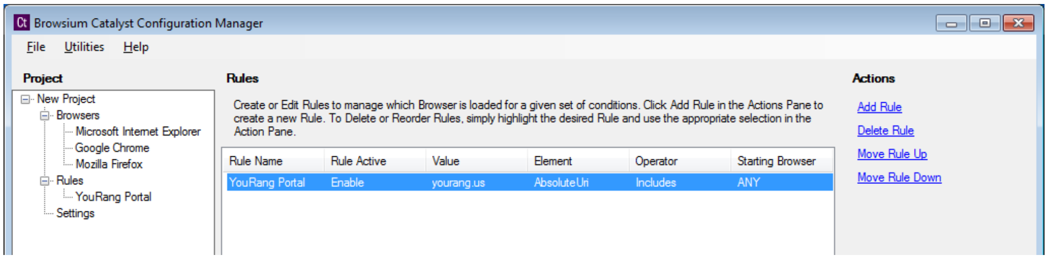
1. Open the Catalyst Configuration Manager and load the Project containing the Rules you want to remove (using either Load Local Settings or Open Project from the File menu). With the Project loaded, click the Rules node to bring up the ordered list of Rules.



Create or Edit Rules to manage which Browser is loaded for a given set of conditions. Click Add Rule in the Actions Pane to create a new Rule. To Delete or Reorder Rules, simply highlight the desired Rule and use the appropriate selection in the Action Pane.

Rule Name	Rule Active	Value	Element	Operator	Starting Browser
YouRang Portal	Enable	yourang.us	AbsoluteUri	Includes	ANY

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



Create or Edit Rules to manage which Browser is loaded for a given set of conditions. Click Add Rule in the Actions Pane to create a new Rule. To Delete or Reorder Rules, simply highlight the desired Rule and use the appropriate selection in the Action Pane.

Rule Name	Rule Active	Value	Element	Operator	Starting Browser
YouRang Portal	Enable	yourang.us	AbsoluteUri	Includes	ANY

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.

5.1. Managing the Catalyst Extension for Internet Explorer

Many organizations utilize Group Policy to enforce settings on end users PCs. These important system configuration options can be managed by Group Policies in both Internet Explorer and in Chrome, however Mozilla Firefox does not natively support Group Policy today.

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 a Visual Basic Script, can also be employed. The following guidance is adapted from articles on Microsoft's TechNet website, and includes the process to identify the GUID/CLSID of the Browsium Catalyst Internet Explorer Extension, which must be located in the registry once it is installed in your environment. Also in this section are the proper settings to enforce the default browser setting.

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.

To set this policy, 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

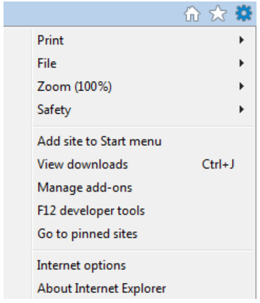
Type: **REG_SZ**

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.

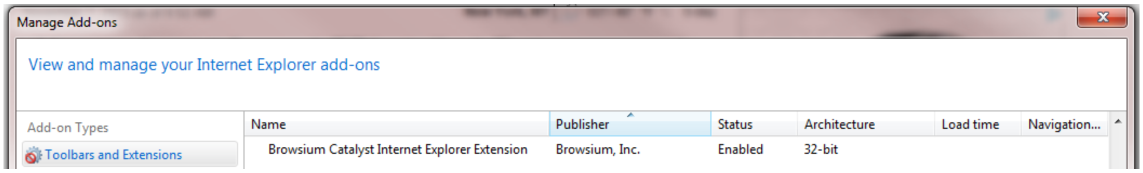
The Add-on (CLSID) lists are empty by default.

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.

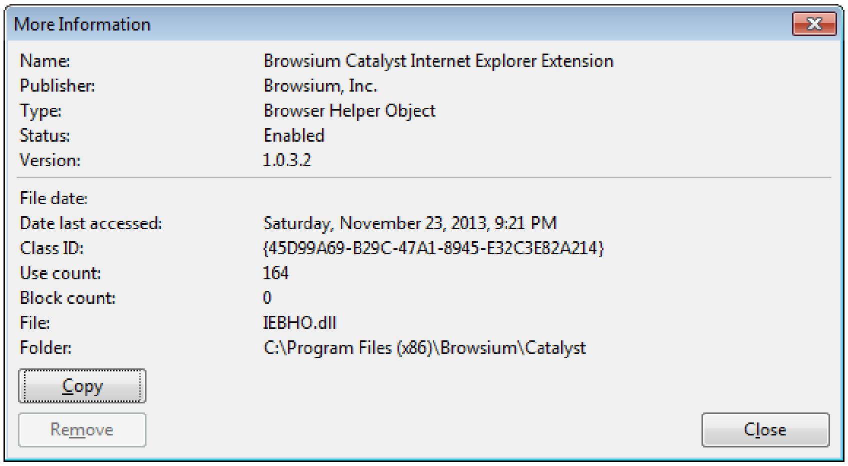
You'll then be presented with the Manage Add-ons interface where you should see Browsium Catalyst Internet Explorer Extension in the list among the Toolbars and Extensions that are currently loaded in Internet Explorer.



Name	Publisher	Status	Architecture	Load time	Navigation...
Browsium Catalyst Internet Explorer Extension	Browsium, Inc.	Enabled	32-bit		

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.



Name: Browsium Catalyst Internet Explorer Extension
Publisher: Browsium, Inc.
Type: Browser Helper Object
Status: Enabled
Version: 1.0.3.2

File date:
Date last accessed: Saturday, November 23, 2013, 9:21 PM
Class ID: {45D99A69-B29C-47A1-8945-E32C3E82A214}
Use count: 164
Block count: 0
File: IEBHO.dll
Folder: C:\Program Files (x86)\Browsium\Catalyst

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 registry.

5.1.2. Disable Internet Explorer's Default Browser Check via Group Policy

This Group Policy is related to the **Prevent changing default browser check** Group Policy setting. The old Group Policy covers IE5 through IE9. The new Group Policy starts with IE10. Also, in IE10, the 'Tell me if Internet Explorer is not the default web browser' check box is on the Advanced tab in the Internet Options dialog box. For earlier versions, it was on the Programs tab of the Internet Options dialog box. This policy prevents Internet Explorer from checking to see whether it is the default browser.

For IE5 – IE9:

Policy Name: Prevent changing default browser check

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

Tell me if Internet Explorer is not the default web browser check box is on the **Programs** tab of the **Internet Options** dialog box. The registry setting to address this is:

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

For IE10:

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

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

Tell me if Internet Explorer is not the default web browser check box is on the **Advanced** tab in the **Internet Options** dialog box. By default, IE10 has the following registry setting already set to 'no'.

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

The Disable the Programs page policy (located in User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), which removes the **Programs** tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored.

If you enable this policy, the **Internet Explorer Should Check to See Whether It Is the Default Browser** check box on the **Programs** tab in the **Internet Options** dialog box appears dimmed. 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. There are two types of templates available, an ADM and an ADMX template. You will want to verify the template type you can use on your network.

The Group Policy templates, and associated guidance, are provided by Google 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 3rd 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.

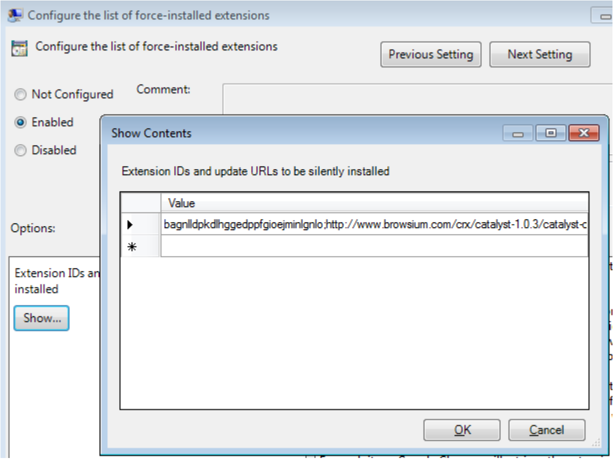
Follow these steps to ensure that this method is properly configured using Group Policy for your domain-joined systems. These instructions assume you're using the ADM template. The Group Policy location will change if using ADMX.

> **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-1.0.3/catalyst-chrome-1.0.3.xml

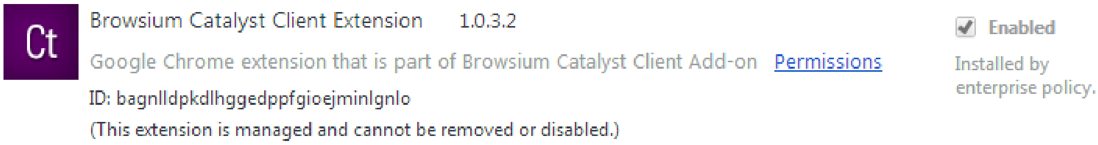


○ Not Configured
● Enabled
○ Disabled

Extension IDs and update URLs to be silently installed

	Value
▶	bagnlldpkdlhggedppfgioejminlgnlo;http://www.browsium.com/crx/catalyst-1.0.3/catalyst-c
*	

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



Browsium Catalyst Client Extension 1.0.3.2

Google Chrome extension that is part of Browsium Catalyst Client Add-on

ID: bagnlldpkdlhggedppfgioejminlgnlo

(This extension is managed and cannot be removed or disabled.)

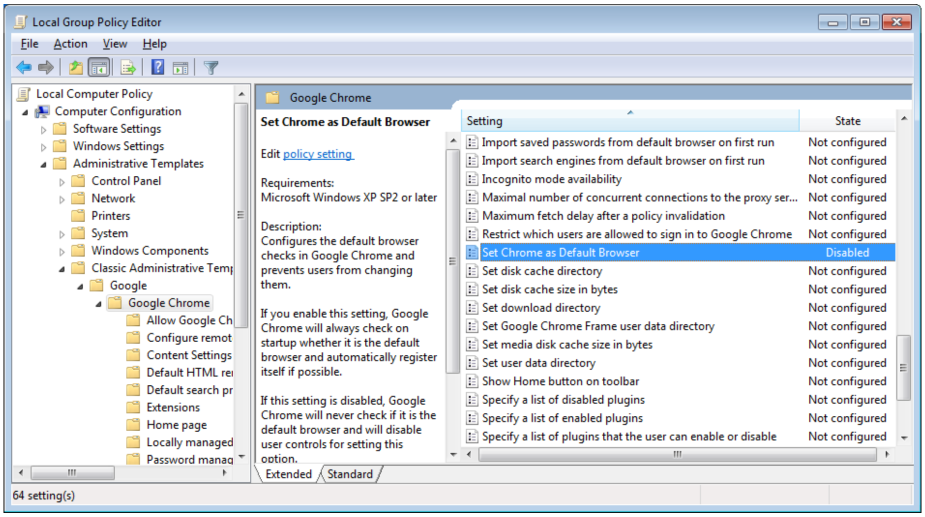
☑ Enabled

Installed by enterprise policy.

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 is Local Computer Policy\Administrative Templates\Classic Administrative Templates (ADM)\Google\Google Chrome.



Set Chrome as Default Browser

Edit policy setting

Requirements:
Microsoft Windows XP SP2 or later

Description:
Configures the default browser checks in Google Chrome and prevents users from changing them.

If you enable this setting, Google Chrome will always check on startup whether it is the default browser and automatically register itself if possible.

If this setting is disabled, Google Chrome will never check if it is the default browser and will disable user controls for setting this option.

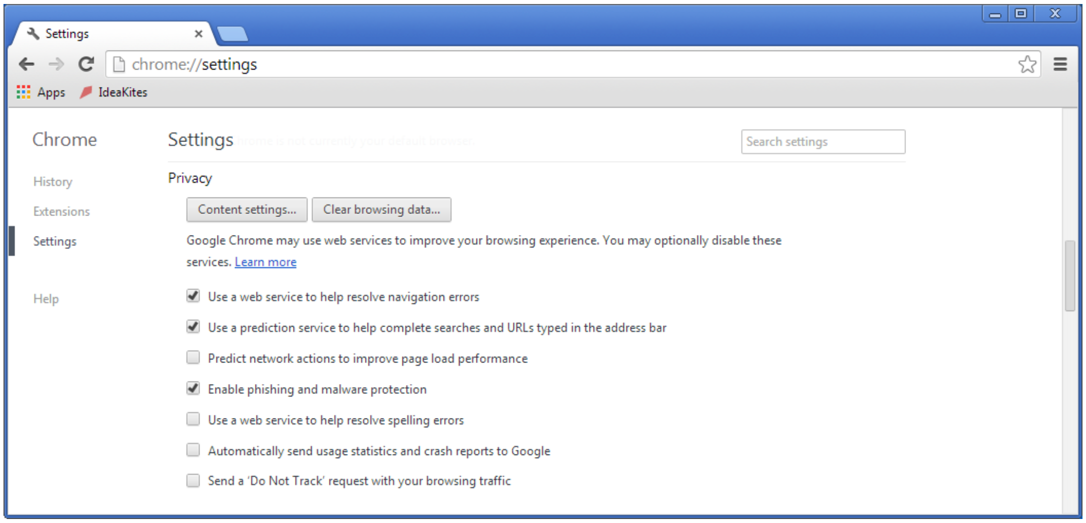
Setting	State
Import saved passwords from default browser on first run	Not configured
Import search engines from default browser on first run	Not configured
Incognito mode availability	Not configured
Maximal number of concurrent connections to the proxy ser...	Not configured
Maximum fetch delay after a policy invalidation	Not configured
Restrict which users are allowed to sign in to Google Chrome	Not configured
Set Chrome as Default Browser	Disabled
Set disk cache directory	Not configured
Set disk cache size in bytes	Not configured
Set download directory	Not configured
Set Google Chrome Frame user data directory	Not configured
Set media disk cache size in bytes	Not configured
Set user data directory	Not configured
Show Home button on toolbar	Not configured
Specify a list of disabled plugins	Not configured
Specify a list of enabled plugins	Not configured
Specify a list of plugins that the user can enable or disable	Not configured

5.2.3. Disable 'Predict network actions' in Google Chrome

Google Chrome includes a 'predictive' network capability, called "predict network actions", 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".



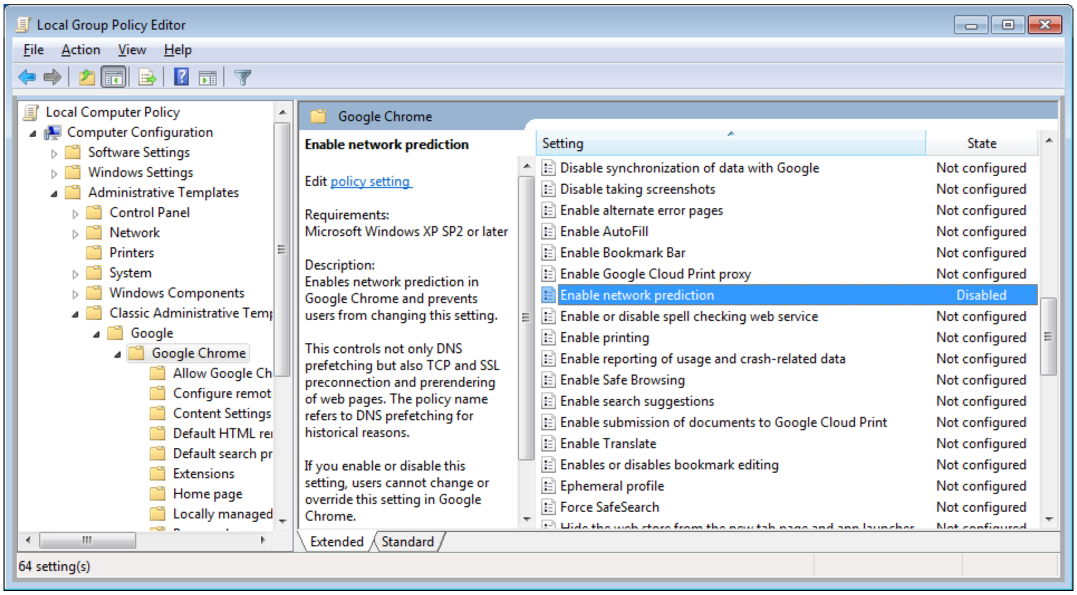
Settings

Privacy

Google Chrome may use web services to improve your browsing experience. You may optionally disable these services. Learn more

- ☑ Use a web service to help resolve navigation errors
- ☑ Use a prediction service to help complete searches and URLs typed in the address bar
- ☐ Predict network actions to improve page load performance
- ☑ Enable phishing and malware protection
- ☐ Use a web service to help resolve spelling errors
- ☐ Automatically send usage statistics and crash reports to Google
- ☐ Send a 'Do Not Track' request with your browsing traffic

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).



Google Chrome

Enable network prediction

Edit policy setting

Requirements:
Microsoft Windows XP SP2 or later

Description:
Enables network prediction in Google Chrome and prevents users from changing this setting.

This controls not only DNS prefetching but also TCP and SSL preconnection and prerendering of web pages. The policy name refers to DNS prefetching for historical reasons.

If you enable or disable this setting, users cannot change or override this setting in Google Chrome.

Setting	State
Disable synchronization of data with Google	Not configured
Disable taking screenshots	Not configured
Enable alternate error pages	Not configured
Enable AutoFill	Not configured
Enable Bookmark Bar	Not configured
Enable Google Cloud Print proxy	Not configured
Enable network prediction	Disabled
Enable or disable spell checking web service	Not configured
Enable printing	Not configured
Enable reporting of usage and crash-related data	Not configured
Enable Safe Browsing	Not configured
Enable search suggestions	Not configured
Enable submission of documents to Google Cloud Print	Not configured
Enable Translate	Not configured
Enables or disables bookmark editing	Not configured
Ephemeral profile	Not configured
Force SafeSearch	Not configured

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 Group 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 Group 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"

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 to provide centralized management in deploying configurations (Settings and Rules) to PCs in an enterprise. The Catalyst Configuration Manager includes an easy-to-use function to export configurations and deploy them to end user PCs.

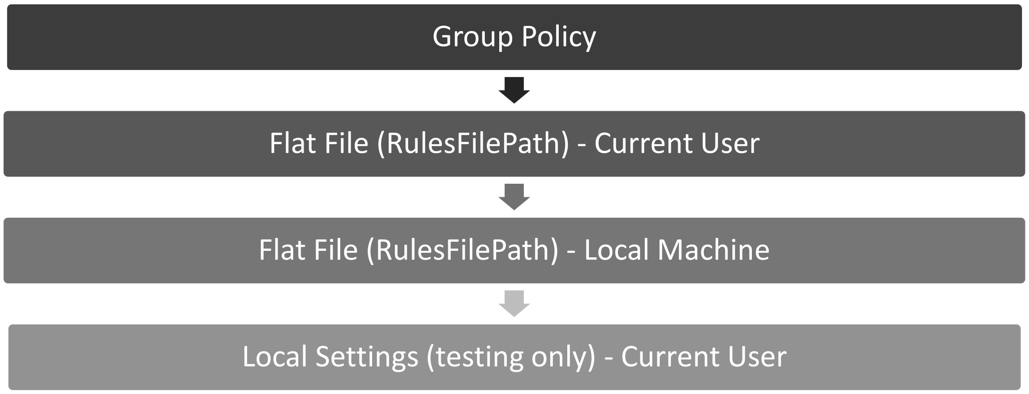
Catalyst supports both ADM and ADMX template export configurations options. ADM templates are used by Windows Server 2003 and 2008 domain controllers as well as client systems from Windows XP to the most versions of Windows. ADMX templates can only be used on Windows Server 2008 Domain Controllers for use with PCs running Windows Vista or newer.

Catalyst also supports flat file configurations, which is Browsium's recommended approach. Flat file configurations instruct Catalyst to load a configuration file from a local or network location. Deploying a Flat File configuration requires a simple, one-time client registry change.

By default, Catalyst will look first in Group Policy for configurations, then flat files (defined by the RulesFilePath registry value), then Local Settings (only used for testing on systems running Catalyst Configuration Manager). Once a valid configuration is found, Catalyst will stop searching and that configuration will be used.

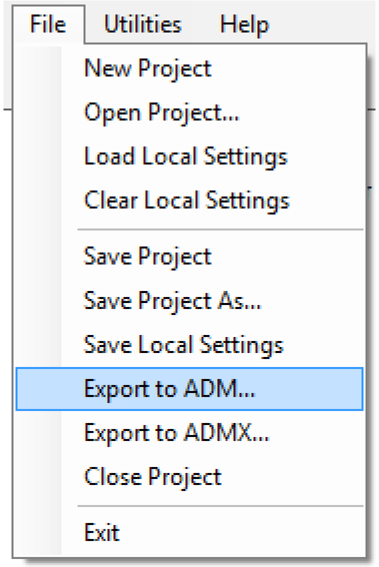
The following table provides a hierarchy of precedence for the evaluation of configurations.

> **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.**


Group Policy
Flat File (RulesFilePath) - Current User
Flat File (RulesFilePath) - Local Machine
Local Settings (testing only) - Current User

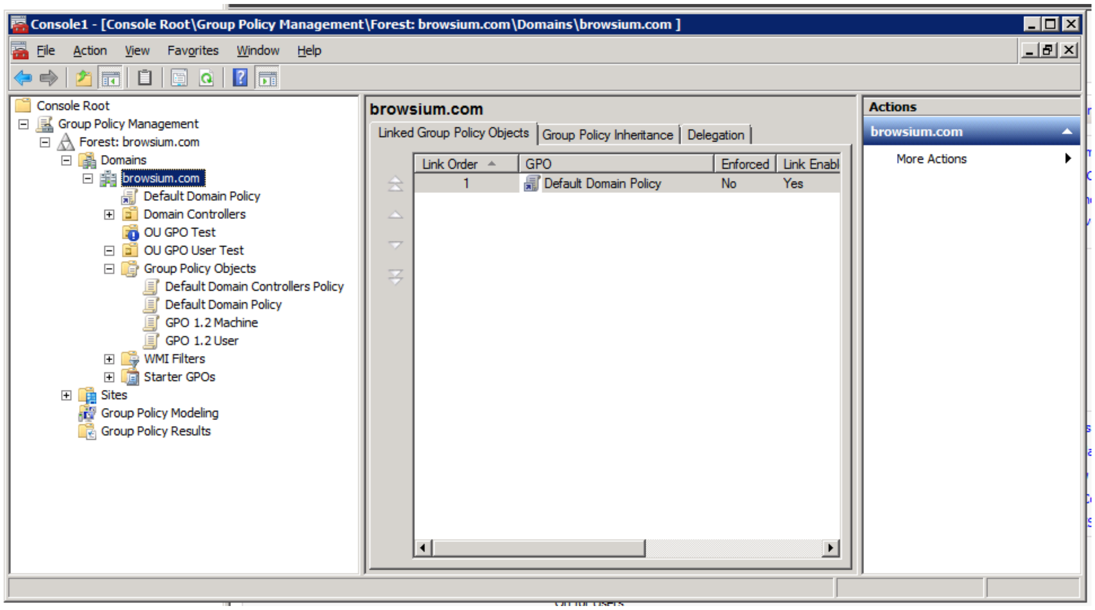
6.1. Deploying via Group Policy with Classic ADM Templates

Using Group Policy to manage Catalyst client configurations is easy. Simply start by exporting the Project file settings by selecting Export to ADM... in the File menu.

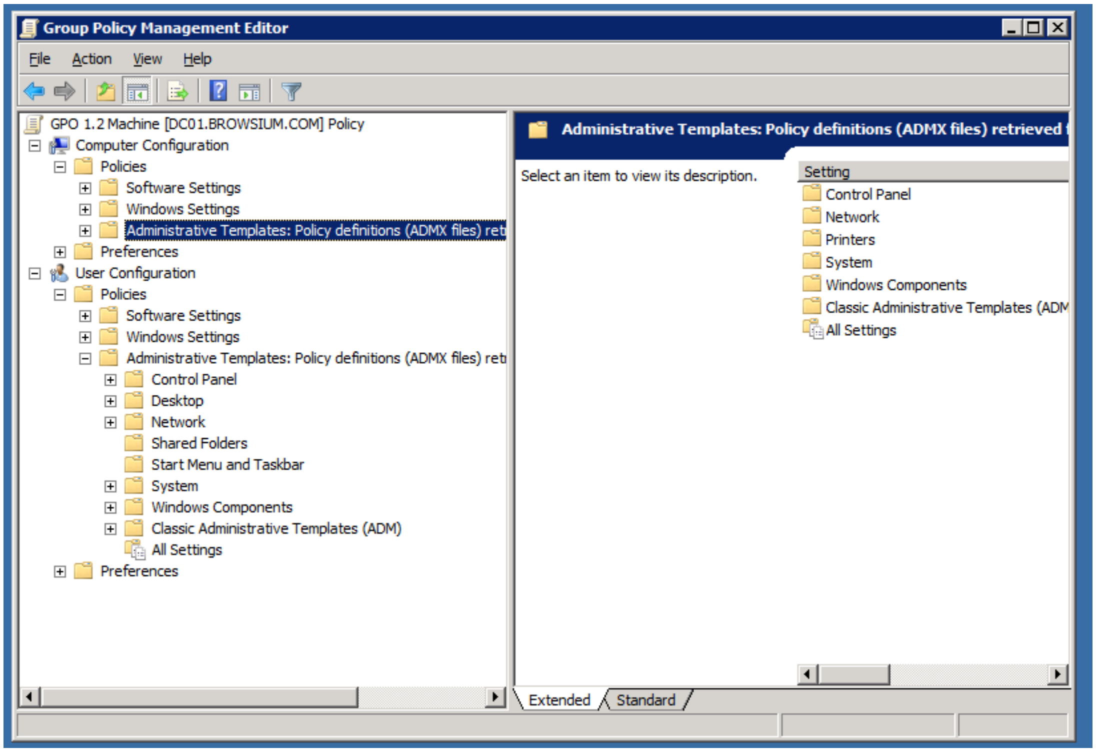


Next, name and save your .ADM file, then transfer the file to a Domain Controller or a machine running Group Policy Manager.

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



Right click the newly created Group Policy Object and select ‘edit’ to launch the Group Policy Editor.


Group Policy Management Editor
File
Action
View
Help
GPO 1.2 Machine [DC01.BROWSIUM.COM] Policy
Computer Configuration
Policies
Software Settings
Windows Settings
Administrative Templates: Policy definitions (ADMX files) ret
Preferences
User Configuration
Policies
Software Settings
Windows Settings
Administrative Templates: Policy definitions (ADMX files) ret
Control Panel
Desktop
Network
Shared Folders
Start Menu and Taskbar
System
Windows Components
Classic Administrative Templates (ADM)
All Settings
Preferences
Administrative Templates: Policy definitions (ADMX files) retrieved
Select an item to view its description.
Setting
Control Panel
Network
Printers
System
Windows Components
Classic Administrative Templates (ADM
All Settings
Extended
Standard

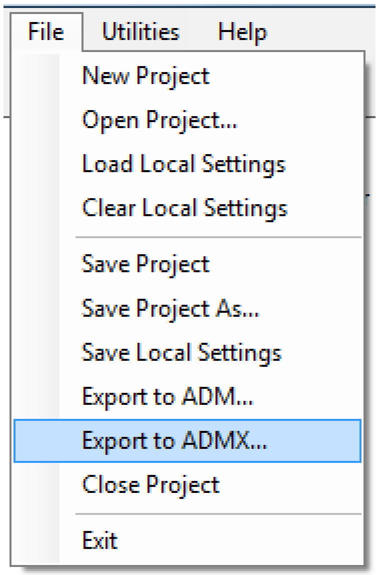
Open the Computer Configuration > Policies node, then right click on Administrative Templates item. Choose the Add/Remove Templates option and select the ADM file exported from the Catalyst Configuration Manager above.

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. Setting the value to Disabled may cause unexpected impacts on client load behavior.**
>
> **In addition, always make changes to Rules and Settings in the Catalyst Configuration Manager and not in the Group Policy Editor.**

6.2. Deploying via Group Policy with ADMX Templates

Using Group Policy to manage Catalyst client configurations is easy, simply start by exporting the Project file settings by selecting the Export to ADMX...option in the File menu.



This will export two files (an .ADMX and .ADML file). Name and save the .ADMX files, then transfer these files to a Domain Controller system.

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.

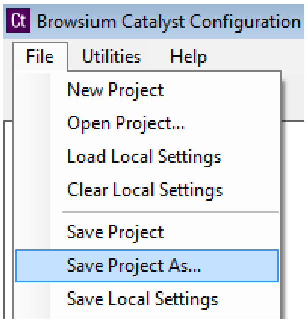
Launch the Group Policy Manager and locate the Catalyst folder within the Default Domain Policy under Administrative Templates: Policy Definitions (ADMX files). Open up each item in these folders and set them to 'Enabled'.

> **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, Rules or Profiles. Setting the value to Disabled may cause unexpected impacts on client load behavior.**

6.3. Deploying via Flat Files

Catalyst supports flat file-based configuration deployments. Projects are standard XML documents, allowing you to take full advantage of this versatile format. However, Catalyst will not look for a flat file configuration by default. You must configure each client system, via the Windows registry, to use a flat file configuration. The following provides specific 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 Browsium Catalyst Configuration Manager.



Then 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 or via a script (for remote deployment). You must define a registry value for either per-user settings (which will impact a single user account on the system), or per-machine settings (which will affect all user accounts on the system).

The Catalyst project file (.cax) must be stored in a user-readable location on the local PC or a network share. You will enter that specific location in the RulesFilePath registry value.

> **Loading a configuration from a network location may result in delays or performance issues due to network traffic.**

For **per-user** settings on **32-bit and 64-bit** Windows systems:

Find HKEY_CURRENT_USER\SOFTWARE\Browsium\Catalyst

For **per-machine** settings on **32-bit** Windows systems:

Find HKEY_LOCAL_MACHINE\SOFTWARE\Browsium\Catalyst

For **per-machine** settings on **64-bit** Windows systems:

Find HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Browsium\Catalyst

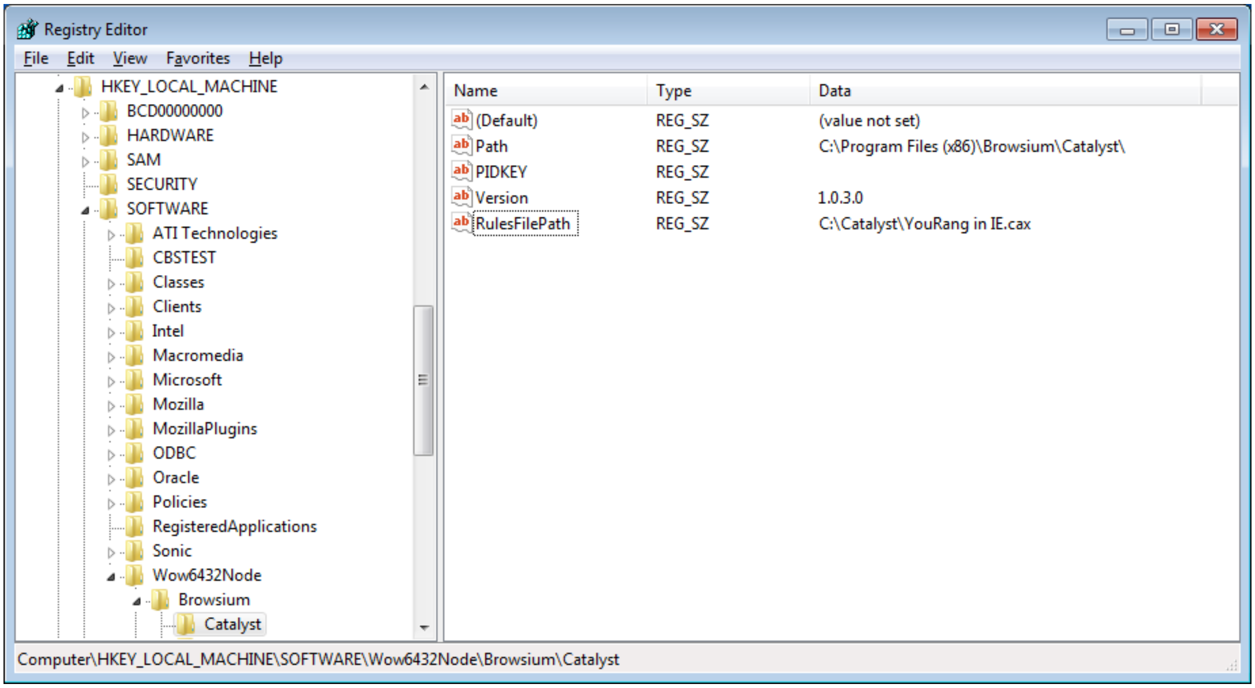
Then create the following String Value in the Catalyst key:
RulesFilePath (REG_SZ) = C:\directory\... [the path to your Catalyst project file (.cax)]

> **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 the following text in a .reg file.

```
Windows registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Browsium\Catalyst]
"RulesFilePath"="C:\\Catalyst\\YouRang in IE.cax"
```



Name	Type	Data
(Default)	REG_SZ	(value not set)
Path	REG_SZ	C:\Program Files (x86)\Browsium\Catalyst\
PIDKEY	REG_SZ	
Version	REG_SZ	1.0.3.0
RulesFilePath	REG_SZ	C:\Catalyst\YouRang in IE.cax

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Browsium\Catalyst

Appendix A

Appendix A: Troubleshooting

In this section you will learn:

- ✓ How to Recognize Issues with an 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 websites based on rules you've created.

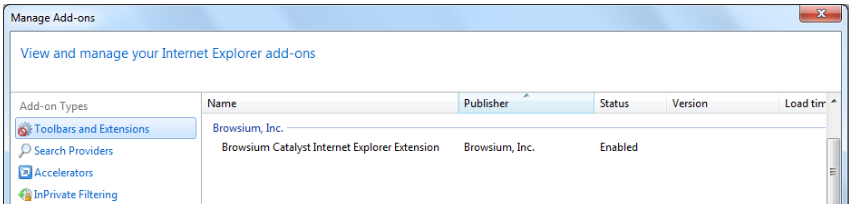
The following points may guide you to a resolution:

- **Review System Prerequisites**
  - Check to see that the target computer meets the performance and storage requirements to run Catalyst.
  - Confirm that .NET 3.5 (or later) is installed on the computer running the Catalyst Client installation.

- **Verify the Catalyst Installation Files**
  - Verify both the Catalyst Configuration Manager and Catalyst Client Add-ons are present, ensure that they are installed and enabled in the browsers.

- **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:



Name	Publisher	Status	Version	Load tim
Browsium, Inc.				
Browsium Catalyst Internet Explorer Extension	Browsium, Inc.	Enabled		

- **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 Not Working Properly in IE11 or Windows 8

At this time Browsium Catalyst is only supported for Internet Explorer 6, 7, 8, 9, and 10, so you will see unexpected behavior when trying to install and run Catalyst with other versions of Internet Explorer or Windows 8.

A.4. The Controller Becomes Unresponsive

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