

This guide provides a procedure for initially configuring your Internet Explorer (IE) browser to use Flash Chat.

Please note that Chrome, Firefox and Safari (Mac) do not require configuration changes.

<b>Installing Adobe Flash Player (All Librarians using chat)</b> .....	1
<b>Configure Internet Explorer for Chat</b> .....	1
<b>Appendix A: Best practices</b> .....	9
<b>Appendix B: Internet Explorer Advanced Security Settings for the Internet Zone</b> .....	9


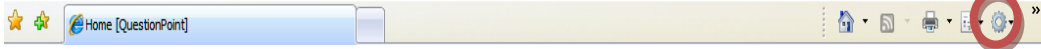
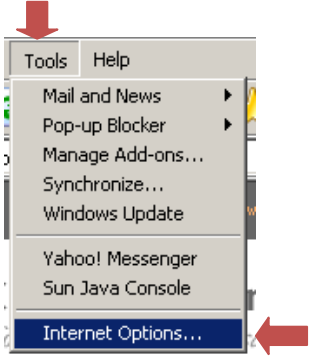
## Installing Adobe Flash Player For IE

Be sure to install Flash from the Adobe Flash download web page @

[http://www.adobe.com/shockwave/download/triggerpages\\_mmcom/flash.html](http://www.adobe.com/shockwave/download/triggerpages_mmcom/flash.html)

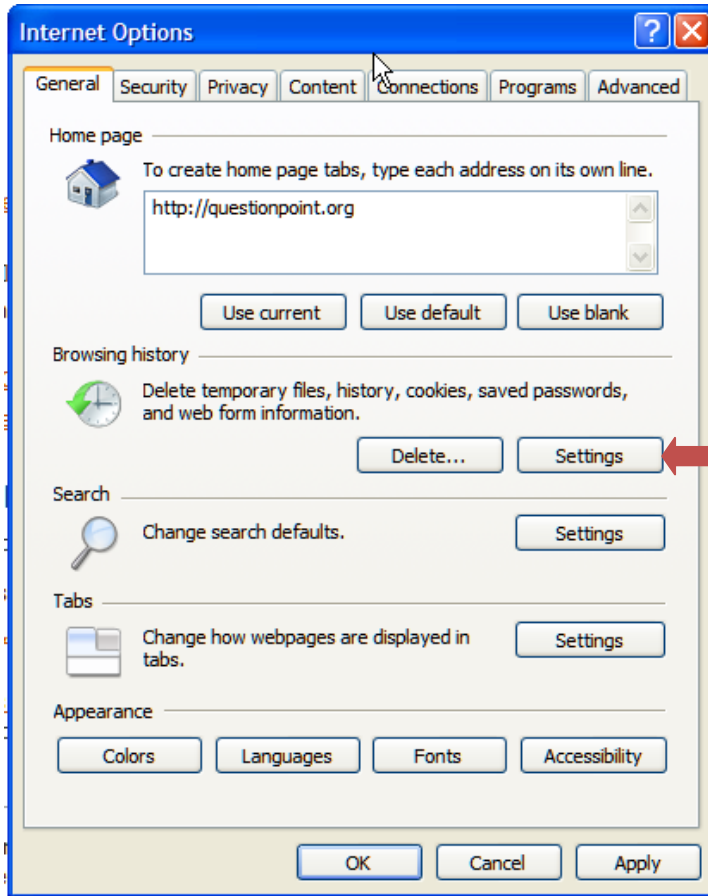
You will need to have ActiveX turned on for this download to install. Many Internet security and antivirus programs will block your ability to install a program using ActiveX. Please follow the directions provided by Adobe but if you are still having problems, contact your system administrator.

## Configure Internet Explorer for Chat

Step	Action
1	Launch Internet Explorer.
2	<p>Click the <b>Gear icon</b>  on the right side of the Command bar</p>  <p>If you do not see the command bar, you can hold down the ALT key and type O to open that menu. Click on <b>Internet Options</b> from the drop-down list.</p> 

**Step****Action**

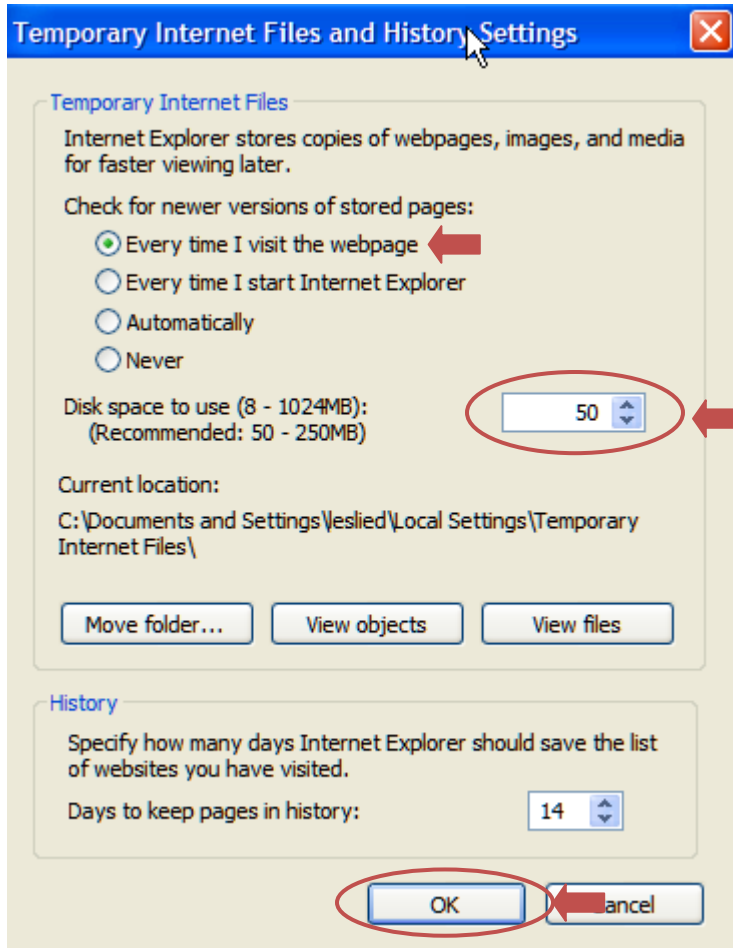
- 3 Click the **Settings** button on the Internet Options screen.



**Step**

**Action**

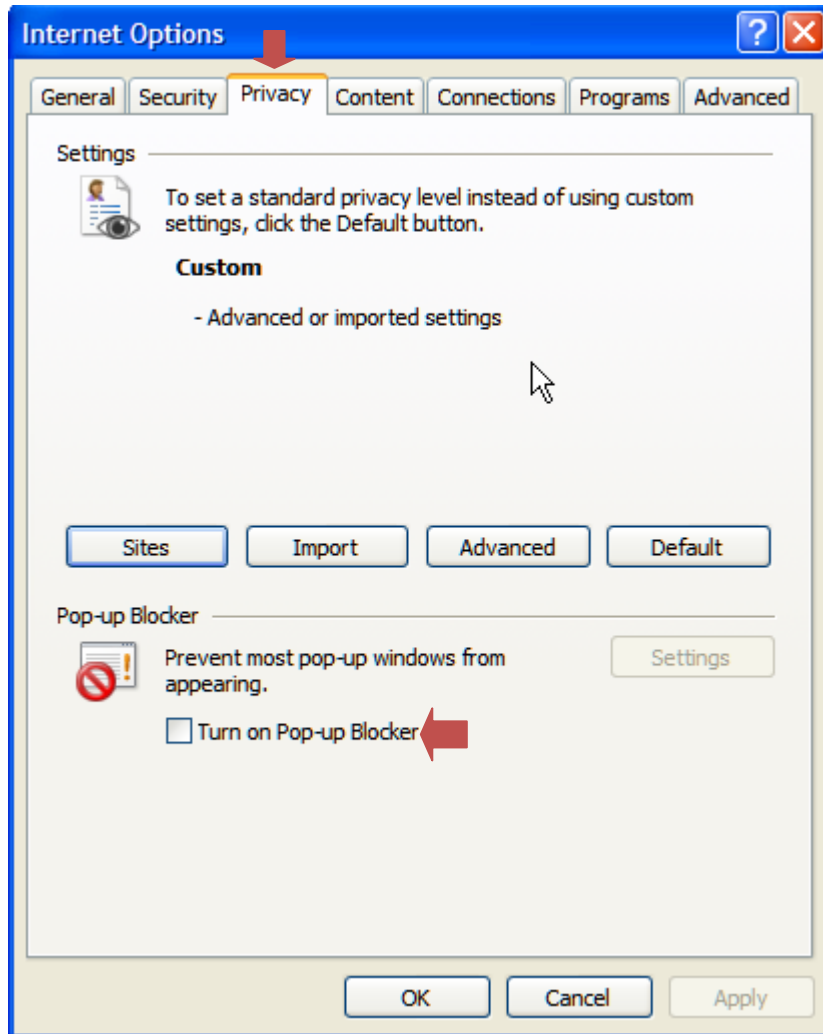
- 4 Click the radio button to the left of **Every visit to the page**, set the size of the **Temporary Internet files folder** to **50 MB\***, and Click **OK**.



\* This is different than the settings for Internet Explorer 6 due to the way temporary Internet files are handled by Internet Explorer 7 and Internet Explorer 8.

**Step****Action**

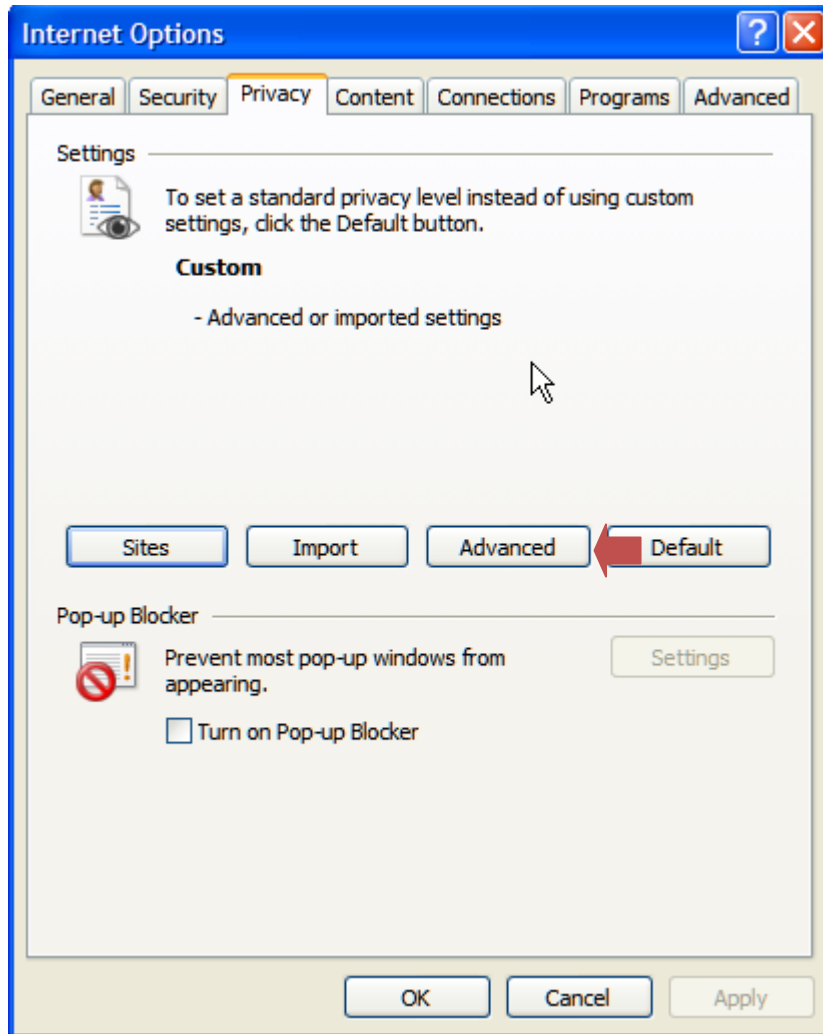
- 5 Click the **Privacy** tab in the *Internet Options* window.



Under Pop-up Blocker, remove the check in the box for **Turn on Pop-up Blocker**

**Step****Action**

6 Click on **Advanced**



7 Under "**Advanced Privacy Settings**", check "**Override automatic cookie handling**"

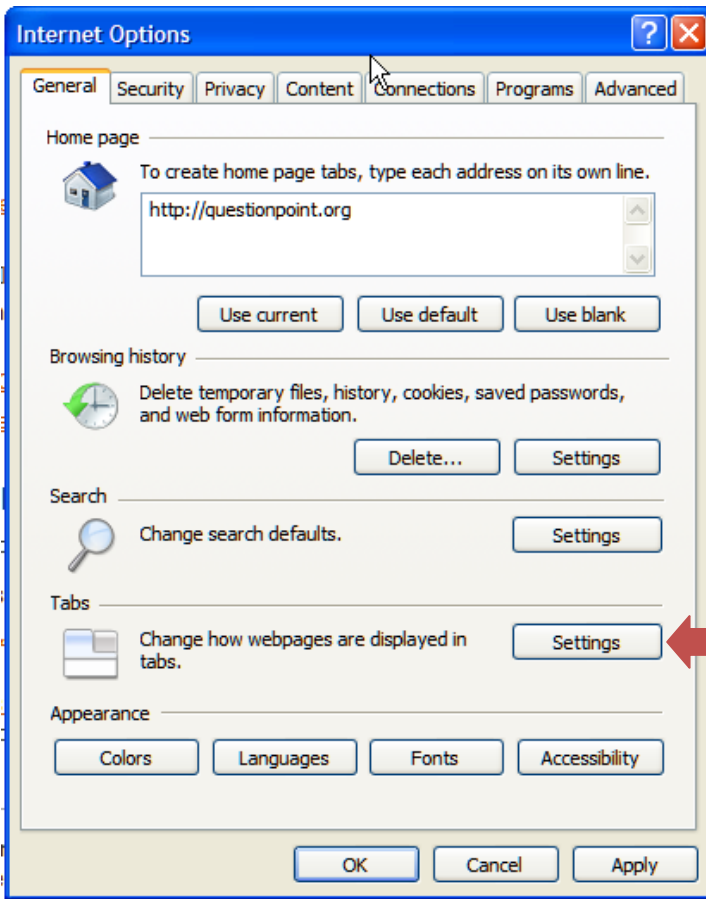


**Step** **Action**

8 Check "Always allow session cookies", and click "OK"

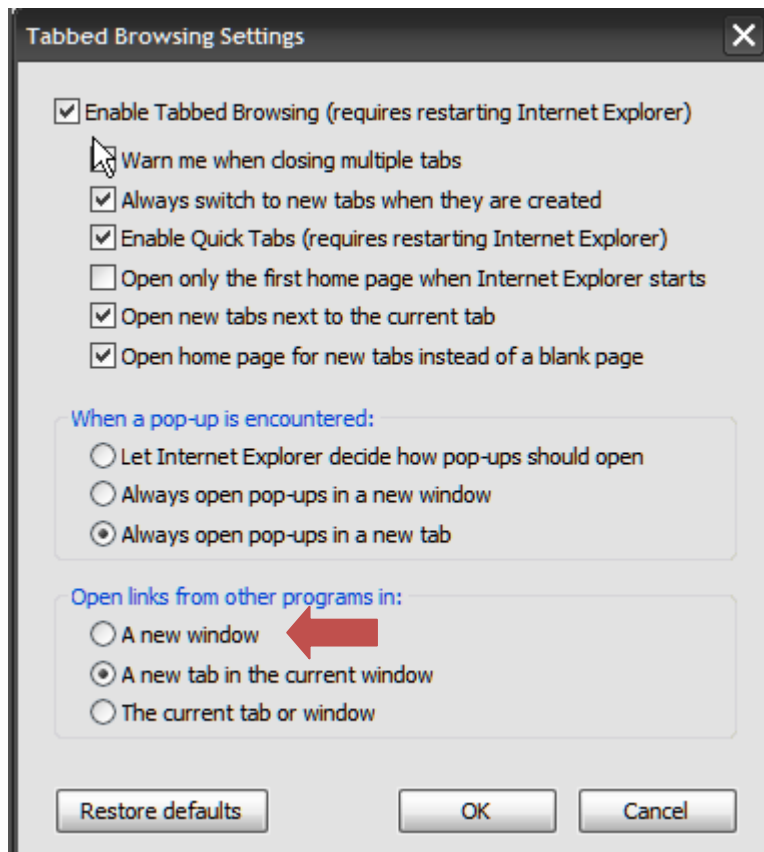


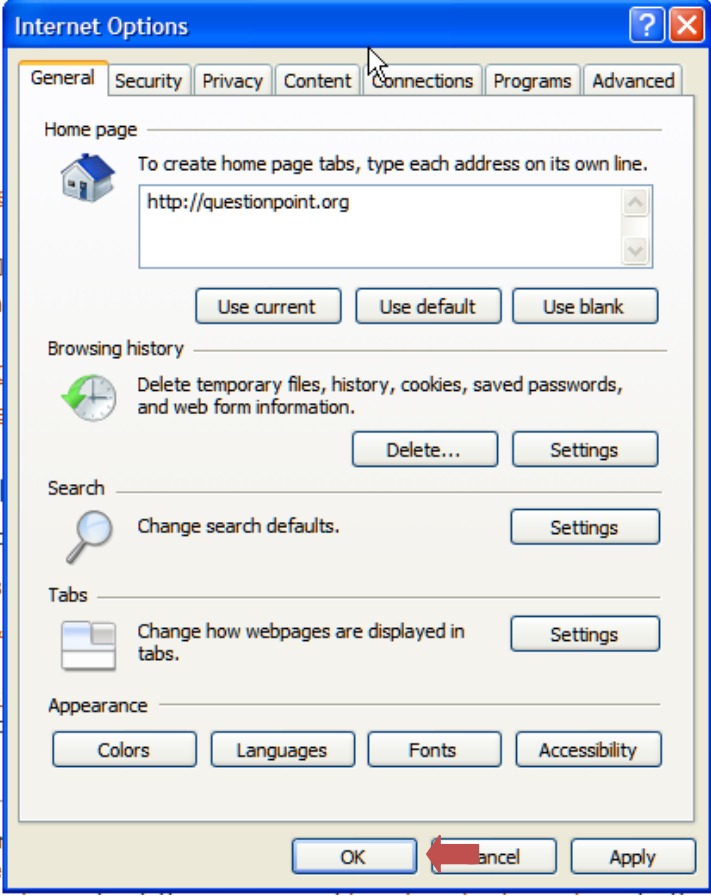
9 Click the **Setting** button in the Tabs section



**Step****Action**

- 10 Look for the "Open Links from other programs in:" section and select **A new window**



Step	Action
11	<p>Click "OK"</p> 

## Troubleshooting and Support

- Document problems that you encounter so you can describe them when you request support.
- **OCLC support staff:** Email: [support@oclc.org](mailto:support@oclc.org)  
Telephone: 1-800-848-5800 (USA) or +1-614-793-8682

## Comments or suggestions

- Please send us your comments about this quick reference at <http://www.oclc.org/content/forms/worldwide/en/questionpoint/feedback.html>



ISO 9001 Certified

The following OCLC product, service and business names are trademarks or service marks of OCLC, Inc.: OCLC, QuestionPoint, The 24/7 Reference Cooperative, WorldCat, and "The world's libraries. Connected." In addition, the WorldCat symbol and OCLC symbol are service marks of OCLC. Third-party product and service names are trademarks or service marks of their respective owners. OCLC grants permission to photocopy this publication as needed.



## Appendix A: Best practices

### Limit the number of other programs running on your computer

When monitoring chat, it is critical to only run those programs that are essential

### Properly end your chat sessions

Always end your patron chat sessions when they are done. Chat sessions that have been ended but not closed create unnecessary strain on QuestionPoint

### Properly end your shift

Always use the Log Out link in the upper right corner of the chat monitor when ending your chat shift. Use the “Close session” link on the confirmation screen. Then use the “Exit” link for your QuestionPoint session when you are ready to leave QuestionPoint.

## Appendix B: Internet Explorer Advanced Security Settings for the Internet Zone

Below are the advance security settings for the Internet Zone. This information is to be used by system administrators to configure the security settings if they have disabled them on your computer.

### .NET Framework

Option	Setting
Loose XAML	Enable
XAML browser applications	Enable
XPS documents	Enable

### .NET Framework – reliant components

Option	Setting
Run components not signed with Authenticode	Disable
Allow Scriptlets	Disable

### ActiveX controls and plug-ins

Option	Setting
Allow previously unused ActiveX controls to run without prompt	Enable
Allow Scriptlets	Disable
Automatic Prompting for ActiveX controls	Disable
Binary and script behaviors	Enable
Display video and animation on a webpage that does not use external media player	Disable
Download signed ActiveX controls	Prompt
Download unsigned ActiveX controls	Disable
Initialize script and ActiveX controls not marked as safe for scripting	Disable
Run ActiveX controls and plug-ins	Enable

Script ActiveX controls marked safe for scripting	Enable
---	--------

## Downloads

Option	Setting
Automatic prompting for file downloads	Disable
File download	Enable
Font download	Enable

## Enable .NET Framework Setup

Option	Setting
Enable .NET Framework Setup	Enable

## Miscellaneous

Option	Setting
Access data sources across domains	Disable
Allow META REFRESH	Enable
Allow scripting of Internet Explorer web browser control	Disable
Allow script-initiated windows without size or position constraints	Disable
Allow webpages to use restricted protocols for active content	Prompt
Allow websites to open windows without address or status bars	Disable
Display mixed content	Prompt
Don't prompt for client certificate selection when no certificate or only one certificate exists	Disable
Drag and drop or copy and paste files	Enable
Include local directory path when uploading path when uploading files to a server	Enable
Installation of desktop items	Prompt
Launching application and unsafe files	Prompt
Launching programs and files in an IFAME	Prompt
Navigate sub-frames across different domains	Disable
Open files based on content, not file extension	Enable
Software channel permissions	Medium Safety
Submit non-encrypted form data	Enable
Use Phishing Filter	Enable
Use Pop-up Blocker	Enable
Usedata persistence	Enable

Websites in less privileged web content zones can navigate into this zone	Enable
---	--------

**Scripting**

Option	Setting
Active Scripting	Enable
Allow Programmatic Clipboard access	Prompt
Allow status bar updates via script	Enable
Allow websites to prompt for information using scripted windows	Disable
Scripting of Java applets	Enable

**User Authentication**

Option	Setting
Logon	Automatic logon only in the Intranet zone