

Internet Explorer 8  
Privacy and User Control

**RC1 Feature Guide**

Published January 2009

Abstract

This paper provides an overview of key privacy-related enhancements in Windows® Internet Explorer® 8, including its enhanced Delete Browsing History, InPrivate™ Browsing, and InPrivate Filtering features. This information is intended to help content publishers; content providers and businesses better understand how these features work and how to configure them for end users. This paper also explores how content providers and advertisers can optimize the content delivery for InPrivate Filtering, including guidance on how to create user information pages that can help users understand the value of—and make informed decisions regarding—the value exchange of user data for advertising-supported content.

The information contained in this document represents the current view of Microsoft Corp. on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This guide is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form, by any means (electronic, mechanical, photocopying, recording or otherwise), or for any purpose, without the express written permission of Microsoft.

Microsoft may have patents, patent applications, trademarks, copyrights or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, e-mail address, logo, person, place or event is intended or should be inferred.

Microsoft, Active Directory, ActiveX, Internet Explorer, the Internet Explorer logo, InPrivate, MSDN, SmartScreen, Windows, Windows Live, and Windows Vista are either registered trademarks or trademarks of Microsoft Corp. in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

© 2009 Microsoft Corp. All rights reserved.

Contents

Introduction 1

Internet Explorer 8 and User Privacy 3

Enhanced Delete Browsing History 4

InPrivate Browsing 6

InPrivate Filtering 9

Status Indicator 10

Enabling InPrivate Filtering 10

InPrivate Filtering Settings 12

Additional Information on Third-Party Content 13

Considerations for Content Providers 14

Creating a Third-Party Information Page 14

InPrivate Filtering Session Status 15

First-Party versus Third-Party Considerations 15

Conclusion 18

For More Information 18

Appendix A: InPrivate Browsing - Data Handling 19

Appendix B: Group Policy Settings and Scenarios 20

Individual Group Policy Settings 20

Common Group Policy Scenarios 22

# Introduction

Browsing the Web is the single most popular activity on the PC, with both the time people spend on the Web and the range of things they can do on it continuing to grow. The Web is transforming how we learn, communicate, work, search and shop, with consumers benefiting from its wealth of content and services more than ever. Those increases are matched by the rate of change on the Web itself, which has transitioned from a collection of primarily static Web pages to a network of interconnected sites and services.

However, as the complexity of the Web continues to increase, so does the number of ways that Web sites can potentially monitor peoples’ online behavior. Consumers are increasingly concerned about their privacy and risks of identity theft, having others find their personal information on shared computers, and knowing where their information is going and how it is used.

For the Web to realize its full potential, people need to be able to trust that their personal information is being used appropriately—in a way that they understand and have agreed to, and that provides specific value to them. The Web browser must be a tool that people can depend on to be fast and resilient, work as expected, and help safeguard their Web browsing and protect their privacy. All of these needs are elements of Microsoft’s framework for Trustworthy Browsing, in which the company is committed to delivering a Web browser that is highly reliable, provides strong security, respects user choice, and helps users retain control over both their PCs and their personal information.

In discussing online privacy, many people immediately think of cookies. However, cookies are only one way that users can disclose information to Web sites. Some people consider the Phishing Filter in Internet Explorer® 7 and the new SmartScreen® Filter in Internet Explorer 8 to be privacy features because they help protect users from unknowingly sharing information, collectively blocking more than 1 million weekly attempts to visit known phishing sites. Similarly, the ability for a user to delete his or her Web browsing history on a shared computer is often considered a means of protecting privacy. This broader view of privacy is the approach taken by Microsoft, with the goal of helping to put users in control of the information and Web browsing history on their computer, making users aware of the third party content providers to whom they’re disclosing information with and, if the user chooses to do so, enabling or disabling disclosing such information.

Privacy is a complex topic that can create conflict —namely, between users who want to protect their privacy and Web sites that want to know as much as possible about the user, for reasons that can range from content personalization to monetization of Web traffic through targeted advertising. Although some people may understand the Web sites they visit have the ability to track their activities, consumers are often not fully aware of the *degree* to which their Web browsing activities can be tracked, especially by third parties who provide content to the Web sites they choose to visit. Providing users with greater control over their data and privacy while making the value exchange (of Web content for user data) more transparent are key goals for Internet Explorer 8.

Microsoft also believes that users should have an understanding of the valuable role that advertising plays in the delivery of “free content” on the Web. It is the revenue derived from these “free” services that pays for much of the rich content that users have come to expect when browsing the Web. At the same time this value exchange can only be maximized when users have trust and confidence in the Web sites they visit. Users have been clear that they equate online trust to freedom from intrusion, protection from harm, and choice and control over how (and by whom) their personal information and browsing history is accessed and used.

The remainder of this paper discusses key privacy-related features in Internet Explorer 8 in greater detail, including how they map to the above principles.

# Internet Explorer 8 and User Privacy

Delivering a Web browser that helps protect user privacy has been a focus for Microsoft for several years. Internet Explorer 6, released in 2001, implemented the World Wide Web Consortium (W3C) Privacy Preferences Project (P3P) standard to block cookies from Web sites without privacy policies that comply with user settings. Internet Explorer 7 built on these investments, introducing the first integrated browser-based phishing filter while also making it easier to delete cookies and other information that can indicate where the user has been on the Web.

User safety, choice, and control also were key themes in the development of Internet Explorer 8, which includes many innovations that contribute to a more trustworthy Web browsing experience. For example, the SmartScreen Filter helps protect against a range of exploits and emerging threats including known phishing and malware sites. In addition, the SmartScreen Filter includes the new Cross-Site Scripting Filter (XSS), which helps to prevent against type-1 cross-site scripting attacks as well as clickjacking exploits, which can be used to capture keystrokes, steal user credentials, deface Web pages, or launch more exotic attacks. Internet Explorer 8 also highlights the domain name in the URL string in the Address Bar in black text, making it easier for users to identify deceptive sites.

Three important privacy-specific features in Internet Explorer 8 include:

* An **enhanced Delete Browsing History** option that enables users to retain cookies and temporary Internet files for their favorite Web sites when deleting their browsing history, so that those favorite sites can continue to retain user preferences providing users increased browsing productivity.
* **InPrivate™ Browsing,** which helps prevent users’ browsing history, temporary Internet files, form data, cookies, and usernames/passwords from being stored or retained locally by the browser.
* **InPrivate Filtering,** which provides greater user choice and control over the third-parties from which content is retrieved and displayed on Web sites that the user visits—and thus how those same third parties can potentially track and aggregate users’ Web browsing activities.

Each of these features is discussed in greater detail in the following sections of this document. This is done from both the end user perspective and from the perspectives of other stakeholders, such as content and advertising syndicators, who may want to know how InPrivate Filtering may impact their businesses and the steps they can take to help maximize the value exchange with consumers.

# Enhanced Delete Browsing History

Have you ever deleted your browsing history, only to find that your favorite Web sites no longer remember who you are? Internet Explorer 7 has a robust Delete Browsing History option that enables users to delete their browsing history retained by Internet Explorer, or to selectively delete temporary Internet files, cookies, history, form data and passwords. However, it doesn’t provide an easy way to delete information for certain sites while preserving it for other sites, such as frequently visited Web sites for which users likely want their personal preferences and temporary Internet files to be retained.

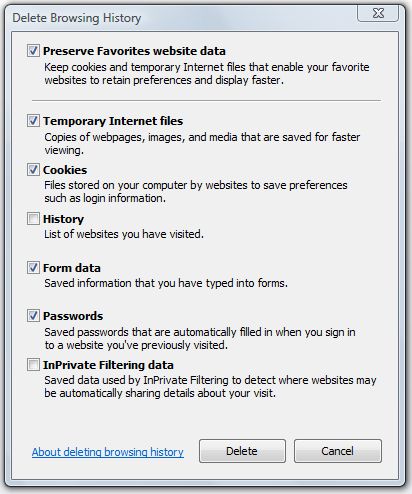
The enhanced Delete Browsing History feature in Internet Explorer 8 (see Figure 1) enables users to do just that. They can choose to preserve cookies and temporary Internet files for sites in their Favorites, thereby enabling those Web sites to retain user preferences and display faster. This added functionality helps users protect their information while ensuring the personalization and performance of their trusted sites they have added to their Favorites.

Figure 1

The ability for a user to delete their browsing was introduced in Internet Explorer 7, but until now several third party add-ons and applications haven’t had a way to take advantage of this user control. New in Internet Explorer 8, we’ve added APIs for Internet Explorer add-ons that allow them to participate in Delete Browsing History and InPrivate Browsing, allowing users added control of their browsing information. For details please refer to MSDN®.

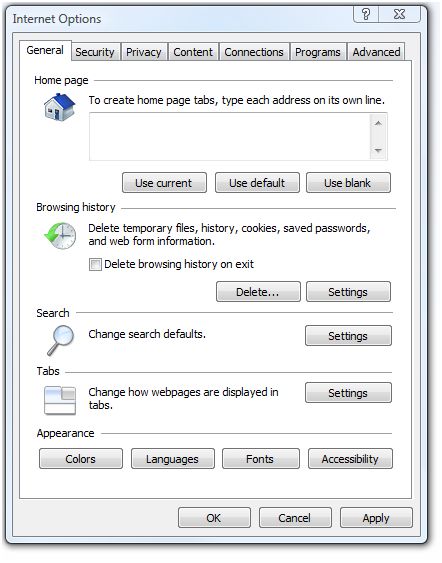
Users can also configure Internet Explorer to delete their browsing history automatically after each Web browsing session is closed. To enable this function, on the **Tools** menu, select **Internet Options.** On the **General** tab, under **Browsing History**, select **Delete Browsing History on Exit**. (See Figure 2.)

Figure 2

# InPrivate Browsing

There are times when users may not want to leave any traces of their Web browsing actions on the computers they are using, such as when researching health information during their lunch break at work, checking e-mail on a friend’s computer, or shopping for a gift on a family PC. InPrivate Browsing in Internet Explorer 8 helps protect user data and privacy by preventing the user’s browsing history, temporary Internet files, form data, cookies and usernames/passwords from being stored or retained locally by the browser, leaving virtually no evidence of the user’s browsing or search history. (See Appendix A for more detail on how InPrivate Browsing handles user data.)

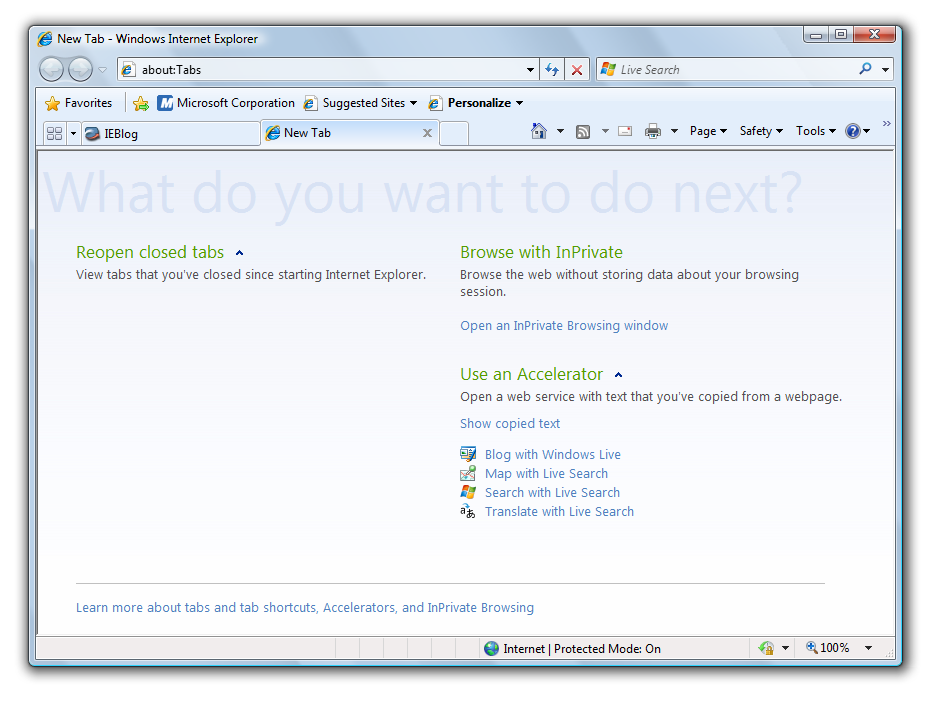
Users can initiate InPrivate Browsing by selecting Start InPrivate Browsing from the New Tab page in Internet Explorer 8 (see Figure 3), from its new Safety menu (see Figure 4), or from a command line. During an InPrivate session, an indicator is displayed to the left of the Address Bar (see Figure 5). The user ends an InPrivate session by simply closing the browser window. Users who want to always browse InPrivate can select “Delete browsing history on exit,” as discussed under Enhanced Delete Browsing History.

Figure 3

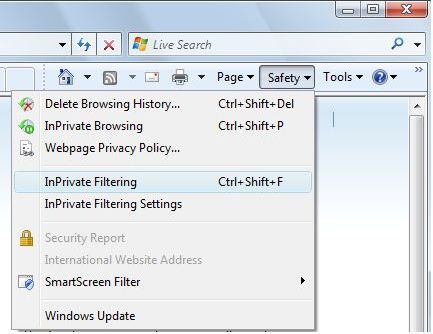


Figure 4

Figure 5

To provide increased privacy protection, Internet Explorer does not send existing persistent cookies to websites. If a website requests to set a persistent cookie, it will honor the request, but set the cookie as a session cookie. When in an InPrivate Browsing session only those cookies set during the session will be sent to a web site.

During an InPrivate Browsing session, files that the user downloads and Web sites added to the user’s Favorites *are* preserved. Also, it is important to note InPrivate Browsing does not limit data from being collected by a router, Internet Service Provider (ISP), wireless hotspot operators, or spyware unknowingly installed on a user’s computer. Network administrators can disable InPrivate Browsing through Group Policy, and parents can disable it using Parental Controls in Windows Vista®, or Windows Live™ Family Safety on Windows® XP.

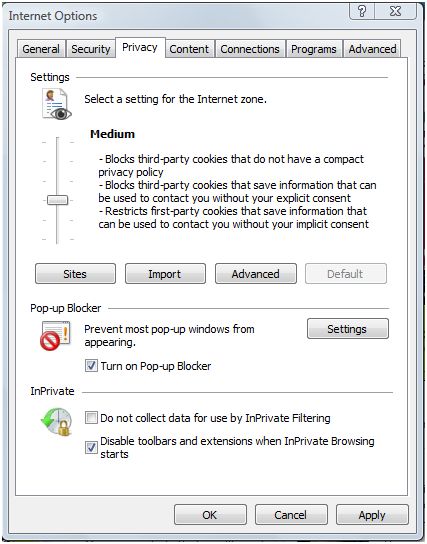
For added privacy control, by default, Internet Explorer 8 also disables toolbars and extensions when an InPrivate session is initiated. This setting can also be adjusted, as shown in Figure 6.

Figure 6

# InPrivate Filtering

Although some people understand that the Web sites they visit can track their activities, and in return the sites provide valuable content, consumers are often not fully aware of the degree to which their Web browsing activities can be tracked *by Web sites or content providers other than those they have consciously chosen to visit.* This is because most Web sites today are mosaics of content from several different sites. When the user visits an intended “first-party” site, the Web page often includes links to content on other, “third-party” sites, which, depending on the user’s browser settings, the browser may also retrieve and display—sometimes with little or no indication to the user.

This behavior is part of the underlying design of the Web and enables tremendous benefits, including a business model for the funding of content on the Web and the ability to optimize content for users. It also enables smaller Web site operators to deliver more content, and, in the case of serving advertisements, can provide revenue streams that enable Web sites to avoid charging for access.

At the same time, bringing together information in this way has important privacy implications because every piece of content that a browser requests from a Web site can disclose information such as the user’s operating system, screen resolution, and IP address to that content provider —even in cases where the user has blocked all cookies. Taken one site at a time, the information disclosed may seem trivial. However, when the user visits multiple first-party sites that use content from the same third party, that third party can potentially aggregate the data it collects to build a profile of the user based on his or her Web surfing activity—again, frequently without notifying the user.

There are security risks inherent to this model as well, in that visiting one Web site exposes the user to potentially malicious content not just from the first-party site, but also from every third-party site or content provider that is referenced. The user visits one site and sees content on it that seems trustworthy—after all, it’s on a site the user trusts—but actually comes from a different source. Third-party Web servers can also be compromised with malicious content, without knowledge of the primary Web site operator. Links served by such compromised sites can direct users to other, more malicious sites, potentially putting the user’s safety and privacy at risk.

InPrivate Filtering in Internet Explorer 8 helps alleviate these issues by providing users with greater choice and control over which third-parties can potentially track and aggregate their Web browsing activities. It works by observing the Web sites a user visits and building a table of the unique calls for third-party content or objects that are observed for each unique domain. When InPrivate Filtering is active, third-party content is blocked based on the default threshold of 10 unique such observances. (Repeated visits to the same first-party domain do not increment this count.)

For example, if Internet Explorer observes that 10 or more unique first-party domains that the user visits over time load the same resource from “Domain X” (such as an image, 1x1 tracking pixel, style sheet, or JavaScript code), InPrivate Filtering will block all requests for that resource across all Web sites the user visits while the feature is enabled.

## Status Indicator

ipf-status bar.JPGAn indicator in the status bar at the bottom of the Internet Explorer 8 window (see Figure 7) shows the status of InPrivate Filtering: On or Off.

Figure 7

## Enabling InPrivate Filtering

InPrivate Filtering is off by default and must be enabled on a per-session basis. Users can enable InPrivate Filtering:

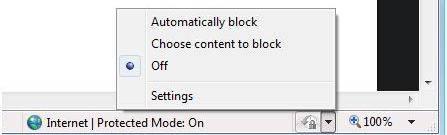
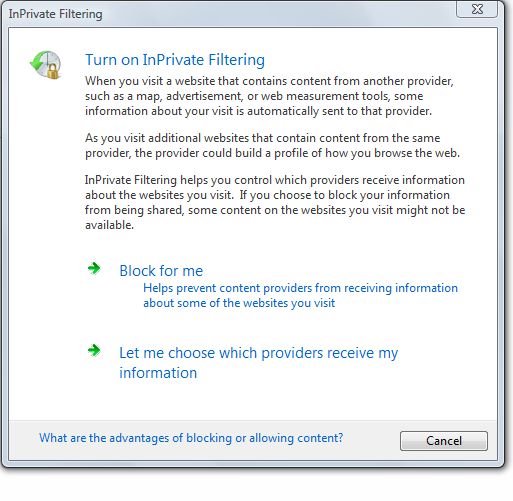
* By selecting **InPrivate Filtering** from the **Safety** menu.
* In the **InPrivate Filtering Settings** window, which can be accessed from the **Safety** menu or by clicking on the **InPrivate Filtering Status icon** in the Internet Explorer 8 status bar (see Figure 8).
* Using the **CTRL+Shift+B** keyboard shortcut

Figure 8

The first time a user enables InPrivate Filtering, he or she is prompted to select automatic (“Block for me”) or manual (“Let me choose”), as shown in Figure 9. This setting is retained for future InPrivate Filtering sessions. When InPrivate Filtering is active, the same settings apply to additional Web browser instances that are started—including InPrivate Browsing sessions—until the last Web browser window is closed, upon which InPrivate Filtering reverts to OFF.



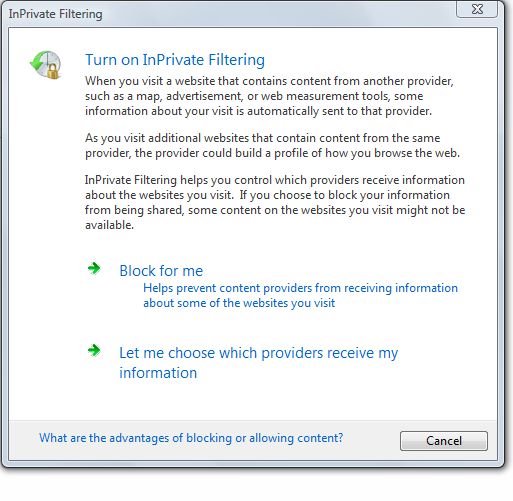


Figure 9

## InPrivate Filtering Settings

Users can review or modify InPrivate Filtering settings by selecting **InPrivate Filtering** **Settings** from the Internet Explorer 8 **Safety** menu or by clicking on the **InPrivate Filtering indicator** in the status bar and selecting **InPrivate Filtering Settings**.

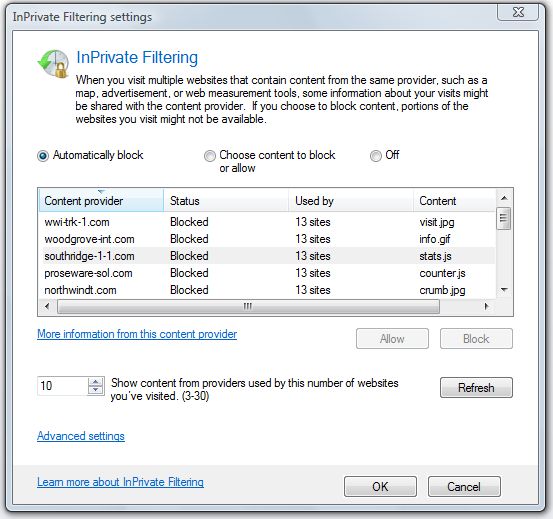
Within the InPrivate Filtering Settings window (see Figure 10), users can choose to automatically block content from third-party sites, manually allow or block content, or turn InPrivate Filtering off. Users also can adjust the “threshold” for InPrivate Filtering from its default of 10 to any number between 3 and 30. (To change the threshold, adjust the number, select **Refresh** to see which items in the displayed list are at or exceed that threshold, and click **OK** to apply the new threshold.)

Figure 10

Using the Internet Explorer 8 Manage Add-ons feature (see Figure 11), users can review the third-party content they have manually blocked or allowed. In addition, users can import and export lists that they or others create, such as those created by their IT departments. Not unlike saving favorites for use on multiple personal computers or a corporate deployment, such lists or “rules” provide added user control.

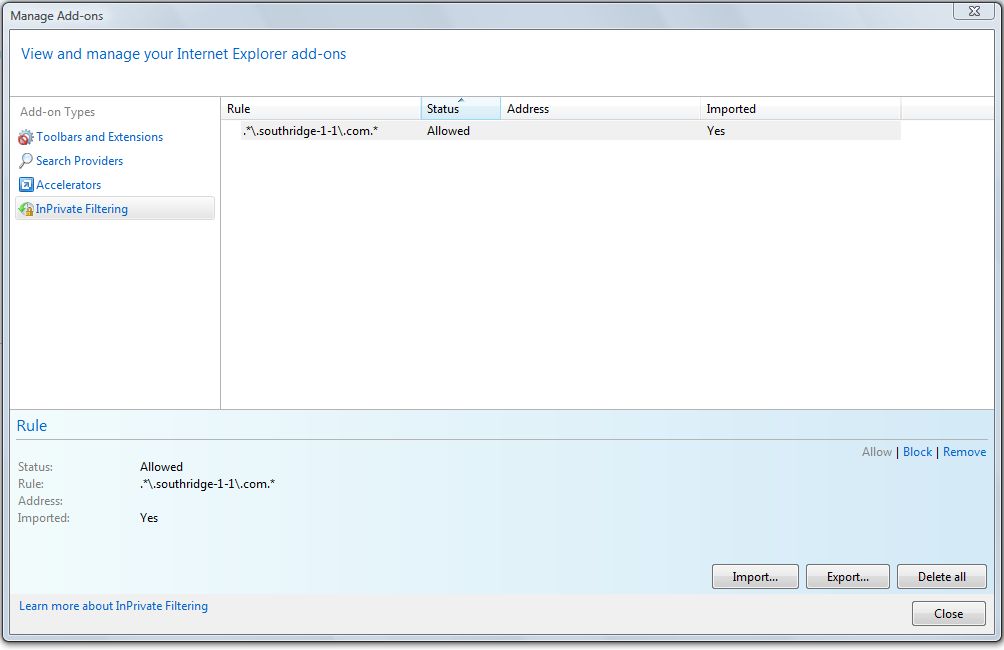


Figure 11

## Additional Information on Third-Party Content

Within the InPrivate Filtering settings window, users can access additional information for listed third-party content providers by highlighting an entry in the list and clicking on the “More information from this website” link. This capability is important to both the user and the third-party content providers, as it can provide content providers with a viable means to communicate to the user who they are, how collected data may be used, and, most importantly, the value the user receives by allowing content to be retrieved.

When users click on the link, Internet Explorer 8 opens a new window and navigates to a “Third-Party.html” page at the same location as the third-party content. For example, as shown in Figure 10, if the item “stats.js” is located at [www.southridge-1-1.com/tracking](http://www.southridge-1-1.com/tracking%20%20), the link to more information will point to [www.southridge-1-1.com/tracking/third-Party.html](http://www.southridge-1-1.com/tracking/3rdParty.html).

*More information on creating a third-party information page can be found in the Considerations for Content Providers section of this document.*

# Considerations for Content Providers

Microsoft recognizes that the wealth of content on the Web is heavily supported by advertising. Without a high degree of assurance that syndicated advertising and content will be displayed, the ability of those businesses to continue participating in that “value exchange” could be marginalized. Such a shift could force Web sites to pursue alternative sources of income such as charging for access, potentially limiting content to those who are able and willing to pay for it.

Microsoft also recognizes that a “fair” value exchange between content publishers and content consumers can only be achieved when people have confidence and trust in the Web sites they visit. Furthermore, users have been clear that obtaining their confidence and trust requires protection from harm, freedom from intrusion, and choice and control over both who has access to their personal information and how it is used.

There are several products on the market that are specifically designed to block advertising. Unfortunately, while many of these products may offer some value to the end user, they can indiscriminately block all advertising and content, effectively marginalizing the value exchange between consumers and publishers of online content.

Microsoft has designed InPrivate Filtering in a manner that is fundamentally different than “ad-blockers”—and that respects the importance of advertising-supported content. InPrivate Filtering simply provides users with awareness and control over their experience on the Web, looking only at content originating from third-party Web sites—ones other than those the user has consciously chosen to visit.

Furthermore, InPrivate does not attempt to distinguish between “good” or “bad” third-party content. Instead, it simply allows the user to make informed decisions about how their Web surfing activities can be tracked—and, if desired, to prevent the disclosure of such information by blocking third-party content on the Web sites they visit. First-party advertisements are not affected, as Microsoft believes they do not present the potential privacy and security risks that may be associated with third party content.

## Creating a Third-Party Information Page

As previously discussed, InPrivate Filtering provides a built-in method for users to navigate to a “third-party.html” page that can help users make informed decisions about how third-party content providers can track their online behavior. While the creation of such Web pages is completely at the discretion of third-party content providers, *it provides them with the opportunity to clearly communicate the value provided by their content—and to clarify their privacy, data collection, and data sharing practices.*

At a minimum, Microsoft recommends that content providers include the following information on their third-party.html page(s):

* Company name, location, and place of business incorporation
* Purpose of content (content, images, advertising, analytics, etc.)
* Link to a privacy policy that addresses and clarifies what data is collected and how it is used Third party accreditation, certification, or audit of privacy policies
* Industry and business organizations in which the content provider is a member in good standing
* Contact information for users who desire additional information

## InPrivate Filtering Session Status

To aid Web site publishers and facilitate the value exchange of content for user data, Internet Explorer 8 enables first-party Web sites to detect when a user has InPrivate Filtering enabled. First party sites can only detect whether the feature is active; they cannot distinguish whether InPrivate Filtering is in Auto or Manual mode, nor can they directly determine if any specific content is being blocked.

This capability is provided through **InPrivateFilteringEnabled**, a DOM-accessible API that returns TRUE when InPrivate Filtering is in Auto or Manual mode. The API is accessible through the **window.external** DOM object and is exposed to binary extensions through the ieframe.dll.

## First-Party versus Third-Party Considerations

Depending on content type, distribution breadth, and structure of business partnerships, first-party and third-party content providers may want to work together to determine of the risk and impact of third-party content being blocked, as well as potential ways to have third-party content appear as first-party content. There are several methods for content originating from third-parties to appear to InPrivate Filtering the as first-party content, with each option having its own pros and cons based on the nature of the content as well as the business and branding objectives of the various parties involved. First-party Web site operators and third-party content providers should check with their network administrators for details and requirements based on their unique IT environments and architectures.

While there are a number of ways to have third-party content appear as first-party content, following are two approaches for consideration.

### First-Party Hosting of Third-Party Content

A first-party content provider may want to host third-party content within their own IT infrastructure—that is, by first moving third-party content to their own servers. Under this approach, security, content management, and visibility into user activity are all within control of the first-party content provider. However, the first party also becomes accountable for security and privacy, and takes on the associated infrastructure requirements. This approach may work best when the content is nonvolatile, such as Web applications.

### DNS CNAME Changes

First-party content providers can use the Domain Name Service (DNS) to issue sub-domains for third-party content providers, so that they operate as a first-party surrogate. Table 1 illustrates a high-level example of this approach, in which the first-party site (contoso.com) creates a DNS CNAME entry for a third-party content provider.

It should be noted that this approach removes inherent publisher security and domain-isolation benefits related to third-party content providers, such as third-party script sandboxing and third-party disclosure around cookie ownership and practices. For publishers that use a content delivery network (CDN) or other network edge technology, an alternative to this approach to have the DNS/Redirection occur at the CDN infrastructure layer.

|  |  |  |
| --- | --- | --- |
| **Entity** | **DNS** | **Destination** |
| First-party Site:  Sub-domain issuance: | www.contoso.com  third-PartyA.contoso.com | xx.xx.xx.xx  [www.third-PartyA.com](http://www.third-PartyA.com) |
| Third-party Site: | www.third-PartyA.com | xx.xx.xx.xx |

Table 1

Organizations considering this approach should evaluate the pros and cons with respect to their unique environments. Content providers who chain content can still be at risk of having their content blocked because DNS will only deliver the initial aliased provider as a first-party site.

For example, say that advertising provider ThirdPartyA.com is used by Consoso.com, and that Consoso.com creates a CNAME that maps ThirdPartyA.contoso.com to ThirdPartyA.com so that third-party content from ThirdPartyA.com on Consoso.com is delivered as first-party content from ThirdPartyA.contoso.com. However, if ThirdPartyA.com calls an external advertising network, all content from that external advertising network will still be considered third-party content by InPrivate Filtering. Because of this, for first-party content providers considering this approach, Microsoft recommends that they be informed of—and proactively manage—all downstream partnerships that may affect the content served on their sites.

# Conclusion

Consumer trust and confidence are necessary for the long-term vitality of advertising-supported Web sites—and thus the Web as a whole. Through Microsoft’s framework for Trustworthy Browsing and the various privacy and security related innovations in Internet Explorer 8, Microsoft is committed to delivering a Web browser that respects user choice and helps keep users in control of both their PC and their personal information.

## For More Information

**Internet Explorer 8 Feature Overview**

[www.microsoft.com/ie8](http://www.microsoft.com/ie8)

**Internet Explorer 8 Blog**

<http://blogs.msdn.com/ie>

**Internet Explorer 8 Readiness Toolkit**

[www.microsoft.com/windows/products/winfamily/ie/ie8/readiness](http://www.microsoft.com/windows/products/winfamily/ie/ie8/readiness)

**Internet Explorer 8 Safety & Privacy Features**

[www.microsoft.com/windows/internetexplorer/beta/features/browse-privately.aspx](http://www.microsoft.com/windows/internetexplorer/beta/features/browse-privately.aspx)

**Internet Explorer 8 – Business Value of Extended Validation SSL Certificates**

[www.microsoft.com/ie/ev](http://www.microsoft.com/ie/ev)

# Appendix A: InPrivate Browsing - Data Handling

|  |  |  |
| --- | --- | --- |
| **Data store or feature** | **Description** | **Behavior for InPrivate Browsing** |
| **Automatic Crash Recovery (ACR) Store** | Contains information used to restore tabs in the event of a crash or accidental tab closure | Remains on when InPrivate Browsing is active, but frame recovery is disabled |
| **ActiveX® Per-site Opt-in** | ActiveX controls can be opted-into on a per-site (domain name) basis | Users’ per-site opt-in choices are not retained after the InPrivate Browsing session is closed |
| **Address Bar  and Search Autocomplete** | The Address Bar and the Search box both store entries typed by the user | Address Bar and Search Autocomplete entries are not stored |
| **Anti-phishing cache** | Used by the SmartScreen filter to accelerate lookups for phishing | The Anti-phishing cache is cleared when the InPrivate Browsing window is closed |
| **Compatibility view** | Stores domain names for Web sites to be shown in compatibility view | When an InPrivate Browsing session is started, the compatibility view list that resides on disk is copied to e temporary list in memory. During InPrivate Browsing, changes are applied to the temporary list. On exit, the temporary list is discarded |
| **Cookies** | Persistent cookies are stored in an on-disk cache | Persistent cookies *are not sent.*  If a website requests to set a persistent cookie, Internet Explorer will honor the request, but set the cookie as a session cookie |
| **DOM Storage** | Provides script authors with “super cookies” that are stored in a WinInet cache container | DOM storage objects created when using InPrivate Browsing are not persisted |
| **Form Data** | Form data is saved when the user selects the “Form Data Autocomplete” feature | Form data is not stored |
| **History** | Browsing history is stored in a WinInet cache container | History is not stored |
| **InPrivate Filtering data** | Contains records of third-party items and the domain names of the first-party sites from which the items were referenced | InPrivate Filtering data is not accumulated |
| **Passwords** | Passwords are saved when the user select the “Form Data Autocomplete” feature | Passwords are not stored |
| **Temporary Internet File (cache)** | The TIF (Temporary Internet Files) directory has on-disk cache containers for Web pages and visited links | Cache entries created while InPrivate Browsing is active are flagged as “privacy impacted.” All flagged entries are deleted when an InPrivate Browsing session is closed |

Table 2 describes how various types of data are handled by InPrivate Browsing.

Table 2

# Appendix B: Group Policy Settings and Scenarios

Group policies can help businesses optimize security settings and better protect user PCs, corporate infrastructure, and data when deploying software. Internet Explorer 8 supports more than 1,300 group policies to aid enterprises in configuring its settings, including those for security and privacy. For example, using group policies, an administrator may automatically enable the SmartScreen Filter, prevent users from clicking-through to Web sites when the SmartScreen Filter displays a warning, and configure privacy settings to help control and protect data based on corporate and regulatory requirements.

## Individual Group Policy Settings

The following are key Active Directory® settings that are specific to InPrivate Browsing and InPrivate Filtering:

### Disable InPrivate Browsing

**Data type:** BOOL

**Acceptable Values:** Enabled, Disabled, Not Configured

**Description:** This policy setting allows you to disable the InPrivate Browsing feature. InPrivate Browsing prevents Internet Explorer from storing data about users’ browsing session. This includes cookies, temporary Internet files, history, and other data. If you enable this policy setting, InPrivate Browsing will be turned off. If you disable this policy setting, InPrivate Browsing will be turned on. If you do not configure this setting, InPrivate Browsing can be turned on or off through the registry. (Note: Deprecates the “Disable InPrivate” key for Internet Explorer 8 Beta 2.)

### Do not collect InPrivate Filtering Data

**Data type:** BOOL

**Acceptable Values:** Enabled, Disabled, Not Configured

**Description:** This policy setting allows you to disable collection of data used by the InPrivate Filtering Automatic mode. The data consists of the URLs of third-party content, along with data about the first-party websites that referenced it. If you enable this policy setting, InPrivate Filtering collection will be turned off in all browsing sessions. If you disable this policy setting, InPrivate Filtering collection will be turned on in all browsing sessions. If you do not configure this setting, InPrivate Filtering data collection can be turned on or off in the Privacy tab in Internet Options.

### InPrivate Filtering Threshold

**Data type:** DWORD (range)

**Acceptable Values:** 3-30

**Description:** This policy setting allows you configure the threshold for InPrivate Filtering Automatic mode. The threshold sets the number of first-party sites that a particular third-party item can be referenced from before it is blocked. Setting this value lower can help prevent more third-party sites from obtaining details about users’ browsing; however doing so will likely prevent some content from being displayed for some Web sites. The allowed value range is 3-30. If you specify a value, the specified value will be enforced. If you do not configure this setting, the InPrivate Filtering threshold defaults to 10 and can be adjusted by the user.

### Disable toolbars and extensions when InPrivate starts

**Data type:** BOOL

**Acceptable Values:** Enabled, Disabled, Not Configured

**Description:** This policy setting allows you to configure whether or not Toolbars and Browser Helper Objects (BHOs) are loaded by default during InPrivate Browsing. Toolbars and BHOs may store data about users’ browsing sessions. By default, they are disabled in InPrivate Browsing. If you enable this policy, toolbars and BHOs will not be loaded by default during InPrivate Browsing. If you disable this policy, toolbars and BHOs will be loaded by default during InPrivate Browsing. If you do not configure this setting, it can be configured on the Privacy tab in Internet Options.

### Disable InPrivate Filtering

**Data type:** BOOL

**Acceptable Values:** Enabled, Disabled, Not Configured

**Description:** This policy setting allows you to disable InPrivate Filtering. InPrivate Filtering helps users control whether third parties can automatically collect information about their browsing based on the sites they visit. InPrivate Filtering does this by identifying third-party content that is used by multiple websites users have visited. If you enable this policy, InPrivate Filtering will be disabled and InPrivate Filtering data will not be collected. If you disable this policy, InPrivate Filtering will be available for use. If you do not configure this setting, it can be configured through the registry.

## Common Group Policy Scenarios

Table 3 shows Group Policy settings for some common scenarios.

|  |  |  |  |
| --- | --- | --- | --- |
| Scenario Name | “Disable InPrivate Browsing” | “Do not collect data for blocking” | “Disable InPrivate Filtering” |
| Enable InPrivate Filtering, disable InPrivate Browsing | Enabled | Disabled/Not Configured | Disabled/ Not Configured |
| Turn off all of InPrivate | Enabled | Overridden (Enabled) | Enabled |
| Enable InPrivate Browsing, disable InPrivate Filtering | Disabled | Overridden (Enabled) | Enabled |

Table 3