

Internet Explorer® 8 Security Guide

Security Compliance Management Toolkit

**Version 1.1**

Published: October 2009 | Updated: April 2010

For the latest information, see  
microsoft.com/securitycompliance

Copyright © 2009 Microsoft Corporation. All rights reserved. Complying with the applicable copyright laws is your responsibility. By using or providing feedback on this documentation, you agree to the license agreement below.

If you are using this documentation solely for non-commercial purposes internally within YOUR company or organization, then this documentation is licensed to you under the Creative Commons Attribution-NonCommercial License. To view a copy of this license, visit http://creativecommons.org/licenses/by-nc/2.5/ or send a letter to Creative Commons, 543 Howard Street, 5th Floor, San Francisco, California, 94105, USA.

This documentation is provided to you for informational purposes only, and is provided to you entirely "AS IS". Your use of the documentation cannot be understood as substituting for customized service and information that might be developed by Microsoft Corporation for a particular user based upon that user’s particular environment. To the extent permitted by law, MICROSOFT MAKES NO WARRANTY OF ANY KIND, DISCLAIMS ALL EXPRESS, IMPLIED AND STATUTORY WARRANTIES, AND ASSUMES NO LIABILITY TO YOU FOR ANY DAMAGES OF ANY TYPE IN CONNECTION WITH THESE MATERIALS OR ANY INTELLECTUAL PROPERTY IN THEM.

Microsoft may have patents, patent applications, trademarks, or other intellectual property rights covering subject matter within this documentation. Except as provided in a separate agreement from Microsoft, your use of this document does not give you any license to these patents, trademarks or other intellectual property.

Information in this document, including URL and other Internet Web site references, is subject to change without notice. Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious.

Microsoft, Access, Active Directory, ActiveX, Authenticode, Excel, InfoPath, Internet Explorer, Internet Explorer 8, JScript, MSDN, Outlook, PowerPoint, Visual Basic, Windows, Windows Server, Windows Server 2008, Windows Server 2003, Windows 7, Windows Vista, and Windows XP are either registered trademarks or trademarks of Microsoft Corporation 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.

You have no obligation to give Microsoft any suggestions, comments or other feedback ("Feedback") relating to the documentation. However, if you do provide any Feedback to Microsoft then you provide to Microsoft, without charge, the right to use, share and commercialize your Feedback in any way and for any purpose. You also give to third parties, without charge, any patent rights needed for their products, technologies and services to use or interface with any specific parts of a Microsoft software or service that includes the Feedback. You will not give Feedback that is subject to a license that requires Microsoft to license its software or documentation to third parties because we include your Feedback in them.

Contents

[Overview 1](#_Toc246843966)

[Who Should Read This Guide 2](#_Toc246843967)

[Skills and Readiness 2](#_Toc246843968)

[Guide Purpose and Scope 2](#_Toc246843969)

[Chapter Summaries 3](#_Toc246843970)

[Style Conventions 4](#_Toc246843971)

[More Information 4](#_Toc246843972)

[Support and Feedback 4](#_Toc246843973)

[Acknowledgments 5](#_Toc246843974)

[Development Team 5](#_Toc246843975)

[Contributors and Reviewers 6](#_Toc246843976)

[Chapter 1: Implementing the Internet Explorer 8 Security Baseline 7](#_Toc246843977)

[Limit User Privileges 8](#_Toc246843978)

[Enterprise Client Environment 8](#_Toc246843979)

[Specialized Security – Limited Functionality Environment 8](#_Toc246843980)

[Managing Internet Explorer 8 9](#_Toc246843981)

[Understanding the Zone Model 10](#_Toc246843982)

[Modifying Zone Settings 12](#_Toc246843983)

[Zone Determination 12](#_Toc246843984)

[Beyond the Zone Model: General Security Settings 13](#_Toc246843985)

[Security Design 13](#_Toc246843986)

[OU Design for Security Policies 13](#_Toc246843987)

[Domain Root 14](#_Toc246843988)

[Domain Controllers OU 14](#_Toc246843989)

[Member Servers OU 14](#_Toc246843990)

[Server Role OUs 15](#_Toc246843991)

[Department OU 15](#_Toc246843992)

[Windows 7 Users OU 15](#_Toc246843993)

[Windows 7 Computers OU 15](#_Toc246843994)

[GPO Design for Security Policies 15](#_Toc246843995)

[Recommended GPOs 17](#_Toc246843996)

[Using a GPO Created with the Security Compliance Manager Tool 19](#_Toc246843997)

[Security and Privacy Features in Internet Explorer 8 21](#_Toc246843998)

[SmartScreen Filter 21](#_Toc246843999)

[Phishing and Malware Protection 21](#_Toc246844000)

[ClickJacking 22](#_Toc246844001)

[Cross-Site Scripting (XSS) Filter 22](#_Toc246844002)

[Domain Highlighting 23](#_Toc246844003)

[Internet Explorer Protected Mode 23](#_Toc246844004)

[ActiveX Opt-in 24](#_Toc246844005)

[InPrivate Browsing 24](#_Toc246844006)

[InPrivate Filtering 25](#_Toc246844007)

[More Information 25](#_Toc246844008)

[Chapter 2: Security Recommendations 27](#_Toc246844009)

[Manage Add-ons 27](#_Toc246844010)

[Restrict ActiveX Controls 27](#_Toc246844011)

[Control Per-Site ActiveX Settings 28](#_Toc246844012)

[Use ActiveX Controls, Plug-ins, and Pre-approved Lists 28](#_Toc246844013)

[Disable Active Scripting 29](#_Toc246844014)

[Support for Scripting 30](#_Toc246844015)

[Enable Scripted Window Security Restrictions 30](#_Toc246844016)

[Zone Security 31](#_Toc246844017)

[Enable Zone Elevation Protection 31](#_Toc246844018)

[Do Not Allow Users to Add or Delete Sites from Zones 32](#_Toc246844019)

[Do Not Allow Users to Change Zone Policies 32](#_Toc246844020)

[Certificate Security 33](#_Toc246844021)

[Prevent Users from Accessing Sites with Certificate Errors 33](#_Toc246844022)

[Reduced Application Privilege 34](#_Toc246844023)

[Turn On Protected Mode 34](#_Toc246844024)

[Use DropMyRights in Windows XP 35](#_Toc246844025)

[Other Security Settings 35](#_Toc246844026)

[MIME Sniffing Safety Feature 35](#_Toc246844027)

[MK Protocol Security Restriction 36](#_Toc246844028)

[Do Not Save Encrypted Pages to Disk 36](#_Toc246844029)

[Make Proxy Settings on a Per Machine Basis 37](#_Toc246844030)

[Turn Off Crash Protection 38](#_Toc246844031)

[Enable the Restrict File Download Setting 39](#_Toc246844032)

[Disable File Downloads for the Restricted Sites Zone 39](#_Toc246844033)

[Use Object Caching Protection 40](#_Toc246844034)

[Java Permissions 41](#_Toc246844035)

[More Information 41](#_Toc246844036)

[Chapter 3: Privacy Setting Recommendations 43](#_Toc246844037)

[Use InPrivate Browsing 44](#_Toc246844038)

[Use InPrivate Filtering 44](#_Toc246844039)

[Delete Browsing History 45](#_Toc246844040)

[Set the Privacy Slider to Medium or Higher 45](#_Toc246844041)

[Automatically Empty the Temporary Internet Files Folder 46](#_Toc246844042)

[Set Form AutoComplete Options to Disabled 47](#_Toc246844043)

[Configure Logon Options for Each Zone 48](#_Toc246844044)

[Enable the SmartScreen Filter 50](#_Toc246844045)

[Use the Cross Site (XSS) Scripting Filter 52](#_Toc246844046)

[More Information 52](#_Toc246844047)

[Appendix A: Security Checklist 53](#_Toc246844048)

Overview

Welcome to the *Internet Explorer 8 Security Guide*. This guide provides instructions and recommendations to help strengthen the security of desktop and laptop computers running Windows® Internet Explorer® 8.

One of the biggest challenges with defining default security settings for a Web browser is balancing required functionality with risks that the functionality can introduce. If the default settings in the browser are too restrictive, users may experience limitations and compatibility issues, and simply ignore warnings or alerts. But if the settings are not restrictive enough, users are susceptible to attack from a wide range of exploits. Finding the right balance of functionality and security is critical for both safety and ease of use.

Web browser developers will typically define default security settings to allow the greatest usability based on calculated risk. Basing decisions on attack scenarios, weighting factors required to exploit potential vulnerabilities and other user scenarios, the developer selects values for the default security settings to enable the browser to function well in a wide range of environments. For most home users, the default settings in the browser are usually sufficient to meet their needs and help protect them from most attacks.

However, some consumers and business users may have more specific requirements based on business needs, as well as regulatory and legal requirements. For example, users in large organizations may be required to comply with government regulations to protect financial data and customer information stored on their network servers.

The security and privacy settings in Internet Explorer 8 have been designed to meet a wide range of requirements, further solidifying security leadership from Microsoft. At the same time, we respect user privacy, the need of organizations to control data use, and the demand to provide recommended options to balance these needs. Internet Explorer 8 offers increased security over previous versions of the browser, as well as new privacy features to help users manage and control personal information. For more information about the new features and settings, visit the [Internet Explorer 8](http://go.microsoft.com/fwlink/?LinkId=122516) Web site.

This guide examines some of the features and settings that you can modify to provide a more "locked down" security configuration that some users and organizations may require. This guide does not provide a complete review of all settings in the browser, and the guidance recommendations are not specifically equivalent to those for the Internet Explorer Enhanced Server Configuration (IE ESC) in Windows Server® 2003 and Windows Server® 2008. The settings and features this guide discusses offer additional security guidance to ensure the broadest impact on users and administrators in organizations in which enhanced security is required.

This guide discusses setting options in Internet Explorer® 8 for Windows® 7, Windows Vista® and Windows® XP. IT professionals can use this guidance to tighten security settings in the browser to meet the specific needs of their organizations.

**Note:**   In many cases, administrators can use the Internet Explorer Administration Kit (IEAK) to create a customized build of Internet Explorer to deploy it across the organization, and then use Group Policy to enforce the settings in the build. This guide does not discuss the IEAK in detail, but you can use many of the settings described in the guidance to create a custom package.

# Who Should Read This Guide

The *Internet Explorer 8 Security Guide* is primarily for IT generalists, security specialists, network architects, and other IT professionals and consultants who plan application or infrastructure development and deployments of desktop and laptop computers running supported Windows client operating systems in a wide variety of organizations.

## Skills and Readiness

The following knowledge and skills are required for the intended audience of this guide, who develop, deploy, and secure client computers running Internet Explorer 8:

* MCSE on Windows Server 2003 or a later certification and two or more years of security-related experience, or equivalent knowledge.
* In-depth knowledge of the organization’s domain and Active Directory environments.
* Experience with the Group Policy Management Console (GPMC).
* Experience in the administration of Group Policy using the GPMC, which provides a single solution for managing all Group Policy–related tasks.
* Experience using management tools including the Microsoft Management Console (MMC), Gpupdate, and Gpresult.
* Experience deploying applications and client computers in enterprise environments.

## Guide Purpose and Scope

The primary purposes of this guide are to enable you to:

* Use the solution guidance to efficiently create and apply tested security baseline configurations using Group Policy.
* Understand the reasoning for the security setting recommendations in the baseline configurations that are included in the guide, and their implications.
* Identify and consider common security scenarios, and how to use specific security features in Internet Explorer 8 to help you manage them in your environment.

The guide is designed to allow you to use only those parts of it that are relevant to the security requirements of your organization. However, readers will gain the most benefit by reading the entire guide. This guide focuses on how to help create and maintain a secure environment for computers running Internet Explorer 8. The guide explains the different stages of how to secure two different environments. The guide also provides prescriptive information and security recommendations. Client computers can run either Windows 7 or Windows Vista SP1 or later. However, the computers that manage these client computers on the network must be able to run Windows Server 2008, Windows Server 2003 R2, or Windows Server 2003 SP2.

There are differences between the settings that appear in the Group Policy Editor and the Internet Explorer configuration tool, **Internet Options**. For example, there are many settings exposed via Group Policy that are not accessible in the **Internet Options** tool, such as all of the settings available at **Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Locked-Down Internet Zone**.

Also note that many settings that appear in the Administrative Templates portion of the Group Policy Editor are recorded in special locations in the registry:

* HKEY\_LOCAL\_MACHINE\Software\Policies
* HKey\_CURRENT\_USER\Software\Policies.

When you use the **Internet Options** tool the settings are recorded in a different location, such as HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Lockdown\_Zones\1. Group Policy works this way to make it easier to avoid problems associated with settings *tattooing* the system. However, this can be confusing when trying to compare the results of settings configured via Group Policy versus those configured by the **Internet Options** tool.

**Note:**   The term *tattooing* in this context refers to how some group policy settings can remain in effect even when the computer or user account is no longer within the scope of group policy. For example, all of the settings located at **Computer Configuration\Windows Settings\Security Settings\Local Policies\Security Options** tattoo the system when configured via domain-based group policy.

# Chapter Summaries

The *Internet Explorer 8* *Security Guide* consists of the following 3 chapters and an appendix:

Chapter 1: Implementing the Internet Explorer 8 Security Baseline

This chapter provides a set of procedures to implement prescribed security settings to enhance the default security of Internet Explorer 8 on client computers. The chapter also discusses the details of the recommended Group Policy deployment configuration and the support requirements for two distinct security environments.

Chapter 2: Security Recommendations

This chapter provides details about the security related features and Group Policy settings for Internet Explorer 8. The setting and feature recommendations are grouped into the following six categories:

* Manage Add-ons
* Disable Active Scripting
* Zone Security
* Certificate Security
* Reducing Application Privilege
* Other Security Settings

Each setting in these categories includes an explanation that describes what each one does, the default behavior in the browser, and the recommended setting configuration for each security environment when applicable.

Chapter 3: Privacy Setting Recommendations

This chapter provides details about the privacy related features and Group Policy settings for Internet Explorer 8.The setting and recommendations in this chapter are primarily focused on the InPrivate Browsing and SmartScreen features in Internet Explorer 8.

Appendix A: Security Checklist

The appendix provides a checklist that includes all of the feature areas and settings that we recommend to consider using as you secure client computers running Internet Explorer 8 in your organization.

## Style Conventions

This guide uses the following style conventions.

| Element | Meaning |
| --- | --- |
| **Bold font** | Signifies characters typed exactly as shown, including commands, switches and file names. User interface elements also appear in bold. |
| *Italic font* | Titles of books and other substantial publications appear in *italic*. New terms when first mentioned also appear in *italic*. |
| *<Italic>* | Placeholders set in italic and angle brackets <*filename*> represent variables. |
| Monospace font | Defines code and script samples. |
| **Note** | Alerts the reader to supplementary information. |
| **Important** | An important note provides information that is essential to the completion of a task. |
| Exclam**Warning** | Alerts the reader to essential supplementary information that should not be ignored. |
| ‡ | This symbol denotes specific Group Policy setting modifications or recommendations. |
| § | This symbol denotes Group Policy settings that are new to Windows 7. |

## More Information

The following resources provide additional information about Internet Explorer 8 security-related topics on Microsoft.com:

* [Internet Explorer 8](http://go.microsoft.com/fwlink/?LinkId=122516) home page.

## Support and Feedback

The Solution Accelerators – Security and Compliance (SA–SC) team would appreciate your thoughts about this and other solution accelerators.

Please direct questions and comments about this guide to [secwish@microsoft.com](mailto:secwish@microsoft.com?subject=Internet%20Explorer%208%20Security%20Guide%20feedback).

We look forward to hearing from you.

# Acknowledgments

The Solution Accelerators – Security and Compliance (SA–SC) team would like to acknowledge and thank the team that produced the Internet Explorer 8 Security Guide. The following people were either directly responsible or made a substantial contribution to the writing, development, and testing of this solution.

## Development Team

Content Developers

Kurt Dillard – *kurtdillard.com*

Richard Harrison – Content Master Ltd.

Developers

Barry Hartmann

Gerald Herbaugh

Haikun Zhang – *Beijing ZZZGroup Co. Ltd*

Jeff Sigman

Jim Riekse

José Maldonado

Michael Tan

ZhiQiang Yuan – *Beijing ZZZGroup Co. Ltd.*

Editors

John Cobb – Wadeware LLC

Steve Wacker – Wadeware LLC

Product Manager

Michelle Arney

Shruti Kala

Stephanie Chacharon – *Xtreme Consulting Group Inc.*

Program Manager

Tom Cloward

Release Manager

Cheri Ahlbeck – *Aquent LLC*

Karina Larson

Test Manager

Sumit Parikh

Testers

Jaideep Bahadur – *Infosys Technologies Ltd.*

Mansi Sharma – *Infosys Technologies Ltd.*

Raxit Gajjar – Infosys Technologies Ltd.

## Contributors and Reviewers

Aaron Margosis, Blake Frantz – *Center for Internet Security*, Dan Fox, Daniel Taylor, *Defense Information System Agency (DISA)*, Derek Seaman – *Lockheed Martin*, Fidelis Ekezue, Greg Cottingham, Guy Hunt, Juan Antonio Díaz Muñoz, Kathy Lambert, Lori Kingery, Mandy Tidwell, Nate Morin, Pete LePage, Rick Munck, Roger Grimes, Roger Podwoski, Susan Bradley – *www.sbsdiva.com*, Susan Fosselman, Steven Rolnick, Tim Clark, TJ Onishile, Yung Chou

**Note**   At the request of Microsoft, the National Security Agency Information Assurance Directorate participated in the review of this Microsoft security guide and provided comments that were incorporated into the published version.

**Note**   During the development of this Microsoft security guide and the associated security baseline settings, members of the Center for Internet Security community collaborated with Microsoft and provided comments that were incorporated into the published version.

Chapter 1: Implementing the Internet Explorer 8 Security Baseline

Windows® Internet Explorer® 8 builds on the security improvements and enhancements included in the release of Internet Explorer 7. In that release, Microsoft introduced several new security features and designs, such as Protected Mode and ActiveX® Opt-In, to help provide a security-in-depth approach by providing layers of protection. Other new features, such as the Phishing Filter, helped protect users against emerging threats to provide protection against attacks targeted at obtaining personal information. Detailed descriptions of the security enhancements in previous versions of Internet Explorer are beyond the scope of this guide. For more information about these improvements, see the [Internet Explorer TechCenter](http://technet.microsoft.com/ie).

The advancements in Internet Explorer 8 are designed to help protect users against many of the latest online threats, and provide them with more streamlined interfaces to make security decisions. The settings in Internet Explorer 8 are designed by default to provide a balance between usability and security for a broad range of worldwide users. In addition, Internet Explorer 8 adds an entirely new set of Privacy controls and features to help users take control of their online browsing activity and information.

This guide focuses on security settings in Internet Explorer 8. However, any review on how to optimally secure an application must also include information about host level security, which is covered in the security guides for Windows® 7 and Windows Vista®. In addition, to avoid any vulnerability in the browser, browser add-ins, and the operating system that you are running it on, you must update them regularly. We recommend installing all operating system updates using tools such as Windows Server® Update Services (WSUS), Systems Management Server (SMS) 2003, Microsoft® System Center Configuration Manager 2007 R2 or Automatic Updates to keep your systems current with the latest updates. In addition, customers are encouraged to register to receive technical security notifications from the [Microsoft Technical Security Notifications](http://go.microsoft.com/fwlink/?LinkId=21163). For more information, see Appendix A, "Security Checklist."

You can harden the default browser configuration using Group Policy objects (GPOs). All of the recommended Group Policy settings are documented in the Internet Explorer 8 Security Baseline Settings Excel® workbook that accompanies this guide.

To deploy the guidance in this chapter, you need to:

* Create an organizational unit (OU) structure for your environment.
* Use the Security Compliance Manager tool included with this guide to create the GPOs for your environment.
* Use the Group Policy Management Console (GPMC) to link and manage the GPOs.

Exclam**Warning**It is essential to thoroughly test your OU and GPO designs before deploying them in a production environment.

The baseline GPOs that accompany this guide provide a combination of tested settings that enhance security for client computers running Windows 7 in the following two distinct security environments:

* **Enterprise Client (EC)**
* **Specialized Security – Limited Functionality (SSLF)**

# Limit User Privileges

When improving the security of computers running Windows® XP, Windows Vista, and Windows 7, one of the most effective countermeasures is to ensure that users log on with standard accounts for their normal, day-to-day activities. They should only use accounts with elevated privileges when they need to perform administrative tasks. The same holds true for Web browsers. Under normal circumstances, users should start Internet Explorer with standard privileges to ensure that protected mode helps reduce the risk of malicious code affecting the computer. This ensures that if a user is compromised by malware, the dangerous code will only be able to affect the user’s profile because it will be limited to the same privileges as the user. Another important consideration is that users with administrative privileges can reconfigure the settings discussed in this guide, thereby increasing the risk of compromise.

# Enterprise Client Environment

The Enterprise Client (EC) environment referred to in this chapter consists of a domain using Active Directory® Domain Services (AD DS) in which computers running Windows Server® 2008, Windows Server® 2003 R2, or Windows Server 2003 SP2 and Active Directory manage client computers that can run Windows 7, Windows Vista or Windows XP Professional SP3. The client computers are managed in this environment through Group Policy, which is applied to sites, domains, and OUs. Group Policy provides a centralized infrastructure within AD DS that enables directory–based change and configuration management of user and computer settings, including security and user data. The EC security baseline helps provide enhanced security that allows sufficient functionality of the operating system and applications for the majority of organizations.

# Specialized Security – Limited Functionality Environment

The Specialized Security – Limited Functionality (SSLF) baseline in this guide addresses the demand to help create highly secure environments for computers running Internet Explorer 8. Concern for security is so great in these environments that a significant loss of functionality and manageability is acceptable.

Exclam **Warning**The SSLF security settings are not intended for the majority of enterprise organizations. The configuration for these settings has been developed for organizations where security is more important than functionality.

If you decide to test and deploy the SSLF configuration settings for the client computers in your environment, the IT resources in your organization may experience an increase in help desk calls related to the limited functionality that the settings impose. Although the configuration for this environment provides a higher level of security for data and the network, it also prevents some services from running that your organization may require. An example of this is disabling access to ActiveX® Controls, which can severely limit user access to the specialized features of some Web sites.

It is important to note that the SSLF baseline is not an addition to the EC baseline: the SSLF baseline provides a distinctly different level of security. For this reason, do not attempt to apply the SSLF baseline and the EC baseline to the same computers. Rather, for the purposes of this guide, it is *imperative* to first identify the level of security that your environment requires, and then decide to apply the EC baseline *or* the SSLF baseline. To compare the setting differences between the EC baseline and SSLF baseline, see the Internet Explorer 8 Security Baseline Settings Excel workbook that accompanies this guide.

Important   If you are considering whether to use the SSLF baseline for your environment, be prepared to exhaustively test the computers in your environment after you apply the SSLF security settings to ensure that they do not prohibit required functionality for the computers in your environment.

# Managing Internet Explorer 8

Depending on the size and complexity of the organization, the two main options that you can use for centralized administration of the settings in Internet Explorer 8 are the [*Internet Explorer Administration Kit (IEAK) 8*](http://technet.microsoft.com/en-us/ie/bb219517.aspx) and GPOs in an Active Directory infrastructure. There are some settings that you can only configure using the IEAK or GPOs, but not both. However, this guide provides setting information for both resources wherever possible.

To help administrators select the optimal setting management solution for their environment, it is important to understand more about both of these resources. In general, the IEAK is for organizations that manage environments without an Active Directory infrastructure or for organizations that want to provide a customized version of the browser, complete with custom settings and options. The IEAK allows administrators to easily build a custom configuration settings file that is applied during installation setup. Administrators using the IEAK to build custom packages can define settings for many, but not all Internet Explorer 8 settings. Installations performed with an IEAK package only maintain settings until the user changes them. For installations created using the **Internal Distribution – Corporate Intranet** mode, you can apply IEAK settings at specified intervals to ensure that user configurations align with company defined standards. Selecting the new **Reset Internet Explorer Settings** option reverts the installation to the customized settings applied by your organization, reverts ActiveX Opt-In settings to their default values, and disables, but does not remove, all toolbars and extensions installed on the computer.

Using GPOs provides you with the ability to create well defined installation configurations that are regularly updated by policy controls to prevent user changes. You can use GPO settings to control hundreds of settings and options in Internet Explorer 8. Working with GPO settings is more complex than using the IEAK. Once you define and apply a GPO template, all affected managed systems follow that configuration unless an administrator changes it. Many attempted user changes are simply ignored or disallowed. In other cases, changes may be possible, but they will reset to enterprise defaults at the next policy application.

We recommend enterprise customers to use GPOs in an Active Directory infrastructure where possible to ensure that security settings remain enforced or unchanged.

# Understanding the Zone Model

Internet Explorer offers administrators a unique security feature that is unavailable in most other browsers: the ability to define security settings for different Web site classes. Unlike most other browsers, Internet Explorer determines the level of security for a given Web page by categorizing it into a URL security zone based on the origin of the Web page.

The five security zones are **Local Machine** (not visible in the Internet Explorer user interface), **Internet**, **Local intranet**, **Trusted sites**, and **Restricted sites**. Web sites on the local computer are grouped into the Local Machine zone, remote servers are in the Internet security zone, and Web sites on a local network are grouped in the Intranet zone. Web sites on servers identified by the user or administrator as potentially malicious are placed in the Restricted sites zone. Web sites on servers identified by the user or administrator as trusted are grouped in the Trusted sites zone.

**Note:**   On computers that are not joined to a domain, the **Local intranet** zone is disabled, and the sites that would normally be accessed in this zone open in the **Internet** zone instead. The Local Machine zone is not visible in the Internet Explorer user interface.

Different levels of security are appropriate for each of these zones. To facilitate this, Internet Explorer uses URL security zone templates. Five templates are available by default: high, medium-high, medium, medium-low, and low. The security zones map to these URL templates to determine the security level as defined in the following table.

Table 1.1 Security Zone Mappings

| **Security zone** | **Security level (URL security zone template)** | **Description** |
| --- | --- | --- |
| Local Machine | Custom | Content found on the user's computer (except for content that Internet Explorer caches on the local system) is treated with a high level of trust. This zone cannot be configured in Internet Explorer. |
| Internet | Medium-High | The Internet zone consists of all Web sites that are not included in the other zones. |
| Local intranet (only available for domain-joined computers) | Medium-low | All sites in this zone should be inside the firewall, and proxy servers should be configured so that an external DNS name cannot be resolved to this zone. |
| Trusted sites | Medium | Sites in the Trusted sites zone are allowed to perform a wider range of operations than other Internet sites and prompt users to make fewer security decisions. External sites should only be added to this zone if you trust all of their content, and are assured they will never perform any harmful operations on your computers. |
| Restricted sites | High | This zone is designed to contain sites considered untrustworthy The default settings for this zone control and restrict Web features, but do not block access to the sites in this zone. Sites can be added by the user or enforced by Group Policy. |

In addition to these zones, there are corresponding locked-down zones that are not visible in the Internet Explorer user interface. The Lockdown\_Zones settings for the Local Machine zone are used by a feature introduced in Windows XP SP2 called "Local Machine Zone Lockdown" (LMZL). By default, when a page is opened in the Local Machine zone, it runs with the more restrictive settings in the Lockdown\_Zones. By default, the LMZL settings disable ActiveX and scripting. If the content in the page tries to use ActiveX or a script, the information bar prompts the user whether to allow them to run. If the user allows the blocked content, Internet Explorer then uses the less-restrictive, normal Local Machine zone settings from that point forward for the lifetime of that browser tab in Internet Explorer 7 and Internet Explorer 8, or the browser window in Internet Explorer 6. The other locked down zones are used for protocols specified in the **Network Protocol Lockdown** setting in Group Policy.

The setting values are stored in the registry in one of several locations, depending on how the setting is configured and whether it applies to users or the computer, as shown in the following table.

Table 1.2 Zone Setting Registry Paths

| **User setting** | **Computer setting** | **Configured via Group Policy** | **Configured locally via Internet Options** | **Path** |
| --- | --- | --- | --- | --- |
| ✓ |  |  | ✓ | HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones |
| ✓ |  | ✓ |  | HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Internet Explorer\Zones\ |
| ✓ |  | ✓ |  | HKEY\_CURRENT\_USER\Software\Policies\Microsoft\Internet Explorer\Lockdown\_Zones\ |
|  | ✓ |  | ✓ | HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Zones\ |
|  | ✓ | ✓ |  | HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\ Internet Settings\Zones\ |
|  | ✓ | ✓ |  | HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\CurrentVersion\ Internet Settings\LockdownZones\ |

There are subkeys in these locations that correspond to each security zone.

The subkeys are:

* 0 = Local Machine Zone
* 1 = Local Intranet Zone
* 2 = Trusted Sites Zone
* 3 = Internet Zone
* 4 = Restricted Sites Zone

The URL security zone templates specify which actions Web pages can perform. For example, the High URL Security Zone template specifies that Web pages cannot run or use ActiveX controls or scripting. By default, if a user visits a site in the **Restricted sites** zone, they cannot use this functionality. For more information about URL security zones and templates, see the MSDN® article "[About URL Security Zones](http://go.microsoft.com/fwlink/?LinkId=26003)."

## Modifying Zone Settings

There are three ways that users can modify zone settings in the **Internet Options** dialog box:

* Move the security zone slider on the **Security** tab to change which URL Security Zone template (security level) applies to the zone. For example, a user could change the security level for the Internet zone from Medium-High to Medium.
* Enter custom settings for a particular zone by clicking the **Custom Level** button on the **Security** tab.
* Add specific sites to a zone by clicking the **Sites** button on the **Security** tab. (This option is not available for the Internet zone, because that zone is for all sites not contained in the other zones.)

The behavior of the **Sites** button is different for the **Local intranet** zone. In this case, the **Sites** button allows you to determine if the intranet network is automatically detected (the default) or which criteria should be used. You can choose to include all local (intranet) sites not included in other zones, all sites that bypass the proxy server, and all Universal Naming Convention (UNC) network paths. It is still possible to add specific sites to the Local intranet zone by clicking the **Advanced** button in the settings dialog box. If you want to use Fully Qualified Domain Names (FQDN) to identify intranet sites, you must manually add these sites to the **Local intranet** zone. This is because Internet Explorer automatically assigns hosts that include dots, for example web.mydomain.com, to the **Internet** zone.

Often administrators want to restrict the ability of users to modify zone settings. For more information about how you can achieve this, see Chapter 2, "Security Recommendations."

## Zone Determination

While the basic concept of zone security permissions is easy to understand, the logic behind zone determination is often unexplained but useful to understand for effective computer management. The core of the determination process is based on input to the Address bar in Internet Explorer, not based on DNS IP value responses or netmask values. As a general rule, zone determination rules center around the user input to the Address bar. The following rules are used by default to determine the zone in which a site opens:

* Any sites listed in the **Restricted sites** zone open in that zone.
* Any sites listed in the **Trusted sites** zone open in that zone.
* Any sites listed in the **Local intranet** zone open in that zone.
* Sites that are on the proxy bypass list open in the **Local intranet** zone.
* Entries in the Address bar that do not include a period and can be resolved to a site open in the **Local intranet** zone (for example http://local).
* Other sites open in the **Internet** zone.

Note   It is not possible to add a site to more than one zone.

It is important to note that these rules sometimes mean that intranet sites open in the **Internet** zone. For example, if an intranet site is referred to by an IP address or a fully qualified domain name (FQDN), the site will open in the **Internet** zone, because the name includes periods.

## Beyond the Zone Model: General Security Settings

Internet Explorer 8 also includes security-related settings that are not zone-specific. These settings are found on the **Privacy**, **Content**, and **Advanced** tabs in the **Internet Options** dialog box that you can access from the **Tools** menu in the browser, and are discussed in more detail later in this guide.

# Security Design

The security design this chapter recommends forms the starting point for the scenarios in this guide, as well as the mitigation suggestions for the scenarios. The remaining sections in this chapter provide design details about the core security structure:

* **OU Design for Security Policies**
* **GPO Design for Security Policies**

Microsoft strongly recommends that you perform your own testing in a lab environment before deploying new security policies to production computers. The settings recommended in this guide and stored as security baselines in the SCM tool have been thoroughly tested. However, your organization’s network has unique business applications that may be impacted by some of these settings. Therefore, it is extremely important to thoroughly test the settings before implementing them on any production computers.

## OU Design for Security Policies

The Microsoft security guides for Windows, Office, and Internet Explorer use organizational units (OUs). An *OU* is a container within a domain that uses AD DS. An OU may contain users, groups, computers, and other OUs. If an OU contains other OUs, it is a parent OU. An OU within a parent OU is a child OU.

You can link a GPO to an OU, which will then apply the GPO's settings to the users and computers that are contained in that OU and its child OUs. And to facilitate administration, you can delegate administrative authority to each OU.

OUs provide an effective way to segment administrative boundaries for users and computers. Microsoft recommends that organizations assign users and computers to separate OUs, because some settings only apply to users and other settings only apply to computers.

You can delegate control over a group or an individual OU by using the Delegation Wizard in the Microsoft® Management Console (MMC) Active Directory Users and Computers snap-in tool. See the "More Information" section at the end of this chapter for links to documentation about how to delegate authority.

One of the primary goals of an OU design for any environment is to provide a foundation for a seamless Group Policy implementation that applies to all client computers in AD DS. This ensures that the client computers meet the security standards of your organization. The OU design must also provide an adequate structure to accommodate security settings for specific types of users in an organization. For example, developers may require access to their computers that average users do not. Also, laptop users may have different security requirements than desktop users.

The following figure illustrates a simple OU structure that is sufficient for the Group Policy discussion in this chapter. This OU structure may differ from the requirements of your organization's environment.

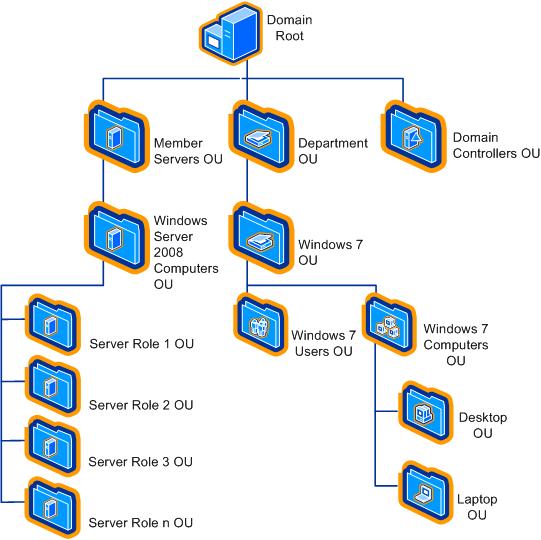


Figure 1.1 Example OU structure for computers running Windows 7 and Windows Server 2008

### Domain Root

You should apply some security settings throughout the domain to control how the domain, as a whole, is configured. These settings are contained in GPOs that apply to the domain. Computers and Users are not managed in this container.

### Domain Controllers OU

Domain controllers hold some of the most sensitive data in your organization — data that controls the security configuration itself. You apply GPOs at this level in the OU structure to configure and protect the domain controllers.

### Member Servers OU

This OU contains child OUs as described below. You should include settings that apply to all servers, but not to workstations, in the GPOs that you apply to this OU.

### Server Role OUs

Microsoft recommends creating an OU for each server role that your organization uses. Each OU should contain only one type of server computer. You can then configure GPO settings and apply them to OUs that are specific to each role.

You can also choose to combine certain roles on the same server, if your organization requires it. For example, you may choose to combine the File and Print server roles. In this case, you can create an OU for these combined server roles called "File and Print Server," and then link the two role-specific GPO policies to that OU.

**Important** Combining server roles on the same computer requires careful planning and testing to ensure that you do not negatively affect the overall security of the server roles that you combine.

### Department OU

Security requirements often vary within an organization. For this reason, it may make sense to create one or more department OUs in your environment. This OU enables you to apply security settings from GPOs to computers and users in their respective department OUs.

### Windows 7 Users OU

This OU contains the user accounts for the EC environment. The settings that you apply to this OU are described in detail in the Windows 7 Security Baseline Settings Excel workbook that accompanies this guide.

### Windows 7 Computers OU

This OU contains child OUs for each type of client computer running Windows 7 in the EC environment. This guide focuses on security guidance for desktop and laptop computers. For this reason, the engineers for this guide created the following computer OUs:

* **Desktop OU**. This OU contains desktop computers that constantly remain connected to the network. The settings applied to this OU are described in detail in the Windows 7 Security Baseline Settings Excel workbook.
* **Laptop OU**. This OU contains laptop computers for mobile users that are not always connected to the network. The Windows 7 Security Baseline Settings Excel workbook also provides details about the settings that apply to this OU.

## GPO Design for Security Policies

A *GPO* is a collection of Group Policy settings that are essentially the files created by the Group Policy snap-in. The settings are stored at the domain level and affect users and computers contained in sites, domains, and OUs.

You can use GPOs to ensure that specific policy settings, user rights, and computer behavior apply to all client computers or users in an OU. Using Group Policy instead of a manual configuration process makes it simple to manage and update changes for many computers and users. Manual configuration, which is inefficient because it requires a technician to visit each client computer, is also potentially ineffective. This is primarily because if the policy settings in domain-based GPOs are different than those applied locally, the domain-based GPO policy settings will overwrite the locally applied policy settings.

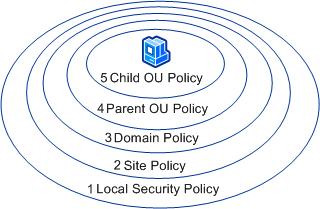


Figure 1.2 GPO order of precedence

The previous figure shows the order of precedence in which GPOs are applied to a computer that is a member of the Child OU, from the lowest priority (1) to the highest priority (5). Group Policy is applied first from the local security policy of each workstation. After the local security policy is applied, GPOs are next applied at the site level, and then at the domain level.

For computers running Windows Server 2008, Windows Server 2003 SP2 or later, and Windows Vista SP1 or Windows XP Professional SP3 or later that are nested in several OU layers, GPOs are applied in order from the parent OU level in the hierarchy to the lowest child OU level. The final GPO is applied from the OU that contains the computer account. This order of GPO processing for Group Policy—local security policy, site, domain, parent OU, and child OU—is significant because settings in GPOs that are applied later in the process will overwrite settings applied earlier. Different values for the same setting configured in different GPOs are never combined. User GPOs are applied in the same manner.

The following considerations apply when you design Group Policy:

* An administrator must set the order in which you link multiple GPOs to an OU, or Group Policy will be applied by default in the order it was linked to the OU, the order of precedence for the GPOs linked to the currently selected OU is shown in the **Link Order** list in the GPMC. If the same setting is configured in multiple policies, the policy that is highest on the policy list for the container will take precedence.
* You may configure a GPO with the **Enforced** option. However, if you select this option, other GPOs cannot override the settings that are configured in this GPO.
* Group Policy settings apply to users and computers, and are based on where the user or computer object is located in AD DS. In some cases, user objects may need policy applied to them based on the location of the computer object, not the location of the user object. The Group Policy loopback feature gives the administrator the ability to apply user Group Policy settings based on which computer the user is logged on to. The "[Loopback Processing of Group Policy](http://support.microsoft.com/Default.aspx?id=231287)" article provides more information about this option.
* You may configure an Active Directory site, domain, or OU with the **Block policy inheritance** option. This option blocks GPO settings from GPOs that are higher in the Active Directory hierarchy unless they have the **Enforced** option selected. In other words, the **Enforced** option has precedence over the **Block policy inheritance** option.

Note   Administrators should only use the Enforced option and the Block policy inheritance option with utmost care because enabling these options can make troubleshooting GPOs difficult and cumbersome.

### Recommended GPOs

To implement the OU design described above requires a minimum of the following GPOs:

* A policy for the domain.
* A policy to provide the baseline security settings for all domain controllers.
* A policy to provide the baseline security settings for all member servers.
* A policy for each server role in your organization.
* A policy for the Windows 7 Users OU.
* A policy for the Desktop OU.
* A policy for the Laptop OU.

The following figure expands on the preliminary OU structure to show the linkage between these GPOs and the OU design.

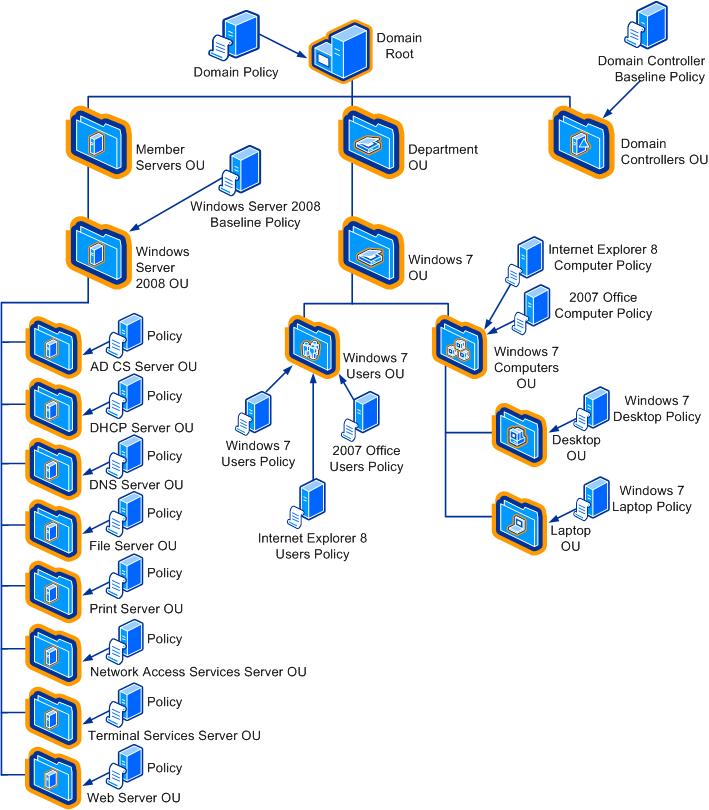


Figure 1.3 Example OU structure and GPO links for computers running Windows 7 and Windows Server 2008

While the guide you are reading only covers a single product from Microsoft, the previous figure illustrates an environment that combines recommendations from the following security guides available in the Security Compliance Management Toolkit Series:

* *Windows Server 2008 Security Guide*
* *Windows 7 Security Guide*
* *2007 Microsoft* *Office Security Guide*
* *Internet Explorer 8.0 Security Guide*

Presumably you network is running multiple versions of the Windows operating system and perhaps 2007 Office or Internet Explorer 2008. The combined example in the previous figure presents a notional AD DS design for OUs and Group Policy objects (GPOs). You will need to design your own OU hierarchy and Group Policy to fit the versions of Windows deployed in your environment, as well as settings for Microsoft Office or Internet Explorer as needed.

In the example in the previous figure, laptop computers are members of the Laptop OU. The first policy that is applied is the local security policy on the laptop computers. Because there is only one site in this example, no GPO is applied at the site level, which leaves the Domain GPO as the next policy that is applied. Finally, the Laptop GPO is applied.

Also in this figure, a File server is a member of the File Server OU. The first policy that is applied to the server is the local security policy. However, in general, little if any configuration of the servers is done by local policy. Security policies and settings should always be enforced by Group Policy.

Because there is only one File server in this example, no GPOs are applied at this level, which leaves the Domain GPO as the next policy that is applied to the servers. The Windows Server 2008 EC Baseline Policy is then applied to the Member Servers OU. Finally, any specific polices for the Web servers in the environment are applied to the Web Server OU.

As a precedence example, consider a scenario in which the policy setting for Allow logon through Terminal Services is set to apply to the following OUs and user groups:

* Member Servers OU – Administrators group
* Web Server OU – Remote Desktop Users and Administrators groups

In this example, logon through Terminal Services has been restricted to the Administrators group for servers in the Member Servers OU. However, a user whose account is in the Remote Desktop Users group can log on to a File server through Terminal Services because the File Servers OU is a child of the Member Servers OU and the child policy takes precedence.

If you enable the Enforced policy option in the GPO for the Member Servers OU, only users with accounts in the Administrators group can log on to the File server computer through Terminal Services. This is because the Enforced option prevents the child OU policy from overwriting the policy applied earlier in the process.

### Using a GPO Created with the Security Compliance Manager Tool

The specific setting recommendations presented in this guide are available as pre-built baselines in the SCM tool. You can use these baselines created by Microsoft "as is", however most organizations will require some customization. When a baseline reflects your organization’s requirements, use the SCM tool to generate a GPO backup file. For more information about using the SCM tool, review the information available in the Help Topics for the tool. You can then use the Group Policy Management Consol (GPMC) to import the settings from the backed-up GPOs into your AD DS domain.

**To import policy settings from a backed-up GPO into a GPO**

1. In the GPMC console tree, expand **Group Policy Objects** in the forest and domain containing the GPO into which you want to import policy settings.
2. Right-click the GPO into which you want to import policy settings, and then click **Import Settings**.
3. When the **Import Settings Wizard** opens, follow the instructions in the wizard that opens, and then click **Finish**.
4. After the import operation completes, a summary will state whether the import succeeded. Click **OK**.

#### Using migration tables

Because some data in a GPO is domain-specific and might not be valid when copied directly to another domain, the GPMC provides migration tables. A migration table is a simple table that specifies a mapping between a source value and a destination value.

A migration table converts, during the copy or import operation, the references in a GPO to new references that will work in the target domain. You can use migration tables to update security principals and UNC paths to new values as part of the import or copy operation. Migration tables are stored with the file name extension .migtable, and are actually XML files. You do not need to know XML to create or edit migration tables; the GPMC provides the MTE for manipulating migration tables.

A migration table consists of one or more mapping entries. Each mapping entry consists of a source type, source reference, and destination reference. If you specify a migration table when performing an import or copy operation, each reference to the source entry is replaced with the destination entry when the policy settings are written into the destination GPO. Before you use a migration table, ensure that the destination references specified in the migration table already exist.

The following items can contain security principals and can be modified by using a migration table:

* Security policy settings of the following types:
* User rights assignments.
* Restricted groups.
* System services.
* File system.
* Registry.
* Advanced folder redirection policy settings.
* The GPO Discretionary Access Control List (DACL), if it is preserved during a copy operation.
* The DACL on software installation objects, which is only preserved if the option to copy the GPO DACL is specified.

Also, the following items can contain UNC paths, which might need to be updated to new values as part of the import or copy operation, because servers in the original domain might not be accessible from the domain to which the GPO is being migrated:

* Folder redirection Group Policy settings.
* Software installation Group Policy settings.
* References to scripts, such as for logon and startup scripts, that are stored outside the source GPO. The script itself is not copied as part of the GPO copy or import operation, unless the script is stored inside the source GPO.

For more information about using the GPMC to import settings see the [Group Policy Planning and Deployment Guide](http://technet.microsoft.com/en-us/library/cc754948(WS.10).aspx).

# Security and Privacy Features in Internet Explorer 8

User safety, choice, and control are key themes in Internet Explorer 8, which includes many innovations that contribute to a more trustworthy Web browsing experience. This section introduces some of the security and privacy features and technologies offered in Internet Explorer 8 including:

* SmartScreen Filter
* Phishing and Malware Protection
* ClickJacking
* Cross-Site Scripting (XSS) Filter
* Domain Highlighting
* Internet Explorer Protected Mode
* ActiveX Opt-In
* InPrivate Browsing
* InPrivate Filtering

## SmartScreen Filter

Internet Explorer 8 includes the SmartScreen Filter, a core set of technologies designed to help protect users from evolving Web and social engineering exploits. The SmartScreen Filter expands on the functionality of the Phishing Filter in Internet Explorer 7.

The SmartScreen Filter helps protect users against known phishing and malware sites as they browse the Internet. In addition, the SmartScreen Filter includes protection from *ClickJacking*, a technique attackers can use to capture keystrokes, steal user credentials, deface Web pages, or launch other types of malicious attacks. The SmartScreen Filter also includes the new Cross-Site Scripting Filter (XSS), which helps to prevent against type-1 cross-site scripting attacks.

### Phishing and Malware Protection

*Phishing* is a technique that many attackers use to trick computer users into revealing personal or financial information through an e-mail message or Web site. *Phishers* masquerade as a legitimate person or business to deceive people into revealing personal information, such as account passwords and credit card numbers. The SmartScreen Filter in Internet Explorer 8 advises users about suspicious or known phishing Web sites to help them more safely browse content on the Internet. The filter analyzes Web site content for known phishing techniques, and uses a global network of data sources to assess the trustworthiness of Web sites. In addition, the SmartScreen Filter provides dynamic protection against malicious software threats, helping protect users from sites known to distribute or contain malicious software and from malicious downloads.

The SmartScreen Filter incorporates a range of technologies and a frequently updated online service, consolidates the latest industry information about fraudulent Web sites, and uses it to help proactively warn and protect customers running Internet Explorer 8.

The SmartScreen Filter combines client-side Web page scans for suspicious Web site characteristics with an opt-in online service. The filter is designed to help protect users from phishing scams and malware sites in three ways:

* Comparing the addresses of known and trusted Web sites that a user attempts to visit with a list of known high-traffic sites stored on the user’s computer. If the site is found in the list, no further checks are performed.
* Analyzing Web sites that users want to visit by checking them for characteristics that are common to phishing sites.
* Sending the Web site address that a user attempts to visit to an online service that Microsoft maintains, which then immediately checks the address against a frequently updated list of phishing and malware sites. These sites have been confirmed by reputable sources as fraudulent or malicious and reported to Microsoft.

Note   The online service is contacted asynchronously over an SSL connection, allowing pages to load and not impact user experience. If the service cannot be contacted, the page renders normally, and a message balloon appears in the status bar indicating that the service cannot be contacted.

Note   You can use Internet Explorer to analyze a Web site to determine whether or not it is likely to be a phishing site at any time by clicking the **Safety** button, pointing to **SmartScreen Filter**, and then clicking **Check This Website**.

To help ensure user privacy, the SmartScreen Filter prompts the user to choose whether to enable or disable the feature — it is not set either way by default. You can remove this choice by disabling the first run experience or using the IEAK to build a custom package for your organization. To properly use the SmartScreen Filter protections, we recommend organizations to configure systems to both automatically enable SmartScreen and prevent users from disabling the SmartScreen Filter. In addition, we recommend removing the **Click to Continue** option that appears on SmartScreen warning screens, which is triggered when the SmartScreen Filter identifies a phishing and malware related Web site. For more information about locking down Internet Explorer to prevent users from disabling the SmartScreen Filter, and stopping users from ignoring the warning screens, see Chapter 3, "Privacy Setting Recommendations."

### ClickJacking

*ClickJacking* occurs when an attacker’s Web page entices the user to click on content delivered from another domain (or from a native security prompt) without the user realizing it. ClickJacking renders most anti-CSRF (cross-site request forgery) mitigations defenseless, and attackers can use it to reconfigure certain browser add-ons in unsafe ways.

The SmartScreen Filter now includes a new security feature designed to help detect and prevent ClickJacking. This feature is part of the Internet Explorer 8 codebase, so it is always enabled and cannot be disabled.

Attackers show a set of dummy buttons, and then load another page over it in a transparent layer. Users think they are clicking the visible buttons, while they are actually performing actions on the hidden page. The hidden page may be an authentic page, and therefore the attackers can trick users into performing actions that they never intended to do. There also is no way to trace such actions later, because users genuinely authenticated themselves on the other page.

For sites to take advantage of the added protection from ClickJacking exploits, they need to add an X-FRAME-OPTIONS tag in either the HTTP header or the HTTP EQUIV meta tag. For more information about ClickJacking, see the [IE8 Security Part VII: ClickJacking Defenses](http://blogs.msdn.com/ie/archive/2009/01/27/ie8-security-part-vii-clickjacking-defenses.aspx) blog.

### Cross-Site Scripting (XSS) Filter

The new Cross-Site Scripting (XSS) Filter in the SmartScreen Filter helps protect users from certain types of server-side application vulnerability attacks. These attacks are known as Type 1, or reflected attacks, and they are among the most common types of cross-site scripting attacks. They occur when code, usually in the form of a script, is passed to a Web server and then reflected back to the user. For example, when information sent from the Web browser is used immediately by server-side scripts to generate a page for the user. If the data input is invalidated, that user-supplied data could be included in the resulting page without HTML encoding, allowing the client-side code to be reflected back into the page sent to the user.

The XSS Filter helps protect users from this type of attack by analyzing the user data input returned to them. By analyzing the data stream, Internet Explorer 8 can identify certain actions that do not appear to have a valid usage scenario and then stop the offending script from running to help protect the user. For more information about managing the XSS Filter setting, see Chapter 2, "Security Recommendations."

Note   Clickjacking and XSS protections are enabled by default. ClickJacking support is part of the browser's defense in depth design and cannot be disabled. However, users can disable the XSS Filter. Users also can enable the SmartScreen Filter for protection from phishing and malware as outlined above.

## Domain Highlighting

Perhaps the most visible change in the Address Bar of Internet Explorer 8 is the *Domain Highlighting* feature. Internet Explorer 8 automatically highlights what it considers to be the owning domain of whatever site user’s view. This helps users to identify the real source of a site when a Web site attempts to deceive them. This new feature is part of the overall Enhanced Address Bar in Internet Explorer 8 that provides users with clearer, more prominent visual cues about the identity of Web sites and the encryption that they use. Domain highlighting is always enabled (it cannot be disabled), and is visible with all other address bar warnings and notifications, including the presence of an Extended Validation (EV) SSL certificate and the warning for phishing sites. For more information about EV SSL Certificates, see the [Internet Explorer and Business Value of Extended Validation SSL certificates](http://www.microsoft.com/ie/ev) page of the Windows Internet Explorer Web site.

## Internet Explorer Protected Mode

Internet Explorer Protected Mode is available in computers running Internet Explorer 7 or Internet Explorer 8 for the following operating systems: Windows 7 and Windows Vista. The *Protected Mode* feature adds additional defenses by limiting application access to only certain areas of the file system and registry. In addition, Protected Mode helps to prevent malicious code from taking over a user’s browser and executing code through elevated privileges.

Protected Mode helps reduce previous software vulnerabilities in extensions for the browser by eliminating the possibility of using them for the silent installation of malicious code. The feature uses mechanisms with higher integrity levels than in Windows 7 and Windows Vista that restrict access to processes, files, and registry keys to accomplish this goal. The Protected Mode application programming interface (API) enables software vendors to develop extensions and add-ons for Internet Explorer that can interact with the file system and registry while the browser is in Protected Mode.

When in Protected Mode, Internet Explorer 8 runs with reduced permissions to help prevent user or system files or settings from changing without the user’s explicit permission. Protected Mode also is now more user-friendly than it was in Internet Explorer 7 when combined with the new *Loosely Coupled Internet Explorer (LCIE)* design. In general, LCIE separates the frame and window processes used in Internet Explorer, allowing Protected Mode tabbed windows to appear side by side with content on other pages not subject to Protected Mode. This enhancement eliminates the need for the "broker" process used by Internet Explorer 7, and instead passes all functions that require elevation to the frame process.

Protected Mode is enabled by default for all users, except when a user is logged on to the built-in Administrator account. Other accounts with administrator permissions run in Protected Mode by default. You can disable Protected Mode by using either the launch option or in a registry/GPO configuration. Starting Internet Explorer 8 on computers running Windows 7 or Windows Vista without Protected Mode requires the user to right-click the Internet Explorer icon, click **Run as Administrator**, type valid higher permission authentication credentials, and then press ENTER.

Protected Mode is enabled by default in Internet Explorer 8 for the **Internet** and **Restricted sites** security zones. However, users can disable the mode, which reduces overall security.

## ActiveX Opt-in

Internet Explorer 7 introduced the ActiveX Opt-in mechanism to automatically disable all controls that are not explicitly allowed by the user, helping to mitigate the potential misuse of preinstalled controls. Internet Explorer 8 extends the security protection of that feature by increasing the ability to fine tune the ActiveX Opt-in settings to a Per-User and Per-Domain level. This added control helps to further ensure users and their systems are protected against malicious attack.

The Information bar in Internet Explorer prompts users before they can access a previously installed ActiveX control that has not yet been used on the Internet. This notification mechanism enables the user to permit or deny access on a control-by-control, site-by-site basis, which helps further reduces the available surface area for attacks. Malicious users cannot use Web sites to launch automated attacks with ActiveX controls that were never intended to be used on the Internet. The added Per-User setting control helps extend that protection by limiting any approved control to only the specific user, helping to minimize the impact on other users. Per-Domain settings help ensure controls are limited to the specific Web site or sites that users intend to access, and leave other domains unable to use the same control without explicit action from the user.

## InPrivate Browsing

InPrivate Browsing lets you control whether or not Internet Explorer 8 saves your browsing history, cookies, and other data. If you are using a shared PC, a borrowed laptop from a friend, or a public PC, sometimes you do not want other people to know where you have been on the Web. The InPrivate Browsing feature in Internet Explorer 8 makes ensure browser privacy easy by not storing history, cookies, temporary Internet files, or other data.

While InPrivate Browsing is active, the following takes place:

* Browser Helper Objects (BHOs) and Toolbars are disabled.
* New cookies are not stored.
* If a Web site attempts to create a persistent cookie, that cookie is created as a session cookie and deleted after the browser session is closed.
* Existing persistent cookies are not sent or read.
* The new DOM storage feature behaves the same way.
* New history entries are not recorded.
* New temporary Internet files are deleted after the Private Browsing window is closed.
* Form data is not stored.
* Passwords are not stored.
* Addresses typed into the address bar are not stored.
* Queries entered into the search box are not stored.

In addition, toolbars and BHOs are disabled by default. Users can enable this functionality on the **Privacy Options** tab of the **Internet Options** dialog box that you can access from the **Tools** menu in the browser.

## InPrivate Filtering

The InPrivate Filtering feature provides users with added control over third-party sites with which they want to share personal browsing activity. Web sites increasingly access content from multiple sources, providing tremendous value to consumers and Web sites. However, users are often not aware that some content, images, ads, and analytics are provided from third-party Web sites or that these sites have the ability to potentially track (by data aggregation correlation) individual user behavior across multiple Web sites. InPrivate Filtering provides users an added level of control and choice about the information that third-party Web sites can potentially use to track browsing activity.

Note   For an in-depth overview of this feature and user settings, see the [*Internet Explorer 8 Privacy and User Control Feature Guide*](http://download.microsoft.com/download/D/5/6/D562FBD1-B072-47F9-8522-AF2B8F786015/IE8%20Privacy%20and%20User%20Control-RC1%20Final.pdf).

# More Information

The following resources provide additional information about Internet Explorer 8 security-related topics on Microsoft.com:

* [About URL Security Zones](http://go.microsoft.com/fwlink/?LinkId=26003).
* [Back Up, Restore, Copy, and Import](http://technet.microsoft.com/en-us/library/cc759276(WS.10).aspx) page on the Windows Server TechCenter.
* [IE8 Security Part VII: ClickJacking Defenses](http://blogs.msdn.com/ie/archive/2009/01/27/ie8-security-part-vii-clickjacking-defenses.aspx) blog.
* [*Internet Explorer 8 Privacy and User Control Feature Guide*](http://download.microsoft.com/download/D/5/6/D562FBD1-B072-47F9-8522-AF2B8F786015/IE8%20Privacy%20and%20User%20Control-RC1%20Final.pdf).
* [*Internet Explorer Administration Kit (IEAK) 8*](http://technet.microsoft.com/en-us/ie/bb219517.aspx).
* [Internet Explorer and Business Value of Extended Validation SSL certificates](http://www.microsoft.com/ie/ev) page of the Windows Internet Explorer Web site.
* [Internet Explorer TechCenter](http://technet.microsoft.com/ie).
* "[Loopback Processing of Group Policy](http://support.microsoft.com/Default.aspx?id=231287)" article.
* [Microsoft Technical Security Notifications](http://go.microsoft.com/fwlink/?LinkId=21163).
* [Remote Server Administration Tools for Windows 7](http://go.microsoft.com/fwlink/?LinkId=130862).

Chapter 2: Security Recommendations

Increasing security in the default settings in Windows® Internet Explorer® 8 requires more than simply changing one setting to another on the **Security** tab of the **Internet Options** dialog box, or moving the security level slider of each security zone on this tab to **High**. Dramatic security changes like these prevent most navigation for users and effectively render the browser useless. This section discusses a variety of changes organizations can make to Internet Explorer 8 on the computers in their environment to increase general browser security without drastically affecting the functionality of the browser.

The Internet Explorer 8 security setting and feature recommendations in this chapter are grouped into six categories:

* Manage Add-ons
* Disable Active Scripting
* Zone Security
* Certificate Security
* Reducing Application Privilege
* Other Security Settings

For a checklist of all the settings that we recommend to consider implementing, see Appendix A, "Security Checklist" at the end of this guide. Each setting and feature recommendation is explained in more detail in this chapter.

Note   In addition to configuring the settings discussed in this chapter, you may also want to use Group Policy to prevent some of the tabs, such as the **Connections** and **Advanced** tabs, in the **Internet Options** dialog box from displaying. However, even if you remove these tabs, you should also enforce individual settings to prevent users from making changes through edits to the local registry.

# Manage Add-ons

Microsoft introduced the ActiveX® platform to provide Web developers with the ability to extend applications and functionality beyond the default capabilities of the browser. Using the ActiveX platform, developers have built rich, interactive applications and integrated data from nearly any source. Although the ActiveX platform is designed with security in mind, and features such as Authenticode® help ensure code security, it is crucial that users follow guidelines to maintain browser safety for this add-on. Internet Explorer 8 allows for controlling these extension features in the Manage Add-ons interface of the browser. This section provides security recommendations for ActiveX controls and other active content.

## Restrict ActiveX Controls

Users often choose to install software such as ActiveX controls that are not permitted by the security policies of their organizations. This software can pose significant security and privacy risks to networks. To prevent users from installing unauthorized ActiveX controls, we recommend using Group Policy to block ActiveX control installation prompts for Internet Explorer Processes, which prevents users from installing ActiveX controls from Internet Explorer. It is important to note that this restriction also includes legitimate ActiveX controls that may provide critical business functionality, such as Windows Update. If you do restrict ActiveX installations, ensure to also use a mechanism such as Group Policy to push any required ActiveX controls to user desktops. For more information about this recommendation, see the next section. Using this restriction also requires an alternative way to provide security updates, such as Windows Server® Update Services (WSUS).

The following table includes the policy object name, and its location in Group Policy.

Table 2.1 Restrict ActiveX Install Settings

| **Policy object** | **Location** |
| --- | --- |
| Internet Explorer Processes (Restrict ActiveX Install) | Computer Configuration\Administrative Templates\ Windows Components  \Internet Explorer\Security Features\Restrict ActiveX Install |

## Control Per-Site ActiveX Settings

Internet Explorer 8 provides administrators with the ability to manage ActiveX controls on a per-site basis, which helps to ensure that ActiveX controls can only run on sites where they are approved for use.

IT professionals administering a system of computers running Internet Explorer 8 may choose to preset allowed controls and their associated domains. You can implement and enforce such settings using Active Directory and Group Policy. Allowed domains and controls are stored in the HKEY\_CURRENT\_USER hive at the following location in the registry:

**HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Ext\Stats\{CLSID} \iexplore\AllowedDomains\{Domain or \*}**

{CLSID} represents the Class ID of a control in question, and {Domain or \*} represents the domains allowed to run the specified control (where \* represents all domains).

Accepted values are:

* REG\_DWORD Blocked
* REG\_DWORD Count
* REG\_DWORD Flags
* REG\_DWORD Binary
* REG\_DWORD Type

## Use ActiveX Controls, Plug-ins, and Pre-approved Lists

The previous setting ensures that ActiveX controls cannot run on a client computer unless they are pre-approved by the organization. However, some organizations find this setting too restrictive. If this is the case for your organization, ensure that at a minimum, the setting **Allow previously unused ActiveX controls to run without prompt** is disabled for the **Internet** and **Restricted sites** zones, which is the default configuration in the browser. This setting, otherwise known as ActiveX Opt-In, ensures that controls operate as intended and systems are not attacked by users simply visiting a Web site. However, one of the tradeoffs associated with the ActiveX Opt-In feature is that users may visit well known or harmless sites that do not work as intended without users approving a control.

No matter how you restrict ActiveX installation, there is the potential of impacting business critical functionality. Therefore, we recommend pushing a list of pre-approved controls out to the user computers that you manage with a feature such as Group Policy, and adding them to the pre-approved list for Windows by adding the CLSID (the globally unique identifier that identifies a COM class object) of the control to the following registry location:

**HKEY\_LOCAL\_MACHINE \SOFTWARE\Microsoft\Windows\CurrentVersion\Ext\PreApproved**

Note   If an ActiveX control contains a security vulnerability that presents a danger to users, Microsoft may disable the control through a security update distributed by Windows Update, Microsoft Update or Windows Server Update Services. In such cases, these services disable the control even if the control is on a pre-approved list.

Installed controls can be enabled or disabled by changing their registry flags, using the globally unique identifier (GUID) key identifier. If you do not already have a catalog of GUIDs that your organization uses, identifying them is an important process to establish. One way to create your GUID list is to build a new computer, manually configure and enable your line-of-business applications, and then review the GUIDs in the Internet Explorer registry branch. That list can serve to provide you with the least number of controls required for your environment. You can then use this list of GUIDs to populate the pre-approved list.

We recommend using GPOs to manage an internal approved list for controls to increase the security and effectiveness of the ActiveX Opt-In feature. For more information about ActiveX security and best practices for managing ActiveX controls in your organization, see the [ActiveX Security: Improvements and Best Practices](http://go.microsoft.com/fwlink/?linkid=131978) on MSDN®.

# Disable Active Scripting

Microsoft introduced the Security Design Lifecycle (SDL) in 2002 to help increase software security quality and reduce the impact of vulnerabilities. While the SDL has proven to be effective, significantly reducing vulnerabilities and exploits, no software or process is perfect. The added functionality of Web 2.0 brings added security risks. While developing secure code is essential, so is the requirement to include a response plan in the event of future compromise or vulnerability. There are times when a vulnerability is exploited before it is responsibly disclosed. This is known as a *zero day* vulnerability.

Other times a vulnerability is disclosed properly, but the update to mitigate it requires time to develop and properly test before it can be released. To help reduce potential exposure, advise users to avoid unknown Web sites and exercise caution before clicking links. Administrators can also use the **Allow Active Scripting** setting to protect against a discovered vulnerability that does not yet have an update to address it. We recommend using Group Policy to change this setting to **Disable** for response to zero day attacks or other critical security scripting attacks. However, under normally conditions this setting should be configured to **Enable** to ensure proper Web site function and reduce user experience issues.

You can review and configure the **Allow Active Scripting** setting in the following location in the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components**

**\Internet Explorer\Internet Control Panel\Security Page\<*zone*>**

The following table provides security setting information specific to this technology in Internet Explorer 8.

Table 2.2 Allow Active Scripting Setting

| **Policy object** | **Description** |
| --- | --- |
| Allow Active Scripting | This setting allows you to manage whether script code on pages in the *<zone>* is run.  By default script code on pages in the *<zone>* can run automatically |

### Support for Scripting

Internet Explorer includes support for client-side scripting. These are computer programs on the Web that are executed in the user’s Web browser. Embedded scripts are a common type of client-side scripts that are interspersed within an HTML document. Another type of client-side script is called an external script. These are separate files that are referenced by the documents that use them. Internet Explorer 8 has built-in support for several scripting languages, including VBScript, JScript®, and ECMAScript.

Client-side scripting is a powerful capability of Web browsers because it allows the viewer to see content that dynamically changes based on a variety of conditions, such as the version of the browser, the time of day, or the user’s logon credentials. Enabling such power involves risks though, and because the script originates on the Web server, you should only allow this type of dynamic content to execute locally when the Web server is trustworthy. Recommendations for reducing the risk of client-side scripting are included in this and later sections.

Note   This section discusses client-side scripts. Do not confuse them with server-side scripts. Web server software, such as Internet Information Services (IIS), typically support server-side scripts written in languages like VBScript, JScript, and Perl. The results of server-side scripts are delivered as standard HTML content, and they generally do not expose users to the same level of risk as client-side scripts.

## Enable Scripted Window Security Restrictions

Internet Explorer allows scripts to programmatically open, resize, and reposition windows of various types. This allows popup windows to appear, and provides the potential for scripts to display windows in which the title and status bars are not visible to the user or obfuscate the title and status bars of other windows. We recommend using Group Policy to prevent these scripts from running in Internet Explorer and Windows Explorer processes.

You can review and configure the Scripted Window Security Restrictions setting in the following location in the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Security Features\Scripted Window Security Restrictions**

The following table provides security setting information specific to this technology in Internet Explorer 8.

Table 2.3 Scripted Window Security Restrictions Setting

| **Policy object** | **Description** |
| --- | --- |
| All Processes | If you enable this policy setting, scripted windows are restricted for all processes.  By default, scripted windows are not restricted in the browser. |

# Zone Security

Most of the security-related settings in Internet Explorer are contained in the security zones. By default, users can make changes to these zones by altering the security level assigned to each zone, creating custom settings for each zone, and by adding sites to the **Local intranet**, **Trusted sites**, and **Restricted sites** zones. In most organization environments, we recommend for administrators to use Group Policy to lock down zone security, and prevent users from making many of these changes. The following sections discuss how to increase zone security in Internet Explorer 8.

## Enable Zone Elevation Protection

Internet Explorer places restrictions on each Web page that it opens. These restrictions depend on the location of the Web page, such as whether the page opens in the **Internet** zone, **Local intranet** zone, or **Local Machine** zone. Web pages on a local computer have the fewest security restrictions and reside in the **Local Machine** zone, which makes this zone a prime target for malicious attackers.

If you enable the **Internet Explorer Processes** zone elevation protection setting, Internet Explorer processes can protect any zone from zone elevation. This approach helps prevent content that runs in one zone from gaining elevated privileges from another zone. If you disable this policy setting, no zone receives such protection for Internet Explorer processes.

Because of the severity and relative frequency of zone elevation attacks, we recommend configuring the **Internet Explorer Processes** zone elevation protection setting to **Enabled**.

You can review and configure the Zone Elevation Protection settings in the following location in the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Security Features\Protection From Zone Elevation**

The following table provides security setting information specific to this technology in Internet Explorer 8.

Table 2.4 Zone Elevation Protection Setting

| **Policy object** | **Description** |
| --- | --- |
| Internet Explorer Processes | Internet Explorer places restrictions on each Web page it opens. The restrictions depend on the location of the Web page (Internet, Intranet, Local Machine zone, and so on.). Web pages on the local computer have the fewest security restrictions and reside in the Local Machine zone, making the Local Machine security zone a prime target for malicious users. Zone Elevation also disables JavaScript navigation if there is no security context.  If you enable this policy setting, any zone can be protected from zone elevation by Internet Explorer processes.  If you disable this policy setting, no zone receives such protection for Internet Explorer processes.  If you do not configure this policy setting, any zone can be protected from zone elevation by Internet Explorer processes. |

## Do Not Allow Users to Add or Delete Sites from Zones

By default users can add and delete sites from the **Local intranet**, **Trusted sites** and **Restricted sites** zones. Adding a site to the **Trusted sites** zone, or removing one from the **Restricted sites** zone, could potentially cause malicious code to run on a computer.

We recommend using Group Policy to prevent users from adding or deleting sites from security zones. Using Group Policy to enable the **Do not allow users to add/delete sites** setting also prevents users from altering settings in the Local intranet zone.

You can review and configure this setting in the following location in the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer**

The following table provides security setting information specific to this technology in Internet Explorer 8.

Table 2.5 Do Not Allow Users to Add/Delete Sites Setting

| **Policy object** | **Description** |
| --- | --- |
| Security Zones: Do not allow users to add/delete sites | This setting prevents users from adding or removing sites from security zones.  If you disable this setting or do not configure it, users can add Web sites or remove sites from the **Trusted sites** and **Restricted sites** zones, and alter settings for the **Local intranet** zone. |

Although we recommend enabling this setting, it can have an impact on user productivity, particularly when combined with additional restrictions to the Internet zone. In some cases, users may add sites to a less restricted zone when they cannot access the site in the Internet zone. If this capability is disabled, users may be unable to access some Web sites until an administrator adds the site to a less restrictive zone on their behalf.

Note   If you enable the **Disable the Security page** setting (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), the **Security** tab is removed from the interface, and the **Disable** setting option takes precedence over this security zone setting.

## Do Not Allow Users to Change Zone Policies

By default, users can change the security level for each zone by moving the zone slider on the **Security** tab in the **Internet Options** dialog box. Users can also create custom settings for each zone. These options allow users to change any settings, potentially lowering security, and allowing malicious code to run.

We recommend using Group Policy to prevent users from changing the security level or modifying the security level of any zones by enabling the **Do not allow users to change policies** setting.

You can review and configure these settings in the following location in the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer**

The following table provides security setting information specific to this technology in Internet Explorer 8.

Table 2.6 Do Not Allow Users to Change Policies Setting

| **Policy object** | **Description** |
| --- | --- |
| Security Zones: Do not allow users to change policies | This setting prevents users from changing security zone settings.  If you disable this setting or do not configure it, users can change the settings for security zones. |

Note   If you enable the **Disable the Security page** setting (located in \User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel), the **Security** tab is removed from the interface, and the **Disable** setting option takes precedence over this security zone setting.

# Certificate Security

Secure communications between the browser and server require using certificates and SSL or Transport Layer Security (TLS) technology. Internet Explorer 8 supports SSL and TLS, and the browser attempts to make users more aware of security issues or errors, such as "expired" or "name mismatch" on certificates. The default setting for Internet Explorer 8 is to show the user a full screen, and a red colored certificate error warning advising to use caution before proceeding. The user can select an option to continue navigation. There are many valid reasons why a certificate contains errors, but publicly accessible well-maintained Web sites should not generate certificates with errors. This feature setting allows administrators to prevent users from "clicking through" a certificate warning, which helps to reduce the potential for malicious attack.

## Prevent Users from Accessing Sites with Certificate Errors

Over time certificates may be revoked or expire. In other cases, the wrong certificate may be used for a particular Web page or the site address may not match the address specified in the certificate. By default, users are warned of certificate errors and allowed to continue navigating to the Web page. The problem is that anyone can create a self-signed certificate that claims to be for a legitimate Web site address, and build a site that mimics the legitimate one. Internet Explorer displays a warning message when it detects a certificate not issued by a trusted certificate authority. However, users who have become accustomed to clicking through error and warning messages without considering their importance can be easily tricked into visiting a malicious site. Although a revoked or expired certificate is not a security issue in its own right, it can be an indication that a site should no longer be trusted. Therefore, we recommend using Group Policy to enable the **Prevent Ignoring Certificate Errors** setting to prevent users from navigating to sites that display certificate errors.

Enabling this policy object will not cause performance issues, but may result in additional support requests from users unable to visit particular sites. Because sites listed in the **Trusted sites** zone are not affected by this setting, if a business critical site contains a certificate that has expired or has a name mismatch, you can add this site to the **Trusted sites** zone as a temporary workaround until the correct certificate is in place.

You can review and configure this setting in the following location in the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel**

The following table provides security setting information specific to this technology in Internet Explorer 8.

Table 2.7 Prevent Ignoring Certificate Errors Setting

| **Policy object** | **Description** |
| --- | --- |
| Prevent Ignoring Certificate Errors | Internet Explorer treats as fatal any SSL/TLS certificate errors that interrupt navigation, such as "expired," "revoked," or "name mismatch" errors.  If you disable this setting or do not configure it, the user may elect to ignore certificate errors and continue navigation.  We recommend enabling this setting, so users are not permitted to continue navigating to sites with invalid or untrusted certificates. |

# Reduced Application Privilege

One way to help keep the client computers in your organization secure is to reduce potential exposure. Security experts frequently remind users to log on to the system with the least possible privilege and increase it only when necessary. Internet Explorer® 8 for Windows® 7 and Windows Vista® enables users to easily follow this advice with the new *Protected Mode* feature. Internet Explorer 8® for Windows® XP provides users with valuable protections that they can take advantage of using the DropMyRights application. For more information, see [Applying the Principle of Least Privilege to User Accounts on Windows XP](http://technet.microsoft.com/en-us/library/bb456992.aspx). While each solution operates differently, they both help users to reduce the potential impact of an elevation of privilege attack. Therefore, we recommend using the solution that is appropriate for your operating system. The following sections discuss each solution.

## Turn On Protected Mode

Protected Mode is enabled by default in Internet Explorer 8 for Windows Vista and Windows 7 in the **Internet** and **Restricted sites** security zones. This feature is designed to provide enhanced user and system protection by limiting the ability of the application to access areas of the file system and registry. These limitations are designed to help isolate the Internet Explorer process, and limit the ability for a malicious Web site or other software from using the browser to damage user information or harm the system. However, users can disable the mode, which reduces overall security. For these reasons, we recommend using Group Policy to ensure that Protected Mode is enabled in the **Internet** and **Restricted sites** zones, and to prevent users from disabling the feature.

You can review and configure this setting in the following location in the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\<*zone*>**

The following table provides security setting information specific to this technology in Internet Explorer 8.

Table 2.8 Turn On Protected Mode Setting

| **Policy object** | **Description** |
| --- | --- |
| Turn on Protected Mode | This setting protects Internet Explorer from vulnerabilities by reducing the locations that Internet Explorer can write to in the registry and the file system.  By default Protected Mode is on, but users can turn it off. |

This setting only applies to Internet Explorer 8 for Windows 7 and Windows Vista. Also, this setting does not apply to Internet Explorer 8 if you run the setting via Windows XP Mode on a computer running Windows 7.

Protected Mode is available for the following security areas and zones in Internet Explorer 8:

* Internet
* Intranet
* Local Machine
* Locked-down Internet
* Locked-down intranet
* Locked-down Local Machine
* Locked-down Restricted sites
* Locked-down Trusted sites
* Restricted sites
* Trusted sites

Note   If a business critical Web site or Web application is prevented from running properly due to an issue with Protected Mode, do not disable protected mode, as doing so will lower overall security in the browser. Instead, contact the site owner to ensure that the owner updates the site to work correctly in Protected Mode. As a temporary workaround, you can add the site to the **Trusted sites** zone.

## Use DropMyRights in Windows XP

DropMyRights is a simple application to help users who must run their computers as an administrator in order to run applications in a much safer context as a nonadministrator. While it is more secure to run a computer as a standard user rather than as an administrator, when you have no alternative you can use this application on computers that run Internet Explorer 8 for Windows XP, because these computers cannot take advantage of Protected Mode.

DropMyRights takes the current user's token, removes various privileges and security identifiers (SIDs) from the token, and then uses the token to start another process. For more information about DropMyRights and to download the source code for this application, see [Browsing the Web and Reading E-mail Safely as an Administrator](http://msdn2.microsoft.com/en-us/library/ms972827.aspx) on MSDN. Once installed, starting Internet Explorer with DropMyRights requires simply creating a new shortcut that points to the DropMyRights executable file, followed by establishing a path to the application that you want to run with lower privilege.

# Other Security Settings

In addition to the security settings discussed in the other chapters of this guide, there are other security options that you can use to help secure the computers in your environment. This section looks at some of these other option and feature settings, and provides recommendations on how you can adjust their default values to increase security in Internet Explorer 8 for users.

## MIME Sniffing Safety Feature

This feature helps to prevent promotion of a file of one type to a more dangerous file type. You can review and configure this setting in the following location in the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Security Features\MIME Sniffing Safety Feature**

The following table lists the settings that are available for this feature.

Table 2.9 MIME Sniffing Safety Feature Settings

| **Policy object** | **Description** |
| --- | --- |
| All Processes | If you configure this setting to **Enabled**, the MIME Sniffing Safety Feature is enabled for all processes. |
| Internet Explorer Processes | If you configure this setting to **Disabled**, Internet Explorer processes allow a MIME sniff promoting a file of one type to a more dangerous file type.  The default (**Not** **configured**) behavior does not allow promotion. ‡ |
| Process List | This policy setting allows administrators to define applications on which they want to prevent or not allow this security feature to run. |

This table provides a simple description for each setting. For more information about a specific setting, see the **Explain** tab of the setting in the Group Policy Object Editor.

## MK Protocol Security Restriction

The MK Protocol Security Restriction policy setting reduces attack surface area by blocking the MK protocol. If this setting is enabled the resources hosted on the MK protocol fail. The MK protocol is an obsolete mechanism for linking Windows Help files to Web pages. You can review and configure this setting in the following location in the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Security Features\MK Protocol Security Restriction**

The following table lists the settings that are available for this feature.

Table 2.10 MK Protocol Security Restriction Settings

| **Policy object** | **Description** |
| --- | --- |
| All Processes | By default this restriction is disabled for all processes. However, if you configure this setting to **Enabled**, the MK Protocol is blocked for all processes and any use of the MK Protocol is blocked. |
| Internet Explorer Processes | If you configure this setting to **Disabled**, applications can use the MK protocol API and resources hosted on the MK protocol will work for the Windows Explorer and Internet Explorer processes.  The default setting prevents the MK Protocol for Windows Explorer and Internet Explorer, and resources hosted on the MK protocol are blocked. ‡ |
| Process List | This policy setting allows administrators to define applications for which they want this security feature to be prevented or allowed. |

This table provides a simple description for each setting. For more information about a specific setting, see the **Explain** tab of the setting in the Group Policy Object Editor.

## Do Not Save Encrypted Pages to Disk

To increase the usability of the browsing experience, Internet Explorer can cache content in a local store (Temporary Internet Files) for immediate local retrieval rather than incur potential delays when repeatedly accessing the network for the same resource. Internet Explorer offers the option to cache both encrypted and unencrypted content, and by default both content types are cached.

Although caching encrypted content could leave HTTPS documents with confidential information in the Temporary Internet Files folder, Microsoft does not enable the setting to cache encrypted files in order to respect Web server caching instructions. Also, caching encrypted data helps prevent user performance issues when repeatedly viewing identical content, such as images. The risk of decrypting local cache files is not normally considered a significant concern, based on both the difficulty required to accomplish this, and the value of the information contained in these files. User name and password data would not normally be visible, even if a malicious attacker were to decrypt the document payload. They would only be able to see the content of pages. However, pages could contain sensitive information, such as account balances or transaction details.

For companies that want to increase Internet Explorer security settings for their users, enabling the Group Policy setting for **Do not save encrypted pages to disk** will prevent local file caching and eliminate the opportunity for malicious users to try and access these files. After enabling this option, organization could potentially experience performance issues, latency, additional network traffic, and a potential increase in help desk calls. Public Web sites may expect this value to be disabled to reduce their network traffic burden, but it should not cause serious application failures.

Enabling this setting can cause problems accessing "on demand" content such as account history reports. The problem occurs where users view the report, then navigate away from the report page, and then press the **Back** button on the browser to view the page again. In properly configured server environments, a specific error message displays telling users that the page has expired or that they need to click the **Refresh** button to view the content.

You can review and configure this setting in the following location in the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Advanced Page**

The following table provides security setting information specific to this technology in Internet Explorer 8.

Table 2.11 Do Not Save Encrypted Pages to Disk Setting

| **Policy object** | **Description** |
| --- | --- |
| Do not save encrypted pages to disk | This setting allows you to enforce whether Internet Explorer can save encrypted pages that contain secure (HTTPS) information, such as passwords and credit card numbers, to the Internet Explorer cache, which may not be a secure location.  If you enable this setting, Internet Explorer cannot save encrypted pages containing secure (HTTPS) information to the cache.  If you disable or do not configure this policy setting, Internet Explorer saves encrypted pages containing secure (HTTPS) information to the cache.  We recommend only enabling this setting in the browser for environments that manage sensitive data on Web pages. |

## Make Proxy Settings on a Per Machine Basis

If a user changes proxy settings, they may be unable to access Web sites. However, for users that are traveling, they may need to alter proxy settings to allow them to access the Web in different locations.

For computers in fixed locations, we recommend to use Group Policy to ensure that proxy settings are determined on a per computer (rather than a per-user) basis. However, for mobile laptops, allow users to change their proxy settings to provide them with more flexible access to the Internet.

You can review and configure this setting in the following location in the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer**

The following table provides security setting information specific to this technology in Internet Explorer 8.

Table 2.12 Make proxy settings per-machine

| **Policy object** | **Description** |
| --- | --- |
| Make proxy settings per-machine (rather than per-user) | This setting applies proxy settings to all users of the same computer. If you enable this policy, users cannot set user-specific proxy settings. They must use the zones created for all users of the computer.  If you disable this setting or do not configure it, users of the same computer can establish their own proxy settings.  This setting is intended to ensure that proxy settings apply uniformly to the same computer and do not vary from user to user.  We recommend enabling this setting for computers in fixed locations, and to disabled this setting in mobile laptops. |

## Turn Off Crash Protection

Internet Explorer 8 offers an error or failure detection feature that generates failure report information that may be of use to troubleshoot problems with Internet Explorer. However, the failure reports may contain sensitive information from the computer’s memory, so for the majority of organizations, we recommend to disable this feature. While the information passed to Microsoft when this feature is enabled is not used for any purpose other than to analyze the failure data, the reports may inadvertently contain information governed by data protection regulations. Disabling this feature can help your organization meet compliance requirements related to information access control. If you disable the failure detection feature, a failure in Internet Explorer will be similar to one on a computer running Windows XP Professional Service Pack 1 (SP1) or earlier: it will invoke Windows Error Reporting, and all policy settings for Windows Error Reporting continue to apply.

If you experience frequent failures and need to report them for follow-up troubleshooting, you may want to temporarily reconfigure the affected computers to enable this feature.

You can review and configure this setting in the following location in the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer**

The following table provides security setting information specific to this technology in Internet Explorer 8.

Table 2.13 Turn Off Crash Detection

| **Policy object** | **Description** |
| --- | --- |
| Turn off Crash Detection | This setting allows you to manage the crash detection feature of Add-on Management.  If you disable or do not configure this setting, the crash detection feature for Add-on Management will work.  We recommend configuring this setting to **Enabled**. |

## Enable the Restrict File Download Setting

In certain circumstances, Web sites can initiate file download prompts without interaction from users. This technique can allow Web sites to put unauthorized files on a user’s hard disk drive if they click the wrong button and accept the download.

We recommend configuring the **Internet Explorer Processes (Restrict File Download)** setting to **Enabled**. This ensures that download prompts that are not user-initiated are blocked for Internet Explorer processes.

You can review and configure this setting in the following location in the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components**

**\Internet Explorer\Security Features\Restrict File Download**

The following table provides security setting information specific to this technology in Internet Explorer 8.

Table 2.14 Restrict File Download Setting

| **Policy object** | **Description** |
| --- | --- |
| Internet Explorer Processes | This setting enables you to block file download prompts that are not user initiated.  If you enable this policy setting, file download prompts that are not user initiated are blocked for Internet Explorer processes.  If you disable this policy setting, permission prompts display for file downloads that are not user initiated for Internet Explorer processes.  If you do not configure this policy setting, the user's preference determines whether to prompt for file downloads that are not user initiated for Internet Explorer processes.  We recommend configuring this setting to **Enabled**. |

## Disable File Downloads for the Restricted Sites Zone

By default, file downloads are disabled for the **Restricted sites** zone. However, we recommend using Group Policy to enforce this restriction of the **Allow File Downloads** setting to ensure that users cannot download files when they are in the **Restricted sites** zone.

You can review and configure this setting in the following location in the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\Restricted Sites Zone**

The following table provides security setting information specific to this technology in Internet Explorer 8.

Table 2.15 Allow File Downloads Setting

| **Policy object** | **Description** |
| --- | --- |
| Allow File Downloads | This setting allows you to manage whether file downloads are permitted from the **Restricted sites** zone. The functionality of this setting option is determined by the zone of the page with the link to the download, not the zone from which the file is delivered.  If you enable this policy setting, users can download files from this zone.  If you disable this policy setting, users are prevented from downloading files from this zone.  If you do not configure this policy setting, users are prevented from downloading files from this zone.  We recommend configuring this setting to **Disabled**. |

## Use Object Caching Protection

Object caching protection prevents cached objects from being referenced after a user navigates away from a Web site. It provides a new security context for all scriptable objects so that access to all cached objects is blocked. In addition, access is blocked when users browse within the same domain. A reference to an object is no longer accessible after the context has changed due to navigation. Application developers should be aware of this greater security restriction and not develop applications that use objects from other Web sites because they may cause content to render incorrectly. This setting is enabled by default for Internet Explorer processes, and we recommend using Group Policy to enforce this behavior by enabling the **Object Caching Protection** setting. Enabling this setting helps to lower the risk of cross-domain security issues. You can review and configure this setting in the following location in the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Security Features\Object Caching Protection**

The following table provides security setting information specific to this technology in Internet Explorer 8.

Table 2.16 Object Caching Protection Setting

| **Policy object** | **Description** |
| --- | --- |
| Internet Explorer Processes | This setting defines whether a reference to an object is accessible when the user navigates within the same domain or to a new domain.  If you enable this policy setting, an object reference is no longer accessible when navigating within or across domains for Internet Explorer processes.  If you disable this policy setting, an object reference is retained when navigating within or across domains for Internet Explorer processes.  If you do not configure this policy setting, an object reference is no longer accessible when navigating within or across domains for Internet Explorer processes.  We recommend configuring this setting to **Enabled**. |

### Java Permissions

There has been some confusion over the Java permissions setting in Internet Explorer. Many people assumed that this setting only affects the Microsoft Java Virtual Machine (MSJVM). Microsoft does not believe that Java virtual machines (JVM) from other vendors appear to check this setting. However, this setting actually blocks the use of the <APPLET> element in HTML. This means that in certain circumstances, the setting can cause content that requires a JVM to fail, even when a third-party JVM is installed. Other HTML elements can use a JVM, so this behavior depends on the Web site content.

This setting is configured to **Enabled:disable** in the **Internet** and **Restricted sites** zones.

You can review and configure this setting in the following location in the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page\<*zone*>**

The following table provides security setting information specific to this technology in Internet Explorer 8.

Table 2.17 Object Caching Protection Setting

| **Policy object** | **Description** |
| --- | --- |
| Java permissions | This policy setting allows you to manage permissions for Java applets.  If you enable this policy setting, you can choose from the following options in a drop-down box:   * **Custom** enables you to control the permissions settings individually. * **Low Safety** enables applets to perform all operations. * **Medium Safety** enables applets to run in their sandbox, an area in memory outside of which the program cannot make calls, as well as capabilities like scratch space, a safe and secure storage area on the client computer, and user-controlled file I/O. * **High Safety** enables applets to run in their sandbox. Disable Java to prevent any applets from running.   If you disable this policy setting, Java applets cannot run.  If you do not configure this policy setting, the permission is set to **High Safety**. |

# More Information

The following resources provide additional information about Internet Explorer 8 security-related topics on Microsoft.com:

* [ActiveX Security: Improvements and Best Practices](http://go.microsoft.com/fwlink/?linkid=131978).
* [Applying the Principle of Least Privilege to User Accounts on Windows XP](http://technet.microsoft.com/en-us/library/bb456992.aspx).
* [Browsing the Web and Reading E-mail Safely as an Administrator](http://msdn2.microsoft.com/en-us/library/ms972827.aspx).

Chapter 3: Privacy Setting Recommendations

Security guidance is often limited to reviewing settings to prevent the manipulation of a system. But a full security settings review must include an analysis of "soft" security settings that affect privacy and the disclosure of personal data. Windows® Internet Explorer® 8 includes several new enhancements to safeguard personal data against entire categories of unwanted disclosure. These enhancements include the SmartScreen Filter that notifies users about phishing Web sites and Web sites containing malicious software.

You also can increase browser security by changing the default actions that control privacy settings for purging data when you exit the browser and form data handling. Deleting the Temporary Internet Files data also helps to ensure personal data is removed from the system regularly, and prevents unwanted disclosure or retrieval of information. Similarly, preventing the ability to autocomplete forms and store passwords helps reduce the risk of other organizations accessing private account credentials and information.

The Internet Explorer 8 privacy setting and feature recommendations in this chapter are grouped into the following nine categories:

* Use InPrivate Browsing
* Use InPrivate Filtering
* Delete Browsing History
* Set the Privacy Slider to Medium or Higher
* Automatically empty the Temporary Internet Files Folder
* Set Form AutoComplete options to disabled
* Configure Logon options for each security zone
* Enable the SmartScreen Filter
* Use the Cross Site (XSS) Scripting Filter

Some organizations want to be able to track their employees’ use of Internet Explorer®. Such organizations need to consider the need to retain a record of browser activities versus the privacy of their employees. They may find it more useful to configure some of the settings discussed in this chapter to the opposite values recommended in order to prevent users from deleting their browsing history and other historical data.

# Use InPrivate Browsing

Sometimes you do not want to leave any trace of Web browsing activity on a computer, such as when shopping for a gift on a family PC. The *InPrivate Browsing* feature in Internet Explorer 8 helps prevent the browser from retaining your browsing history, temporary Internet files, form data, cookies, and usernames and passwords so that no evidence of your browsing or search history remains.

To start InPrivate Browsing click the **Safety** button on the main toolbar of the browser window, and then select **InPrivate Browsing**. After you complete this action, Internet Explorer 8 launches a new browser session that will not record any information, including searches or Web page visits. To end your InPrivate Browsing session, simply close the browser window.

When using the InPrivate Browsing feature the following occurs:

* Browser Helper Objects (BHOs) and toolbars are disabled.
* All new cookies become "session" cookies and are deleted when you exit the browser.
* Existing cookies cannot be read.
* The existing functionality of the new DOM storage feature cannot change.
* New history entries are not be recorded
* New temporary Internet files are deleted after the Private Browsing window closes.
* Form data is not stored.
* Passwords are not stored.
* Addresses typed into the address bar are not stored.
* Queries entered into the search box are not stored.
* Visited links are not stored.

Organizations can choose to allow or deny this feature, depending on business requirements, rules, and governance issues that may apply to them. You can set the InPrivate Browsing feature as the default mode of the browser by adding the –private argument to the command line when you start Internet Explorer as in the following example:

"C:\Program Files\Internet Explorer\iexplore.exe" –private

# Use InPrivate Filtering

The *InPrivate Filtering* feature is designed to monitor and block only content from other organizations that appears with a high frequency across sites that you visit. No content is blocked until such levels are detected, nor is any such content blocked which is served directly by the site that you are visiting. Depending on your Web browsing activity and the sites you visit, the amount of time required for this feature to run can vary widely before such content is automatically blocked. Both administrators and users can control the frequency level of monitoring sites that are added to the Filtering list by setting the level to any value between 3 and 30. To deploy a standardized set of sites to allow (or block), users can manually import the list from a corporate share or other source. We recommend enabling InPrivate Filtering unless it causes problems with Web sites required for normal business operations.

# Delete Browsing History

While the ability to delete browsing history is not new to Internet Explorer, this browser feature has been enhanced in several ways for Internet Explorer 8. Now when you delete browsing history, you can choose to preserve cookies and temporary Internet files for sites in your Favorites folder. These added options help to protect your information and privacy while preserving your data on your trusted favorite sites. Your preferences and cookies are preserved, which helps to get you to your trusted sites faster with greater confidence. These enhancements also allow users to delete data collected for the InPrivate Filtering feature as shown in the following figure.

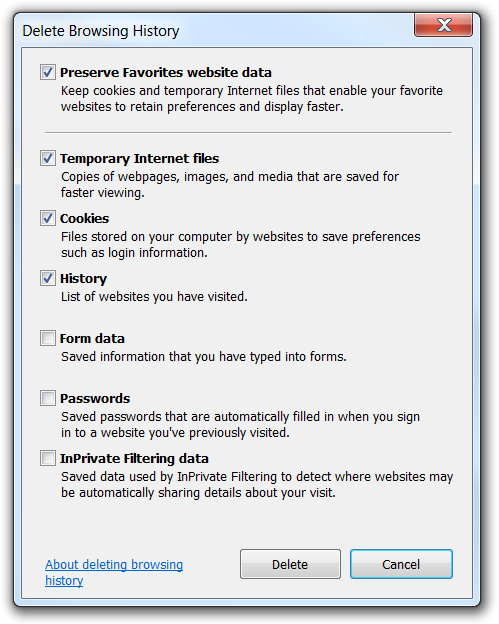


Figure 3.1 Delete Browsing History options

The new **Delete Browsing History** interface also contains individual checkboxes, allowing users to increase their control about what data is removed and what data is left untouched in the browser.

# Set the Privacy Slider to Medium or Higher

Some Web sites store information in a small text file on your computer in an attempt to offer a more a robust personalized online experience. These files are called *cookies*, and they can be used to correlate online activities for a specific user. Microsoft strongly supports the use of cookies and believes they do not represent a security or malicious software threat. However, Internet Explorer 8 has several mechanisms to control the use of cookies, and allow users to control them by managing privacy settings.

There are two different types of cookies. A *first-party cookie* either originates on or is sent to the Web site you are currently viewing. These cookies are commonly used to store information, such as your preferences when you visit that site. A *third-party cookie* either originates on or is sent to a Web site that is different from the one you are currently viewing. Third-party Web sites usually provide some content on the Web site you are viewing. For example, many sites use advertising from third-party Web sites, and those third-party Web sites may use cookies. A common use for this type of cookie is to track your Web page use for advertising or other marketing purposes.

Security settings that affect privacy issues can be found on the **Privacy** tab in the **Internet Options** dialog box of the browser. This tab contains the Privacy slider, which allows the user to select one of six options that range from **Block All Cookies** to **Accept All Cookies**. The Privacy slider works only for the Internet zone. All cookies are automatically accepted from Web sites in both the **Local intranet** and **Trusted sites** zones, and all cookies are automatically blocked from Web sites in the **Restricted sites** zone.

Each organization must determine their own policy regarding cookies. We recommend using at least the default setting of **Medium**, which does the following:

* Blocks third-party cookies that do not have a compact privacy policy.
* Blocks third-party cookies that use personally identifiable information without implicit consent.
* Restricts first-party cookies that use personally identifiable information without implicit consent.

The **High** setting limits all cookies, whereas the rest of the settings allow them under certain conditions. The **Low** setting allows all cookies without condition.

**Note**   By default, users can change the default setting of the privacy slider, although you can use Group Policy to prevent this by disabling the **Privacy** tab in **Internet Options** dialog box.

Specific sites can be added to bypass the overall setting. The choices for adding a site are to **Always Block** or **Always Allow**. Regardless of whether you choose to be more restrictive or less restrictive with the browser, you can add sites. You can use Group Policy to enforce not only the cookie settings, but also to add sites. For maximum privacy while maintaining the benefits of cookies (for example, retaining logon information, user preferences, and so on) we recommend blocking all third-party cookies and allowing all first-party cookies.

# Automatically Empty the Temporary Internet Files Folder

To increase page load speed and reduce network bandwidth, Internet Explorer provides a Temporary Internet Files folder in which a copy of many Web document objects (HTML, video, images, and so on) are maintained as the viewer navigates between sites. This storage area is designed to be temporary and may be overwritten at any time. Although not considered a remotely accessible threat, these files do represent a potential disclosure of personal information or privacy when viewed by other users who may access the computer. These local files are placed by default in the %userprofile%\AppData\Local\Microsoft\Windows\Temporary Internet Files folder. However, you can use the [*Internet Explorer Administration Kit (IEAK) 8*](http://technet.microsoft.com/en-us/ie/bb219517.aspx) or a GPO to modify the location through a setting in the Internet Control Panel of the browser. We recommend changing the default setting for this feature to **Enable**, so that all locally stored files are removed when the user closes the browser. Changing this setting has no impact on functionality, but it may affect application performance speed and result in additional user support calls.

You can review and configure this setting in the following location in the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Advanced Page**

The following table provides security setting information specific to this technology in Internet Explorer 8.

Table 3.1 Temporary Internet Files Setting

| **Policy object** | **Description** |
| --- | --- |
| Empty Temporary Internet Files folder when browser is closed | This setting allows you to manage whether Internet Explorer deletes the contents of the Temporary Internet Files folder after all browser windows are closed on the computer. This protects against storing dangerous files on the computer, storing sensitive files that other users could see, and helps to manage total disk space usage.  By Default, Internet Explorer does not delete the contents of the Temporary Internet Files folder when browser windows are closed.  We recommend enabling this setting. |

**Note**   For organizations that need to follow regulatory requirements for data control and privacy regulations, this feature can help to ensure information is deleted on a routine basis. This feature does not prevent data from being recovered using forensic tools. For this reason, organizations are encouraged to verify if using this feature is sufficient to meet their compliance requirements.

# Set Form AutoComplete Options to Disabled

Similar to the previous setting, this feature allows Internet Explorer to remember form entry data for later retrieval and submission. A common data value used in many forms is the Street Address field. This AutoComplete feature enables Internet Explorer to read form entry values and automatically enter information so users do not need to type them again. Although fields such as Street Address do not pose a direct security threat, this information can be useful to a malicious Web site.

More importantly, this feature is unable to discriminate between highly sensitive data, such as a credit card details, and more publicly accessible information like a telephone number. It is precisely because of these limitations that users may be exposed to an unnecessary and unintentional release of private information. The options for this feature are available in the **AutoComplete settings** dialog box, which you can access by clicking the **Settings** button of the **AutoComplete** area on the **Content** tab of the **Internet Options** dialog box.

Internet Explorer 8 can also remember user names and passwords on forms. Users must remember and increasing number of user names and passwords to access computer systems. Internet Explorer offers users the ability to store credentials and automatically fill in forms when such information is requested. There are some basic security mechanisms defining which data must be typed in a given form to prevent the wrong credentials from being used for a given Web site. Despite these security measures, a well-crafted Web site may be able to mimic enough parameters to trick the user into submitting their logon credentials to a malicious Web site. The credential data store is also secured, kept locally on the system and it is not accessible from a remote system. We recommend disabling the AutoComplete feature for forms and preventing the use of this feature for user names and passwords on forms.

Changing the setting options for this feature will not affect application performance, but may result in user complaints, or potentially in users resorting to low strength passwords that are easier to remember. Administrators are advised to examine their password requirement and validation processes to ensure that users do not use passwords that are not secure.

You can review and configure these setting options in the following location in the Group Policy Object Editor:

**User Configuration\Administrative Templates\Windows Components\**

**Internet Explorer**

The following table provides security setting information specific to this technology in Internet Explorer 8.

Table 3.2 AutoComplete Setting Options

| **Policy object** | **Description** |
| --- | --- |
| Disable AutoComplete for forms | This setting suggests possible matches when users are filling out forms. If you enable this setting, users do not receive suggested matches when filling out forms and the users cannot change the setting configuration.  If you disable this setting, users will receive suggested possible matches when filling out forms and they will not be able to turn them off.  By default, users can turn on and off the AutoComplete feature for forms.  We recommend enabling this setting option. |
| Turn on the auto-complete feature for user names and passwords on forms | This setting controls the AutoComplete feature in Internet Explorer which provides the ability to retain, suggest, and complete user names and passwords on forms. If you enable this setting, users will have access to this feature and will not be able to change the options for **User names and passwords on forms** or **Ask me before saving passwords**. When this setting is enabled, you must decide whether to select the checkbox for **Ask me before saving passwords**.  If you disable this setting, users will not have access to this feature and cannot change any of the options for it.  If you do not configure this setting, users can turn on AutoComplete to enable these setting options. Users can access these options by clicking the **Settings** button on the **Content** tab of the **Internet Options** dialog box that they can access from **Tools** on the main menu of the browser.  We recommend disabling this setting option. |

**Note**   For organizations that need to follow regulatory requirements for data control and privacy regulations, this feature can help to ensure information is not stored or shared with unauthorized users.

# Configure Logon Options for Each Zone

Enterprise and business customers can use Windows domains to keep intranet information secure while users seamlessly access network documents without repeatedly typing user credentials. Internet Explorer can use system authentication credentials and provide users with NTLM authentication information for Intranet zone sites. This feature setting provides a greater level of control beyond the basic Enable or Disable options. By default the **Automatic logon only in Intranet zone** setting is set for the **Internet**, **Local intranet** and **Trusted sites** zones, while **Prompt for Username and Password** is set for use in the **Restricted sites** zone. The net result is that users are automatically logged onto to sites in the Intranet zone when possible, but they are prompted for credentials when logging onto sites in other security zones.

You can review and configure these settings in the following location in the Group Policy Object Editor:

**Computer Configuration\Administrative Templates\Windows Components\**

**Internet Explorer\Internet Control Panel\Security Page\*<zone>***

The following table provides security setting information specific to this technology in Internet Explorer 8.

Table 3.3 Logon Options

| **Policy object** | **Description** |
| --- | --- |
| Logon Options  (Internet Zone) | This setting allows you to manage settings for logon options. If you enable this policy setting, you can choose from the following logon options.   * **Anonymous logon** to disable HTTP authentication and use the guest account only for the Common Internet File System (CIFS) protocol. * **Prompt for user name and password** to query users for user IDs and passwords. After a user is queried, these values can be used silently for the remainder of the session. * **Automatic logon only in Intranet zone** to query users for user IDs and passwords in other zones. After a user is queried, these values can be used silently for the remainder of the session. * **Automatic logon with current user name and password** to attempt logon using Windows NT Challenge Response (also known as NTLM authentication). If Windows NT Challenge Response is supported by the server, the logon uses the user's network user name and password for logon. If Windows NT Challenge Response is not supported by the server, the user is queried to provide the user name and password.   If you disable this policy setting, logon is set to Automatic logon only in Intranet zone. If you do not configure this policy setting, logon is set to Automatic logon only in Intranet zone.  We recommend enabling the setting option **Prompt for username and password**. |
| Logon Options  (Intranet Zone) | We recommend enabling the setting option **Automatic Logon with Current Username and Password**. |
| Logon Options  (Restricted Sites Zone) | We recommend enabling the setting option **Anonymous Logon**. |
| Logon Options  (Trusted Sites Zone) | We recommend enabling the setting option **Automatic Logon only in Intranet Zone**. |

**Note**   For organizations that need to follow regulatory requirements for data control and privacy regulations, this feature can help to ensure information is not stored or shared with unauthorized users.

# Enable the SmartScreen Filter

Users are exposed to an increasing number of online threats and malicious Web sites attempting to steal credentials. One of the new security features included with Internet Explorer 8 is the *SmartScreen Filter*, which provides a combination of client computer heuristic analysis technologies and online services to help protect users against emerging threats and Web sites that attempt to steal personal information or distribute malicious software. By default, when you first launch Internet Explorer 8, the SmartScreen Filter alerts the user to enable automatic checking, and require manual checking or disable it entirely—there is no preset selection. The feature offers an "all or nothing" security approach where automatic checking is enabled or disabled. When the SmartScreen Filter is disabled, users can still use the feature on a case by case basis, manually forcing a check on any given Web site.

It is important that system and network administrators understand the applications running in their environments. Internet Explorer and the SmartScreen Filter feature are no exception—understanding how this feature works enables you to get more value from it and greater protection against malicious software downloads or disclosure of personal data. This is especially critical given the importance and potential legal requirements of protecting confidential information in today’s online environments.

Malware and phishing protection in the SmartScreen Filter rely on the Microsoft URL Reputation Service (URS), which is staffed 24/7 for support and escalation support. When enabled, the SmartScreen Filter checks locally against a list of known legitimate sites and performs an online validation of the URL against the URS. To prevent latency, the URS checks are done asynchronously so user navigation is not adversely affected. To prevent excess network traffic, a client computer encrypted DAT file contains thousands of the most visited Web sites—all Web sites in this file are exempt from SmartScreen Filter checks. The SmartScreen Filter also uses a URL local cache mechanism in an attempt to match a previous request rating and prevent unnecessary traffic. One of the ways the URS identifies potential phishing sites is by collecting user feedback for previously unknown sites. Users can decide whether or not to submit a site that they suspect may be nefarious.

To help detect and guard against phishing and malware exploits, which are growing in complexity, the SmartScreen Filter examines the entire URL string instead of a subset of all URLs that the user has visited. It should be noted that it is possible for personally identifiable information (PII) to be transmitted to the URS, because the URL string itself may contain such data. Microsoft has taken extensive measures to help ensure that data is secure and remains private to the user, is not shared with any other organizations, and is stripped from the data once it has been evaluated for security threats. For more information, see the [Windows Internet Explorer 8 Privacy Statement](http://go.microsoft.com/fwlink/?linkid=128106).

As mentioned earlier, you must explicitly enable or disable the SmartScreen Filter in order for the feature to provide you with malware and phishing protection – there is no default setting. When enabled, all sites that do not appear in the local encrypted DAT file are validated locally and against the URS. No checking is performed when the SmartScreen Filter is disabled. Although Microsoft strongly encourages always using the SmartScreen Filter to help protect users, there may be situations in which administrators want to manage the feature in their environments.

**Note:**   ClickJacking and XSS protection is enabled by default. ClickJacking protection is part of the product design and cannot be disabled. But users can disable the XSS Filter. Users also can enable the SmartScreen Filter for protection against phishing and malware as outlined above.

By design, you can enable or disable the SmartScreen Filter for each security zone, but the global feature setting must be enabled for it to work. By default, the SmartScreen Filter is enabled for all zones except the **intranet** zone. We recommend administrators to enable the SmartScreen Filter feature in their environments.

If you want to exclude a list of sites from SmartScreen Filter checks (such as an extranet site which with your company has a trust relationship), instead of disabling the filter, We recommend enabling the global setting for the SmartScreen Filter, and then to disable filter for the **Trusted sites** zone only. Then you can add your list of sites to the **Trusted sites** zone.

We also recommend using Group Policy to prevent users from turning off the SmartScreen Filter and setting the operating mode to **Automatic**. However, administrators should be aware that this configuration automatically causes the browser to send information to Microsoft without prompting the user. Such data usage is limited to the enhancement of Microsoft services and user protection. It is not shared with any other organizations or used to personally identify users. For more information, see the [Windows Internet Explorer 8 Privacy Statement](http://go.microsoft.com/fwlink/?linkid=128106).

You can review and configure these settings in the following location in the Group Policy Object Editor:

**User Configuration\Administrative Templates\Windows Components\**

**Internet Explorer\Internet Control Panel\Security Page\*<zone>***

The following table provides security setting information specific to this technology in Internet Explorer 8.

Table 3.4 SmartScreen Filter Zone Options

| **Policy object** | **Description** |
| --- | --- |
| Use SmartScreen Filter | This setting controls whether the SmartScreen Filter scans pages in this zone for malicious content.  If you enable this policy setting, the SmartScreen Filter scans pages in this zone for malicious content. If you disable this policy setting, the filter does not scan pages in this zone for malicious content.  By default, users can configure this setting.  We recommend enabling this setting. |

In addition to this per-zone setting, you can review and configure two global SmartScreen settings in the following location in the Group Policy Object Editor:

**User Configuration\Administrative Templates\Windows Components\**

**Internet Explorer**

The following table provides security setting information specific to this technology in Internet Explorer 8.

Table 3.5 Global SmartScreen Filter options

| **Policy object** | **Description** |
| --- | --- |
| Turn off Managing SmartScreen Filter | This setting allows users to enable the SmartScreen Filter, which then warns if a Web site being visited is known for fraudulent attempts to gather personal information through "phishing," or is known to host malware.  If you enable this setting, users are not prompted to enable the SmartScreen Filter, and all Web site addresses not contained on the filter's allow list are sent automatically to Microsoft without prompting users.  If the feature is disabled or not configured, users are prompted to decide the mode of operation for the SmartScreen Filter the first time the browser is run. We recommend enabling this setting. |
| Prevent Bypassing SmartScreen Filter Warnings | This setting controls the SmartScreen Filter behavior.  If you enable this setting, users are not permitted to navigate to sites identified as unsafe by the SmartScreen Filter.  If you disable this setting or do not configure it, users can ignore SmartScreen Filter warnings and navigate to unsafe sites.  We recommend enabling this setting. |

# Use the Cross Site (XSS) Scripting Filter

The Cross-Site Scripting (XSS) Filter is designed to prevent users from becoming victims of unintentional information disclosure. This is especially helpful for organizations that are required to meet regulatory or compliance requirements.

We recommend leaving this feature enabled (the default setting) to ensure users are protected. If users encounter a mission critical Web site that triggers the XSS Filter, you should first attempt to identify what is causing the issue. As a last resort you can disable this feature, but it should be enabled again as soon as possible.

You can review and configure these settings in the following location in the Group Policy Object Editor:

**User Configuration\Administrative Templates\Windows Components\Internet Explorer\Internet Control Panel\Security Page*\<zone>***

The following table provides security setting information specific to this technology in Internet Explorer 8.

Table 3.6 Cross-Site Scripting (XSS) Filter Options

| **Policy object** | **Description** |
| --- | --- |
| Turn on Cross-Site Scripting (XSS) Filter | This setting controls if the Cross-Site Scripting (XSS) Filter detects and prevents cross-site script injection into Web sites in this zone.  If you enable this policy setting, the XSS Filter attempts to block cross-site script injections for sites in this zone.  If you disable this policy setting, the XSS Filter permits cross-site script injections for sites in this zone.  We recommend enabling this setting. |

# More Information

The following resources provide additional information about Internet Explorer 8 security-related topics on Microsoft.com:

* [*Internet Explorer Administration Kit (IEAK) 8*](http://technet.microsoft.com/en-us/ie/bb219517.aspx).
* [Windows Internet Explorer 8 Privacy Statement](http://go.microsoft.com/fwlink/?linkid=128106).

Appendix A: Security Checklist

The following checklist includes all of the feature areas and settings that we recommend to consider using as you secure client computers running Windows® Internet Explorer® 8 in your organization.

Table A.1 Internet Explorer 8 Security Checklist

|  |  |
| --- | --- |
| ✓ | Active Content Security |
|  | Restrict ActiveX® Install. |
|  | Control per-site ActiveX settings. |
|  | Add ActiveX controls and plug-ins to pre-approved list. |
|  | Disable Allow active scripting in response to specific threats. |
|  | Enable Scripted Window Security Restrictions. |
| ✓ | Zone Security |
|  | Enable Zone Elevation Protection. |
|  | Do not allow users to add or delete sites from security zones. |
|  | Do not allow users to change policies for security zones. |
|  | Do Not Configure Security Zones: Machine Only Settings. |
| ✓ | Certificate Security |
|  | Prevent navigating to sites with certificate errors. |
| ✓ | Reduce Application Privilege |
|  | Use Protected Mode on computers running Windows Vista®. |
|  | Use DropMyRights on computers running Windows® XP. |
| ✓ | Privacy Settings |
|  | Use the InPrivate Browsing feature. |
|  | Use the InPrivate Filtering feature. |
|  | Use Delete Browsing History. |
|  | Set the Privacy Slider to Medium or Higher. |
|  | Empty the Temporary Internet Files folder when users close the browser. |
|  | Set Form AutoComplete options to disabled. |
|  | Disable Password Caching. |
|  | Configure logon options for each security zone. |
|  | Enable the SmartScreen Filter. |
|  | Use the Cross-Site (XSS) Scripting Filter. |
| ✓ | Other Security Settings |
|  | Make proxy settings per machine (rather than per user). |
|  | Turn off Crash Protection. |
|  | Restrict File Downloads. |
|  | Disable Allow File Downloads for Restricted Zone. |
|  | Enable Object Caching Protection. |