



# Sitecore CMS 7.0 or later Browser Configuration Reference

*Optimizing Internet Explorer and other web browsers to work with Sitecore*

## Table of Contents

Chapter 1	Introduction .....	3
1.1	Supported Web Browsers.....	4
Chapter 2	Configuring Microsoft Internet Explorer .....	5
2.1	How to Determine the Internet Explorer Version .....	6
2.2	Internet Explorer Configuration Summary .....	7
2.3	Required Configuration.....	9
2.3.1	Trusted Sites Zone .....	9
2.3.2	Pop-up Blocker.....	10
2.3.3	Word Document Field Type Configuration.....	11
2.3.4	WebDAV Configuration.....	12
	Windows Web Folders Client or the Windows Desktop Experience.....	12
	The WebClient Windows Service .....	12
2.4	Recommended Configuration .....	13
2.4.1	Disable the SmartScreen or Phishing Filter .....	13
	Internet Explorer 8 .....	13
	Internet Explorer 9 and 10 .....	13
2.4.2	Install Adobe Flash .....	14
2.4.3	Minor Issues.....	14
2.4.4	Configure Management of Temporary Internet Files.....	15
2.5	Optional Configuration.....	17
2.5.1	New Windows or New Tabs.....	17
2.5.2	Internet Explorer 8, 9, and 10 Session Merging.....	17
	The New Session Command.....	17
	The -NoSessionMerging Command Line Parameter .....	18
	The SessionMerging Registry Setting.....	18
2.5.3	Concurrent HTTP Request Limits .....	19
2.5.4	Miscellaneous Settings.....	20
Chapter 3	Troubleshooting Microsoft Internet Explorer.....	22
3.1	Troubleshooting Process .....	23
3.1.1	Check Sitecore Client Requirements.....	23
3.1.2	Check Browser Configuration .....	23
3.1.3	Disable Browser Plug-ins.....	23
3.1.4	Clear Browser Temporary Files .....	23
3.1.5	Patch Windows and Components .....	24
3.1.6	Check Internet Security Software.....	24
3.1.7	Reset Internet Explorer Configuration .....	24
3.1.8	Reproduce the Issue Using another Browser .....	25
3.1.9	Reproduce the Issue as another User.....	25
3.1.10	Reproduce the Issue from another Machine.....	25
3.2	Additional Troubleshooting Resources.....	26
Chapter 4	Configuring Other Browsers.....	27
4.1	Enabling Pop-up Windows in Google Chrome .....	28
4.2	Enabling Pop-up Windows in Other Browsers.....	29
4.3	Preventing Mozilla Firefox from Showing Confirmation Dialog Box in the Page Editor .....	30

# Chapter 1

## Introduction

This document describes how to optimize Microsoft Internet Explorer and other web browsers to work with Sitecore. It also describes how to troubleshoot browser issues.

This document contains the following chapters:

- **Chapter 1 — Introduction**
- **Chapter 2 — Configuring Microsoft Internet Explorer**
- **Chapter 3 — Troubleshooting Microsoft Internet Explorer**
- **Chapter 4 — Configuring Other Browsers**

## 1.1 Supported Web Browsers

Sitecore currently supports the following web browsers:

- Microsoft Internet Explorer 8, 9, and 10.
- Mozilla Firefox 17 and later.
- Google Chrome 25 and later.
- Apple Safari 6 for Mac OS — Windows is not supported by Apple.

### Note

Sitecore CMS 7.0 supports all current stable versions of these browsers unless stated otherwise.

### Note

Sitecore only supports Word and WebDAV with Internet Explorer, and only when they are configured according to the instructions described in this document.

## Chapter 2

# Configuring Microsoft Internet Explorer

This chapter describes how to configure Microsoft Internet Explorer to work with Sitecore. Some of these considerations may also apply to other browsers, although the UI instructions may differ from browser to browser.

This chapter contains the following sections:

- How to Determine the Internet Explorer Version
- Internet Explorer Configuration Summary
- Required Configuration
- Recommended Configuration
- Optional Configuration

## 2.1 How to Determine the Internet Explorer Version

To determine which version of Internet Explorer is installed on your computer:

In Internet Explorer, click the **Help** menu or press ALT-H, and then click **About Internet Explorer**.

The **About Internet Explorer** dialog box appears and tells you which version of Internet Explorer you are running.



### Important

Some of the instructions described in this document may require Windows administrative rights.

## 2.2 Internet Explorer Configuration Summary

When you are familiar with the configuration process, you can use this summary as a configuration checklist.

- Install Adobe Flash —*recommended*.  
For more information, see the section *Install Adobe Flash*.
- Install Windows Web Folders or the Windows Desktop Experience —*required for WebDAV*.  
For more information, see the section *Windows Web Folders Client or the Windows Desktop Experience*.
- Use the **Internet Options, Security** tab to configure the **Trusted Sites** zone:
  - Add the CMS to the Internet Explorer Trusted Sites zone — *required*.  
For more information, see the section *Trusted Sites Zone*.
  - Enable Automatic Prompting for ActiveX Controls — *required for the Word Document field type*.  
For more information, see the section *Word Document Field Type Configuration*.
  - Enable launching programs and files in an IFRAME — *recommended for WebDAV*.  
For more information, see the section *WebDAV Configuration*.
  - Disable the Pop-up Blocker — *required*.  
For more information, see the section *Pop-up Blocker*.
  - Disable the SmartScreen/Phishing Filter — *recommended*.  
For more information, see the section *Disable the SmartScreen or Phishing Filter*.
  - Allow script-initiated windows without size or position constraints — *optional*.  
For more information, see the section *Minor Issues*.
  - Allow websites to open windows without the address or status bars — *optional*.  
For more information, see section *Minor Issues*.
  - Enable Programmatic clipboard access — *optional*.  
For more information, see the section *Minor Issues*.
  - Display mixed content — *optional*.  
For more information, see the section *Minor Issues*.
- Ensure that the WebClient Windows Service is active (**required for WebDAV**).
- On the **Internet Options, General** tab:
  - Select the tab preferences that you want to use (optional) — see the section *New Windows or New Tabs*.
  - Configure the browser cache (optional) — see the section *Configure Management of Temporary Internet Files*.
- On the **Internet Options, Advanced** tab:
  - Select the **Empty temporary internet files folder when browser is closed** option — *optional*.  
For more information, see the section *Configure Management of Temporary Internet Files*.
  - Clear the **Disable script debugging** check box — *optional*.

For more information, see the section *Miscellaneous Settings*.

- Display a notification about every script error — *optional*.

For more information, see the section *Miscellaneous Settings*.

- Disable Reuse windows for launching shortcuts — *optional*.

For more information, see the section *Miscellaneous Settings*.

- Disable Show friendly HTTP error messages — *optional*.

For more information, see the section *Miscellaneous Settings*.

- Disable session merging — *optional*.

For more information, see the section *Internet Explorer 8, 9, and 10 Session Merging*.

- Configure concurrent HTTP request limits (optional) — see the section *Concurrent HTTP Request Limits*.



## 2.3 Required Configuration

This section describes the configuration that you should apply to every instance of Internet Explorer that you use to access Sitecore.

### Important

Backup the system before making any changes.

### Important

Before configuring Internet Explorer, close all the Internet Explorer windows, and only open Internet Explorer when needed. After any configuration task, close all the Internet Explorer windows. Reboot the computer after you make any registry changes.

### 2.3.1 Trusted Sites Zone

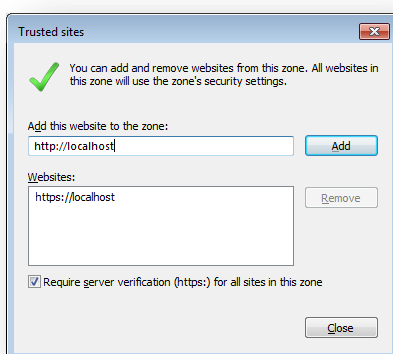
In Internet Explorer, Add all the Sitecore instances to the Trusted Sites zone.

To add a Sitecore instance to the Trusted Sites zone in Internet Explorer 8, 9, and 10:

1. Ensure that there is only one open instance of **Internet Explorer**.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Internet Options** and the **Internet Options** dialog box appears.
3. In the **Internet Options** dialog box, click the **Security** tab.
4. On the **Security** tab, click the **Trusted Sites** zone, and then click **Sites**. The **Trusted sites** dialog box appears.



5. In the **Trusted sites** dialog box, in the **Add this Website to the zone** field, enter the URL of the Sitecore instance, such as `http://localhost`.



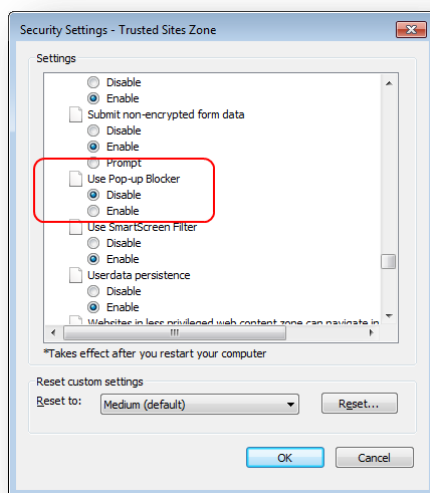
6. If the Sitecore instance does not use the HTTPS protocol, in the **Trusted Sites** dialog box, clear the **Require server verification (https:) for all sites in this zone** check box.
7. In the **Trusted sites** dialog box, click **Add**, and then click **Close**.

## 2.3.2 Pop-up Blocker

You can enable pop-ups for the sites that are listed the Internet Explorer Trusted Sites zone or for individual Sitecore instances.

To enable pop-ups for all the sites in the Internet Explorer Trusted Sites zone in Internet Explorer 8:

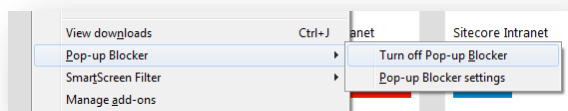
1. Ensure that there is only one open instance of **Internet Explorer**.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Internet Options**. The **Internet Options** dialog box appears.
3. In the **Internet Options** dialog box, click the **Security** tab.
4. On the **Security** tab, click the **Trusted Sites** zone, and then click **Custom Level**. The **Security Settings - Trusted Sites Zone** dialog box appears.
5. In the **Security Settings - Trusted Sites Zone** dialog box, in the **Miscellaneous** section, under **Use Pop-up Blocker**, select **Disable**, and then click **OK**.



6. If a confirmation prompt appears, click **Yes**.

To enable pop-ups for all the sites in the Internet Explorer Trusted Sites zone in Internet Explorer 9 and 10:

1. Ensure that there is only one open instance of **Internet Explorer**.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Pop-Up Blocker**, **Turn off Pop-up Blocker**.



Alternatively, to enable pop-ups for an individual Sitecore instance, access that instance of Sitecore. When the Internet Explorer Information Bar appears at the top or bottom of the browser window (depending on the browser version) to indicate that Internet Explorer has blocked a pop-up:

1. If an **Information Bar** alert appears, click **Close**.
2. In **Internet Explorer**, right-click the **Information Bar**, then click **Pop-Up Blocked**, and then click **Always Allow Pop-ups from This Site**. If a confirmation prompt appears, click **Yes**.

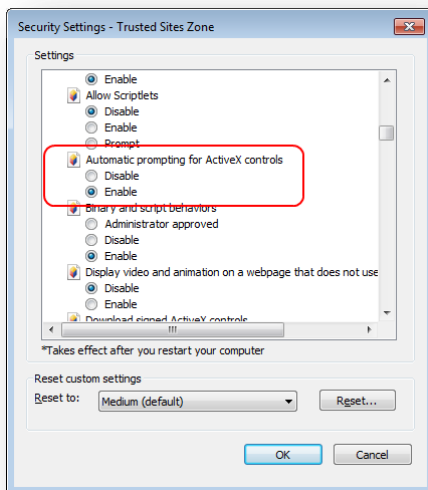
**Important**

Disable any additional pop-up blockers, or configure them to allow pop-ups for Sitecore.

**2.3.3 Word Document Field Type Configuration**

To configure Internet Explorer to support the Word Document field type:

1. Ensure that there is only one open instance of **Internet Explorer**.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Internet Options**. The **Internet Options** dialog box appears.
3. In the **Internet Options** dialog, click the **Security** tab.
4. On the **Security** tab, click the **Trusted Sites** zone, and then click **Custom Level**. The **Security Settings Trusted Sites Zone** dialog box appears.
5. In the **Security Settings Trusted Sites Zone** dialog box, in the **ActiveX controls and plug-ins** section, under **Automatic prompting for ActiveX controls**, select **Enable**, and then click **OK**.



6. If a confirmation prompt appears, click **Yes**.

If you would prefer not to enable automatic prompting, install the Word OCX control as follows:

1. Extract the contents of the `/sitecore/shell/Applications/Content Manager/officeviewer.cab` file to a temporary directory.
2. Open a Windows command prompt as a local administrator.
3. In the Windows command prompt, navigate to the directory that contains the files you just extracted.
4. In the Windows command prompt, execute the following command:

```
regsvr32 officeviewer.ocx
```

**Note**

You can use the following command to uninstall the Word OCX control:

```
regsvr32 /u officeviewer.ocx
```

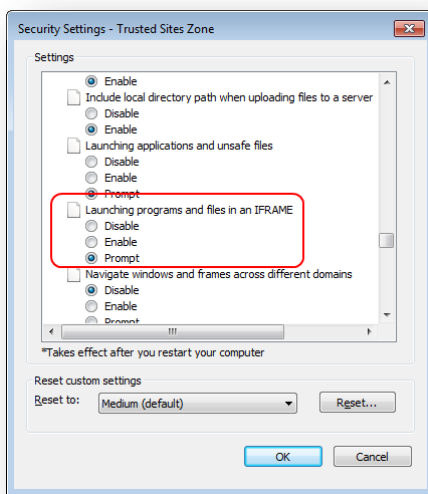
**Note**

After installing or uninstalling the Word OCX control, you can delete the files you extracted previously.

## 2.3.4 WebDAV Configuration

To configure Internet Explorer to support WebDAV and the File Drop Area field type:

1. Ensure that there is only one open instance of **Internet Explorer**.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Internet Options**. The **Internet Options** dialog box appears.
3. In the **Internet Options** dialog box, click the **Security** tab.
4. On the **Security** tab, click the **Trusted Sites** zone, and then click **Custom Level**. The **Security Settings Trusted Sites Zone** dialog box appears.
5. In the **Security Settings Trusted Sites Zone** dialog box, in the **Miscellaneous** section, under **Launching programs and files in an IFRAME**, select **Enable**, and then click **OK**.



6. If a confirmation prompt appears, click **Yes**.

## Windows Web Folders Client or the Windows Desktop Experience

If you want the client to use the Sitecore WebDAV features, install the Microsoft Windows Web Folders Client, including any available updates.

On Windows 2008, install the Windows Desktop Experience.

For more information, see <http://www.microsoft.com/downloads/details.aspx?FamilyId=17C36612-632E-4C04-9382-987622ED1D64&displaylang=en>.

## The WebClient Windows Service

The Internet Explorer WebDAV implementation depends on the WebClient Windows service. Ensure that the WebClient Windows service is active and configured to start automatically.

## 2.4 Recommended Configuration

This section describes the extra Internet Explorer configuration that Sitecore recommends.

### 2.4.1 Disable the SmartScreen or Phishing Filter

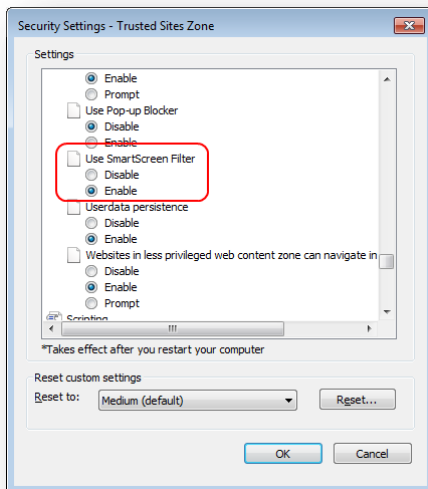
The SmartScreen Filter — previously known as the Phishing Filter — may adversely affect the performance of Sitecore clients.

Disabling the SmartScreen or Phishing filter can improve browser performance.

#### Internet Explorer 8

To disable the SmartScreen Filter for all the websites in the Internet Explorer Trusted Sites zone in Internet Explorer 8:

1. Ensure that there is only one open instance of **Internet Explorer**.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Internet Options**. The **Internet Options** dialog box appears.
3. In the **Internet Options** dialog box, click the **Security** tab.
4. On the **Security** tab, click the **Trusted Sites** zone, and then click **Custom Level**. The **Security Settings Trusted Sites Zone** dialog box appears.
5. In the **Security Settings Trusted Sites Zone** dialog box, in the **Miscellaneous** section, under **Use SmartScreen Filter**, select **Disable**, and then click **OK**.



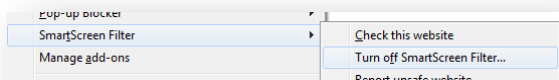
6. If a confirmation prompt appears, click **Yes**.

#### Internet Explorer 9 and 10

To disable the SmartScreen Filter for all sites in the Internet Explorer Trusted Sites zone in Internet Explorer 9 and 10:

1. Ensure that there is only one open instance of **Internet Explorer**.

- In **Internet Explorer**, click the **Tools** menu or press ALT-T, select **SmartScreen Filter**, and then click **Turn off SmartScreen Filter**.



## 2.4.2 Install Adobe Flash

To install Adobe Flash in Internet Explorer 8, 9, and 10:

- In **Internet Explorer**, open <http://get.adobe.com/flashplayer/>.
- On the <http://get.adobe.com/flashplayer/> webpage, clear the **Install Google Chrome** check box.
- Follow the tips displayed on the page.

### Note

The default user interface that you use to upload files to the Sitecore media library uses Adobe Flash. Some reporting interfaces in the Digital Marketing Suite (DMS) require Adobe Flash.

If you cannot install Adobe Flash, you can configure Sitecore to use an HTML user interface to upload media by changing the `Upload.Classic` setting in the `web.config` file on the Sitecore server to `true`.

## 2.4.3 Minor Issues

This section describes the configuration that you should apply to avoid various minor issues.

To avoid various minor issues in Internet Explorer:

- Ensure that there is only one open instance of **Internet Explorer**.
- In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Internet Options**. The **Internet Options** dialog box appears.
- In the **Internet Options** dialog box, click the **Security** tab.
- On the **Security** tab, click the **Trusted Sites** zone, and then click **Custom Level**. The **Security Settings - Trusted Sites Zone** dialog box appears.
- In the **Security Settings - Trusted Sites Zone** dialog box, in the **Miscellaneous** section, select the following settings:

Setting	Value
<b>Allow script-initiated windows without size or position constraints</b>	Enable
<b>Allow websites to open windows without address or status bars</b>	Enable
<b>Display mixed content</b>	Enable

### Note

In the **Security Settings Trusted Sites Zone** dialog box, in the **Scripting** section, under **Allow Programmatic clipboard access**, select **Enable**. The **Allow Programmatic clipboard access** setting only applies to content management environments that use the HTTPS protocol.

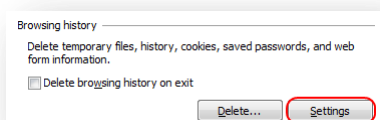
- In the **Security Settings trusted Sites Zone** dialog box, click **OK**.
- If a confirmation prompt appears, click **Yes**.

## 2.4.4 Configure Management of Temporary Internet Files

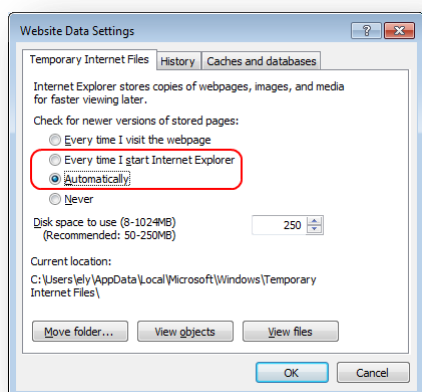
To increase the stability of Internet Explorer at the cost of performance, you can configure some Internet Explorer caching options.

To configure the browser cache in Internet Explorer 8, 9, and 10:

1. Ensure that there is only one open instance of **Internet Explorer**.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Internet Options**. The **Internet Options** dialog box appears.
3. In the **Internet Options** dialog box, click the **General** tab.
4. On the **General** tab in the **Browsing history** section, click **Settings**. The **Website Data Settings** dialog box appears.



5. In the **Website Data Settings** dialog box, on the **Temporary Internet Files** tab, in the **Check for newer versions of stored pages** setting, select the **Automatically** or the **Every time I Start Internet Explorer** option, and then click **OK**.



**Note**

If you select to clear the cache **Automatically**, you may experience improved performance with Sitecore and other browser-based Web sites and applications. Clear the browser cache manually if you experience any issues. If you select **Every Time I Start Internet Explorer**, you should rarely need to clear the browser cache manually.

To configure Internet Explorer 8 to clear the cache when Internet Explorer closes:

1. Ensure that there is only one open instance of **Internet Explorer**.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Internet Options**. The **Internet Options** dialog box appears.
3. In the **Internet Options** dialog box, click the **Advanced** tab.
4. In the **Settings** field, scroll down to the **Security** section and select the **Empty Temporary Internet Files folder when browser is closed** check box, and then click **OK**.

To configure Internet Explorer 9 and 10 to clear the cache when Internet Explorer closes:

1. Ensure that there is only one open instance of **Internet Explorer**.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Internet Options**. The **Internet Options** dialog box appears.
3. Select the **Delete browsing history on exit** check box.

**Warning**

While it may assist with some cases of cache corruption, you cannot rely on this setting to clear the browser cache. For example, if Internet Explorer crashes, then Internet Explorer may not clear the browser cache.



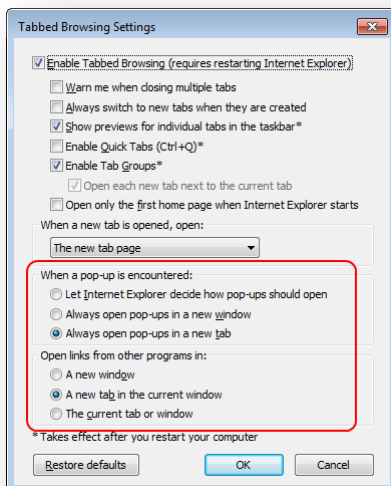
## 2.5 Optional Configuration

This section describes optional techniques and Internet Explorer configuration that you can apply to achieve specific objectives and address various issues.

### 2.5.1 New Windows or New Tabs

To control whether Internet Explorer 9 and 10 open pop-ups as new windows or as new tabs:

1. Ensure that there is only one open instance of **Internet Explorer**.
2. Click the **Tools** menu or press ALT-T, and then click **Internet Options**. The **Internet Options** dialog box appears.
3. In the **Internet Options** dialog box, click the **General** tab, and then click **Tabs**. The **Tabbed Browsing Settings** dialog box appears. In earlier versions of IE (Internet Explorer 8), on the **General** tab in the **Tabs** section, click **Settings**.
4. In the **Tabbed Browsing Settings** dialog box, to control how Internet Explorer handles pop-ups, select an option in the **When a pop-up is encountered** section.
5. In the **Tabbed Browsing Settings** dialog box, to control how Internet Explorer opens links activated from other applications, such as email clients, select an option under **Open links from other programs**.



### 2.5.2 Internet Explorer 8, 9, and 10 Session Merging

Internet Explorer 8 introduced a feature known as Merged Frame Process, or MFP. MFP shares client session data, including authentication and other cookies, between all Internet Explorer tabs and windows. New Internet Explorer processes merge with an existing Internet Explorer process and then terminate. The new browser window uses session data from the pre-existing Internet Explorer process.

MFP presents limitations for users, including Sitecore developers that work in multiple Sitecore modes and security contexts. You can use any of the techniques described in this section to work in multiple Internet Explorer sessions.

#### The New Session Command

To open a window in a new session, click the **File** menu or press ALT-F, and then click **New Session**.

## The -NoSessionMerging Command Line Parameter

To open a new browser window with a new session, add the `-NoSessionMerging` parameter to the command line:

```
iexplore -NoSessionMerging http://localhost/sitecore
```

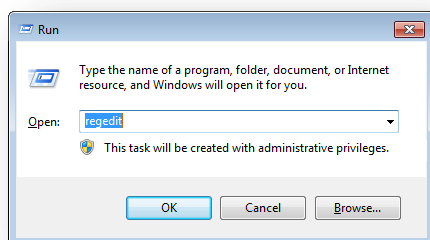
## The SessionMerging Registry Setting

To disable session merging for all new Internet Explorer processes for a Windows user:

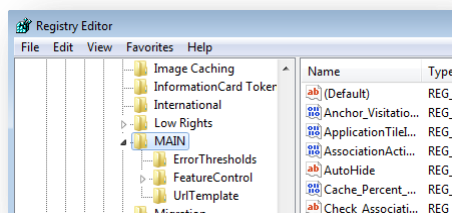
### Warning

Backup the system before updating the registry, and be cautious when working in the Registry Editor.

1. Hold down the **WINDOWS** key and press **R**. The **Run** dialog box appears.
2. In the **Run** dialog box, type `regedit`, click **OK** and the **Registry Editor** appears.



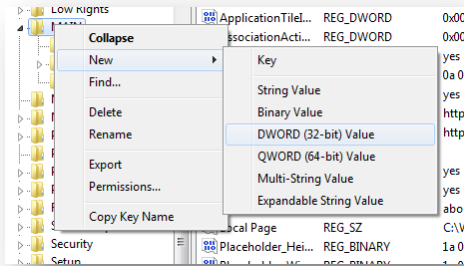
3. In the **Registry Editor**, expand `HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main`.



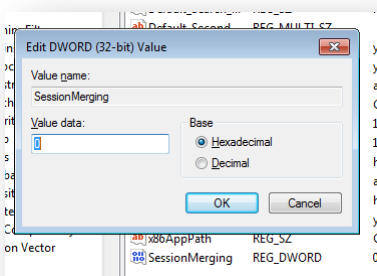
### Note

You may be able to apply this setting for all Windows users by making the corresponding change under `HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main` instead of under `HKEY_CURRENT_USER`.

4. In the **Registry Editor**, right-click **Internet Options**, and then select **New DWORD (32-bit) Value**. Name the new entry **SessionMerging**.



5. In the **Registry Editor**, right-click **SessionMerging**, and then select **Modify**. The **Edit DWORD (32-bit) Value** dialog box appears.



6. In the **Edit DWORD (32-bit) Value** dialog box, for **Value data**, enter **0**, and then click **OK**.
7. Reboot.

### 2.5.3 Concurrent HTTP Request Limits

In some cases, you can improve the performance of Internet Explorer by configuring it to allow more than the default number of concurrent HTTP requests to a single Web server.

#### Warning

Backup the system before updating the registry, and be cautious when working in the Registry Editor.

#### Important

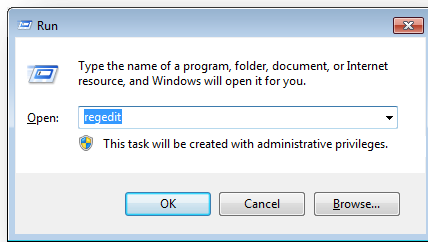
Do not exceed the concurrent request limits of the Web servers that you access. Three clients configured to allow two concurrent requests can exceed this limit.

#### Note

This change may apply to other user agents installed on the same machine and used by the same user.

To configure a Windows account to allow more than the default number of HTTP connections to any single Web server:

1. Hold down the **WINDOWS** key and press **R**. The **Run** dialog box appears. In the **Run** dialog box, type `regedit`, and then click **OK**. The Registry Editor appears.



2. In the **Registry Editor**, expand `HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings`.

#### Note

You may be able to apply this setting for all Windows users by making the corresponding change under

`HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings` instead of under `HKEY_CURRENT_USER`.

3. In the **Registry Editor**, right-click **Internet Settings**, and then click **New, DWORD (32-bit) Value**. Name the new entry `MaxConnectionsPer1_0Server`.
4. In the **Registry Editor**, double-click `MaxConnectionsPer1_0Server`. The **Edit DWORD (32-bit) Value** dialog box appears.
5. In the **Edit DWORD (32-bit) Value** dialog box, select **Decimal**, and then for **Value data**, enter the maximum number of concurrent connections to allow for HTTP 1.0 servers, and then click **OK**.
6. In the **Registry Editor**, right-click **Internet Settings**, and then select **New DWORD (32-bit) Value**. Name the new entry `MaxConnectionsPerServer`.
7. In the **Registry Editor**, right-click `MaxConnectionsPerServer`, and then select **Modify**. The **Edit DWORD (32-bit) Value** dialog box appears.
8. In the **Edit DWORD (32-bit) Value** dialog box, select **Decimal**, and for **Value data**, enter the maximum number of concurrent connections to allow for HTTP 1.1 servers, and then click **OK**.
9. Reboot.

## 2.5.4 Miscellaneous Settings

You can choose to follow any of the following suggestions:

1. In **Internet Explorer**, click the **Tools** menu or press **ALT-T**, and then click **Internet Options**. The **Internet Options** dialog box appears.
2. In the **Internet Options** dialog box, click the **Advanced** tab.
3. On the **Advanced** tab, in the **Browsing** section:

Setting	Value
<b>Disable script debugging (Internet Explorer)</b>	Clear

Setting	Value
Display a notification about every script error	Select
Reuse windows for launching shortcuts (when tabbed browsing is off)	Clear
Show friendly HTTP error messages	Clear

4. In the **Internet Options** dialog box, click **OK**.

## Chapter 3

# Troubleshooting Microsoft Internet Explorer

This chapter contains instructions for troubleshooting issues with Internet Explorer. Some of these considerations may also apply to other browsers, although the UI instructions may differ from browser to browser.

This chapter contains the following sections:

- Troubleshooting Process
- Additional Troubleshooting Resources

## 3.1 Troubleshooting Process

This section describes the process that you can follow to troubleshoot issues with Internet Explorer. To summarize the troubleshooting process:

- Check Sitecore Client Requirements.
- Check Browser Configuration.
- Disable Browser Plug-ins.
- Clear Browser Temporary Files.
- Patch Windows and Components.
- Check Internet Security Software.
- Reset Internet Explorer Configuration.
- Reproduce the Issue Using another Browser.
- Reproduce the Issue as another User.
- Reproduce the Issue from another Machine.

### 3.1.1 Check Sitecore Client Requirements

Ensure that the client meets the Sitecore client requirements. For more information about the Sitecore client requirements, see the Sitecore CMS installation guide for the version that you are using.

### 3.1.2 Check Browser Configuration

Ensure that you have correctly followed the appropriate steps outlined in this document.

### 3.1.3 Disable Browser Plug-ins

Uninstall or disable any browser plug-ins such as toolbars, pop-up blockers, and other components.

### 3.1.4 Clear Browser Temporary Files

Users are unable to reproduce numerous issues after clearing the Internet Explorer cache or all temporary files.

#### **Important**

To force Internet Explorer to retrieve any updated resources, you should always clear the browser cache after upgrading Sitecore.

To clear the browser cache in Internet Explorer 8, 9 and 10:

1. Ensure that there is only one open instance of **Internet Explorer**.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Delete browsing history**. The **Delete Browsing History** dialog box appears.
3. In the **Delete Browsing History** dialog box, ensure that **Temporary Internet Files** is the only selection, and then click **Delete**.
4. Close **Internet Explorer**.

If the issue persists:

**Important**

To avoid losing personal data, skip this step, and return to this section after exhausting all other troubleshooting options.

**Note**

In some environments, instead of deleting all of the browser cookies, you may be able to delete only the cookie associated with the Sitecore instance.

1. Ensure that there is only one open instance of **Internet Explorer**.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Delete browsing history**. The **Delete Browsing History** dialog box appears.
3. In the **Delete Browsing History** dialog box, clear the **Preserve Favorites website data** check box, select all of the other options, and then click **Delete**.
4. Close **Internet Explorer**.

### 3.1.5 Patch Windows and Components

Use Windows Update to patch Windows, Internet Explorer, MSXML, and other system components. Reboot even if no updates were available.

### 3.1.6 Check Internet Security Software

Software firewalls, antivirus, and other Internet security software can adversely affect Web applications. To determine if the issue could be a software conflict:

1. Disable your security software,
2. Close every **Internet Explorer** window.
3. Clear the **Internet Explorer** cache as described in the section *Clear Browser Temporary Files*.
4. Reboot.
5. Attempt the failed operation again.

If you cannot reproduce an issue with the security software disabled, and can reproduce that issue with that software enabled, then contact Sitecore as described in the section *Additional Troubleshooting Resources*.

### 3.1.7 Reset Internet Explorer Configuration

If you cannot determine the cause of an issue, you can reset Internet Explorer to its default state, and then apply the configuration described in this document.

To reset the Internet Explorer configuration:

1. Ensure that there is only one open instance of **Internet Explorer**.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Internet Options**. The **Internet Options** dialog box appears.
3. In the **Internet Options** dialog box, click the **General** tab, and then in the **Tabs** section, click **Tabs**. The **Tabbed Browsing Settings** dialog box appears.
4. In the **Tabbed Browsing Settings** dialog box, click **Restore Defaults**, and then click **OK**.
5. In the **Internet Options** dialog box, click the **Security** tab, then click **Trusted Sites**, and then click **Default Level**.



6. In the **Internet Options** dialog box, click the **Advanced** tab, and then click **Restore Advanced Settings**.
7. In the **Internet Options** dialog box, on the **Advanced** tab, click **Reset**, acknowledge the prompt, and then click **OK**.
8. Close every **Internet Explorer** window.
9. Apply the configuration that is described in this document.

### 3.1.8 Reproduce the Issue Using another Browser

An issue that you cannot reproduce using another browser probably results from the Internet Explorer configuration or the cache. If you can reproduce the issue using multiple browsers, the root cause may be something other than Internet Explorer configuration, such as the network or server configuration.

### 3.1.9 Reproduce the Issue as another User

An issue that you cannot reproduce as another user likely results from permissions, browser cookies, profile settings, or other user-specific configuration.

### 3.1.10 Reproduce the Issue from another Machine

An issue that does not result from browser or user configuration and that you cannot reproduce from another machine is likely to result from machine or network configuration.

## 3.2 Additional Troubleshooting Resources

If you cannot resolve an issue after applying the instructions in this document, check for proper server configuration. Describe the issue and the troubleshooting steps you have attempted using the General Forum on the Sitecore Developer Network. If you are a certified Sitecore developer, file a case in the Sitecore Support Portal. Otherwise, have a certified Sitecore developer in your organization investigate your configuration and file a case on your behalf.

**Tip**

To copy an error message to the Windows clipboard, press `ALT-PRTSCLN` and paste the image into a document or email message.

## Chapter 4

# Configuring Other Browsers

This chapter describes the configuration issues that are related to other popular browsers.

This chapter contains the following sections:

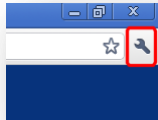
- Enabling Pop-up Windows in Google Chrome
- Enabling Pop-up Windows in Other Browsers
- Preventing Mozilla Firefox from Showing Confirmation Dialog Box in the Page Editor

## 4.1 Enabling Pop-up Windows in Google Chrome

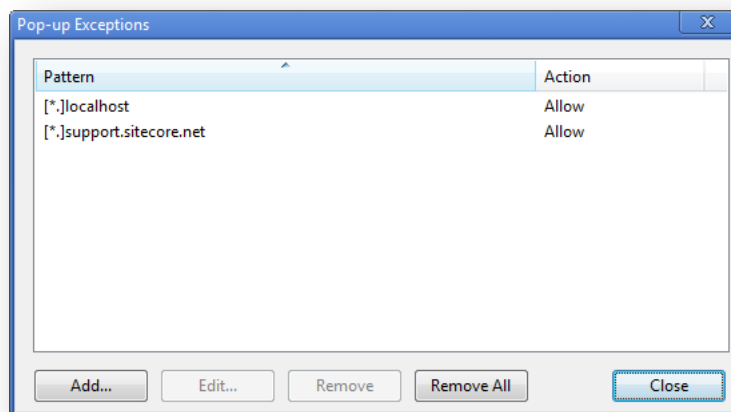
Google Chrome can run Sitecore but does not have pop-ups enabled by default. Create an exception in Google Chrome to only allow pop-ups for Sitecore web sites. This requires you to make an exception in the Content Settings window.

To create an exception in Google Chrome:

1. Open your Google Chrome browser.
2. Click the Spanner icon in the top right of the browser window: *Customize and control Google Chrome*.



3. In the drop-down menu, click **Options**.
4. Click the **Under the Hood** tab.
5. In **Privacy**, click **Content settings**.
6. In the **Content Settings** window, click **Pop-ups** and then select the **do not allow any site to show pop-ups (recommended)** radio button.
7. Click **Exceptions** to open the **Pop-up Exceptions** window.



8. In the **Pop-up Exceptions** window, add the following exceptions:

```
[*.]localhost  
[*.]support.sitecore.net
```

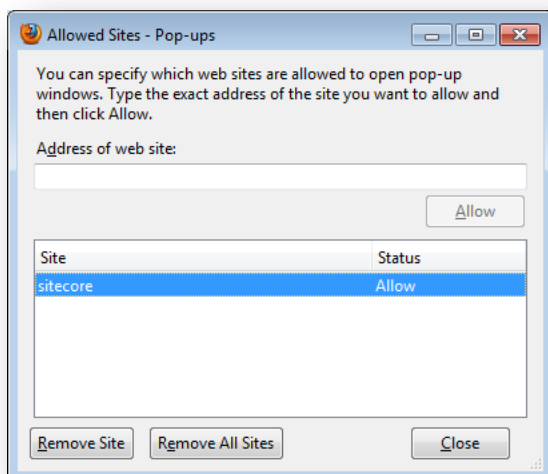
This ensures that pop-ups are blocked on all web sites unless it is a Sitecore site or running on local host.

9. Click **Close** and return to your web browser.

## 4.2 Enabling Pop-up Windows in Other Browsers

In Mozilla Firefox and Apple Safari it is not necessary to enable pop-up windows.

In Firefox, when you first open Sitecore you are prompted to enable or block pop-ups. An exception for Sitecore is added to the **Allowed Sites** window in Firefox.



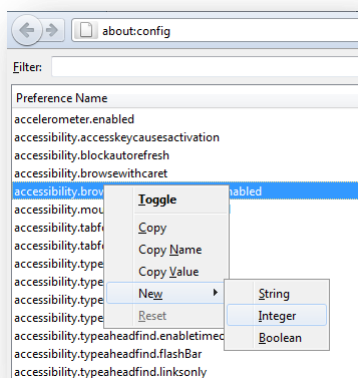
To view allowed sites in a Firefox browser:

1. Click **Tools, Options**, and then click the **Content** tab.
2. Ensure the **Block pop-up windows** check box is selected, and then click **Exceptions**.

### 4.3 Preventing Mozilla Firefox from Showing Confirmation Dialog Box in the Page Editor

In the Page Editor, Mozilla Firefox may show the *Prevent this page from creating additional dialogs* confirmation dialog box if you open modal dialogs too often. To prevent Mozilla Firefox from showing this confirmation dialog box:

1. In the browser address bar, enter *about:config*.
2. Right-click on the preferences area and then click **New, Integer**.



3. In the **New Integer Value** dialog box, enter *dom.successive\_dialog\_time\_limit* and click **Ok**.
4. In the **Enter Integer Value** dialog box, enter *0* and click **OK**.