

The Following Internet Settings apply to the Trusted Sites area only.

To properly configure the Security Settings in Internet Explorer 7, do the following:

- 1) In **Internet Explorer 7**, click on **Tools > Internet Options**
- 2) Click on the **Security** Tab
- 3) Click on the **Custom Level** Button
- 4) Enter the settings that are outlined below:
 1. .NET Framework
 - a. Loose XAML
 - i. Disable
 - ii. Enable**
 - iii. Prompt
 - b. XAML browser applications
 - i. Disable
 - ii. Enable**
 - iii. Prompt
 - c. XPS documents
 - i. Disable
 - ii. Enable**
 - iii. Prompt
 2. .NET Framework-related components
 - a. Run components not signed with Authenticode
 - i. Disable
 - ii. Enable**
 - iii. Prompt
 - b. Run components signed with Authenticode
 - i. Disable
 - ii. Enable**
 - iii. Prompt
 3. ActiveX controls and plug-ins
 - a. Allow previously unused ActiveX controls to run without prompt
 - i. Disable
 - ii. Enable**
 - b. Allow Scriptlets
 - i. Disable
 - ii. Enable**
 - iii. Prompt
 - c. Automatic Prompting for ActiveX controls
 - i. Disable**
 - ii. Enable
 - d. Binary and script behaviors
 - i. Administrator approved
 - ii. Disable
 - iii. Enable**
 - e. Display video and animation on a webpage.....
 - i. Disable

- iii. Prompt

- f. Allow websites to open windows without address...
 - i. Disable
 - ii. **Enable**
- g. Display mixed content
 - i. **Disable**
 - ii. Enable
 - iii. Prompt
- h. Don't prompt for client certificate selection when
 - i. Disable
 - ii. **Enable**

- i. Drag and drop or copy and paste files
 - i. Disable
 - ii. **Enable**
 - iii. Prompt
- j. Include local directory path when uploading files to a server...
 - i. Disable
 - ii. **Enable**
- k. Installation of desktop items
 - i. Disable
 - ii. Enable
 - iii. **Prompt**
- l. Launching applications and unsafe files
 - i. Disable
 - ii. **Enable**
 - iii. Prompt
- m. Launching programs and files in an IFRAME
 - i. **Disable**
 - ii. Enable
 - iii. Prompt
- n. Navigate sub-frames across different domains
 - i. **Disable**
 - ii. Enable
 - iii. Prompt
- o. Open files based on content, not file extension
 - i. Disable
 - ii. **Enable**
- p. Software channel permissions
 - i. High safety
 - ii. **Low safety**
 - iii. Medium safety
- q. Submit non-encrypted form data
 - i. Disable
 - ii. **Enable**
 - iii. Prompt
- r. Use Phishing Filter
 - i. **Disable**
 - ii. Enable
 - iii. Prompt
- s. Use Pop-Up blocker
 - i. **Disable**
 - ii. Enable
 - iii. Prompt
- t. Userdata persistence
 - i. Disable

