Securing Your Web Browser

Will Dormann and Jason Rafail

This paper will help you configure your web browser for safer internet surfing. It is written for home computer users, students, small business workers, and any other person who works with limited Information Technology (IT) support and broadband (cable modem, DSL) or dial-up connectivity. Although the information in this document may be applicable to users with formal IT support as well, organizational IT policies should supersede these recommendations. If you are responsible for IT policies for your organization, please consider implementing these recommendations as part of your policy.

I. Why Secure Your Web Browser?

Today, web browsers such as Internet Explorer, Mozilla Firefox, and Apple Safari (to name a few), are installed on almost all computers. Because web browsers are used so frequently, it is vital to configure them securely. Often, the web browser that comes with an operating system is not set up in a secure default configuration. Not securing your web browser can lead quickly to a variety of computer problems caused by anything from spyware being installed without your knowledge to intruders taking control of your computer.

Ideally, computer users should evaluate the risks from the software they use. Many computers are sold with software already loaded. Whether installed by a computer manufacturer, operating system maker, Internet Service Provider, or by a retail store, the first step in assessing the vulnerability of your computer is to find out what software is installed and how one program will interact with another. Unfortunately, it is not practical for most people to perform this level of analysis.

There is an increasing threat from software attacks that take advantage of vulnerable web browsers. We have observed a trend whereby new software vulnerabilities are exploited and directed at web browsers through use of compromised or malicious web sites. This problem is made worse by a number of factors, including the following:

- Many users have a tendency to click on links without considering the risks of their actions.
- Web page addresses can be disguised or take you to an unexpected site.
- Many web browsers are configured to provide increased functionality at the cost of decreased security.
- New security vulnerabilities may have been discovered since the software was configured and packaged by the manufacturer.
- Computer systems and software packages may be bundled with additional software, which increases the number of vulnerabilities that may be attacked.
- Third-party software may not have a mechanism for receiving security updates.
- Many web sites require that users enable certain features or install more software, putting the computer at additional risk.
- Many users do not know how to configure their web browsers securely.
- Many users are unwilling to enable or disable functionality as required to secure their web browser.

As a result, exploiting vulnerabilities in web browsers has become a popular way for attackers to compromise computer systems.

In addition to following this paper's recommendations, refer to the documentation in the References section for other steps you can take to secure your system.

II. Web Browser Features and Risks

It is important to understand the functionality and features of the web browser you use. Enabling some web browser features may lower security. Often, vendors will enable features by default to improve the computing experience, but these features may end up increasing the risk to the computer.

Attackers focus on exploiting client-side systems (your computer) through various vulnerabilities. They use these vulnerabilities to take control of your computer, steal your information, destroy your files, and use your computer to attack other computers. A low-cost way attackers do this is by exploiting vulnerabilities in web browsers. An attacker can create a malicious web page that will install Trojan software or spyware that will steal your information. Additional information about spyware is available in the following document: http://www.cert.org/archive/pdf/spyware2005.pdf. Rather than actively targeting and attacking vulnerable systems, a malicious web site can passively compromise systems as the site is visited. A malicious HTML document can also be emailed to victims. In these cases, the act of opening the email or attachment can compromise the system.

Some specific web browser features and associated risks are briefly described below. Understanding what different features do will help you understand how they affect your web browser's functionality and the security of your computer.

ActiveX is a technology used by Microsoft Internet Explorer on Microsoft Windows systems. ActiveX allows applications or parts of applications to be utilized by the web browser. A web page can use ActiveX components that may already reside on a Windows system, or a site may provide the component as a downloadable object. This gives extra functionality to traditional web browsing, but may also introduce more severe vulnerabilities if not properly implemented.

ActiveX has been plagued with various vulnerabilities and implementation issues. One problem with using ActiveX in a web browser is that it greatly increases the attack surface, or “attackability,” of a system. Installing any Windows application introduces the possibility of new ActiveX controls being installed. Vulnerabilities in ActiveX objects may be exploited via Internet Explorer, even if the object was never designed to be used in a web browser (VU#680526). In 2000, the CERT/CC held a workshop to analyze security in ActiveX. The results from that workshop may be viewed at http://www.cert.org/reports/activeX_report.pdf. Many vulnerabilities with respect to ActiveX controls lead to severe impacts. Often an attacker can take control of the computer. You can search the Vulnerability Notes Database for ActiveX vulnerabilities at http://www.kb.cert.org/vuls/byid?searchview&query=activex.

Java is an object-oriented programming language that can be used to develop active content for web sites. A Java Virtual Machine, or JVM, is used to execute the Java code, or “applet,” provided by the web site. Some operating systems come with a JVM, while others require a JVM to be installed before Java can be used. Java applets are operating system independent.

Java applets usually execute within a “sandbox” where the interaction with the rest of the system is limited. However, various implementations of the JVM contain vulnerabilities that allow an applet to bypass these restrictions. Signed Java applets can also bypass sandbox restrictions, but they generally prompt the user before they can execute. You can search the Vulnerability Notes Database for Java vulnerabilities at http://www.kb.cert.org/vuls/byid?searchview&query=java.

Plug-ins are applications intended for use in the web browser. Netscape has developed the NPAPI standard for developing plug-ins, but this standard is used by multiple web browsers, including Mozilla Firefox and Safari. Plug-ins are similar to ActiveX controls but cannot be executed outside of a web browser. Adobe Flash is an example of an application that is available as a plug-in.

Plug-ins can contain programming flaws such as buffer overflows, or they may contain design flaws such as cross-domain violations, which arises when the same origin policy is not followed.

Cookies are files placed on your system to store data for specific web sites. A cookie can contain any information that a web site is designed to place in it. Cookies may contain information about the sites you visited, or may even contain credentials for accessing the site. Cookies are designed to be readable only by the web site that created the cookie. Session cookies are cleared when the browser is closed, and persistent cookies will remain on the computer until the specified expiration date is reached.

Cookies can be used to uniquely identify visitors of a web site, which some people consider a violation of privacy. If a web site uses cookies for authentication, then an attacker may be able to acquire unauthorized access to that site by obtaining the cookie. Persistent cookies pose a higher risk than session cookies because they remain on the computer longer.

JavaScript, also known as ECMAScript, is a scripting language that is used to make web sites more interactive. There are specifications in the JavaScript standard that restrict certain features such as accessing local files.

VBScript is another scripting language that is unique to Microsoft Windows Internet Explorer. VBScript is similar to JavaScript, but it is not as widely used in web sites because of limited compatibility with other browsers.

The ability to run a scripting language such as JavaScript or VBScript allows web page authors to add a significant amount of features and interactivity to a web page. However, this same capability can be abused by attackers. The default configuration for most web browsers enables scripting support, which can introduce multiple vulnerabilities, such as the following:

- **Cross-Site Scripting**

  Cross-Site Scripting, often referred to as XSS, is a vulnerability in a web site that permits an attacker to leverage the trust relationship that you have with that site. For a high-level description of XSS attacks, please see the whitepaper published at http://www.cert.org/archive/pdf/cross_site_scripting.pdf. Note that Cross-Site Scripting is not usually caused by a failure in the web browser. You can search the Vulnerability Notes Database for Cross-Site Scripting vulnerabilities at http://www.kb.cert.org/vuls/byid?searchview&query=cross-site+scripting.

- **Cross-Zone and Cross-Domain Vulnerabilities**

Most web browsers employ security models to prevent script in a web site from accessing data in a different domain. These security models are primarily based on the Netscape Same Origin Policy: http://www.mozilla.org/projects/security/components/same-origin.html. Internet Explorer also has a policy to enforce security zone separation: http://www.microsoft.com/windows/ie/ie6/using/howto/security/setup.mspx.

Vulnerabilities that violate these security models can be used to perform actions that a site could not normally perform. The impact can be similar to a cross-site scripting vulnerability. However, if a vulnerability allows for an attacker to cross into the local machine zone or other protected areas, the attacker may be able to execute arbitrary commands on the vulnerable system. You can search the Vulnerability Notes Database for cross-zone and cross-domain vulnerabilities at http://www.kb.cert.org/vuls/byid?searchview&query=cross-domain.

- **Detection evasion**

  Anti-virus, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) generally work by looking for specific patterns in content. If a “known bad” pattern is detected, then the appropriate actions can take place to protect the user. But because of the dynamic nature of programming languages, scripting in web pages can be used to evade such protective systems.

III. How to Secure Your Web Browser

Some software features that provide functionality to a web browser, such as ActiveX, Java, Scripting (JavaScript, VBScript, etc), may also introduce vulnerabilities to the computer system. These may stem from poor implementation, poor design, or an insecure configuration. For these reasons, you should understand which browsers support which features and the risks they could introduce. Some web browsers permit you to fully disable the use of these technologies, while others may permit you to enable features on a per-site basis.

This section shows you how to securely configure a few of the most popular web browsers and how to disable features that can cause vulnerabilities. We encourage you to visit the vendor's web site for the browser you use to learn more. If a vendor does not provide documentation on how to secure the browser, we encourage you to contact them and request more information.

Multiple web browsers may be installed on your computer. Other software applications on your computer, such as email clients or document viewers, may use a different browser than the one you normally use to access the web. Also, certain file types may be configured to open with a different web browser. Using one web browser for manually interacting with web sites does not mean other applications will automatically use the same browser. For this reason, it is important to securely configure each web browser that may be installed on your computer. One advantage to having multiple web browsers is that one browser can be used for only sensitive activities such as online banking, and the other can be used for general purpose web browsing. This can minimize the chances that a vulnerability in a web browser, web site, or related software can be used to compromise sensitive information.

Web browsers are frequently updated. Depending on the version of your software, the features and options may move or change.

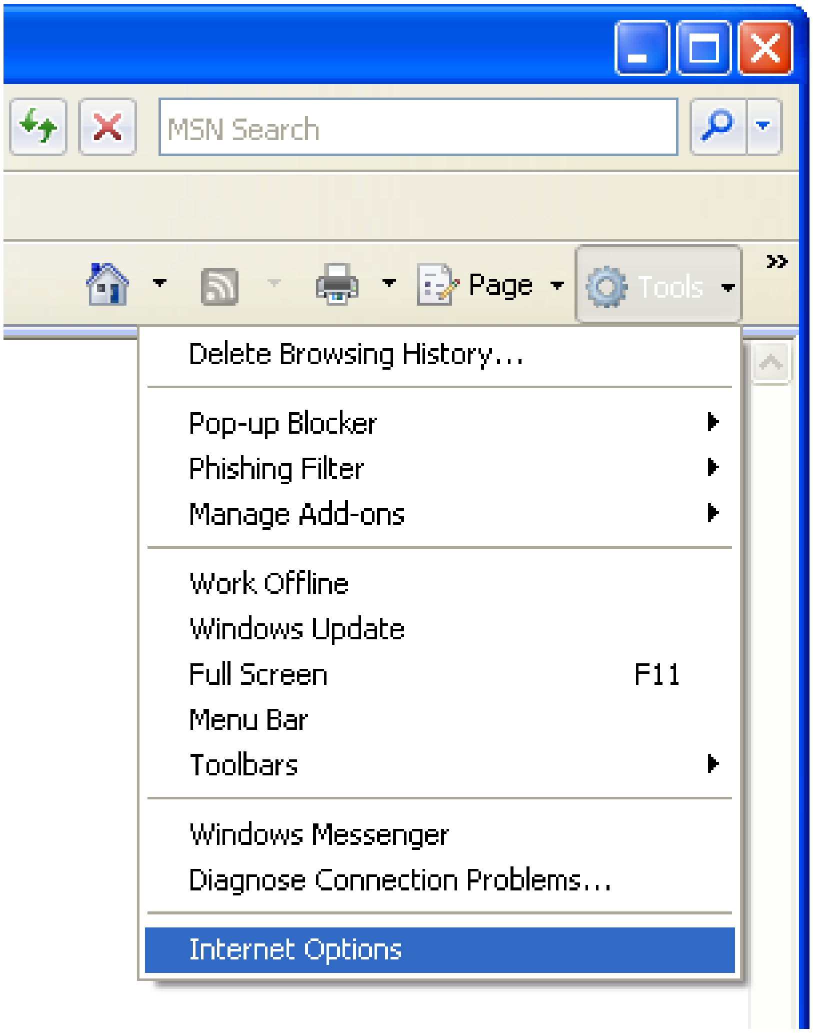
A. Microsoft Internet Explorer

Microsoft Internet Explorer (IE) is a web browser integrated into the Microsoft Windows operating system. Removal of this application is not practical.

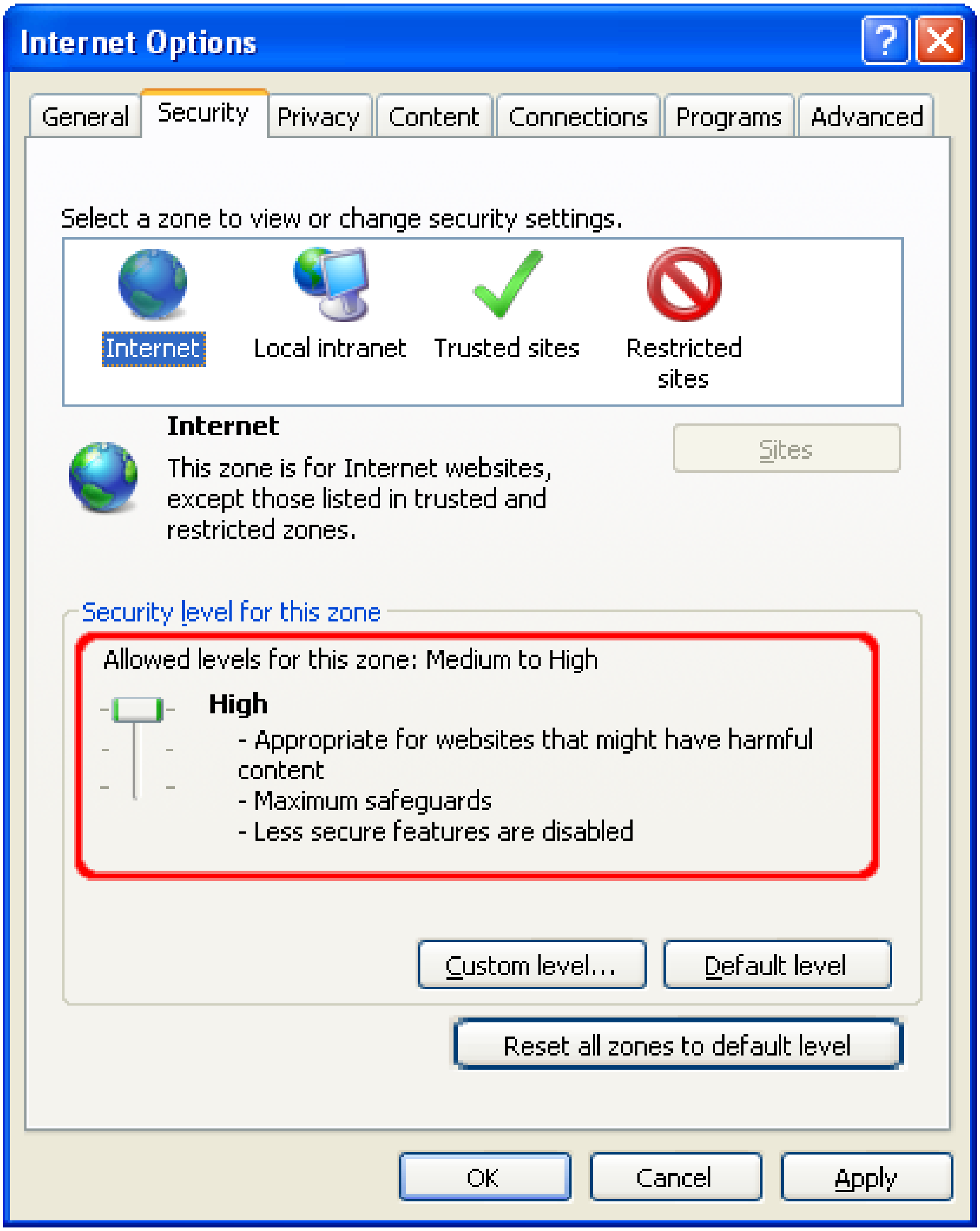
In addition to supporting Java, scripting and other forms of active content, Internet Explorer implements ActiveX technology. While any application is potentially vulnerable to attack, it is possible to mitigate a number of serious vulnerabilities by using a web browser that does not support ActiveX controls. However, using an alternate browser may affect the functionality of some sites that require the use of ActiveX controls. Note that using a different web browser will not remove IE, or other Windows components from the system. Other software, such as email clients, may use IE, the WebBrowser ActiveX control (WebOC), or the IE HTML rendering engine (MSHTML). Results from the CERT/CC ActiveX workshop in 2000 are available at http://www.cert.org/reports/activeX_report.pdf.

Here are steps to disable various features in Internet Explorer 7. Note that menu options may vary between versions of IE, so you should adapt the steps below as appropriate.

In order to change settings for Internet Explorer, select **Tools** then **Internet Options…**



Select the **Security** tab. On this tab you will find a section at the top that lists the various security zones that Internet Explorer uses. More information about Internet Explorer security zones is available in the Microsoft document Setting Up Security Zones. For each of these zones, you can select a Custom Level of protection. By clicking the **Custom Level** button, you will see a second window open that permits you to select various security settings for that zone. The **Internet** zone is where all sites initially start out. The security settings for this zone apply to all the web sites that are not listed in the other security zones. We recommend the **High** security setting be applied for this zone. By selecting the High security setting, several features including ActiveX, Active scripting, and Java will be disabled. With these features disabled, the browser will be more secure. Click the **Default Level** button and then drag the slider control up to **High**.



Select a zone to view or change security settings.

Internet

This zone is for Internet websites, except those listed in trusted and restricted zones.

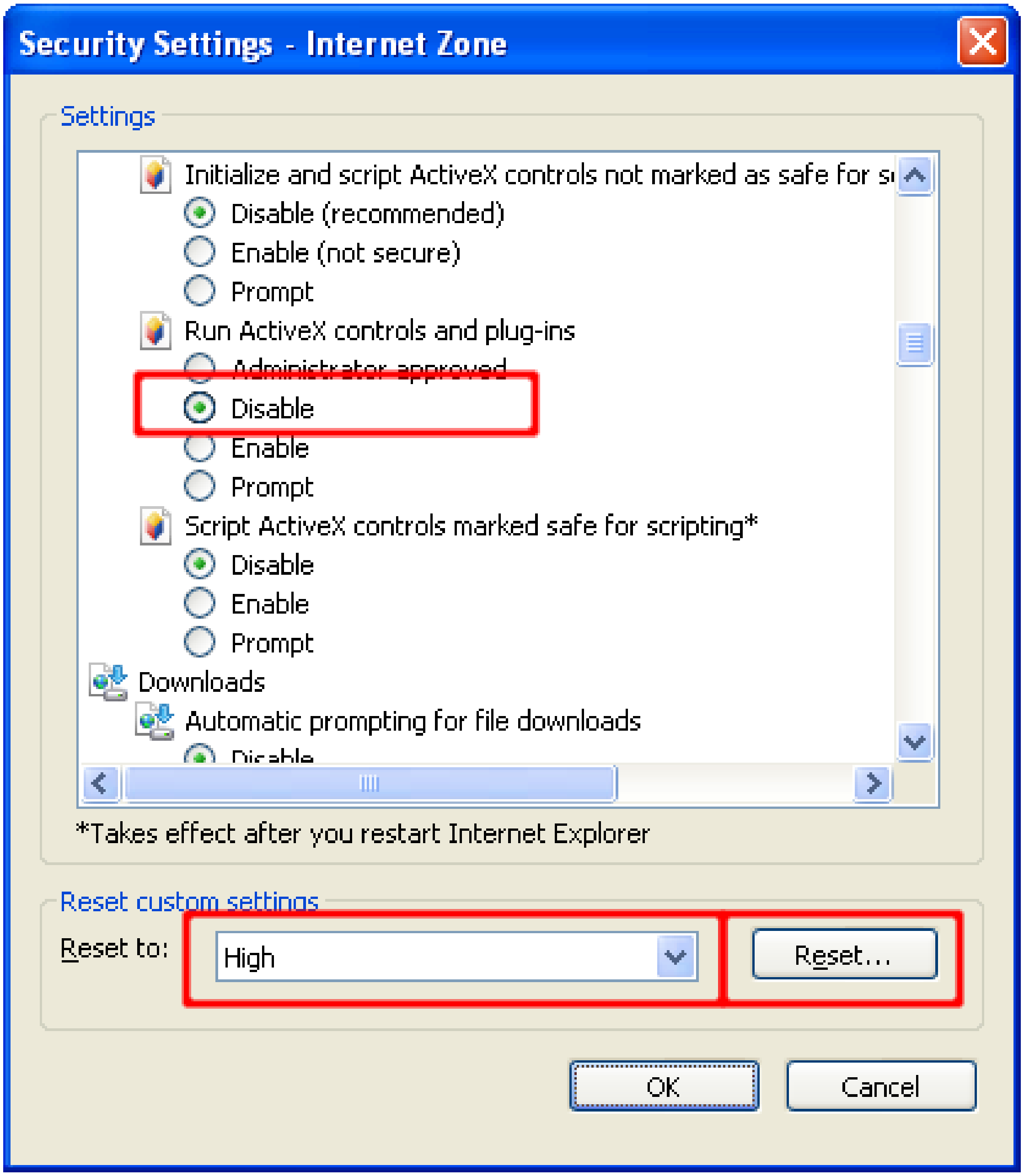
Security level for this zone

Allowed levels for this zone: Medium to High

High

- Appropriate for websites that might have harmful content
- Maximum safeguards
- Less secure features are disabled

For a more fine-grained control over what features are allowed in the zone, click the **Custom Level** button. Here you can control the specific security options that apply to the current zone. For example ActiveX can be disabled by selecting **Disable** for **Run ActiveX controls and plug-ins**. Default values for the High security setting can be selected by choosing **High** and clicking the **Reset** button to apply the changes.



Security Settings - Internet Zone

Settings

Initialize and script ActiveX controls not marked as safe for s

● Disable (recommended)

○ Enable (not secure)

○ Prompt

Run ActiveX controls and plug-ins

○ Administrator approved

● Disable

○ Enable

○ Prompt

Script ActiveX controls marked safe for scripting*

● Disable

○ Enable

○ Prompt

Downloads

Automatic prompting for file downloads

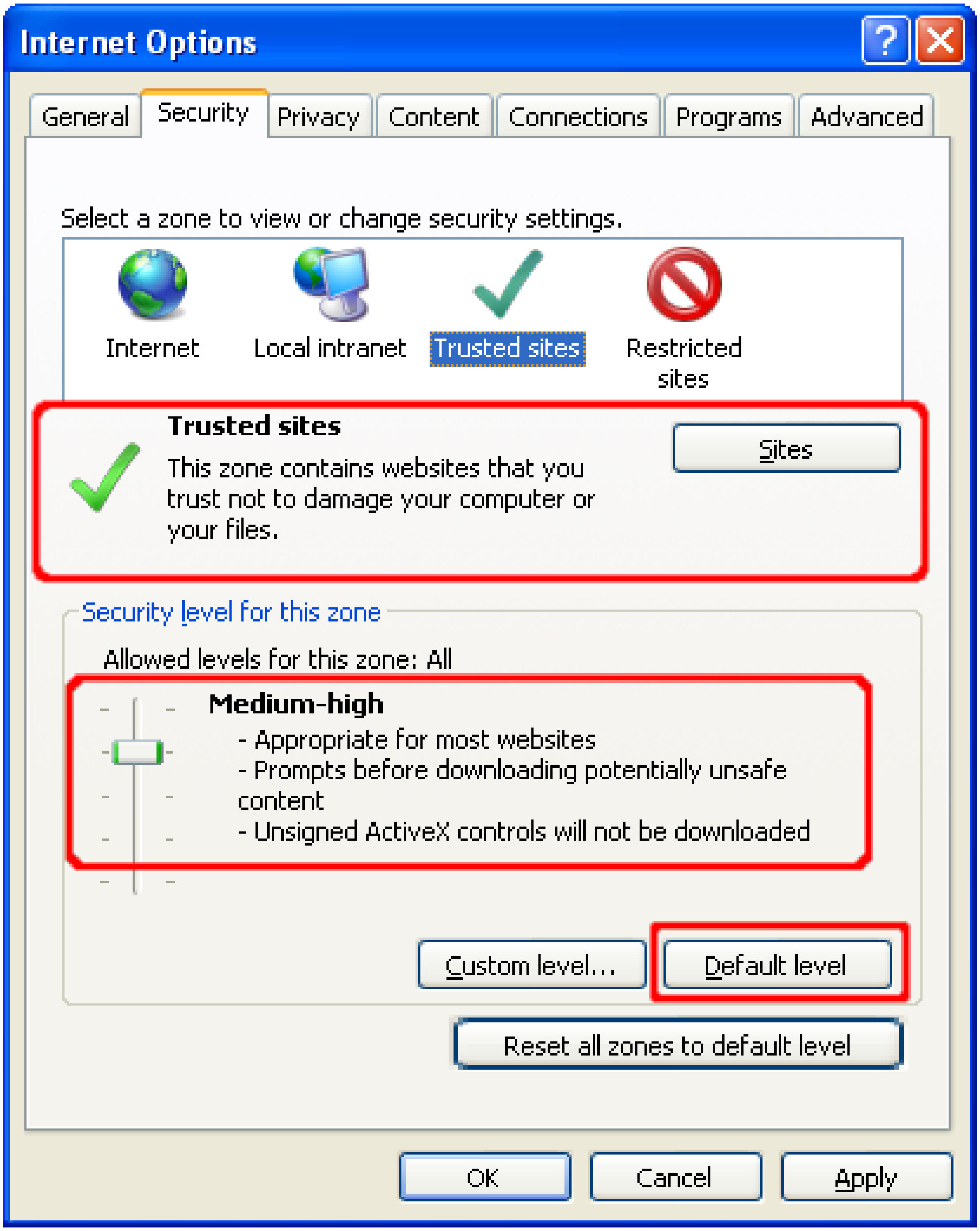
● Disable

*Takes effect after you restart Internet Explorer

Reset custom settings

Reset to: High

The **Trusted sites** zone is a security zone for sites that you think are safe to visit. You believe that the site is designed with security in mind and that it can be trusted not to contain malicious content. To add or remove sites from this zone, you can click the **Sites…** button. This will open a secondary window listing the sites that you trust and permitting you to add or remove them. You may also require that only verified sites (HTTPS) can be included in this zone. This gives you greater assurance that the site you are visiting is the site that it claims to be.



Internet Options

Select a zone to view or change security settings.

Trusted sites

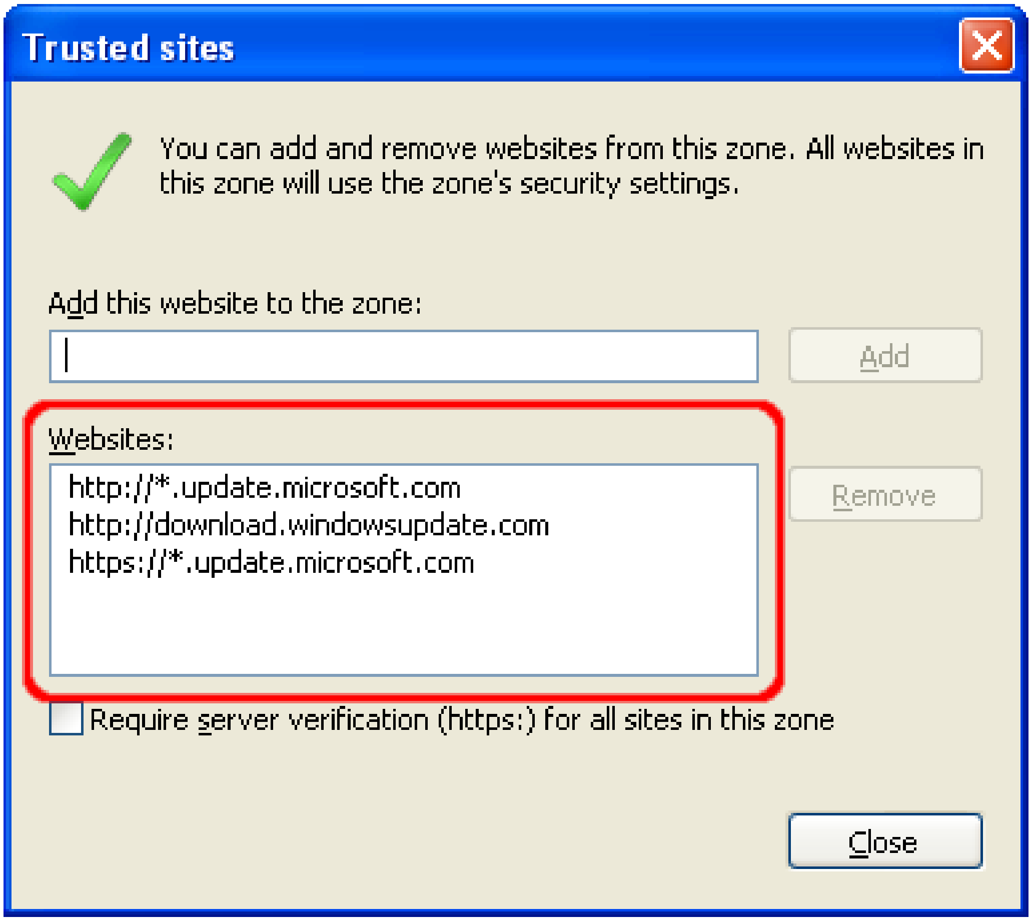
This zone contains websites that you trust not to damage your computer or your files.

Security level for this zone

Allowed levels for this zone: All

Medium-high

- Appropriate for most websites
- Prompts before downloading potentially unsafe content
- Unsigned ActiveX controls will not be downloaded



Trusted sites

You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

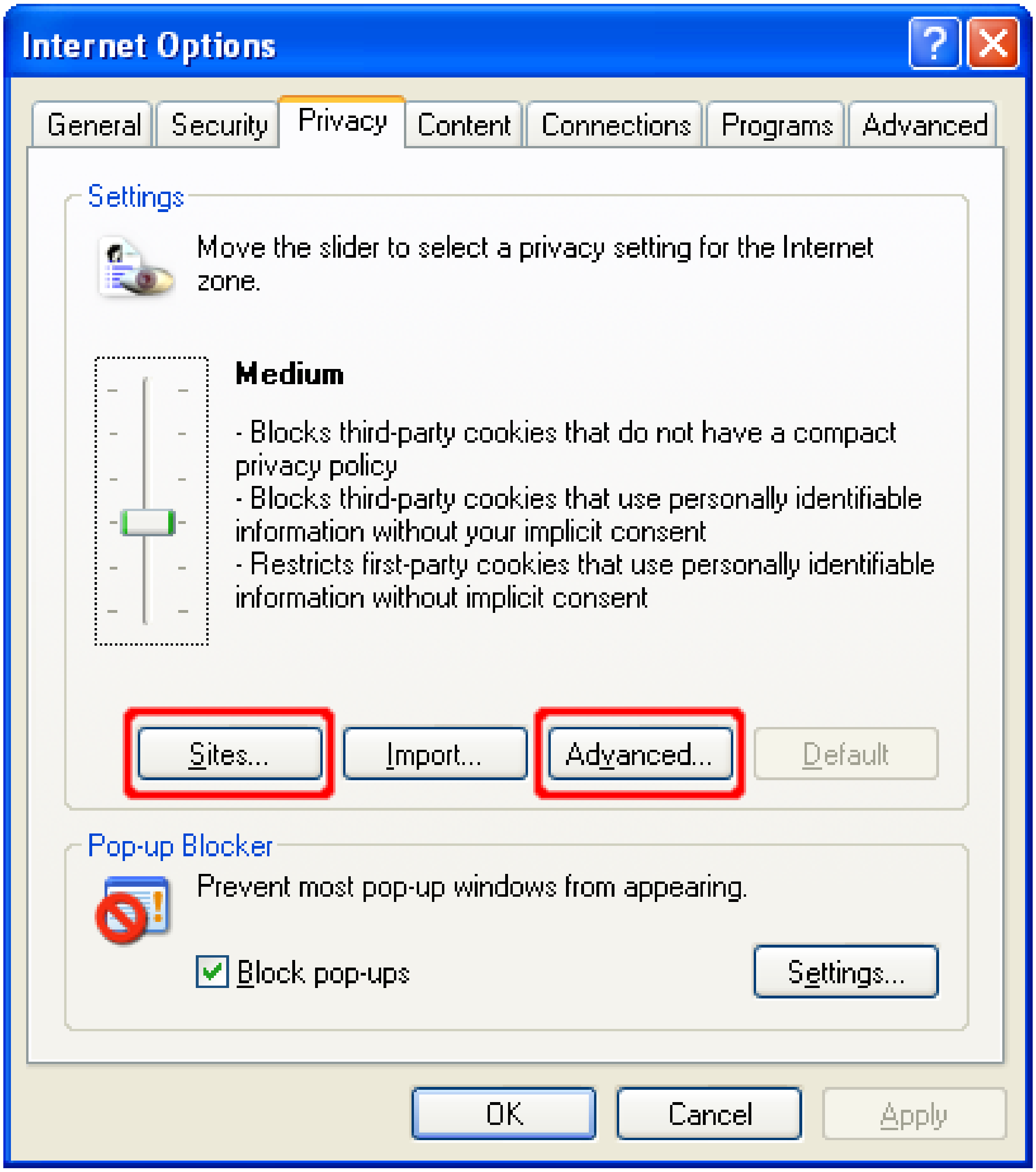
Websites:

http://*.update.microsoft.com
http://download.windowsupdate.com
https://*.update.microsoft.com

□ Require server verification (https:) for all sites in this zone

We recommend setting the security level for the **Trusted sites** zone to **Medium-high** (or **Medium** for Internet Explorer 6 and earlier). When the Internet Zone is set to **High**, you may encounter web sites that do not function properly due to one or more of the associated security settings. This is where the **Trusted sites** zone can help. If you trust that the site will not contain malicious content, you can add it to the list of sites in the Trusted sites zone. Once a site is added to this zone, features such as ActiveX and Active scripting will be enabled for the site. The benefit of this type of configuration is that IE will be more secure by default, and sites can be “whitelisted” in the Trusted sites zone to gain extra functionality.

The **Privacy** tab contains settings for cookies. Cookies are text files placed on your computer by various sites that you visit either directly (first-party) or indirectly (third-party) through ad banners, for example. A cookie can contain any data that a site wishes to store. It is often used to track your computer as you move through a web site and store information such as preferences or credentials. We recommend that you select the **Advanced** button and select **Override automatic cookie handling**. Then select **Prompt** for both first and third-party cookies. This will prompt you each time a site tries to place a cookie on your machine. If the number of cookie prompts is too excessive, the option to **Always allow session cookies** can be enabled. This will allow non-persistent cookies to be accepted without user interaction. Session cookies have less risk than persistent cookies.



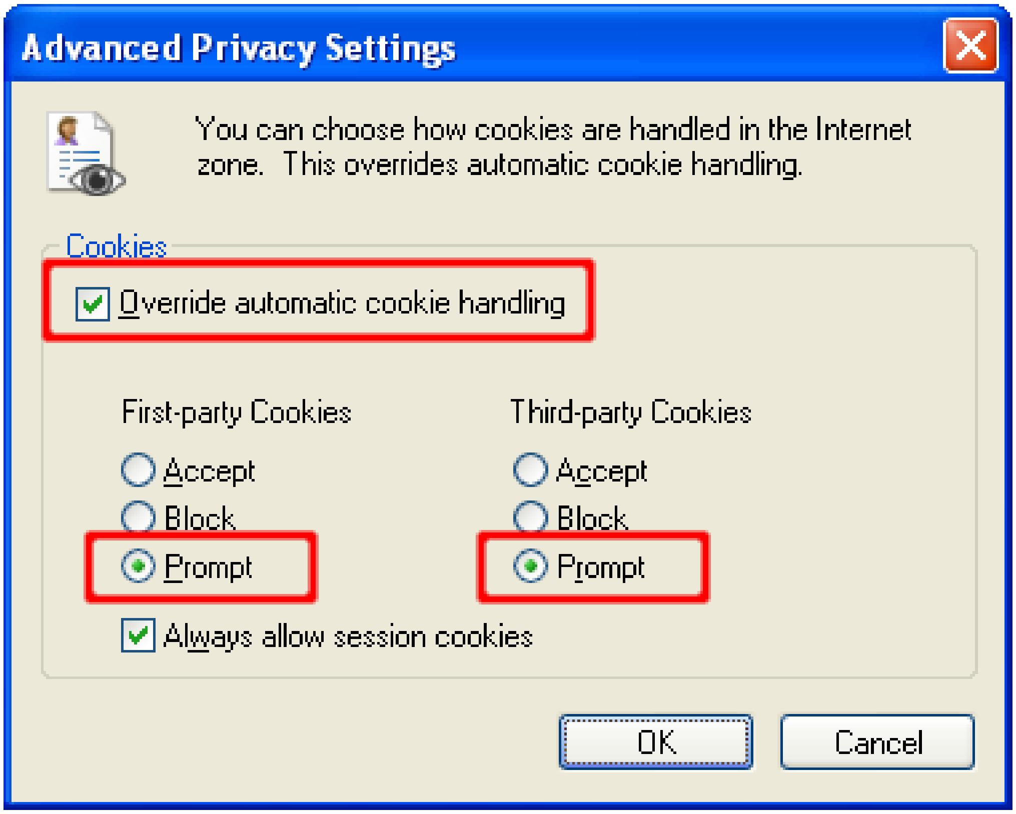
Move the slider to select a privacy setting for the Internet zone.

Medium

- Blocks third-party cookies that do not have a compact privacy policy
- Blocks third-party cookies that use personally identifiable information without your implicit consent
- Restricts first-party cookies that use personally identifiable information without implicit consent

Prevent most pop-up windows from appearing.

☑ Block pop-ups



You can choose how cookies are handled in the Internet zone. This overrides automatic cookie handling.

Cookies

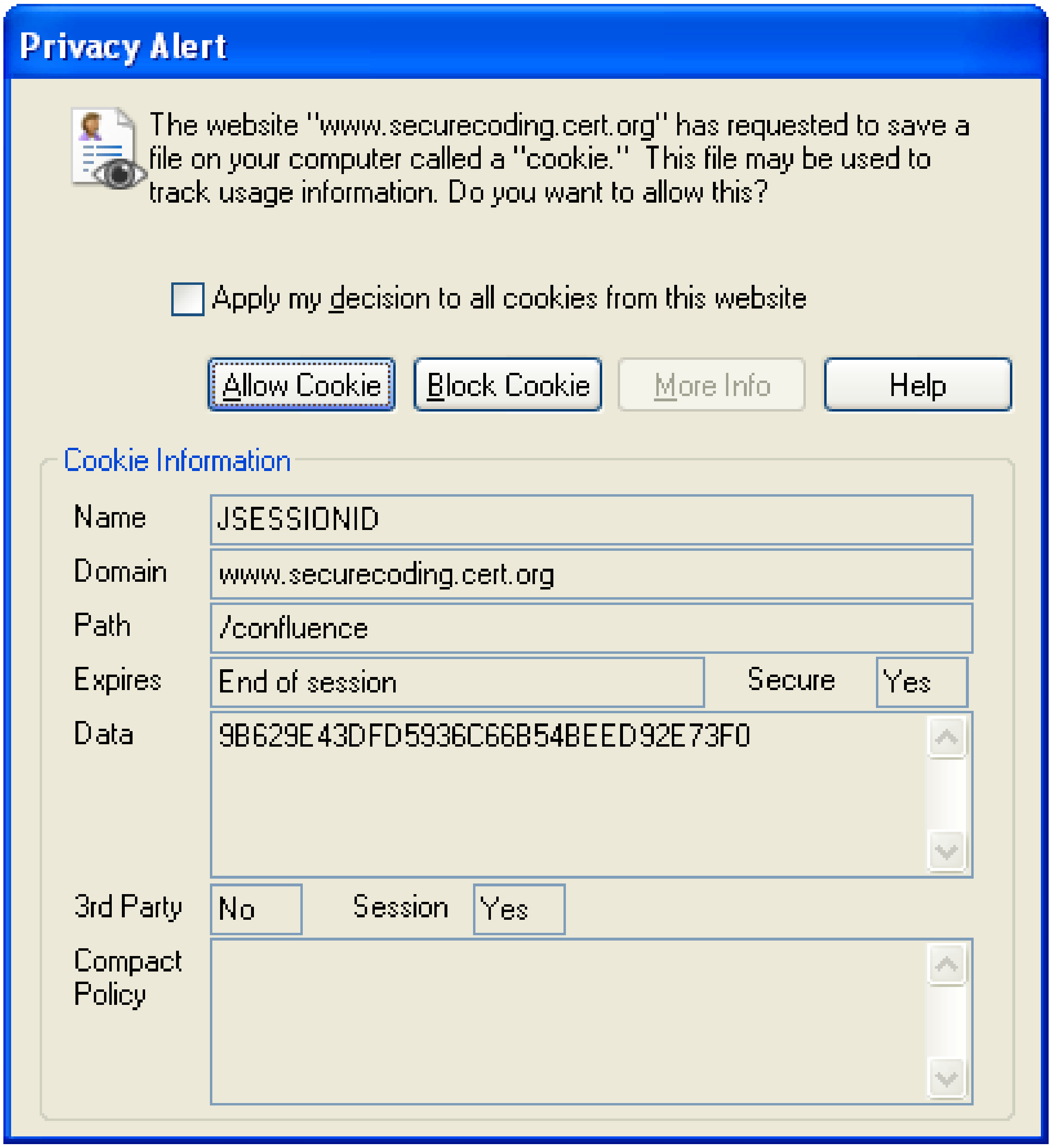
☑ Override automatic cookie handling

First-party Cookies
○ Accept
○ Block
● Prompt

Third-party Cookies
○ Accept
○ Block
● Prompt

☑ Always allow session cookies

You can then evaluate the originating site, whether you wish to accept or deny the cookie, and what action to take (allow or block, with the option to remember the decision for all future cookies from that web site). For example, if visiting a web site causes a cookie prompt from a web domain that is associated with advertising, you may wish to click **Block Cookie** to prevent that domain from being able to set cookies on your computer, for privacy reasons.



The website "www.securecoding.cert.org" has requested to save a file on your computer called a "cookie." This file may be used to track usage information. Do you want to allow this?

□ Apply my decision to all cookies from this website

Name: JSESSIONID

Domain: www.securecoding.cert.org

Path: /confluence

Expires: End of session

Secure: Yes

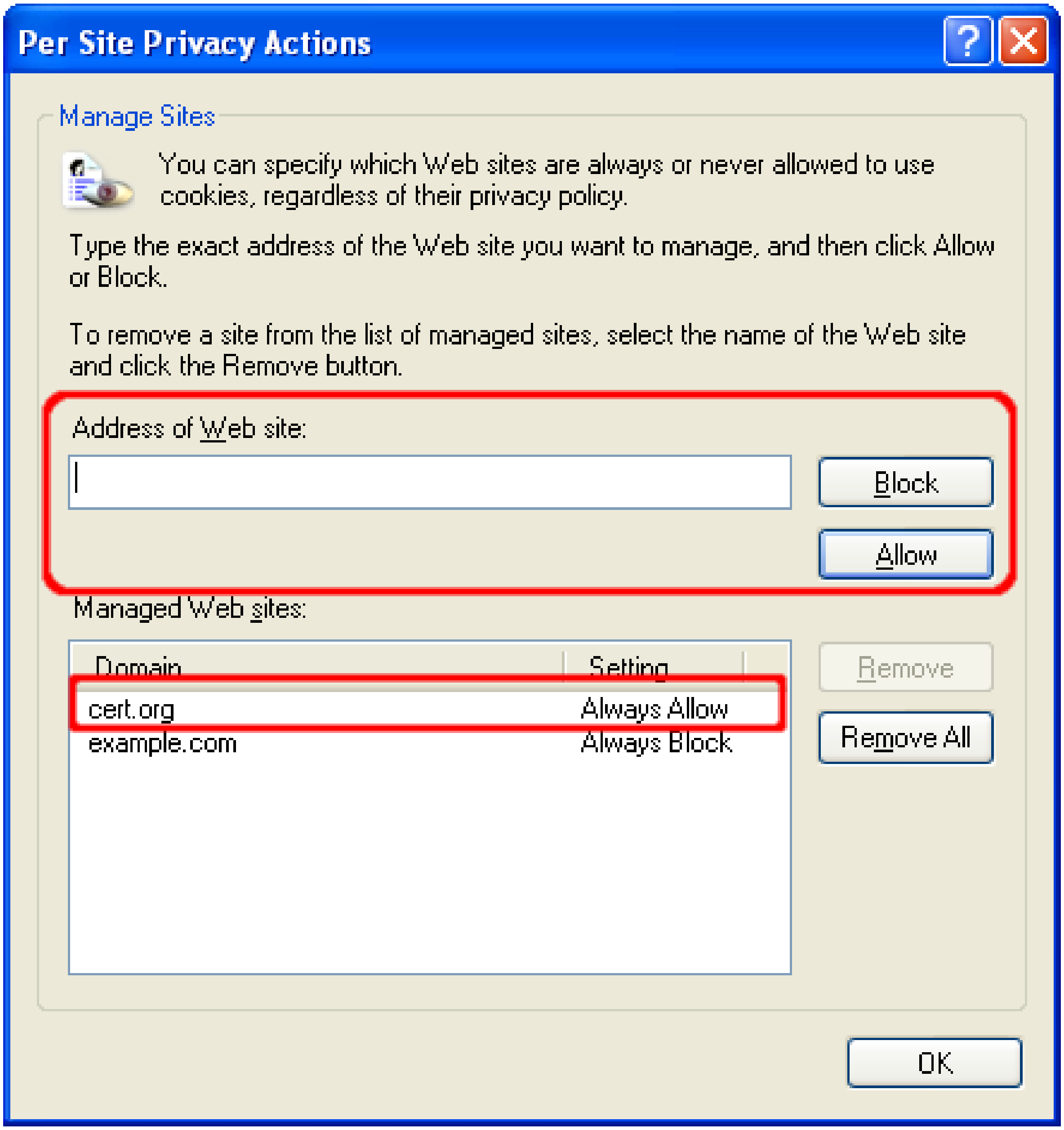
Data: 9B629E43DFD5936C66B54BEED92E73F0

3rd Party: No

Session: Yes

Compact Policy:

By selecting the **Sites...** button, you can manage the cookie settings for specific sites. You can add or remove sites, and you can change the current settings for existing sites. The bottom section of this window will specify the domain of the site and the action to take when that site wants to place a cookie on your machine. You can use the upper section of this window to change these settings.



Per Site Privacy Actions

Manage Sites

You can specify which Web sites are always or never allowed to use cookies, regardless of their privacy policy.

Type the exact address of the Web site you want to manage, and then click Allow or Block.

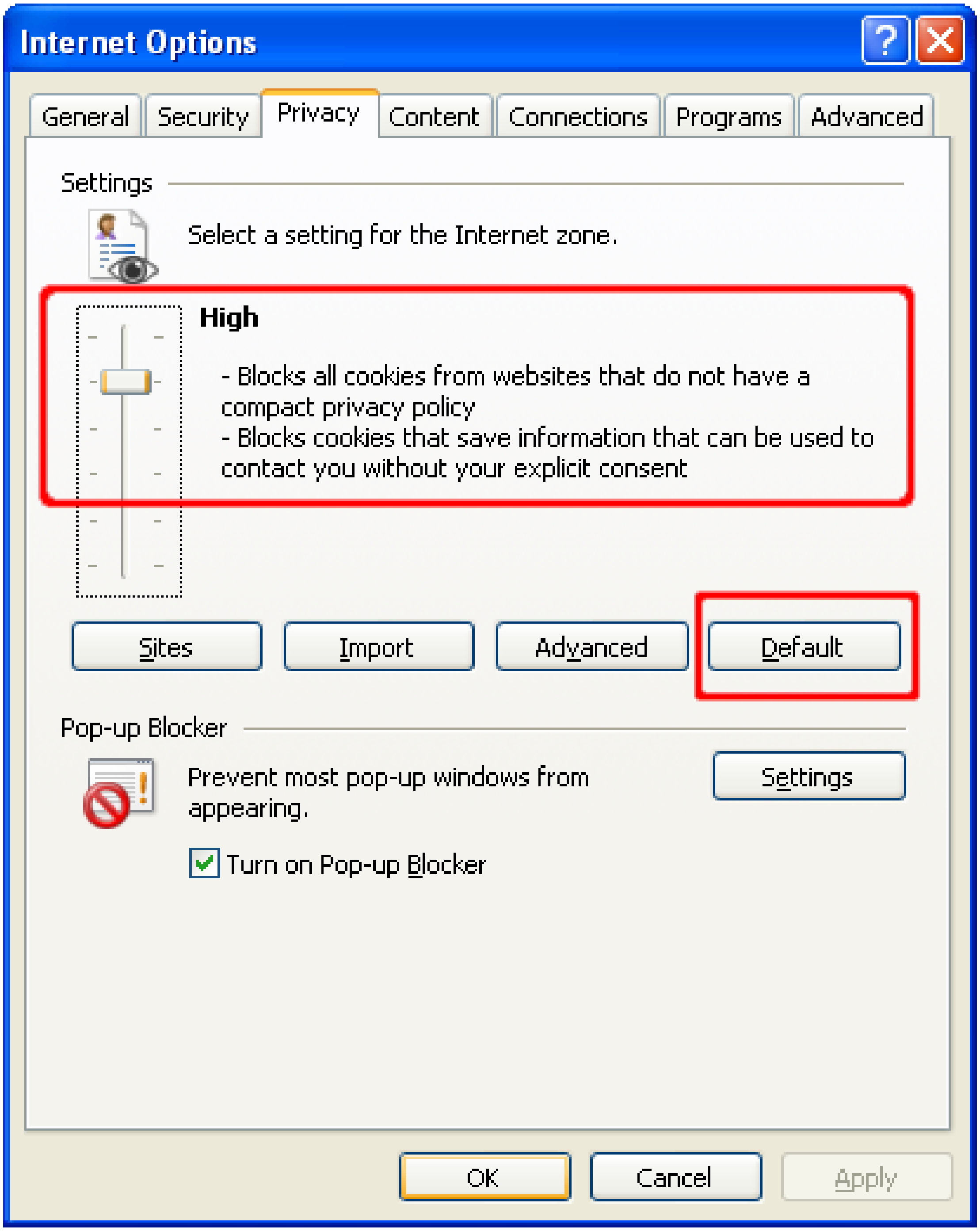
To remove a site from the list of managed sites, select the name of the Web site and click the Remove button.

Address of Web site:

Managed Web sites:

Domain	Setting
cert.org	Always Allow
example.com	Always Block

Alternatively, if you do not wish to receive warning dialogs when a site attempts to set a cookie, you can use Internet Explorer's pre-set privacy rules. Click the **Default** button and then drag the slider up to **High**. Note that some web sites may fail to function properly with the **High** setting. In such cases, you may add the site to the list of sites for which cookies are allowed, as described above.



Select a setting for the Internet zone.

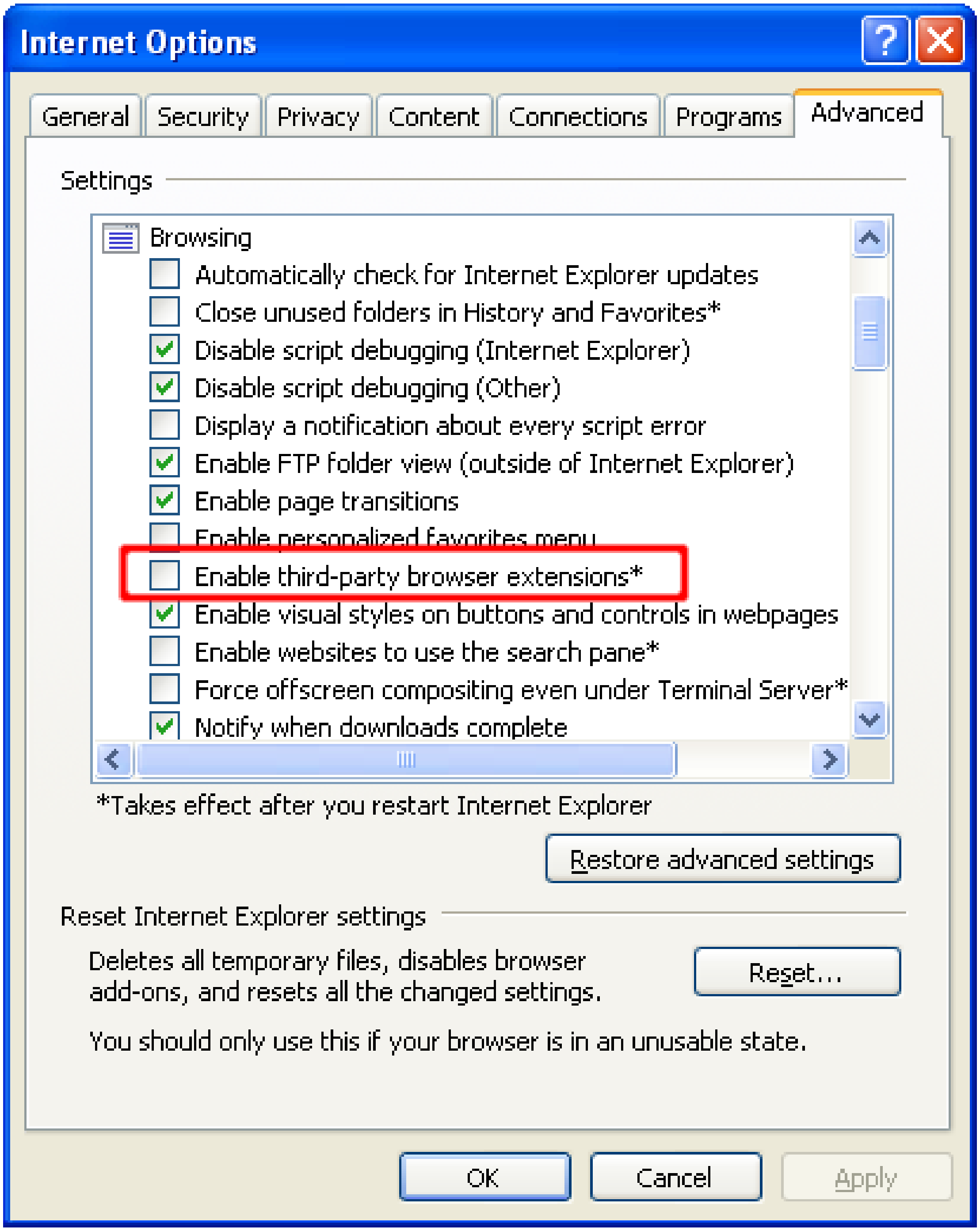
High

- Blocks all cookies from websites that do not have a compact privacy policy
- Blocks cookies that save information that can be used to contact you without your explicit consent

Prevent most pop-up windows from appearing.

☑ Turn on Pop-up Blocker

The **Advanced** tab contains settings that apply to all of the security zones. We recommend that you **disable** the **Enable third-party browser extensions** option. This option includes tool bars and Browser Helper Objects (BHOs). While some add-ons can be useful, they also have the ability to violate your privacy. For example, a browser add-on may monitor your web browsing habits, or even change the contents of web pages in an attempt to gather personal information.



Browsing

- □ Automatically check for Internet Explorer updates
- □ Close unused folders in History and Favorites*
- ☑ Disable script debugging (Internet Explorer)
- ☑ Disable script debugging (Other)
- □ Display a notification about every script error
- ☑ Enable FTP folder view (outside of Internet Explorer)
- ☑ Enable page transitions
- □ Enable personalized favorites menu
- □ Enable third-party browser extensions*
- ☑ Enable visual styles on buttons and controls in webpages
- □ Enable websites to use the search pane*
- □ Force offscreen compositing even under Terminal Server*
- ☑ Notify when downloads complete

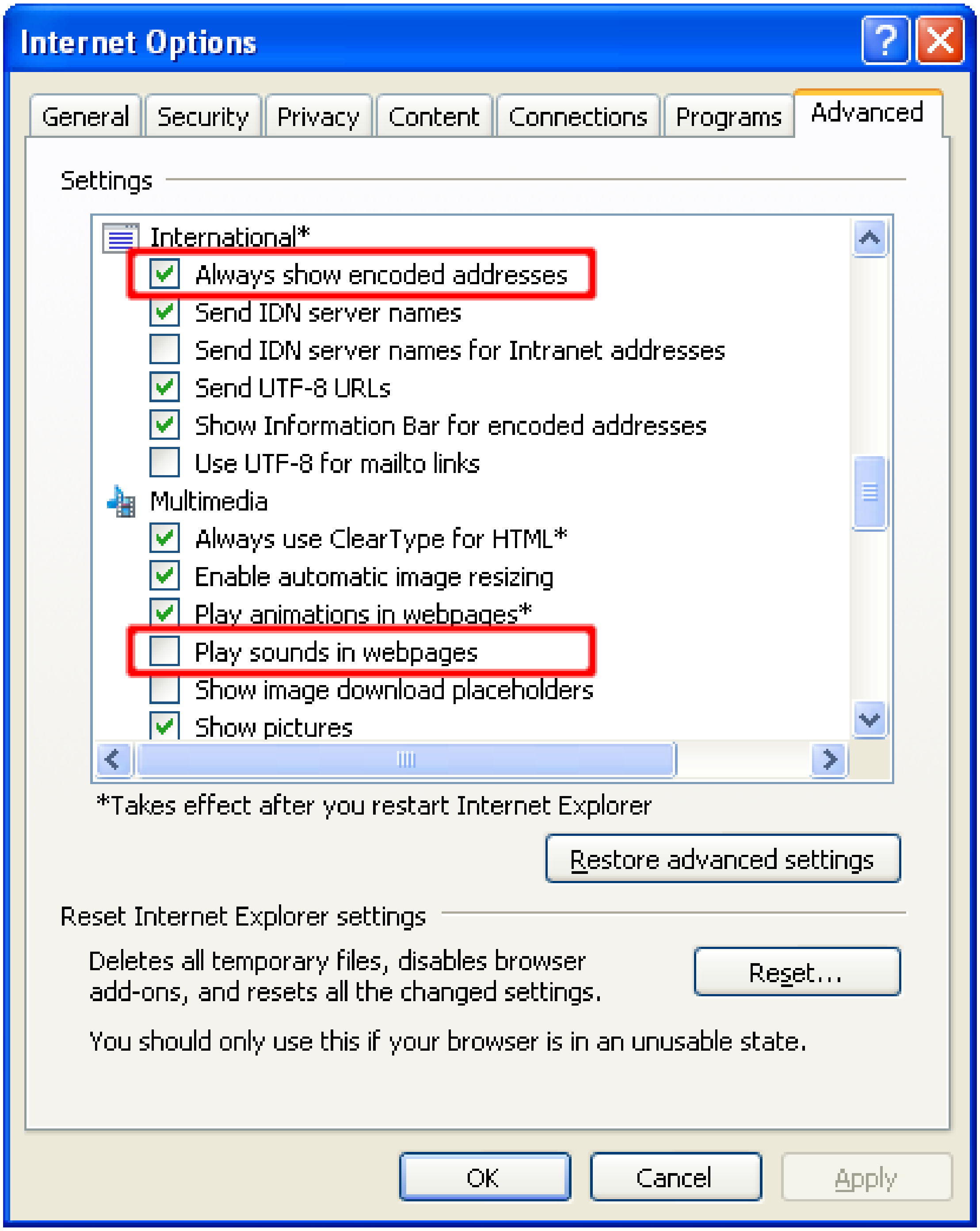
*Takes effect after you restart Internet Explorer

Deletes all temporary files, disables browser add-ons, and resets all the changed settings.

You should only use this if your browser is in an unusable state.

Internationalized Domain Names (IDN) can be abused to allow spoofing of web page addresses. This can allow phishing attacks to be more convincing. More details about IDN spoofing can be found in Vulnerability Note VU#273262. To protect against IDN spoofing in Internet Explorer, enable the **Always show encoded addresses** option. This will cause IDN addresses to be displayed in an encoded form in the Internet Explorer address bar and status bar, which will remove the visual similarity to the spoofing target address.

We also recommend that you **disable** the **Play sounds in webpages** option. Sounds in web pages are rarely integral to web page content, and may also introduce security risks by having the browser process additional untrusted data. This option is for Internet Explorer's ability to natively handle sounds. It will not interfere with other software, such as Adobe Flash or Apple QuickTime.



Settings

International*
- ☑ Always show encoded addresses
- ☑ Send IDN server names
- □ Send IDN server names for Intranet addresses
- ☑ Send UTF-8 URLs
- ☑ Show Information Bar for encoded addresses
- □ Use UTF-8 for mailto links

Multimedia
- ☑ Always use ClearType for HTML*
- ☑ Enable automatic image resizing
- ☑ Play animations in webpages*
- □ Play sounds in webpages
- □ Show image download placeholders
- ☑ Show pictures

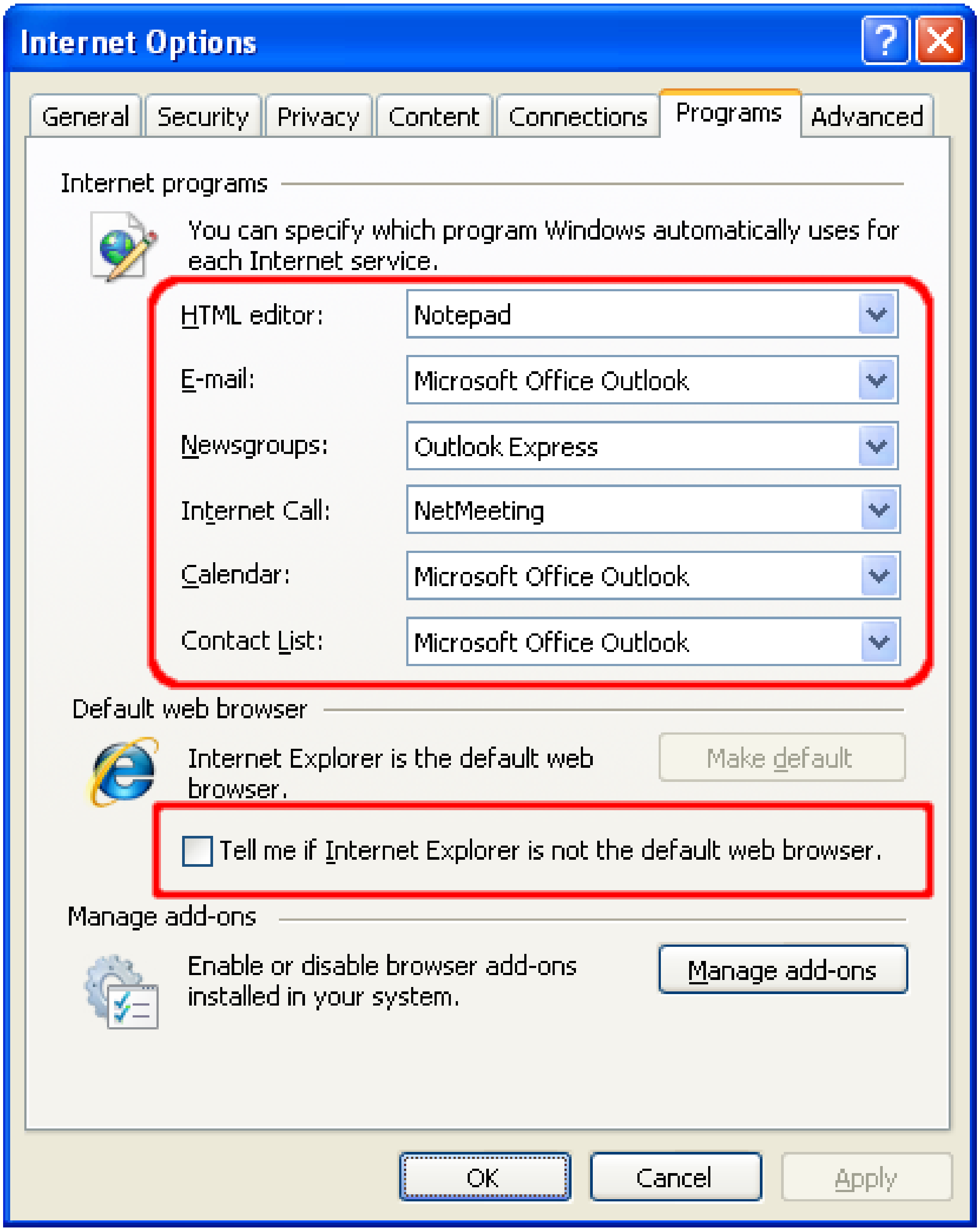
*Takes effect after you restart Internet Explorer

Reset Internet Explorer settings

Deletes all temporary files, disables browser add-ons, and resets all the changed settings.

You should only use this if your browser is in an unusable state.

Under the **Programs** tab, you can specify your default applications for viewing web sites, email messages and various other network related tasks. You can also disable Internet Explorer from asking you if you would like it to be your default web browser here.



Internet programs

You can specify which program Windows automatically uses for each Internet service.

HTML editor: Notepad

E-mail: Microsoft Office Outlook

Newsgroups: Outlook Express

Internet Call: NetMeeting

Calendar: Microsoft Office Outlook

Contact List: Microsoft Office Outlook

Default web browser

Internet Explorer is the default web browser.

□ Tell me if Internet Explorer is not the default web browser.

Manage add-ons

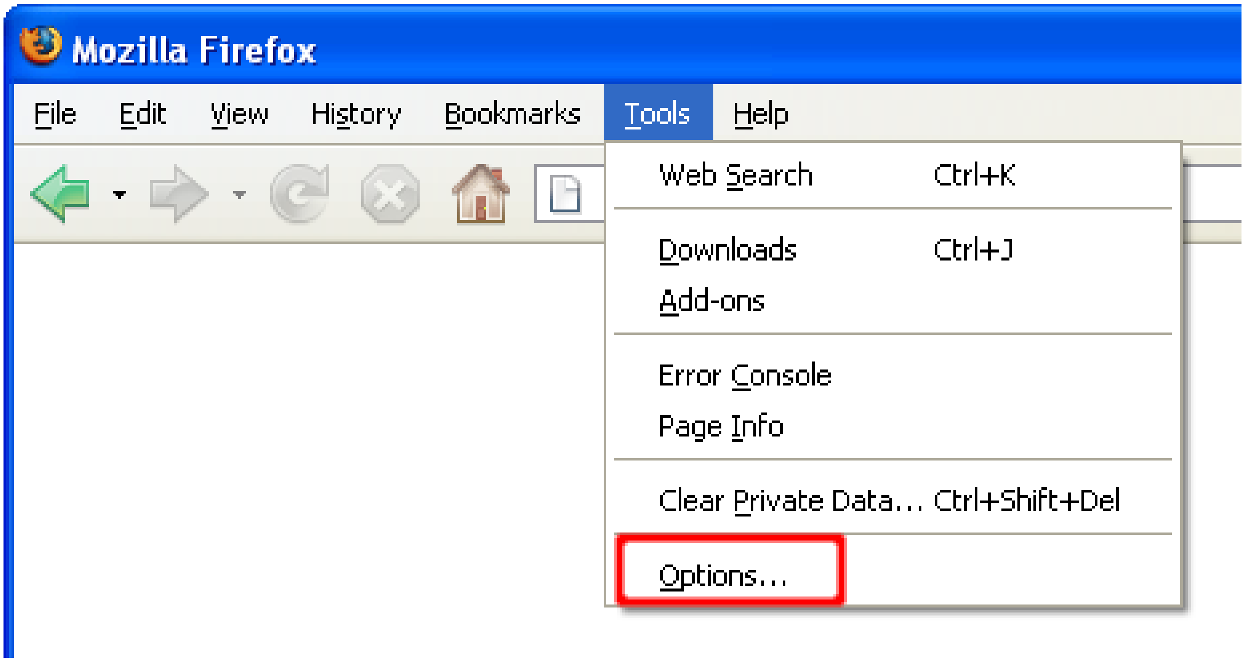
Enable or disable browser add-ons installed in your system.

B. Mozilla Firefox

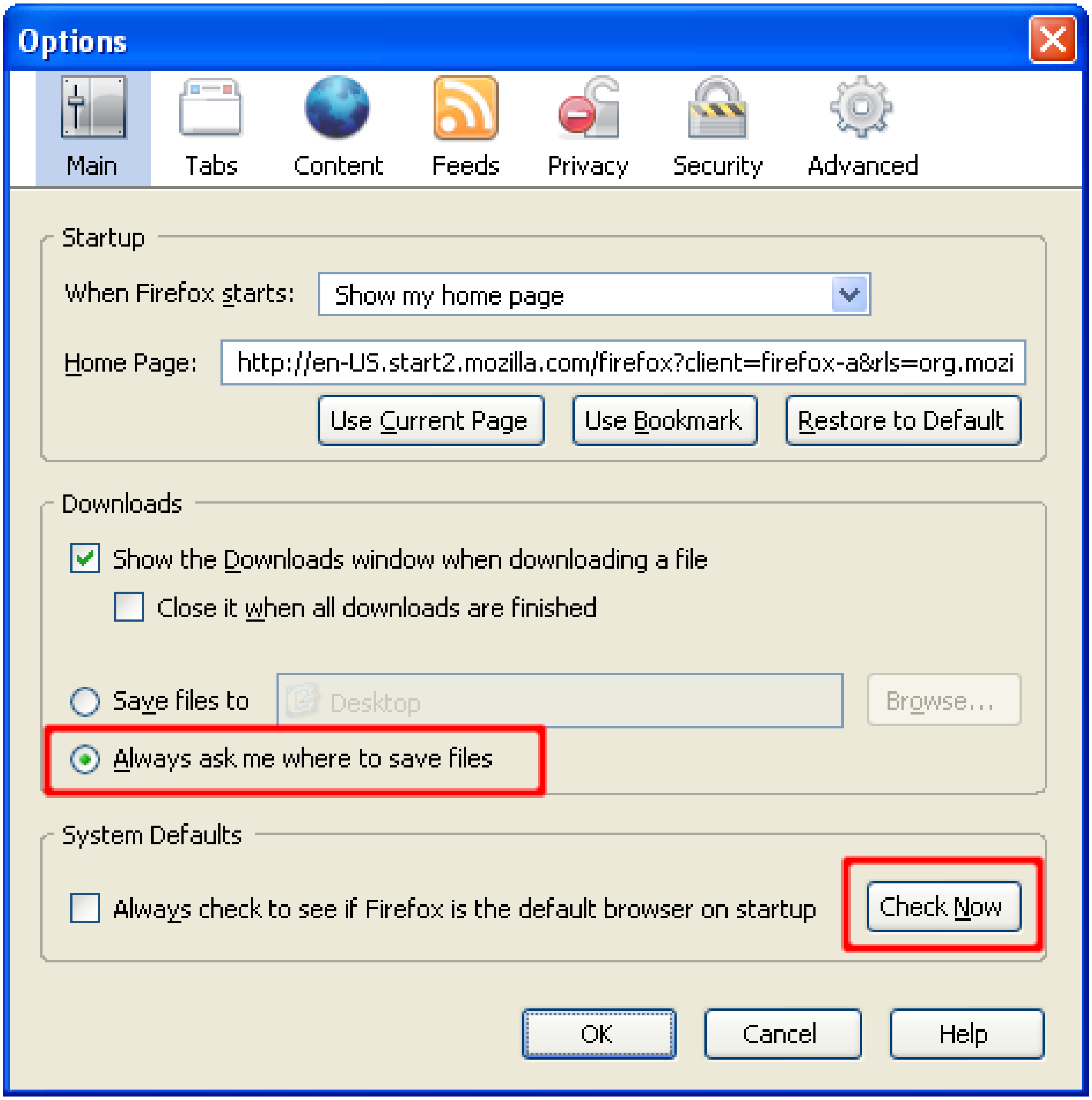
Mozilla Firefox supports many features of the same features as Internet Explorer, with the exception of ActiveX and the Security Zone model. Mozilla Firefox does have the underlying support for configurable security policies (CAPS), which is similar to Internet Explorer's Security Zone model, however there is no graphical user interface for setting these options. We recommend looking in the **Help, For Internet Explorer Users** menu to help users understand how terminology differs between the two applications.

The following are some steps to disable various features in Mozilla Firefox. Note that some menu options may change between versions or may appear in different locations depending on the host operating system. You should adapt the steps below as appropriate.

To edit the settings for Mozilla Firefox, select **Tools**, then **Options**.



You will then see an Options window that has a Category row at the top and the features for that category below. The first category of interest is the **General** category. Under this section, you can set Firefox as your default browser. Also select the option **Always ask me where to save files**. This will make it more obvious when a web page attempts to save a file to your computer.



Startup

When Firefox starts: Show my home page

Home Page: http://en-US.start2.mozilla.com/firefox?client=firefox-a&rls=org.mozi

Downloads

☑ Show the Downloads window when downloading a file

□ Close it when all downloads are finished

○ Save files to Desktop

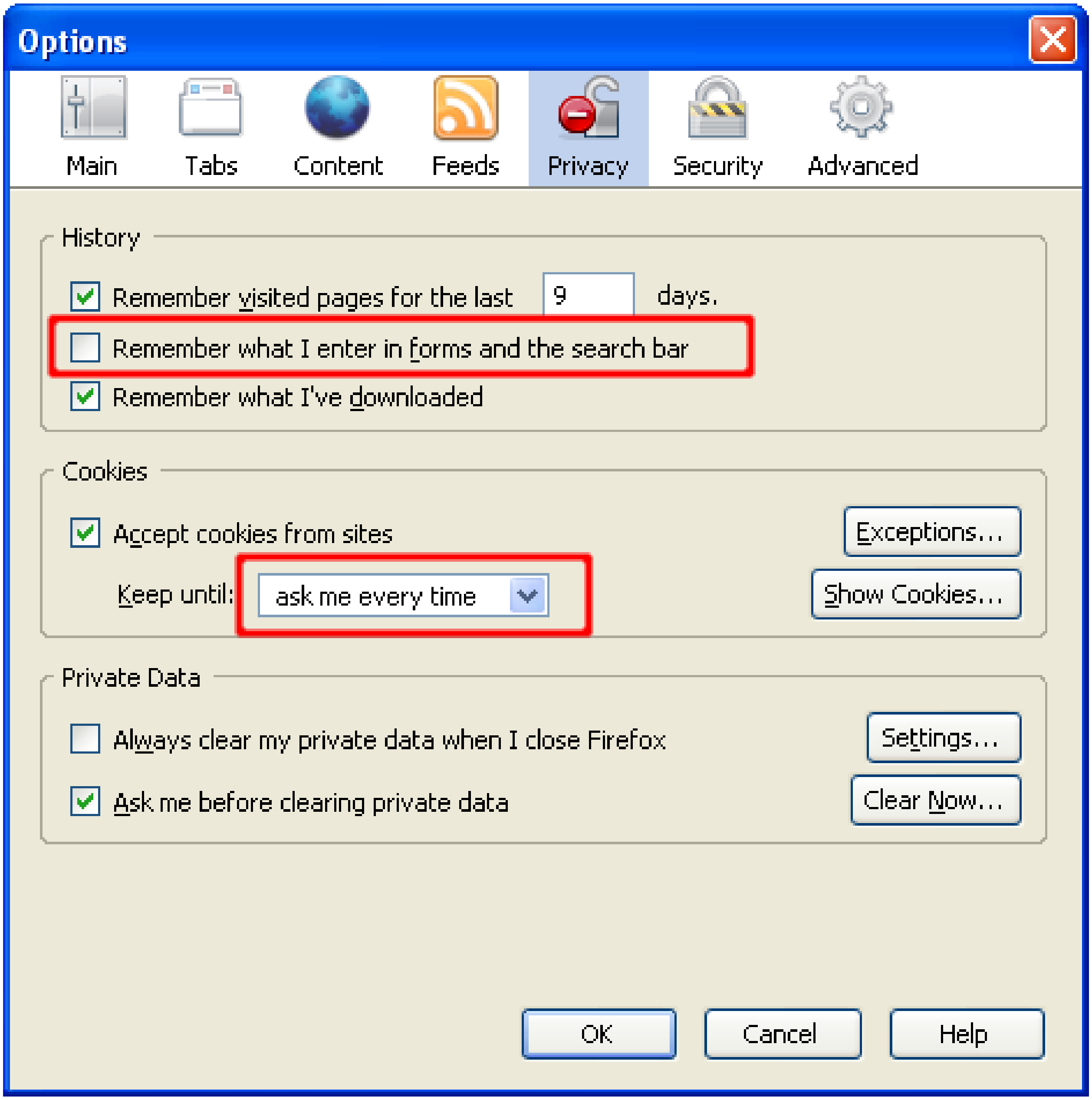
● Always ask me where to save files

System Defaults

□ Always check to see if Firefox is the default browser on startup

Under the **Privacy** category, you will find options for browser History and Cookies. In the History section, disable the option to **Remember what I enter in forms and the search bar**. If the browser remembers these options, it can be a privacy violation, especially if the browser is used in a shared environment. Visited page and download history can be disabled here too.

In the Cookie section, select **ask me every time**. This will help make it clear when a web site is attempting to set a cookie.



History

☑ Remember visited pages for the last 9 days.

□ Remember what I enter in forms and the search bar

☑ Remember what I've downloaded

Cookies

☑ Accept cookies from sites

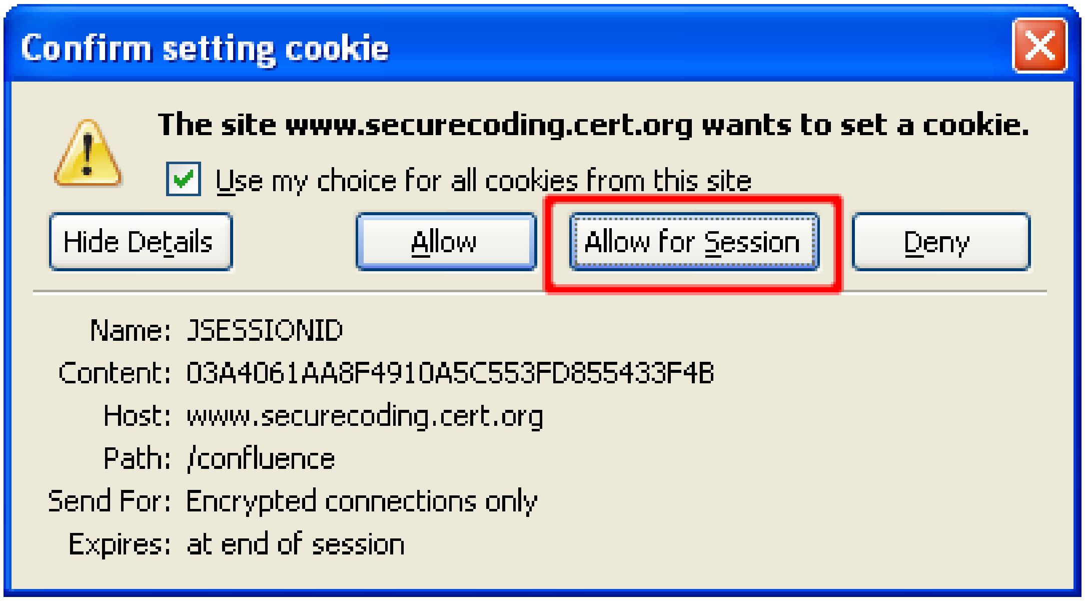
Keep until: ask me every time

Private Data

□ Always clear my private data when I close Firefox

☑ Ask me before clearing private data

When the user is prompted, the contents of the cookie can be viewed and the user can select whether to **Deny**, **Allow for Session**, or **Allow** the cookie. This gives the user more information about what sites are using cookies and also gives more granular control of cookies as opposed to globally enabling them. Select **Use my choice for all cookies from this site** to have the browser remember your decision so that you will not be prompted each time you return to the site. Clicking the **Allow for Session** button will cause the cookie to be cleared when the browser is restarted. If prompting for each cookie is too excessive, the user may wish to select the **Keep until: I close Firefox** option. This will prevent web sites from being able to set persistent cookies.



Confirm setting cookie

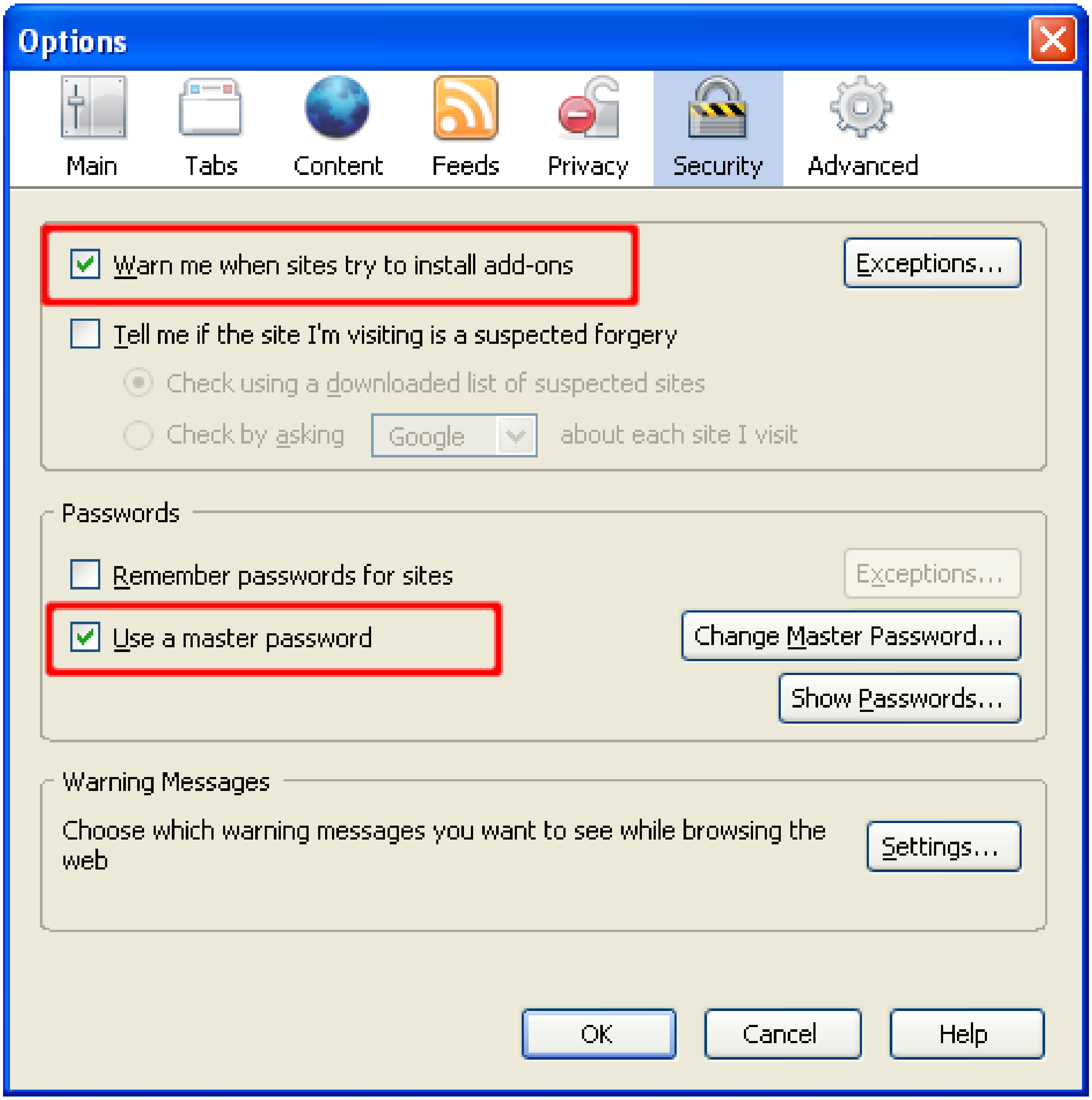
The site www.securecoding.cert.org wants to set a cookie.

☑ Use my choice for all cookies from this site

Name: JSESSIONID
Content: 03A4061AA8F4910A5C553FD855433F4B
Host: www.securecoding.cert.org
Path: /confluence
Send For: Encrypted connections only
Expires: at end of session

Many web browsers will offer the ability to store login information. In general, we recommend against using such features. Should you decide to use the feature, ensure that you use the measures available to protect the password data on your computer. Under the **Security** category, the **Passwords** section contains various options to manage stored passwords, and a **Master Password** feature to encrypt the data on your system. We encourage you to use this option if you decide to let Mozilla Firefox manage your passwords.

The **Warn me when sites try to install add-ons** option will display a warning bar at the top of the browser when a web site attempts to take such an action.



☑ Warn me when sites try to install add-ons

□ Tell me if the site I'm visiting is a suspected forgery

● Check using a downloaded list of suspected sites

○ Check by asking Google about each site I visit

Passwords

□ Remember passwords for sites

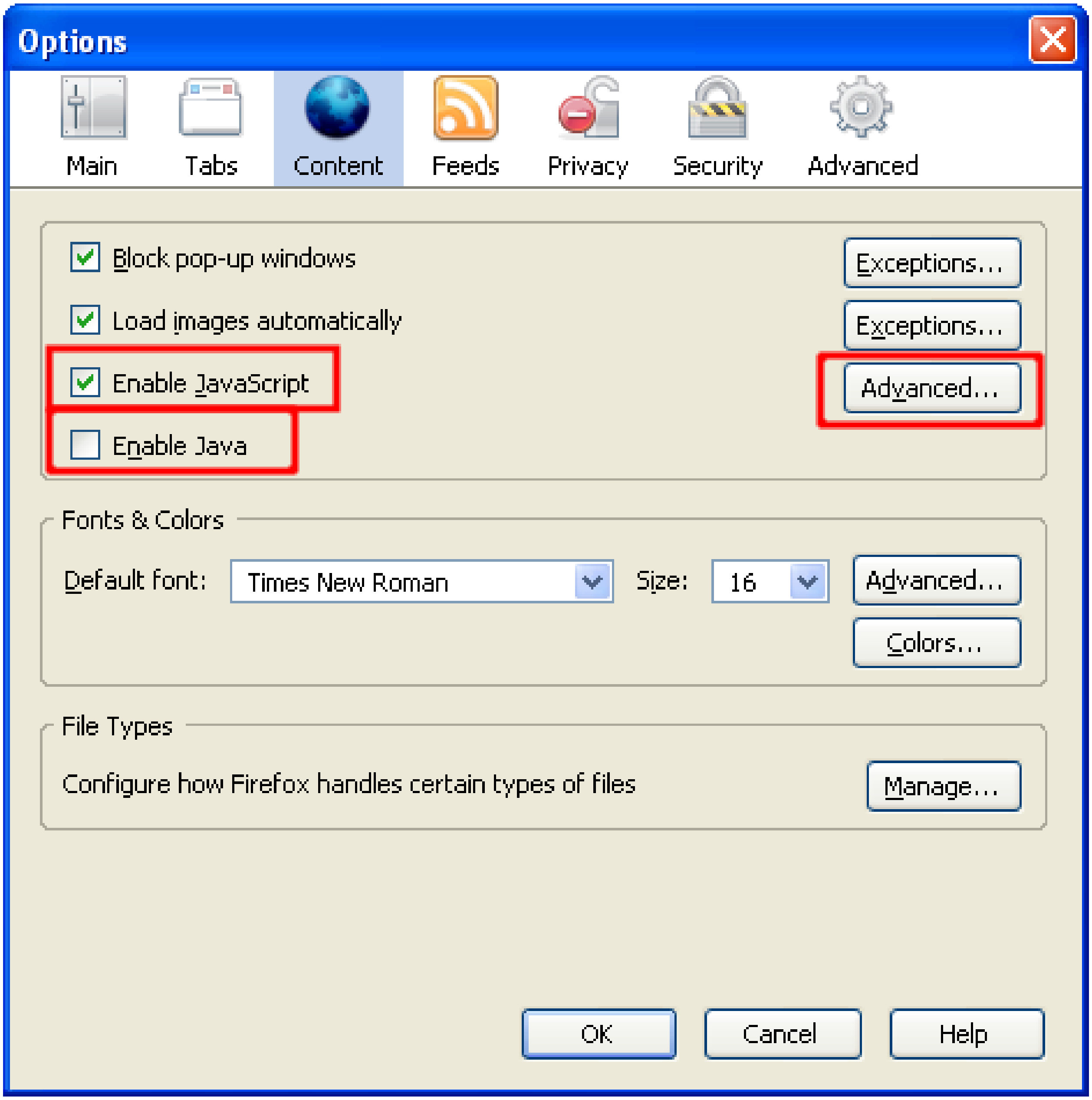
☑ Use a master password

Warning Messages

Choose which warning messages you want to see while browsing the web

The **Content** category contains an option to **Enable Java**. Java is a programming language that permits web site designers to run applications on your computer. We recommend **disabling** this feature unless required by the trusted site you wish to visit. Again, you should determine if this site is trustworthy and whether you want to enable Java to view the site's content. After you are finished visiting the site, we recommend disabling Java until needed again.

Press the **Advanced** button to disable specific JavaScript features. We recommend disabling all of the options displayed in this dialog.



☑ Block pop-up windows

☑ Load images automatically

☑ Enable JavaScript

□ Enable Java

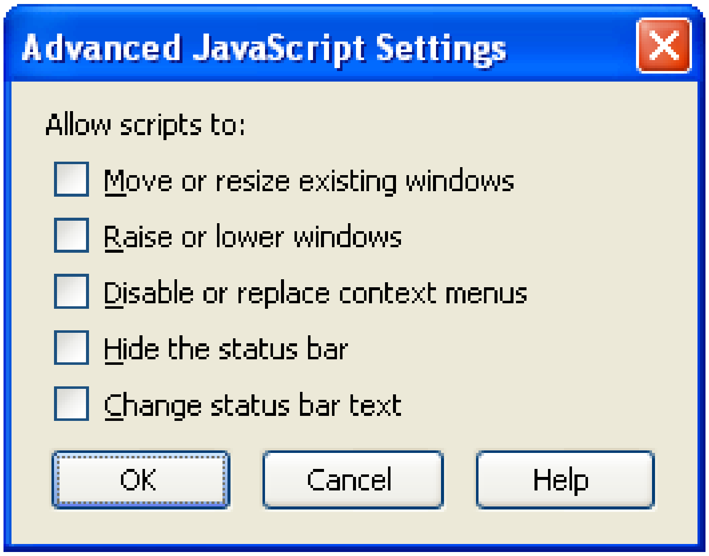
Fonts & Colors

Default font: Times New Roman

Size: 16

File Types

Configure how Firefox handles certain types of files



Allow scripts to:

□ Move or resize existing windows

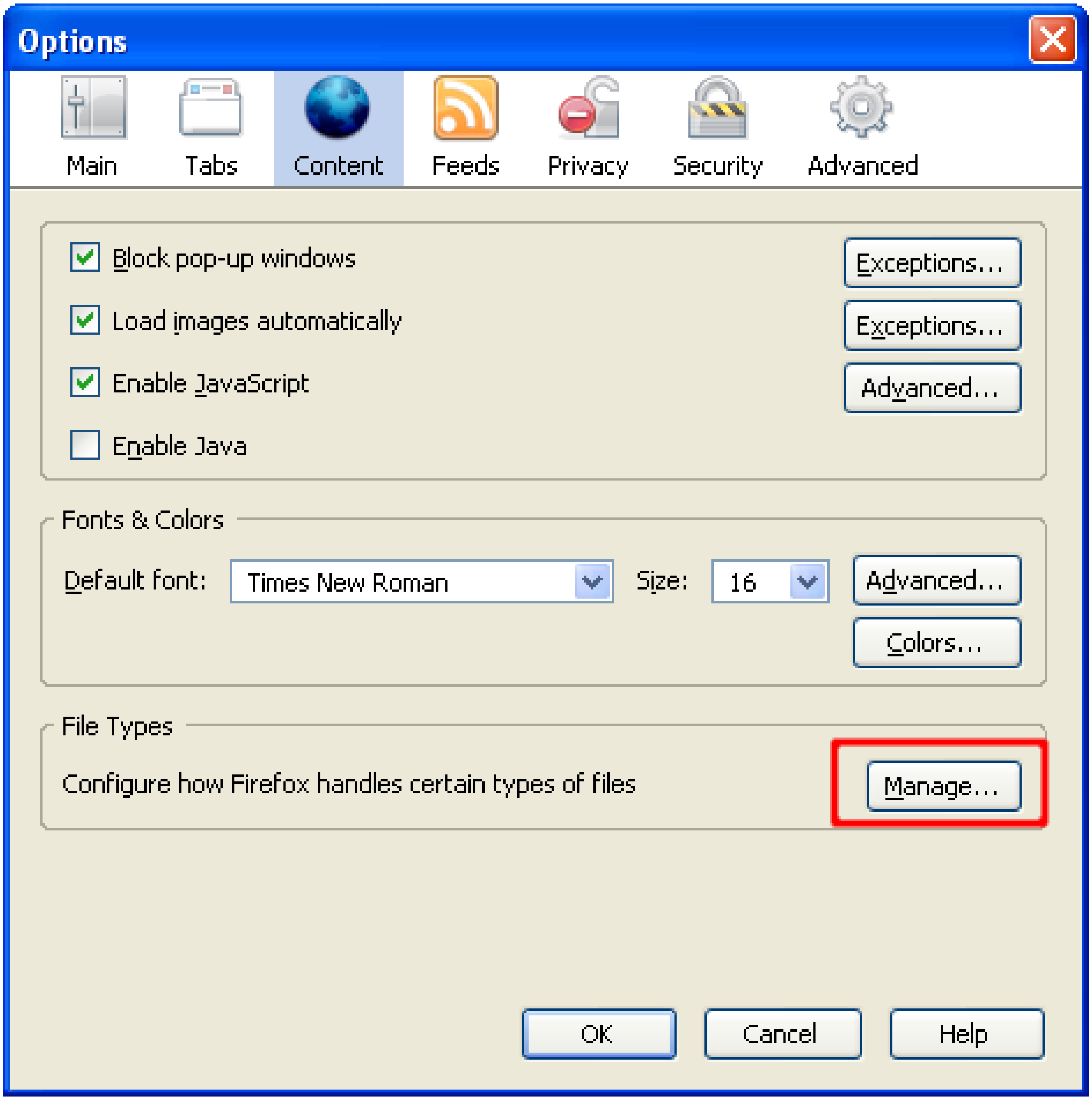
□ Raise or lower windows

□ Disable or replace context menus

□ Hide the status bar

□ Change status bar text

The **Content** section has an option to modify actions taken when files are downloaded. Any time a file type is configured to automatically open with an associated application, this can make the browser more dangerous to use. Vulnerabilities in these associated applications can be exploited more easily when they are configured to automatically open. Click the **Manage** button to view the current download settings and modify them if necessary.



☑ Block pop-up windows

☑ Load images automatically

☑ Enable JavaScript

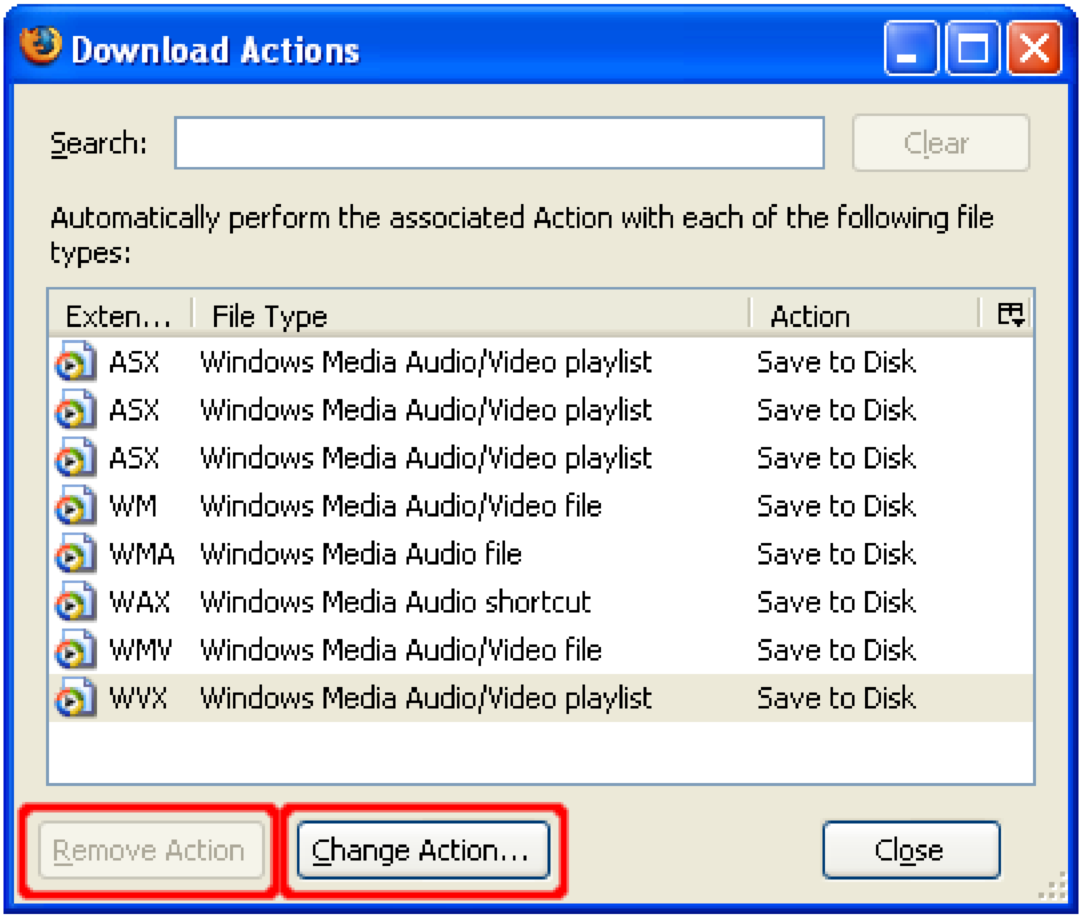
☐ Enable Java

Default font: Times New Roman

Size: 16

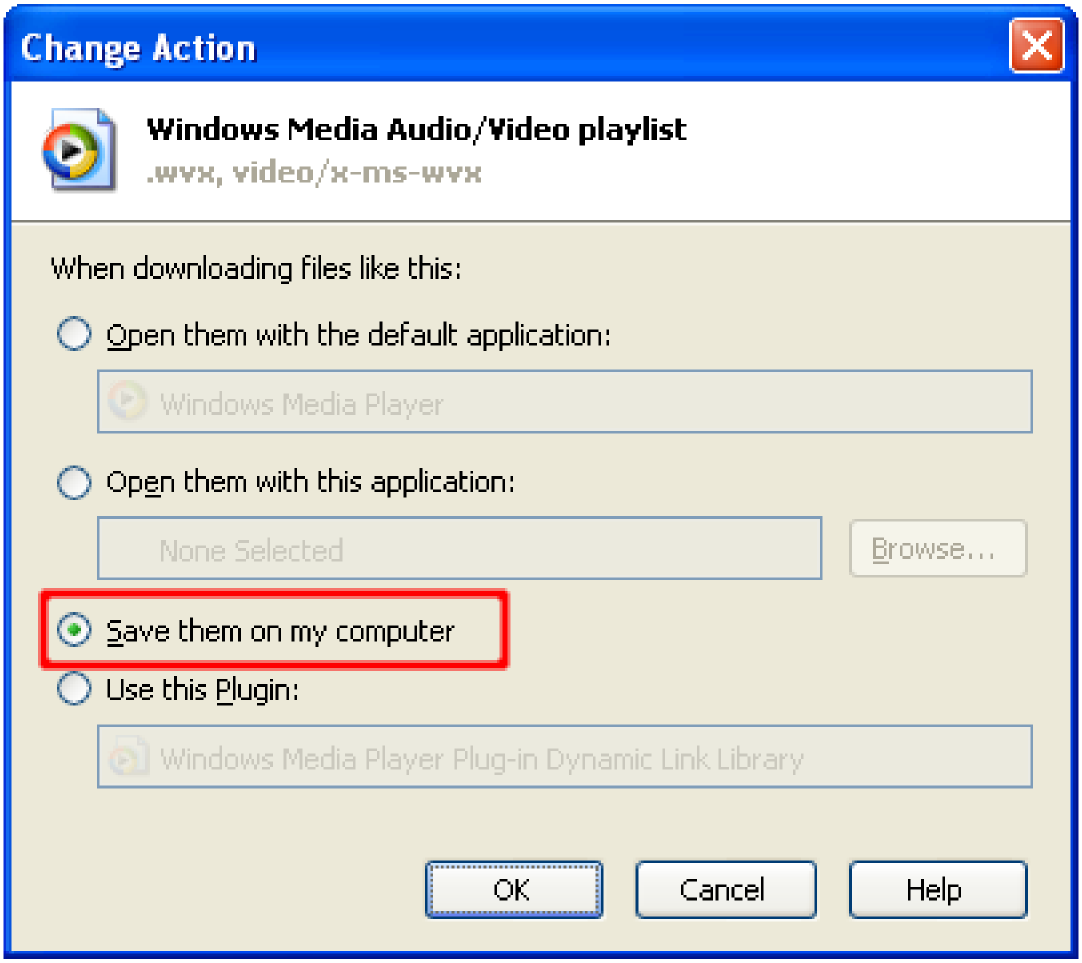
Configure how Firefox handles certain types of files

The Download Actions dialog will show the file types and the currently configured actions to take when the browser encounters such a file. For **all** listed file types, either select **Remove Action** or **Change Action...** to modify the action to save the file to the computer. This increases the amount of user action required to launch the associated applications, and will therefore help prevent automated exploitation of vulnerabilities that may exist in these applications.



Automatically perform the associated Action with each of the following file types:

Exten...	File Type	Action
ASX	Windows Media Audio/Video playlist	Save to Disk
ASX	Windows Media Audio/Video playlist	Save to Disk
ASX	Windows Media Audio/Video playlist	Save to Disk
WM	Windows Media Audio/Video file	Save to Disk
WMA	Windows Media Audio file	Save to Disk
WAX	Windows Media Audio shortcut	Save to Disk
WMV	Windows Media Audio/Video file	Save to Disk
WVX	Windows Media Audio/Video playlist	Save to Disk



Windows Media Audio/Video playlist
.wvx, video/x-ms-wvx

When downloading files like this:

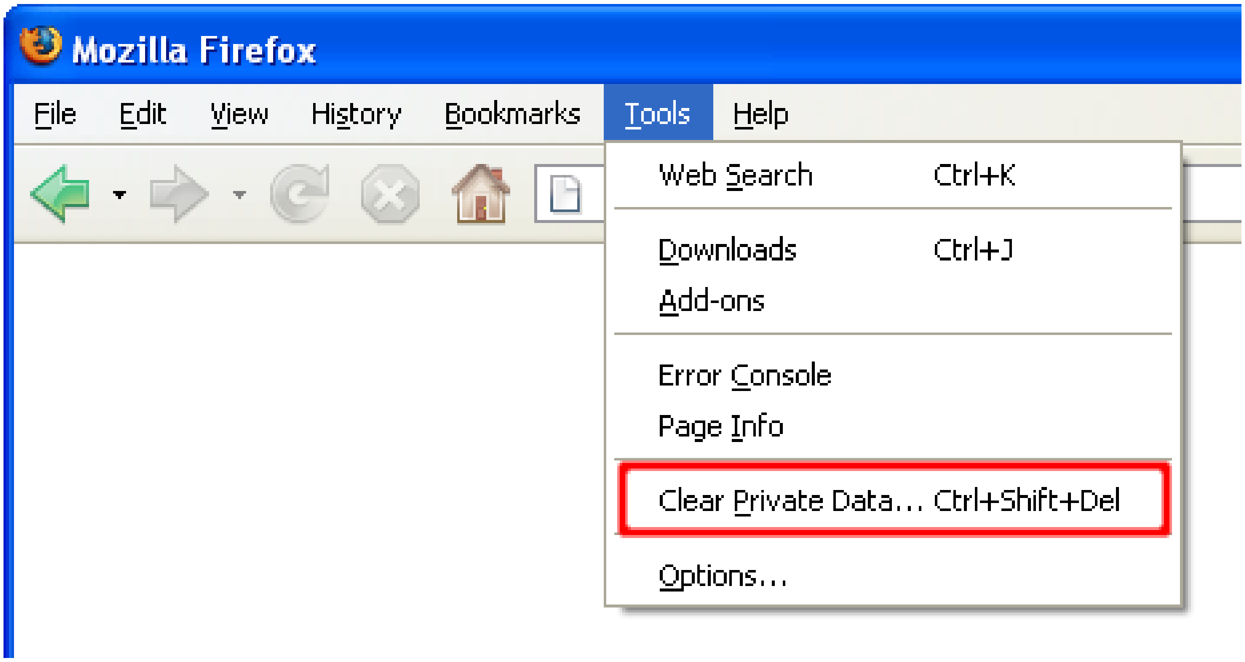
○ Open them with the default application:
Windows Media Player

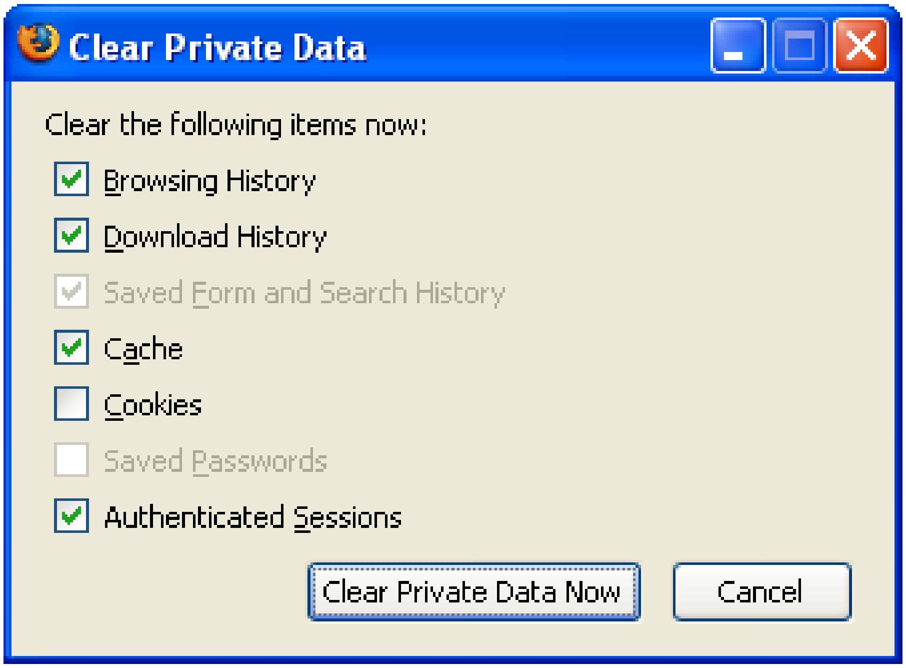
○ Open them with this application:
None Selected
Browse...

● Save them on my computer

○ Use this Plugin:
Windows Media Player Plug-in Dynamic Link Library

Firefox 1.5 and later include a feature to **Clear Private Data**. This option will remove potentially sensitive information from the web browser. Select **Clear Private Data...** from the **Tools** menu to use this privacy feature.





Clear the following items now:

☑ Browsing History

☑ Download History

☑ Saved Form and Search History

☑ Cache

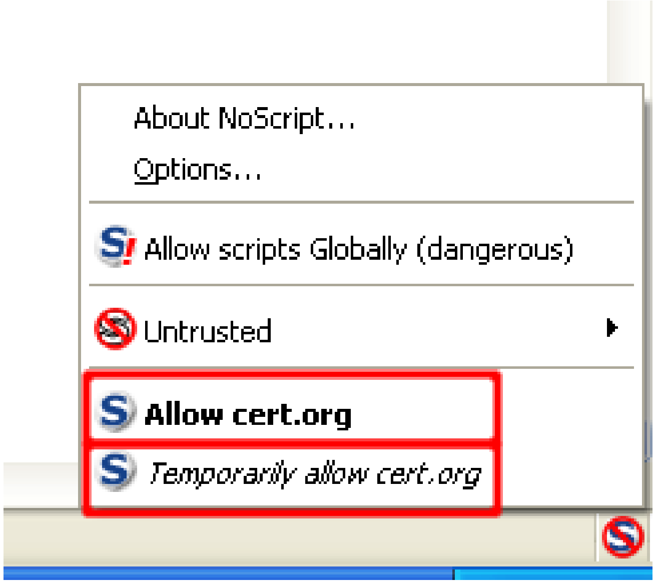
☐ Cookies

☐ Saved Passwords

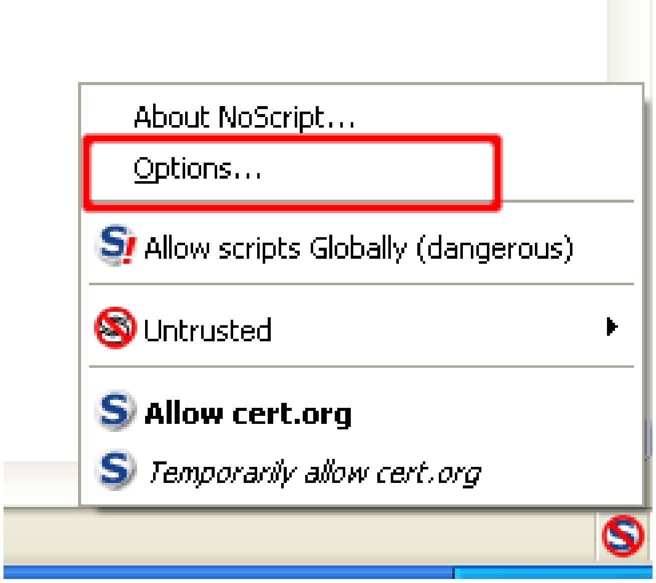
☑ Authenticated Sessions

Because Firefox does not have easily-configured security zones like Internet Explorer, it can be difficult to configure the web browser options on a per-site basis. For example, a user may wish to enable JavaScript for a specific, trusted site, but have it disabled for all other sites. This functionality can be added to Firefox with an add-on, such as NoScript.

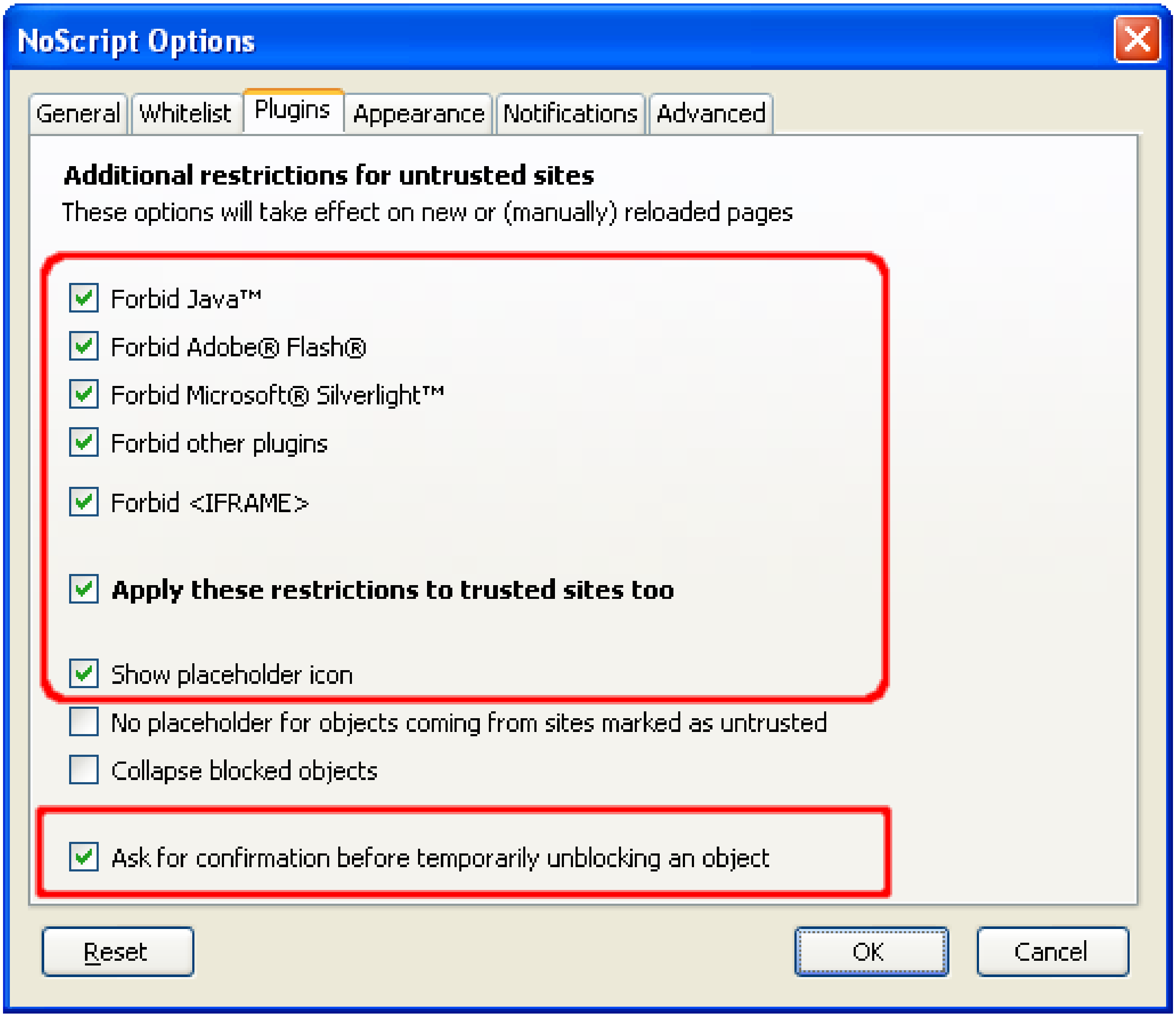
With NoScript installed, JavaScript will be disabled for sites by default. The user can allow scripts for a web site by using the NoScript icon menu. Scripts can be allowed for a site on a temporary or a more permanent basis. If **Temporarily allow** is selected, then scripts are enabled for that site until the browser is closed.


About NoScript...
Options...
Allow scripts Globally (dangerous)
Untrusted
Allow cert.org
Temporarily allow cert.org

Because many web browser vulnerabilities require scripting, configuring the browser to have scripting disabled by default greatly reduces the chances of exploitation. To extend this protection even further, NoScript can be configured to also block Java, Flash, and other plug-ins by default. This can help to mitigate any vulnerabilities in these plug-in technologies. NoScript will replace these elements with a placeholder icon, which can be clicked to enable the element. Click the NoScript icon and then click **Options...** to get to the NoScript configuration screen.


About NoScript...
Options...
Allow scripts Globally (dangerous)
Untrusted
Allow cert.org
Temporarily allow cert.org

On the **Plugins** tab, select the options as follows:



Additional restrictions for untrusted sites

These options will take effect on new or (manually) reloaded pages

☑ Forbid Java™

☑ Forbid Adobe® Flash®

☑ Forbid Microsoft® Silverlight™

☑ Forbid other plugins

☑ Forbid <IFRAME>

☑ **Apply these restrictions to trusted sites too**

☑ Show placeholder icon

□ No placeholder for objects coming from sites marked as untrusted

□ Collapse blocked objects

☑ Ask for confirmation before temporarily unblocking an object

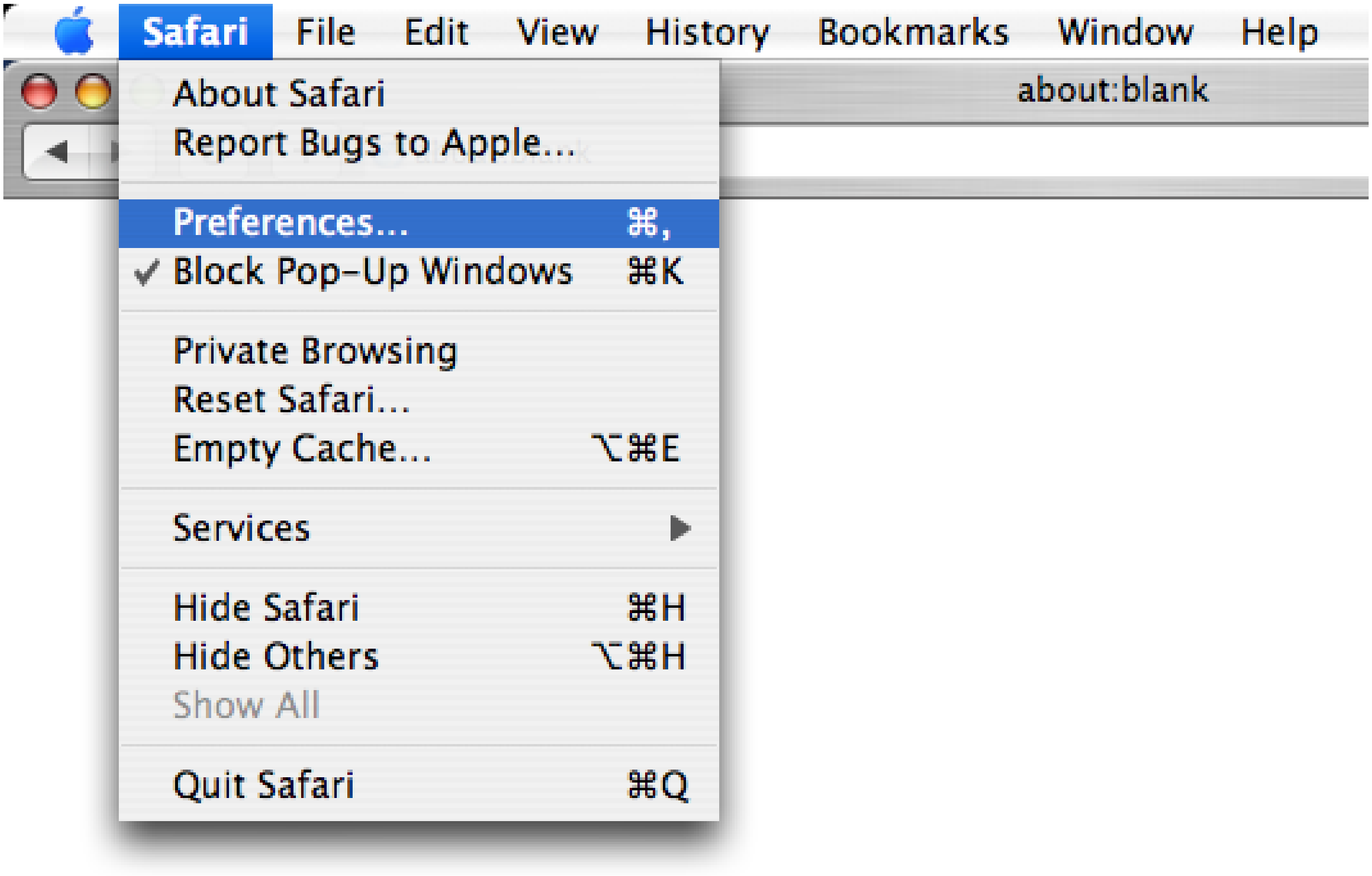
Aside from visiting web sites that are inherently malicious, users can also be put at risk when a legitimate, trusted site is compromised. For this reason, we recommend enabling the option to **Apply these restrictions to trusted sites too**. If this option is too intrusive, it can be turned off at the cost of increased risk.

C. Apple Safari

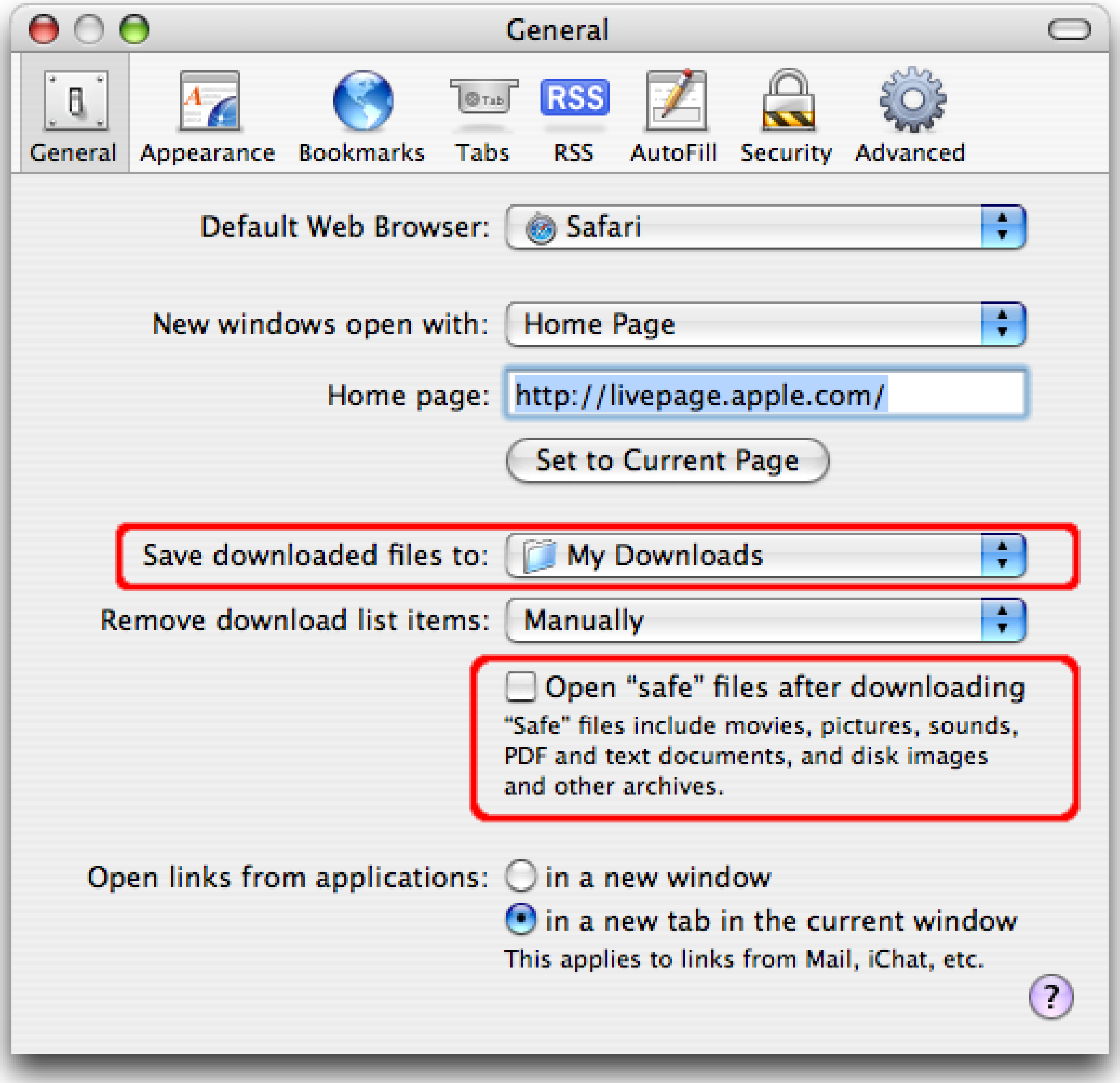
The Safari web browser supports many of the same features as Mozilla Firefox. The following are some steps to disable various features in Safari on Mac OS X. The options for Safari for Microsoft Windows may differ slightly. Also note that some menu options may change over time, and you should adapt the steps below as appropriate.

In order to change settings for Safari, select **Safari** then **Preferences…**

Note that on the Safari menu, you can also select the option “Block Pop-up Windows”. This option will prevent sites from opening another window through the use of scripting or active content. Be aware that while Pop-up Windows are often associated with advertisements, some sites may attempt to display relevant content in a new window. Therefore, setting this option may disable the functionality of some sites.



Once you select the **Preferences** menu, the window below will open. The first tab to look at is the **General** tab. On this tab you can set up many options such as **Save downloaded files to:** and **Open "safe" files after downloading**. We recommend that you download files to a folder that you create for that purpose. We also recommend that you deselect the **Open "safe" files after downloading** option.



Default Web Browser: Safari

New windows open with: Home Page

Home page: http://livepage.apple.com/

Set to Current Page

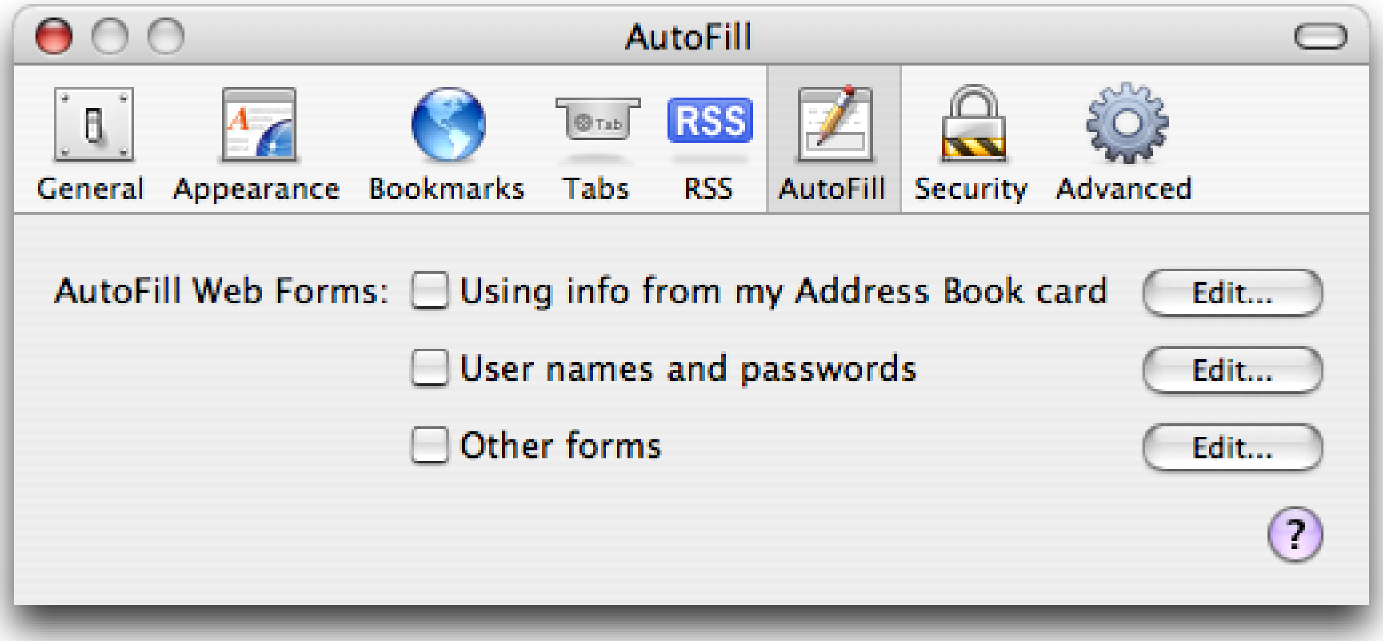
Save downloaded files to: My Downloads

Remove download list items: Manually

□ Open "safe" files after downloading
"Safe" files include movies, pictures, sounds, PDF and text documents, and disk images and other archives.

Open links from applications: ○ in a new window
● in a new tab in the current window
This applies to links from Mail, iChat, etc.

The next section of interest is the **AutoFill** tab. On this tab, you can select what types of forms your browser will fill in automatically. In general, we recommend against using AutoFill features. If someone can gain access to your machine, or the AutoFill data files, then the AutoFill feature may allow them to use the stored credentials to access to other sites that they would not otherwise have the ability to access. However, if used with appropriate protective measures, it may be acceptable to enable AutoFill. We recommend using filesystem encryption software such as OS X FileVault along with the **Use secure virtual memory** option to provide additional security for files that reside in a user's home directory.



AutoFill Web Forms: □ Using info from my Address Book card

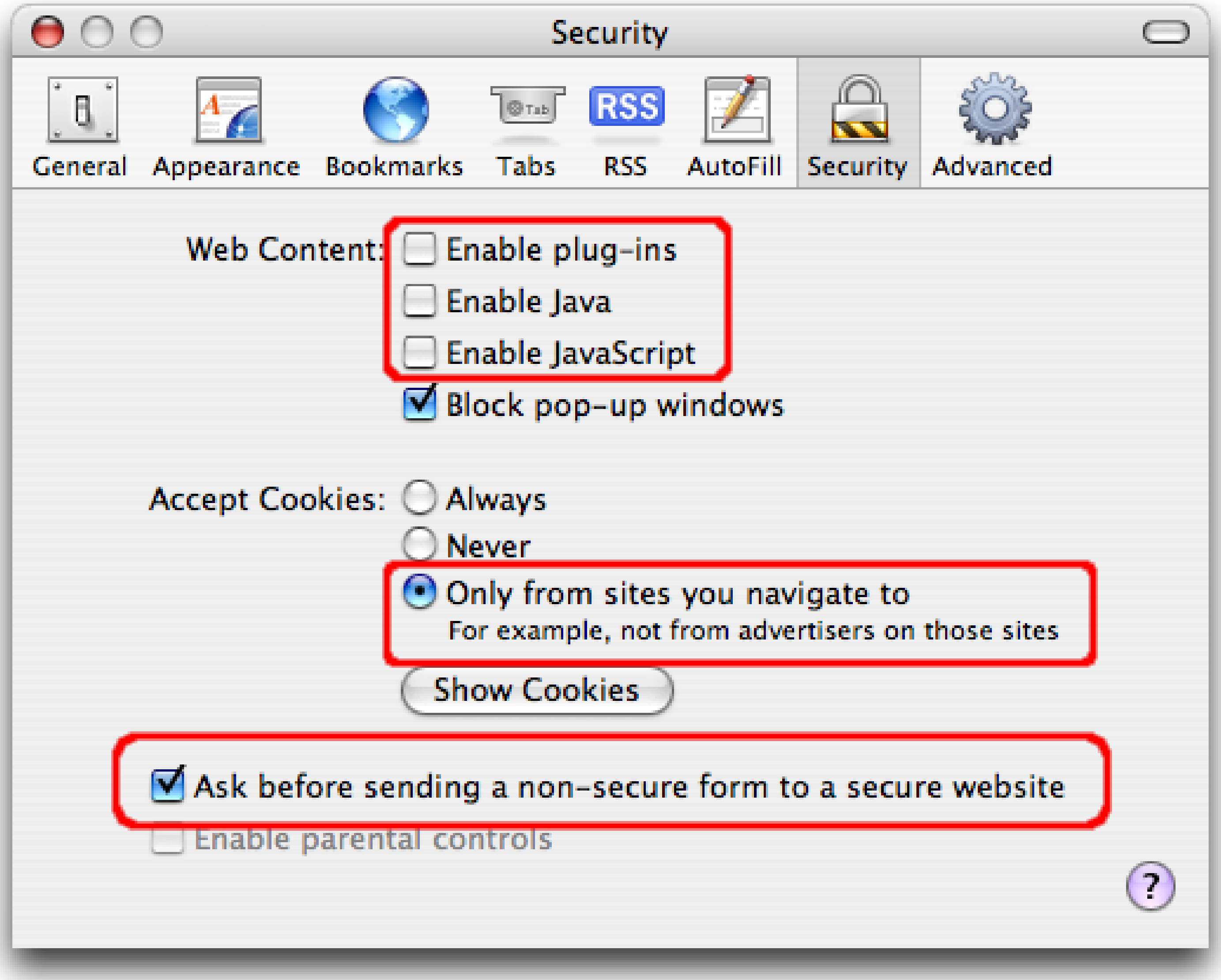
□ User names and passwords

□ Other forms

The **Security** tab provides several options. The **Web Content** section permits you to enable or disable various forms of scripting and active content. We recommend disabling the first three options in this section, and only enabling them based on site-specific cases. We recommend selecting the **Block Pop-up Windows** option. Remember that this option will prevent sites from opening another window through the use of scripting, or active content. Again, be aware that while Pop-up Windows are often associated with advertisements, some sites may attempt to display relevant content in a new window. Therefore, setting this option may disable the functionality of some sites.

It is safer to use Safari without plug-ins and Java, so we recommend **disabling** the options **Enable plug-ins** and **Enable Java**. It is also safer to **disable JavaScript**. However, many web sites require JavaScript for proper operation.

In this dialog you can disable cookies and also view or remove cookies that have been set. In general we recommend disabling cookies, and enabling them only when you visit a site that requires their use. At this point, you should determine if the site is trustworthy and whether you want to enable cookies to view the site’s content. After you are finished visiting the site, we recommend disabling cookies until needed again. You can choose to only accept cookies from the sites that visit by selecting the **Only from sites you navigate to** option. This will permit sites that you visit to set cookies, but not third-party sites. Finally, we recommend selecting the **Ask before sending a non-secure form to a secure website** option. This will prompt you before sending unencrypted form data when viewing an HTTPS-secured web site.



Web Content: □ Enable plug-ins
□ Enable Java
□ Enable JavaScript
☑ Block pop-up windows

Accept Cookies: ○ Always
○ Never
● Only from sites you navigate to
For example, not from advertisers on those sites

☑ Ask before sending a non-secure form to a secure website
□ Enable parental controls

D. Other Browsers

Other web browsers may have similar options to those described above. Please refer to the browser documentation to determine which options are available and how to make the necessary changes. For example, the links below show where to find information for four popular web browsers:

Opera - http://www.opera.com/support/tutorials/security
Mozilla SeaMonkey - http://www.mozilla.org/projects/seamonkey
Konqueror - http://www.konqueror.org
Netscape - http://browser.netscape.com

> Note that official support for Netscape has ended on February 1st, 2008. If you are using Netscape, we strongly recommend switching to a browser that is still supported.

IV. Keeping Your Computer Secure

In addition to selecting and securing your web browser, you can take measures to increase protection to your computer in general. The following are steps and links to information resources that will help you secure your computer.

1. **Read the Home Network Security and Home Computer Security documents.**

2. **Enable automatic software updates if available**

   Vendors will usually release patches for their software when a vulnerability has been discovered. Most product documentation offers a method to get updates and patches. You should be able to obtain updates from the vendor's web site. Read the manuals or browse the vendor's web site for more information.

   Some applications will automatically check for available updates, and many vendors offer automatic notification of updates via a mailing list. Look on your vendor's web site for information about automatic notification. If no mailing list or other automated notification mechanism is offered, you may need to check the vendor's web site periodically for updates.

3. **Install and use antivirus software**

   While an up-to-date antivirus software package cannot protect against all malicious code, for most users it remains the best first-line of defense against malicious code attacks. Many antivirus packages support automatic updates of virus definitions. We recommend using these automatic updates when available. A partial list of antivirus vendors is available is available on the CERT/CC web site.

4. **Avoid unsafe behavior**

   Additional information on this topic can be found in the Home Network Security document.
   - Use caution when opening email attachments or when using peer-to-peer file sharing, instant messaging, or chat rooms.
   - Don't enable file sharing on network interfaces exposed directly to the internet.

5. **Follow the principle of least privilege — don't enable it if you don't need it**

   Consider creating and using an account with limited privileges instead of an 'administrator' or 'root' level account for everyday tasks. Depending on the operating system, you only need to use administrator level access when installing new software, changing system configurations, etc. Many vulnerability exploits (e.g., viruses, Trojan horses) are executed with the privileges of the user that runs them — making it far more risky to be logged in as an administrator all the time.

References

CERT/CC References

- Before You Connect a New Computer to the Internet — http://www.cert.org/tech_tips/before_you_plug_in.html
- Home Network Security — http://www.cert.org/tech_tips/home_networks.html
- Home Computer Security — http://www.cert.org/homeusers/HomeComputerSecurity/
- Technical Trends in Phishing Attacks — http://www.cert.org/archive/pdf/Phishing_trends.pdf
- Spyware — http://www.cert.org/archive/pdf/spyware2005.pdf

US-CERT References

- Understanding Your Computer: Web Browsers — http://www.us-cert.gov/cas/tips/ST04-022.html
- Evaluating Your Web Browser's Security Settings — http://www.us-cert.gov/cas/tips/ST05-001.html
- Browsing Safely: Understanding Active Content and Cookies — http://www.us-cert.gov/cas/tips/ST04-012.html
- Understanding Web Site Certificates — http://www.us-cert.gov/cas/tips/ST05-010.html
- Understanding Internationalized Domain Names — http://www.us-cert.gov/cas/tips/ST05-016.html
- Avoiding Social Engineering — http://www.us-cert.gov/cas/tips/ST04-014.html

Microsoft Windows XP References

- Improve the safety of your browsing and e-mail activities — http://www.microsoft.com/athome/security/online/browsing_safety.mspx
- Microsoft's Protect Your PC — http://www.microsoft.com/protect/
- Using Windows Firewall — http://www.microsoft.com/windowsxp/using/networking/security/winfirewall.mspx
- Microsoft Windows XP Baseline Security Checklist — http://www.microsoft.com/technet/archive/security/chklist/xpcl.mspx
- Microsoft Windows XP Service Pack 2 — http://www.microsoft.com/windowsxp/sp2/default.mspx
- Setting Up Security Zones — http://www.microsoft.com/windows/ie/using/howto/security/setup.mspx

Apple Macintosh OSX References

- Apple Product Security — http://www.apple.com/support/security/

- How to Keep Network Computers Secure — http://docs.info.apple.com/article.html?artnum=61534
- OSX Security Features Overview — http://www.apple.com/macosx/features/security/
- Apple Security Updates — http://docs.info.apple.com/article.html?artnum=61798
- Mac OS X Security Configuration — http://images.apple.com/server/pdfs/Tiger_Security_Config.pdf

Linux References

- Ubuntu Security notices — http://www.ubuntu.com/usn/
- Mandriva Security Advisories — http://www.mandriva.com/security/advisories
- SUSE Security (US/Canada) — http://www.novell.com/linux/security/securitysupport.html
- RedHat Security and Errata — http://www.redhat.com/apps/support/errata/
- Debian Security Information — http://www.debian.org/security/
- Gentoo Security Handbook — http://www.gentoo.org/doc/en/security/
- Slackware Security Advisories — http://www.slackware.com/security/

System Administrator References

- Description of Internet Explorer security zones registry entries — http://support.microsoft.com/?kbid=182569
- How To Set Advanced Settings In Internet Explorer by Using Group Policy Objects — http://support.microsoft.com/?kbid=274846
- Internet Explorer Administration Kit — http://www.microsoft.com/technet/prodtechnol/ie/ieak

Revision History

January 23, 2006	Inital Release
February 14, 2008	Updated Internet Explorer and Firefox guidelines

Produced by US-CERT 2006, 2008