



CompuGroup™
Medical

Configure Internet Explorer™

Version 10 Settings for

CGM® webPRACTICE™

CGMwebPRACTICE™

Fully Web-Based Practice Management Suite



Table of Contents

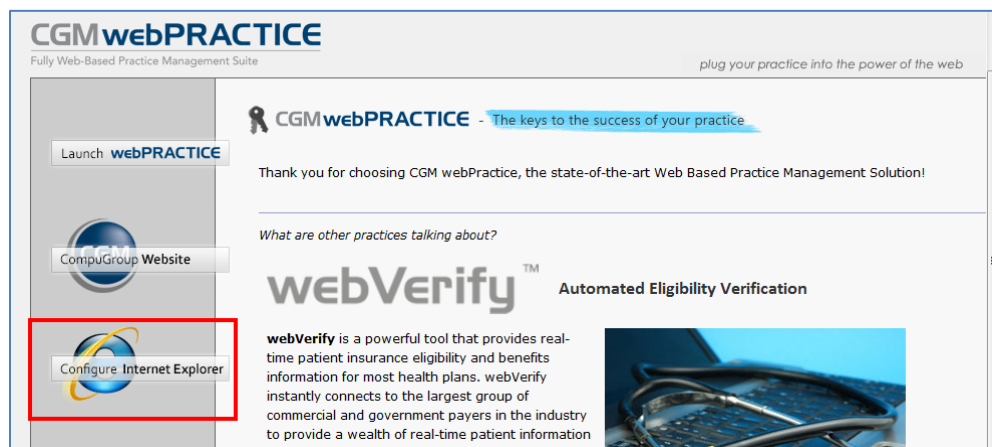
About this Document	3
Configuring IE Automatically Using CGM webPractice	3
Configuring IE Manually	4
Verify SmartScreen Filter is Turned On	4
Caching	5
Security Settings	8
Trusted Sites Settings	8
ActiveX Settings	10
Downloads Settings	11
Miscellaneous Settings	11
Scripting Settings	13
Advanced Settings	14
Privacy Settings	15
Printing Settings	16
Enable Compatibility View	17

ABOUT THIS DOCUMENT

These instructions apply to Internet Explorer (IE) version 10. It is important you complete all of the following instructions to make sure Internet Explorer has been set up properly. The quickest method to configure IE is to do so automatically using CGM webPractice, but if your permission settings do not allow it, manual instructions have also been included below.

CONFIGURING IE AUTOMATICALLY USING CGM WEBPRACTICE

On the **CGM webPractice** Homepage, click **Configure Internet Explorer**.



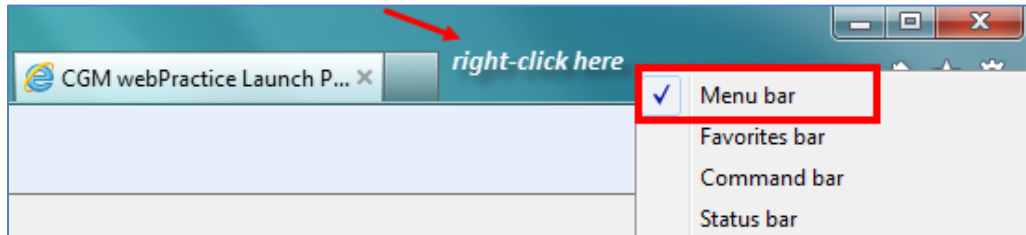
Notes:

- Do not use this automated function if you are running Windows 8.
- You must be a local administrator on your computer and have **User Access Control** disabled to complete this task using CGM webPractice. Verify this with your IT Department prior to using this feature.

When the Configure Internet Explorer function is complete, you will need to perform the steps for the **Printing Settings** and **Enable Compatibility View** to complete the process.

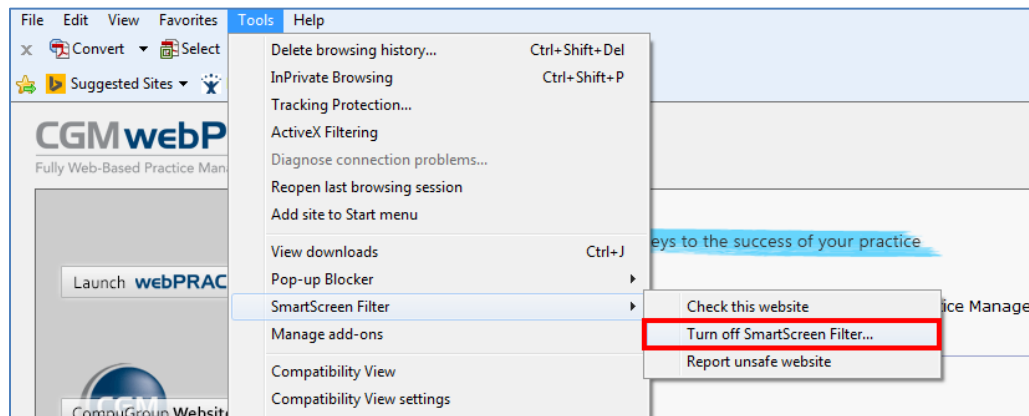
CONFIGURING IE MANUALLY

On the **CGM webPractice** Homepage, verify the **Menu bar** is displayed. If the **Menu bar** is not displayed, right-click in the empty space on the command bar, to the right of the tab and select **Menu bar**.



Verify SmartScreen Filter is Turned On

IE 10 typically loads with the **SmartScreen Filter** already turned on. To verify it is turned on, select **Tools** on the menu bar, scroll down to **SmartScreen Filter** and when the pop-up menu appears, verify it shows **Turn Off SmartScreen Filter**. This indicates that the **SmartScreen Filter** is on.



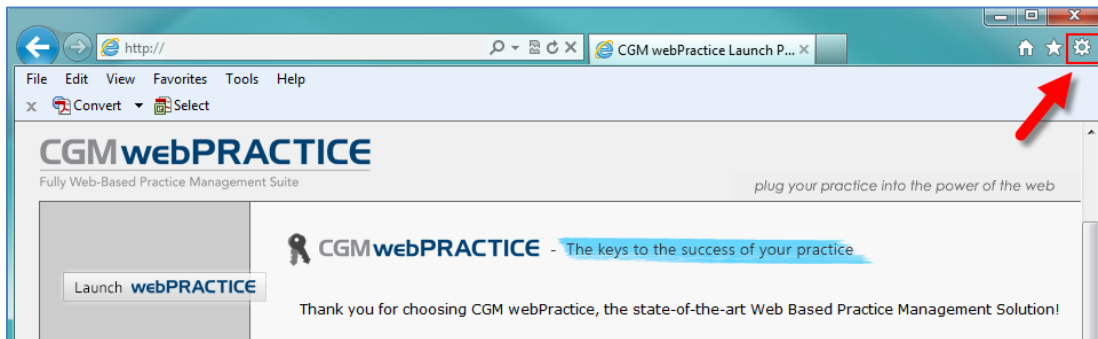
Caching

To provide faster loading times on webpages, Internet Explorer caches or stores webpages on your hard drive. For CGM webPractice to run properly, it is critical that caching be turned off.

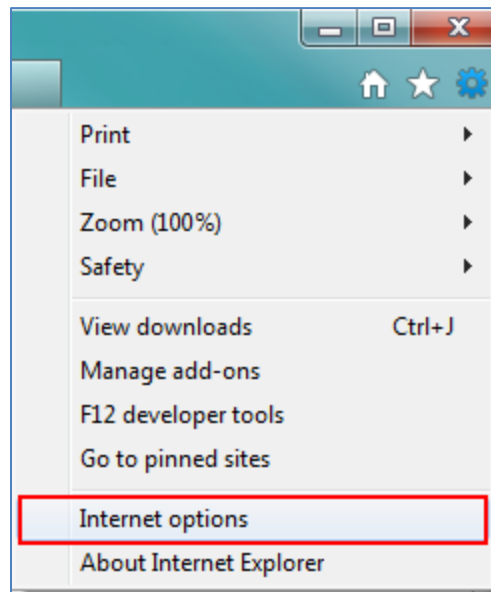
***NOTE:** CGM webPractice will not run properly if stored pages from the hard drive are used.

Turning off Caching

Click the **Tools** button  to display the **Tools** menu.

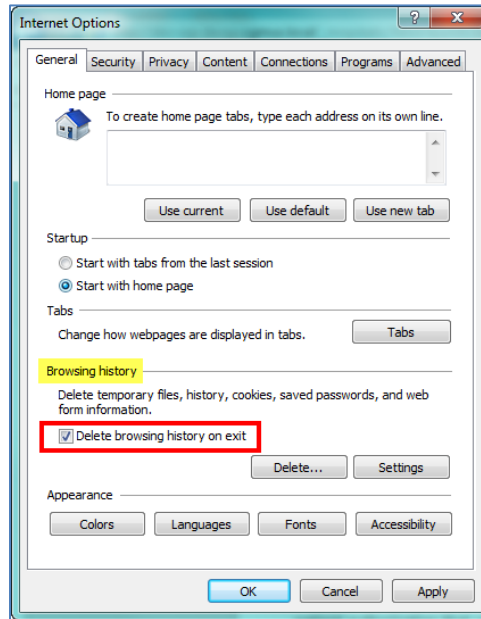


Click **Internet Options**.

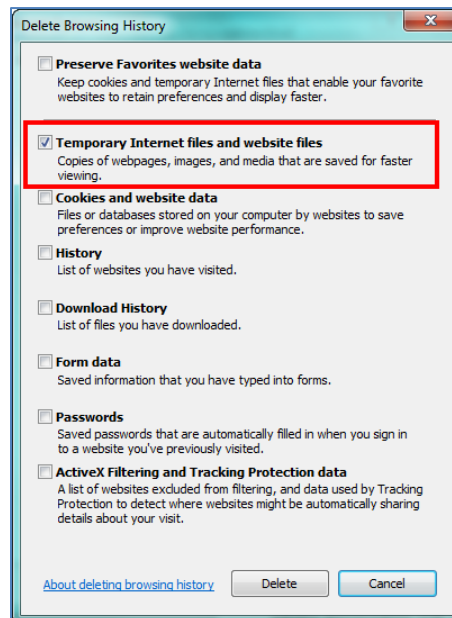


Caching (cont.)

Click the **General** tab if it is not already displayed. In the **Browsing history** section, Select the **Delete browsing history on exit** check box and then click **Delete**.

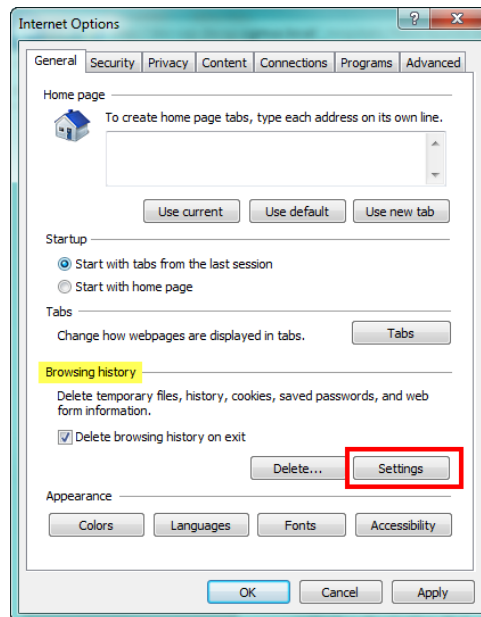


In the **Delete Browsing History** dialog box, select the **Temporary Internet Files and website files** check box and click **Delete**.

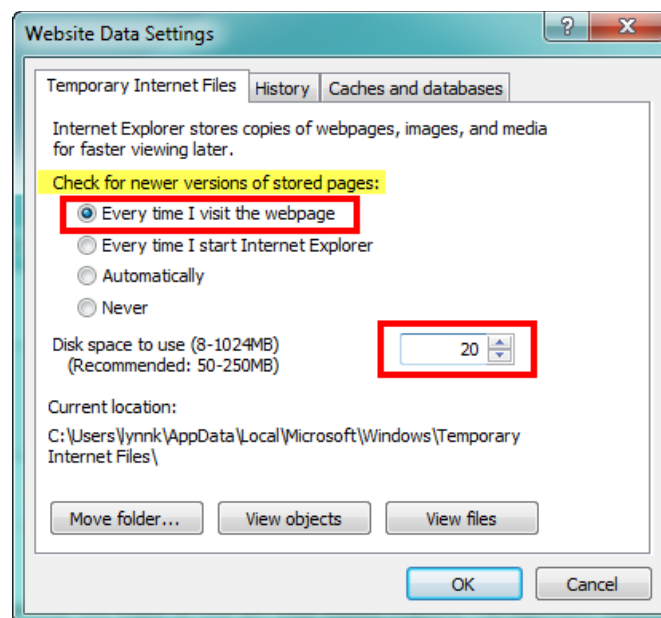


Caching (cont.)

In the **Browsing history** section, click **Settings**.

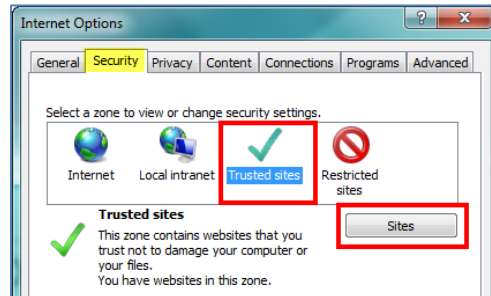


On the **Temporary Internet Files** tab, for the **Check for newer versions of stored pages** option, select **Every time I visit the webpage**. In the **Disk space to use** box, select **20** and click **OK**.



Security Settings

Select the **Security** tab. (If you just completed the *Caching* section, the **Internet Options** dialog box should still be open, otherwise perform Steps 1 and 2 under the *Caching* section and then select the **Security** tab.) Click **Trusted sites** and then click **Sites**.



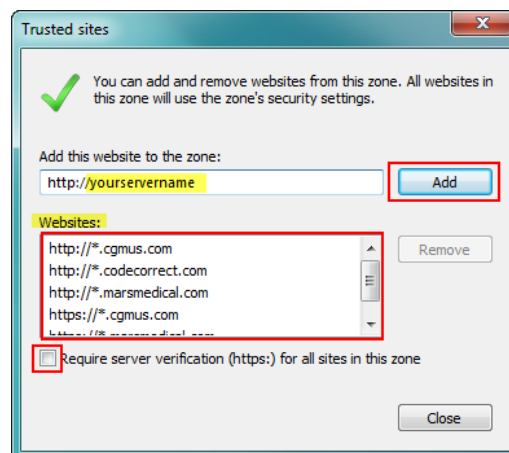
Trusted Sites Settings

In the **Add this website to the zone:** box, type: **http://YourServerName or address**. This URL will be provided by either CompuGroup Medical or your IT Department. Click **Add**.

Verify that the following sites are also set up as trusted sites.

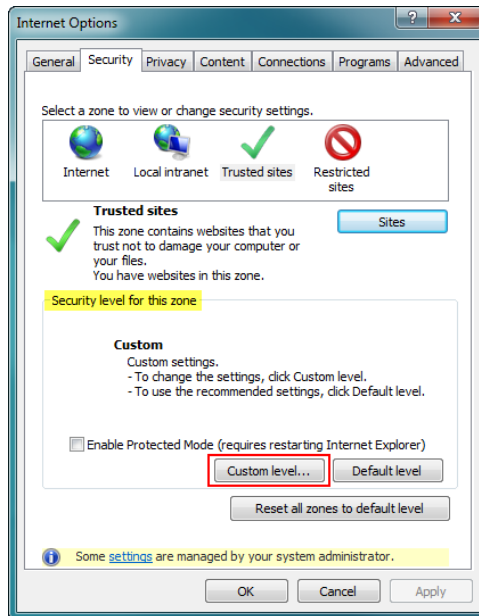
http://*.cgmus.com	
https://*.cgmus.com	
https://*.marsmedical.com	
http://*.codecorrect.com	(for webCoder)
http://*.noteworthymedical.com	(for ASP clients)
https://*.noteworthymedical.com	(for ASP clients)
https://*.mpaygateway.com	(for webPay)
https://*.payspan.com	(for webPay)

Clear the **Require server verification (https:) for all sites in this zone** check box and click **Close**.

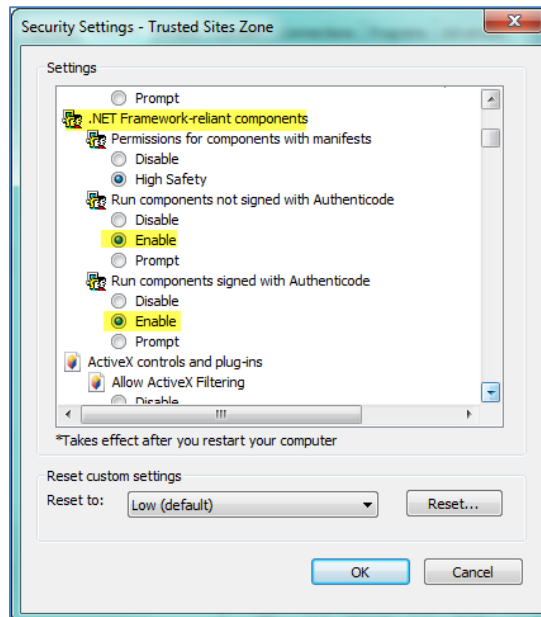


Security Settings (cont.)

In the **Security level for this zone** section, click **Custom Level**.



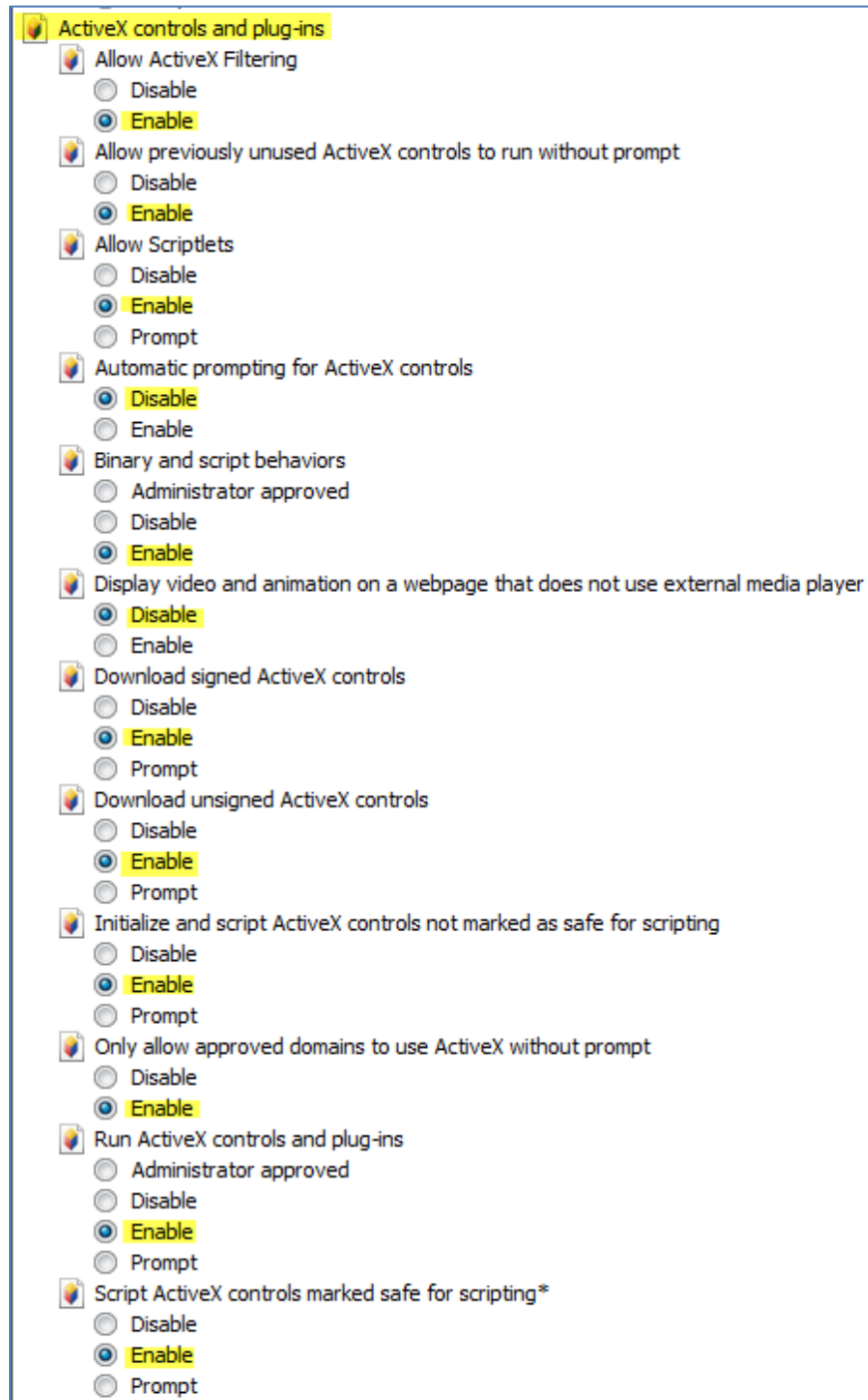
When the **Security Settings – Trusted Sites Zone** dialog box displays, scroll down to the **.NET Framework-reliant components** settings. Change the settings to match those shown in the image below.



Security Settings (cont.)

ActiveX Settings

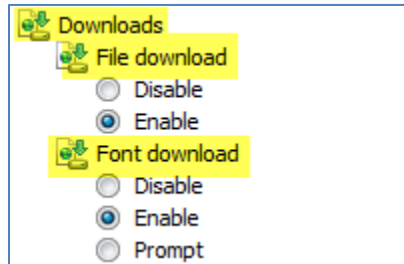
Scroll down to the **ActiveX controls and plug-ins** section. Change the settings to match those shown in the image below.



Security Settings (cont.)

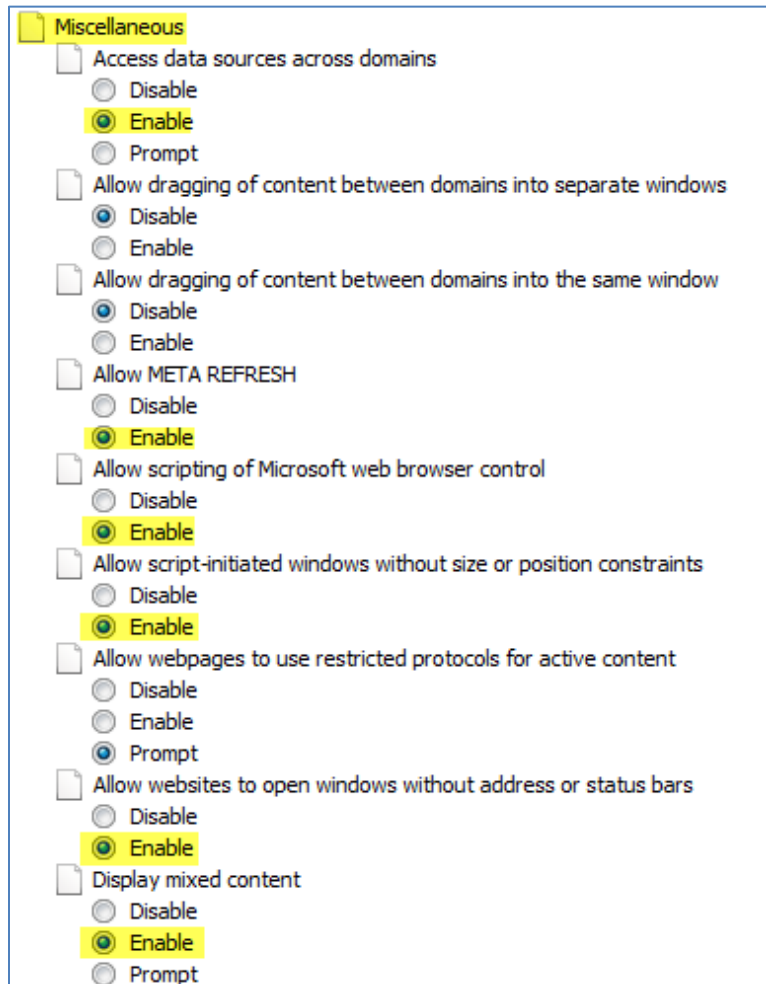
Downloads Settings

Scroll down to the **Downloads** section. Verify the following highlighted settings are set to **Enable**.



Miscellaneous Settings

Scroll down to the **Miscellaneous** settings. Change the settings to match those shown in the image below. If a setting option has not been highlighted it can be left at the default setting.



Security Settings (cont.)

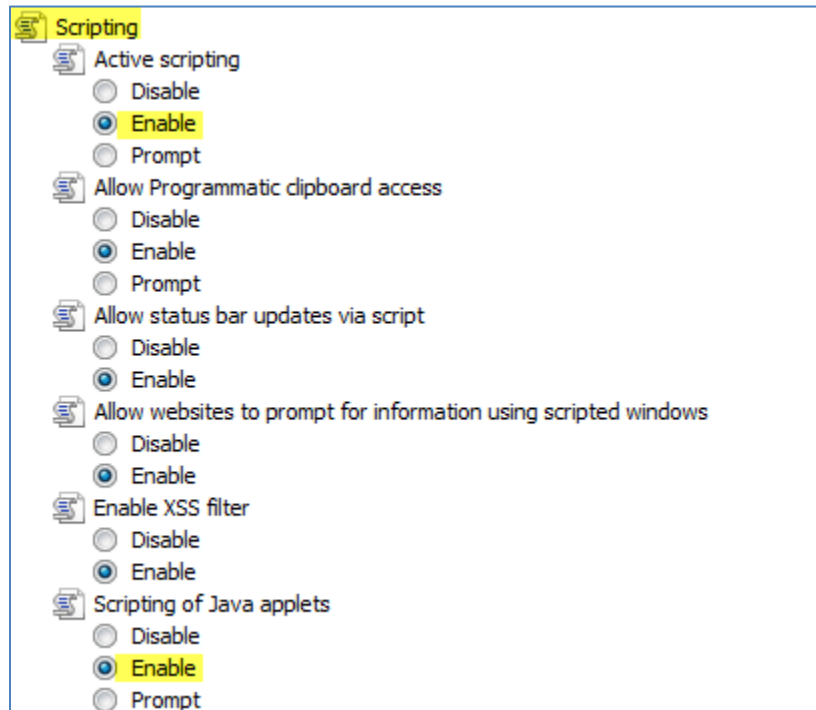
Miscellaneous Settings (cont.)

<input type="checkbox"/>	Don't prompt for client certificate selection when only one certificate exists
<input type="radio"/>	Disable
<input checked="" type="radio"/>	Enable
<input type="checkbox"/>	Drag and drop or copy and paste files
<input type="radio"/>	Disable
<input checked="" type="radio"/>	Enable
<input type="radio"/>	Prompt
<input type="checkbox"/>	Enable MIME Sniffing
<input type="radio"/>	Disable
<input checked="" type="radio"/>	Enable
<input type="checkbox"/>	Include local directory path when uploading files to a server
<input type="radio"/>	Disable
<input checked="" type="radio"/>	Enable
<input type="checkbox"/>	Launching applications and unsafe files
<input type="radio"/>	Disable
<input checked="" type="radio"/>	Enable
<input type="radio"/>	Prompt
<input type="checkbox"/>	Launching programs and files in an IFRAME
<input type="radio"/>	Disable
<input checked="" type="radio"/>	Enable
<input type="radio"/>	Prompt
<input type="checkbox"/>	Navigate windows and frames across different domains
<input type="radio"/>	Disable
<input checked="" type="radio"/>	Enable
<input type="radio"/>	Prompt
<input type="checkbox"/>	Render legacy filters
<input type="radio"/>	Disable
<input checked="" type="radio"/>	Enable
<input type="checkbox"/>	Submit non-encrypted form data
<input type="radio"/>	Disable
<input checked="" type="radio"/>	Enable
<input type="radio"/>	Prompt
<input type="checkbox"/>	Use Pop-up Blocker
<input checked="" type="radio"/>	Disable
<input type="radio"/>	Enable
<input type="checkbox"/>	Use SmartScreen Filter
<input type="radio"/>	Disable
<input checked="" type="radio"/>	Enable
<input type="checkbox"/>	Userdata persistence
<input type="radio"/>	Disable
<input checked="" type="radio"/>	Enable
<input type="checkbox"/>	Websites in less privileged web content zone can navigate into this zone
<input type="radio"/>	Disable
<input type="radio"/>	Enable
<input checked="" type="radio"/>	Prompt

Security Settings (cont.)

Scripting Settings

Scroll down to the **Scripting** settings. Change the settings to match those shown in the image below. If a setting option has not been highlighted it can be left at the default setting.



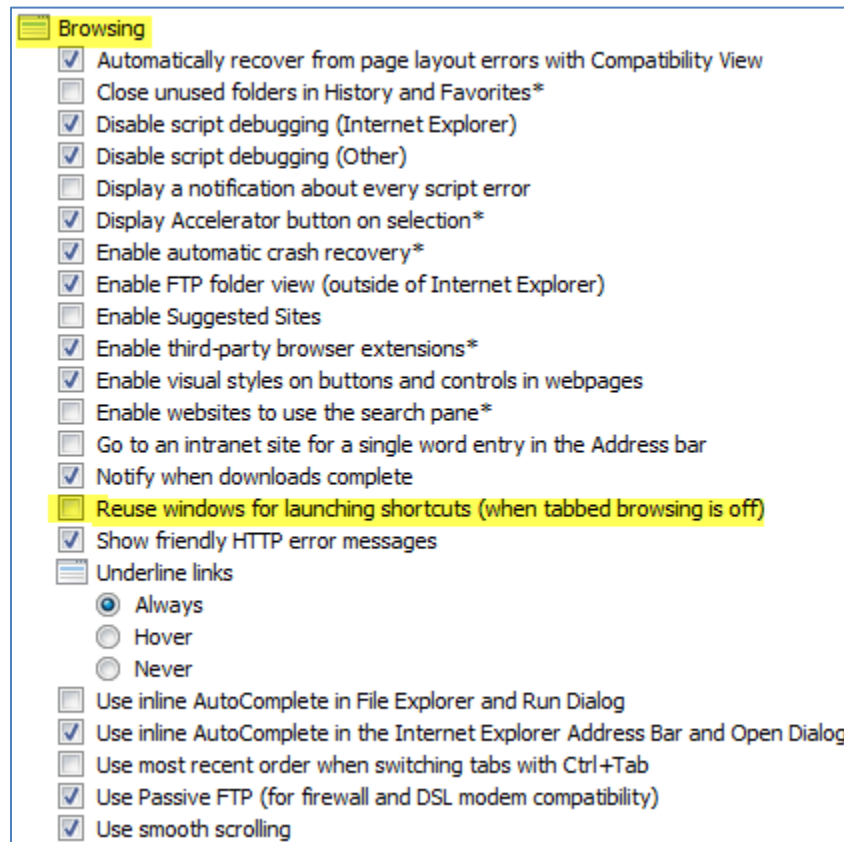
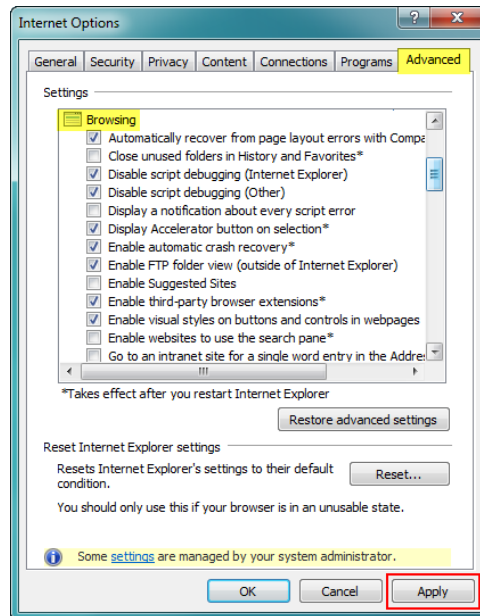
On the **Security Settings – Trusted Sites Zone** dialog box, click **OK**.

When you receive the warning message, “*Are you sure you want to change the settings for this zone?*” click **Yes**.

Note: These changes will not take effect until Internet Explorer has been restarted, which you will be instructed to do later in this document.

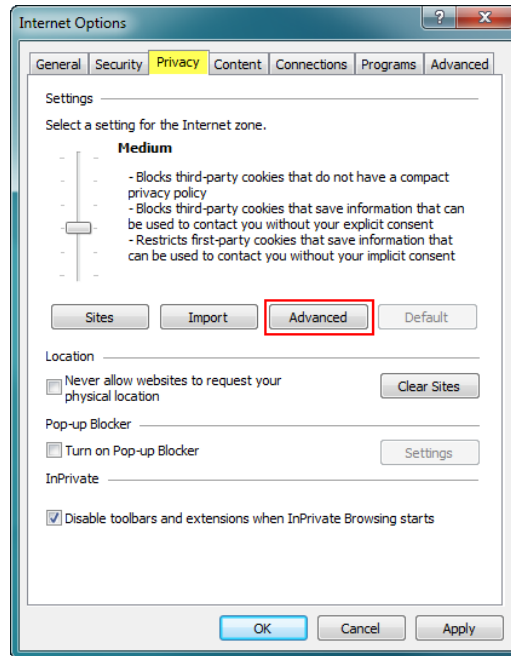
Advanced Settings

Select the **Advanced** tab. Scroll down to the **Browsing** section and clear the **Reuse windows for launching shortcuts** check box. Click **Apply**.

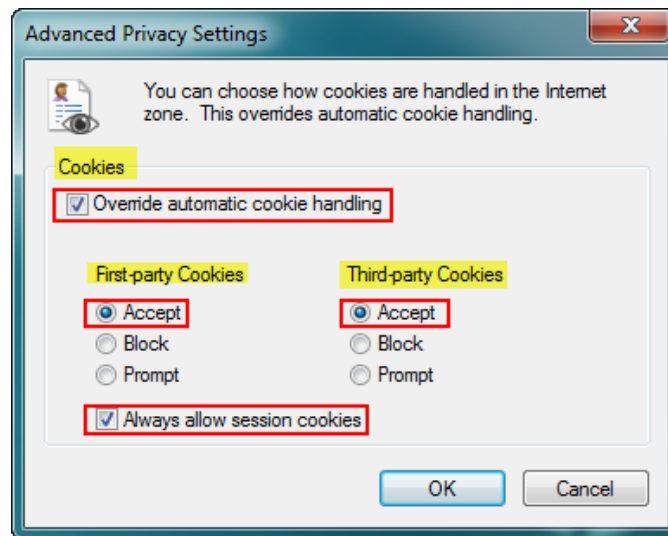


Privacy Settings

Select the **Privacy** tab. In the **Settings** section, click **Advanced**.



Select the **Override automatic cookie handling** check box.
For both the **First-party** and **Third-party Cookies**, select **Accept**.
Select the **Always allow session cookies** check box. Click **OK**.

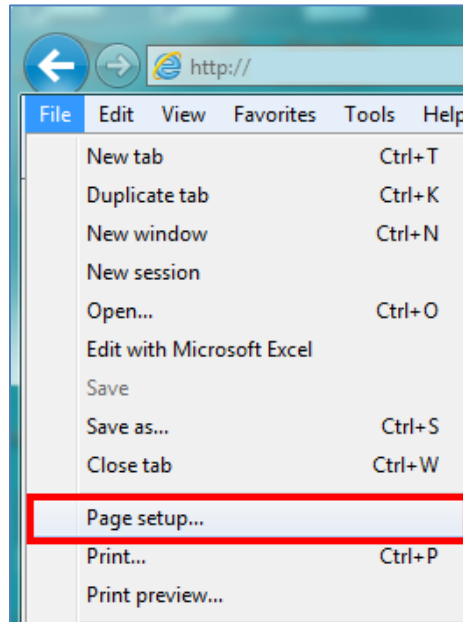


On the **Internet Options** dialog box, click **OK**.

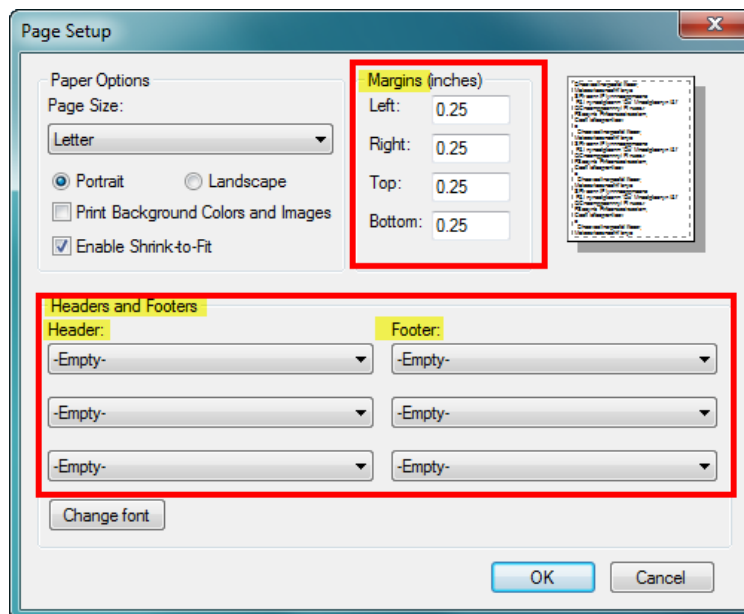
To make the changes effective, you will need to close IE by closing the **CGM webPractice** Homepage.

PRINTING SETTINGS

Open the **CGM webPractice** Homepage and click **File** in the **Menu bar** and then **Page Setup**.





In the **Margins** section, in the **Left, Right, Top, and Bottom** boxes, type **.25**.
For each of the **Header** and **Footer** list boxes, select **Empty** and then click **OK**.



ENABLE COMPATIBILITY VIEW

It is necessary to enable **Compatibility View** for IE version 10 to prevent display issues while working in CGM webPractice.

Step 1: If you just completed the *Printing Settings* section, the CGM webPractice launch page should still be open, otherwise Navigate to it.

Step 2: Click the Compatibility View icon  to enable it. It will turn blue when it becomes 'active' .



Step 3: Click **Launch webPRACTICE** and login as usual.

