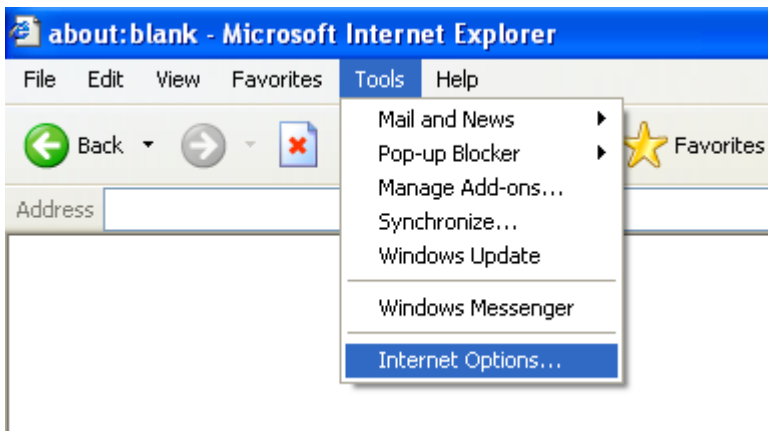




## How to Secure the Microsoft Internet Explorer Web Browser

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

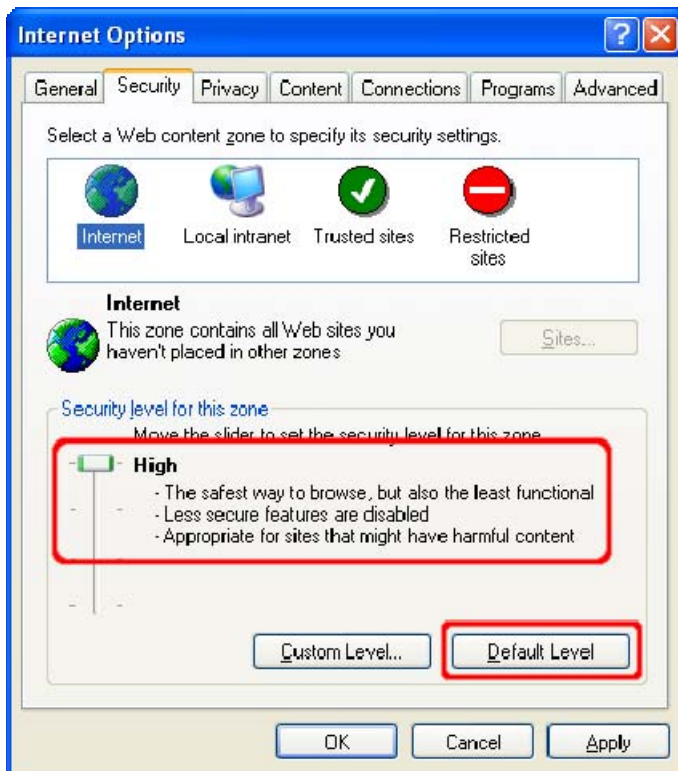
In order to change settings for Internet Explorer, select **Tools** then **Internet Options...**



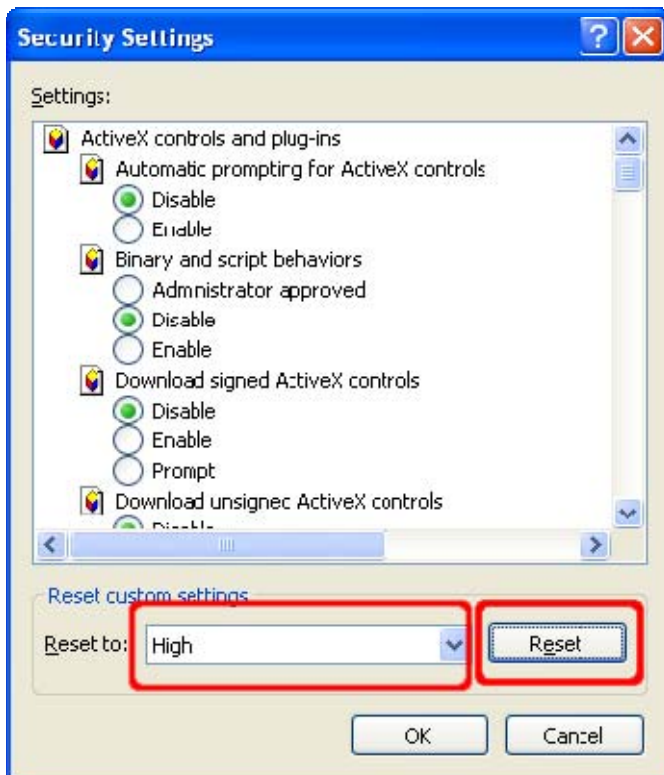
Select the **Security** tab. On this tab you will find a section at the top, which lists the various security zones that Internet Explorer uses.

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.

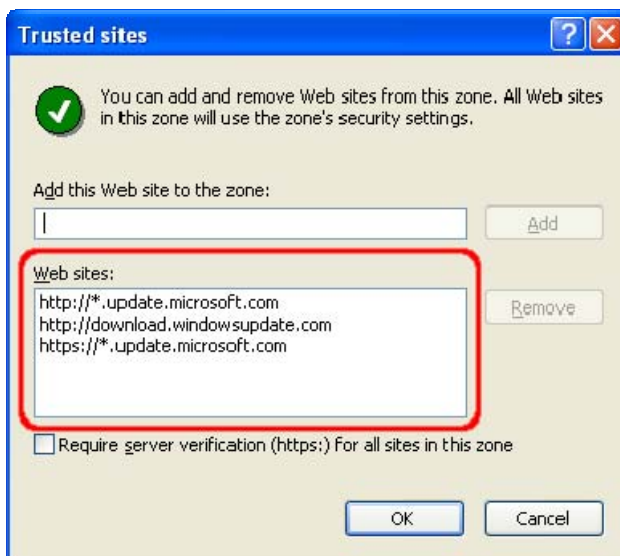
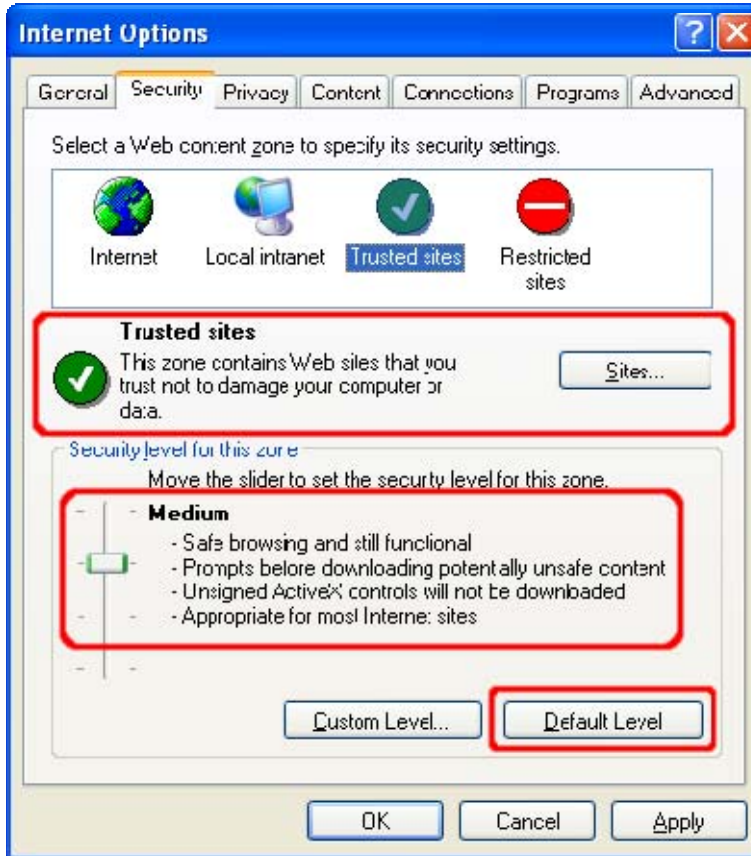
We recommend the **High** security setting be applied for this zone. By selecting the High security setting, several features including ActiveX, Active scripting, and Java will be disabled. With these features disabled, the browser will be more secure. Click the **Default Level** button and then drag the slider control up to **High**.



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. Default values for the High security setting can be selected by choosing **High** and clicking the **Reset** button to apply the changes.

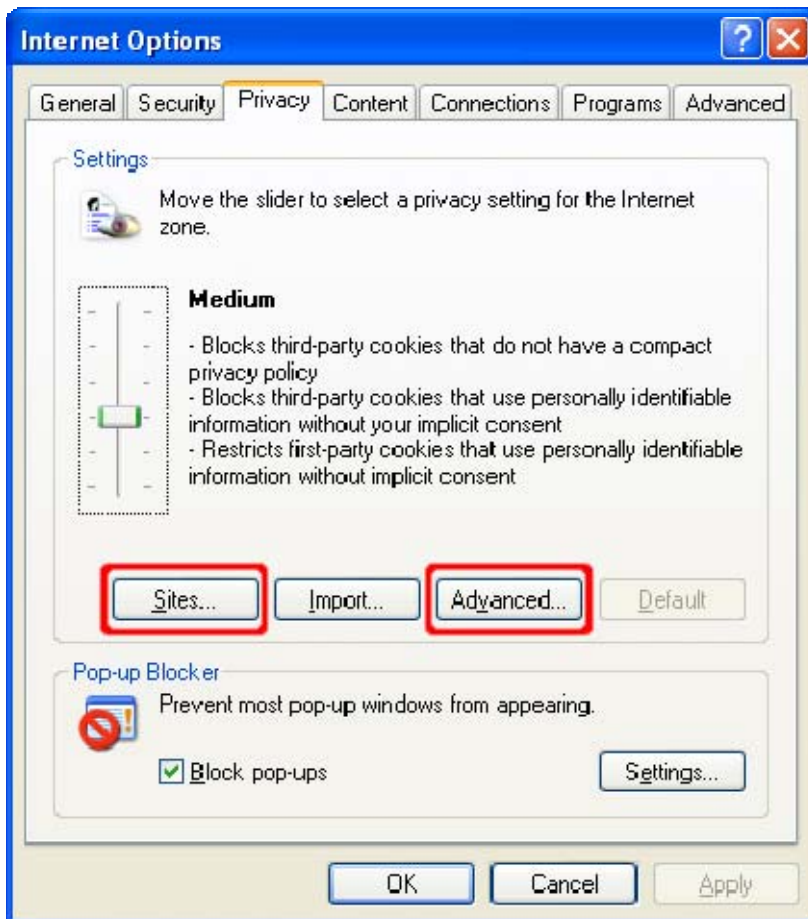


**Trusted sites** is a security zone for web sites that you believe are securely designed and contain trustworthy content. To add or remove sites from this zone, you can click the **Sites...** button. This will open a new window that will list the sites that you trust and permit you to add or remove sites. You may also require that only sites with Secure Sockets Layer (SSL) implemented can be active in this zone. This permits you to verify that the site you are visiting is the site that it claims to be.



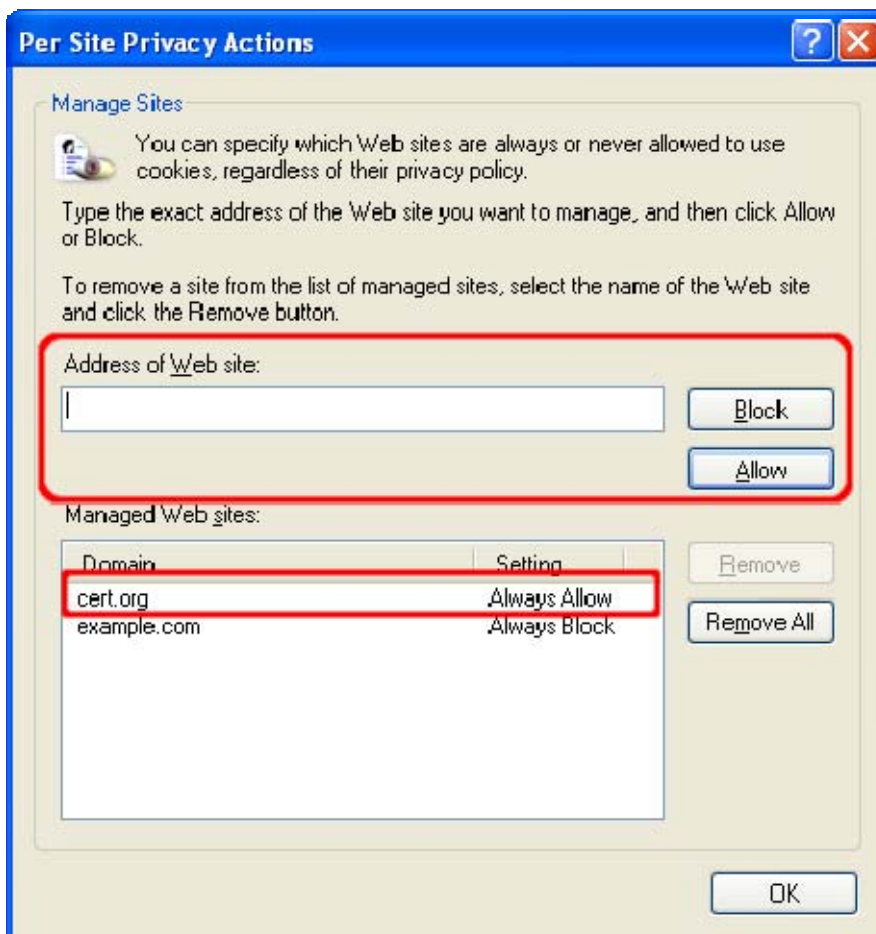
We recommend setting the security level for the **Trusted sites** zone to **Medium**. When the Internet Zone is set to **High**, you may encounter web sites that do not function properly due to one or more of the associated security settings. This is where the **Trusted sites** zone can help. If you trust that the site will not contain malicious code, 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. 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 computer. You can then evaluate the originating site, whether you wish to accept or deny the cookie, and what action to take in the future (always accept, always block, or continue to ask).

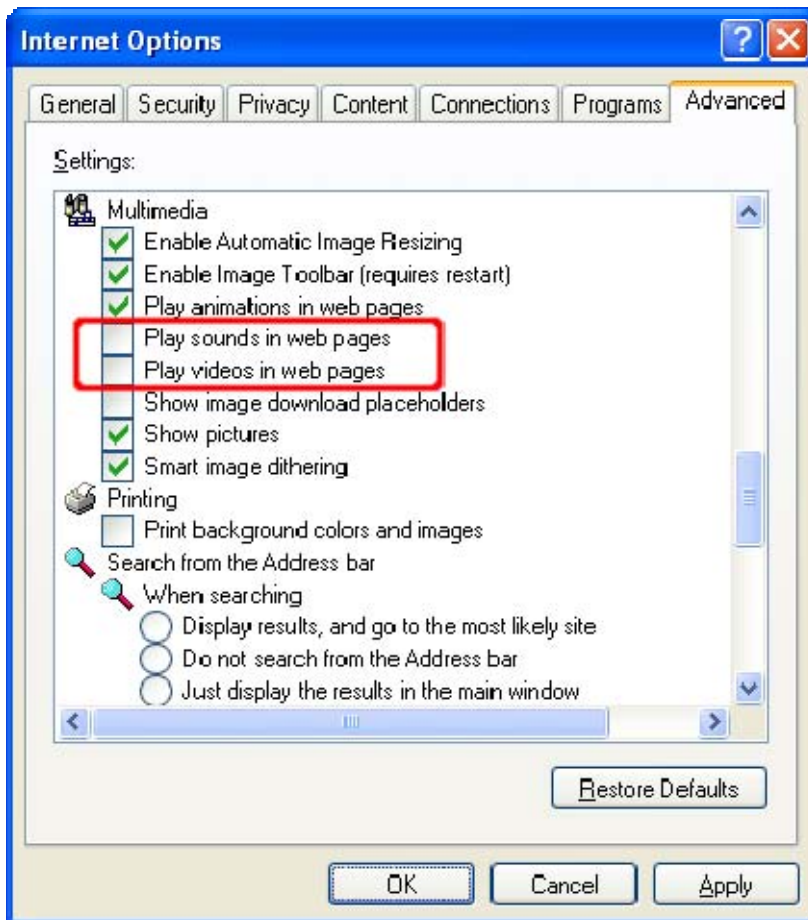




By selecting the **Sites...** button, you can manage the cookie settings for specific sites. You can add or remove sites, and you can change the current settings for existing sites. The bottom section of this window will specify the domain of the site and the action to take when that site wants to place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



The **Advanced** tab contains settings used by all zones. The settings contained in the **Multimedia** section have features that you can adjust to protect against some potential vulnerabilities. For instance, attackers may be able to track your usage or exploit the software you use to play multimedia data. We recommend disabling the options to play sounds and videos:



Under the **Programs** tab, you can specify your default applications for viewing web sites, email messages, and other network related tasks. You can also prevent Internet Explorer from showing you a message asking to be your default web browser.

