Sitecore CMS 6.2

Internet Explorer Configuration Reference

Optimize Microsoft Internet Explorer for Use with Sitecore

Table of Contents

Chapter 1

Introduction

This document describes required, recommended, and optional configuration to optimize the Microsoft Internet Explorer Web browser for use with Sitecore, along with instructions to troubleshoot issues with the browser.

This document contains the following chapters:

- Chapter 1 — Introduction
- Chapter 2 — Configuring Internet Explorer
- Chapter 3 — Troubleshooting Internet Explorer

Chapter 2

Configuring Internet Explorer

This chapter provides required, recommended, and optional instructions to configure Microsoft Internet Explorer for use with Sitecore.

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 the version of Internet Explorer installed:

- In **Internet Explorer**, click the **Help** menu or press ALT-H, and then click **About Internet Explorer**. The **About Internet Explorer dialog appears**, indicating the Internet Explorer version number.

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

Note
Sitecore supports Microsoft Internet Explorer 6 and higher. Sitecore recommends Internet Explorer 7 or higher. To update the Internet Explorer version, see the section Patch Windows and Components.

Note
This document does not describe configuration of Internet Explorer 6. Internet Explorer 6 users, to the extent possible, apply configuration that corresponds to the instructions in this document.

2.2 Internet Explorer Configuration Summary

This section summarizes the Internet Explorer configuration described in this document. After you are familiar with the configuration process, you can use this summary as a configuration checklist.

- Install Adobe Flash (**recommended**) — see Install Adobe Flash.
- Install Windows Web Folders or the Windows Desktop Experience (**required for WebDAV**) — see 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**) — see the section Trusted Sites Zone.
    - Enable Automatic Prompting for ActiveX Controls (**required for the Word Document field type**) — see the section Word Document Field Type .
    - Enable Launching programs and files in an IFRAME (**recommended for WebDAV**) — see the section WebDAV Configuration.
    - Ensure that the WebClient Windows Service is active (**required for WebDAV**).
    - Disable the Pop-up blocker (**required**) — see the section Pop-up Blocker.
    - Disable the SmartScreen/Phishing Filter (**recommended**) — the section SmartScreen (Phishing) Filter.
    - Allow script-initiated windows without size or position constraints (optional) — see the section Cosmetic Issues.
    - Allow websites to open windows without address or status bars (optional) — see the section Cosmetic Issues.
    - Enable Programmatic clipboard access (optional) — see the section Cosmetic Issues.
    - Display mixed content (optional) — the section see Cosmetic Issues.
- Using the Internet Options General tab:
    - Select tab preferences (optional) — see the section New Windows or New Tabs.
    - Configure browser cache (optional) — see the section Configure Management of Temporary Internet Files.
- Using the Internet Options Advanced tab:
    - Empty temporary internet files folder when browser is closed (optional) — see the section Configure Management of Temporary Internet Files.
    - Enable script debugging (optional) — see the section Miscellaneous Settings.
    - Display a notification about every script error (optional) — see the section Miscellaneous Settings.
    - Disable Reuse windows for launching shortcuts (optional) — see the section Miscellaneous Settings.
    - Disable Show friendly HTTP error messages (optional) — see the section Miscellaneous Settings.
- Disable session merging (optional) — see the section Internet Explorer 8 Session Merging.
- Configure concurrent HTTP request limits (optional) — see the section Concurrent HTTP Request Limits.

2.3 Required Configuration

This section describes configuration you should apply to all installations of Internet Explorer used to access Sitecore.

Important
Backup the system before making any changes.

Important
Before performing any Internet Explorer configuration task, close all Internet Explorer windows, and open Internet Explorer only when needed. After any configuration task, close all Internet Explorer windows. Reboot after registry changes.

2.3.1 Trusted Sites Zone

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

To add a Sitecore instance to the Trusted Sites zone in Internet Explorer 7 or 8:

1. Close all Internet Explorer windows, and then open a single **Internet Explorer** window.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Internet Options**. The **Internet Options** dialog appears.
3. In the **Internet Options** dialog, click the **Security** tab.
4. In the **Internet Options** dialog, on the **Security** tab, click the **Trusted Sites** zone, and then click **Sites**. The **Trusted Sites** dialog appears.
5. In the **Trusted Sites** dialog, for **Add this Website to the zone**, enter the URL of the Sitecore instance, such as `http://localhost`.
6. If the Sitecore instance does not use the HTTPS protocol, then in the **Trusted Sites** dialog, disable **Require server verification (https:) for all sites in this zone**.
7. In the **Trusted Sites** dialog, click **Add**, and then click **Close**.

2.3.2 Pop-up Blocker

Enable pop-ups for sites in the Internet Explorer Trusted Sites zone or for individual Sitecore instances.

To enable pop-ups for all sites in the Internet Explorer Trusted Sites zone in Internet Explorer 7 or 8:

1. Close all Internet Explorer windows, and then open a single **Internet Explorer** window.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Internet Options**. The **Internet Options** dialog appears.
3. In the **Internet Options** dialog, click the **Security** tab, then click the **Trusted Sites** zone, and then click **Custom Level**. The **Security Settings Trusted Sites Zone** dialog appears.
4. In the **Security Settings Trusted Sites Zone** dialog, in the **Miscellaneous** section, under **Use Pop-up Blocker**, select **Disable**, and then click **OK**. If a confirmation prompt appears, then click **Yes**.

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 of the browser window to indicate that Internet Explorer has blocked a pop-up:

1. If an **Information Bar** alert appears, then 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, then 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. Close all Internet Explorer windows, and then open a single **Internet Explorer** window.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Internet Options**. The **Internet Options** dialog appears.
3. In the **Internet Options** dialog, click the **Security** tab, then click the **Trusted Sites** zone, and then click **Custom Level**. The **Security Settings Trusted Sites Zone** dialog appears.
4. In the **Security Settings Trusted Sites Zone** dialog, in the **ActiveX controls and plug-ins** section, under **Automatic Prompting for ActiveX Controls**, select **Enable**, and then click **OK**. If a confirmation prompt appears, then click **Yes**.

If you prefer not to enable automatic prompting, then you can use the following approach to install the Word OCX control:

1. Extract the contents of the file `/sitecore/shell/Applications/Content Manager/officeviewer.cab` to a temporary directory.
2. Start a Windows command prompt as a local administrator.
3. In the Windows command prompt, navigate to the directory that contains files extracted previously.
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 extracted previously.

2.3.4 WebDAV Configuration

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

1. Close all Internet Explorer windows, and then open a single **Internet Explorer** window.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Internet Options**. The **Internet Options** dialog appears.
3. In the **Internet Options** dialog, click the **Security** tab, then click the **Trusted Sites** zone, and then click **Custom Level**. The **Security Settings Trusted Sites Zone** dialog appears.
4. In the **Security Settings Trusted Sites Zone** dialog, in the **Miscellaneous** section, under **Launching programs and files in an IFRAME**, select **Enable**, and then click **OK**. If a confirmation prompt appears, then click **Yes**.

Windows Web Folders Client or the Windows Desktop Experience

If the client will use Sitecore WebDAV features, then install the Microsoft Windows Web Folders Client, including any available updates.[1] On Windows 2008, install the Windows Desktop Experience.

[1] 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 optional Internet Explorer configuration that Sitecore recommends.

2.4.1 SmartScreen (Phishing) Filter

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

Note
Disabling the SmartScreen or Phishing filter can improve browser performance.

Internet Explorer 7

To disable the Phishing Filter for all sites in the Internet Explorer Trusted Sites zone in Internet Explorer 7:

1. Close all Internet Explorer windows, and then open a single **Internet Explorer** window.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Internet Options**. The **Internet Options** dialog appears.
3. In the **Internet Options** dialog, click the **Security** tab, then click the **Trusted Sites** zone, and then click **Custom Level**. The **Security Settings Trusted Sites Zone** dialog appears.
4. In the **Security Settings Trusted Sites Zone** dialog, in the **Miscellaneous** section, under **Use Phishing Filter**, select **Disable**, and then click **OK**. If a confirmation prompt appears, then click **Yes**.

Internet Explorer 8

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

1. Close all Internet Explorer windows, and then open a single **Internet Explorer** window.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Internet Options**. The **Internet Options** dialog appears.
3. In the **Internet Options** dialog, click the **Security** tab, then click the **Trusted Sites** zone, and then click **Custom** Level. The **Security Settings Trusted Sites Zone** dialog appears.
4. In the **Security Settings Trusted Sites Zone** dialog, in the **Miscellaneous** section, under **Use SmartScreen Filter**, select **Disable**, and then click **OK**. If a confirmation prompt appears, then click **Yes**.

2.4.2 Install Adobe Flash

To install Adobe Flash in Internet Explorer 7 or 8:

1. In **Internet Explorer**, access http://get.adobe.com/flashplayer/.
2. In Internet Explorer, at http://get.adobe.com/flashplayer/, disable **Free Google Toolbar**.
3. In Internet Explorer, at http://get.adobe.com/flashplayer/, click **Agree and install now**. The **Internet Explorer Information Bar** appears at the top of the browser window.
4. In **Internet Explorer**, right-click the **Information Bar**, and then click **Install This Add-on for All Users on This Computer…**. The **Internet Explorer Security Warning** dialog appears.
5. In the **Internet Explorer Security Warning** dialog, click **Install**.
6. After installation, close all **Internet Explorer** windows.

Note
The default user interface to upload files into the Sitecore media library uses Adobe Flash. Some reporting interfaces in the Online Marketing Suite (OMS) require Adobe Flash.

Note
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 Cosmetic Issues

This section describes configuration you should apply to avoid various cosmetic issues.

To avoid various cosmetic issues in Internet Explorer 7 and 8:

1. Close all Internet Explorer windows, and then open a single **Internet Explorer** window.
2. In **Internet Explore**r, click the **Tools** menu or press ALT-T, and then click **Internet Options**. The **Internet Options** dialog appears.
3. In the **Internet Options** dialog, click the **Security** tab, then click the **Trusted Sites** zone, and then click **Custom Level**. The **Security Settings Trusted Sites Zone** dialog appears.
4. In the **Security Settings Trusted Sites Zone** dialog, in the **Miscellaneous** section, under **Allow script-initiated windows without size or position constraints**, select **Enable**.
5. In the **Security Settings Trusted Sites Zone** dialog, in the **Miscellaneous** section, under **Allow websites to open windows without address or status bars**, select **Enable**.
6. In the **Security Settings Trusted Sites Zone** dialog, in the **Scripting** section, under **Allow Programmatic clipboard access**, select **Enable**.
7. In the **Security Settings Trusted Sites Zone** dialog, in the **Miscellaneous** section, under **Display mixed content**, select **Enable**.

Note
This setting only applies to content management environments that use the HTTPS protocol.

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

2.4.4 Configure Management of Temporary Internet Files

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

To configure the browser cache in Internet Explorer 7 or 8:

1. Close all Internet Explorer windows, and then open a single **Internet Explorer** window.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Internet Options**. The **Internet Options** dialog appears.
3. In the **Internet Options** dialog, click the **General** tab.
4. In the **Internet Options** dialog, under **Browsing history**, click **Settings**. The **Temporary Internet Files and History Settings** dialog appears.
5. In the **Temporary Internet Files and History Settings** dialog, select **Automatically** or **Every time I Start Internet Explorer**, and then click **OK**.

Note
If you select to clear the cache **Automatically**, you may experience greater performance with Sitecore and other browser-based Web sites and applications. Clear the browser cache manually if

you experience any issue. If you select **Every Time I Start Internet Explorer**, you should rarely need to clear the browser cache manually.

To configure Internet Explorer 7 or 8 to clear the cache when Internet Explorer closes:

1. Close all Internet Explorer windows, and then open a single **Internet Explorer** window.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Internet Options**. The **Internet Options** dialog appears.
3. In the **Internet Options** dialog, click the **Advanced** tab.
4. In the **Internet Options** dialog, under **Security**, select **Empty Temporary Internet Files Folder when browser is closed**, and then click **OK**.

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 7 and 8 open pop-ups as new windows or as new tabs:

1. Close all Internet Explorer windows, and then open a single **Internet Explorer** window.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Internet Options**. The **Internet Options** dialog appears.
3. In the **Internet Options** dialog, click the **General** tab, and then under **Tabs**, click **Settings**. The **Tabbed Browsing Settings** dialog appears.
4. In the **Tabbed Browsing Settings** dialog, to control how Internet Explorer handles pop-ups, select an option under **When a pop-up is encountered**.
5. In the **Tabbed Browsing Settings** dialog, to control how Internet Explorer opens links activated from other applications, such as email clients, select an option under **Open links from other programs**.
6. In the **Tabbed Browsing Settings** dialog, click **OK**.

2.5.2 Internet Explorer 8 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. While holding down the WINDOWS key, press the R key. The Windows **Run** dialog appears. In the Windows **Run** dialog, type `regedit`, and then click **OK**. The **Registry Editor** appears.
2. 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`.

3. In the **Registry Editor**, right-click **Internet Options**, and then select **New DWORD (32-bit) Value**. Name the new entry `SessionMerging`.
4. In the **Registry Editor**, right-click **SessionMerging**, and then select **Modify**. The **Edit DWORD (32-bit) Value** dialog appears.
5. In the **Edit DWORD (32-bit) Value** dialog, for **Value data**, enter `0`, and then click **OK**.
6. Reboot.

2.5.3 Concurrent HTTP Request Limits

In some cases, you can improve Internet Explorer performance by configuring the Internet Explorer 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. For example, Windows XP limits IIS to five concurrent HTTP connections from all clients, responding to additional requests with HTTP errors, resulting in unpredictable browser behavior. 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. While holding down the WINDOWS key, press the R key. The Windows **Run** dialog appears. In the Windows **Run** dialog, 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 select **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 appears.
5. In the **Edit DWORD (32-bit) Value** dialog, 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 appears.
8. In the **Edit DWORD (32-bit) Value** dialog, 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 appears.
2. In the **Internet Options** dialog, click the **Advanced** tab.
3. In the **Internet Options** dialog, on the **Advanced** tab, under **Browsing**, disable **Disable script debugging (Internet Explorer)**.
4. In the **Internet Options** dialog, on the **Advanced** tab, under **Browsing**, select **Display a notification about every script error**.
5. In the **Internet Options** dialog, on the **Advanced** tab, under **Browsing**, disable **Reuse windows for launching shortcuts (when tabbed browsing is off)**.
6. In the **Internet Options** dialog, on the **Advanced** tab, under **Browsing**, disable **Show friendly HTTP error messages**.
7. In the **Internet Options** dialog, click OK.

Chapter 3

Troubleshooting Internet Explorer

This chapter contains instructions for troubleshooting issues with Internet Explorer.

This chapter contains the following sections:

- The Troubleshooting Process
- Additional Troubleshooting Resources

3.1 The Troubleshooting Process

This section describes steps in 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 Sitecore client requirements.[2]

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.

Important
Close all Internet Explorer windows and clear the browser cache after any troubleshooting operation that may have repopulated the cache.

To clear the browser cache in Internet Explorer 7 or 8:

1. Close all Internet Explorer windows, and then open a single **Internet Explorer** window.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Delete Browsing History**. The **Delete Browsing History** dialog appears.

[2] For more information about Sitecore client requirements, see http://sdn.sitecore.net/Products/Sitecore%20V5/Sitecore%20CMS%206/Installation.aspx.

3. In the **Delete Browsing History** dialog, 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. Close all Internet Explorer windows, and then open a single **Internet Explorer** window.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Delete Browsing History**. The **Delete Browsing History** dialog appears.
3. In the **Delete Browsing History** dialog, disable **Preserve Favorites** website data, then 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.[3] 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 software firewalls,
2. Close all Internet Explorer windows.
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 Internet Explorer configuration:

1. Close all Internet Explorer windows, and then open a single **Internet Explorer** window.
2. In **Internet Explorer**, click the **Tools** menu or press ALT-T, and then click **Internet Options**. The **Internet Options** dialog appears.

[3] http://update.microsoft.com.

3. In the **Internet Options** dialog, click the **General** tab, and then under **Tabs**, click **Settings**. The **Tabbed Browsing Settings** dialog appears.
4. In the **Tabbed Browsing Settings** dialog, click **Restore Defaults**, and then click **OK**.
5. In the **Internet Options** dialog, click the **Security** tab, then click **Trusted Sites**, and then click **Default Level**.
6. In the **Internet Options** dialog, click the **Advanced** tab, and then click **Restore Advanced Settings**.
7. In the **Internet Options** dialog, on the **Advanced** tab, click **Reset**, acknowledge the prompt, and then click **OK**.
8. Close all Internet Explorer windows.
9. Apply configuration as described in this document.

3.1.8 Reproduce the Issue Using another Browser

An issue that you cannot reproduce using another browser likely results from Internet Explorer configuration or cache. If you can reproduce the issue using multiple browsers, the root cause may be something other than Internet Explorer configuration, such as 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.[4] Describe the issue and the troubleshooting steps you have attempted using the General Forum on the Sitecore Developer Network.[5] If you are a certified Sitecore developer, file a case in the Sitecore Support Portal.[6] Otherwise, have a certified Sitecore developer in your organization investigate your configuration and file a case on your behalf.

Tip
You can press `ALT-PRTSCN` to copy an error message to the Windows clipboard, and paste that into a document or email message.

[4] http://sdn.sitecore.net/Products/Sitecore%20V5/Sitecore%20CMS%206/Installation.aspx and http://sdn.sitecore.net/Products/Sitecore%20V5/Sitecore%20CMS%206/Installation%20Troubleshooting.aspx.
[5] http://sdn.sitecore.net/Forum/ShowForum.aspx?ForumID=10.
[6] http://support.sitecore.net.