Access session security in IE 8

Internet Explorer 8 integrates many new security features that make the browser process much more secure than previous versions.

***Network* Explorer - Internet Explorer 8 integrates many new security features that make the browser process much more secure than previous versions. These new features are quite efficient and flexible so they can be used in a number of different environments.**

In this article we will explore these new features of Internet Explorer 8 and how to configure them for use in different situations.

Discover Privacy of Internet Explorer

Before understanding the private browser method, we need to know how Internet Explorer stores information about users' browser sessions.

First and foremost, if you are interested in the number of traces that can be left on a computer after accessing the Internet with the default configuration of Internet Explorer. It's best to care about this information. Certain users with a habit of accessing browser history, cookies, and data sessions will know what sites you have visited and what actions to take on them. Worse, hackers can use that information to steal passwords, take over the browsing session and get all your personal information.

Here are some locations where such data types are usually stored when users access the Internet:

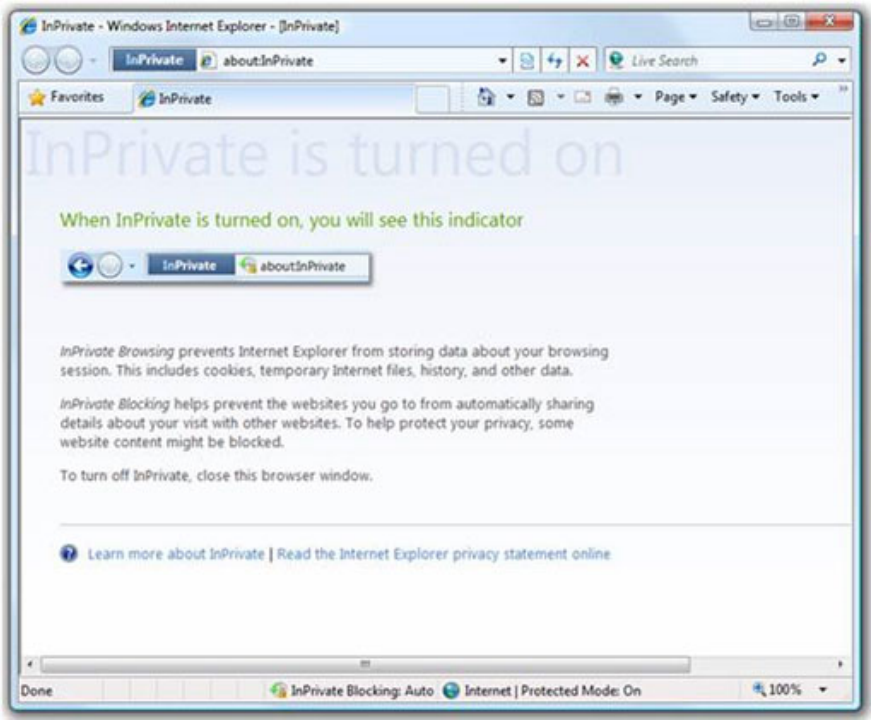
1. **Folder Temp of Internet Explorer** (also known as Cache). This folder is in the ***C: Users path AppDataLocalMicrosoftWindowsTemporary Internet Files*** .
2. **IE Cookies** . There is path ***C: UsersAppDataRoamingMicrosoftWindowsCookies*** .
3. **IE History** . History is in the path ***C: UsersAppDataLocalMicrosoftWindowsHistory*** .
4. **IE Typed URL** (only accessible disks). These addresses are stored in the ***HKEY_CURRENT_USERSoftwareMicrosoftInternet ExplorerTypedUrls*** key.
5. **IE Forms AutoComplete** (stored information after entering data into the form on the website). This information is stored in the ***HKEY_CURRENT_USERSoftwareMicrosoftInternet ExplorerIntelliFormsStorage1*** key.
6. **IE Password AutoComplete** (save passwords used on websites). These passwords are stored in ***HKEY_CURRENT_USERSoftwareMicrosoftInternet ExplorerIntelliFormsStorage2*** .

Of course, users can delete all of this information by going to the **Tools** menu, selecting **Internet Options** and pressing the **Delete** button. However, allowing Internet Explorer to store this information immediately after access is a bit annoying and we cannot often prompt users to remove this information for security reasons.

InPrivate Browsing

Normally when accessing the Internet we never think of another user who can easily access all personal information through Cookies and browser session information. That's why Microsoft integrated InPrivate Browsing for Internet Explorer 8. If you use a public computer and you don't want people to know what you've accessed, you just need to launch InPrivate Browsing.

InPrivate Browsing is easy to use. To access it, simply press the **[Ctrl + Shift + P]** key combination after opening **Internet Explorer 8** , then you will see the **InPrivate** browser window appear.



In this mode the following types of information will not be stored:

1. **Cookies** .
2. **History** .
3. **Temporary Internet** files will be deleted after closing the InPrivate browser window.
4. Data **form** .
5. **Password**
6. The **URL** has been accessed.
7. **Search queries** .
8. The **links** have been accessed.

When using this mode all information about your browser session will not be stored, and of course you will not have to perform a difficult operation to go to Internet Options to delete them after the end of the browser session.

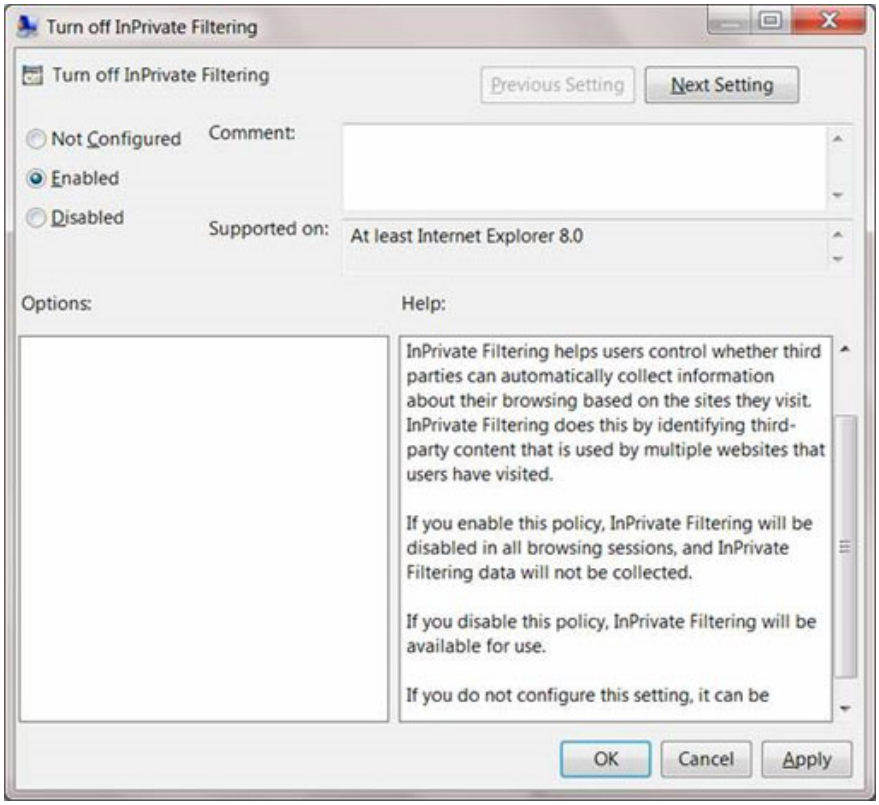
Block InPrivate Browsing using Group Policy

InPrivate Browsing is very effective in ensuring the security of the system, but it is not really effective in managing employees. Since there is no information about the login session stored, you cannot have proof that the employee has neglected the job. This is why Microsoft has integrated an additional administration tool to control InPrivate Browsing using Group Policy.

In this case we need to turn off InPrivate Browsing mode. To turn off this mode, we must first create a new **Group Policy Object** . In this new **Group Policy Object** , browse to **Computer Configuration | Administrative Templates | Windows Components | Internet Explorer | InPrivate** .

There are a number of options you can choose from here, but our goal is to disable InPrivate Browsing mode so

we only pay attention to the option **Turn off InPrivate Browsing** . The setting for this option is **Enabled** and then applies it to specific users or groups so that they cannot use InPrivate Browsing to delete any browser traces.



InPrivate Filtering

Along with InPrivate Browsing, Microsoft has also introduced InPrivate Filtering, which provides information about 3rd party applications that want to use the user's browser information.

Have you ever encountered the case after buying an item online, you visited another website and the banner ads on that page displayed the same type of product you searched for earlier? This is a good example of how websites use user tracking code without using cookies.

As another example, suppose you browse to the website with the address *www.fakewebsitegoeshere.com* . This website contains the following code: