Analysis of Security Policies in Major Web Browsers and Development of a Multibrowser and Multiplatform Browser Configuration Tool: Open Browser GP

A Thesis

Presented in Partial Fulfillment of the Requirements for the

Degree of Master of Science

with a

Major in Computer Science

in the

College of Graduate Studies at

University of Idaho

by

Venkata Anirudh Bhandari

Major Professor: Daniel Conte de Leon, Ph.D.

Committee Members: Jim Alves-Foss, Ph.D.; Gregory W. Donohoe, Ph.D.

Department Administrator: Gregory W. Donohoe, Ph.D.

May 2015

Authorization to Submit Thesis

This thesis of Venkata Anirudh Bhandari, submitted for the degree of Master of Science with a Major in Computer Science and titled **"Analysis of Security Policies in Major Web Browsers and Development of a Multibrowser and Multiplatform Browser Configuration Tool: Open Browser GP,"** has been reviewed in final form. Permission, as indicated by the signatures and dates given below, is now granted to submit final copies to the College of Graduate Studies for approval.

Major Professor: _____ Date _____
Dr. Daniel Conte de Leon

Committee members: _____ Date _____
Dr. Jim Alves-Foss

_____ Date _____
Dr. Gregory W. Donohoe

Department Administrator: _____ Date _____
Dr. Gregory W. Donohoe

Abstract

Web browsers are used frequently to access resources from the World Wide Web (WWW). However, they are vulnerable to various attacks which may affect specific applications or an entire operating system. The current administrative tools used for configuring browser settings, in order to mitigate security vulnerabilities in browsers, follow different procedures for each browser. This variance increases the complexity for system administrators to analyze and configure similar security settings in all browsers.

In this thesis, firstly, we analyze and categorize secure browsing policies. Secondly, we argue that a set of common settings and a common configuration language for multiple browsers is needed. Thirdly, we introduce Open Browser GP: A Multiplatform and Multibrowser Policy Configuration tool that enables the remote configuration of security related settings in three major browsers: Internet Explorer, Google Chrome and Mozilla Firefox for Windows 7 and Windows 8 client systems.

Acknowledgements

I would like to thank my advisor, Dr. Daniel Conte de Leon for his support, encouragement, and wonderful edits.

I would also like to thank my committee members, Dr. Jim Alves-Foss and Dr. Gregory W. Donohoe for their valuable input on my thesis.

I would like to thank all of my professors and teachers who have helped to impart the knowledge which has helped me along in my academic career.

I would also like to thank my friends and family who have been supportive of my endeavors.

I would like to thank Lee VanGundy for making this template.

This thesis work was made possible with the financial support of a State of Idaho IGEM grant with the Center for Secure and Dependable Systems.

Table of Contents

List of Figures

List of Tables

List of Listings

Chapter 1

Introduction, Problem, and Overview

Chapter 1 introduces the need and advantages of using multiple platforms and multiple browsers, and briefly presents the distribution of the browsers and operating systems. Secondly, it describes some of the problems involved in securely configuring browsers and a set of possible solutions. This chapter concludes with an overview of this thesis document.

1.1 Operating Systems

The Operating System is the software component which is responsible for the interaction between hardware and an application program. The main goal of an operating system is to provide a user friendly and efficient environment to an end user, such that they can perform their required tasks and execute necessary programs [33]. Operating systems are available in various configurations (personal computers, business applications, gaming applications and many more) which can either be used for a single specific application or can be used for multiple purposes. For example, an open source operating system associated with chromium projects called Chromium OS was released back in 2009 [5]. The main purpose of this operating system was to provide pre-installed and efficient applications for users who spend most of their time on the web. This operating system was specially developed for maintaining and executing web applications, so people working in this field will prefer to use this specific operating system.

However, other users require other operating systems to use multiple applications of different types. Fortunately, multiple operating systems are available which can perform multiple tasks. Many operating systems such as Linux and FreeBSD have been released as open source editions, such that their code is freely available and documented. These operating systems can now be used for research purposes and further studies can be conducted to improve available features in them. Some of the requirements and advantages of having multiple operating systems in an organization are:

1. Provides more flexibility for a user to choose an appropriate platform.
2. Using multiple operating systems minimizes the risk of simultaneous attacks.
3. Increases the ability to work on different file formats and systems, and the availability of tools.

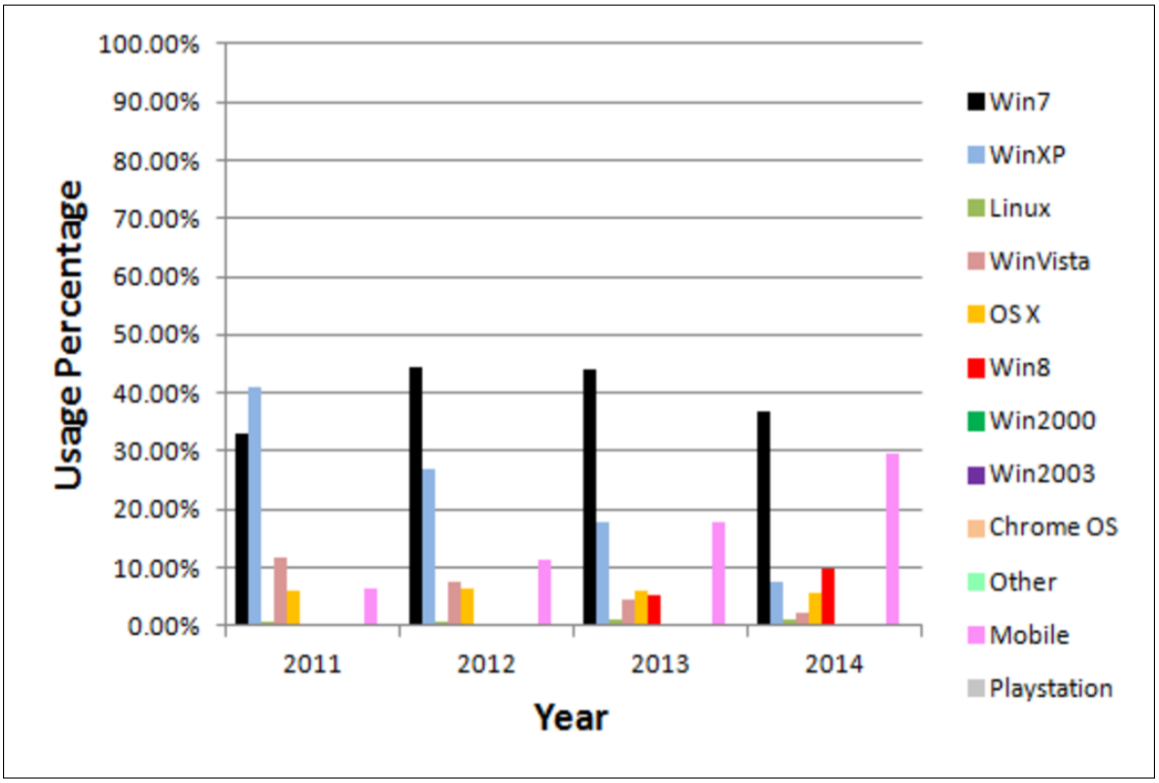


Figure 1.1: Distribution of Operating Systems

The number of people using an operating system initially depends on its efficiency, its multi-tasking capacity, cost, marketing, etc. Later, it gradually increases depending on improvements, however its usage may decrease due to competition available by different operating systems. A recent article from StatCounter Global Stats presents the annual analysis of the usage percentage of operating systems for the last four years across more than 3 million sites globally tracked by StatCounter service [34]. In Figure 1.1 we can observe that different users use different operating systems. One of the interesting observations to notice from this graph is that, even though multiple operating systems are available there are one or two operating systems which are more popular and dominate the percentage of usage of other operating systems. The usage of mobile operating systems have increased vastly recently, some of them even outnumber some of the desktop operating systems. In this thesis we worked with desktop operating systems and explain the possibilities of extending the analysis and results to mobile technologies in Chapter 6 of this thesis. Figure 1.1 indicates us that until 2011 Windows XP was the most popular operating system and from that point onwards Windows 7 is the most used operating system with Windows 8 as the second most popular operating system starting in 2014. These statistics increased our interest towards the recent most popular operating systems and drove

our focus in configuring browser security related settings of Windows 7 and Windows 8 client systems.

1.2 Web Browsers

A browser is a software application which is used to display web pages and transfer information between different client and server systems mostly through the use of the HTTP protocol [25]. Many browsers are available these days, most of them are available free of cost. The popularity of a browser depends partly upon the number of functionalities it provides and its speed. Mosaic was the first browser which was accessible by everyone to interact with the web; it was introduced in 1993. Later, many browsers were introduced which increased the competition between different developers to create an efficient and fast browser. Although most browsers are available freely they act as a medium between a user and the web, so this idea influenced most of the developers to develop browsers which can be beneficial in different possible ways. This eventually led to a phase which the people in the web community called "*Browser Wars*" [25]. Some of the advantages of having multiple browsers in an organization are:

1. Increases the ability to perform multiple tasks.
2. Provides more flexibility for users to choose an appropriate browser for the task.
3. Most of the browsers are available free of cost.
4. Increases the ability to work on different browser specific applications and scripts.

However, we come across certain drawbacks while having multiple browsers in an organization; some of them are:

1. Maintenance and updating multiple browsers is a difficult task.
2. Configuring similar security settings in multiple browsers in all platforms is a difficult task.

Many organizations provide benchmarking and analysis of the popularity of different browsers; some of them are performed specifically for research purpose, whereas some are analyzed for improving the available browser capabilities. A recent article presents the annual analysis of the usage percentage of browsers across more than 3 million sites globally tracked by StatCounter service [34]. In Figure 1.2 we can observe that similar to operating systems, some of the browsers are more popular and widely utilized when compared to other browsers. Initially

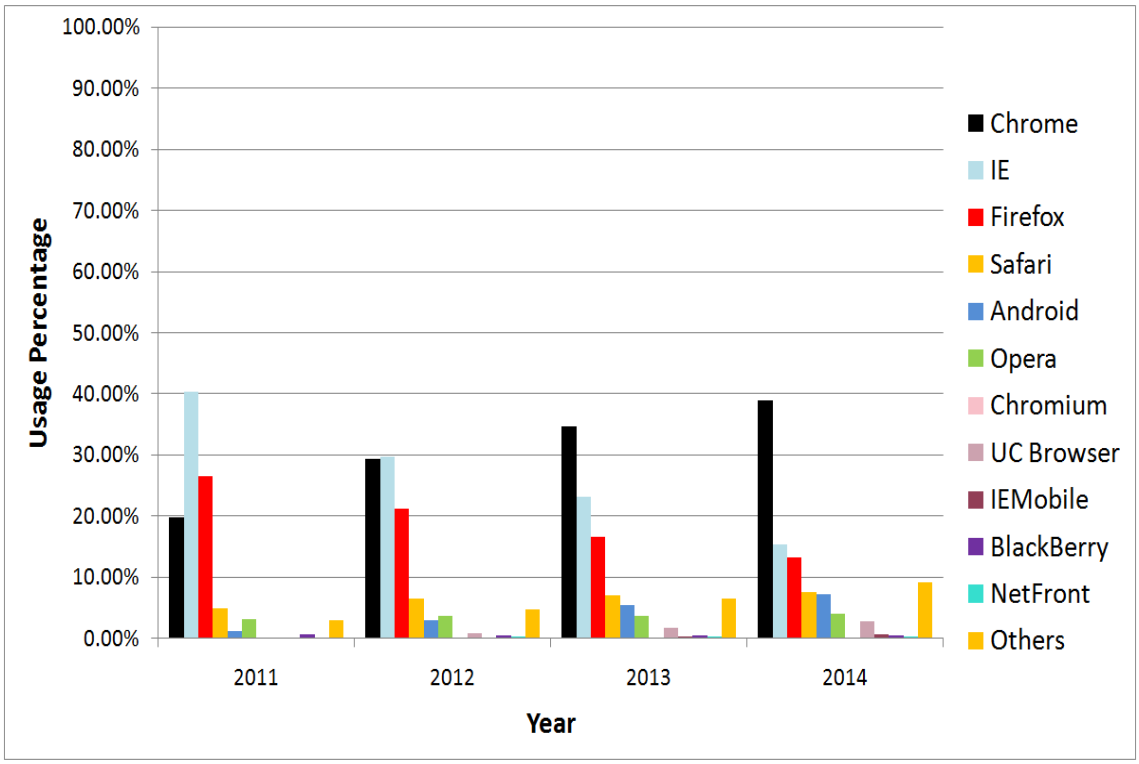


Figure 1.2: Distribution of Browsers

this graph shows that Internet Explorer (IE) was a popular browser but these statistics change with the growing popularity of Google Chrome (Chrome) at the present moment. Currently, we can observe that there are three dominant browsers (Internet Explorer, Google Chrome, and Mozilla Firefox). This observation drove our focus on these 3 major popular browsers. Hence, we concentrated on these specific browsers and this thesis discusses issues and solutions for configuring security related settings of these three browsers. The term *major browsers*, in context of this thesis, should be understood as a reference to Internet Explorer, Google Chrome, and Mozilla Firefox browsers.

1.3 Security Vulnerabilities in Browsers

Web browsers have evolved into powerful and useful applications which are used at high frequency to communicate and transfer information through the web, but they have some drawbacks. One of the most important drawbacks is that they are vulnerable to different attacks. Dormann and Rafail [3] explained the factors which lead to browser attacks, some of them are:

1. Redirected web pages can be malicious.

2. Novice users tend to click on unknown links and visit websites which can be malicious.

3. Some of the browsers concentrate on speed and popularity, thereby neglecting security features.

4. Some users avoid security updates if they are not compatible with some applications.

5. Most users don't have the required knowledge to configure advanced security features in browsers.

Browsers are vulnerable to various attacks such as Cross-Site Scripting, Trojans, and Denial Of Service (DOS) attacks. In recent years, Golovanov [4] described the different vulnerabilities and the need for secure browsing. Golovanov and colleagues at Kaspersky Lab's cloud service conducted analysis of 10.5 million computers across the globe, these computer users were willing to take part in this survey so that this analysis could be used to provide secure browsing in the future. They observed the most popular browsers installed in these systems and provided the statistics in Table 1.1. The article stated that among these computers about 10% of users installed more than one browser (Table 1.1) and 50-60% of the users had the latest versions of browsers installed on their computers.

These statistics were analyzed in 2012 where Google Chrome was at the initial stages of becoming the most popular browser. Even though the Safari browser is available by default in Mac operating systems and Internet Explorer is available by default in Windows operating systems, the number of users utilizing Google Chrome outnumbered these other browsers, making it the most popular browser as reported by the Kaspersky lab's analysis. This analysis is further utilized to categorize and find possible threats with respect to each browser.

Figure 1.3 chart shows the distribution of browsers used among the 10.5 million users who participated in the Kaspersky lab's survey. The authors of this article later provided an analysis about the top 20 categories of threats faced by different browsers. Some of the common threats in major browsers are:

1. *WMUF:(blocked)*: WMUF is an anti phishing technology in Kaspersky cloud services which is used to maintain malicious site URL. The threat observed during the analysis was that this feature was blocked.

2. *HEUR:Trojan.Script.Generic*: Browsers were vulnerable to malicious scripts.

Table 1.1: Most Popular Browser. Data from: Kaspersky Lab's cloud service [4]

Browser	Number of Browsers Analyzed	Percentage of Browsers Analyzed
GOOGLE CHROME	3,472,506	30.26%
INTERNET EXPLORER	3,324,190	28.97%
FIREFOX	3,096,316	26.97%
OPERA	1,575,880	13.73%
SAFARI	7,648	0.07%
Total number of browsers	11,476,540	100.00%

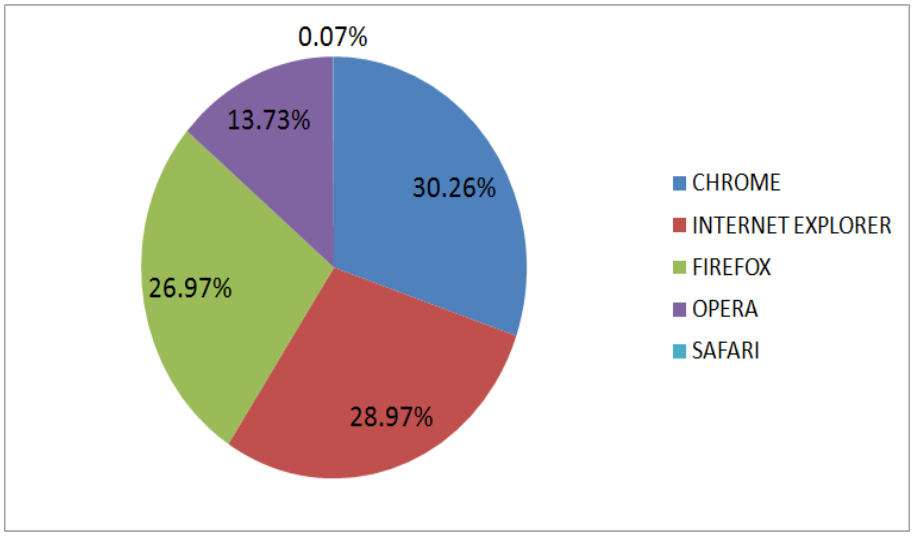


Figure 1.3: Browsers Distribution Statistics

3. *HEUR:Trojan.Script.Iframer*: This threat was related to the concept where browsers were vulnerable to scripts that return IFRAMEs to infected sites.

According to the statistics provided by Golovanov [4] we can observe that the 5 browsers were vulnerable to various attacks. On a personal computer a user is responsible to configure browsers and operating systems on their own. However, to minimize these attacks in a large organization, system administrators are often hired to configure browser and operating system settings.

1.4 Current Problems when Configuring Browsers for Better Security

Organizations allow their employees to utilize web browsers to access resources from the World Wide Web, in order to avoid data corruption and data loss due to the vulnerabilities in browsers, these organizations have to develop secure browsing infrastructure. This thesis concentrates on current problems and potential solutions for secure browsing configuration from these organization's and end user's point of view.

1. *End Users*: End users are responsible for configuring browsers settings on their own. The disadvantage of this category is that most users don't have the required knowledge to configure advanced security features in browsers. This leads to inconsistent and insecure browsing evironment.

2. *Small Scale Organization*: These organizations consists of small number of employees and computers; these computers are used for specific limited purposes such as data maintenance, word processing, monthly budgets, etc. For example let's consider the model shown in Figure 1.4 which represents a small scale organization. In this scenario the company can decide that of all their computers will run Windows 7 operating systems with either IE or Google Chrome as their browsers. However, they may not be able to afford a server which can be used to configure all of the client systems and browsers remotely, so the system administrator has to manually configure each browser in each computer.

3. *Medium Scale Organization*: Some of the organizations can be categorized into medium scale organizations, these organizations can accommodate a larger number of operating systems and browsers. Eventually they face the same problems, where the system administrator has to manually configure each browser in each computer.

4. *Large Scale Organization*: These organizations consists of hundreds of employees and computers which are used for multiple purposes. These companies maintain I.T. departments with system administrators in order to maintain their computing infrastructure. The model shown in Figure 1.5 presents the current complexity in configuring major browsers in major operating systems. In a scenario where a company consist of N groups of users with multiple operating systems and multiple browsers, it is a complex and tedious job for the system administrators to configure all browser settings manually.

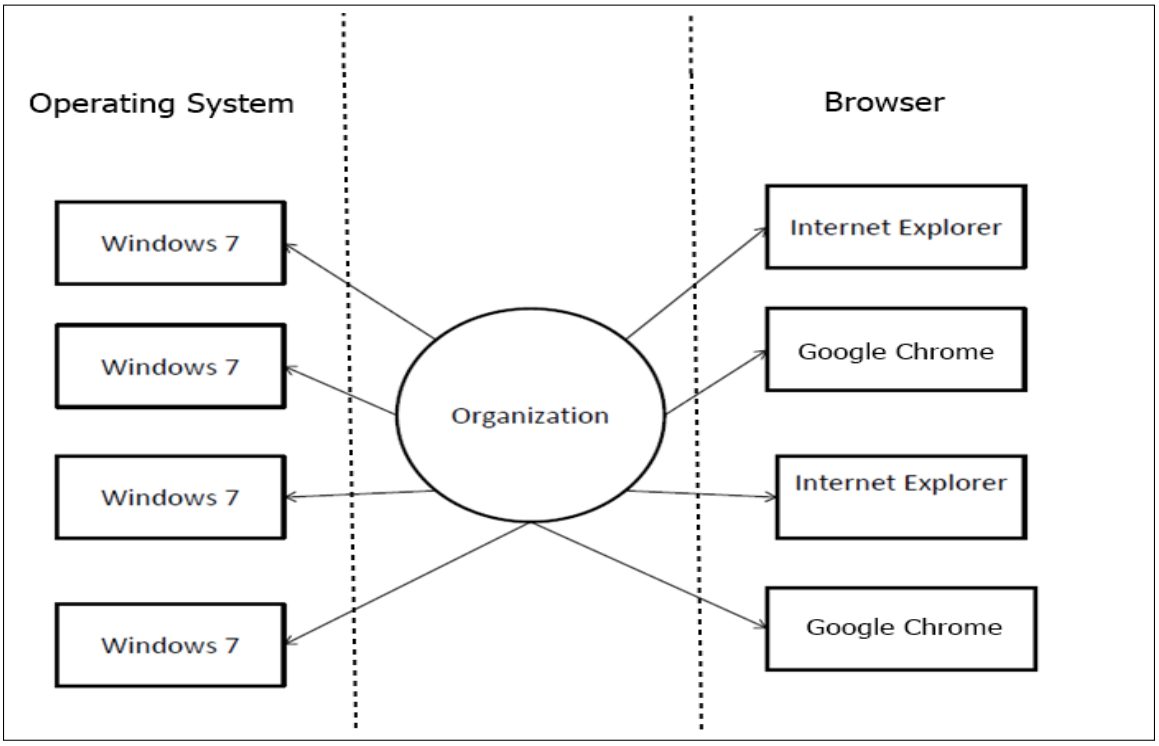


Figure 1.4: Small Scale Organizations

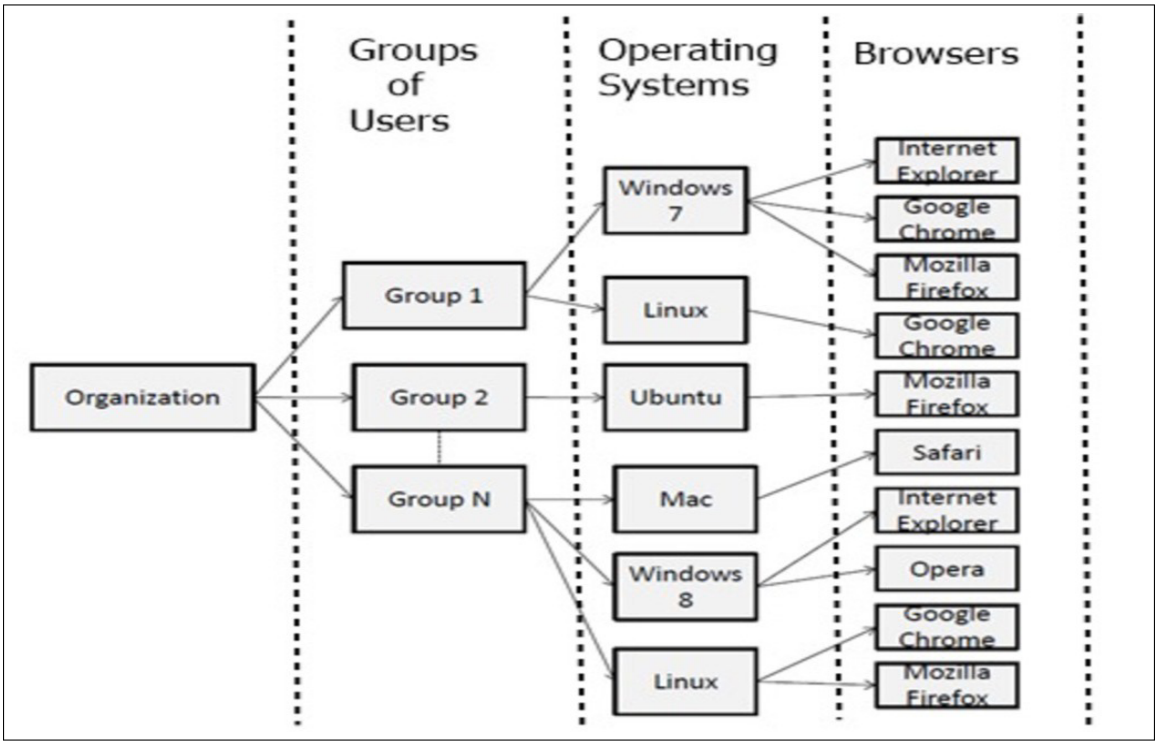


Figure 1.5: Large Scale Organizations

1.5 Proposed Solutions

To overcome these problems faced by organizations we propose three contributions in this thesis, in order to help system administrators to configure and maintain secure browsing settings in multiple browsers in multiple operating systems.

1. We analyzed and categorized secure browsing policies.
2. We mapped the policies of each major browser which are similar with respect to other browsers and labelled them with a common name for each setting.
3. We introduced an Open Browser GP: A Multiplatform and Multibrowser Policy Configuration tool to configure security related settings in major browsers.

1.6 Overview of this Thesis

The remainder of this thesis is organized as follows: Chapter 2: *Current Procedures and Tools for Configuring Major Browsers* provides background information on available solutions to remotely configure browsers and presents some of the drawbacks associated with these solutions. Chapter 3: *Analysis and Categorization of Policies in Major Browsers* explains the results of analysis and classification of different policies along with the mapping of similar policies and dissimilar policies in different major browsers. Chapter 4: *Toward a Common Language to Achieve Secure Browsing Systems* discusses the need to create and utilize a common language to configure settings in all browsers and all platforms. Chapter 5: *Open Browser GP: A Multiplatform and Multibrowser Policy Configuration Tool* discusses the different technologies used in building this tool, the procedure involved to setup and utilize this tool, then finally provides the advantages and limitations of using this tool in a network to configure major browsers. For the remainder of this thesis *GP* should be understood as a reference to Group Policy. Chapter 6: *Conclusions and Future Work* summarizes the findings and future work. The end of this thesis includes a bibliography and an appendix.

Chapter 2

Current Procedures and Tools for Configuring Major Browsers

This chapter introduces existing solutions to overcome some of the problems faced by different browsers. Firstly, it includes a brief description of the Windows Registry and the different possible ways of configuring registry entries. Secondly it provides a brief description of Windows server and Active Directory (AD), along with the reason behind the creation and utilization of ADMX (Administrative templates in XML) and ADML (Administrative language specific templates) file systems. Finally, this chapter presents some of the problems faced when using the existing solutions.

2.1 Background Information about the Windows Registry

Microsoft Computer Dictionary [17], defines the registry as:
"*A central hierarchical database in Windows 9x, Windows CE, Windows NT, and Windows 2000 used to store information necessary to configure the system for one or more users, applications, and hardware devices.*"

The Registry consists of information that is frequently referenced by the Windows operating system to execute and maintain settings of the system. Although the registry is common to all the Windows operating systems, there are few variations among different Windows versions. Most registry modifications can be done only by an administrator, but a few operations can be done by users. The Registry consists of certain predefined registry root keys [19] used by the Windows operating system (Table 2.1). These root keys may contain one of the registry value types (Table 2.2). Each registry entry has its own predefined syntax and functionality, so users should be careful when creating or modifying registry entries. For example a string value cannot be assigned to REG_DWORD data type, it has to be assigned to REG_SZ.

These registry values can be modified by an administrator by using various methods and tools [19]. Some of them are:

1. **Windows user interface**: Different graphical user interface options are provided by a Windows user interface which automatically changes registry values. However, these are not reliable for performing advanced operations.

2. **Registry Editor**: The Registry Editor can be opened by typing *regedit* in the command prompt. The Registry Editor enables viewing and modification of all registry keys. Users

Table 2.1: Registry Root Keys

KEYS	Description
HKEY_CURRENT_USER	Contains information to configure currently logged on user.
HKEY_USERS	Contains information to configure all users on the computer.
HKEY_LOCAL_MACHINE	Contains information to configure a particular computer (any user).
HKEY_CLASSES_ROOT	Contains information to configure software on the computer.
HKEY_CURRENT_CONFIG	Contains information about hardware components used by the local computer.

can navigate through the different tree structures to find a key, sub key, or value. Windows Registry editor allows administrative users to add, change, delete and rename keys or sub keys of all registry keys and the users of a computer system.

3. **Group policy**: Administrative tools can be used to manage the group policies of specific computers, services and other system components. One of the group policy tools is group policy object editor (GPO) which uses administrative templates (ADMX or ADM) to control a computer or a group of computers.

4. **Registry Entries**: Modifications can be made to the Windows Registry by creating registry entry files with ".reg" format and executing them with administrator privileges to make the required changes on a computer. These .reg files can be run manually or by using a logon script.

5. **Windows Script Host**: Various scripts such as VBScripts and JScripts can be run directly on an operating system by using Windows script host methods to delete, read, and write the registry keys and values.

Some of these methods can be used to configure a single Windows operating system, whereas other methods can be utilized to configure multiple client systems from a central server. Windows Server with Active Directory (AD) is one of the methods which is currently used by system administrators to configure multiple client systems.

Table 2.2: Registry Value Types

Key Name	Data Type	Description
Binary	REG_BINARY	Contains raw binary data and is displayed in registry editor in hexadecimal format.
DWORD	REG_DWORD	Contains data represented by a number that is 4 bytes long and can be displayed in different formats (binary, hexadecimal, or decimal format).
Expandable String	REG_EXPAND_SZ	Contains data string which is variable length.
Multi-String	REG_MULTI_SZ	Contains multiple strings.
String	REG_SZ	Contains fixed length text string.
Binary	REG_RESOURCE_LIST	Contains a resource list that is used by a hardware device.
Binary	REG_RESOURCE_REQUIREMENTS_LIST	Contains resource list requirements that is used by a hardware device.
Binary	REG_FULL_RESOURCE_DESCRIPTOR	Contains a resource list description that is used by a hardware device.
None	REG_NONE	Contains data without any particular data type.
Link	REG_LINK	Contains string with a symbolic link.
QWORD	REG_QWORD	Contains data represented by a number that is a 64-bit integer.

2.2 Windows Server and Active Directory Group Policies

The Windows Server uses Administrative Templates as a popular and useful way of configuring applications and browsers in the Windows client systems. ADM files are the previously used administrative template files by Active Directory to maintain settings in the registry. ADM files were template files for Windows NT, Windows 2000, Windows 2003 and Windows XP. These files had their own special markup language [7]. ADM files were used individually because each language had it's own ADM file. For example, if we want the ADM file in U.S. English and French they used to write it separately and place them in separate folders in *%systemroot%\sysvol\domain\policies\PolicyDefinitions* folder in the operating system, where %systemroot% is the Windows directory. Whenever an update had to be installed in multiple systems, developers had to create different files for each language depending on the requirements

Listing 2.1: ADM Template for Altering the Exit Sound of Windows Computer System. Example From: Group Policy Article [21]

```
1 CLASS USER
2 CATEGORY SOUNDS
3 POLICY 'Sound to hear when Exiting Windows'
4 KEYNAME 'AppEvents Scheme Apps Default SystemExit Current' PART '
    What sound do you want?' EDITTEXT REQUIRED
5 VALUENAME ''
6 END PART
7 END POLICY
8 END CATEGORY
```

of the end user. One of the examples provided by Moskowitz [20] presents the policy to alter the sound when a user exists the Windows system. This example is shown in Listing 2.1

ADMX and ADML are *Administrative Template Files* which were introduced by Windows Vista and Windows 2008 server. Most of the new operating systems and applications use ADMX (X stands for XML) and ADML files. Because they are in XML based formats it is easy to read, write, understand and edit them. Some of the tools used to edit XML files are XML Notepad 2007 [18], Stylus studio [2] and Notepad++ [9]. ADMX and ADML are both used in new versions of the Windows Operating Systems, where ADMX is rather a generic file which is generally written in English and does not include policy descriptions. These ADMX files are referenced to ADML files which are separate files for each language [21]. The ADMX file consists of various elements and attributes to create different styles of templates in GPO such as radio box, check box and list. It is divided into seven main sections [16] such that the *policyDefinitions* element section consists of all other sections except the *XML declaration* section. A brief description is given about a few elements which are used to build basic ADMX files in Table 2.3. In this table E stands for Element, A stands for Attribute and R stands for Required.

Table 2.3: Structure of ADMX File Format

Parent	Child	E/A	R	Description
XML	No	No	No	XML declaration is an optional feature which can be added to ADMX file if a developer wants to specify that this is an XML document. It consists of xml version followed by the encoding attribute. ADMX files are always UTF-8 encoded and XML version is 1.0.

policyDefinitions	Yes	E	Yes	Used to define a set of registry policy settings and to declare a default namespace for all the elements. This element consists of five attributes out of them three are optional, but they are used to make ADMX files as a fully formed XML file. It is the document element, so except XML declaration it contains all the other sections in the document representing the ADMX file.
policyNamespaces	Yes	E	Yes	Used to map ADMX files to a unique namespace in ADMX files and can also reference an existing namespace from a different policyNamespace.
	target	E	Yes	Used to specify a unique name for the policy namespace in a given ADMX file.
	using	E	No	An optional feature which can be used if a developer is interested in referencing a policyNamespace from a different policyNamespace.
resource	No	E	Yes	Used to mention the minimum revision level in an ADMX file to its matching ADML file.
supportedOn	Yes	E	No	An optional element which is mainly used for mapping of products to its definitions. It specifies reference to localized text strings defining the applications affected by a specific policy setting.
	definitions	E	Yes	The supported product information definitions are located in this field of element.
categories	Yes	E	Yes	Consists of a group of category elements which are used to specify a unique name to be displayed on the group policy object (GPO) editor. If a category name already exists, a duplicate name is created. The categories element is only defined once in every ADMX file.
	category	E	Yes	Used to create a unique name for each category of the template files.
policies	Yes	E	Yes	Used at most once in an ADMX file, it consists of a group of policy elements which are in turn used to represent policy settings.
	policy	E	Yes	Used to represent settings of a single policy.

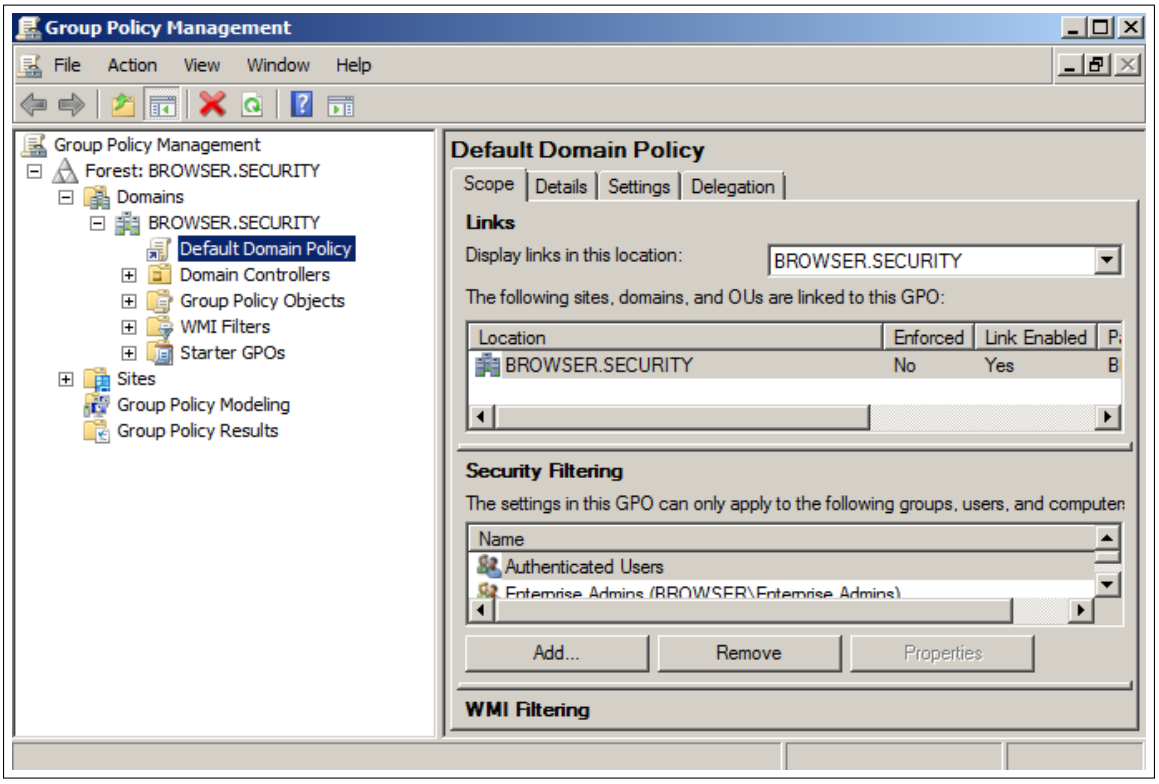


Figure 2.1: Group Selection in GPMC

2.3 Remote Configuration of Clients and Group Policy Objects

Remote Configuration of Clients and Group Policy Objects method is used in the Windows Server to configure multiple client systems remotely which are connected to the domain server as a group of clients. This method is used by large organizations to configure multiple Windows client operating systems by using a single Windows Server. This thesis used Windows Server 2012 operating system as a server and Windows 7 Enterprise operating system as client system.

1. Initially we have to connect the client systems to the domain server. For example, we can open "*System Settings*" in control panel of a Windows client machine and enter the domain name of the Windows Server. In order to add a Client system to a Server we need administrative privileges of the Client system.

2. Move the ADMX file into *%systemroot%\sysvol\domain\policies\PolicyDefinitions* and the ADML file into *%systemroot%\sysvol\domain\policies\PolicyDefinitions\en-us* so that these templates are available in the Group Policy Management Console (GPMC) tool.

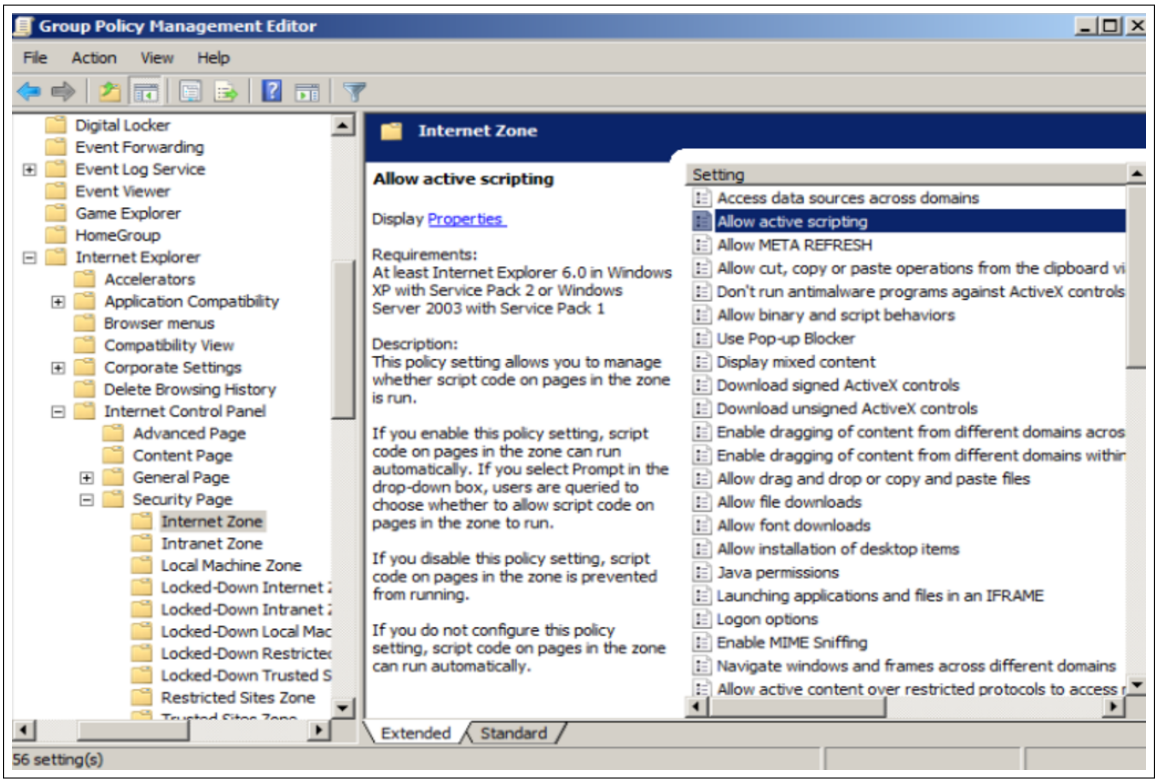


Figure 2.2: Browser Policies Selection in GPMC

3. Now in command prompt type in *GPMC.msc* and press enter, if the current operating system supports GPO it opens a window named Group Policy Management Console. Group Policy Management Console is shown in Figure 2.1.

4. Different groups of client systems which are connected to the current server are displayed on the monitor. Select the required group to configure required settings.

5. Computer configuration and user configuration are the two configurations available on the left side of this window. The policies of an ADMX are displayed in either of these configurations or both of them based on the class attribute value of a policy. For example, by using "*Group Policy Management Console*" we can navigate to "*Security Page*" category in Internet Explorer to find "*Java Permissions*" setting configure this setting which corresponding to IE browser. Browser Policies Selection in GPMC is shown in Figure 2.2.

6. Now a system administrator can select *Administrative Templates* from either of the configurations depending on the requirement of a user and can navigate through the different directories on the right side in this window to find a required policy and double click on

the policy to open another window (Figure 2.4) which gives options to enable, disable or set it to not configured. By default all policies are set to not configured.

7. Click on "*Apply*" to save changes made on a particular policy.

8. The selected settings will be applied on the clients once the group policy in the client is restarted. In order to restart group policies in client systems we can use `gpupdate/force` [13] command remotely from the Server or restart the client systems manually.

Active Directory has multiple options to configure different settings in the Windows client systems. Some of the ADMX files correspond to the configuration files of the major browsers. These settings can be utilized to configure major browsers on the Windows client systems in a network. Detailed analysis of the files with respect to major browsers settings will be discussed in Chapter 3 and Chapter 4 of this thesis.

2.4 Local Group Policy Editor in Client Systems

Using Local Group Policy Editor, policies can be enabled manually in certain client operating systems which have the "*local group policy object editor*". This method can be used by small organizations to manually configure each browser in each client system individually. Some of the Windows client operating systems which have Local Group Policy Editor are Vista Business, Vista Ultimate, Vista Enterprise, Windows 7 Professional, Windows 7 Ultimate, Windows 7 Enterprise, Windows 8 Pro, and Windows 8 Enterprise editions [8]. Client systems can be used to manually configure ADMX files by using the following steps :

1. Create an ADMX and corresponding ADML file or download them from a reliable source. Microsoft provides an Internet Explorer ADMX file.

2. In order to parse administrative templates in the GPO editor, move the ADMX file into *%systemroot%\Policy Definitions*, here %systemroot% is the Windows directory and ADML file into *%systemroot%\Policy Definitions\en-us*, here en-us is for US english.

3. Now in command prompt type in *gpedit.msc* and press enter, if the current operating system supports GPO it opens a window named Local Group Policy Editor. For example, by using "*Local Group Policy Editor*" we can navigate to "*Security Page*" category in Internet Explorer to find "*Java Permissions*" setting configure this setting which corresponding to IE browser. Local Group Policy Editor is shown in Figure 2.3.

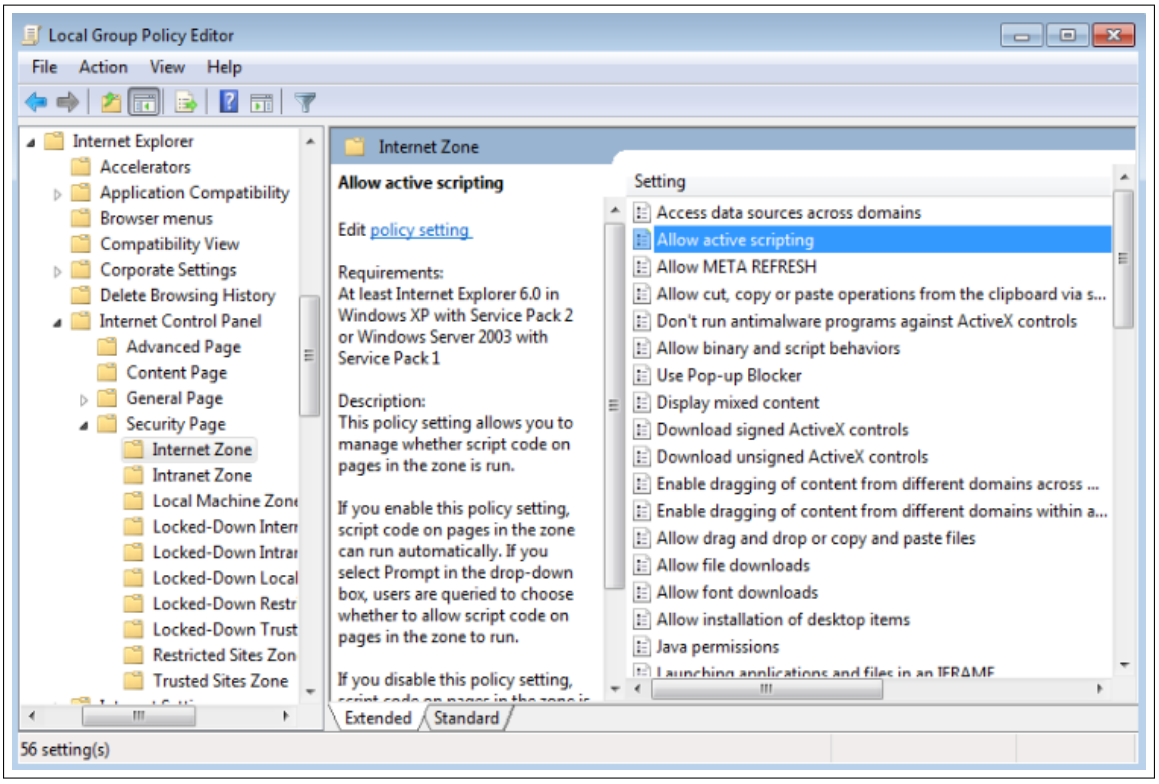


Figure 2.3: Local Group Policy Editor in Windows 7

4. Computer configuration and user configuration are the two configurations available on the left side of this window. The policies of an ADMX are displayed in either of these configurations or both of them, this is based on the class attribute value of a policy.

5. Now a user with a supported Windows client operating system can select *Administrative Templates* from either of the configurations depending on the requirement of a user and can navigate through the different directories on the right side in this window to find a required policy and double click on the policy to open another window which gives options to enable, disable or set it to not configured. By default all policies are set to not configured. Selected Setting Options Window is shown Figure 2.4.

6. Click on apply to save changes made on a particular policy.

2.5 Procedure Involved in Configuring Internet Explorer Settings using Local Group Policy Object Editor and Group Policy Management Console

Internet Explorer (IE) ADMX files are already available in *Policy Definitions* folder in all the Windows operating systems and these files get updated as soon as this browser gets updated.

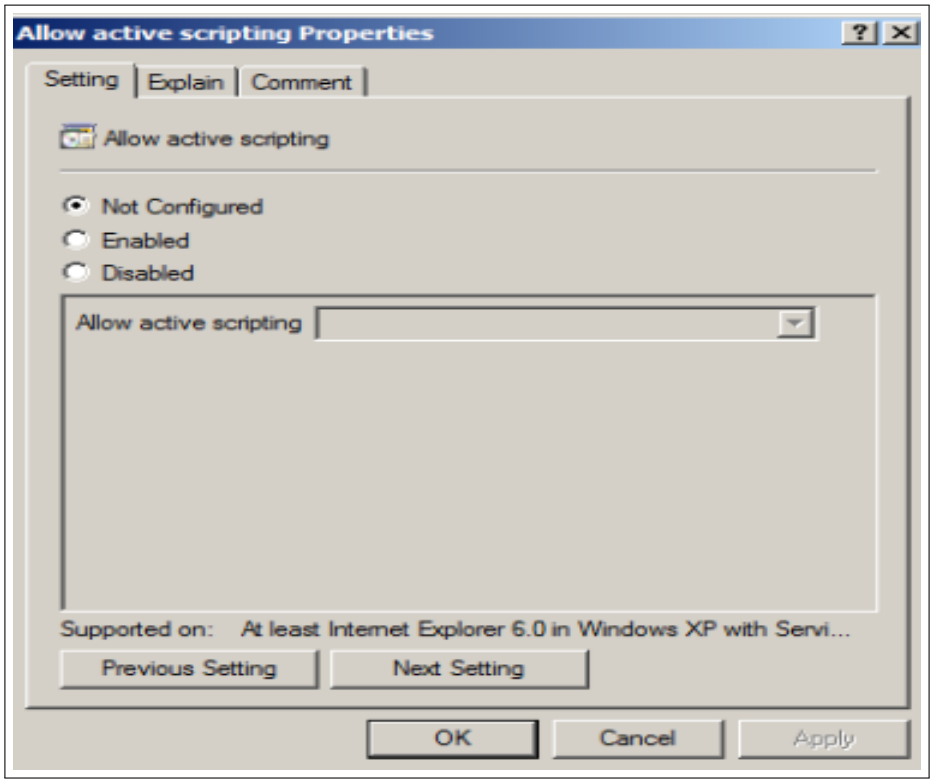


Figure 2.4: Selected Setting Options Window

This automatic update is possible because the Windows operating systems and ADMX files corresponding to IE are developed by Microsoft so they are compatible with each other. If system administrators intend to create new custom files and configure each client manually, they should create and store an ADMX file in %systemroot%\Policy Definitions in client machines in order to allow "*Local Group Policy Editor*" to apply changes on individual client systems or if they intend to remotely configure multiple client systems they can store ADMX and ADML files in *%systemroot%\sysvol\domain\policies\PolicyDefinitions* in domain server system in order to allow "*Group Policy Management Console*" to apply changes to client systems remotely. They can use file name as *inetres.admx* and ADML file in *%systemroot%\Policy Definitions\en-us* with file name as *inetres.adml*. Other names can also be used for ADMX files but ADML file name should match to its corresponding ADMX file name. ADMX file modifications are reflected in the GPO editor in *machine configuration* or *user configuration* or in *both* sections depending on the value of the *class* attribute in the policies of an ADMX file. Each policy is placed in the policies portion of the ADMX file. From now on the terms *Internet Explorer or IE*, in context of this thesis, should be understood as a reference to Internet Explorer version 10.0.9200.

2.6 Procedure Involved in Configuring Google Chrome Settings using Local Group Policy Object Editor and Group Policy Management Console

Google chrome ADMX and ADML files can be created [35] [24] and copied to %system-root%\Policy Definitions in client machines for manual configuration of each client by using "*Local Group Policy Editor*" or if system administrators intend to remotely configure multiple client systems they can place ADMX and ADML files in domain server system in *%system-root%\sysvol\domain\policies\PolicyDefinitions* in order to allow "*Group Policy Management Console*" to apply changes to client systems remotely. Each policy is placed in the policies portion of the ADMX file. From now on the terms *Google Chrome or Chrome*, in context of this thesis, should be understood as a reference to Google Chrome version 37.0.2062.

2.7 Procedure Involved in Configuring Mozilla Firefox Settings using Local Group Policy Object Editor and Group Policy Management Console

Mozilla Firefox is one of the popular major browsers, but it is a third party browser which is not connected to Windows Registry. Thus it is not directly affected by any registry changes specific to this browser. This increases the complexity of adding Mozilla Firefox ADMX and ADML files to AD. From now on the terms *Mozilla Firefox or Firefox*, in context of this thesis, should be understood as a reference to Mozilla Firefox version 33.0.2. Mozilla Firefox settings can be configured by changing entries in *about:config* [23]. Each entry in *about:config* consists of preference name, status, type and value. These entries can be configured mainly as three types: boolean, integer and string. Firefox requires an external add-on called "GPO for Firefox" to configure administrative templates and connect Firefox to the Windows registry [30]. However, Firefox doesn't have many settings in the ADMX file and it is not developed by Mozilla support services so these files have to be acquired from third party developers which may not be trustworthy.

The procedure for installing GPO for Firefox add-on is:

1. Acquire the GPO for Firefox add-on from a trusted web site [22].
2. Extract the xpi file using WinZip or WinRaR.
3. Open install.rdf file in GPO for Firefox add-on directory with a text editor.
4. Use the ID string value as the folder name for the add-on folder.

5. After renaming the folder, place it in the firefox extensions folder. By default firefox extensions in Windows 32 bit is "*C:\Program Files\Mozilla Firefox\extensions*" and in Windows 64 bit it is "*C:\Program Files (x86)\Mozilla Firefox\extensions*".

6. Then the add-on will automatically install and pop-ups an alert the next time Firefox is opened to confirm whether a user trusts that add-on. It can be whitelisted add-on or allow it in Firefox.

This process involves manual installation and configuration of different entries in Mozilla Firefox. It is a complex task and only experienced system administrators or experienced users would be in general capable of installing and managing these settings.

2.8 FreeIPA for Linux Environment

In order to expand the administrative tools to configure security configuration in Linux networked environment RED HAT [28] developed the FreeIPA project [29]. FreeIPA can be used to configure multiple browsers in Linux operating systems. This is an open source project which focuses on solving one of the limitations faced by Active Directory, which allows it to remotely configure only Windows operating systems. However, FreeIPA overcomes this limitation since it can be used to configure Linux client systems and can be integrated with Active Directory to configure the Windows client systems. FreeIPA concentrates on expanding the administrative tools to Linux operating system but it was not created to create a secure browsing environment. The main issues we may come across if we use FreeIPA to configure security settings of multiple browsers in multiple platforms are:

1. FreeIPA requires Active Directory in order to configure browser settings in Windows client systems. This eventually leads to the same problems involved in using Active Directory, these problems are presented in Section 2.9.

2. FreeIPA does not map similar settings in different browsers. This is similar to the problems we have with Windows browsers configurations. This leads to an issue where system administrators have to manually configure individual similar settings in each browser.

2.9 Drawbacks of Available Solutions

Organizations which intend to remotely configure multiple browsers by using currently available methods and administrative tools will come across certain scenarios. Some of the drawbacks of this available solutions are:

1. *Small Companies cannot afford a Microsoft Windows server infrastructure:* Many small scale companies can afford to buy licensed versions of Windows Server but they don't have enough funds to hire staff to setup and maintain Active Directory.

2. *Experienced IT employees are required to maintain AD:* Employees should have experience to handle the AD in the server which controls all the client systems to avoid any data or financial loss.

3. *Active Directory is only available for Windows operating systems:* Active Directory cannot completely configure all operating systems which limits the users to use only windows operating system. According to the statistics discussed in Chapter 1, we can observe that different users prefer to use different operating systems, so the level of productivity by the user decreases unless they have flexibility with respect to selecting operating systems.

4. *Manual configuration of similar policies in multiple browsers:* System administrators using current remote configuration tools have to manually configure each browser setting in order to achieve the same configurations in all browsers. This problem occurs because current tools do not map similar settings in different browsers and they do not implement a common language between different browsers.

Chapter 3

Contribution 1: Analysis and Categorization of Policies in Major Browsers

This chapter presents the procedures we followed to extract the policies of each major browser. Secondly, it introduces a classification of each policy in individual major browsers in such a way that it will be convenient to concentrate on security related settings. Thirdly, it presents mapping of similar policies in different browsers which are syntactically different from each other but are semantically similar. This mapping of similar policies is one of the contributions of this thesis, it shows the available common features between different major browsers. Finally, this chapter provides a mapping of differences between policies of different major browsers.

3.1 Procedure Followed to Extract the Policies of Major Browsers

Each major browser has different methods to implement specific features, so they have to be configured in different procedures as shown in Section 2.5, Section 2.6 and Section 2.7. In order to extract configuration settings from the different procedures of each major browser, we had to follow different methods and utilize different scripts.

Policies Extraction in Each Major Browser

1. *Internet Explorer*: To extract policies from the ADMX and ADML files of this browser we used python script with*"xml.dom.minidom"* library. This python script parses both the administrative files (ADMX and ADML files) and extracts the attributes of each policy into a database file. The Internet Explorer version 10.0.9200 has 874 policies by default in it's ADMX file. However, we are presently interested in configuring "Machine Level" settings so this script does not extracts the policies with "User" class attribute, so this python script extracts 770 Internet Explorer policies into our databse file.

2. *Google Chrome*: To extract policies from the ADMX and ADML files of this browser we used similar python script utilized for Internet Explorer, since both have similar file structures. However, the ADMX of this browser file does not consists policies with "User" class attribute, so all the 158 policies avaliable in the ADMX file of Google Chrome 37.0.2062 are extracted by this python script into our database file.

3. *Mozilla Firefox*: This browser does not have official ADMX and ADML files. However, we can acquire it's ADMX and ADML files from third party users, which may not be trustworthy. Hence, we created a python script which directly copies the about:config entries from this browser. The python script which we utilized autommatically creates and runs a virtual basic script to send keyboard simulations into the browser to copy each individual about:config entry into a text file. This script extracted 2256 default entries of Mozilla Firefox 33.0.2. However, the MozillaZine [23] database does not consists of the descriptions and functionalities of all thes entries, so we created another python script which parsed the text file which had all the extracted about:config entries and MozillaZine database in order to the find the common entries in these two files. This resulted in creating 263 policies of Mozilla Firefox into our databse file.

3.2 Classification of Policies in Major Browsers

Browsers have multiple policies available to configure required settings. However, many of the policies which can be utilized for security purposes are not placed in the security category because they may be related to Graphical User Interface (GUI) settings which can be configured by all users. This issue can be overcome by classifying each policy and creating a new classification display block to a user or system administrator to configure client settings from a central server. This thesis, we classified policies of each major browser into one of the classifications mentioned in Table 3.1. This classification shows a significant distinction between security and non-security settings in major browsers.

Notations for Table 3.1

1. Classification: Classification of Policies

2. Display Name: Display name of policy classification in Open Browser GP Tool

This thesis uses four classifications tags to categorize "Machine Level" settings in each major browser. In future we can add more tags in the Erlang database to create new classifications for major browsers. From now on we will concentrate on the policies which are classified as security related settings, since we are interested in secure browsing. However, even non-security related settings are also included in the Open Browser GP Tool. The syntax of classification we used in the Erlang database along with an example of a policy classification in the Erlang database is presented below:

Table 3.1: Classification of Policies

Classification	Display Name
GUI_SEC	GUI and Security related setting.
GUI_NSEC	GUI and Non-Security related setting.
NGUI_SEC	Non-GUI and Security related setting.
NGUI_NSEC	Non-GUI and Non-Security related setting.

Syntax: {'Policy_Classification_Tag','Browser_Name','Policy_Name','Classification'}.

Example: {'policyEntryClassification','Internet_Explorer','NoPrinting','GUI'}.

Erlang's *aggregate_all* command was used to analyze the number of classifications in each major browser. A detailed explanation of the Erlang database will be given in Chapter 5.

An example to find number of GUI_SEC classifications in IE:

Command:

aggregate_all(count,{'policyEntryClassification','Internet_Explorer',X,'GUI_SEC'},Count_GUI_SEC).

Output:

Count_GUI_SEC = 260.

3.3 Analysis of Similar Policies in Major Browsers

Developers of different browsers create various settings and policies to allow the user to configure their browsers. They can use custom or built-in settings to implement similar or different functionalities in different manners. After analyzing different "Machine Level" policies in major browsers we were able to extract the common policies among the major browser. These policies were created either for maintaining similar security settings, or they might be the most used for GUI related settings. The results of the mapping of similar policies is shown in Table 3.3. Among these settings, only six are common to all the three major browsers and rest are common in at least two of the major browsers. This is a policy to policy mapping, which shows corresponding policies in different browsers. Some of the configurations created by a single policy in a browser can be replicated by using multiple policies in other browsers. However, this mapping only represents policies which can perform similar functionalities by modifying a corresponding single policy in multiple browsers. This implies that these policies follow the concept of one-to-one policy mapping. These settings are categorized into the "All Browsers" section, so that we can

Table 3.2: Number of Classifications of Major Browsers Policies per Category

Browser	Classification	Count
Internet_Explorer	GUI_SEC	260
	GUI_NSEC	300
	NGUI_SEC	210
	NGUI_NSEC	0
	Total	770
Google_Chrome	GUI_SEC	58
	GUI_NSEC	78
	NGUI_SEC	22
	NGUI_NSEC	0
	Total	158
Mozilla_Firefox	GUI_SEC	47
	GUI_NSEC	147
	NGUI_SEC	69
	NGUI_NSEC	0
	Total	263

create a new category in the browsers section of Open Browser GP tool which gives us the ability to configure similar settings by configuring a corresponding single setting in all major browsers. Once the "All Browser" settings are configured in the Open Browser GP tool, all the corresponding settings in multiple browsers are modified internally by the Open Browser tool itself. Similar to the example shown in Listing 3.1, the mapping of policies has to be represented in the Erlang database for the Open Browser GP tool to parse it and configure corresponding settings.

Description of each Predicate from Listing 3.1

1. *policyEntryMapping* is used for mapping similar policies in different browsers.

2. *All_Browsers* is used to identify this settings belongs to all browsers category in Open Browser GP Tool.

Listing 3.1: An Excerpt of the Erlang Database Showing Javascript Policy Mapping

```
1 {'policyEntryName','JavaScript'}.
2 {'policyEntryDescription','All_Browsers','JavaScript','This
    policy setting configures whether JavaScript is enabled or
    disabled in Internet Explorer, Google Chrome and Mozilla
    Firefox Browsers. It corresponds to (Allow active scripting)
    in Internet Explorer, (Default JavaScript setting) in Google
    Chrome and (Setting to enable or disable Javascripts) in
    Mozilla Firefox. Internet Explorer has the same setting in
    different zones, we are using the setting available in (
    Internet Zone). If we want to map this setting to other zones
    we can change the mapping policy name in the database and
    change the zone name in the description to avoid confusion.'}.
3 {'policyEntryDisplayName','All_Browsers','JavaScript','Allow and
    disallow JavaScript'}.
4 {'policyEntrySupportedOn','All_Browsers','JavaScript','Internet
    Explorer version10, Google Chrome version37 and Mozilla
    Firefox version33'}.
5 {'policyEntryParent','All_Browsers','JavaScript','Scripts'}.
6 {'policyEntryMapping','All_Browsers','JavaScript','
    Internet_Explorer','IZ_PolicyActiveScripting_1','0','3'}.
7 {'policyEntryMapping','All_Browsers','JavaScript','Google_Chrome'
    ,'DefaultJavaScriptSetting','1','2'}.
8 {'policyEntryMapping','All_Browsers','JavaScript','
    Mozilla_Firefox','JavaScriptEnabled','enabled','disabled'}.
```

3. *JavaScript* is used to specify a common name for all the corresponding policies.

4. *Internet_ Explorer, Google_ Chrome and Mozilla_ Firefox* are used to specify the mapped policy browser name.

5. *IZ_ PolicyActiveScripting_ 1, DefaultJavaScriptSetting and JavaScript* are used to specify the policy name available in the Erlang database.

6. The remaining predicates allow enabling and disabling values of a selected policy.

Note that if a system administrator wants to only map policies of two browsers he/she can only enter those predicates by skipping the third browser mapping predicate in the Erlang database.

Notations for Table 3.3

1. All Browsers: Policy name for All Browsers

2. IE: Policy name in Internet Explorer mapped to the All browsers policy

3. Chrome: Policy name in Google Chrome mapped to the All browsers policy

4. Firefox: Policy name in Mozilla Firefox mapped to the All browsers policy

5. N/A: Policy is not available in this browser

Table 3.3: Mapping of Similar Policies in Major Browsers

EN	All Browsers	IE	Chrome	Firefox
	Description			
1	Cache_Size_-Setting	DefaultDomain-CacheLimitInMB	DiskCacheSize	Cache_Size
	This policy setting is used to set the cache size in Internet Explorer, Google Chrome and Mozilla Firefox Browsers. In Internet Explorer it is set in MB, whereas in Google Chrome and Firefox it is set in KB. So set this policy setting according to the requirements and available system cache size. It corresponds to (Set default storage limits for websites) in Internet Explorer, (Set disk cache size in bytes) in Google Chrome and (Set Browser Cache Size) in Mozilla Firefox.			
2	CrashRestore	DisableACR-Prompt	N/A	Crash_restore
	This policy setting allows us to configure the browser to prompt when the browser tries to recover from any crash sessions. It corresponds to (Turn off Automatic Crash Recovery) in Internet Explorer and (Crash Recovery) in Mozilla Firefox.			
3	DNSPrefetching	N/A	DnsPrefetchin-gEnabled	DNS
	This policy setting is used to activate or deactivate DNS prefetching. If we enable this setting DNS prefetcing is activated and deactivated if we disable this setting. It corresponds to (Enable network prediction) in Google Chrome and (Disable DNS Prefetching) in Mozilla Firefox.			
4	Default_-Browser_Check	N/A	DefaultBrowser-SettingEnabled	Check_Default_-Browser
	This policy setting configures to check whether the browser is the default browser in a given system in Google Chrome and Mozilla Firefox Browsers. If we enable this setting then the browser will prompt if it is not the default browser. It corresponds to (Set Chrome as Default Browser) in Google Chrome and (Check if firefox is the default browser) in Mozilla Firefox.			
5	DeveloperTools	DisableDeveloper-Tools	DeveloperTools-Disabled	N/A
	This policy setting configures whether a browser allows or disallows access to developer tools. If we enable this policy developer tools cannot be accessed by a user in Internet Explorer and Google Chrome. It corresponds to (Turn off Developer Tools) in Internet Explorer and (Disable Developer Tools) in Google Chrome.			

6	Display_Images	N/A	DefaultImagesSetting	Permission_Images
	This policy setting configures whether we can display images or not while pages load in Google Chrome and Mozilla Firefox Browsers. It corresponds to (Default images setting) in Google Chrome and (Allow or disallow images to load) in Mozilla Firefox.			
7	Download-DirectorySetting	N/A	DownloadDirectory	Download_Dir
	This policy setting is used to set the download directory of the browser. It corresponds to (Set download directory) in Google Chrome and (Set Download Directory) in Mozilla Firefox.			
8	Geo_Location_Setting	GeolocationDisable	DefaultGeolocationSetting	Geo_Location
	This policy setting configures whether a browser can track GEO location of the system. If we enable this setting then GEO location is tracked by websites and disallowed if it is disabled in Internet Explorer, Google Chrome and Mozilla Firefox Browsers. It corresponds to (Turn off browser geolocation) in Internet Explorer, (Default geolocation setting) in Google Chrome and (Setting to enable or disable GEO location) in Mozilla Firefox.			
9	HomePage	N/A	HomepageLocation	Home_Page
	This policy setting configures home page of Google Chrome and Mozilla Firefox Browsers. It corresponds to (Configure the home page URL) in Google Chrome and (Home Page) in Mozilla Firefox.			
10	JavaScript	IZ_PolicyActiveScripting_1	DefaultJavaScriptSetting	JavaScriptEnabled
	This policy setting configures whether Javascript is enabled or disabled in Internet Explorer, Google Chrome and Mozilla Firefox Browsers. It corresponds to (Allow active scripting) in Internet Explorer, (Default JavaScript setting) in Google Chrome and (Setting to enable or disable Javascripts) in Mozilla Firefox. Internet Explorer has the same setting in different zones, we are using the setting available in (Internet Zone). If we want to map this setting to other zones we can change the mapping policy name in the database and change the zone name in the description to avoid confusion.			
11	Max_Proxy_Setting	N/A	MaxConnectionsPerProxy	Max_Proxy
	This policy setting is used to set the maximum number of connections per proxy in Google Chrome and Mozilla Firefox Browsers. It corresponds to (Maximal number of concurrent connections to the proxy server) in Google Chrome and (Set maximum number of connections to proxy server) in Mozilla Firefox.			

12	Plugin_Prompt_-Setting	IZ_PolicyRunActiveXControls_1	DefaultPluginsSetting	Plugin_Prompt
	This policy setting configures whether a browser should run plugins only after click or run plugins automatically. If we enable this policy then we will get a prompt to run plugins in Internet Explorer, Google Chrome and Mozilla Firefox Browsers. It corresponds to (Run ActiveX controls and plugins) in Internet Explorer, (Default plugins setting) in Google Chrome and (Setting to run plugins only on click) in Mozilla Firefox. Internet Explorer has same setting in different zones, we are using the setting available in (Internet Zone). If we want to map this setting to other zones we can change the mapping policy name in the database and change the zone name in the description to avoid confusion.			
13	Plugin_Setting	IZ_PolicyRunActiveXControls_1	DefaultPluginsSetting	N/A
	This policy setting configures whether a browser allows or disallows plugins. If we enable this policy all plugins can run in Internet Explorer and Google Chrome. It corresponds to (Run ActiveX controls and plugins) in Internet Explorer and (Default plugins setting) in Google Chrome. Internet Explorer has same setting in different zones, we are using the setting available in (Internet Zone). If we want to map this setting to other zones we can change the mapping policy name in the database and change the zone name in the description to avoid confusion.			
14	PopUpBlocker	IZ_PolicyBlock-PopupWindows_1	DefaultPopupsSetting	PopUpsDisabled
	This policy setting configures whether pop-ups are allowed or disallowed in Internet Explorer, Google Chrome and Mozilla Firefox Browsers. It corresponds to (Use Pop-up Blocker) in Internet Explorer, (Default popups setting) in Google Chrome and (Setting to configure Pop-ups) in Mozilla Firefox. Internet Explorer has same setting in different zones, we are using the setting available in (Internet Zone). If we want to map this setting to other zones we can change the mapping policy name in the database and change the zone name in the description to avoid confusion. If this setting is disabled it will allow pop-ups on white-listed pages in Mozilla firefox, it was mapped in that manner since it was a recommended setting. If you want to disable it on all sites change the disabled mapping value for Mozilla firefox to 3 instead of 2.			
15	PrintSetting	NoPrinting	PrintingEnabled	N/A
	This policy setting is used to allow or disallow printing in Internet Explorer and Google Chrome Browsers. If we enable this setting then the user can print a webpage or document from the specified browser and if it is disabled users cannot print. It corresponds to (Turn off Print Menu) in Internet Explorer and (Enable printing) in Google Chrome.			

16	Restore_-Previous_-Session	ContinuousBrowsing	RestoreOnStartup	Start_Up_Pages
	This policy setting configures the browser such that, it restarts with the web pages from last browsing session. If we enable this setting the browsers will restart with last browsing session and if we disable this setting they will start with a blank page in Internet Explorer, Google Chrome and Mozilla Firefox Browsers. It corresponds to (Start Internet Explorer with tabs from last browsing session) in Internet Explorer, (Action on startup) in Google Chrome and (Set how the browser should start) in Mozilla Firefox.			
17	SafeBrowsing-Setting	N/A	SafeBrowsingEnabled	Safe_Browsing
	This policy setting is used to activate or deactivate safe browsing to detect phishing malware while loading websites. If we enable this setting safe browsing is activated and deactivated if we disable this setting. It corresponds to (Enable Safe Browsing) in Google Chrome and (Enable Safe Browsing) in Mozilla Firefox.			

We used python scripts to extract the data and the predetermined policy names from ADMX and ADML files of IE and Chrome browsers into Table 3.3. Each row in this table is numbered in ascending order and consists of two sub rows, the first column of the first sub row consists of an "*All Browsers*" policy name, the second, third and fourth columns of the first sub row presents policy names with respect to Internet Explorer, Google Chrome and Mozilla Firefox respectively. The second sub row of each row provides a brief description about the All Browsers policy. This description is added manually. In the future, when a new browser is configured by using Open Browser GP tool, it can be mapped in all browsers section to represent similar settings among different browsers.Notice that most of the policy names have underscores but none of them have hyphens, these are only used to show the continuations of the policy name in each column.

Table 3.4: Classifications of Common Settings in Major Browsers

Category	**Classification**	**Count**
All_Browsers	GUI_SEC	8
	GUI_NSEC	7
	NGUI_SEC	2
	NGUI_NSEC	0
	Total	17

The "All Browsers" settings were classified similar to the classifications of policies in each major browser, this classification provides information about the existence of common security settings. All Browsers settings classifications are shown in Table 3.4. Further details about the advantages and need to develop common settings is discussed in Chapter 4.

3.4 Analysis of Dissimilar Policies in Major Browsers

This section presents the results of analyzing dissimilarities between different policies in different major browsers. Each browser can be configured in different ways; some of the configuration policies may have similar functionalities and some of them can implement different policies in different manners. Since we are interested in security related settings in this thesis, we extracted only the security related classifications of each browser and eliminated the settings which are common in all major browsers, then mapped each setting of each major browser individually in three different tables. The results of analyzing security settings are GUI_SEC and NGUI_SEC settings, which are presented in Table 3.2. These tables propose the possible ways of configuring security settings in different browsers with respect to each browser setting.

The Google Chrome, Internet Explorer and Mozilla Firefox dissimilarities mapping tables were too long to show more than an excerpt of these tables. A policy number is provided which can be referred to in Table A.1, Table A.2 and Table A.3 respectively.

Each row in Table 3.5 is numbered with reference number in Table A.3 and consists of two sub rows. The first column of the first sub row consists of a Mozilla policy name followed by its display name in parenthesis, the second and third column of the first sub row provide information about the possible ways of configuring similar setting in Internet Explorer and Google Chrome. The second sub row of each row provides a brief description about the Mozilla Firefox policy.

Similarly Table 3.6 entries can be referred in Table A.1 and Table 3.7 entries can be referred in Table A.2. These tables will be a useful reference to verify whether a similar configuration in multiple browsers can be accomplished by modifying single or multiple available settings. The data in Table A.1, Table A.2 and Table A.3 were extracted from the Erlang database of the Open Browser GP tool by using python scripts. However, the text which is in `monospace font` in these tables was modified manually by analyzing descriptions of each policy, this font is used to represent the difference between extracted data from the Erlang database and the manual data entries.

Notations for Table 3.5

1. IE: Camparison in Internet Explorer
2. Chrome: Camparison in Google Chrome
3. Firefox: Mozilla Firefox (policy name and display name)
4. Description: Description about the policy in Mozilla Firefox
5. N/A: Policy is not available in this browser
6. RN Reference number in Table A.3

Table 3.5: An Excerpt of Comparison of Security Related Settings for Mozilla Firefox with Respect to Internet Explorer and Google Chrome

RN	Firefox	IE	Google Chrome
	Description		
1	Extensions_Delay (Delay When Installing Extensions)	N/A	N/A
	This policy allows us to configure browser such that, we can set the time delay during installing new extensions.		
2	DNS (Disable DNS Prefetching)	N/A	This Setting is available as DnsPrefetchingEnabled (Enable network prediction) in this browser.
	This feature allows Firefox to perform domain name resolution proactively. If we enable this setting, DNS prefetching is disabled. If it is disabled Firefox can activate DNS prefetching.		
3	Safe_Browsing (Enable Safe Browsing)	Similar semantics can be achieved by modifying multiple settings at different zones	This Setting is available as SafeBrowsingEnabled (Enable Safe Browsing) in this browser.
	This setting allows us to enable safe browsing mode such that the browser can detect malicious content in web pages. If we enable this setting safe browsing is activated and deactivated if we disable this setting.		

Notations for Table 3.6

1. IE: Camparison in Internet Explorer
2. Chrome: Google Chrome (policy name and display name)
3. Firefox: Camparison in Mozilla Firefox
4. Description: Description about the policy in Google Chrome
5. N/A: Setting is not available in this browser
6. RN Reference number in Table A.1

Table 3.6: An Excerpt of Comparison of Security Related Settings for Google Chrome with Respect to Internet Explorer and Mozilla Firefox

RN	Chrome	IE	Firefox
	Description		
75	URLBlacklist (Block access to a list of URLs)	`Similar semantics can be achieved by modifying multiple settings at different zones`	`Similar semantics can be achieved by using different third party Add-ons`
	Blocks access to the listed URLs. This policy prevents the user from loading web pages from blacklisted URLs. A URL has the format scheme://host:port/path. The optional scheme can be http, https or ftp. Only this scheme will be blocked; if none is specified, all schemes are blocked. The host can be a hostname or an IP address. Subdomains of a hostname will also be blocked. To prevent blocking subdomains, include a . before the hostname. The special hostname * will block all domains. The optional port is a valid port number from 1 to 65535. If none is specified, all ports are blocked. If the optional path is specified, only paths with that prefix will be blocked. Exceptions can be defined in the URL whitelist policy. These policies are limited to 1000 entries; subsequent entries will be ignored. If this policy is not set no URL will be blacklisted in the browser.		
13	ImagesAllowedForUrls (Allow images on these sites)	`N/A`	`N/A`
	Allows you to set a list of url patterns that specify sites which are allowed to display images. If this policy is left not set the global default value will be used for all sites either from the DefaultImagesSetting policy if it is set, or the users personal configuration otherwise.		

38	DeveloperToolsDisabled (Disable Developer Tools)	`Setting is available as DisableDeveloperTools (Turn off Developer Tools) in this browser`	`Similar semantics can be achieved by modifying multiple entries in about:config`
	Disables the Developer Tools and the JavaScript console. If you enable this setting, the Developer Tools can not be accessed and web-site elements can not be inspected anymore. Any keyboard shortcuts and any menu or context menu entries to open the Developer Tools or the JavaScript Console will be disabled. Setting this option to disabled or leaving it not set will allow the use to use the Developer Tools and the JavaScript console.		

Notations for Table 3.7

1. IE: Internet Explorer (policy name and display name)
2. Chrome: Camparison in Google Chrome
3. Firefox: Camparison in Mozilla Firefox
4. Description: Description about the policy in Internet Explorer
5. N/A: Setting is not available in this browser
6. RN Reference number in Table A.2

Table 3.7: An Excerpt of Comparison of Security Related Settings for Internet Explorer with Respect to Google Chrome and Mozilla Firefox

RN	IE	Chrome	Firefox
	Description		
76	PopupBlocker_AllowList (Pop-up allow list)	`Similar semantics can be achieved by modifying multiple settings`	`Similar semantics can be achieved by using different third party Add-ons.`
	This policy setting allows you to specify a list of web sites that will be allowed to open pop-up windows regardless of the Internet Explorer processs Pop-Up Blocker settings. If you enable this policy setting, you can enter a list of sites which will be allowed to open pop-up windows regardless of user settings. Only the domain name is allowed, so www.contoso.com is valid, but not http://www.contoso.com. Wildcards are allowed, so *.contoso.com is also valid. If you disable this or do not configure this policy setting, you will not be able to provide a default Pop-up Blocker exception list. Note: You can disable users from adding or removing websites to the exception list by enabling Turn off Managing Pop-up Allow list policy.		

90	IZ_Policy_Phishing_-1, IZ_Policy_-Phishing_2, IZ_-Policy_Phishing_-3, IZ_Policy_-Phishing_4, IZ_-Policy_Phishing_5, IZ_Policy_Phishing_-6, IZ_Policy_-Phishing_7, IZ_-Policy_Phishing_8, IZ_Policy_Phishing_-9, IZ_Policy_-Phishing_10 (Turn on SmartScreen Filter scan)	N/A	N/A
	This policy setting controls whether SmartScreen Filter scans pages in this zone for malicious content. If you enable this policy setting, SmartScreen Filter scans pages in this zone for malicious content. If you disable this policy setting, SmartScreen Filter does not scan pages in this zone for malicious content. If you do not configure this policy setting, the user can choose whether SmartScreen Filter scans pages in this zone for malicious content. Note: In Internet Explorer 7, this policy setting controls whether Phishing Filter scans pages in this zone for malicious content.		
147	IZ_Zonemaps (Site to Zone Assignment List)	N/A	N/A
	This policy setting allows you to manage a list of sites that you want to associate with a particular security zone. These zone numbers have associated security settings that apply to all of the sites in the zone. Internet Explorer has 4 security zones, numbered 1-4, and these are used by this policy setting to associate sites to zones. They are: (1) Intranet zone, (2) Trusted Sites zone, (3) Internet zone, and (4) Restricted Sites zone. Security settings can be set for each of these zones through other policy settings, and their default settings are: Trusted Sites zone (Low template), Intranet zone (Medium-Low template), Internet zone (Medium template), and Restricted Sites zone (High template). (The Local Machine zone and its locked down equivalent have special security settings that protect your local computer.) If you enable this policy setting, you can enter a list of sites and their related zone numbers. The association of a site with a zone will ensure that the security settings for the specified zone are applied to the site. For each entry that you add to the list, enter the following information: Valuename A host for an intranet site, or a fully qualified domain name for other sites. The valuename may also include a specific protocol. For example, if you enter http://www.contoso.com as the valuename, other protocols are not affected. If you enter just www.contoso.com,then all protocols are affected for that site, including http, https, ftp, and so on. The site may also be expressed as an IP address (e.g., 127.0.0.1) or range (e.g., 127.0.0.1-10). To avoid creating conflicting policies, do not include additional characters after the domain such as trailing slashes or URL path. For example, policy settings for www.contoso.com and www.contoso.com/mail would be treated as the same policy setting by Internet Explorer, and would therefore be in conflict. Value - A number indicating the zone with which this site should be associated for security settings. The Internet Explorer zones described above are 1-4. If you disable or do not configure this policy, users may choose their own site-to-zone assignments.		

The total number of security related policies in IE is 470. In Table A.2 we eliminated the settings which are common in all major browsers. Finally, some of the settings in IE are available

in multiple zones but they perform the same functionality with respect to the specified zone, so these were grouped into a single setting to represent the data in an efficient manner. An example of this grouping is shown with "*Turn on SmartScreen Filter scan*" setting in Table 3.7. This grouping decreases Table A.2 to 171 data entries. These tables provide information about some of the security related policies in each browser and the possible ways of configuring similar settings in other major browsers.

Chapter 4

Contribution 2: Toward a Common Language to Achieve Secure Browsing Systems

This chapter provides some examples which illustrate the need for common browser security settings and explain the complexity in configuring individual settings in one or multiple browsers. Secondly, it presents the need for common language and common settings to configure major browsers and propose some possible solutions to develop and maintain common configurations. Finally, this chapter provides some advantages of using a common procedure and language to configure different major browsers.

4.1 Need for a Common Language and Common Settings

Each browser has some preconfigured settings developed and updated for different versions by the browser developers, while some of the settings are available in the browser's menu, many of them are only available through a configuration file in the ADMX format. However, these ADMX files must be individually developed and imported in the GPMC tool (Group Policy Management Console as discussed in Section 2.2) to load different settings. This increases the complexity of updating each configuration file in the directory for GPMC tool to read. A system administrator would need to learn all the possible ways to configure multiple browsers, corresponding administrative tools, and templates to configure client systems in large organizations. Also, small organizations usually do not have dedicated system administrators. Managing specific settings in different browsers is a complex task for the system administrators, since the project managers or end users will only give a generic description about the configuration they require, but the system administrator has to know all the corresponding settings in each browser to configure them.

For example, if a system administrator has to configure browsers to allow JavaScript only on trusted websites he/she has to configure multiple settings or use different techniques to achieve this goal, as explained in "*Steps to Configure Settings in Major Browsers to Allow JavaScript only on Trusted Websites*". This is not the only way to accomplish these settings but it is one of the possible ways followed by most system administrators using the GPMC tool (Active Directory). The same procedure can be followed with an Open Browser GP tool to achieve the goals mentioned in this example.

Steps to Configure Settings in Major Browsers to Allow JavaScript only on Trusted Websites

1. *In Internet Explorer:* The system administrator has to load an administrative tool such as GPMC or Open Browser GP tool, navigate to Internet Explorer settings, then assign required trusted websites to trusted zone by using "Site to Zone Assignment List" setting with policy name (IZ_Zonemaps), since IE organizes some of it's settings in zones the administrators have to find the "Allow active scripting" setting in different zones with policy names (IZ_PolicyActiveScripting_1, IZ_PolicyActiveScripting_2, IZ_PolicyActiveScripting_3, IZ_PolicyActiveScripting_4, IZ_PolicyActiveScripting_6, IZ_PolicyActiveScripting_7, IZ_PolicyActiveScripting_8, IZ_PolicyActiveScripting_9, IZ_PolicyActiveScripting_10) and disable all 9 settings; next they have to navigate to trusted zone to find "Allow active scripting" setting with policy name (IZ_PolicyActiveScripting_5) and enable this setting to allow scripts only on the websites categorized in this zone for Internet Explorer.

2. *In Google Chrome:* The system administrator has to load an administrative tool such as GPMC tool or Open Browser GP tool, navigate to Google Chrome settings, then navigate through different categories to find a setting labelled "Default JavaScript setting" with policy name (DefaultJavaScriptsetting) and disable this setting, next they have to navigate through the hierarchy of folders in Google Chrome to find "Allow JavaScript on these sites" setting with policy name (JavaScriptAllowedForUrls) and configure the list of websites to allow JavaScripts in this setting for Google Chrome.

3. *In Mozilla Firefox:* The system administrator can't directly configure this browser to allow only selected websites to run JavaScript, they have to use one of the third party add-ons to configure this setting. They can use remote execution and install an add-on called "NoScript" [12] which allows JavaScript on specific websites, but the add-on can only be locally configured at each client system by the administrator.

In Open Browser GP, we mapped similar settings in major browsers and created a new category called "All Browsers", this mapping is shown in Table 3.3. Notice that the total number of policies that can be configured by our Open Browser GP tool is 951 this is inferred from Table 3.2 and Table 3.4, but they were only 17 similar policies out of which 6 policies were present in all major browsers and the rest of them were present in any two of the browsers. After observing

the classifications of only the settings which are common for all major browsers, we noticed that among those 6 settings, 2 of them are GUI-Non Security related settings "*Allow and disallow geo location tracking*" and "*Restore browser to previous session*". By eliminating these two settings we are left with a total of 4 security settings which are common for all major browsers. This statistic shows us that only 4 out of 951 policies are common security settings in all major browsers. This implies that 0.42% of the policies are common security related settings, which leads to the question: "*How can system administrators successfully configure security policies in browsers to maintain a safe browsing environment in spite of the complexity?*". Many security settings are available in each browser which can be useful in every browser, some of the browsers many implement these settings in different manners, but they should be represented in a procedure which makes it easier for the system administrators to analyze and configure them. For example, in Internet Explorer we have a setting called "*Turn on Cross-Site Scripting Filter*", in Google Chrome we have a setting called "*Allow images on these sites*" and in Mozilla Firefox we have a setting called "*Enable Safe Browsing*", these are security related settings which are not implemented in all major browsers. Implementing similar security settings increases the possibility of creating a secure browsing environment. It is also important to develop common GUI settings to provide the end users a generic presentation in all browsers. This analysis helps us to understand the need for common settings however, to create similar settings we require a common language to maintain a mapping between these settings.

4.2 Proposed Methods for a Common Language

In Open Browser GP tool we created a database to maintain major browser settings in a common format. Similarly we are proposing to create a common language to configure all the available browsers. This language should not be limited to the server side database but it should be able to manage the settings at client side once it is transferred to a client system. This language should be either loaded directly by the browsers or executed by an agent administrative tool. There are two possible methods to create this proposed language.

Method 1: We create a "JSON" file similar to the example shown in Listing 4.1 in order to deploy browser settings into client systems and a browser has to detect these updated files which will be placed in a specific location in their operating systems. Similar to ADML files we create a separate file to accommodate the corresponding display names and description of each policy

Listing 4.1: An Example of Proposed JSON File with a Policy to Globally Disable JavaScript in Major Browsers

```
{
  "policies": {
    "policy": {
      "name": "JavaScript",
      "globally": "disabled",
      "browsers": {
        "supportedBrowser": {
          {
            "browserName": "Internet_Explorer",
            "browserVersion": "10.0.9200"
          },
          {
            "browserName": "Google_Chrome",
            "browserVersion": "37.0.2062"
          },
          {
            "browserName": "Mozilla_Firefox",
            "browserVersion": "33.0.2"
          }
        }
      }
    }
  }
}
```

Listing 4.2: An Example of Proposed XML File with a Policy to Globally Disable JavaScript in Major Browsers

```
<policies>
  <policy>
    <name>JavaScript</name>
    <globally>disabled</globally>
    <browsers>
      <supportedBrowser>
        <browserName>Internet_Explorer</browserName>
        <browserVersion>10.0.9200</browserVersion>
      </supportedBrowser>
      <supportedBrowser>
        <browserName>Google_Chrome</browserName>
        <browserVersion>37.0.2062</browserVersion>
      </supportedBrowser>
      <supportedBrowser>
        <browserName>Mozilla_Firefox</browserName>
        <browserVersion>33.0.2</browserVersion>
      </supportedBrowser>
    </browsers>
  </policy>
</policies>
```

in order to provide flexibility to create language specific files. Once an update is detected they have to create a log file, modify the respective settings and notify the server system about their updated configurations.

Method 2: We create an "XML" file similar to the example shown in Listing 4.2 in order to deploy browser settings into client systems. This XML format is similar to the ADMX files which

were presented in Section 2.2, but the ADMX files are created individually and most of them have to be updated manually. The XML files which we propose in this section should contain configurations applicable to all browsers in one single file with different versions mentioned within its tags, this allows us to update the same file when new versions of a browser are updated in an operating system. Similar to ADML files we create a seperate file to accommodate the corresponding display names and description of each policy in order to provide flexibility to create language specific files. This also allows an administrative tool to effectively map similar policies in different browsers, so it will be easier for system administrators to administer browsers security settings.

This idea of creating deployment files which can be parsed by the browsers themselves will help us to create platform independent methods of configuring multiple browsers. Based on this analysis a larger number of common settings and a common language are required in the future to help to achieve secure browsing infrastructure.

4.3 Advantages of Common Language and Common Settings

1. System administrators would be able to configure necessary browser settings effectively and efficiently in all browsers.

2. Small organizations would not need to hire experienced system administrators, minimum knowledge about browser configurations would be sufficient.

3. End users will have flexibility in choosing preferred browsers, if all the browsers have a common configuration mechanism. This will not impact the ability of users or system administrators to securely configure their browsers.

4. System administrators would not need to manually update administrative files for different browsers but just once for all browsers.

5. Novice technicians can learn a common browser configuration language easily when compared to learning different languages for each browser.

6. If the browsers can automatically parse the language of their configuration files, these files can be deployed in all operating systems and all browsers. In addition, these secure configuration files can be shared.

7. Mapping between policies of different browsers is possible if all the configurations are available in a common language.

8. It would enable the creation and maintenance of secure browsing environment in all browsers and OS platforms.

Chapter 5

Contribution 3: Open Browser GP: A Multiplatform and Multibrowser Policy Configuration Tool

This chapter briefly describes the background information about the technologies referred and used during the development of our Open Browser GP tool. Secondly, it describes the process followed to create and analyze the Open Browser GP: A Multiplatform and Multibrowser Policy Configuration Tool. Thirdly, it provides a step-by-step procedure to setup and utilize this tool. Finally, this chapter discusses the advantages and limitations of using Open Browser GP: A Multiplatform and Multibrowser Policy Configuration Tool.

5.1 Different Technologies Utilized

In order to configure secure browsing settings in major browsers we develop a user friendly, efficient, and secure tool. In this thesis, we describe *"Open Browser GP: A Multiplatform and Multibrowser Policy Configuration Tool"*. This tool would help to overcome the various problems faced by organizations when configuring web browsers. This section briefly explains the different technologies utilized to develop our tool and further details of using these technologies in our tool are explained in Section 5.2 of this thesis.

Initially, we needed to collect configuration settings from ADMX and ADML files of Internet Explorer and Google Chrome browsers. This extraction can be performed manually; however, the ADMX and ADML files contain about 1000 policies. Two individual parsers were created using the "*Python*" programming language to extract IE and Chrome policy configurations. Python is a high level, object oriented scripting language which is easy to learn, read and maintain [36]. ADMX and ADML files are in XML format, so we used the *"xml.dom.minidom"* library in Python. This library is a minimal implementation of the Document Object Model interface [26]. The libraries and modules of these parsers are written in Python 3.4.1. These parsers read the corresponding ADMX and ADML files of the specified browser and extract the required configurations for each policy into corresponding files in Erlang format for our Open Browser GP tool.

"*Erlang*" is a programming language which is used to build scalable real time systems. It was created by software developers in the Ericsson Computer Science Laboratory in 1986 to maintain systems with high availability in their laboratory [11]. Later in 1988 open source versions

Listing 5.1: An Example of Yaws Web Page

```
<html>
  <h1>Heading from HTML Tag</h1>
  <erl>
  out(Arg) -> {html, "<h2> Heading from Erlang Tag</h2>"}.
  </erl>
</html>
```

of Erlang were released which had in-built support for concurrency, distribution, and fault tolerance. The Erlang syntax is similar to the Prolog language; this allows Open Browser GP tool to read the data by using a parallel assignment. Erlang can be used to execute commands similar to prolog to extract data from an Erlang database.

In order to allow end users to easily configure multiple browsers the tool provides a GUI interface. The "Yaws" server [10] in Ubuntu was used to develop a Web-based GUI for Open Browser GP tool [10]. Yaws stands for Yet Another Web Server; it has its own dynamic content and handle requests. Yaws is capable of converting Erlang code into HTML format and display it on the web page, so the web content which is in HTML is executed similar to XML parsing and the content which is presented between Erlang tags (<erl>) is converted into HTML code by the Yaws server. An example of the Yaws code is shown in Listing 5.1.

In addition, we needed a procedure at the client side to edit the browser settings. Among the major browsers, IE and Chrome browsers settings can be configured by registry entries in the Windows operating system. The procedure to connect Firefox to the Registry is explained in Section 5.2 of this thesis. To configure the browser settings using registry entries we can import registry files in the registry or run scripts to add, modify and delete registry entries. The registry files are in ".reg format". Batch scripting is used at the client side for registry entries; however, these scripts have to be run as an administrator to apply changes in the registry. Microsoft publishes information about libraries and procedures to configure Windows operating systems for advanced users, one of these articles [14] provided the needed information regarding registry entries. The same syntax was used to create batch scripts by using the Erlang database and Open Browser GP tool at the Ubuntu server.

Syntax of Registry Entry:

```
reg add KeyName [/v EntryName|/ve] [/t DataType] [/s separator] [/d value] [/f]
```

Example of Registry Entry:

```
Reg.exe add "HKLM\SOFTWARE\Policies\Microsoft\Internet Explorer\ContinuousBrowsin-
g" /v "Enabled" /t REG_DWORD /d "1" /f
```

Finally, we needed a method to transfer and remotely execute the batch scripts in the Windows client systems. Our first attempt was to use a Windows client to configure multiple Windows clients in a network by using the "PSEXEC" tool developed by Russinovich [31] and published by Microsoft. However, we came across some drawbacks by using this tool with respect to our tool and goals. Some of the reasons for avoiding "PSEXEC" tool are:

1. It can only execute batch scripts on client systems, but cannot transfer them to client systems.
2. It needs elevated privileges to execute batch scripts.
3. It sends user name and password of client systems through the network, which would lead to security vulnerabilities to users.
4. It needs to bypass User Access Control (UAC), this leads to security vulnerabilities.

Later, we used "OSSEC" to transfer and execute batch scripts in a Windows client from an Ubuntu server. We also integrated OSSEC commands in "Open Browser GP Tool" for automatically configuring major browsers in clients by using this tool. OSSEC stands for Open Source Host-based Intrusion Detection System. It can be used for log analysis, file integrity checking, and active response. OSSEC can be used for building server-agent infrastructure [6]. Some of the reasons for choosing the OSSEC tool were:

1. The OSSEC server can transfer and execute batch scripts securely on client systems. However, it requires few modifications to perform these two tasks, the necessary modifications are described in Section 5.2 and Section 5.7 of this thesis.
2. OSSEC provides a one time installation of client-server infrastructure.
3. Mutual authentication can be performed at client systems and server system by using authentication keys created by OSSEC.
4. OSSEC does not send user credentials across the network. The server-agent traffic is encrypted and validated using pre-shared keys among the server and agent systems [6].
5. The OSSEC Client is supported in multiple operating systems. For example, OSSEC client can be installed in Linux and BSD and Mac OS X operating systems.

5.2 Development of Open Browser GP: A Multiplatform and Multibrowser Policy Configuration Tool

The Open Browser GP provides GUI interface, developed with the objective of enabling configurations of multiple browsers on multiple platforms. We created Open Browser GP tool based on the single screen concept to navigate and configure different browser settings in an efficient and user friendly manner.

Initially, we installed "*Open SSH*" server in Ubuntu to run it as a server. This can be installed from the repository and must be started by running:

```
sudo service ssh start
```

Secondly, we used the Python parsers to extract data from the ADMX and ADML into a file with Erlang format. This file acts as a database for Open Browser GP Tool, some of the entries in this database were manually inserted. An excerpt of the Erlang database is shown in Listing 5.2. This excerpt presents the Erlang format of representing settings of one of the policies in order to configure browser settings using the Open Browser GP tool.

Description about each predicate in Listing 5.2

1. *policyEntryName:* It is used for specifying a policy name.
2. *policyEntryDescription:* It is used for specifying a policy description.
3. *policyEntryBrowser:* It is used for specifying the browser corresponding to a policy.
4. *policyEntryDisplayName:* It is used for specifying the display name corresponding to a policy.
5. *policyEntrySupportedOn:* It is used for specifying the supported on version of a browser corresponding to a policy.
6. *policyEntryParent:* It is used for specifying the parent folder of a browser corresponding to a policy.
7. *policyEntryDefKey:* It is used for specifying a key in registry corresponding to a policy.
8. *policyEntryDefKeyValue:* It is used for specifying a key value in registry corresponding to a policy.
9. *policyEntryDefSubKey:* It is optional and is used for specifying a sub key in Open Browser GP corresponding to a policy. We used different sub key types to represent different

Listing 5.2: An Excerpt of the Erlang Database for our Open Browser GP Tool

```
1 {'policyEntryName','URLBlacklist'}.
2 {'policyEntryDescription','Google_Chrome','URLBlacklist','Blocks
    access to the listed URLs.  This policy prevents the user from
     loading web pages from blacklisted URLs.  A URL has the
    format scheme://host:port/path. The optional scheme can be
    http, https or ftp. Only this scheme will be blocked; if none
    is specified, all schemes are blocked. The host can be a
    hostname or an IP address. Subdomains of a hostname will also
    be blocked. To prevent blocking subdomains, include a . before
     the hostname. The special hostname * will block all domains.
    The optional port is a valid port number from 1 to 65535. If
    none is specified, all ports are blocked. If the optional path
     is specified, only paths with that prefix will be blocked.
    Exceptions can be defined in the URL whitelist policy. These
    policies are limited to 1000 entries; subsequent entries will
    be ignored.  If this policy is not set no URL will be
    blacklisted in the browser.'}.
3 {'policyEntryBrowser','Google_Chrome','URLBlacklist'}.
4 {'policyEntryDisplayName','Google_Chrome','URLBlacklist','Block
    access to a list of URLs'}.
5 {'policyEntrySupportedOn','Google_Chrome','URLBlacklist','
    Microsoft Windows XP SP2 or later'}.
6 {'policyEntryParent','Google_Chrome','URLBlacklist','Google
    Chrome'}.
7 {'policyEntryDefKey','Google_Chrome','URLBlacklist','Software/
    Policies/Google/Chrome'}.
8 {'policyEntryDefKeyValue','Google_Chrome','URLBlacklist','NULL'}.
9 {'policyEntryDefSubKey','Google_Chrome','URLBlacklist','listBox',
    'Software/Policies/Google/Chrome/URLBlacklist'}.
10 {'policyEntryDataType','Google_Chrome','URLBlacklist','REG_DWORD'
    }.
```

options, for example: text box, dropdown list etc. If a policy has to be presented in one of these formats and does not has a sub key then we can mention its key as NULL.

10. *policyEntryDataType:* It is used for specifying a data type in registry corresponding to a policy.

The importance of the Yaws webserver with respect to Open Browser GP tool was explained in Section 5.1 of this thesis. By default, Yaws was developed to listen on port 8000 [10] however, we can change the port number and content directory by modifying them in the yaws.config file. We set the port number to "8081" and the content directory to read yaws web pages to "/etc/yaws/www". Now we can place all the yaws web pages in this directory to access them from a client-side web browser, further details about starting yaws and loading Open Browser GP are discussed in Section 5.5 of this thesis.

Figure 5.1 shows an example setting of Internet Explorer in the Open Browser GP tool. Once the Open Browser GP tool is loaded we can observe that it is divided into five sections.

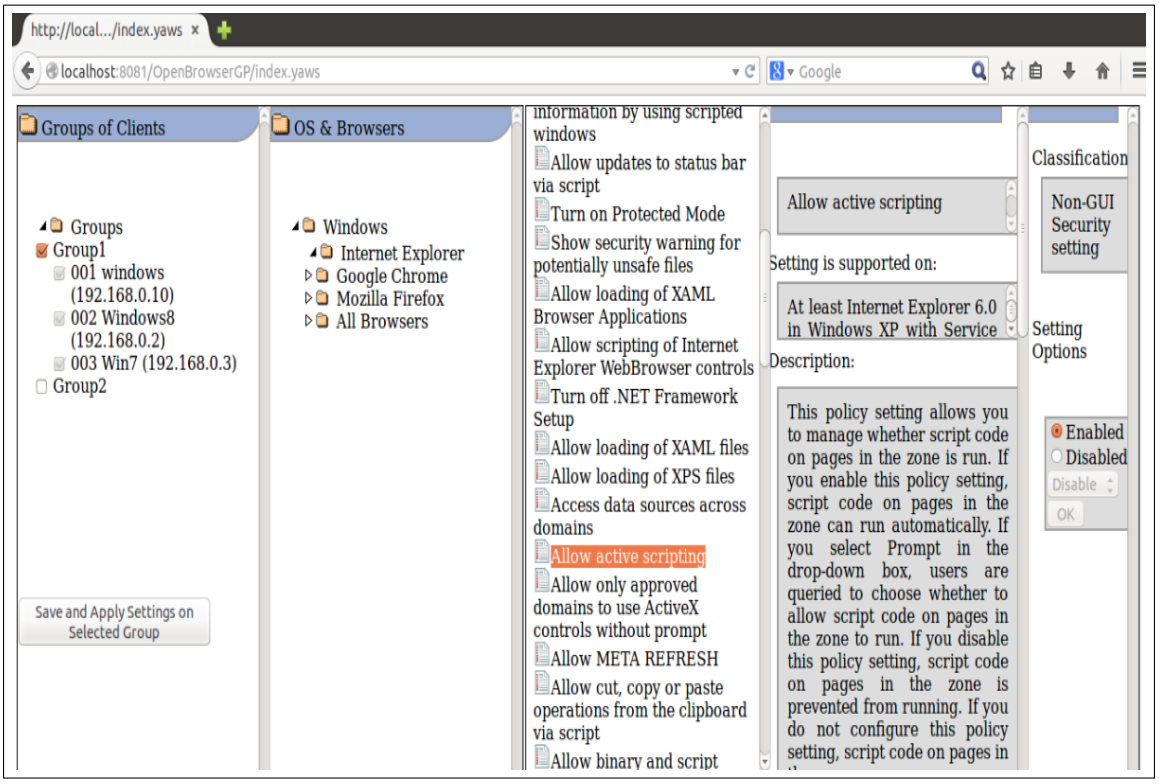


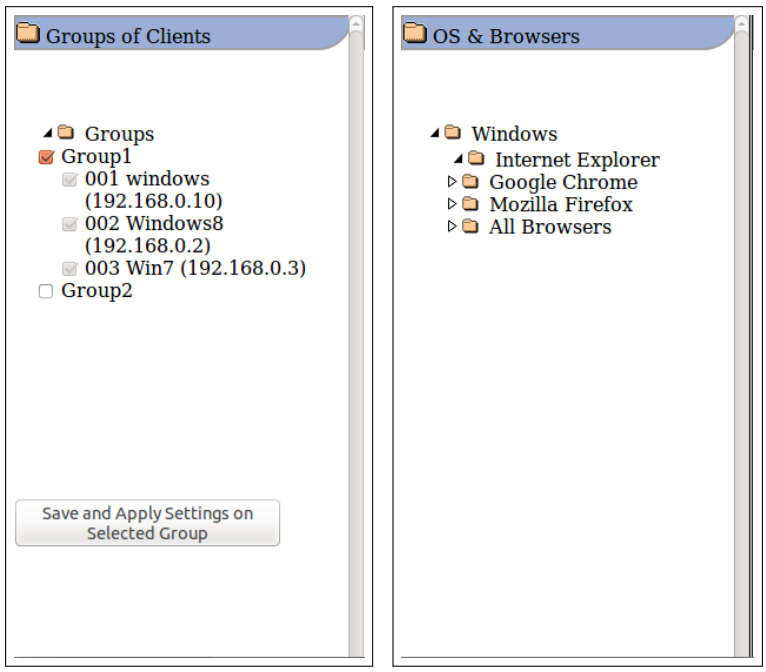
Figure 5.1: Open Browser GP: A Multiplatform and Multibrowser Policy Configuration Tool

1. *Client Groups* section in Open Browser GP tool as shown in Figure 5.2 (a) consists of options to select one of the groups of client systems connected to our server, this information is loaded from groups.pl file which we create to map the corresponding OSSEC clients connected, in this section one of groups has to be selected for Open Browser GP to work.

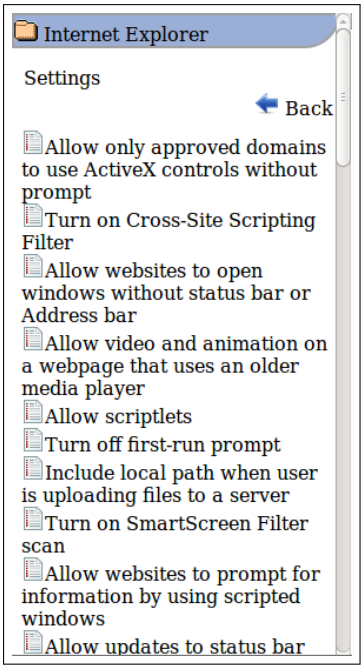
2. *OS and Browsers* section in Open Browser GP tool as shown in Figure 5.2 (b) consists of operating systems and browsers for the system administrators to select required options.

3. *Settings in Corresponding Browsers* section in Open Browser GP tool as shown in Figure 5.2 (c) consists of the available settings in each individual browser.

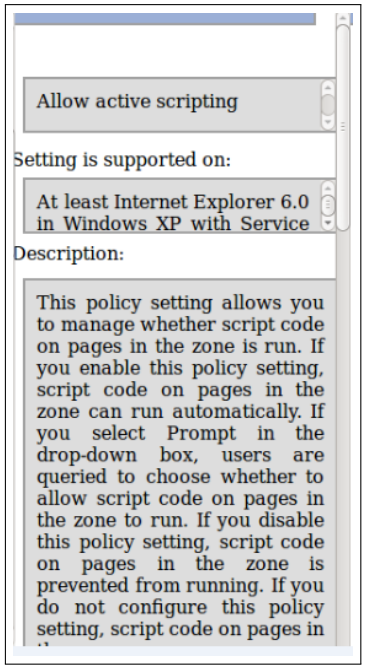
4. *Description of Browser Settings* section in Open Browser GP tool as shown in Figure 5.2 (d) consists of policy display name of the selected setting, supported on version of the setting and description of this setting, users can hide this section by clicking on standard view option.



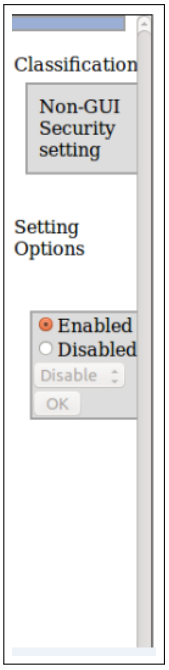
(a) Client Groups (b) OS and Browsers



(c) Settings in Corresponding Browsers



(d) Description of Browser Settings



(e) Classifications and Browser Setting Options

Figure 5.2: Individual Sections of Open Browser GP Tool: (a) Client Groups, (b) OS and Browsers, (c) Settings in Corresponding Browsers, (d) Description of Browser Settings and (e) Classifications and Browser Setting Options

Listing 5.3: An Excerpt of Groups.pl File

```
1 {'deviceGroup','Group1'}.
2 {'deviceGroupIp','Group1','001','Windows7Enterprise','
    192.168.0.10'}.
3 {'deviceGroupIp','Group1','002','Windows8','192.168.0.2'}.
4 {'deviceGroupIp','Group1','003','Windows7','192.168.0.3'}.
```

5. *Classifications and Browser Setting Options* section in Open Browser GP tool as shown in Figure 5.2 (e) consists of classification for each policy and different possible options to configure a selected setting.

After these batch scripts files were created, OSSEC server was installed in the Ubuntu system and an agent in Windows systems. Server OSSEC installation and modifications are explained in this section of the thesis since it is a one time installation. However, they should be able to manage agent settings and install OSSEC agents on client systems depending on their requirements so those instructions are presented in Section 5.6 and Section 5.7 of this thesis. We followed the installation steps from Chapter 2 of a book entitled "OSSEC Host-Based Intrusion Detection Guide" [6] and made certain modifications to OSSEC config file (Listing 5.4).

Open Browser GP tool logs the settings configured in each client system in *Browser_-settings.log* log file in logs folder of OSSEC in the server system. Each client has its own log file consisting of information about the settings sent from the server in the active-responses folder, this log file is also labelled *Browser_ settings.log*.

Along with the browser configurations Erlang database, there is a separate Erlang file called "Groups.pl", this file is used to group the client systems in Open Browser GP tool. The concept of grouping client systems is used in Open Browser GP tool because it is created to configure similar browser settings in multiple client systems. However, a system administrator can create a group in "Groups.pl" file with only one client system in order to configure multiple browsers in a single client system. This file is used to create, add or remove groups from Open Browser GP tool. An excerpt of Groups.pl file is shown in Listing 5.3. Each group should be created with a "deviceGroup" constant followed by the group name, then each fact should be created with constants "deviceGroupIp", group name, OSSEC client ID, client name and client IP address. These predicates should match exactly with the OSSEC client details maintained by the OSSEC server.

5.3 Steps to Install the OSSEC Server

1. Download the updated version of OSSEC-HIDS server [1]. It is an open source software under the terms of the GNU General Public License which allows us to redistribute it and/or modify.

2. Unzip the tar file and start the installation by typing %Installation file path%/install.sh. This step has to be performed with sudo command.

3. Then a command prompt appears asking which kind of installation you want; select server in this option.

4. Next we have to select a directory to install the server. For example: OSSEC/Server directory.

5. Next if we prefer to receive email notifications we can configure this option or skip.

6. Next we can select to run the integrity check daemon and rootkit detection engine. Currently, we are not using these option in Open Browser GP, but we recommend to enable these feature since we may use it in future.

7. Next we can enable active response feature. This feature allows the server to remotely run commands on client systems. This option must be enabled for Open Browser GP to work.

8. Next we are prompted to add IP addresses to a whitelist. OSSEC sever enables active responses for the clients in this white list.

9. Finally, we are prompted to enable remote syslogs of client systems, this feature allows server to remotely track client system logs, this is an optional feature.

10. Once the installation is completed we can start OSSEC server by using `%OSSEC server installed path%/bin/ossec-control start`. This step has to be performed with sudo command or root privileges. Here %OSSEC server installed path% is the path where OSSEC Server is installed.

Note: ossec-control is a script that allows these possible options in OSSEC:
`%OSSEC server installed path%/bin/ossec-control {start|stop|restart|status|enable|disable}` [1]

Listing 5.4: Modifications in OSSEC Config File in Server

```
<command>
  <name>IE_Registry_Configurations</name>
  <executable>IE_Registry_Configurations.bat</executable>
  <expect></expect>
  <timeout_allowed>no</timeout_allowed>
</command>
<active-response>
  <command>IE_Registry_Configurations</command>
  <location>local</location>
</active-response>
<command>
  <name>Chrome_Registry_Configurations</name>
  <executable>Chrome_Registry_Configurations.bat</executable>
  <expect></expect>
  <timeout_allowed>no</timeout_allowed>
</command>
<active-response>
  <command>Chrome_Registry_Configurations</command>
  <location>local</location>
</active-response>
<command>
  <name>Firefox_Registry_Configurations</name>
  <executable>Firefox_Registry_Configurations.bat</executable>
  <expect></expect>
  <timeout_allowed>no</timeout_allowed>
</command>
<active-response>
  <command>Firefox_Registry_Configurations</command>
  <location>local</location>
</active-response>
<command>
  <name>move_bat_files</name>
  <executable>move.bat</executable>
  <expect></expect>
  <timeout_allowed>no</timeout_allowed>
</command>
<active-response>
  <command>move_bat_files</command>
  <location>local</location>
</active-response>
```

5.4 Modifications in the OSSEC Server to Create Open Browser GP tool

In order to transfer and execute batch scripts, we had to make some modifications in OSSEC configuration file in Ubuntu. These modifications are shown in Listing 5.4. By default OSSEC server can execute batch scripts and executables available in %OSSEC client installed path%/active-response/bin folder of client systems. We created a procedure to transfer the batch scripts from the server to this folder in client systems, this procedure is explained in Open Browser GP Client Installer section of this thesis. Once the batch scripts reaches the %OSSEC client installed path%active-response/bin folder of client systems, we use certain commands to run these scripts and OSSEC allows us to create custom commands in the config file. In Listing

5.4 the command tag is used to create a command with specific name tag, executable tag is used to run predefined executable files, expect tag is used to accept input parameters and the timeout allowed tag is used to specify a time to revert a command. The active response tags are used to run the corresponding commands and the local tag is used to specify the location of running the commands, it is set to local since these commands will run locally on the client systems. After saving this modifications we have to restart OSSEC server by using restart option in ossec-control.

In order to verify whether the new OSSEC commands are updated, run the following command:

```
%OSSEC server installed path%/bin/agent_control -L
```

An Excerpt of the output:

```
Response name:  IE_Registry_Configurations0, command:  IE_Registry_Configurations.bat
```

The response name in this excerpt is appended with a zero, since we opted not to set a time out for this command. All the corresponding commands to execute batch scripts in clients are integrated into Open Browser GP tool, so these settings are performed automatically as soon as a system administrator selects and applies the settings from Open Browser GP tool.

5.5 Functionalities of Open Browser GP Client Installer

1. Open Browser GP Client Installer enables the active response feature in client system. By default active responses is disabled in the Client Agents. Hence, OSSEC users have to manually enable it in the *OSSEC Client* config file by changing the disable tag corresponding to active responses tag from "yes" to "no". This modification is automatically done when we execute the Open Browser GP client.

2. Open Browser GP Client Installer creates a batch script to move the batch script from %OSSEC client installation path%/ossec-agent/shared folder to %OSSEC client installation path%/active-responses/bin folder in client systems. By default we can transfer files from OSSEC server to agents by using central deployment option by placing the files in the shared folder of the server and restarting the manager to push these files into Client Agents. However, we can remotely only execute scripts placed in %OSSEC client installation path%/active-responses/bin folder. This move batch script is automatically created when we install Open Browser GP client executable.

3. Open Browser GP Client Installer renames "registry.pol" file to allow registry entries to modify Google Chrome settings. Registry.pol is used to maintain log information about settings configured by local group editor, so whenever the local group editor is used in a client system we have to run the Open Browser GP Client Installer.

4. Open Browser GP Client Installer installs the "GPO for Firefox" add-on to allow registry entries to modify Mozilla Firefox settings. In case Firefox is installed after installing Open Browser GP Client Installer the add-on can be manually installed. However, we recommend to reinstall Open Browser GP Client Installer.

5. We use two separate Open Browser GP Client Installers one for 64 bit and the other for 32 bit Windows operating systems, so these setup files will query the registry to find the paths for the above modifications depending on the operating system.

These executables were initially created using the python programming language which are later converted to Windows executable format by using the "py2exe" [27] library. This library cannot be used in the latest python editions. We downgraded to Python 2.7 and created two executables, one for 64 bit and another for 32 bit Windows client systems. This library creates two separate folders which include all the dependencies to make it portable to transfer to other MS Windows client systems, this includes systems which don't have python installed in them.

These are the technologies and procedures used to develop "Open Browser GP: A Multiplatform and Multibrowser Policy Configuration Tool". Most users would not need to configure these settings since they will given an Ubuntu virtual machine which can be directly imported and utilized. However, they have to follow the instructions specified in Section 5.6 and Section 5.7 of this thesis to manage server-agent infrastructure.

5.6 Steps to Add Client Systems to Open Browser GP tool

1. Initially system administrators can use an Ubuntu Virtual Machine (VM) which is preconfigured with Open Browser GP tool and it's dependencies to utilize as a central Ubuntu server. They can also create their own Ubuntu server by acquiring required installation files and by following the steps used in Section 5.4 and Section 5.3 of this thesis.

2. They have to connect this VM to the client systems through a network and verify the connection by using the ping command.

3. Now the system administrators can add new agents in OSSEC at server side [6] by opening a command prompt and running OSSEC manage_agents. All the commands should be run with sudo command or root privileges, so they have to run %OSSEC server installed path%/bin manage_agents and press enter. "OSSEC server installed path" is path where OSSEC is installed in the server. We set this path to "/project/server". However, this path can be changed according to the system administrators requirements.

4. System administrators will be prompted to select one of these option: "add an agent", "extract key for an agent", "list already added agents", "remove an agent" and "quit".

5. They have to type "A" to add an agent, they will be prompted to enter a name for an agent, the IP address of the client system and a unique ID for the new agent. The ID's should be a numeric value with no special characters and spaces are not allowed in client names.

6. Then a prompt appears requesting to confirm the agent details type "y" to accept.

7. In case a system administrator decides to remove an agent, they have to start manage_-agents and select remove agents options ("R"). They are also prompted to enter the ID of the agent to remove. This process will remove the agent but the ID number cannot be reallocated to a agent. To configure this ID to default value a system administrator can browse to %OSSEC server installed path%/etc/client.keys and remove the ID corresponding to the agent removed. Only after this process they can assign this ID to other agents.

8. In Ubuntu server, they have to open ports 514 to allow syslogs from client systems and 1514 for OSSEC server to communicate with it's agents. These ports can be opened [32] for only specified Windows client systems. For example: if they want to connect client system with IP address 192.16.0.10 to the Ubuntu server they should run:
   `sudo ufw allow from 192.168.0.10 to any port 514`
   `sudo ufw allow proto udp from 192.168.0.10 to any port 1514`.

9. Now, they have to restart the OSSEC server by running:
   `%OSSEC server installed path%/bin/ossec-control restart` .

10. In order to verify that the client information has been updated in the OSSEC server they can run:
    `%OSSEC server installed path%/bin/agent_control -l` in the command prompt. By default the client will show as "Never Connected" until we configure OSSEC agent in the client system.

11. After verifying the connection they need to add the client information into the Erlang database of Open Browser GP tool. The client information in Open Browser GP is maintained in *"etc/yaws/www/OpenBrowerGP/Groups.pl"*, an excerpt of "Groups.pl" file is shown in Listing 5.3.

5.7 Steps to Install OSSEC agents and Open Browser GP Client Installer

1. In the client systems, system administrators have to run the OSSEC Client installer, this installer can be acquired from the official OSSEC webpage [1]). Please always run this installation file with administrative privileges.

2. Then they have to start the OSSEC agent in the client system, it will prompt to enter the OSSEC server IP address. We set this IP address to 192.168.0.40. The next text box will prompt to enter the *"Authentication key"*, this is created in the server which helps for mutual authentication between the server and client agents. A system administrator should extract the key from manage_agents in the server and transfer it to the client, since it is an alphanumeric key the users can transfer it by using a pen drive, email or write it down on a piece of paper. Usually Ubuntu clients can extract authentication key by using SSH. In Windows they can use *"Putty"* to view the authentication key in the client sytems.

3. After the key is transferred into the client system, they have to paste it in the authentication key block in OSSEC agent and click on save.

4. The OSSEC agent will show a confirmation message about the client ID and server IP address to the system administrators. They have to click on "OK" and restart the OSSEC agent.

5. OSSEC agents might not set the environment variables in Windows so they have to make sure it is updated, otherwise they can manually enter the ossec-agent path in environment

variables. By default the path is "C:\Program Files (x86)\ossec-agent" in 64 bit Windows systems and it is "C:\Program Files\ossec-agent" in 32 bit Windows systems client systems.

6. The next step is to transfer the Open Browser GP Client installation files into the client system. Depending on the operating system they have to select the required installation folder.

7. System Administrators have to navigate to the *"dist folder"* in Open Browser GP Client installation files, then right click on the setup file and run it as administrator. Use *"agent-setup-win32.exe"* for 32 bit Windows operating machines and *"agent-setup-win64.exe"* for 64 bit Windows operating systems.

8. If this installation is successfully completed then they will be prompted with a confirmation message, otherwise it will prompt the error message on the command prompt.

5.8 Steps to Configure Browsers Settings in Client System by using Open Browser GP tool in Ubuntu Server

1. Finally, after completing *"Steps to Install OSSEC agents and Open Browser GP Client Installer"* a system administrator should start the Ubuntu server, then open a command prompt and start yaws by typing *"yaws"* with sudo command or with root privileges.

2. Now a system administrator can open a browser and type the local host path to load Open Browser GP tool. By default, its path is `http://localhost:8081/Open-BrowserGP/index.yaws`, since we configured it to listen to port 8081 system administrators have to use this URL. However, a system administrator can change the port number in the yaws config file.

3. Once the Open Browser GP tool is loaded he/she has to select one of the groups in the first section of the Open Browser GP tool.

4. Next they have to select a respective browser in second section.

5. Next they have to navigate through different folders to find the required settings and select the necessary options for each setting in the last section.

6. The selected options of the settings can be viewed by clicking on the respective setting. However, these settings will not be saved unless he/she clicks on "Save and Apply Settings on Selected Group".

7. The final step will be to click on "Save and Apply Settings on Selected Group" button to save and apply all the modifications on the selected group of clients.

8. Once the "Save and Apply Settings on Selected Group" button is clicked in the Open Browser GP tool, a progress bar appears on the Open Browser GP tool. This progress bar shows the percentage of configurations applied on client systems, at this point don't refresh or abort the Open Browser GP tool, since it may cause connection loss between OSSEC server and OSSEC clients.

9. The configurations may be applied on client systems with some amount of time delay, these time delays were created to maintain connections between OSSEC server and agents.

5.9 Advantages of Using Open Browser GP: A Multiplatform and Multibrowser Policy Configuration Tool

1. It would help in creating a secure browsing environment.

2. It provides authentication between client and server by using an authentication key.

3. It provides the ability to configure Internet Explorer, Google Chrome, and Mozilla Firefox settings on the Windows client systems

4. A one time installation of the server will allow us to configure major browsers in client systems multiple times.

5. A one time installation of the Client Open Browser GP agent provides us the ability to configure their major browsers multiple times.

6. Easy to use Web-based GUI allows new users to learn the procedure involved in using Open Browser GP tool.

7. It has similar visual appearance and techniques with respect to the Microsoft GPMC tool to allow experienced system administrators to understand and utilize Open Browser GP tool.

8. It can co-exist with GPMC tool and configure same clients, both these tools can be connected to same client systems.

9. It remotely sends configuration files without sending user credentials of client systems over the wire to avoid network sniffing.

10. It can run batch scripts in client systems with administrator privileges since it uses OSSEC agent.

11. It can be used in organizations ranging from small scale private industries to large scale corporate companies.

12. All the technologies used in this tool are open source techniques, so it is flexible with respect to modifications and improvements.

13. OSSEC is a host based intrusion detection system, so it is convenient to track intrusions by integrating it's commands in Open Browser GP.

14. We allow ports 514 and 1514 for only specified client systems, which in turn reduces the probability of attacks on the server.

15. The Open Browser GP tool logs the configured browser settings at both ends of the client-server infrastructure. These logs can be used in forensic analysis.

16. Open Browser GP tool displays the classification tag of each policy in major browsers. These classifications are introduced in this thesis in order to provide adequate information about the policies to the system administrators.

17. OSSEC agents can be installed in Linux and BSD based operating system, including Mac OS X operating systems, so we easily extend Open Browser GP tool to other platforms in the future.

18. Open Browser GP tool is used for mapping similar policies in different browsers and categorized them into "All Browsers" group. Currently, All Browsers category only consists of only major browsers mapping but in future we can map more browsers, this mapping helps us to analyze the existing common settings and the need to develop new common settings.

5.10 Limitations of Open Browser GP: A Multiplatform and Multibrowser Policy Configuration Tool

1. Currently, the procedure involved in extracting information from ADMX and ADML files, configuration of OSSEC server-agent, mapping of similar policies and installing Open Browser GP tool is not performed automatically.

2. Currently, Open Browser GP cannot configure all browsers in all operating systems, it can only configure Internet Explorer, Google Chrome and Mozilla Firefox in Windows 7 and Windows 8 operating systems.

3. OSSEC server cannot read individual registry entries made in client machines. OSSEC cannot be used to read the user keys of a registry. This leads to the limitation of Open Browser GP tool of not being able to configure "User" class settings in Internet Explorer. The policies with class attribute set to "User" are called User class settings. From the 874 policies in Internet Explorer version 10 the number of policies which come under "User" class are 104 policies. Except these policies rest of the 770 policies can be configured by Open Browser GP tool. This implies that Open Browser GP tool has 88.10% coverage rate with respect to IE policy settings. However, further research is required in order to configure all the policies in IE browser.

4. Open Browser GP tool uses the central deployment technique in OSSEC to transfer batch scripts created by Open Browser GP tool. Scripts are transferred to all the groups of clients configured in the OSSEC server. Central deployment technique is the process of creating configuration files in shared folder in the OSSEC server in order to allow the server to push these files into the OSSEC shared folder of all the client systems. Currently, we execute the scripts only on selected clients. Further modifications are required in OSSEC to allow selective transmission of configuration files.

5. Open Browser GP tool always needs "GPO for firefox" add-on to modify configuration settings in Mozilla Firefox. GPO for firefox is a third party add-on.

Observing these different advantages and functionalities of Open Browser GP tool, we propose that it can be utilized in industrial organizations by system administrators to configure major browser settings in major platforms. There are very few limitations of this tool when compared to the advantages it provides. However, an ideal secure browsing configuration tool

should have maximum flexibility and security. Hence, we propose some of the possible ways of reducing these limitations in Chapter 6: Conclusions and Future Work of this thesis.

Chapter 6

Conclusions and Future Work

6.1 Conclusions

The enormous utilization of today's browsers by many users to perform multiple tasks in an organization leads to the need for system administrators to learn detailed information about configuring each browser's security features remotely in order to make the browsers secure.

Most system administrators utilize the GPMC (Active Directory) tool to configure multiple Windows machines from a central Windows Server. However they fail to configure multiple browsers in multiple platforms, since Windows Server can only perform complete configuration settings on Windows clients, and it can completely configure only IE.

In addition, smaller companies cannot afford to maintain an client-server infrastructure and cannot hire an experienced system administrator. Therefore, an effective and user-friendly browser configuration tool would help to overcome these problems.
The contributions this thesis provides toward solving these problems are:

1. Provided an in-depth analysis of different policies of each major browser to understand the procedures followed by them to configure their security related settings.

2. Proposed the need and advantages for a generic language for achieving a secure browsing environment among all major browsers.

3. Classified each policy in each major browser in order to categorize GUI, Non-GUI, Security and Non-Security related settings.

4. Mapped similar settings in different major browsers and developed a process to embed these common settings in the Open Browser GP tool.

5. Developed a user-friendly, multi browser, and multi platform prototype tool called "*Open Browser GP*". This tool can be used to configure security policies in multiple browsers in multiple client systems across a network.

The techniques described in this thesis are not necessary sufficient conditions for mitigating all the current vulnerabilities in the browsers. However, these techniques will open new research field and studies with respect to creating a secure browsing environment. Overall, the results of this thesis demonstrate that it is possible to configure Internet Explorer, Google Chrome and

Mozilla Firefox browsers settings by following certain procedures and techniques to facilitate the secure configurations of multiple browsers in multiple platforms. In addition, the results of this thesis work shows that we can expand a client-server environment into multiple operating systems in order to configure all browsers in all operating systems.

6.2 Future Directions

There are three main research areas where future work in needed. Firstly, more work is needed to develop common settings and a common language for configuring multiple browsers. Secondly, we need to expand OSSEC technology with respect to Open Browser GP tool. Lastly, further research is needed in order to validate Open Browser GP tool in production settings. We expand on each of these three areas below.

6.2.1 Development of Common Settings and Common Language for Multiple Browsers

This thesis presented the need and the advantages of developing a set of common settings and a generic language as shown in Chapter 4. We did not provide a full working demonstration of this new language, but provided the different possible methods which will be useful to develop a new language. These common settings and a common language would be desirable to create a secure browsing environment in all the browsers.

Furthermore, it would be desirable to provide well-documented open source instructions with respect to this new language, which will help and provide an overview about internal configurations for new system administrators. We hope that the work provided in this thesis serves as a platform to initiate a discussion and the development of a generic language that can be used to configure settings in all browsers.

6.2.2 Embedding OSSEC into Open Browser GP tool

As mentioned in Chapter 5, we have used some of the OSSEC commands in Open Browser GP and currently we have to install OSSEC setup files as well as Open Browser GP tool individually. We can embed all the functionalities of OSSEC in our tool with further research. OSSEC is an open source tool, so we can make modifications in it to eliminate some of the limitations faced by Open Browser GP tool. This expansion of OSSEC tool can lead to a scenario where we can setup client-server infrastructure in very few steps compared to the present number steps we follow to connect and configure client systems. This user-friendly installation and the ability

to perform browser security configurations will eventually lead to the popularity of our Open Browser GP tool.

6.2.3 Validation and Expansion of Open Browser GP tool

In order to configure multiple browsers in multiple platforms we introduced an Open Browser GP tool in this thesis. This tool is in initial stages of development and we tested it on only specific tasks. However, we did not formally perform all the testing techniques to check if it can work in anomaly conditions. OSSEC is a "Host-based Intrusion Detection System", which we partially integrated into Open Browser GP tool, this provides a level of security to our tool. We believe with some adjustments in Open Browser GP tool we can expand this tool into a highly reliable browser security configuration tool, which will be supported in all operating systems including mobile technologies.

Bibliography

[1] D. B. Cid. Ossec. http://www.ossec.net/, 2004.

[2] S. S. Corporate. Stylus studio. http://www.stylusstudio.com/, May 2014.

[3] W. Dormann and J. Rafail. Securing your web browser. https://www.us-cert.gov/publications/securing-your-web-browser, February 2008.

[4] S. Golovanov. An analysis of web browsers. http://securelist.com/blog/research/57767/ksn-an-analysis-of-web-browsers, October 2012.

[5] Google. Chromium os. http://www.chromium.org/chromium-os, November 2009.

[6] A. Hay, D. Cid, and R. Bray. Ossec host-based intrusion detection guide, 2008.

[7] J. H. Heidelberg. Managing Windows Vista Group Policy (part 1). http://www.windowsecurity.com/articles-tutorials/authentication_and_encryption/Managing-Windows-Vista-Group-Policy-Part1.html, November 2006.

[8] J. Herman. Managing group policy admx files step-by-step guide. http://msdn.microsoft.com/en-us/library/bb530196.aspx#manageadmxfiles_topic2, June 2007.

[9] D. Ho. Notepad++. http://notepad-plus-plus.org/, November 2003.

[10] Z. Kessin. Building web applications with erlang, June 2012.

[11] S. S. Laurent. Introducing erlang, January 2013.

[12] G. Maone. Noscript security suite. https://addons.mozilla.org/en-US/firefox/addon/noscript/, 2009.

[13] Microsoft Corp. Gpupdate. https://technet.microsoft.com/en-us/library/bb490983.aspx.

[14] Microsoft Corp. Reg. https://technet.microsoft.com/en-us/library/bb490984.aspx.

[15] Microsoft Corp. Windows server, April 2003.

[16] Microsoft Corp. .admx and .adml file structure. http://technet.microsoft.com/en-us/library/cc772507(v=ws.10).aspx, April 2007.

[17] Microsoft Corp. The Microsoft Computer Dictionary, Fifth Edition, April 2007.

[18] Microsoft Corp. Xml notepad. http://www.microsoft.com/en-us/download/details.aspx?id=7973, September 2007.

[19] Microsoft Corp. Windows Registry information for advanced users. http://support.microsoft.com/kb/256986/en-usl, September 2012.

[20] J. Moskowitz. Group policy, profiles and intellimirror for windows2003, windowsxp and windows2000. http://www.gpanswers.com/wp-content/uploads/2013/01/4447_web01.pdf, March 2004.

[21] J. Moskowitz. Inside adm and admx templates for group policy. http://technet.microsoft.com/en-us/magazine/2008.01.layout.aspx, January 2008.

[22] Mozilla Support. Gpo for firefox add-on. https://addons.mozilla.org/en-US/firefox/addon/gpo-for-firefox//.

[23] MozillaZine Knowledge Base. About:config entries. http://kb.mozillazine.org/About:config_entries.

[24] National Security Agency/Central Security Service. Deploying and securing google chrome in a windows enterprise. https://www.nsa.gov/ia/_files/app/deploying_and_securing_google_chrome_in_a_windows_enterprise.pdf, October 2012.

[25] J. Nielson, C. Williamson, and M. Arlitt. Benchmarking modern web browsers. http://www.aqualab.cs.northwestern.edu/conferences/HotWeb08/papers/Nielson-BMW.pdf, 2008.

[26] Python Software Foundation. Minimal dom implementation. https://docs.python.org/2/library/xml.dom.minidom.html.

[27] Python Software Foundation. Py2exe. https://pypi.python.org/pypi/py2exe.

[28] Red Hat Inc. Red Hat Inc. http://www.redhat.com/en, 1993.

[29] Red Hat Inc. FreeIPA. http://www.freeipa.org/page/About/, November 2014.

[30] Redkitten Corp. How to install a firefox add-on. http://www.redkitten.co.uk/firefox/how-to-install-a-firefox-add-on-for-all-users-remotely/.

[31] M. Russinovich. Windows sysinternals pstools. https://technet.microsoft.com/en-us/sysinternals/bb897553.aspx, May 2014.

[32] Security Onion Project. Ufw - uncomplicated firewall. https://code.google.com/p/security-onion/wiki/Firewall, 2014.

[33] A. Silberschatz, P. B. Galvin, and G. Gagne. Operating System Concepts 8th edition, 2009.

[34] StatCounter. Statcounter global stats. http://gs.statcounter.com/, December 2014.

[35] J. Stromberg. Configuring google chrome via group policy. http://jackstromberg.com/2013/08/configuring-google-chrome-via-group-policy/, August 2013.

[36] G. van Rossum. Python Programming Language. http://www.tutorialspoint.com/python/python_overview.htm.

Appendix A

A.1 Appendix Description

Appendix A.2 contains tables summarizes the comparison of differences with respect to each major browser's security related setting. Table A.1 presents the security related Google Chrome policies. Notice that here security related settings refers to GUI_SEC and NGUI_SEC, these terms are discussed in Chapter 3 of this thesis.

Each row in this table is numbered in ascending order and consists of two sub rows, the first column of the first sub row consists of a Google Chrome policy name followed by it's display name, the second and third column of the first sub row provides information about the possible ways of configuring similar setting in Google Chrome setting with respect to Internet Explorer and Mozilla Firefox. The second sub row of each row provides a brief description about the Google Chrome policy. Since Internet Explorer follows a zone level policy categorization we mentioned in some policies that similar Google Chrome policy can be achieved by changing multiple settings in multiple zones. Mozilla Firefox settings can be configured by using different third party add-ons and modifying multiple entries in *about:config* to achieve similar Google Chrome Policies. Notice that "N/A" means that this policy cannot be configured in the corresponding browser.

Table A.2 uses the same representation to present security related policies in Internet Explorer with respect to Google Chrome and Mozilla Firefox. Table A.3 uses the same representation to present security related policies in Mozilla Firefox with respect to Internet Explorer and Google Chrome. These tables can be extracted from the Erlang databse of the Open Browser GP tool by using python scripts, the data in `monospace format` in these tables was manually entered by analysing descriptions of each policy. These tables will be a useful reference to verify whether a similar configuration in multiple browsers can be accomplished by modifying multiple available settings and provide information to a system administrator that a currently available settings in one browser cannot be configured in a other browsers.

A.2 Dissimilarities Tables

Notations for Table A.1

1. IE: Comparison with Internet Explorer
2. Firefox: Comparison with Mozilla Firefox

3. Chrome: Google Chrome (policy name and display name)

4. Description: Description about the policy in Google Chrome

5. N/A: Setting is not available in this browser

Table A.1: Comparison of Security Related Settings for Google Chrome with Respect to Internet Explorer and Mozilla Firefox

EN	Chrome	IE	Firefox
	Description		
1	ChromeFrameContentTypes (Allow Google Chrome Frame to handle the listed content types)	N/A	N/A
	Allow Google Chrome Frame to handle the listed content types. If this policy is not set the default renderer will be used for all sites as specified by the ChromeFrameRendererSettings policy.		
2	RemoteAccessHostFirewallTraversal (Enable firewall traversal from remote access host)	N/A	N/A
	Enables usage of STUN and relay servers when remote clients are trying to establish a connection to this machine. If this setting is enabled, then remote clients can discover and connect to this machines even if they are separated by a firewall. If this setting is disabled and outgoing UDP connections are filtered by the firewall, then this machine will only allow connections from client machines within the local network. If this policy is left not set the setting will be enabled.		
3	RemoteAccessHostDomain (Configure the required domain name for remote access hosts)	N/A	N/A
	Configures the required host domain name that will be imposed on remote access hosts and prevents users from changing it. If this setting is enabled, then hosts can be shared only using accounts registered on the specified domain name. If this setting is disabled or not set, then hosts can be shared using any account.		
4	RemoteAccessHostRequireTwoFactor (Enable two-factor authentication for remote access hosts)	N/A	N/A
	Enables two-factor authentication for remote access hosts instead of a user-specified PIN. If this setting is enabled, then users must provide a valid two-factor code when accessing a host. If this setting is disabled or not set, then two-factor will not be enabled and the default behavior of having a user-defined PIN will be used.		

5	RemoteAccessHostTalkGadgetPrefix (Configure the TalkGadget prefix for remote access hosts)	N/A	N/A
	Configures the TalkGadget prefix that will be used by remote access hosts and prevents users from changing it. If specified, this prefix is prepended to the base TalkGadget name to create a full domain name for the TalkGadget. The base TalkGadget domain name is .talkgadget.google.com. If this setting is enabled, then hosts will use the custom domain name when accessing the TalkGadget instead of the default domain name. If this setting is disabled or not set, then the default TalkGadget domain name (chromoting-host.talkgadget.google.com) will be used for all hosts. Remote access clients are not affected by this policy setting. They will always use chromoting-client.talkgadget.google.com to access the TalkGadget.		
6	RemoteAccessHostRequireCurtain (Enable curtaining of remote access hosts)	N/A	N/A
	Enables curtaining of remote access hosts while a connection is in progress. If this setting is enabled, then hosts physical input and output devices are disabled while a remote connection is in progress. If this setting is disabled or not set, then both local and remote users can interact with the host when it is being shared.		
7	RemoteAccessHostAllowClientPairing (Enable or disable PIN-less authentication)	N/A	N/A
	If this setting is enabled or not configured, then users can opt to pair clients and hosts at connection time, eliminating the need to enter a PIN every time. If this setting is disabled, then this feature will not be available.		
8	DefaultCookiesSetting (Default cookies setting)	Similar semantics can be achieved by modifying multiple settings	N/A
	Allows you to set whether websites are allowed to set local data. Setting local data can be either allowed for all websites or denied for all websites. If this policy is left not set, AllowCookies will be used and the user will be able to change it.		
9	DefaultNotificationsSetting (Default notification setting)	N/A	Similar semantics can be achieved by modifying multiple options
	Allows you to set whether websites are allowed to display desktop notifications. Displaying desktop notifications can be allowed by default, denied by default or the user can be asked every time a website wants to show desktop notifications. If this policy is left not set, AskNotifications will be used and the user will be able to change it.		

10	CookiesAllowedForUrls (Allow cookies on these sites)	Similar semantics can be achieved by modifying multiple settings at different zones	Similar semantics can be achieved by using different third party Add-ons
	Allows you to set a list of url patterns that specify sites which are allowed to set cookies. If this policy is left not set the global default value will be used for all sites either from the DefaultCookiesSetting policy if it is set, or the users personal configuration otherwise.		
11	CookiesBlockedForUrls (Block cookies on these sites)	Similar semantics can be achieved by modifying multiple settings at different zones	Similar semantics can be achieved by using different third party Add-ons
	Allows you to set a list of url patterns that specify sites which are not allowed to set cookies. If this policy is left not set the global default value will be used for all sites either from the DefaultCookiesSetting policy if it is set, or the users personal configuration otherwise.		
12	CookiesSessionOnly-ForUrls (Allow session only cookies on these sites)	Similar semantics can be achieved by modifying multiple settings at different zones	N/A
	Allows you to set a list of url patterns that specify sites which are allowed to set session only cookies. If this policy is left not set the global default value will be used for all sites either from the DefaultCookiesSetting policy if it is set, or the users personal configuration otherwise. If the "RestoreOnStartup" policy is set to restore URLs from previous sessions this policy will not be respectred and cookies will be stored permanently for those sites.		
13	ImagesAllowedForUrls (Allow images on these sites)	N/A	N/A
	Allows you to set a list of url patterns that specify sites which are allowed to display images. If this policy is left not set the global default value will be used for all sites either from the DefaultImagesSetting policy if it is set, or the users personal configuration otherwise.		
14	ImagesBlockedForUrls (Block images on these sites)	N/A	N/A
	Allows you to set a list of url patterns that specify sites which are not allowed to display images. If this policy is left not set the global default value will be used for all sites either from the DefaultImagesSetting policy if it is set, or the users personal configuration otherwise.		

15	JavaScriptAllowedForUrls (Allow JavaScript on these sites)	Similar semantics can be achieved by modifying multiple settings at different zones	Similar semantics can be achieved by using different third party Add-ons
	Allows you to set a list of url patterns that specify sites which are allowed to run JavaScript. If this policy is left not set the global default value will be used for all sites either from the DefaultJavaScriptSetting policy if it is set, or the users personal configuration otherwise.		
16	JavaScriptBlockedForUrls (Block JavaScript on these sites)	Similar semantics can be achieved by modifying multiple settings at different zones	Similar semantics can be achieved by using different third party Add-ons
	Allows you to set a list of url patterns that specify sites which are not allowed to run JavaScript. If this policy is left not set the global default value will be used for all sites either from the DefaultJavaScriptSetting policy if it is set, or the users personal configuration otherwise.		
17	PluginsAllowedForUrls (Allow plugins on these sites)	Similar semantics can be achieved by modifying multiple settings	N/A
	Allows you to set a list of url patterns that specify sites which are allowed to run plugins. If this policy is left not set the global default value will be used for all sites either from the DefaultPluginsSetting policy if it is set, or the users personal configuration otherwise.		
18	PluginsBlockedForUrls (Block plugins on these sites)	Similar semantics can be achieved by modifying multiple settings at different zones	N/A
	Allows you to set a list of url patterns that specify sites which are not allowed to run plugins. If this policy is left not set the global default value will be used for all sites either from the DefaultPluginsSetting policy if it is set, or the users personal configuration otherwise.		
19	PopupsAllowedForUrls (Allow popups on these sites)	Similar semantics can be achieved by modifying multiple settings at different zones	N/A
	Allows you to set a list of url patterns that specify sites which are allowed to open popups. If this policy is left not set the global default value will be used for all sites either from the DefaultPopupsSetting policy if it is set, or the users personal configuration otherwise.		

20	PopupsBlockedForUrls (Block popups on these sites)	Similar semantics can be achieved by modifying multiple settings at different zones	Similar semantics can be achieved by using different third party Add-ons
	Allows you to set a list of url patterns that specify sites which are not allowed to open popups. If this policy is left not set the global default value will be used for all sites either from the DefaultPopupsSetting policy if it is set, or the users personal configuration otherwise.		
21	NotificationsAllowed-ForUrls (Allow notifications on these sites)	Similar semantics can be achieved by modifying multiple settings at different zones	Similar semantics can be achieved by using different third party Add-ons
	Allows you to set a list of url patterns that specify sites which are allowed to display notifications. If this policy is left not set the global default value will be used for all sites either from the DefaultNotificationsSetting policy if it is set, or the users personal configuration otherwise.		
22	NotificationsBlocked-ForUrls (Block notifications on these sites)	N/A	N/A
	Allows you to set a list of url patterns that specify sites which are not allowed to display notifications. If this policy is left not set the global default value will be used for all sites either from the DefaultNotificationsSetting policy if it is set, or the users personal configuration otherwise.		
23	ChromeFrameRenderer-erSettings (Default HTML renderer for Google Chrome Frame)	N/A	N/A
	Allows you to configure the default HTML renderer when Google Chrome Frame is installed. The default setting used when this policy is left not set is to allow the host browser do the rendering, but you can optionally override this and have Google Chrome Frame render HTML pages by default.		
24	RenderInHostList(Always render the following URL patterns in the host browser)	N/A	N/A
	Customize the list of URL patterns that should always be rendered by the host browser. If this policy is not set the default renderer will be used for all sites as specified by the ChromeFrameRendererSettings policy. For example patterns see http://www.chromium.org/developers- /how-tos/chrome-frame-getting-started.		
25	AdditionalLaunchParameters (Additional command line parameters for Google Chrome)	N/A	N/A
	Allows you to specify additional parameters that are used when Google Chrome Frame launches Google Chrome. If this policy is not set the default command line will be used.		

26	SkipMetadataCheck(Skip the meta tag check in Google Chrome Frame)	N/A	N/A
	Normally pages with X-UA-Compatible set to chrome=1 will be rendered in Google Chrome Frame regardless of the ChromeFrameRendererSettings policy. If you enable this setting, pages will not be scanned for meta tags. If you disable this setting, pages will be scanned for meta tags. If this policy is not set, pages will be scanned for meta tags.		
27	ExtensionInstallBlacklist (Configure extension installation blacklist)	Similar semantics can be achieved by modifying multiple settings	Similar semantics can be achieved by modifying multiple entries in about:config
	Allows you to specify which extensions the users can NOT install. Extensions already installed will be removed if blacklisted. A blacklist value of * means all extensions are blacklisted unless they are explicitly listed in the whitelist. If this policy is left not set the user can install any extension in Google Chrome.		
28	ExtensionInstallWhitelist (Configure extension installation whitelist)	Similar semantics can be achieved by modifying multiple settings	Similar semantics can be achieved by modifying multiple entries in about:config
	Allows you to specify which extensions are not subject to the blacklist. A blacklist value of * means all extensions are blacklisted and users can only install extensions listed in the whitelist. By default, all extensions are whitelisted, but if all extensions have been blacklisted by policy, the whitelist can be used to override that policy.		
29	ExtensionInstallForcelist (Configure the list of force-installed extensions)	N/A	N/A
	Allows you to specify a list of extensions that will be installed silently, without user interaction. Each item of the list is a string that contains an extension ID and an update URL delimited by a semicolon (;). The extension ID is the 32-letter string found e.g. on chrome://extensions when in developer mode. The update URL should point to an Update Manifest XML document as described at http://code.google.com/chrome /extensions/autoupdate.html. Note that the update URL set in this policy is only used for the initial installation; subsequent updates of the extension will use the update URL indicated in the extensions manifest. For each item, Google Chrome will retrieve the extension specified by the extension ID from the update service at the specified update URL and silently install it. For example, lcncmkcnkcdbbanbjakcencbaoegdjlp;https://clients2.google.com/service/update2/crx installs the Google SSL Web Search extension from the standard Chrome Web Store update URL. For more information about hosting extensions, see: http://code.google.com/chrome/exten- sions/hosting.html. Users will be unable to uninstall extensions that are specified by this policy. If you remove an extension from this list, then it will be automatically uninstalled by Google Chrome. Extensions specified in this list are also automatically whitelisted for installation; the ExtensionsInstallBlacklist does not affect them. If this policy is left not set the user can uninstall any extension in Google Chrome.		

30	ExtensionInstallSources (Configure extension, app, and user script install sources)	N/A	N/A
	Allows you to specify which URLs are allowed to install extensions, apps, and themes. Starting in Chrome 21, it is more difficult to install extensions, apps, and user scripts from outside the Chrome Web Store. Previously, users could click on a link to a *.crx file, and Chrome would offer to install the file after a few warnings. After Chrome 21, such files must be downloaded and dragged onto the Chrome settings page. This setting allows specific URLs to have the old, easier installation flow. Each item in this list is an extension-style match pattern (see http://code.google.com/chrome/ extensions/match_patterns.html). Users will be able to easily install items from any URL that matches an item in this list. Both the location of the *.crx file and the page where the download is started from (i.e. the referrer) must be allowed by these patterns. ExtensionInstallBlacklist takes precedence over this policy. That is, an extension on the blacklist wont be installed, even if it happens from a site on this list.		
31	ExtensionAllowedTypes (Configure allowed app/extension types)	Similar semantics can be achieved by modifying multiple settings at different zones	N/A
	Controls which app/extension types are allowed to be installed. This setting white-lists the allowed types of extensioN/Apps that can be installed in Google Chrome. The value is a list of strings, each of which should be one of the following: "extension", "theme", "user_script", "hosted_app", "legacy_packaged_app", "platform_app". See the Chrome extensions documentation for more information on these types. Note that this policy also affects extensions and apps to be force-installed via ExtensionInstallForcelist. If this setting is configured, extensions/apps which have a type that is not on the list will not be installed. If this settings is left not-configured, no restrictions on the acceptable extensioN/App types are enforced.		
32	BlockThirdPartyCookies (Block third party cookies)	N/A	Similar semantics can be achieved by modifying multiple entries in about:config
	Blocks third party cookies. Enabling this setting prevents cookies from being set by web page elements that are not from the domain that is in the browsers address bar. Disabling this setting allows cookies to be set by web page elements that are not from the domain that is in the browsers address bar and prevents users from changing this setting. If this policy is left not set, third party cookies will be enabled but the user will be able to change that.		
33	BlockThirdPartyCookies_recommended (Block third party cookies)	N/A	N/A
	Blocks third party cookies. Enabling this setting prevents cookies from being set by web page elements that are not from the domain that is in the browsers address bar. Disabling this setting allows cookies to be set by web page elements that are not from the domain that is in the browsers address bar and prevents users from changing this setting. If this policy is left not set, third party cookies will be enabled but the user will be able to change that.		

34	BookmarkBarEnabled (Enable Bookmark Bar)	N/A	N/A
	Enables the bookmark bar on Google Chrome. If you enable this setting, Google Chrome will show a bookmark bar. If you disable this setting, users will never see the bookmark bar. If you enable or disable this setting, users cannot change or override it in Google Chrome. If this setting is left not set the user can decide to use this function or not.		
35	BookmarkBarEnabled_recommended (Enable Bookmark Bar)	N/A	N/A
	Enables the bookmark bar on Google Chrome. If you enable this setting, Google Chrome will show a bookmark bar. If you disable this setting, users will never see the bookmark bar. If you enable or disable this setting, users cannot change or override it in Google Chrome. If this setting is left not set the user can decide to use this function or not.		
36	BuiltInDnsClientEnabled (Use built-in DNS client)	N/A	N/A
	Controls whether the built-in DNS client is used in Google Chrome. If this policy is set to true, the built-in DNS client will be used, if available. If this policy is set to false, the built-in DNS client will never be used. If this policy is left not set, the users will be able to change whether the built-in DNS client is used by editing chrome://flags or specifying a command-line flag.		
37	DefaultBrowserSettingEnabled (Set Chrome as Default Browser)	N/A	N/A
	Configures the default browser checks in Google Chrome and prevents users from changing them. If you enable this setting, Google Chrome will always check on startup whether it is the default browser and automatically register itself if possible. If this setting is disabled, Google Chrome will never check if it is the default browser and will disable user controls for setting this option. If this setting is not set, Google Chrome will allow the user to control whether it is the default browser and whether user notifications should be shown when it isnt.		
38	DeveloperToolsDisabled (Disable Developer Tools)	Setting is available as DisableDeveloperTools (Turn off Developer Tools) in this browser	Similar semantics can be achieved by modifying multiple entries in about:config
	Disables the Developer Tools and the JavaScript console. If you enable this setting, the Developer Tools can not be accessed and web-site elements can not be inspected anymore. Any keyboard shortcuts and any menu or context menu entries to open the Developer Tools or the JavaScript Console will be disabled. Setting this option to disabled or leaving it not set will allow the use to use the Developer Tools and the JavaScript console.		

39	DisablePluginFinder (Specify whether the plugin finder should be disabled)	N/A	N/A
	If you set this setting to enabled the automatic search and installation of missing plugins will be disabled in Google Chrome. Setting this option to disabled or leave it not set the plugin finder will be active.		
40	DisableSSLRecordSplitting (Disable SSL record splitting)	N/A	N/A
	Specifies whether SSL record splitting should be disabled. Record splitting is a workaround for a weakness in SSL 3.0 and TLS 1.0 but can cause compatibility issues with some HTTPS servers and proxies. If the policy is not set, or is set to false, then record splitting will be used on SSL/TLS connections which use CBC ciphersuites.		
41	DisableSafeBrowsingProceedAnyway (Disable proceeding from the Safe Browsing warning page)	N/A	N/A
	The Safe Browsing service shows a warning page when users navigate to sites that are flagged as potentially mallicious. Enabling this setting prevents users from proceeding anyway from the warning page to the malicious site. If this setting is disabled or not configured then users can choose to proceed to the flagged site after being shown the warning.		
42	DisabledPlugins (Specify a list of disabled plugins)	N/A	N/A
	Specifies a list of plugins that are disabled in Google Chrome and prevents users from changing this setting. The wildcard characters * and ? can be used to match sequences of arbitrary characters. * matches an arbitrary number of characters while ? specifies an optional single character, i.e. matches zero or one characters. The escape character is /, so to match actual *, ?, or / characters, you can put a / in front of them. If you enable this setting, the specified list of plugins is never used in Google Chrome. The plugins are marked as disabled in about:plugins and users cannot enable them. Note that this policy can be overridden by EnabledPlugins and DisabledPluginsExceptions. If this policy is left not set the user can use any plugin installed on the system except for hard-coded incompatible, outdated or dangerous plugins.		

43	DisabledPluginsExceptions (Specify a list of plugins that the user can enable or disable)	N/A	N/A
	Specifies a list of plugins that user can enable or disable in Google Chrome. The wildcard characters * and ? can be used to match sequences of arbitrary characters. * matches an arbitrary number of characters while ? specifies an optional single character, i.e. matches zero or one characters. The escape character is /, so to match actual *, ?, or / characters, you can put a / in front of them. If you enable this setting, the specified list of plugins can be used in Google Chrome. Users can enable or disable them in about:plugins, even if the plugin also matches a pattern in DisabledPlugins. Users can also enable and disable plugins that dont match any patterns in DisabledPlugins, DisabledPluginsExceptions and EnabledPlugins. This policy is meant to allow for strict plugin blacklisting where the DisabledPlugins list contains wildcarded entries like disable all plugins * or disable all Java plugins *Java* but the administrator wishes to enable some particular version like IcedTea Java 2.3. This particular versions can be specified in this policy. If this policy is left not set any plugin that matches the patterns in the DisabledPlugins will be locked disabled and the user wont be able to enable them.		
44	SupervisedUserCreationEnabled (Enable creation of supervised users)	N/A	N/A
	If set to false, supervised-user creation by this user will be disabled. Any existing supervised users will still be available. If set to true or not configured, supervised users can be created and managed by this user.		
45	PasswordManagerEnabled (Enable the password manager)	Similar semantics can be achieved by modifying multiple settings at different zones	N/A
	Enables saving passwords and using saved passwords in Google Chrome. If you enable this setting, users can have Google Chrome memorize passwords and provide them automatically the next time they log in to a site. If you disable this setting, users are not able to save passwords or use already saved passwords. If you enable or disable this setting, users cannot change or override this setting in Google Chrome. If this policy is left not set, this will be enabled but the user will be able to change it.		
46	PasswordManagerAllowShowPasswords (Allow users to show passwords in Password Manager)	N/A	N/A
	Controls whether the user may show passwords in clear text in the password manager. If you disable this setting, the password manager does not allow showing stored passwords in clear text in the password manager window. If you enable or do not set this policy, users can view their passwords in clear text in the password manager.		

47	PasswordManagerEnabled_recommended (Enable the password manager)	N/A	N/A
	Enables saving passwords and using saved passwords in Google Chrome. If you enable this setting, users can have Google Chrome memorize passwords and provide them automatically the next time they log in to a site. If you disable this setting, users are not able to save passwords or use already saved passwords. If you enable or disable this setting, users cannot change or override this setting in Google Chrome. If this policy is left not set, this will be enabled but the user will be able to change it.		
48	AuthSchemes (Supported authentication schemes)	N/A	N/A
	Specifies which HTTP Authentication schemes are supported by Google Chrome. Possible values are basic, digest, ntlm and negotiate. Separate multiple values with commas. If this policy is left not set, all four schemes will be used.		
49	DisableAuthNegotiateCnameLookup (Disable CNAME lookup when negotiating Kerberos authentication)	N/A	N/A
	Specifies whether the generated Kerberos SPN is based on the canonical DNS name or the original name entered. If you enable this setting, CNAME lookup will be skipped and the server name will be used as entered. If you disable this setting or leave it not set, the canonical name of the server will be determined via CNAME lookup.		
50	EnableAuthNegotiatePort (Include non-standard port in Kerberos SPN)	N/A	N/A
	Specifies whether the generated Kerberos SPN should include a non-standard port. If you enable this setting, and a non-standard port (i.e., a port other than 80 or 443) is entered, it will be included in the generated Kerberos SPN. If you disable this setting or leave it not set, the generated Kerberos SPN will not include a port in any case.		
51	AuthServerWhitelist (Authentication server whitelist)	Similar semantics can be achieved by modifying multiple settings at different zones	N/A
	Specifies which servers should be whitelisted for integrated authentication. Integrated authentication is only enabled when Google Chrome receives an authentication challenge from a proxy or from a server which is in this permitted list. Separate multiple server names with commas. Wildcards (*) are allowed. If you leave this policy not set Chrome will try to detect if a server is on the Intranet and only then will it respond to IWA requests. If a server is detected as Internet then IWA requests from it will be ignored by Chrome.		

52	AuthNegotiateDelegate-Whitelist (Kerberos delegation server whitelist)	N/A	N/A
	Servers that Google Chrome may delegate to. Separate multiple server names with commas. Wildcards (*) are allowed. If you leave this policy not set Chrome will not delegate user credentials even if a server is detected as Intranet.		
53	AllowCrossOriginAuth-Prompt (Cross-origin HTTP Basic Auth prompts)	N/A	N/A
	Controls whether third-party sub-content on a page is allowed to pop-up an HTTP Basic Auth dialog box. Typically this is disabled as a phishing defense. If this policy is not set, this is disabled and third-party sub-content will not be allowed to pop up a HTTP Basic Auth dialog box.		
54	ProxyMode (Choose how to specify proxy server settings)	N/A	N/A
	Allows you to specify the proxy server used by Google Chrome and prevents users from changing proxy settings. If you choose to never use a proxy server and always connect directly, all other options are ignored. If you choose to use system proxy settings or auto detect the proxy server, all other options are ignored. If you choose fixed server proxy mode, you can specify further options in Address or URL of proxy server and Comma-separated list of proxy bypass rules. If you choose to use a .pac proxy script, you must specify the URL to the script in URL to a proxy .pac file. For detailed examples, visit: http://www.chromium.org/developers- /design-documents/network-settings#TOC-Command-line-options-for-proxy-sett If you enable this setting, Google Chrome ignores all proxy-related options specified from the command line. Leaving this policy not set will allow the users to choose the proxy settings on their own.		
55	ProxyServer (Address or URL of proxy server)	N/A	N/A
	You can specify the URL of the proxy server here. This policy only takes effect if you have selected manual proxy settings at Choose how to specify proxy server settings. You should leave this policy not set if you have selected any other mode for setting proxy policies. For more options and detailed examples, visit: http://www.chromium.org/developers- /design-documents/network-settings#TOC-Command-line-options-for-proxy-sett		
56	ProxyPacUrl (URL to a proxy .pac file)	N/A	N/A
	You can specify a URL to a proxy .pac file here. This policy only takes effect if you have selected manual proxy settings at Choose how to specify proxy server settings. You should leave this policy not set if you have selected any other mode for setting proxy policies. For detailed examples, visit: http://www.chromium.org/developers- /design-documents/network-settings#TOC-Command-line-options-for-proxy-sett		

57	ProxyBypassList (Proxy bypass rules)	N/A	N/A
	Google Chrome will bypass any proxy for the list of hosts given here. This policy only takes effect if you have selected manual proxy settings at Choose how to specify proxy server settings. You should leave this policy not set if you have selected any other mode for setting proxy policies. For more detailed examples, visit: http://www.chromium.org/developers- /design-documents/network-settings#TOC-Command-line-options-for-proxy-sett		
58	AllowOutdatedPlugins (Allow running plugins that are outdated)	N/A	N/A
	Allows Google Chrome to run plugins that are outdated. If you enable this setting, outdated plugins are used as normal plugins. If you disable this setting, outdated plugins will not be used and users will not be asked for permission to run them. If this setting is not set, users will be asked for permission to run outdated plugins.		
59	DnsPrefetchingEnabled (Enable network prediction)	N/A	Setting is available as DNS (Disable DNS Prefetching) in this browser
	Enables network prediction in Google Chrome and prevents users from changing this setting. This controls not only DNS prefetching but also TCP and SSL preconnection and prerendering of web pages. The policy name refers to DNS prefetching for historical reasons. If you enable or disable this setting, users cannot change or override this setting in Google Chrome. If this policy is left not set, this will be enabled but the user will be able to change it.		
60	EnableOnlineRevocationChecks (Whether online OCSP/CRL checks are performed)	N/A	N/A
	In light of the fact that soft-fail, online revocation checks provide no effective security benefit, they are disabled by default in Google Chrome version 19 and later. By setting this policy to true, the previous behaviour is restored and online OCSP/CRL checks will be performed. If the policy is not set, or is set to false, then Chrome will not perform online revocation checks in Chrome 19 and later.		
61	EnabledPlugins (Specify a list of enabled plugins)	N/A	N/A
	Specifies a list of plugins that are enabled in Google Chrome and prevents users from changing this setting. The wildcard characters * and ? can be used to match sequences of arbitrary characters. * matches an arbitrary number of characters while ? specifies an optional single character, i.e. matches zero or one characters. The escape character is /, so to match actual *, ?, or / characters, you can put a / in front of them. The specified list of plugins is always used in Google Chrome if they are installed. The plugins are marked as enabled in about:plugins and users cannot disable them. Note that this policy overrides both DisabledPlugins and DisabledPluginsExceptions. If this policy is left not set the user can disable any plugin installed on the system.		

62	ImportBookmarks (Import bookmarks from default browser on first run)	N/A	N/A
	This policy forces bookmarks to be imported from the current default browser if enabled. If enabled, this policy also affects the import dialog. If disabled, no bookmarks are imported. If it is not set, the user may be asked whether to import, or importing may happen automatically.		
63	ImportBookmarks_recommended (Import bookmarks from default browser on first run)	N/A	N/A
	This policy forces bookmarks to be imported from the current default browser if enabled. If enabled, this policy also affects the import dialog. If disabled, no bookmarks are imported. If it is not set, the user may be asked whether to import, or importing may happen automatically.		
64	ImportHistory (Import browsing history from default browser on first run)	Similar semantics can be achieved by modifying multiple settings at different zones	Similar semantics can be achieved by using different third party Add-ons
	This policy forces the browsing history to be imported from the current default browser if enabled. If enabled, this policy also affects the import dialog. If disabled, no browsing history is imported. If it is not set, the user may be asked whether to import, or importing may happen automatically.		
65	ImportHistory_recommended (Import browsing history from default browser on first run)	N/A	N/A
	This policy forces the browsing history to be imported from the current default browser if enabled. If enabled, this policy also affects the import dialog. If disabled, no browsing history is imported. If it is not set, the user may be asked whether to import, or importing may happen automatically.		
66	ImportSavedPasswords (Import saved passwords from default browser on first run)	Similar semantics can be achieved by modifying multiple settings at different zones	Similar semantics can be achieved by using different third party Add-ons
	This policy forces the saved passwords to be imported from the previous default browser if enabled. If enabled, this policy also affects the import dialog. If disabled, the saved passwords are not imported. If it is not set, the user may be asked whether to import, or importing may happen automatically.		

67	ImportSavedPasswords_-recommended (Import saved passwords from default browser on first run)	N/A	N/A
	This policy forces the saved passwords to be imported from the previous default browser if enabled. If enabled, this policy also affects the import dialog. If disabled, the saved passwords are not imported. If it is not set, the user may be asked whether to import, or importing may happen automatically.		
68	MaxConnectionsPerProxy (Maximal number of concurrent connections to the proxy server)	N/A	Setting is available as Max_Proxy (Set maximum number of connections to proxy server) in this browser
	Specifies the maximal number of simultaneous connections to the proxy server. Some proxy servers can not handle high number of concurrent connections per client and this can be solved by setting this policy to a lower value. The value of this policy should be lower than 100 and higher than 6 and the default value is 32. Some web apps are known to consume many connections with hanging GETs, so lowering below 32 may lead to browser networking hangs if too many such web apps are open. Lower below the default at your own risk. If this policy is left not set the default value will be used which is 32.		
69	MaxInvalidationFetchDelay (Maximum fetch delay after a policy invalidation)	N/A	N/A
	Specifies the maximum delay in milliseconds between receiving a policy invalidation and fetching the new policy from the device management service. Setting this policy overrides the default value of 5000 milliseconds. Valid values for this policy are in the range from 1000 (1 second) to 300000 (5 minutes). Any values not in this range will be clamped to the respective boundary. Leaving this policy not set will make Google Chrome use the default value of 5000 milliseconds.		
70	MediaCacheSize (Set media disk cache size in bytes)	N/A	N/A
	Configures the cache size that Google Chrome will use for storing cached media files on the disk. If you set this policy, Google Chrome will use the provided cache size regardless whether the user has specified the –media-cache-size flag or not. If the value of this policy is 0, the default cache size will be used but the user will not be able to change it. If this policy is not set the default size will be used and the user will be able to override it with the –media-cache-size flag.		

71	MetricsReportingEnabled_recommended (Enable reporting of usage and crash-related data)	N/A	N/A
	Enables anonymous reporting of usage and crash-related data about Google Chrome to Google and prevents users from changing this setting. If you enable this setting, anonymous reporting of usage and crash-related data is sent to Google. If you disable this setting, anonymous reporting of usage and crash-related data is never sent to Google. If you enable or disable this setting, users cannot change or override this setting in Google Chrome. If this policy is left not set the setting will be what the user chose upon installation / first run.		
72	SafeBrowsingEnabled (Enable Safe Browsing)	N/A	Setting is available as Safe_Browsing (Enable Safe Browsing) in this browser
	Enables Google Chromes Safe Browsing feature and prevents users from changing this setting. If you enable this setting, Safe Browsing is always active. If you disable this setting, Safe Browsing is never active. If you enable or disable this setting, users cannot change or override the "Enable phishing and malware protection" setting in Google Chrome. If this policy is left not set, this will be enabled but the user will be able to change it.		
73	SafeBrowsingEnabled_recommended (Enable Safe Browsing)	N/A	N/A
	Enables Google Chromes Safe Browsing feature and prevents users from changing this setting. If you enable this setting, Safe Browsing is always active. If you disable this setting, Safe Browsing is never active. If you enable or disable this setting, users cannot change or override the "Enable phishing and malware protection" setting in Google Chrome. If this policy is left not set, this will be enabled but the user will be able to change it.		
74	SavingBrowserHistoryDisabled (Disable saving browser history)	Similar semantics can be achieved by modifying multiple settings at different zones	Similar semantics can be achieved by modifying multiple entries in about:config
	Disables saving browser history in Google Chrome and prevents users from changing this setting. If this setting is enabled, browsing history is not saved. If this setting is disabled or not set, browsing history is saved.		

75	URLBlacklist (Block access to a list of URLs)	Similar semantics can be achieved by modifying multiple settings at different zones	Similar semantics can be achieved by using different third party Add-ons
	Blocks access to the listed URLs. This policy prevents the user from loading web pages from blacklisted URLs. A URL has the format scheme://host:port/path. The optional scheme can be http, https or ftp. Only this scheme will be blocked; if none is specified, all schemes are blocked. The host can be a hostname or an IP address. Subdomains of a hostname will also be blocked. To prevent blocking subdomains, include a . before the hostname. The special hostname * will block all domains. The optional port is a valid port number from 1 to 65535. If none is specified, all ports are blocked. If the optional path is specified, only paths with that prefix will be blocked. Exceptions can be defined in the URL whitelist policy. These policies are limited to 1000 entries; subsequent entries will be ignored. If this policy is not set no URL will be blacklisted in the browser.		
76	URLWhitelist (Allows access to a list of URLs)	Similar semantics can be achieved by modifying multiple settings at different zones	Similar semantics can be achieved by using different third party Add-ons
	Allows access to the listed URLs, as exceptions to the URL blacklist. See the description of the URL blacklist policy for the format of entries of this list. This policy can be used to open exceptions to restrictive blacklists. For example, * can be blacklisted to block all requests, and this policy can be used to allow access to a limited list of URLs. It can be used to open exceptions to certain schemes, subdomains of other domains, ports, or specific paths. The most specific filter will determine if a URL is blocked or allowed. The whitelist takes precedence over the blacklist. This policy is limited to 1000 entries; subsequent entries will be ignored. If this policy is not set there will be no exceptions to the blacklist from the URLBlacklist policy.		

Notations for Table A.2

1. Firefox: Comparison in Mozilla Firefox
2. Chrome: Comparison in Google Chrome
3. IE: Internet Explorer (policy name and display name)
4. Description: Description about the policy in Internet Explorer
5. N/A: Setting is not available in this browser

Table A.2: Comparison of Security Related Settings for Internet Explorer with Respect to Google Chrome and Mozilla Firefox

EN	**IE**	**Google Chrome**	**Firefox**
	Description		

1	Advanced_CertificateRevocation (Check for server certificate revocation)	N/A	N/A
	This policy setting allows you to manage whether Internet Explorer will check revocation status of servers certificates. Certificates are revoked when they have been compromised or are no longer valid, and this option protects users from submitting confidential data to a site that may be fraudulent or not secure. If you enable this policy setting, Internet Explorer will check to see if server certificates have been revoked. If you disable this policy setting, Internet Explorer will not check server certificates to see if they have been revoked. If you do not configure this policy setting, Internet Explorer will not check server certificates to see if they have been revoked.		
2	Advanced_EnableEnhancedProtectedMode (Turn on Enhanced Protected Mode)	N/A	N/A
	Enhanced Protected Mode provides additional protection against malicious websites by using 64-bit processes on 64-bit versions of Windows. For computers running at least Windows 8, Enhanced Protected Mode also limits the locations Internet Explorer can read from in the registry and the file system. If you enable this policy setting, Enhanced Protected Mode will be turned on. Any zone that has Protected Mode enabled will use Enhanced Protected Mode. Users will not be able to disable Enhanced Protected Mode. If you disable this policy setting, Enhanced Protected Mode will be turned off. Any zone that has Protected Mode enabled will use the version of Protected Mode introduced in Internet Explorer 7 for Windows Vista. If you do not configure this policy, users will be able to turn on or turn off Enhanced Protected Mode on the Advanced tab of the Internet Options dialog.		
3	Advanced_DisableEPMCompat (Do not allow ActiveX controls to run in Protected Mode when Enhanced Protected Mode is enabled)	N/A	N/A
	This policy setting prevents ActiveX controls from running in Protected Mode when Enhanced Protected Mode is enabled. When a user has an ActiveX control installed that is not compatible with Enhanced Protected Mode and a website attempts to load the control, Internet Explorer notifies the user and gives the option to run the website in regular Protected Mode. This policy setting disables this notification and forces all websites to run in Enhanced Protected Mode. Enhanced Protected Mode provides additional protection against malicious websites by using 64-bit processes on 64-bit versions of Windows. For computers running at least Windows 8, Enhanced Protected Mode also limits the locations Internet Explorer can read from in the registry and the file system. When Enhanced Protected Mode is enabled, and a user encounters a website that attempts to load an ActiveX control that is not compatible with Enhanced Protected Mode, Internet Explorer notifies the user and gives the option to disable Enhanced Protected Mode for that particular website. If you enable this policy setting, Internet Explorer will not give the user the option to disable Enhanced Protected Mode. All Protected Mode websites will run in Enhanced Protected Mode. If you disable or do not configure this policy setting, Internet Explorer notifies users and provides an option to run websites with incompatible ActiveX controls in regular Protected Mode. This is the default behavior.		

4	Advanced_Enable-Http1_1 (Use HTTP 1.1)	N/A	N/A
	This policy setting allows you to manage whether Internet Explorer uses HTTP 1.1. If you enable this policy setting, Internet Explorer uses HTTP 1.1. If you disable this policy setting, Internet Explorer does not use HTTP 1.1. If you do not configure this policy setting, users can configure Internet Explorer to use or not use HTTP 1.1.		
5	Advanced_ProxyHttp1_1 (Use HTTP 1.1 through proxy connections)	N/A	N/A
	This policy setting allows you to manage whether Internet Explorer uses HTTP 1.1 through proxy connections. If you enable this policy setting, Internet Explorer uses HTTP 1.1 through proxy connections. If you disable this policy setting, Internet Explorer does not use HTTP 1.1 through proxy connections. If you do not configure this policy setting, users can configure Internet Explorer to use or not use HTTP 1.1 through proxy connections.		
6	Advanced_SetWinInet-Protocols (Turn off encryption support)	N/A	N/A
	This policy setting allows you to turn off support for Transport Layer Security (TLS) 1.0, TLS 1.1, TLS 1.2, Secure Sockets Layer (SSL) 2.0, or SSL 3.0 in the browser. TLS and SSL are protocols that help protect communication between the browser and the target server. When the browser attempts to set up a protected communication with the target server, the browser and server negotiate which protocol and version to use. The browser and server attempt to match each others list of supported protocols and versions, and they select the most preferred match. If you enable this policy setting, the browser negotiates or does not negotiate an encryption tunnel by using the encryption methods that you select from the drop-down list. If you disable or do not configure this policy setting, the user can select which encryption method the browser supports. Note: SSL 2.0 is off by default. SSL 2.0 is an outdated security protocol, and enabling SSL 2.0 impairs the performance and functionality of TLS 1.0.		
7	Advanced_InstallOnDemand_IE (Allow Install On Demand (Internet Explorer))	N/A	N/A
	This policy setting allows you to manage whether users can automatically download and install Web components (such as fonts) that can installed by Internet Explorer Active Setup. For example, if you open a Web page that requires Japanese-text display support, Internet Explorer could prompt the user to download the Japanese Language Pack component if it is not already installed. If you enable this policy setting, Web components such as fonts will be automatically installed as necessary. If you disable this policy setting, users will be prompted when Web Components such as fonts would be downloaded. If you do not configure this policy, users will be prompted when Web Components such as fonts would be downloaded.		

8	Advanced_InstallOnDemand_Other (Allow Install On Demand (except Internet Explorer))	N/A	N/A
	This policy setting allows you to manage whether users can download and install self-installing program files (non-Internet Explorer components) that are registered with Internet Explorer (such as Macromedia and Java) that are required in order to view web pages as intended. If you enable this policy setting, non-Internet Explorer components will be automatically installed as necessary. If you disable this policy setting, users will be prompted when non-Internet Explorer components would be installed. If you do not configure this policy setting, non-Internet Explorer components will be automatically installed as necessary.		
9	Advanced_InternetExplorerUpdates (Automatically check for Internet Explorer updates)	N/A	N/A
	This policy setting allows you to manage whether Internet Explorer checks the Internet for newer versions. When Internet Explorer is set to do this, the checks occur approximately every 30 days, and users are prompted to install new versions as they become available. If you enable this policy setting, Internet Explorer checks the Internet for a new version approximately every 30 days and prompts the user to download new versions when they are available. If you disable this policy setting, Internet Explorer does not check the Internet for new versions of the browser, so does not prompt users to install them. If you do not configure this policy setting, Internet Explorer does not check the Internet for new versions of the browser, so does not prompt users to install them.		
10	Advanced_InvalidSignatureBlock (Allow software to run or install even if the signature is invalid)	N/A	N/A
	This policy setting allows you to manage whether software, such as ActiveX controls and file downloads, can be installed or run by the user even though the signature is invalid. An invalid signature might indicate that someone has tampered with the file. If you enable this policy setting, users will be prompted to install or run files with an invalid signature. If you disable this policy setting, users cannot run or install files with an invalid signature. If you do not configure this policy, users can choose to run or install files with an invalid signature.		
11	Advanced_SaveEncryptedPages (Do not save encrypted pages to disk)	N/A	N/A
	This policy setting allows you to manage whether Internet Explorer will save encrypted pages that contain secure (HTTPS) information such as passwords and credit card numbers to the Internet Explorer cache, which may be insecure. If you enable this policy setting, Internet Explorer will not save encrypted pages containing secure (HTTPS) information to the cache. If you disable this policy setting, Internet Explorer will save encrypted pages containing secure (HTTPS) information to the cache. If you do not configure this policy, Internet Explorer will save encrypted pages containing secure (HTTPS) information to the cache.		

12	Advanced_Temporary-InternetFiles (Empty Temporary Internet Files folder when browser is closed)	`Similar semantics can be achieved by modifying multiple settings`	`N/A`
	This policy setting allows you to manage whether Internet Explorer deletes the contents of the Temporary Internet Files folder after all browser windows are closed. This protects against storing dangerous files on the computer, or storing sensitive files that other users could see, in addition to managing total disk space usage. If you enable this policy setting, Internet Explorer will delete the contents of the users Temporary Internet Files folder when all browser windows are closed. If you disable this policy setting, Internet Explorer will not delete the contents of the users Temporary Internet Files folder when browser windows are closed. If you do not configure this policy, Internet Explorer will not delete the contents of the Temporary Internet Files folder when browser windows are closed.		
13	ControlPanel_Restrict-SecurityTab (Disable the Security page)	`N/A`	`N/A`
	Removes the Security tab from the interface in the Internet Options dialog box. If you enable this policy, it prevents users from seeing and changing settings for security zones, such as scripting, downloads, and user authentication. If you disable this policy or do not configure it, users can see and change these settings. When you set this policy, you do not need to set the following Internet Explorer policies, because this policy removes the Security tab from the interface: Security zones: Do not allow users to change policies Security zones: Do not allow users to add/delete sites		
14	ControlPanel_-SendIDNNames (Send internationalized domain names)	`N/A`	`N/A`
	This policy setting allows you to manage whether Internet Explorer converts Unicode domain names to internationalized domain name (IDN) format (Punycode) before sending them to Domain Name System (DNS) servers or to proxy servers. If you enable this policy setting, you must specify when IDN server names should be sent: 0) Unicode domain names are never converted to IDN format. 1) Unicode domain names are converted to IDN format only for addresses that are not in the Intranet zone. 2) Unicode domain names are converted to IDN format only for addresses that are in the Intranet zone. 3) Unicode domain names are always converted to IDN format. If you disable or do not configure this policy setting, the user can control this setting by using Advanced Options in Internet Control Panel. By default, domain names are converted to IDN format only for addresses that are not in the Intranet zone.		
15	ControlPanel_-SendUTF8Query (Use UTF-8 for mailto links)	`N/A`	`N/A`
	This policy setting allows you to manage whether Internet Explorer uses 8-bit Unicode Transformation Format (UTF-8) for mailto links. If you enable this policy setting, Internet Explorer encodes mailto links in UTF-8. If you disable or do not configure this policy setting, Internet Explorer sends mailto links encoded through the users code page. This behavior matches the behavior of Internet Explorer 6 and earlier. The user can change this behavior on the Internet Explorer Tools menu: Click Internet Options, click the Advanced tab, and then under International, select the Use UTF-8 for mailto links check box.		

16	NoCertError (Prevent ignoring certificate errors)	N/A	N/A
	This policy setting prevents the user from ignoring Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificate errors that interrupt browsing (such as expired, revoked, or name mismatch errors) in Internet Explorer. If you enable this policy setting, the user cannot continue browsing. If you disable or do not configure this policy setting, the user can choose to ignore certificate errors and continue browsing.		
17	AddonManagement_AddOnList (Add-on List)	Similar semantics can be achieved by modifying multiple settings	Similar semantics can be achieved by modifying multiple entries in about:config
	This policy setting allows you to manage a list of add-ons to be allowed or denied by Internet Explorer. Add-ons in this case are controls like ActiveX Controls, Toolbars, and Browser Helper Objects (BHOs) which are specifically written to extend or enhance the functionality of the browser or web pages. This list can be used with the Deny all add-ons unless specifically allowed in the Add-on List policy setting, which defines whether add-ons not listed here are assumed to be denied. If you enable this policy setting, you can enter a list of add-ons to be allowed or denied by Internet Explorer. For each entry that you add to the list, enter the following information: Name of the Value the CLSID (class identifier) for the add on you wish to add to the list. The CLSID should be in brackets for example, 000000000-0000-0000-0000-0000000000000. The CLSID for an addon can be obtained by reading the OBJECT tag from a Web page on which the addon is referenced. Value - A number indicating whether Internet Explorer should deny or allow the add-on to be loaded. To specify that an add-on should be denied enter a 0 (zero) into this field. To specify that an add-on should be allowed, enter a 1 (one) into this field. To specify that an add-on should be allowed and also permit the user to manage the add-on through Add-on Manager, enter a 2 (two) into this field. If you disable this policy setting, the list is deleted. The Deny all add-ons unless specifically allowed in the Add-on List policy setting will still determine whether add-ons not in this list are assumed to be denied.		
18	AddonManagement_ManagementMode (Deny all add-ons unless specifically allowed in the Add-on List)	N/A	N/A
	This policy setting allows you to ensure that any Internet Explorer add-ons not listed in the Add-on List policy setting are denied. Add-ons in this case are controls like ActiveX Controls, Toolbars, and Browser Helper Objects (BHOs) which are specifically written to extend or enhance the functionality of the browser or web pages. By default, the Add-on List policy setting defines a list of add-ons to be allowed or denied through Group Policy. However, users can still use the Add-on Manager within Internet Explorer to manage add-ons not listed within the Add-on List policy setting. This policy setting effectively removes this option from users - all add-ons are assumed to be denied unless they are specifically allowed through the Add-on List policy setting. If you enable this policy setting, Internet Explorer only allows add-ons that are specifically listed (and allowed) through the Add-on List policy setting. If you disable or do not configure this policy setting, users may use Add-on Manager to allow or deny any add-ons that are not included in the Add-on List policy setting. Note: If an add-on is listed in the Add-on List policy setting, the user cannot change its state through Add-on Manager (unless its value has been set to allow user management - see the Add-on List policy for more details).		

19	IESF_PolicyProcessList_13 (Process List)	N/A	N/A
	This policy setting allows you to manage whether the listed processes respect add-on management user preferences (as entered into Add-on Manager) or policy settings. By default, only Internet Explorer processes use the add-on management user preferences and policy settings. This policy setting allows you to extend support for these user preferences and policy settings to specific processes listed in the process list. If you enable this policy setting and enter a Value of 1, the process entered will respect the add-on management user preferences and policy settings. If you enter a Value of 0, the add-on management user preferences and policy settings are ignored by the specified process. The Value Name is the name of the executable. If a Value Name is empty or the Value is not 0 or 1, the policy setting is ignored. Do not enter Internet Explorer processes in this list because these processes always respect add-on management user preferences and policy settings. If the All Processes policy setting is enabled, the processes configured in this policy setting take precedence over that setting. If you do not configure this policy, processes other than the Internet Explorer processes will not be affected by add-on management user preferences or policy settings (unless All Processes is enabled).		
20	IESF_Policy_BinaryBehaviorAdminAllow (Admin-approved behaviors)	N/A	N/A
	For each zone, the Binary and Scripted Behavior security restrictions may be configured to allow only a list of admin-approved behaviors. This list may be configured here, and applies to all processes which have opted in to the behavior, and to all zones. (Behaviors are components that encapsulate specific functionality or behavior on a page.) If you enable this policy setting, this sets the list of behaviors permitted in each zone for which Script and Binary Behaviors is set to admin-approved. Behaviors must be entered in #package#behavior notation, e.g., #default#vml. If you disable this policy setting, no behaviors will be allowed in zones set to admin-approved, just as if those zones were set to disable. If you do not configure this policy setting, only VML will be allowed in zones set to admin-approved. Note. If this policy is set in both Computer Configuration and User Configuration, both lists of behaviors will be allowed as appropriate.		
21	IESF_PolicyExplorerProcesses_2 (Internet Explorer Processes)	N/A	N/A
	Internet Explorer contains dynamic binary behaviors: components that encapsulate specific functionality for the HTML elements to which they are attached. This policy setting controls whether the Binary Behavior Security Restriction setting is prevented or allowed. If you enable this policy setting, binary behaviors are prevented for the File Explorer and Internet Explorer processes. If you disable this policy setting, binary behaviors are allowed for the File Explorer and Internet Explorer processes. If you do not configure this policy setting, binary behaviors are prevented for the File Explorer and Internet Explorer processes.		

22	IESF_PolicyProcessList_2 (Process List)	N/A	N/A
	Internet Explorer contains dynamic binary behaviors: components that encapsulate specific functionality for the HTML elements to which they are attached. This policy setting controls whether the Binary Behavior Security Restriction setting is prevented or allowed. This policy setting allows administrators to define applications for which they want this security feature to be prevented or allowed. If you enable this policy setting and enter a Value of 1 binary behaviors are prevented. If you enter a Value of 0 binary behaviors are allowed. The Value Name is the name of the executable. If a Value Name is empty or the Value is not 0 or 1, the policy setting is ignored. Do not enter the Internet Explorer processes in this list: use the related Internet Explorer Processes policy to enable or disable IE processes. If the All Processes policy setting is enabled, the processes configured in this box take precedence over that setting. If you disable or do not configure this policy setting, the security feature is allowed.		
23	IESF_PolicyExplorerProcesses_5 (Internet Explorer Processes)	N/A	N/A
	Internet Explorer uses Multipurpose Internet Mail Extensions (MIME) data to determine file handling procedures for files received through a Web server. This policy setting determines whether Internet Explorer requires that all file-type information provided by Web servers be consistent. For example, if the MIME type of a file is text/plain but the MIME sniff indicates that the file is really an executable file, Internet Explorer renames the file by saving it in the Internet Explorer cache and changing its extension. If you enable this policy setting, Internet Explorer requires consistent MIME data for all received files. If you disable this policy setting, Internet Explorer will not require consistent MIME data for all received files. If you do not configure this policy setting, Internet Explorer requires consistent MIME data for all received files.		
24	IESF_PolicyProcessList_5 (Process List)	N/A	N/A
	Internet Explorer uses Multipurpose Internet Mail Extensions (MIME) data to determine file handling procedures for files received through a Web server. This policy setting determines whether Internet Explorer requires that all file-type information provided by Web servers be consistent. For example, if the MIME type of a file is text/plain but the MIME sniff indicates that the file is really an executable file, Internet Explorer renames the file by saving it in the Internet Explorer cache and changing its extension. This policy setting allows administrators to define applications for which they want this security feature to be prevented or allowed. If you enable this policy setting and enter a Value of 1, MIME handling is in effect. If you enter a Value of 0 file-type information is allowed to be inconsistent. The Value Name is the name of the executable. If a Value Name is empty or the Value is not 0 or 1, the policy setting is ignored. Do not enter the Internet Explorer processes in this list: use the related Internet Explorer Processes policy to enable or disable IE processes. If the All Processes policy setting is enabled, the processes configured in this box take precedence over that setting. If you disable or do not configure this policy setting, the security feature is allowed.		

25	IESF_PolicyExplorerProcesses_10 (Internet Explorer Processes)	`Similar semantics can be achieved by modifying multiple settings`	`N/A`
	This policy setting allows you to manage whether the Notification bar is displayed for Internet Explorer processes when file or code installs are restricted. By default, the Notification bar is displayed for Internet Explorer processes. If you enable this policy setting, the Notification bar will be displayed for Internet Explorer Processes. If you disable this policy setting, the Notification bar will not be displayed for Internet Explorer processes. If you do not configure this policy setting, the Notification bar will be displayed for Internet Explorer Processes.		
26	IESF_PolicyProcessList_10 (Process List)	`N/A`	`N/A`
	This policy setting allows you to manage whether the Notification bar is displayed for specific processes when file or code installs are restricted. By default, the Notification bar is not displayed for any process when file or code installs are restricted (except for the Internet Explorer Processes, for which the Notification bar is displayed by default). If you enable this policy setting and enter a Value of 1, the Notification bar is displayed. If you enter a Value of 0 the Notification bar is not displayed. The Value Name is the name of the executable. If a Value Name is empty or the Value is not 0 or 1, the policy setting is ignored. Do not enter the Internet Explorer processes in this list: use the related Internet Explorer Processes policy to enable or disable for IE processes. If the All Processes policy setting is enabled, the processes configured in this box take precedence over that setting. If you disable or do not configure this policy setting, the Notification bar is not displayed for the specified processes.		
27	IESF_PolicyExplorerProcesses_4 (Internet Explorer Processes)	`N/A`	`N/A`
	Internet Explorer places zone restrictions on each Web page it opens, which are dependent upon the location of the Web page (Internet, Intranet, Local Machine zone, etc.). Web pages on the local computer have the fewest security restrictions and reside in the Local Machine zone. Local Machine zone security applies to all local files and content processed by Internet Explorer. This feature helps to mitigate attacks where the Local Machine zone is used as an attack vector to load malicious HTML code. If you enable this policy setting, the Local Machine zone security applies to all local files and content processed by Internet Explorer. If you disable this policy setting, Local Machine zone security is not applied to local files or content processed by Internet Explorer. If you do not configure this policy setting, the Local Machine zone security applies to all local files and content processed by Internet Explorer.		

28	IESF_PolicyProcessList_4 (Process List)	N/A	N/A
	Internet Explorer places zone restrictions on each Web page it opens, which are dependent upon 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. Local Machine zone security applies to all local files and content. This feature helps to mitigate attacks where the Local Machine zone is used as an attack vector to load malicious HTML code. If you enable this policy setting and enter a value of 1, Local Machine Zone security applies. If you enter a value of 0, Local Machine Zone security does not apply. If a Value Name is empty or the Value is not 0 or 1, the policy setting is ignored. Do not enter the Internet Explorer processes in this list: use the related Internet Explorer Processes policy to enable or disable IE processes. If the All Processes policy setting is enabled, the processes configured in this box take precedence over that setting. If you disable or do not configure this policy setting, the security feature is allowed.		
29	IESF_PolicyExplorerProcesses_6 (Internet Explorer Processes)	N/A	N/A
	This policy setting determines whether Internet Explorer MIME sniffing will prevent promotion of a file of one type to a more dangerous file type. If you enable this policy setting, MIME sniffing will never promote a file of one type to a more dangerous file type. If you disable this policy setting, Internet Explorer processes will allow a MIME sniff promoting a file of one type to a more dangerous file type. If you do not configure this policy setting, MIME sniffing will never promote a file of one type to a more dangerous file type.		
30	IESF_PolicyProcessList_6 (Process List)	N/A	N/A
	This policy setting determines whether Internet Explorer MIME sniffing will prevent promotion of a file of one type to a more dangerous file type. This policy setting allows administrators to define applications for which they want this security feature to be prevented or allowed. If you enable this policy setting and enter a Value of 1, this protection will be in effect. If you enter a Value of 0, any file may be promoted to more dangerous file types. The Value Name is the name of the executable. If a Value Name is empty or the Value is not 0 or 1, the policy setting is ignored. Do not enter the Internet Explorer processes in this list: use the related Internet Explorer Processes policy to enable or disable IE processes. If the All Processes policy setting is enabled, the processes configured in this box take precedence over that setting. If you disable or do not configure this policy setting, the security feature is allowed.		
31	IESF_PolicyExplorerProcesses_3 (Internet Explorer Processes)	N/A	N/A
	The MK Protocol Security Restriction policy setting reduces attack surface area by preventing the MK protocol. Resources hosted on the MK protocol will fail. If you enable this policy setting, the MK Protocol is prevented for File Explorer and Internet Explorer, and resources hosted on the MK protocol will fail. If you disable this policy setting, applications can use the MK protocol API. Resources hosted on the MK protocol will work for the File Explorer and Internet Explorer processes. If you do not configure this policy setting, the MK Protocol is prevented for File Explorer and Internet Explorer, and resources hosted on the MK protocol will fail.		

32	IESF_PolicyProcessList_3 (Process List)	N/A	N/A
	The MK Protocol Security Restriction policy setting reduces attack surface area by preventing the MK protocol. Resources hosted on the MK protocol will fail. This policy setting allows administrators to define applications for which they want this security feature to be prevented or allowed. If you enable this policy setting and enter a Value of 1, use of the MK protocol is prevented. If you enter a Value of 0, use of the MK protocol is allowed. If a Value Name is empty or the Value is not 0 or 1, the policy setting is ignored. Do not enter the Internet Explorer processes in this list: use the related Internet Explorer Processes policy to enable or disable IE processes. If the All Processes policy setting is enabled, the processes configured in this box take precedence over that setting. If you disable or do not configure this policy setting, the policy setting is ignored.		
33	IESF_PolicyExplorerProcesses_13 (Internet Explorer Processes)	N/A	N/A
	File Explorer and Internet Explorer may be configured to prevent active content obtained through restricted protocols from running in an unsafe manner. This policy setting controls whether restricting content obtained through restricted protocols is prevented or allowed. If you enable this policy setting, restricting content obtained through restricted protocols is allowed for File Explorer and Internet Explorer processes. For example, you can restrict active content from pages served over the http and https protocols by adding the value names http and https. If you disable this policy setting, restricting content obtained through restricted protocols is prevented for File Explorer and Internet Explorer processes. If you do not configure this policy setting, the policy setting is ignored.		
34	IESF_PolicyProcessList_14 (Process List)	N/A	N/A
	Internet Explorer may be configured to prevent active content obtained through restricted protocols from running in an unsafe manner. This policy setting controls whether restricting content obtained through restricted protocols is prevented or allowed. This policy setting allows administrators to define applications for which they want restricting content obtained through restricted protocols to be prevented or allowed. If you enable this policy setting and enter a Value of 1, restricting content obtained through restricted protocols is allowed. If you enter a Value of 0, restricting content obtained through restricted protocols is blocked. The Value Name is the name of the executable. If a Value Name is empty or the Value is not 0 or 1, the policy setting is ignored. Do not enter the File Explorer or Internet Explorer processes in this list: use the related Internet Explorer Processes policy to enable or disable these processes. If the All Processes policy setting is enabled, the processes configured in this box take precedence over that setting. If you disable or do not configure this policy setting, the security feature is allowed.		

35	IESF_PolicyExplorerProcesses_7 (Internet Explorer Processes)	N/A	N/A
	This policy 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.		
36	IESF_PolicyProcessList_7 (Process List)	N/A	N/A
	This policy setting defines whether a reference to an object is accessible when the user navigates within the same domain or to a new domain. This policy setting allows administrators to define applications for which they want this security feature to be prevented or allowed. If you enable this policy setting and enter a Value of 1, references to objects are inaccessible after navigation. If you enter a Value of 0, references to objects are still accessible after navigation. The Value Name is the name of the executable. If a Value Name is empty or the Value is not 0 or 1, the policy setting is ignored. Do not enter the Internet Explorer processes in this list: use the related Internet Explorer Processes policy to enable or disable IE processes. If the All Processes policy setting is enabled, the processes configured in this box take precedence over that setting. If you disable or do not configure this policy setting, the security feature is allowed.		
37	IESF_PolicyExplorerProcesses_9 (Internet Explorer Processes)	N/A	N/A
	Internet Explorer places restrictions on each Web page it opens. The restrictions are dependent upon the location of the Web page (Internet, Intranet, Local Machine zone, etc.). 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.		

38	IESF_PolicyProcessList_9 (Process List)	N/A	N/A
	Internet Explorer places restrictions on each Web page it opens. The restrictions are dependent upon 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. This policy setting allows administrators to define applications for which they want this security feature to be prevented or allowed. If you enable this policy setting and enter a Value of 1, elevation to more privileged zones can be prevented. If you enter a Value of 0, elevation to any zone is allowed. The Value Name is the name of the executable. If a Value Name is empty or the Value is not 0 or 1, the policy setting is ignored. Do not enter the Internet Explorer processes in this list: use the related Internet Explorer Processes policy to enable or disable IE processes. If the All Processes policy setting is enabled, the processes configured in this box take precedence over that setting. If you disable or do not configure this policy setting, the security feature is allowed.		
39	IESF_PolicyExplorerProcesses_11 (Internet Explorer Processes)	N/A	N/A
	This policy setting enables blocking of ActiveX control installation prompts for Internet Explorer processes. If you enable this policy setting, prompting for ActiveX control installations will be blocked for Internet Explorer processes. If you disable this policy setting, prompting for ActiveX control installations will not be blocked for Internet Explorer processes. If you do not configure this policy setting, the users preference will be used to determine whether to block ActiveX control installations for Internet Explorer processes.		
40	IESF_PolicyProcessList_11 (Process List)	N/A	N/A
	This policy setting enables applications hosting the Web Browser Control to block automatic prompting of ActiveX control installation. If you enable this policy setting and enter a Value of 1, automatic prompting of ActiveX control installation is blocked. If you enter a Value of 0, automatic prompting of ActiveX control installation is allowed. The Value Name is the name of the executable. If a Value Name is empty or the Value is not 0 or 1, the policy setting is ignored. Do not enter the Internet Explorer processes in this list: use the related Internet Explorer Processes policy to enable or disable IE processes. If the All Processes policy setting is enabled, the processes configured in this box take precedence over that setting. If you disable or do not configure this policy setting, the security feature is allowed.		
41	IESF_PolicyExplorerProcesses_12 (Internet Explorer Processes)	N/A	N/A
	This policy setting enables blocking of file download prompts that are not user initiated. If you enable this policy setting, file download prompts that are not user initiated will be blocked for Internet Explorer processes. If you disable this policy setting, prompting will occur for file downloads that are not user initiated for Internet Explorer processes. If you do not configure this policy setting, the users preference determines whether to prompt for file downloads that are not user initiated for Internet Explorer processes.		

42	IESF_PolicyProcessList_12 (Process List)	N/A	N/A
	This policy setting enables applications hosting the Web Browser Control to block automatic prompting of file downloads that are not user initiated. If you enable this policy setting and enter a Value of 1, automatic prompting of non-initiated file downloads is blocked. If you enter a Value of 0, automatic prompting of non-initiated file downloads is allowed. The Value Name is the name of the executable. If a Value Name is empty or the Value is not 0 or 1, the policy setting is ignored. Do not enter the Internet Explorer processes in this list: use the related Internet Explorer Processes policy to enable or disable IE processes. If the All Processes policy setting is enabled, the processes configured in this box take precedence over that setting. If you disable or do not configure this policy setting, the security feature is allowed.		
43	IESF_PolicyExplorerProcesses_8 (Internet Explorer Processes)	N/A	N/A
	Internet Explorer allows scripts to programmatically open, resize, and reposition windows of various types. The Window Restrictions security feature restricts popup windows and prohibits scripts from displaying windows in which the title and status bars are not visible to the user or obfuscate other Windows title and status bars. If you enable this policy setting, popup windows and other restrictions apply for File Explorer and Internet Explorer processes. If you disable this policy setting, scripts can continue to create popup windows and windows that obfuscate other windows. If you do not configure this policy setting, popup windows and other restrictions apply for File Explorer and Internet Explorer processes.		
44	IESF_PolicyProcessList_8 (Process List)	N/A	N/A
	Internet Explorer allows scripts to programmatically open, resize, and reposition windows of various types. The Window Restrictions security feature restricts popup windows and prohibits scripts from displaying windows in which the title and status bars are not visible to the user or obfuscate other Windows title and status bars. This policy setting allows administrators to define applications for which they want this security feature to be prevented or allowed. If you enable this policy setting and enter a Value of 1, such windows may not be opened. If you enter a Value of 0, windows have none of these restrictions. The Value Name is the name of the executable. If a Value Name is empty or the Value is not 0 or 1, the policy setting is ignored. Do not enter the Internet Explorer processes in this list: use the related Internet Explorer Processes policy to enable or disable IE processes. If the All Processes policy setting is enabled, the processes configured in this box take precedence over that setting. If you disable or do not configure this policy setting, the security feature is allowed.		

45	IESF_NPLRest_InternetZone (Internet Zone Restricted Protocols)	N/A	N/A
	For each zone, the Network Protocol Lockdown security restriction may be configured to prevent active content obtained through restricted protocols from running in an unsafe manner, either by prompting the user, or simply disabling the content. For each zone, this list of protocols may be configured here, and applies to all processes which have opted in to the security restriction. If you enable this policy setting for a zone, this sets the list of protocols to be restricted if that zone is set to Prompt or Disable for Allow active content over restricted protocols to access my computer. If you disable or do not configure this policy setting for a zone, no protocols are restricted for that zone, regardless of the setting for Allow active content over restricted protocols to access my computer. Note. If policy for a zone is set in both Computer Configuration and User Configuration, both lists of protocols will be restricted for that zone.		
46	IESF_NPLRest_IntranetZone (Intranet Zone Restricted Protocols)	N/A	N/A
	For each zone, the Network Protocol Lockdown security restriction may be configured to prevent active content obtained through restricted protocols from running in an unsafe manner, either by prompting the user, or simply disabling the content. For each zone, this list of protocols may be configured here, and applies to all processes which have opted in to the security restriction. If you enable this policy setting for a zone, this sets the list of protocols to be restricted if that zone is set to Prompt or Disable for Allow active content over restricted protocols to access my computer. If you disable or do not configure this policy setting for a zone, no protocols are restricted for that zone, regardless of the setting for Allow active content over restricted protocols to access my computer. Note. If policy for a zone is set in both Computer Configuration and User Configuration, both lists of protocols will be restricted for that zone.		
47	IESF_NPLRest_LocalMachineZone (Local Machine Zone Restricted Protocols)	N/A	N/A
	For each zone, the Network Protocol Lockdown security restriction may be configured to prevent active content obtained through restricted protocols from running in an unsafe manner, either by prompting the user, or simply disabling the content. For each zone, this list of protocols may be configured here, and applies to all processes which have opted in to the security restriction. If you enable this policy setting for a zone, this sets the list of protocols to be restricted if that zone is set to Prompt or Disable for Allow active content over restricted protocols to access my computer. If you disable or do not configure this policy setting for a zone, no protocols are restricted for that zone, regardless of the setting for Allow active content over restricted protocols to access my computer. Note. If policy for a zone is set in both Computer Configuration and User Configuration, both lists of protocols will be restricted for that zone.		

48	IESF_NPLRest_RestrictedSitesZone (Restricted Sites Zone Restricted Protocols)	N/A	N/A
	For each zone, the Network Protocol Lockdown security restriction may be configured to prevent active content obtained through restricted protocols from running in an unsafe manner, either by prompting the user, or simply disabling the content. For each zone, this list of protocols may be configured here, and applies to all processes which have opted in to the security restriction. If you enable this policy setting for a zone, this sets the list of protocols to be restricted if that zone is set to Prompt or Disable for Allow active content over restricted protocols to access my computer. If you disable or do not configure this policy setting for a zone, no protocols are restricted for that zone, regardless of the setting for Allow active content over restricted protocols to access my computer. Note. If policy for a zone is set in both Computer Configuration and User Configuration, both lists of protocols will be restricted for that zone.		
49	IESF_NPLRest_TrustedSitesZone (Trusted Sites Zone Restricted Protocols)	N/A	N/A
	For each zone, the Network Protocol Lockdown security restriction may be configured to prevent active content obtained through restricted protocols from running in an unsafe manner, either by prompting the user, or simply disabling the content. For each zone, this list of protocols may be configured here, and applies to all processes which have opted in to the security restriction. If you enable this policy setting for a zone, this sets the list of protocols to be restricted if that zone is set to Prompt or Disable for Allow active content over restricted protocols to access my computer. If you disable or do not configure this policy setting for a zone, no protocols are restricted for that zone, regardless of the setting for Allow active content over restricted protocols to access my computer. Note. If policy for a zone is set in both Computer Configuration and User Configuration, both lists of protocols will be restricted for that zone.		
50	AddonManagement_RestrictCrashDetection (Turn off Crash Detection)	N/A	N/A
	This policy setting allows you to manage the crash detection feature of add-on Management. If you enable this policy setting, a crash in Internet Explorer will exhibit behavior found in Windows XP Professional Service Pack 1 and earlier, namely to invoke Windows Error Reporting. All policy settings for Windows Error Reporting continue to apply. If you disable or do not configure this policy setting, the crash detection feature for add-on management will be functional.		
51	AddonManagement_RestrictExtensionManagement (Do not allow users to enable or disable add-ons)	Similar semantics can be achieved by modifying multiple settings	N/A
	This policy setting allows you to manage whether users have the ability to allow or deny add-ons through Add-On Manager. If you enable this policy setting, users cannot enable or disable add-ons through Add-On Manager. The only exception occurs if an add-on has been specifically entered into the Add-On List policy setting in such a way as to allow users to continue to manage the add-on. In this case, the user can still manage the add-on through the Add-On Manager. If you disable or do not configure this policy setting, the appropriate controls in the Add-On Manager will be available to the user.		

52	Disable_Fix_Security_-Settings (Prevent Fix settings functionality)	N/A	N/A
	This policy setting prevents the user from using the Fix settings functionality related to Security Settings Check. If you enable this policy setting, the user cannot use the Fix settings functionality. If you disable or do not configure this policy setting, the user can use the Fix settings functionality. Note: When this policy setting is enabled, the Fix settings command on the Notification bar shortcut menu should be disabled.		
53	Disable_Managing_-Phishing_Filter (Prevent managing the phishing filter)	N/A	N/A
	This policy setting prevents the user from managing a filter that warns the user if the website being visited is known for fraudulent attempts to gather personal information through phishing. If you enable this policy setting, the user is not prompted to enable the phishing filter. You must specify which mode the phishing filter uses: manual, automatic, or off. If you select manual mode, the phishing filter performs only local analysis, and the user is prompted to permit any data to be sent to Microsoft. If the feature is fully enabled, all website addresses that are not on the filters allow list are sent automatically to Microsoft without prompting the user. If you disable or do not configure this policy setting, the user is prompted to decide the mode of operation for the phishing filter.		
54	Disable_Managing_-Safety_Filter_IE8 (Turn off Managing SmartScreen Filter for Internet Explorer 8)	N/A	N/A
	This policy setting allows the user to enable the SmartScreen Filter, which warns the user if the website being visited is known for fraudulent attempts to gather personal information through phishing, or is known to host malware. If you enable this policy setting, the user is not prompted to turn on SmartScreen Filter. You must specify which mode the SmartScreen Filter uses: on, or off.All website addresses that are not on the filters allow list are sent automatically to Microsoft without prompting the user. If you disable or do not configure this policy setting, the user is prompted to decide whether to turn on the SmartScreen Filter during the first-run experience.		
55	Disable_Managing_-Safety_Filter_IE9 (Prevent managing SmartScreen Filter)	N/A	N/A
	This policy setting prevents the user from managing SmartScreen Filter, which warns the user if the website being visited is known for fraudulent attempts to gather personal information through phishing, or is known to host malware. If you enable this policy setting, the user is not prompted to turn on SmartScreen Filter. All website addresses that are not on the filters allow list are sent automatically to Microsoft without prompting the user. If you disable or do not configure this policy setting, the user is prompted to decide whether to turn on SmartScreen Filter during the first-run experience.		

56	DisableSafetyFilterOverride (Prevent bypassing SmartScreen Filter warnings)	N/A	N/A
	This policy setting determines whether the user can bypass warnings from SmartScreen Filter. SmartScreen Filter prevents the user from browsing to or downloading from sites that are known to host malicious content. SmartScreen Filter also prevents the execution of files that are known to be malicious. If you enable this policy setting, SmartScreen Filter warnings block the user. If you disable or do not configure this policy setting, the user can bypass SmartScreen Filter warnings.		
57	DisableSafetyFilterOverrideForAppRepUnknown (Prevent bypassing SmartScreen Filter warnings about files that are not commonly downloaded from the Internet)	N/A	N/A
	This policy setting determines whether the user can bypass warnings from SmartScreen Filter. SmartScreen Filter warns the user about executable files that Internet Explorer users do not commonly download from the Internet. If you enable this policy setting, SmartScreen Filter warnings block the user. If you disable or do not configure this policy setting, the user can bypass SmartScreen Filter warnings.		
58	Disable_Security_Settings_Check (Turn off the Security Settings Check feature)	N/A	N/A
	This policy setting turns off the Security Settings Check feature, which checks Internet Explorer security settings to determine when the settings put Internet Explorer at risk. If you enable this policy setting, the feature is turned off. If you disable or do not configure this policy setting, the feature is turned on.		
59	DisablePopupFilterLevel (Prevent changing pop-up filter level)	N/A	N/A
	This policy setting prevents the user from changing the level of pop-up filtering. The available levels are as follows: High: Block all pop-ups. Medium: Block most automatic pop-ups. Low: Allow pop-ups from secure sites. If you enable this policy setting, the user cannot change the filter level. You can specify the filter level by importing Privacy settings from your computer under Internet Explorer Maintenance. If you disable or do not configure this policy setting, the user can manage pop-ups by changing the filter level. You may also want to enable the Prevent managing pop-up exception list and Turn off pop-up management policy settings to prevent the user from configuring pop-up behavior.		

60	DisableFlashInIE (Turn off Adobe Flash in Internet Explorer and prevent applications from using Internet Explorer technology to instantiate Flash objects)	N/A	N/A
	This policy setting turns off Adobe Flash in Internet Explorer and prevents applications from using Internet Explorer technology to instantiate Flash objects. If you enable this policy setting, Flash is turned off for Internet Explorer, and applications cannot use Internet Explorer technology to instantiate Flash objects. In the Manage Add-ons dialog box, the Flash status will be Disabled, and users cannot enable Flash. If you enable this policy setting, Internet Explorer will ignore settings made for Adobe Flash through the Add-on List and Deny all add-ons unless specifically allowed in the Add-on List policy settings. If you disable, or do not configure this policy setting, Flash is turned on for Internet Explorer, and applications can use Internet Explorer technology to instantiate Flash objects. Users can enable or disable Flash in the Manage Add-ons dialog box. Note that Adobe Flash can still be disabled through the Add-on List and Deny all add-ons unless specifically allowed in the Add-on List policy settings, even if this policy setting is disabled, or not configured. However, if Adobe Flash is disabled through the Add-on List and Deny all add-ons unless specifically allowed in the Add-on List policy settings and not through this policy setting, all applications that use Internet Explorer technology to instantiate Flash object can still do so. For more information, see Group Policy Settings in Internet Explorer 10 in the Internet Explorer TechNet library.		
61	AddonManagement_-IgnoreAddonApproval-Status (Automatically activate newly installed add-ons)	Similar semantics can be achieved by modifying multiple settings	Similar semantics can be achieved by modifying multiple entries in about:config
	This policy setting allows you to configure whether newly installed add-ons are automatically activated in the Internet Explorer 9 browser. Any add-ons that were activated in a previous version of Internet Explorer are considered to be the same as newly installed add-ons and are not activated when the user upgrades to Internet Explorer 9. In Internet Explorer 9, add-ons are defined as toolbars, Browser Helper Objects, or Explorer bars. ActiveX controls are referred to as plug-ins and are not part of this definition. If you enable this policy setting, newly installed add-ons are automatically activated in the browser. If you disable or do not configure this policy setting, newly installed add-ons are not automatically activated in the browser. Internet Explorer notifies the user when newly installed add-ons are ready for use. The user must choose to activate them by responding to the notification, using Manage Add-ons, or using other methods.		
62	TurnOnActiveXFiltering (Turn on ActiveX Filtering)	N/A	N/A
	This policy setting controls the ActiveX Filtering feature for websites that are running ActiveX controls. The user can choose to turn off ActiveX Filtering for specific websites so that ActiveX controls can run properly. If you enable this policy setting, ActiveX Filtering is enabled by default for the user. The user cannot turn off ActiveX Filtering, although they may add per-site exceptions. If you disable or do not configure this policy setting, ActiveX Filtering is not enabled by default for the user. The user can turn ActiveX Filtering on or off.		

63	NoDelBrowsingHistory (Prevent access to Delete Browsing History)	`Similar semantics can be achieved by modifying multiple settings`	`Similar semantics can be achieved by modifying multiple entries in about:config`
	This policy setting prevents the user from performing actions which will delete browsing history. For more information on browsing history Group Policy settings, see Group Policies Settings in Internet Explorer 10 in the TechNet technical library. If you enable this policy setting, the user cannot access the Delete Browsing History dialog box. Starting with Windows 8, users cannot click the Delete Browsing History button on the Settings charm. If you disable or do not configure this policy setting, the user can access the Delete Browsing History dialog box. Starting with Windows 8, users can click the Delete Browsing History button on the Settings charm.		
64	NoDelForms (Prevent deleting form data)	`N/A`	`N/A`
	This policy setting prevents the user from deleting form data. This feature is available in the Delete Browsing History dialog box. If you enable this policy setting, form data is preserved when the user clicks Delete. If you disable this policy setting, form data is deleted when the user clicks Delete. If you do not configure this policy setting, the user can choose whether to delete or preserve form data when he or she clicks Delete. If the Prevent access to Delete Browsing History policy setting is enabled, this policy setting is enabled by default.		
65	NoDelPasswords (Prevent deleting passwords)	`Similar semantics can be achieved by modifying multiple settings`	`N/A`
	This policy setting prevents users from deleting passwords. This feature is available in the Delete Browsing History dialog box. If you enable this policy setting, passwords are preserved when the user clicks Delete. If you disable this policy setting, passwords are deleted when the user clicks Delete. If you do not configure this policy setting, the user can choose whether to delete or preserve passwords when he or she clicks Delete. If the Prevent access to Delete Browsing History policy setting is enabled, this policy setting is enabled by default.		
66	DBHDisableDeleteCookies (Prevent deleting cookies)	`N/A`	`N/A`
	This policy setting prevents the user from deleting cookies. This feature is available in the Delete Browsing History dialog box. If you enable this policy setting, cookies are preserved when the user clicks Delete. If you disable this policy setting, cookies are deleted when the user clicks Delete. If you do not configure this policy setting, the user can choose whether to delete or preserve cookies when he or she clicks Delete. If the Prevent access to Delete Browsing History policy setting is enabled, this policy setting is enabled by default.		

67	DBHDisableDeleteHistory (Prevent deleting websites that the user has visited)	N/A	N/A
	This policy setting prevents the user from deleting the history of websites that he or she has visited. This feature is available in the Delete Browsing History dialog box. If you enable this policy setting, websites that the user has visited are preserved when he or she clicks Delete. If you disable this policy setting, websites that the user has visited are deleted when he or she clicks Delete. If you do not configure this policy setting, the user can choose whether to delete or preserve visited websites when he or she clicks Delete. If the Prevent access to Delete Browsing History policy setting is enabled, this policy setting is enabled by default.		
68	DBHDisableDeleteDownloadHistory (Prevent deleting download history)	N/A	N/A
	This policy setting prevents the user from deleting his or her download history. This feature is available in the Delete Browsing History dialog box. If you enable this policy setting, download history is preserved when the user clicks Delete. If you disable this policy setting, download history is deleted when the user clicks Delete. If you do not configure this policy setting, the user can choose whether to delete or preserve download history when he or she clicks Delete. If the Prevent access to Delete Browsing History policy setting is enabled, this policy setting is enabled by default.		
69	DBHDisableDeleteTIF (Prevent deleting temporary Internet files)	Similar semantics can be achieved by modifying multiple settings	Similar semantics can be achieved by modifying multiple entries in about:config
	This policy setting prevents the user from deleting temporary Internet files. This feature is available in the Delete Browsing History dialog box. If you enable this policy setting, temporary Internet files are preserved when the user clicks Delete. If you disable this policy setting, temporary Internet files are deleted when the user clicks Delete. If you do not configure this policy setting, the user can choose whether to delete or preserve temporary Internet files when he or she clicks Delete. If the Prevent access to Delete Browsing History policy setting is enabled, this policy setting is enabled by default.		
70	DBHDisableDeleteInPrivateDataV8 (Prevent deleting InPrivate Filtering data)	N/A	N/A
	This policy setting prevents the user from deleting InPrivate Filtering data. Internet Explorer collects InPrivate Filtering data during browser sessions other than InPrivate Browsing sessions to determine which third-party items should be blocked when InPrivate Filtering is enabled. This feature is available in the Delete Browsing History dialog box. If you enable this policy setting, InPrivate Filtering data is preserved when the user clicks Delete. If you disable this policy setting, InPrivate Filtering data is deleted when the user clicks Delete. If you do not configure this policy setting, the user can choose whether to delete or preserve InPrivate Filtering data when he or she clicks Delete.		

71	DBHDisableDeleteInPrivateDataV9 (Prevent deleting ActiveX Filtering and Tracking Protection data)	N/A	N/A
	This policy setting prevents the user from deleting ActiveX Filtering and Tracking Protection data. This data is the list of websites on which the user has chosen to disable ActiveX Filtering or Tracking Protection. Additionally, Tracking Protection data is collected when the Personalized Tracking Protection List is enabled to determine which third-party items should be blocked while the user is browsing. This feature is available in the Delete Browsing History dialog box. If you enable this policy setting, ActiveX Filtering and Tracking Protection data is preserved when the user clicks Delete. If you disable this policy setting, ActiveX Filtering and Tracking Protection data is deleted when the user clicks Delete. If you do not configure this policy setting, the user can choose whether to delete or preserve ActiveX Filtering and Tracking Protection data when he or she clicks Delete.		
72	DBHDisableKeepFavorites (Prevent deleting favorites site data)	N/A	N/A
	This policy setting prevents the user from deleting favorites site data. This feature is available in the Delete Browsing History dialog box. If you enable this policy setting, favorites site data is preserved when the user clicks Delete. If you disable this policy setting, favorites site data is deleted when the user clicks Delete. If you do not configure this policy setting, the user can choose whether to delete or preserve favorites site data when he or she clicks Delete. If the Prevent access to Delete Browsing History policy setting is enabled, this policy setting has no effect.		
73	DBHDisableDeleteOnExit (Allow deleting browsing history on exit)	N/A	N/A
	This policy setting allows the automatic deletion of specified items when the last browser window closes. The preferences selected in the Delete Browsing History dialog box (such as deleting temporary Internet files, cookies, history, form data, and passwords) are applied, and those items are deleted. If you enable this policy setting, deleting browsing history on exit is turned on. If you disable this policy setting, deleting browsing history on exit is turned off. If you do not configure this policy setting, it can be configured on the General tab in Internet Options. If the Prevent access to Delete Browsing History policy setting is enabled, this policy setting has no effect.		
74	NoJITSetup (Disable Automatic Install of Internet Explorer components)	N/A	N/A
	Prevents Internet Explorer from automatically installing components. If you enable this policy, it prevents Internet Explorer from downloading a component when users browse to a Web site that needs that component. If you disable this policy or do not configure it, users will be prompted to download and install a component when visiting a Web site that uses that component. This policy is intended to help the administrator control which components the user installs.		

75	NoUpdateCheck (Disable Periodic Check for Internet Explorer software updates)	N/A	N/A
	Prevents Internet Explorer from checking whether a new version of the browser is available. If you enable this policy, it prevents Internet Explorer from checking to see whether it is the latest available browser version and notifying users if a new version is available. If you disable this policy or do not configure it, Internet Explorer checks every 30 days by default, and then notifies users if a new version is available. This policy is intended to help the administrator maintain version control for Internet Explorer by preventing users from being notified about new versions of the browser.		
76	PopupBlocker_AllowList (Pop-up allow list)	Similar semantics can be achieved by modifying multiple settings	Similar semantics can be achieved by using different third party Add-ons.
	This policy setting allows you to specify a list of web sites that will be allowed to open pop-up windows regardless of the Internet Explorer processs Pop-Up Blocker settings. If you enable this policy setting, you can enter a list of sites which will be allowed to open pop-up windows regardless of user settings. Only the domain name is allowed, so www.contoso.com is valid, but not http://www.contoso.com. Wildcards are allowed, so *.contoso.com is also valid. If you disable this or do not configure this policy setting, you will not be able to provide a default Pop-up Blocker exception list. Note: You can disable users from adding or removing websites to the exception list by enabling Turn off Managing Pop-up Allow list policy.		
77	RestrictAutoconfig (Disable changing Automatic Configuration settings)	N/A	N/A
	This setting specifies to automatically detect the proxy server settings used to connect to the Internet and customize Internet Explorer. This setting specifies that Internet explorer use the configuration settings provided in a file by the system administrator. If you enable this policy setting, the user will not be able to do automatic configuration. You can import your current connection settings from your machine using Internet Explorer Maintenance under Admin Templates using group policy editor. If you disable or do no configure this policy setting, the user will have the freedom to automatically configure these settings.		
78	RestrictConnectionSettings_2 (Disable changing connection settings)	N/A	N/A
	Prevents users from changing dial-up settings. If you enable this policy, the Settings button on the Connections tab in the Internet Options dialog box appears dimmed. If you disable this policy or do not configure it, users can change their settings for dial-up connections. If you set the Disable the Connections page policy (located in /User Configuration/Administrative Templates/Windows Components/Internet Explorer/Internet Control Panel), you do not need to set this policy, because the Disable the Connections page policy removes the Connections tab from the interface.		

79	RestrictHistory (Disable Configuring History)	N/A	N/A
	This setting specifies the number of days that Internet Explorer tracks views of pages in the History List. To access the Temporary Internet Files and History Settings dialog box, from the Menu bar, on the Tools menu, click Internet Options, click the General tab, and then click Settings under Browsing history. If you enable this policy setting, a user cannot set the number of days that Internet Explorer tracks views of the pages in the History List. You must specify the number of days that Internet Explorer tracks views of pages in the History List. Users can not delete browsing history. If you disable or do not configure this policy setting, a user can set the number of days that Internet Explorer tracks views of pages in the History list. Users can delete browsing history.		
80	RestrictPopupException-List (Prevent managing pop-up exception list)	N/A	N/A
	You can allow pop-ups from specific websites by adding the sites to the exception list. If you enable this policy setting, the user cannot add websites to or remove websites from the exception list. If you disable or do not configure this policy setting, the user can add websites to or remove websites from the exception list. Note: You can allow a default list of sites that can open pop-up windows regardless of the Internet Explorer processs Pop-Up Blocker settings by enabling the Specify pop-up allow list policy setting.		
81	RestrictPopupManage-ment (Turn off pop-up management)	N/A	N/A
	This policy setting allows you to manage pop-up management functionality in Internet Explorer. If you enable this policy setting, the Control Panel information relating to pop-up management will be unavailable (grayed out) and all other pop-up manager controls, notifications, and dialog boxes will not appear. Pop-up windows will continue to function as they did in Windows XP Service Pack 1 or earlier, although windows launched off screen will continue to be re-positioned onscreen. If you disable or do not configure this policy setting, the popup management feature will be functional.		
82	RestrictProxy (Prevent changing proxy settings)	N/A	N/A
	This policy setting specifies if a user can change proxy settings. If you enable this policy setting, the user will not be able to configure proxy settings. If you disable or do not configure this policy setting, the user can configure proxy settings.		
83	RestrictSettings (Prevent the deletion of temporary Internet files and cookies)	N/A	N/A
	This policy setting is used to manage temporary Internet files and cookies associated with your Internet browsing history, available by clicking Tools, Internet Options, and then Delete Browsing History in Internet Explorer. If you enable this policy setting, users will not be able to delete temporary Internet files and cookies. If you disable or do not configure this policy setting, users will be able to delete temporary Internet files and cookies.		

84	Security_HKLM_only (Security Zones: Use only machine settings)	N/A	N/A
	Applies security zone information to all users of the same computer. A security zone is a group of Web sites with the same security level. If you enable this policy, changes that the user makes to a security zone will apply to all users of that computer. If you disable this policy or do not configure it, users of the same computer can establish their own security zone settings. This policy is intended to ensure that security zone settings apply uniformly to the same computer and do not vary from user to user. Also, see the Security zones: Do not allow users to change policies policy.		
85	Security_options_edit (Security Zones: Do not allow users to change policies)	N/A	N/A
	Prevents users from changing security zone settings. A security zone is a group of Web sites with the same security level. If you enable this policy, the Custom Level button and security-level slider on the Security tab in the Internet Options dialog box are disabled. If you disable this policy or do not configure it, users can change the settings for security zones. This policy prevents users from changing security zone settings established by the administrator. Note: The Disable the Security page policy (located in /User Configuration/Administrative Templates/Windows Components/Internet Explorer/Internet Control Panel), which removes the Security tab from Internet Explorer in Control Panel, takes precedence over this policy. If it is enabled, this policy is ignored. Also, see the Security zones: Use only machine settings policy.		
86	Security_zones_map_-edit (Security Zones: Do not allow users to add/delete sites)	N/A	N/A
	Prevents users from adding or removing sites from security zones. A security zone is a group of Web sites with the same security level. If you enable this policy, the site management settings for security zones are disabled. (To see the site management settings for security zones, in the Internet Options dialog box, click the Security tab, and then click the Sites button.) If you disable this policy or do not configure it, users can add Web sites to or remove sites from the Trusted Sites and Restricted Sites zones, and alter settings for the Local Intranet zone. This policy prevents users from changing site management settings for security zones established by the administrator. Note: The Disable the Security page policy (located in /User Configuration/Administrative Templates/Windows Components/Internet Explorer/Internet Control Panel), which removes the Security tab from the interface, takes precedence over this policy. If it is enabled, this policy is ignored. Also, see the Security zones: Use only machine settings policy.		

87	ShellNotifications (Disable software update shell notifications on program launch)	N/A	N/A
	Specifies that programs using the Microsoft Software Distribution Channel will not notify users when they install new components. The Software Distribution Channel is a means of updating software dynamically on users computers by using Open Software Distribution (.osd) technologies. If you enable this policy, users will not be notified if their programs are updated using Software Distribution Channels. If you disable this policy or do not configure it, users will be notified before their programs are updated. This policy is intended for administrators who want to use Software Distribution Channels to update their users programs without user intervention.		
88	UserProxy (Make proxy settings per-machine (rather than per-user))	N/A	N/A
	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 policy or do not configure it, users of the same computer can establish their own proxy settings. This policy is intended to ensure that proxy settings apply uniformly to the same computer and do not vary from user to user.		
89	IZ_Policy_-AllowScriptlets_-1, IZ_Policy_-AllowScriptlets_-2, IZ_Policy_-AllowScriptlets_-3, IZ_Policy_-AllowScriptlets_-4, IZ_Policy_-AllowScriptlets_-5, IZ_Policy_-AllowScriptlets_-6, IZ_Policy_-AllowScriptlets_-7, IZ_Policy_-AllowScriptlets_-8, IZ_Policy_-AllowScriptlets_-9, IZ_Policy_-AllowScriptlets_10 (Allow scriptlets)	N/A	N/A
	This policy setting allows you to manage whether the user can run scriptlets. If you enable this policy setting, the user can run scriptlets. If you disable this policy setting, the user cannot run scriptlets. If you do not configure this policy setting, the user can enable or disable scriptlets.		

90	IZ_Policy_Phishing_1, IZ_Policy_Phishing_2, IZ_Policy_Phishing_3, IZ_Policy_Phishing_4, IZ_Policy_Phishing_5, IZ_Policy_Phishing_6, IZ_Policy_Phishing_7, IZ_Policy_Phishing_8, IZ_Policy_Phishing_9, IZ_Policy_Phishing_10 (Turn on SmartScreen Filter scan)	N/A	N/A
	This policy setting controls whether SmartScreen Filter scans pages in this zone for malicious content. If you enable this policy setting, SmartScreen Filter scans pages in this zone for malicious content. If you disable this policy setting, SmartScreen Filter does not scan pages in this zone for malicious content. If you do not configure this policy setting, the user can choose whether SmartScreen Filter scans pages in this zone for malicious content. Note: In Internet Explorer 7, this policy setting controls whether Phishing Filter scans pages in this zone for malicious content.		
91	IZ_Policy_-ScriptPrompt_1, IZ_-Policy_ScriptPrompt_-2, IZ_Policy_-ScriptPrompt_3, IZ_-Policy_ScriptPrompt_-4, IZ_Policy_-ScriptPrompt_5, IZ_-Policy_ScriptPrompt_-6, IZ_Policy_-ScriptPrompt_7, IZ_-Policy_ScriptPrompt_-8, IZ_Policy_-ScriptPrompt_9, IZ_-Policy_ScriptPrompt_10 (Allow websites to prompt for information by using scripted windows)	N/A	N/A
	This policy setting determines whether scripted windows are automatically displayed. If you enable this policy setting, scripted windows are displayed. If you disable this policy setting, the user must choose to display any scripted windows by using the Notification bar. If you do not configure this policy setting, the user can enable or disable the Notification bar behavior.		

92	IZ_Policy_-ScriptStatusBar_-1, IZ_Policy_-ScriptStatusBar_-2, IZ_Policy_-ScriptStatusBar_-3, IZ_Policy_-ScriptStatusBar_-4, IZ_Policy_-ScriptStatusBar_-5, IZ_Policy_-ScriptStatusBar_-6, IZ_Policy_-ScriptStatusBar_-7, IZ_Policy_-ScriptStatusBar_-8, IZ_Policy_-ScriptStatusBar_-9, IZ_Policy_-ScriptStatusBar_10 (Allow updates to status bar via script)	N/A	N/A
	This policy setting allows you to manage whether script is allowed to update the status bar within the zone. If you enable this policy setting, script is allowed to update the status bar. If you disable or do not configure this policy setting, script is not allowed to update the status bar.		
93	IZ_Policy_-TurnOnProtectedMode_-1, IZ_Policy_-TurnOnProtectedMode_-2, IZ_Policy_-TurnOnProtectedMode_-3, IZ_Policy_-TurnOnProtectedMode_-4, IZ_Policy_-TurnOnProtectedMode_-5, IZ_Policy_-TurnOnProtectedMode_-6, IZ_Policy_-TurnOnProtectedMode_-7, IZ_Policy_-TurnOnProtectedMode_-8, IZ_Policy_-TurnOnProtectedMode_-9, IZ_Policy_-TurnOnProtectedMode_10 (Turn on Protected Mode)	Similar semantics can be achieved by modifying multiple settings	N/A
	This policy setting allows you to turn on Protected Mode. Protected Mode helps protect Internet Explorer from exploited vulnerabilities by reducing the locations that Internet Explorer can write to in the registry and the file system. If you enable this policy setting, Protected Mode is turned on. The user cannot turn off Protected Mode. If you disable this policy setting, Protected Mode is turned off. The user cannot turn on Protected Mode. If you do not configure this policy setting, the user can turn on or turn off Protected Mode.		

94	IZ_Policy_-UnsafeFiles_1, IZ_-Policy_UnsafeFiles_-2, IZ_Policy_-UnsafeFiles_3, IZ_-Policy_UnsafeFiles_-4, IZ_Policy_-UnsafeFiles_5, IZ_-Policy_UnsafeFiles_-6, IZ_Policy_-UnsafeFiles_7, IZ_-Policy_UnsafeFiles_-8, IZ_Policy_-UnsafeFiles_9, IZ_-Policy_UnsafeFiles_10 (Show security warning for potentially unsafe files)	N/A	N/A
	This policy setting controls whether or not the Open File - Security Warning message appears when the user tries to open executable files or other potentially unsafe files (from an intranet file share by using File Explorer, for example). If you enable this policy setting and set the drop-down box to Enable, these files open without a security warning. If you set the drop-down box to Prompt, a security warning appears before the files open. If you disable this policy setting, these files do not open. If you do not configure this policy setting, the user can configure how the computer handles these files. By default, these files are blocked in the Restricted zone, enabled in the Intranet and Local Computer zones, and set to prompt in the Internet and Trusted zones.		

95	IZ_Policy_-WebBrowserApps_-1, IZ_Policy_-WebBrowserApps_-2, IZ_Policy_-WebBrowserApps_-3, IZ_Policy_-WebBrowserApps_-4, IZ_Policy_-WebBrowserApps_-5, IZ_Policy_-WebBrowserApps_-6, IZ_Policy_-WebBrowserApps_-7, IZ_Policy_-WebBrowserApps_-8, IZ_Policy_-WebBrowserApps_-9, IZ_Policy_-WebBrowserApps_10 (Allow loading of XAML Browser Applications)	N/A	N/A
	This policy setting allows you to manage the loading of XAML Browser Applications (XBAPs). These are browser-hosted, ClickOnce-deployed applications built via WinFX. These applications run in a security sandbox and take advantage of the Windows Presentation Foundation platform for the web. If you enable this policy setting and set the drop-down box to Enable, XBAPs are automatically loaded inside Internet Explorer. The user cannot change this behavior. If you set the drop-down box to Prompt, the user is prompted for loading XBAPs. If you disable this policy setting, XBAPs are not loaded inside Internet Explorer. The user cannot change this behavior. If you do not configure this policy setting, the user can decide whether to load XBAPs inside Internet Explorer.		

96	IZ_Policy_-WebBrowserControl_-1, IZ_Policy_-WebBrowserControl_-2, IZ_Policy_-WebBrowserControl_-3, IZ_Policy_-WebBrowserControl_-4, IZ_Policy_-WebBrowserControl_-5, IZ_Policy_-WebBrowserControl_-6, IZ_Policy_-WebBrowserControl_-7, IZ_Policy_-WebBrowserControl_-8, IZ_Policy_-WebBrowserControl_-9, IZ_Policy_-WebBrowserControl_10 (Allow scripting of Internet Explorer WebBrowser controls)	N/A	N/A
	This policy setting determines whether a page can control embedded WebBrowser controls via script. If you enable this policy setting, script access to the WebBrowser control is allowed. If you disable this policy setting, script access to the WebBrowser control is not allowed. If you do not configure this policy setting, the user can enable or disable script access to the WebBrowser control. By default, script access to the WebBrowser control is allowed only in the Local Machine and Intranet zones.		

97	IZ_Policy_-WinFXRuntimeComponent_-1, IZ_Policy_-WinFXRuntimeComponent_-2, IZ_Policy_-WinFXRuntimeComponent_-3, IZ_Policy_-WinFXRuntimeComponent_-4, IZ_Policy_-WinFXRuntimeComponent_-5, IZ_Policy_-WinFXRuntimeComponent_-6, IZ_Policy_-WinFXRuntimeComponent_-7, IZ_Policy_-WinFXRuntimeComponent_-8, IZ_Policy_-WinFXRuntimeComponent_-9, IZ_Policy_-WinFXRuntimeComponent_-10 (Turn off .NET Framework Setup)	N/A	N/A
	This policy setting prevents the users computer from starting Microsoft .NET Framework Setup when the user is browsing to .NET Framework content in Internet Explorer. The .NET Framework is the next-generation platform for Windows. It uses the common language runtime and incorporates support from multiple developer tools. It includes the new managed code APIs for Windows. If you enable this policy setting, .NET Framework Setup is turned off. The user cannot change this behavior. If you disable this policy setting, .NET Framework Setup is turned on. The user cannot change this behavior. If you do not configure this policy setting, .NET Framework Setup is turned on by default. The user can change this behavior.		

98	IZ_PolicyAccessData-SourcesAcrossDomains_-1, IZ_-PolicyAccessData-SourcesAcrossDomains_-2, IZ_-PolicyAccessData-SourcesAcrossDomains_-3, IZ_-PolicyAccessData-SourcesAcrossDomains_-4, IZ_-PolicyAccessData-SourcesAcrossDomains_-5, IZ_-PolicyAccessData-SourcesAcrossDomains_-6, IZ_-PolicyAccessData-SourcesAcrossDomains_-7, IZ_-PolicyAccessData-SourcesAcrossDomains_-8, IZ_-PolicyAccessData-SourcesAcrossDomains_-9, IZ_-PolicyAccessData-SourcesAcrossDomains_-10 (Access data sources across domains)	N/A	N/A
	This policy setting allows you to manage whether Internet Explorer can access data from another security zone using the Microsoft XML Parser (MSXML) or ActiveX Data Objects (ADO). If you enable this policy setting, users can load a page in the zone that uses MSXML or ADO to access data from another site in the zone. If you select Prompt in the drop-down box, users are queried to choose whether to allow a page to be loaded in the zone that uses MSXML or ADO to access data from another site in the zone. If you disable this policy setting, users cannot load a page in the zone that uses MSXML or ADO to access data from another site in the zone. If you do not configure this policy setting, users cannot load a page in the zone that uses MSXML or ADO to access data from another site in the zone.		

99	IZ_PolicyOnlyAllow-ApprovedDomainsToUse-ActiveXWithoutPrompt_-Both_LocalMachine, IZ_PolicyOnlyAllow-ApprovedDomainsToUse-ActiveXWithoutPrompt_-Both_Intranet, IZ_-PolicyOnlyAllow-ApprovedDomainsToUse-ActiveXWithoutPrompt_-Both_Trusted, IZ_-PolicyOnlyAllow-ApprovedDomainsToUse-ActiveXWithoutPrompt_-Both_Internet, IZ_-PolicyOnlyAllow-ApprovedDomainsToUse-ActiveXWithoutPrompt_-Both_Restricted, IZ_PolicyOnlyAllow-ApprovedDomainsToUse-ActiveXWithoutPrompt_-Both_-LocalMachineLockdown, IZ_PolicyOnlyAllow-ApprovedDomainsToUse-ActiveXWithoutPrompt_-Both_IntranetLockdown, IZ_PolicyOnlyAllow-ApprovedDomainsToUse-ActiveXWithoutPrompt_-Both_TrustedLockdown, IZ_PolicyOnlyAllow-ApprovedDomainsToUse-ActiveXWithoutPrompt_-Both_InternetLockdown, IZ_PolicyOnlyAllow-ApprovedDomainsToUse-ActiveXWithoutPrompt_-Both_-RestrictedLockdown (Allow only approved domains to use ActiveX controls without prompt)	N/A	N/A
	This policy setting controls whether or not the user is prompted to allow ActiveX controls to run on websites other than the website that installed the ActiveX control. If you enable this policy setting, the user is prompted before ActiveX controls can run from websites in this zone. The user can choose to allow the control to run from the current site or from all sites. If you disable this policy setting, the user does not see the per-site ActiveX prompt, and ActiveX controls can run from all sites in this zone.		

100	IZ_PolicyAllow-METAREFRESH_1, IZ_PolicyAllow-METAREFRESH_2, IZ_PolicyAllow-METAREFRESH_3, IZ_PolicyAllow-METAREFRESH_4, IZ_PolicyAllow-METAREFRESH_5, IZ_PolicyAllow-METAREFRESH_6, IZ_PolicyAllow-METAREFRESH_7, IZ_PolicyAllow-METAREFRESH_8, IZ_PolicyAllow-METAREFRESH_9, IZ_PolicyAllow-METAREFRESH_10 (Allow META REFRESH)	N/A	N/A
	This policy setting allows you to manage whether a users browser can be redirected to another Web page if the author of the Web page uses the Meta Refresh setting (tag) to redirect browsers to another Web page. If you enable this policy setting, a users browser that loads a page containing an active Meta Refresh setting can be redirected to another Web page. If you disable this policy setting, a users browser that loads a page containing an active Meta Refresh setting cannot be redirected to another Web page. If you do not configure this policy setting, a users browser that loads a page containing an active Meta Refresh setting can be redirected to another Web page.		

101	IZ_-PolicyAllowPasteViaScript_1, IZ_-PolicyAllowPasteViaScript_2, IZ_-PolicyAllowPasteViaScript_3, IZ_-PolicyAllowPasteViaScript_4, IZ_-PolicyAllowPasteViaScript_5, IZ_-PolicyAllowPasteViaScript_6, IZ_-PolicyAllowPasteViaScript_7, IZ_-PolicyAllowPasteViaScript_8, IZ_-PolicyAllowPasteViaScript_9, IZ_-PolicyAllowPasteViaScript_10 (Allow cut, copy or paste operations from the clipboard via script)	N/A	N/A
	This policy setting allows you to manage whether scripts can perform a clipboard operation (for example, cut, copy, and paste) in a specified region. If you enable this policy setting, a script can perform a clipboard operation. If you select Prompt in the drop-down box, users are queried as to whether to perform clipboard operations. If you disable this policy setting, a script cannot perform a clipboard operation. If you do not configure this policy setting, a script can perform a clipboard operation.		

102	IZ_PolicyDisplayMixed-Content_1, IZ_-PolicyDisplayMixed-Content_2, IZ_-PolicyDisplayMixed-Content_3, IZ_-PolicyDisplayMixed-Content_4, IZ_-PolicyDisplayMixed-Content_5, IZ_-PolicyDisplayMixed-Content_6, IZ_-PolicyDisplayMixed-Content_7, IZ_-PolicyDisplayMixed-Content_8, IZ_-PolicyDisplayMixed-Content_9, IZ_-PolicyDisplayMixed-Content_10 (Display mixed content)	N/A	N/A
	This policy setting allows you to manage whether users can display nonsecure items and manage whether users receive a security information message to display pages containing both secure and nonsecure items. If you enable this policy setting, and the drop-down box is set to Enable, the user does not receive a security information message (This page contains both secure and nonsecure items. Do you want to display the nonsecure items?) and nonsecure content can be displayed. If the drop-down box is set to Prompt, the user will receive the security information message on the Web pages that contain both secure (https://) and nonsecure (http://) content. If you disable this policy setting, users cannot receive the security information message and nonsecure content cannot be displayed. If you do not configure this policy setting, the user will receive the security information message on the Web pages that contain both secure (https://) and nonsecure (http://) content.		

103	IZ_-PolicyDownloadSigned-ActiveX_1, IZ_-PolicyDownloadSigned-ActiveX_2, IZ_-PolicyDownloadSigned-ActiveX_3, IZ_-PolicyDownloadSigned-ActiveX_4, IZ_-PolicyDownloadSigned-ActiveX_5, IZ_-PolicyDownloadSigned-ActiveX_6, IZ_-PolicyDownloadSigned-ActiveX_7, IZ_-PolicyDownloadSigned-ActiveX_8, IZ_-PolicyDownloadSigned-ActiveX_9, IZ_-PolicyDownloadSigned-ActiveX_10 (Download signed ActiveX controls)	N/A	N/A
	This policy setting allows you to manage whether users may download signed ActiveX controls from a page in the zone. If you enable this policy, users can download signed controls without user intervention. If you select Prompt in the drop-down box, users are queried whether to download controls signed by publishers who arent trusted. Code signed by trusted publishers is silently downloaded. If you disable the policy setting, signed controls cannot be downloaded. If you do not configure this policy setting, users are queried whether to download controls signed by publishers who arent trusted. Code signed by trusted publishers is silently downloaded.		

104	IZ_-PolicyDownloadUnsigned-ActiveX_1, IZ_-PolicyDownloadUnsigned-ActiveX_2, IZ_-PolicyDownloadUnsigned-ActiveX_3, IZ_-PolicyDownloadUnsigned-ActiveX_4, IZ_-PolicyDownloadUnsigned-ActiveX_5, IZ_-PolicyDownloadUnsigned-ActiveX_6, IZ_-PolicyDownloadUnsigned-ActiveX_7, IZ_-PolicyDownloadUnsigned-ActiveX_8, IZ_-PolicyDownloadUnsigned-ActiveX_9, IZ_-PolicyDownloadUnsigned-ActiveX_10 (Download unsigned ActiveX controls)	N/A	N/A
	This policy setting allows you to manage whether users may download unsigned ActiveX controls from the zone. Such code is potentially harmful, especially when coming from an untrusted zone. If you enable this policy setting, users can run unsigned controls without user intervention. If you select Prompt in the drop-down box, users are queried to choose whether to allow the unsigned control to run. If you disable this policy setting, users cannot run unsigned controls. If you do not configure this policy setting, users cannot run unsigned controls.		

105	IZ_PolicyRenderLegacy-Filters_1, IZ_-PolicyRenderLegacy-Filters_2, IZ_-PolicyRenderLegacy-Filters_3, IZ_-PolicyRenderLegacy-Filters_4, IZ_-PolicyRenderLegacy-Filters_5, IZ_-PolicyRenderLegacy-Filters_6, IZ_-PolicyRenderLegacy-Filters_7, IZ_-PolicyRenderLegacy-Filters_8, IZ_-PolicyRenderLegacy-Filters_9, IZ_-PolicyRenderLegacy-Filters_10 (Render legacy filters)	N/A	N/A
	This policy setting specifies whether Internet Explorer renders legacy visual filters in this zone. If you enable this policy setting, you can control whether or not Internet Explorer renders legacy filters by selecting Enable, or Disable, under Options in Group Policy Editor. If you disable, or do not configure this policy setting, users can choose whether or not to render filters in this zone. Users can change this setting on the Security tab of the Internet Options dialog box. Filters are not rendered by default in this zone.		

106	IZ_-PolicyJavaPermissions_-1, IZ_-PolicyJavaPermissions_-2, IZ_-PolicyJavaPermissions_-3, IZ_-PolicyJavaPermissions_-4, IZ_-PolicyJavaPermissions_-5, IZ_-PolicyJavaPermissions_-6, IZ_-PolicyJavaPermissions_-7, IZ_-PolicyJavaPermissions_-8, IZ_-PolicyJavaPermissions_-9, IZ_-PolicyJavaPermissions_-10 (Java permissions)	Similar semantics can be achieved by modifying multiple settings	Similar semantics can be achieved by using different third party Add-ons
	This policy setting allows you to manage permissions for Java applets. If you enable this policy setting, you can choose options from the drop-down box. Custom, to control 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), plus 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.		

107	IZ_-PolicyLaunchAppsAnd-FilesInIFRAME_1, IZ_-PolicyLaunchAppsAnd-FilesInIFRAME_2, IZ_-PolicyLaunchAppsAnd-FilesInIFRAME_3, IZ_-PolicyLaunchAppsAnd-FilesInIFRAME_4, IZ_-PolicyLaunchAppsAnd-FilesInIFRAME_5, IZ_-PolicyLaunchAppsAnd-FilesInIFRAME_6, IZ_-PolicyLaunchAppsAnd-FilesInIFRAME_7, IZ_-PolicyLaunchAppsAnd-FilesInIFRAME_8, IZ_-PolicyLaunchAppsAnd-FilesInIFRAME_9, IZ_-PolicyLaunchAppsAnd-FilesInIFRAME_10 (Launching applications and files in an IFRAME)	N/A	N/A
	This policy setting allows you to manage whether applications may be run and files may be downloaded from an IFRAME reference in the HTML of the pages in this zone. If you enable this policy setting, users can run applications and download files from IFRAMEs on the pages in this zone without user intervention. If you select Prompt in the drop-down box, users are queried to choose whether to run applications and download files from IFRAMEs on the pages in this zone. If you disable this policy setting, users are prevented from running applications and downloading files from IFRAMEs on the pages in this zone. If you do not configure this policy setting, users are queried to choose whether to run applications and download files from IFRAMEs on the pages in this zone.		

108	IZ_PolicyLogon_1, IZ_PolicyLogon_2, IZ_PolicyLogon_3, IZ_PolicyLogon_4, IZ_PolicyLogon_5, IZ_PolicyLogon_6, IZ_PolicyLogon_7, IZ_PolicyLogon_8, IZ_PolicyLogon_9, IZ_PolicyLogon_10 (Logon options)	Similar semantics can be achieved by modifying multiple settings	N/A
	This policy 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 users 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.		

109	IZ_-PolicyDragDropAcross-DomainsWithinWindow_-Both_Internet, IZ_-PolicyDragDropAcross-DomainsWithinWindow_-Both_-InternetLockdown, IZ_-PolicyDragDropAcross-DomainsWithinWindow_-Both_-IntranetLockdown, IZ_-PolicyDragDropAcross-DomainsWithinWindow_-Both_Trusted, IZ_-PolicyDragDropAcross-DomainsWithinWindow_-Both_TrustedLockdown (Enable dragging of content from different domains within a window)	N/A	N/A
	This policy setting allows you to set options for dragging content from one domain to a different domain when the source and destination are in the same window. If you enable this policy setting and click Enable, users can drag content from one domain to a different domain when the source and destination are in the same window. Users cannot change this setting. If you enable this policy setting and click Disable, users cannot drag content from one domain to a different domain when the source and destination are in the same window. Users cannot change this setting in the Internet Options dialog. In Internet Explorer 10, if you disable this policy setting or do not configure it, users cannot drag content from one domain to a different domain when the source and destination are in the same window. Users can change this setting in the Internet Options dialog. In Internet Explorer 9 and earlier versions, if you disable this policy setting or do not configure it, users can drag content from one domain to a different domain when the source and destination are in the same window. Users cannot change this setting in the Internet Options dialog.		

110	IZ_-PolicyDragDropAcross-DomainsAcrossWindows_-Both_Internet, IZ_-PolicyDragDropAcross-DomainsAcrossWindows_-Both_-InternetLockdown, IZ_-PolicyDragDropAcross-DomainsAcrossWindows_-Both_-IntranetLockdown, IZ_-PolicyDragDropAcross-DomainsAcrossWindows_-Both_Trusted, IZ_-PolicyDragDropAcross-DomainsAcrossWindows_-Both_TrustedLockdown (Enable dragging of content from different domains across windows)	N/A	N/A
	This policy setting allows you to set options for dragging content from one domain to a different domain when the source and destination are in different windows. If you enable this policy setting and click Enable, users can drag content from one domain to a different domain when the source and destination are in different windows. Users cannot change this setting. If you enable this policy setting and click Disable, users cannot drag content from one domain to a different domain when both the source and destination are in different windows. Users cannot change this setting. In Internet Explorer 10, if you disable this policy setting or do not configure it, users cannot drag content from one domain to a different domain when the source and destination are in different windows. Users can change this setting in the Internet Options dialog. In Internet Explorer 9 and earlier versions, if you disable this policy or do not configure it, users can drag content from one domain to a different domain when the source and destination are in different windows. Users cannot change this setting.		

111	IZ_PolicyNavigateSub-framesAcrossDomains_1, IZ_PolicyNavigateSub-framesAcrossDomains_2, IZ_PolicyNavigateSub-framesAcrossDomains_3, IZ_PolicyNavigateSub-framesAcrossDomains_4, IZ_PolicyNavigateSub-framesAcrossDomains_5, IZ_PolicyNavigateSub-framesAcrossDomains_6, IZ_PolicyNavigateSub-framesAcrossDomains_7, IZ_PolicyNavigateSub-framesAcrossDomains_8, IZ_PolicyNavigateSub-framesAcrossDomains_9, IZ_PolicyNavigateSub-framesAcrossDomains_10 (Navigate windows and frames across different domains)	N/A	N/A
	This policy setting allows you to manage the opening of windows and frames and access of applications across different domains. If you enable this policy setting, users can open windows and frames from othe domains and access applications from other domains. If you select Prompt in the drop-down box, users are queried whether to allow windows and frames to access applications from other domains. If you disable this policy setting, users cannot open windows and frames to access applications from different domains. If you do not configure this policy setting, users can open windows and frames from othe domains and access applications from other domains.		
112	IZ_-PolicyNetworkProtocol-Lockdown_1, IZ_-PolicyNetworkProtocol-Lockdown_2, IZ_-PolicyNetworkProtocol-Lockdown_3, IZ_-PolicyNetworkProtocol-Lockdown_5 (Allow active content over restricted protocols to access my computer)	N/A	N/A
	This policy setting allows you to manage whether a resource hosted on an admin-restricted protocol in the Intranet Zone can run active content such as script, ActiveX, Java and Binary Behaviors. The list of restricted protocols may be set in the Intranet Zone Restricted Protocols section under Network Protocol Lockdown policy. If you enable this policy setting, no Intranet Zone content accessed is affected, even for protocols on the restricted list. If you select Prompt from the drop-down box, the Notification bar will appear to allow control over questionable content accessed over any restricted protocols; content over other protocols is unaffected. If you disable this policy setting, all attempts to access such content over the restricted protocols is blocked. If you do not configure this policy setting, the Notification bar will appear to allow control over questionable content accessed over any restricted protocols when the Network Protocol Lockdown security feature is enabled.		

113	IZ_-PolicyNoPromptForOne-OrNoClientCertificate_-1, IZ_-PolicyNoPromptForOne-OrNoClientCertificate_-4, IZ_-PolicyNoPromptForOne-OrNoClientCertificate_-6, IZ_-PolicyNoPromptForOne-OrNoClientCertificate_-7,IZ_-PolicyNoPromptForOne-OrNoClientCertificate_-8, IZ_-PolicyNoPromptForOne-OrNoClientCertificate_-10 (Do not prompt for client certificate selection when no certificates or only one certificate exists.)	N/A	N/A
	This policy setting allows you to manage whether users are prompted to select a certificate when no certificate or only one certificate exists. If you enable this policy setting, Internet Explorer does not prompt users with a Client Authentication message when they connect to a Web site that has no certificate or only one certificate. If you disable this policy setting, Internet Explorer prompts users with a Client Authentication message when they connect to a Web site that has no certificate or only one certificate. If you do not configure this policy setting, Internet Explorer prompts users with a Client Authentication message when they connect to a Web site that has no certificate or only one certificate.		
114	IZ_-PolicyScriptActiveX-MarkedSafe_1, IZ_-PolicyScriptActiveX-MarkedSafe_2, IZ_-PolicyScriptActiveX-MarkedSafe_3, IZ_-PolicyScriptActiveX-MarkedSafe_4, IZ_-PolicyScriptActiveX-MarkedSafe_5, IZ_-PolicyScriptActiveX-MarkedSafe_6, IZ_-PolicyScriptActiveX-MarkedSafe_9, IZ_-PolicyScriptActiveX-MarkedSafe_10 (Script ActiveX controls marked safe for scripting)	N/A	N/A
	This policy setting allows you to manage whether an ActiveX control marked safe for scripting can interact with a script. If you enable this policy setting, script interaction can occur automatically without user intervention. If you select Prompt in the drop-down box, users are queried to choose whether to allow script interaction. If you disable this policy setting, script interaction is prevented from occurring. If you do not configure this policy setting, script interaction can occur automatically without user intervention.		

115	IZ_-PolicyScriptActiveX-NotMarkedSafe_1, IZ_-PolicyScriptActiveX-NotMarkedSafe_2, IZ_-PolicyScriptActiveX-NotMarkedSafe_3, IZ_-PolicyScriptActiveX-NotMarkedSafe_4, IZ_-PolicyScriptActiveX-NotMarkedSafe_6, IZ_-PolicyScriptActiveX-NotMarkedSafe_7, IZ_-PolicyScriptActiveX-NotMarkedSafe_8, IZ_-PolicyScriptActiveX-NotMarkedSafe_10 (Initialize and script ActiveX controls not marked as safe)	N/A	N/A
	This policy setting allows you to manage ActiveX controls not marked as safe. If you enable this policy setting, ActiveX controls are run, loaded with parameters, and scripted without setting object safety for untrusted data or scripts. This setting is not recommended, except for secure and administered zones. This setting causes both unsafe and safe controls to be initialized and scripted, ignoring the Script ActiveX controls marked safe for scripting option. If you enable this policy setting and select Prompt in the drop-down box, users are queried whether to allow the control to be loaded with parameters or scripted. If you disable this policy setting, ActiveX controls that cannot be made safe are not loaded with parameters or scripted. If you do not configure this policy setting, ActiveX controls that cannot be made safe are not loaded with parameters or scripted.		
116	IZ_-PolicyScriptingOfJava-Applets_1, IZ_-PolicyScriptingOfJava-Applets_2, IZ_-PolicyScriptingOfJava-Applets_3, IZ_-PolicyScriptingOfJava-Applets_4, IZ_-PolicyScriptingOfJava-Applets_5, IZ_-PolicyScriptingOfJava-Applets_6, IZ_-PolicyScriptingOfJava-Applets_9, IZ_-PolicyScriptingOfJava-Applets_10 (Scripting of Java applets)	N/A	N/A
	This policy setting allows you to manage whether applets are exposed to scripts within the zone. If you enable this policy setting, scripts can access applets automatically without user intervention. If you select Prompt in the drop-down box, users are queried to choose whether to allow scripts to access applets. If you disable this policy setting, scripts are prevented from accessing applets. If you do not configure this policy setting, scripts can access applets automatically without user intervention.		

117	IZ_-PolicySoftwareChannel-Permissions_1, IZ_-PolicySoftwareChannel-Permissions_3 (Software channel permissions)	N/A	N/A
	This policy setting allows you to manage software channel permissions. If you enable this policy setting, you can choose the following options from the drop-down box. Low safety to allow users to be notified of software updates by e-mail, software packages to be automatically downloaded to users computers, and software packages to be automatically installed on users computers. Medium safety to allow users to be notified of software updates by e-mail and software packages to be automatically downloaded to (but not installed on) users computers. High safety to prevent users from being notified of software updates by e-mail, software packages from being automatically downloaded to users computers, and software packages from being automatically installed on users computers. If you disable this policy setting, permissions are set to high safety. If you do not configure this policy setting, permissions are set to Medium safety.		
118	IZ_PolicySubmitNon-encryptedFormData_1, IZ_PolicySubmitNon-encryptedFormData_2, IZ_PolicySubmitNon-encryptedFormData_7, IZ_PolicySubmitNon-encryptedFormData_8 (Submit non-encrypted form data)	N/A	N/A
	This policy setting allows you to manage whether data on HTML forms on pages in the zone may be submitted. Forms sent with SSL (Secure Sockets Layer) encryption are always allowed; this setting only affects non-SSL form data submission. If you enable this policy setting, information using HTML forms on pages in this zone can be submitted automatically. If you select Prompt in the drop-down box, users are queried to choose whether to allow information using HTML forms on pages in this zone to be submitted. If you disable this policy setting, information using HTML forms on pages in this zone is prevented from being submitted. If you do not configure this policy setting, users are queried to choose whether to allow information using HTML forms on pages in this zone to be submitted.		

119	IZ_-PolicyTurnOnXSSFilter_-Both_-LocalMachine, IZ_-PolicyTurnOnXSSFilter_-Both_Intranet, IZ_-PolicyTurnOnXSSFilter_-Both_Trusted, IZ_-PolicyTurnOnXSSFilter_-Both_Internet, IZ_-PolicyTurnOnXSSFilter_-Both_-RestrictedLockdown, IZ_-PolicyTurnOnXSSFilter_-Both_Restricted, IZ_-PolicyTurnOnXSSFilter_-Both_-LocalMachineLockdown, IZ_-PolicyTurnOnXSSFilter_-Both_-IntranetLockdown, IZ_-PolicyTurnOnXSSFilter_-Both_-TrustedLockdown, IZ_-PolicyTurnOnXSSFilter_-Both_InternetLockdown (Turn on Cross-Site Scripting Filter)	N/A	N/A
	This policy controls whether or not the Cross-Site Scripting (XSS) Filter will detect and prevent cross-site script injections into websites in this zone. If you enable this policy setting, the XSS Filter is turned on for sites in this zone, and the XSS Filter attempts to block cross-site script injections. If you disable this policy setting, the XSS Filter is turned off for sites in this zone, and Internet Explorer permits cross-site script injections.		

120	IZ_PolicyWindows-RestrictionsURLaction_-1, IZ_PolicyWindows-RestrictionsURLaction_-2, IZ_PolicyWindows-RestrictionsURLaction_-4, IZ_PolicyWindows-RestrictionsURLaction_-6, IZ_PolicyWindows-RestrictionsURLaction_-7, IZ_PolicyWindows-RestrictionsURLaction_-8 (Allow script-initiated windows without size or position constraints)	N/A	N/A
	This policy setting allows you to manage restrictions on script-initiated pop-up windows and windows that include the title and status bars. If you enable this policy setting, Windows Restrictions security will not apply in this zone. The security zone runs without the added layer of security provided by this feature. If you disable this policy setting, the possible harmful actions contained in script-initiated pop-up windows and windows that include the title and status bars cannot be run. This Internet Explorer security feature will be on in this zone as dictated by the Scripted Windows Security Restrictions feature control setting for the process. If you do not configure this policy setting, the possible harmful actions contained in script-initiated pop-up windows and windows that include the title and status bars cannot be run. This Internet Explorer security feature will be on in this zone as dictated by the Scripted Windows Security Restrictions feature control setting for the process.		
121	IZ_-PolicyZoneElevation-URLaction_1, IZ_-PolicyZoneElevation-URLaction_3 (Web sites in less privileged Web content zones can navigate into this zone)	N/A	N/A
	This policy setting allows you to manage whether Web sites from less privileged zones, such as Restricted Sites, can navigate into this zone. If you enable this policy setting, Web sites from less privileged zones can open new windows in, or navigate into, this zone. The security zone will run without the added layer of security that is provided by the Protection from Zone Elevation security feature. If you select Prompt in the drop-down box, a warning is issued to the user that potentially risky navigation is about to occur. If you disable this policy setting, the possibly harmful navigations are prevented. The Internet Explorer security feature will be on in this zone as set by Protection from Zone Elevation feature control. If you do not configure this policy setting, Web sites from less privileged zones can open new windows in, or navigate into, this zone.		

122	IZ_-PolicySoftwareChannel-Permissions_2, IZ_-PolicySoftwareChannel-Permissions_4, IZ_-PolicySoftwareChannel-Permissions_5, IZ_-PolicySoftwareChannel-Permissions_6, IZ_-PolicySoftwareChannel-Permissions_8, IZ_-PolicySoftwareChannel-Permissions_9, IZ_-PolicySoftwareChannelPermissions_10 (Software channel permissions)	N/A	N/A
	This policy setting allows you to manage software channel permissions. If you enable this policy setting, you can choose the following options from the drop-down box. Low safety to allow users to be notified of software updates by e-mail, software packages to be automatically downloaded to users computers, and software packages to be automatically installed on users computers. Medium safety to allow users to be notified of software updates by e-mail and software packages to be automatically downloaded to (but not installed on) users computers. High safety to prevent users from being notified of software updates by e-mail, software packages from being automatically downloaded to users computers, and software packages from being automatically installed on users computers. If you disable this policy setting, permissions are set to high safety. If you do not configure this policy setting, permissions are set to Low safety.		
123	IZ_PolicyUserdata-Persistence_2, IZ_-PolicyUserdata-Persistence_3 (Userdata persistence)	N/A	N/A
	This policy setting allows you to manage the preservation of information in the browsers history, in favorites, in an XML store, or directly within a Web page saved to disk. When a user returns to a persisted page, the state of the page can be restored if this policy setting is appropriately configured. If you enable this policy setting, users can preserve information in the browsers history, in favorites, in an XML store, or directly within a Web page saved to disk. If you disable this policy setting, users cannot preserve information in the browsers history, in favorites, in an XML store, or directly within a Web page saved to disk. If you do not configure this policy setting, users can preserve information in the browsers history, in favorites, in an XML store, or directly within a Web page saved to disk.		

124	IZ_-PolicyZoneElevation-URLaction_2, IZ_-PolicyZoneElevation-URLaction_4, IZ_-PolicyZoneElevation-URLaction_6, IZ_-PolicyZoneElevation-URLaction_7, IZ_-PolicyZoneElevation-URLaction_8, IZ_-PolicyZoneElevation-URLaction_9, IZ_-PolicyZoneElevation-URLaction_10 (Web sites in less privileged Web content zones can navigate into this zone)	N/A	N/A
	This policy setting allows you to manage whether Web sites from less privileged zones, such as Internet sites, can navigate into this zone. If you enable this policy setting, Web sites from less privileged zones can open new windows in, or navigate into, this zone. The security zone will run without the added layer of security that is provided by the Protection from Zone Elevation security feature. If you select Prompt in the drop-down box, a warning is issued to the user that potentially risky navigation is about to occur. If you disable this policy setting, the possibly harmful navigations are prevented. The Internet Explorer security feature will be on in this zone as set by Protection from Zone Elevation feature control. If you do not configure this policy setting, the possibly harmful navigations are prevented. The Internet Explorer security feature will be on in this zone as set by Protection from Zone Elevation feature control.		
125	IZ_-PolicyNoPromptForOne-OrNoClientCertificate_-3, IZ_-PolicyNoPromptForOne-OrNoClientCertificate_-5, IZ_-PolicyNoPromptForOne-OrNoClientCertificate_-9 (Do not prompt for client certificate selection when no certificates or only one certificate exists.)	N/A	N/A
	This policy setting allows you to manage whether users are prompted to select a certificate when no certificate or only one certificate exists. If you enable this policy setting, Internet Explorer does not prompt users with a Client Authentication message when they connect to a Web site that has no certificate or only one certificate. If you disable this policy setting, Internet Explorer prompts users with a Client Authentication message when they connect to a Web site that has no certificate or only one certificate. If you do not configure this policy setting, Internet Explorer does not prompt users with a Client Authentication message when they connect to a Web site that has no certificate or only one certificate.		

126	IZ_PolicySubmitNon-encryptedFormData_3, IZ_PolicySubmitNon-encryptedFormData_4, IZ_PolicySubmitNon-encryptedFormData_5, IZ_PolicySubmitNon-encryptedFormData_6, IZ_PolicySubmitNon-encryptedFormData_9, IZ_PolicySubmitNon-encryptedFormData_10 (Submit non-encrypted form data)	N/A	N/A
	This policy setting allows you to manage whether data on HTML forms on pages in the zone may be submitted. Forms sent with SSL (Secure Sockets Layer) encryption are always allowed; this setting only affects non-SSL form data submission. If you enable this policy setting, information using HTML forms on pages in this zone can be submitted automatically. If you select Prompt in the drop-down box, users are queried to choose whether to allow information using HTML forms on pages in this zone to be submitted. If you disable this policy setting, information using HTML forms on pages in this zone is prevented from being submitted. If you do not configure this policy setting, information using HTML forms on pages in this zone can be submitted automatically.		
127	IZ_PolicyWindows-RestrictionsURLaction_-3, IZ_PolicyWindows-RestrictionsURLaction_-5, IZ_PolicyWindows-RestrictionsURLaction_-9 (Allow script-initiated windows without size or position constraints)	N/A	N/A
	This policy setting allows you to manage restrictions on script-initiated pop-up windows and windows that include the title and status bars. If you enable this policy setting, Windows Restrictions security will not apply in this zone. The security zone runs without the added layer of security provided by this feature. If you disable this policy setting, the possible harmful actions contained in script-initiated pop-up windows and windows that include the title and status bars cannot be run. This Internet Explorer security feature will be on in this zone as dictated by the Scripted Windows Security Restrictions feature control setting for the process. If you do not configure this policy setting, Windows Restrictions security will not apply in this zone. The security zone runs without the added layer of security provided by this feature.		

128	IZ_-PolicyScriptActiveXNot-MarkedSafe_9, IZ_-PolicyScriptActiveXNot-MarkedSafe_5 (Initialize and script ActiveX controls not marked as safe)	N/A	N/A
	This policy setting allows you to manage ActiveX controls not marked as safe. If you enable this policy setting, ActiveX controls are run, loaded with parameters, and scripted without setting object safety for untrusted data or scripts. This setting is not recommended, except for secure and administered zones. This setting causes both unsafe and safe controls to be initialized and scripted, ignoring the Script ActiveX controls marked safe for scripting option. If you enable this policy setting and select Prompt in the drop-down box, users are queried whether to allow the control to be loaded with parameters or scripted. If you disable this policy setting, ActiveX controls that cannot be made safe are not loaded with parameters or scripted. If you do not configure this policy setting, users are queried whether to allow the control to be loaded with parameters or scripted.		
129	IZ_PolicyNetworkProtocolLockdown_4 (Allow active content over restricted protocols to access my computer)	N/A	N/A
	This policy setting allows you to manage whether a resource hosted on an admin-restricted protocol in the Trusted Sites Zone can run active content such as script, ActiveX, Java and Binary Behaviors. The list of restricted protocols may be set in the Trusted Sites Zone Restricted Protocols section under Network Protocol Lockdown policy. If you enable this policy setting, no Trusted Sites Zone content accessed is affected, even for protocols on the restricted list. If you select Prompt from the drop-down box, the Notification bar will appear to allow control over questionable content accessed over any restricted protocols; content over other protocols is unaffected. If you disable this policy setting, all attempts to access such content over the restricted protocols is blocked. If you do not configure this policy setting, all attempts to access such content over the restricted protocols is blocked when the Network Protocol Lockdown security feature is enabled.		
130	IZ_-PolicyScriptActiveX-MarkedSafe_7, IZ_-PolicyScriptActiveX-MarkedSafe_8 (Script ActiveX controls marked safe for scripting)	N/A	N/A
	This policy setting allows you to manage whether an ActiveX control marked safe for scripting can interact with a script. If you enable this policy setting, script interaction can occur automatically without user intervention. If you select Prompt in the drop-down box, users are queried to choose whether to allow script interaction. If you disable this policy setting, script interaction is prevented from occurring. If you do not configure this policy setting, script interaction is prevented from occurring.		

131	IZ_-PolicyScriptingOfJava-Applets_7, IZ_-PolicyScriptingOfJava-Applets_8 (Scripting of Java applets)	N/A	N/A
	This policy setting allows you to manage whether applets are exposed to scripts within the zone. If you enable this policy setting, scripts can access applets automatically without user intervention. If you select Prompt in the drop-down box, users are queried to choose whether to allow scripts to access applets. If you disable this policy setting, scripts are prevented from accessing applets. If you do not configure this policy setting, scripts are prevented from accessing applets.		
132	IZ_PolicySoftwareChannelPermissions_7 (Software channel permissions)	N/A	N/A
	This policy setting allows you to manage software channel permissions. If you enable this policy setting, you can choose the following options from the drop-down box. Low safety to allow users to be notified of software updates by e-mail, software packages to be automatically downloaded to users computers, and software packages to be automatically installed on users computers. Medium safety to allow users to be notified of software updates by e-mail and software packages to be automatically downloaded to (but not installed on) users computers. High safety to prevent users from being notified of software updates by e-mail, software packages from being automatically downloaded to users computers, and software packages from being automatically installed on users computers. If you disable this policy setting, permissions are set to high safety. If you do not configure this policy setting, permissions are set to High safety.		
133	IZ_IncludeUnspecifiedLocalSites (Intranet Sites: Include all local (intranet) sites not listed in other zones)	N/A	N/A
	This policy setting controls whether local sites which are not explicitly mapped into any Security Zone are forced into the local Intranet security zone. If you enable this policy setting, local sites which are not explicitly mapped into a zone are considered to be in the Intranet Zone. If you disable this policy setting, local sites which are not explicitly mapped into a zone will not be considered to be in the Intranet Zone (so would typically be in the Internet Zone). If you do not configure this policy setting, users choose whether to force local sites into the Intranet Zone.		
134	IZ_PolicyWarnCertMismatch (Turn on certificate address mismatch warning)	N/A	N/A
	This policy setting allows you to turn on the certificate address mismatch security warning. When this policy setting is turned on, the user is warned when visiting Secure HTTP (HTTPS) websites that present certificates issued for a different website address. This warning helps prevent spoofing attacks. If you enable this policy setting, the certificate address mismatch warning always appears. If you disable or do not configure this policy setting, the user can choose whether the certificate address mismatch warning appears (by using the Advanced page in the Internet Control panel).		

135	IZ_PolicyInternetZone-LockdownTemplate (Locked-Down Internet Zone Template)	N/A	N/A
	This template policy setting allows you to configure policy settings in this zone consistent with a selected security level, for example, Low, Medium Low, Medium, or High. If you enable this template policy setting and select a security level, all values for individual settings in the zone will be overwritten by the standard template defaults. If you disable this template policy setting, no security level is configured. If you do not configure this template policy setting, no security level is configured. Note. Local Machine Zone Lockdown Security and Network Protocol Lockdown operate by comparing the settings in the active URLs zone against those in the Locked-Down equivalent zone. If you select a security level for any zone (including selecting no security), the same change should be made to the Locked-Down equivalent. Note. It is recommended to configure template policy settings in one Group Policy object (GPO) and configure any related individual policy settings in a separate GPO. You can then use Group Policy management features (for example, precedence, inheritance, or enforce) to apply individual settings to specific targets.		
136	IZ_PolicyInternet-ZoneTemplate (Internet Zone Template)	N/A	N/A
	This template policy setting allows you to configure policy settings in this zone consistent with a selected security level, for example, Low, Medium Low, Medium, or High. If you enable this template policy setting and select a security level, all values for individual settings in the zone will be overwritten by the standard template defaults. If you disable this template policy setting, no security level is configured. If you do not configure this template policy setting, no security level is configured. Note. Local Machine Zone Lockdown Security and Network Protocol Lockdown operate by comparing the settings in the active URLs zone against those in the Locked-Down equivalent zone. If you select a security level for any zone (including selecting no security), the same change should be made to the Locked-Down equivalent. Note. It is recommended to configure template policy settings in one Group Policy object (GPO) and configure any related individual policy settings in a separate GPO. You can then use Group Policy management features (for example, precedence, inheritance, or enforce) to apply individual settings to specific targets.		
137	IZ_PolicyIntranetZone-LockdownTemplate (Locked-Down Intranet Zone Template)	N/A	N/A
	This template policy setting allows you to configure policy settings in this zone consistent with a selected security level, for example, Low, Medium Low, Medium, or High. If you enable this template policy setting and select a security level, all values for individual settings in the zone will be overwritten by the standard template defaults. If you disable this template policy setting, no security level is configured. If you do not configure this template policy setting, no security level is configured. Note. Local Machine Zone Lockdown Security and Network Protocol Lockdown operate by comparing the settings in the active URLs zone against those in the Locked-Down equivalent zone. If you select a security level for any zone (including selecting no security), the same change should be made to the Locked-Down equivalent. Note. It is recommended to configure template policy settings in one Group Policy object (GPO) and configure any related individual policy settings in a separate GPO. You can then use Group Policy management features (for example, precedence, inheritance, or enforce) to apply individual settings to specific targets.		

138	IZ_PolicyIntranet-ZoneTemplate (Intranet Zone Template)	N/A	N/A
	This template policy setting allows you to configure policy settings in this zone consistent with a selected security level, for example, Low, Medium Low, Medium, or High. If you enable this template policy setting and select a security level, all values for individual settings in the zone will be overwritten by the standard template defaults. If you disable this template policy setting, no security level is configured. If you do not configure this template policy setting, no security level is configured. Note. Local Machine Zone Lockdown Security and Network Protocol Lockdown operate by comparing the settings in the active URLs zone against those in the Locked-Down equivalent zone. If you select a security level for any zone (including selecting no security), the same change should be made to the Locked-Down equivalent. Note. It is recommended to configure template policy settings in one Group Policy object (GPO) and configure any related individual policy settings in a separate GPO. You can then use Group Policy management features (for example, precedence, inheritance, or enforce) to apply individual settings to specific targets.		
139	IZ_PolicyLocalMachine-ZoneLockdownTemplate (Locked-Down Local Machine Zone Template)	N/A	N/A
	This template policy setting allows you to configure policy settings in this zone consistent with a selected security level, for example, Low, Medium Low, Medium, or High. If you enable this template policy setting and select a security level, all values for individual settings in the zone will be overwritten by the standard template defaults. If you disable this template policy setting, no security level is configured. If you do not configure this template policy setting, no security level is configured. Note. Local Machine Zone Lockdown Security and Network Protocol Lockdown operate by comparing the settings in the active URLs zone against those in the Locked-Down equivalent zone. If you select a security level for any zone (including selecting no security), the same change should be made to the Locked-Down equivalent. Note. It is recommended to configure template policy settings in one Group Policy object (GPO) and configure any related individual policy settings in a separate GPO. You can then use Group Policy management features (for example, precedence, inheritance, or enforce) to apply individual settings to specific targets.		
140	IZ_PolicyLocalMachine-ZoneTemplate (Local Machine Zone Template)	N/A	N/A
	This template policy setting allows you to configure policy settings in this zone consistent with a selected security level, for example, Low, Medium Low, Medium, or High. If you enable this template policy setting and select a security level, all values for individual settings in the zone will be overwritten by the standard template defaults. If you disable this template policy setting, no security level is configured. If you do not configure this template policy setting, no security level is configured. Note. Local Machine Zone Lockdown Security and Network Protocol Lockdown operate by comparing the settings in the active URLs zone against those in the Locked-Down equivalent zone. If you select a security level for any zone (including selecting no security), the same change should be made to the Locked-Down equivalent. Note. It is recommended to configure template policy settings in one Group Policy object (GPO) and configure any related individual policy settings in a separate GPO. You can then use Group Policy management features (for example, precedence, inheritance, or enforce) to apply individual settings to specific targets.		

141	IZ_PolicyRestrictedSites-ZoneLockdownTemplate (Locked-Down Restricted Sites Zone Template)	N/A	N/A
	This template policy setting allows you to configure policy settings in this zone consistent with a selected security level, for example, Low, Medium Low, Medium, or High. If you enable this template policy setting and select a security level, all values for individual settings in the zone will be overwritten by the standard template defaults. If you disable this template policy setting, no security level is configured. If you do not configure this template policy setting, no security level is configured. Note. Local Machine Zone Lockdown Security and Network Protocol Lockdown operate by comparing the settings in the active URLs zone against those in the Locked-Down equivalent zone. If you select a security level for any zone (including selecting no security), the same change should be made to the Locked-Down equivalent. Note. It is recommended to configure template policy settings in one Group Policy object (GPO) and configure any related individual policy settings in a separate GPO. You can then use Group Policy management features (for example, precedence, inheritance, or enforce) to apply individual settings to specific targets.		
142	IZ_PolicyRestrictedSites-ZoneTemplate (Restricted Sites Zone Template)	N/A	N/A
	This template policy setting allows you to configure policy settings in this zone consistent with a selected security level, for example, Low, Medium Low, Medium, or High. If you enable this template policy setting and select a security level, all values for individual settings in the zone will be overwritten by the standard template defaults. If you disable this template policy setting, no security level is configured. If you do not configure this template policy setting, no security level is configured. Note. Local Machine Zone Lockdown Security and Network Protocol Lockdown operate by comparing the settings in the active URLs zone against those in the Locked-Down equivalent zone. If you select a security level for any zone (including selecting no security), the same change should be made to the Locked-Down equivalent. Note. It is recommended to configure template policy settings in one Group Policy object (GPO) and configure any related individual policy settings in a separate GPO. You can then use Group Policy management features (for example, precedence, inheritance, or enforce) to apply individual settings to specific targets.		
143	IZ_PolicyTrustedSites-ZoneLockdownTemplate (Locked-Down Trusted Sites Zone Template)	N/A	N/A
	This template policy setting allows you to configure policy settings in this zone consistent with a selected security level, for example, Low, Medium Low, Medium, or High. If you enable this template policy setting and select a security level, all values for individual settings in the zone will be overwritten by the standard template defaults. If you disable this template policy setting, no security level is configured. If you do not configure this template policy setting, no security level is configured. Note. Local Machine Zone Lockdown Security and Network Protocol Lockdown operate by comparing the settings in the active URLs zone against those in the Locked-Down equivalent zone. If you select a security level for any zone (including selecting no security), the same change should be made to the Locked-Down equivalent. Note. It is recommended to configure template policy settings in one Group Policy object (GPO) and configure any related individual policy settings in a separate GPO. You can then use Group Policy management features (for example, precedence, inheritance, or enforce) to apply individual settings to specific targets.		

144	IZ_PolicyTrustedSites-ZoneTemplate (Trusted Sites Zone Template)	N/A	N/A
	This template policy setting allows you to configure policy settings in this zone consistent with a selected security level, for example, Low, Medium Low, Medium, or High. If you enable this template policy setting and select a security level, all values for individual settings in the zone will be overwritten by the standard template defaults. If you disable this template policy setting, no security level is configured. If you do not configure this template policy setting, no security level is configured. Note. Local Machine Zone Lockdown Security and Network Protocol Lockdown operate by comparing the settings in the active URLs zone against those in the Locked-Down equivalent zone. If you select a security level for any zone (including selecting no security), the same change should be made to the Locked-Down equivalent. Note. It is recommended to configure template policy settings in one Group Policy object (GPO) and configure any related individual policy settings in a separate GPO. You can then use Group Policy management features (for example, precedence, inheritance, or enforce) to apply individual settings to specific targets.		
145	IZ_ProxyByPass (Intranet Sites: Include all sites that bypass the proxy server)	N/A	N/A
	This policy setting controls whether sites which bypass the proxy server are mapped into the local Intranet security zone. If you enable this policy setting, sites which bypass the proxy server are mapped into the Intranet Zone. If you disable this policy setting, sites which bypass the proxy server arent necessarily mapped into the Intranet Zone (other rules might map one there). If you do not configure this policy setting, users choose whether sites which bypass the proxy server are mapped into the Intranet Zone.		
146	IZ_UNCAsIntranet (Intranet Sites: Include all network paths (UNCs))	N/A	N/A
	This policy setting controls whether URLs representing UNCs are mapped into the local Intranet security zone. If you enable this policy setting, all network paths are mapped into the Intranet Zone. If you disable this policy setting, network paths are not necessarily mapped into the Intranet Zone (other rules might map one there). If you do not configure this policy setting, users choose whether network paths are mapped into the Intranet Zone.		

147	IZ_Zonemaps (Site to Zone Assignment List)	N/A	N/A
	This policy setting allows you to manage a list of sites that you want to associate with a particular security zone. These zone numbers have associated security settings that apply to all of the sites in the zone. Internet Explorer has 4 security zones, numbered 1-4, and these are used by this policy setting to associate sites to zones. They are: (1) Intranet zone, (2) Trusted Sites zone, (3) Internet zone, and (4) Restricted Sites zone. Security settings can be set for each of these zones through other policy settings, and their default settings are: Trusted Sites zone (Low template), Intranet zone (Medium-Low template), Internet zone (Medium template), and Restricted Sites zone (High template). (The Local Machine zone and its locked down equivalent have special security settings that protect your local computer.) If you enable this policy setting, you can enter a list of sites and their related zone numbers. The association of a site with a zone will ensure that the security settings for the specified zone are applied to the site. For each entry that you add to the list, enter the following information: Valuename A host for an intranet site, or a fully qualified domain name for other sites. The valuename may also include a specific protocol. For example, if you enter http://www.contoso.com as the valuename, other protocols are not affected.If you enter just www.contoso.com,then all protocols are affected for that site, including http, https, ftp, and so on. The site may also be expressed as an IP address (e.g., 127.0.0.1) or range (e.g., 127.0.0.1-10). To avoid creating conflicting policies, do not include additional characters after the domain such as trailing slashes or URL path. For example, policy settings for www.contoso.com and www.contoso.com/mail would be treated as the same policy setting by Internet Explorer, and would therefore be in conflict. Value - A number indicating the zone with which this site should be associated for security settings. The Internet Explorer zones described above are 1-4. If you disable or do not configure this policy, users may choose their own site-to-zone assignments.		
148	SecurityPage_AutoDetect (Turn on automatic detection of intranet)	N/A	N/A
	This policy setting enables intranet mapping rules to be applied automatically if the computer belongs to a domain. If you enable this policy setting, automatic detection of the intranet is turned on, and intranet mapping rules are applied automatically if the computer belongs to a domain. If you disable this policy setting, automatic detection of the intranet is turned off, and intranet mapping rules are applied however they are configured. If this policy setting is not configured, the user can choose whether or not to automatically detect the intranet through the intranet settings dialog in Control Panel.		

149	SecurityPage_WarnOnIntranet (Turn on Notification bar notification for intranet content)	N/A	N/A
	This policy setting causes a Notification bar notification to appear when intranet content is loaded and the intranet mapping rules have not been configured. The Notification bar allows the user to enable intranet mappings, if they require them. If you enable this policy setting, a Notification bar notification appears whenever the user browses to a page that loads content from an intranet site. If you disable this policy setting, a Notification bar notification does not appear when the user loads content from an intranet site that is being treated as though it is in the Internet zone. If this policy setting is not configured, a Notification bar notification appears for intranet content loaded on a browser on a computer that is not a domain member, until the user turns off the Notification bar.		
150	IZ_PolicyZoneElevationURLaction_5 (Web sites in less privileged Web content zones can navigate into this zone)	N/A	N/A
	This policy setting allows you to manage whether Web sites from less privileged zones, such as Restricted Sites, can navigate into this zone. If you enable this policy setting, Web sites from less privileged zones can open new windows in, or navigate into, this zone. The security zone will run without the added layer of security that is provided by the Protection from Zone Elevation security feature. If you select Prompt in the drop-down box, a warning is issued to the user that potentially risky navigation is about to occur. If you disable this policy setting, the possibly harmful navigations are prevented. The Internet Explorer security feature will be on in this zone as set by Protection from Zone Elevation feature control. If you do not configure this policy setting, a warning is issued to the user that potentially risky navigation is about to occur.		
151	IESF_DisablePasswordRevealButton (Do not display the reveal password button)	N/A	N/A
	This policy setting allows you to hide the reveal password button when Internet Explorer prompts users for a password. The reveal password button is displayed during password entry. When the user clicks the button, the current password value is visible until the mouse button is released (or until the tap ends). If you enable this policy setting, the reveal password button will be hidden for all password fields. Users and developers will not be able to depend on the reveal password button being displayed in any web form or web application. If you disable or do not configure this policy setting, the reveal password button can be shown by the application as a user types in a password. The reveal password button is visible by default. On at least Windows 8, if the Do not display the reveal password button policy setting located in Computer Configuration/Administrative Templates/Windows Components/Credential User Interface is enabled for the system, it will override this policy setting.		

152	IESF_MaxConnectionPerServer (Change the maximum number of connections per host (HTTP 1.1))	N/A	N/A
	This policy setting allows you to change the default connection limit for HTTP 1.1 from 6 connections per host to a limit of your choice (from 2 through 128). If you enable this policy setting, Internet Explorer uses the connection limit of your choice for HTTP 1.1. If you disable or do not configure this policy setting, Internet Explorer uses the default connection limit for HTTP 1.1 (6 connections per host). In versions of Internet Explorer before Internet Explorer 8, the default connection limit for HTTP 1.1 was 2.		
153	IESF_MaxConnectionPer1_0Server (Maximum number of connections per server (HTTP 1.0))	N/A	N/A
	This policy setting allows you to change the default connection limit for HTTP 1.0 from 6 connections per host to a limit of your choice (from 2 through 128). If you disable or do not configure this policy setting, Internet Explorer will use the default connection limit for HTTP 1.0 (6 connections per host). In versions of Internet Explorer prior to Internet Explorer 8, the default connection limit for HTTP 1.0 was 4.		
154	IESF_WebSocketMaxConnectionsPerServer (Set the maximum number of WebSocket connections per server)	N/A	N/A
	This policy setting allows you to change the default limit of WebSocket connections per server. The default limit is 6; you can select a value from 2 through 128. If you enable this policy setting, Internet Explorer uses the WebSocket connection limit that you set with this policy setting. If you disable or do not configure this policy setting, Internet Explorer uses the default limit of 6 WebSocket connections per server.		
155	DisableDeveloperTools (Turn off Developer Tools)	Setting is available as DisableDeveloperTools (Disable Developer Tools) in this browser	Similar semantics can be achieved by modifying multiple entries in about:config
	This policy setting allows you to manage whether the user can access Developer Tools in Internet Explorer. If you enable this policy setting, the user cannot access Developer Tools. If you disable or do not configure this policy setting, the user can access Developer Tools.		
156	UpdateIntervalPol (Prevent specifying the update check interval (in days))	Similar semantics can be achieved by modifying multiple settings	Similar semantics can be achieved by using different third party Add-ons
	This policy setting prevents the user from specifying the update check interval. The default value is 30 days. If you enable this policy setting, the user cannot specify the update check interval. You must specify the update check interval. If you disable or do not configure this policy setting, the user can specify the update check interval.		

157	UpdatePagePol (Prevent changing the URL for checking updates to Internet Explorer and Internet Tools)	N/A	N/A
	This policy setting prevents the user from changing the default URL for checking updates to Internet Explorer and Internet Tools. If you enable this policy setting, the user cannot change the URL that is displayed for checking updates to Internet Explorer and Internet Tools. You must specify this URL. If you disable or do not configure this policy setting, the user can change the URL that is displayed for checking updates to Internet Explorer and Internet Tools.		
158	DisablePerUserActiveX-Install (Prevent per-user installation of ActiveX controls)	N/A	N/A
	This policy setting allows you to prevent the installation of ActiveX controls on a per-user basis. If you enable this policy setting, ActiveX controls cannot be installed on a per-user basis. If you disable or do not configure this policy setting, ActiveX controls can be installed on a per-user basis.		
159	OnlyUseAXISForActiveX-Install (Specify use of ActiveX Installer Service for installation of ActiveX controls)	N/A	N/A
	This policy setting allows you to specify how ActiveX controls are installed. If you enable this policy setting, ActiveX controls are installed only if the ActiveX Installer Service is present and has been configured to allow the installation of ActiveX controls. If you disable or do not configure this policy setting, ActiveX controls, including per-user controls, are installed through the standard installation process.		
160	DisableInPrivateBrowsing (Turn off InPrivate Browsing)	Similar semantics can be achieved by modifying multiple settings	N/A
	This policy setting allows you to turn off the InPrivate Browsing feature. InPrivate Browsing prevents Internet Explorer from storing data about a users browsing session. This includes cookies, temporary Internet files, history, and other data. If you enable this policy setting, InPrivate Browsing is turned off. If you disable this policy setting, InPrivate Browsing is available for use. If you do not configure this policy setting, InPrivate Browsing can be turned on or off through the registry.		
161	DisableInPrivateLogging (Turn off collection of InPrivate Filtering data)	N/A	N/A
	This policy setting allows you to turn off the collection of data used by the InPrivate Filtering Automatic mode. The data consists of the URLs of third-party content, along with data about the first-party websites that referenced it. It is collected during non-InPrivate (normal) browsing sessions. If you enable this policy setting, InPrivate Filtering data collection is turned off. If you disable this policy setting, InPrivate Filtering collection is turned on. If you do not configure this policy setting, InPrivate Filtering data collection can be turned on or off on the Privacy tab in Internet Options.		

162	InPrivateBlockingThresholdV8 (Establish InPrivate Filtering threshold)	N/A	N/A
	This policy setting allows you to establish the threshold for InPrivate Filtering Automatic mode. The threshold sets the number of first-party sites that a particular third-party item can be referenced from before it is blocked. Setting this value lower can help prevent more third-party sites from obtaining details about a users browsing. However, doing so may cause compatibility issues on some websites. The allowed value range is 3 through 30. If you enable this policy setting, the selected value is enforced. If you disable or do not configure this policy setting, the user can establish the InPrivate Filtering threshold by clicking the Safety button and then clicking InPrivate Filtering.		
163	DisableInPrivateBlockingV8 (Turn off InPrivate Filtering)	N/A	N/A
	This policy setting allows you to turn off InPrivate Filtering. InPrivate Filtering helps users control whether third parties can automatically collect information about their browsing based on the sites that they visit. InPrivate Filtering does this by identifying third-party content that is used by multiple websites that users have visited. If you enable this policy setting, InPrivate Filtering is turned off in all browsing sessions, and InPrivate Filtering data is not collected. If you disable this policy setting, InPrivate Filtering is available for use. If you do not configure this policy setting, it can be configured through the registry.		
164	InPrivateBlockingThresholdV9 (Establish Tracking Protection threshold)	N/A	N/A
	This policy setting allows you to establish the threshold for Tracking Protection Automatic mode. The threshold sets the number of first-party sites that a particular third-party item can be referenced from before it is blocked. Setting this value lower can help prevent more third-party sites from obtaining details about a users browsing. However, doing so may cause compatibility issues on some websites. The allowed value range is 3 through 30. If you enable this policy setting, the selected value is enforced. If you disable or do not configure this policy setting, the user can establish the Tracking Protection threshold by clicking the Safety button and then clicking Tracking Protection.		
165	DisableInPrivateBlockingV9 (Turn off Tracking Protection)	N/A	N/A
	This policy setting allows you to turn off Tracking Protection. Tracking Protection helps users control whether third parties can automatically collect information about their browsing based on the sites that they visit. Tracking Protection does this by identifying third-party content that is used by multiple websites that users have visited. If you enable this policy setting, Tracking Protection is disabled in all browsing sessions, and Tracking Protection data is not collected. If you disable this policy setting, Tracking Protection is available for use. If you do not configure this policy setting, it can be configured through the registry.		

166	UsePolicyAccelerators (Restrict Accelerators to those deployed through Group Policy)	N/A	N/A
	This policy setting restricts the list of Accelerators that the user can access to only the set deployed through Group Policy. If you enable this policy setting, the user can access only Accelerators that are deployed through Group Policy. The user cannot add or delete Accelerators. If you disable or do not configure this policy setting, the user can access any Accelerators that he or she has installed.		
167	IndexedDB_MaxTrusted-DomainLimitInMB (Set indexed database storage limits for individual domains)	N/A	N/A
	This policy setting sets data storage limits for indexed databases of websites that have been allowed to exceed their storage limit. The Set default storage limits for websites policy setting sets the data storage limits for indexed databases. If a domain exceeds the indexed database storage limit for an individual domain, Internet Explorer sends an error to the website. No notification is sent to the user. This group policy sets the maximum data storage limit for domains that are trusted by users. When you set this policy setting, you provide the cache limit, in MB. The default is 500 MB. If you enable this policy setting, Internet Explorer will allow trusted domains to store additional data in indexed databases, up to the limit set in this group policy. If you disable or do not configure this policy setting, Internet Explorer will use the default maximum storage limit for all indexed databases. The default is 500 MB.		
168	IndexedDB_TotalLim-itInMB (Set maximum indexed database storage limit for all domains)	N/A	N/A
	This policy setting sets the data storage limit for all combined indexed databases for a user. When you set this policy setting, you provide the storage limit in MB. When the limit is reached, Internet Explorer notifies the user, and the user must delete indexed databases before an updated database can be saved on their computer. The default maximum storage limit for all indexed databases is 4 GB. If you enable this policy setting, you can set the maximum storage limit for all indexed databases. The default is 4 GB. If you disable or do not configure this policy setting, Internet Explorer will use the default maximum storage limit for all indexed databases. The default is 4 GB.		
169	AppCache_AllowWeb-siteCaches (Allow websites to store application caches on client computers)	N/A	N/A
	This policy setting allows websites to store file resources in application caches on client computers. If you enable this policy setting, websites will be able to store application caches on client computers. Allow website database and caches on Website Data Settings will be unavailable to users. If you disable this policy setting, websites will not be able to store application caches on client computers. Allow website database and caches on Website Data Settings will be unavailable to users. If you do not configure this policy setting, websites will be able to store application caches on client computers. Allow website database and caches on Website Data Settings will be available to users. Users can choose whether or not to allow websites to store data on their computers.		

170	AppCache_MaxTrusted-DomainLimitInMB (Set application cache storage limits for individual domains)	N/A	N/A
	This policy setting sets file storage limits for application caches of websites that have been allowed to exceed their storage limit. The Set default storage limits for websites policy setting sets the data storage limits for application caches. If a domain exceeds the application cache storage limit for an individual domain, Internet Explorer sends an error to the website. No notification will be displayed to the user. This group policy sets the maximum file storage limit for domains that are trusted by users. When you set this policy setting, you provide the cache limit, in MB. The default is 50 MB. If you enable this policy setting, Internet Explorer will allow trusted domains to store additional files in application caches, up to the limit set in this policy setting. If you disable or do not configure this policy setting, Internet Explorer will use the default maximum storage limit for all application caches. The default is 50 MB.		
171	EnableAutoUpgrade (Install new versions of Internet Explorer automatically)	N/A	N/A
	This policy setting configures Internet Explorer to automatically install new versions of Internet Explorer when they are available. If you enable this policy setting, automatic upgrade of Internet Explorer will be turned on. If you disable this policy setting, automatic upgrade of Internet Explorer will be turned off. If you do not configure this policy, users can turn on or turn off automatic updates from the About Internet Explorer dialog.		

Notations for Table A.3

1. IE: Camparison in Internet Explorer
2. Chrome: Camparison in Google Chrome
3. Firefox: Mozilla Firefox (policy name and display name)
4. Description: Description about the policy in Mozilla Firefox
5. N/A: Policy is not available in this browser

Table A.3: Comparison of Security Related Settings for Mozilla Firefox with Respect to Internet Explorer and Google Chrome

EN	**Firefox**	**IE**	**Google Chrome**
	Description		

1	Add_On_Delay (Delay When Installing Add-ons)	N/A	N/A
	This policy allows us to configure browser such that, we can set the time delay during installing new add-ons.		
2	Extensions_Delay (Delay When Installing Extensions)	N/A	N/A
	This policy allows us to configure browser such that, we can set the time delay during installing new extensions.		
3	DNS (Disable DNS Prefetching)	N/A	This Setting is available as DnsPrefetchingEnabled (Enable network prediction) in this browser.
	This feature allows Firefox to perform domain name resolution proactively. If we enable this setting, DNS prefetching is disabled. If it is disabled Firefox can activate DNS prefetching.		
4	Safe_Browsing (Enable Safe Browsing)	Similar semantics can be achieved by modifying multiple settings at different zones	This Setting is available as SafeBrowsingEnabled (Enable Safe Browsing) in this browser.
	This setting allows us to enable safe browsing mode such that the browser can detect malicious content in web pages. If we enable this setting safe browsing is activated and deactivated if we disable this setting.		
5	Crash_restore (Crash Recovery)	This Setting is available as DisableACRPrompt (Turn off Automatic Crash Recovery) in this browser	N/A
	This setting allows us to activate or deactivate crash recovery of Mozilla Firefox browser.		
6	Security_Ocsp_Enabled (Security Ocsp Enabled)	N/A	N/A
	Determines behavior of OCSP-based certificate verification/validation. 0 (default in Firefox 2 and below): Do not use OCSP for certificate validation 1 (default in Firefox 3 and above): Use OCSP to validate only certificates that specify an OCSP service URL (see bug 110161). 2: Enable and use values in security.OCSP.URL and security.OCSP.signingCA for validation. Notes: In Firefox, this can be changed via Tools ? Options ? Advanced ? Validation ? OCSP. In SeaMonkey 2, this can be changed via the first checkbox and the radio buttons under Edit ? Preferences ? Privacy & Security ? Validation ? OCSP.		

7	Network_Http_Keep_-Alive_Timeout (Network Http Keep Alive Timeout)	N/A	N/A
	Requested timeout for Keep-Alive connections in seconds. Default value is 300.		
8	Network_Auth_Use_-Sspi (Network Auth Use Sspi)	N/A	N/A
	True (default in Windows): Use SSPI instead of GSSAPI for Kerberos-based authentication False: Opposite of the above Note: Firefox 1.5 and above only.		
9	Browser_Sessionhistory_Max_Total_Viewers (Browser Sessionhistory Max Total Viewers)	N/A	N/A
	Determines the maximum number of content viewers to cache for bfcache (fast back-/forward navigation). Default value is -1 (calculate based on available memory). All values less than 0 are equivalent. Note: Firefox 1.5 and above only. Supersedes browser.sessionhistory.max_viewers.		
10	Network_Cookie_Alwaysacceptsessioncookies (Network Cookie Alwaysacceptsessioncookies)	Similar semantics can be achieved by modifying multiple settings at different zones	N/A
	Determines whether to accept session cookies (kept for the duration of the browser session, then removed) if network.cookie.lifetimePolicy is 1. True: Accept session cookies without prompting False (default): Prompt before accepting session cookies		
11	Security_Ask_For_Password (Security Ask For Password)	N/A	N/A
	Determines when Mozilla Mail should ask for the master password. 0 (default): Only the first time its needed 1: Every time its needed 2: Every n minutes, where n is the value in security.password_lifetime.		
12	Network_Http_Use_-Cache (Network Http Use Cache)	N/A	N/A
	Determines whether to enable caching of HTTP documents. True (default): Enable caching False: Opposite of the above		
13	Security_Checkloaduri (Security Checkloaduri)	N/A	N/A
	Pref removed (use CAPS instead). Previously: Determines how to handle access across schemes (e.g., loading file: URLs from http: URLs) True (default): Perform security checks and block access for insecure access False: Opposite of the above		

14	Network_Negotiate_-Auth_Gsslib (Network Negotiate Auth Gsslib)	N/A	N/A
	Path to a specific GSSAPI library. Allows the browser (e.g.) to load different Kerberos implementations at the users request. Default value is an empty string. Note: See bug 295109 for more information.		
15	Extensions_Update_Enabled (Extensions Update Enabled)	Similar semantics can be achieved by modifying multiple settings at different zones	Similar semantics can be achieved by modifying multiple settings
	True (default): Allow checking for updates False: Opposite of the above Can be overridden on a per-extension basis by setting extensions.GUID.update.enabled.		
16	Network_Http_Pipelining_Maxrequests (Network Http Pipelining Maxrequests)	N/A	N/A
	Determines the maximum number of HTTP requests in the pipeline (sent sequentially without waiting for a response). Values greater than 8 are assumed to be 8; values less than 1 are assumed to be 1. Default value is 4.		
17	Network_Proxy_Type (Network Proxy Type)	Similar semantics can be achieved by modifying multiple settings at different zones	Similar semantics can be achieved by modifying multiple settings
	Determines how the browser uses proxies. 0 (default): Direct connection to the Internet (no proxy used) 1: Manual proxy configuration (use values in network.proxy.*) 2: Autoconfiguration by URL (use value in network.proxy.autoconfig_url) 3: Same as 0 for compatibility reasons (see bug 115720) and will be reset to 0 4: Auto-detect proxy settings for this network		
18	Browser_Sessionhistory_Max_Entries (Browser Sessionhistory Max Entries)	N/A	N/A
	The maximum number of pages in the browsers session history, i.e. the maximum number of URLs you can traverse purely through the Back/Forward buttons. Default value is 50.		
19	Network_Protocol_Handler_Warn_External_-Default (Network Protocol Handler Warn External Default)	N/A	N/A
	Determines whether to warn the user before loading an unlisted external handler True (default): Warn the user False: Opposite of the above		

20	Extensions_Update_Url (Extensions Update Url)	N/A	N/A
	Determines the URL queried when polling for extension updates. Can be overridden on a per-extension basis by setting extensions.GUID.update.url. Default value is pulled from chrome://mozapps/locale/update/update.properties.		
21	Browser_Search_Log (Browser Search Log)	N/A	N/A
	True: Log debugging information about the search service to the JavaScript Console and stdout. False (default): Do not log debugging information. Note: Firefox 2.0 and above only.		
22	Browser_Urlbar_Match_Url (Browser Urlbar Match Url)	N/A	N/A
	Returns results that match the text in the URL		
23	Network_Http_Max_Persistent_Connections_Per_Server (Network Http Max Persistent Connections Per Server)	Similar semantics can be achieved by modifying multiple settings at different zones	N/A
	If network.http.keep-alive is true, and if a proxy server is not configured, then a new connection will only be attempted if the number of active persistent connections to the server is less than this preference. Default value is 6. Valid values are between 1 and 255 inclusive.		
24	Security_Default_Personal_Cert (Security Default Personal Cert)	N/A	N/A
	Determines the selection of a security certificate to present to web sites that require one. Select Automatically (default): Automatically choose the certificate Ask Every Time: Prompt user with a choice of certificate options every time Note: In Firefox, this can be changed via Tools ? Options ? Advanced ? Certificates ? Client Certificate Selection		
25	Network_Automatic_Ntlm_Auth_Trusted_Uris (Network Automatic Ntlm Auth Trusted Uris)	N/A	N/A
	A comma-and-space-delimited list of URIs with which to automatically authenticate via NTLM (Windows domain logon). Default value is an empty string. (See Integrated Authentication for more information)		
26	General_Useragent_Locale (General Useragent Locale)	N/A	N/A
	ISO 639-2 value representing the users language for the User-Agent string		

27	Browser_Urlbar_Restrict_Tag (Browser Urlbar Restrict Tag)	N/A	N/A
	Returns only results that have been tagged		
28	General_Config_Obscure_Value (General Config Obscure Value)	N/A	N/A
	An integer to use when obscuring the AutoConfig file saved to and read from disk. Default value is 13 (effectively, ROT-13 the content).		
29	Xpinstall_Whitelist_Required (Xpinstall Whitelist Required)	Similar semantics can be achieved by modifying multiple settings at different zones	Similar semantics can be achieved by modifying multiple settings
	True (default): When installing extensions from remote hosts, remote host must be on the whitelist False: Opposite of the above		
30	Network_Autodial_Helper_Enabled (Network Autodial Helper Enabled)	N/A	N/A
	Help Windows NT, 2000, and XP dialup a RAS connection when a network address is unreachable. True (default): Launch dialer (if one is configured) when address is unreachable False: Display error message		
31	Network_Protocol_Handler_External_Default (Network Protocol Handler External Default)	N/A	N/A
	Determines the default action for unlisted external protocol handlers True (default): Try to load False: Opposite of the above		
32	Profile_Confirm_Automigration (Profile Confirm Automigration)	N/A	N/A
	True (default): Ask user before performing an automigration False: Opposite of the above		
33	Security_Password_Lifetime (Security Password Lifetime)	N/A	N/A
	Determines how long (in minutes) to go without asking for the master password in Mozilla Mail when security.ask_for_password is 2. Default value is 30.		

34	Network_Negotiate_Auth_Delegation_Uris (Network Negotiate Auth Delegation Uris)	N/A	N/A
	A comma-and-space-delimited list of sites for which the browser may delegate user authorization to the server. (See Integrated Authentication for more information.) Default value is an empty string.		
35	Network_Protocol_Handler_Expose_All (Network Protocol Handler Expose All)	N/A	N/A
	Determines whether to expose (enable) all protocol handlers. This preference overrides more specific preferences, e.g. network.protocol-handler.expose.mailto. True: Try to open link clicks in browser first, then fail over to system handlers False: Do not expose all protocol handlers		
36	Privacy_Popups_Showbrowsermessage (Privacy Popups Showbrowsermessage)	N/A	N/A
	True (default): Display a message at the top of the browser window when a popup has been blocked False: Display a status bar icon to indicate when a popup has been blocked		
37	Intl_Charset_Detector (Intl Charset Detector)	N/A	N/A
	Determines which locale URI sets how character set are detected in the browser		
38	Network_Http_Sendsecurexsitereferrer (Network Http Sendsecurexsitereferrer)	N/A	N/A
	Determines how to handle Referer HTTP header when navigating between secure (HTTPS) hosts. True (default): Send referring URL normally (default for compatibility reasons, see bug 141641) False: Send no referring URL		
39	Network_Http_Accept_Default (Network Http Accept Default)	N/A	N/A
	Comma-separated list of MIME types to accept from server. Sent with HTTP requests in Accept header. Default value istext/xml,application/xml,application/xhtml+xml,text/html; q=0.9,text/plain;q=0.8,image/png,*/*;q=0.5. (The space is actually not present and was only inserted to make it wrap.)		
40	Intl_Menuitems_Alwaysappendaccesskeys (Intl Menuitems Alwaysappendaccesskeys)	N/A	N/A
	Specifies URI to determine if access keys are appended to menu items		

41	Network_Proxy_No_-Proxies_On (Network Proxy No Proxies On)	N/A	N/A
	A comma-and-space-delimited list of hosts for which the specified proxies should not be used. (See No proxy for for syntax.) Note: In Firefox, this can be changed via Tools ? Options ? General (Firefox 2.0+: Advanced ? Network) ? Connection Settings... ? Manual proxy configuration ? No Proxy for		
42	Network_Http_Redirection_Limit (Network Http Redirection Limit)	N/A	N/A
	Determines how many consecutive HTTP redirects the browser will follow. Default value is 20. Setting it to 0 will stop all redirects from occuring. Note: These are header-based redirects, not (for example) meta http-equiv=refresh HTML-based redirects.		
43	Network_Idn_Show_-Punycode (Network Idn Show Punycode)	N/A	N/A
	Determines how to display IDN hostnames in the Location Bar (see bug 282270). True (default): All IDN (UTF-8) domain names will be normalized to punycode. False: Display IDN domain names in UTF-8 Note: Addresses may be input as UTF-8 regardless of this setting.		
44	Browser_Cache_Check_-Doc_Frequency (Browser Cache Check Doc Frequency)	N/A	N/A
	How often to check the remote page for a newer version than what might be in the cache 0: Check once per browser session 1: Check every time I view the page 2: Never check (always use cached page) 3 (default): Check when the page is out of date (automatically determined)		
45	Signed_Applets_Codebase_Principal_Support (Signed Applets Codebase Principal Support)	N/A	N/A
	True: Give scripts using codebase principals access advanced scripting capabilities. Setting this preference to true is often used to allow IRC websites to gain access to the OSs clipboard at the expense of a security risk. False (default): Only trusted/signed scripts can access advanced scripting capabilities Note: file: and resource: schemes are considered special and may get extra capabilities regardless of this preferences setting.		
46	Browser_Urlbar_Restrict_History (Browser Urlbar Restrict History)	N/A	N/A
	Returns only results that are from the browsers history.		

47	Network_Ftp_Idleconnectiontimeout (Network Ftp Idleconnectiontimeout)	N/A	N/A
	Time in seconds until an idle FTP connection is dropped. Default value is 300.		
48	Plugin_Override_Internal_Types (Plugin Override Internal Types)	N/A	N/A
	True: Allow plugins to override internal imglib decoder MIME types in full-page mode False (default): Opposite of the above		
49	Network_Proxy_Socks_Remote_Dns (Network Proxy Socks Remote Dns)	N/A	N/A
	True: Perform all DNS lookups on remote proxy server (see bug 134105) False (default): Perform all DNS lookups client-side		
50	Network_Dns_Disableipv6 (Network Dns Disableipv6)	N/A	N/A
	Determines whether to perform IPv6 name lookups (see bug 68796) True (default in OS X): Do not perform lookups False (default in all others): Opposite of the above		
51	Browser_Tabs_Loaddivertedinbackground (Browser Tabs Loaddivertedinbackground)	N/A	N/A
	Determines behavior of pages normally meant to open in a new window (such as target=_blank or from an external program), but that have instead been loaded in a new tab. True: Load the new tab in the background, leaving focus on the current tab False (default): Load the new tab in the foreground, taking the focus from the current tab. Note: Setting this preference to True will still bring the browser to the front when opening links from outside the browser. Note: target=_new creates/reuses a window named _new and is frequently used by Google. target=_blank loads the designated document in a new, unnamed window [[1]].		
52	Network_Dir_Format (Network Dir Format)	N/A	N/A
	How to format directory listings (e.g., from FTP servers) 1: Raw - exactly what comes off the network 2 (default): HTML 3: application/http-index-format (requires code to parse/display that is not present by default in Firefox; it is present in the Mozilla application suite)		
53	Intl_Keyboard_Per_Window_Layout (Intl Keyboard Per Window Layout)	N/A	N/A
	True: Allow different windows to retain their own keyboard locale settings (see bug 186549) False (default): Opposite of the above		

54	Privacy_Popups_Policy (Privacy Popups Policy)	N/A	N/A
	Determines the popup blocker behavior. 1: Allow popups 2: Reject popups Note: Seems to be deprecated in favor of dom.disable_open_during_load		
55	Browser_Urlbar_Autofill (Browser Urlbar Autofill)	N/A	N/A
	True: Enables inline autocomplete. False (default): Opposite of above.		
56	Network_Manage_Offline_Status (Network Manage Offline Status)	N/A	N/A
	(Applies to Firefox 3.5 and above) Determines whether Firefox is allowed to automatically set itself to offline mode in response to certain Web sites, or if the network connection is interrupted. (See bug 620472 and this and following messages for more information.) True (implicit default in Firefox 3.5 and 3.6): Allows automatically setting offline mode. False (default in Firefox 4): Prevents automatically setting offline mode. True in SeaMonkey 2.0 and above but SeaMonkey and Thunderbird have a separate offline manager as part of MailNews.		
57	Network_Ntlm_Send_Lm_Response (Network Ntlm Send Lm Response)	N/A	N/A
	Determines whether or not the LM hash will be included in response to a NTLM challenge. Servers should almost never need the LM hash, and the LM hash is what makes NTLM authentication less secure. True: Send the LM hash False (default): Opposite of the above Note: Does not affect network.automatic-ntlm-auth.* settings. See bug 250961 for more information.		
58	Network_Cookie_Lifetimepolicy (Network Cookie Lifetimepolicy)	N/A	N/A
	Determines how browser sets cookie lifetimes. 0 (default): Use supplied lifetime 1: Ask before accepting 2: Accept for session only 3: Cookies last for the number of days specified in network.cookie.lifetime.days Note: In Firefox, this can be changed via Tools ? Options ? Privacy ? Cookies ? Keep Cookies: (Firefox 1.5 and below) or via Tools ? Options ? Privacy / Cookies ? Keep until: (Firefox 2).		
59	Network_Standard_Url_Escape_Utf8 (Network Standard Url Escape Utf8)	N/A	N/A
	Determines whether URLs with UTF-8 characters are escaped per the spec True (default): Escape UTF-8 characters False: Send URLs as they are		
60	Browser_Cache_Disk_Enable (Browser Cache Disk Enable)	N/A	N/A
	True (default): Use disk cache, up to capacity specified in browser.cache.disk.capacity False: Disable disk cache (same effect as setting browser.cache.disk.capacity to 0)		

61	View_Source_Editor_External (View Source Editor External)	N/A	N/A
	True: The program defined in view_source. editor. path should be used when View Source is requested. False (default): The internal viewer should be used when View Source is requested.		
62	Network_Dnscacheentries (Network Dnscacheentries)	N/A	N/A
	Determines the maximum number of entries to keep in the DNS cache. Default value is 20.		
63	Security_Directory (Security Directory)	N/A	N/A
	Seemingly unused.		
64	Dom_Popup_Maximum (Dom Popup Maximum)	N/A	N/A
	The maximum number of simultaneously open popup windows. Default value is 20.		
65	Network_Cookie_Cookiebehavior (Network Cookie Cookiebehavior)	N/A	N/A
	Determines how the browser should handle cookies. 0 : Enable all cookies (default) 1: Allow cookies from originating server only 2: Disable all cookies 3: Use P3P policy to decide (Mozilla Suite/SeaMonkey only) Note: In Firefox, this can be changed via Tools ? Options ? Privacy ? Cookies ? Allow sites to set cookies / for the originating web site only (Firefox 1.5 and below) or Tools ? Options ? Privacy / Cookies ? Accept cookies from sites (Firefox 2); or, in Mozilla Suite/SeaMonkey, via Edit - Preferences - Privacy & Security - Cookies / Cookie Acceptance Policy. Note: The option to limit cookies to the originating server was removed from the UI in Firefox 2.		
66	Network_Http_Accept_Encoding (Network Http Accept Encoding)	N/A	N/A
	Comma-separated list of encoding types to accept from server. Sent with HTTP requests in Accept-Encoding header. Default value is gzip, deflate. Note: compress is not a supported encoding (see bug 196406).		
67	Network_Proxy_Autoconfig_Url (Network Proxy Autoconfig Url)	N/A	N/A
	The automatic proxy configuration URL used by the browser to determine a proxy server. Used when network.proxy.type is 2. Default value is an empty string. Note: In Firefox, this can be changed via Tools ? Options ? Advanced ? Network (Firefox 1.5 and 1.0.x: General) ? Connection Settings... ? Automatic proxy configuration URL		

68	Extensions_Logging_Enabled (Extensions Logging Enabled)	N/A	N/A
	True: Enables some extra extension system logging (can reduce performance) False (default): Opposite of the above Note: Nightlies only		
69	Network_Proxy_Socks_Version (Network Proxy Socks Version)	N/A	N/A
	Determines which version of SOCKS to use with the server specified in network.proxy.socks. Default value is 5. (The only other valid version is 4.)		
70	Network_Proxy_Share_Proxy_Settings (Network Proxy Share Proxy Settings)	N/A	N/A
	Determines whether to use the same proxy server for all protocols. True: Use one proxy for all protocols False (default): Opposite of the above Note: In Firefox, this can be changed via Tools ? Options ? General (Firefox 2.0+: Advanced ? Network) ? Connection Settings... ? Manual proxy configuration ? Use the same proxy for all protocols		
71	Extensions_Dss_Enabled (Extensions Dss Enabled)	N/A	N/A
	True: Enable dynamic skin (theme) switching. False (default): Require a browser restart when switching themes. Note: Switching themes dynamically is buggy (see bug 226791).		
72	Network_Http_Proxy_Pipelining (Network Http Proxy Pipelining)	N/A	N/A
	Determines whether to use HTTP/1.1 pipelining when a proxy server is configured. True: Enable pipelining False (default): Disable pipelining Note: Pipelining is not well-supported by some servers and proxies. Things may break - use with caution.		
73	Privacy_Sanitize_Sanitizeonshutdown (Privacy Sanitize Sanitizeonshutdown)	N/A	N/A
	True: Perform the Clear Private Data operation when closing the browser (Firefox 1.5 and above only) False (default): Clear Private Data only when asked Note: In Firefox 1.5 and above, this can be changed via Tools ? Options ? Privacy ? Settings...		
74	Network_Online (Network Online)	N/A	N/A
	Indicates whether the user is currently online. Used for enabling/disabling various options in the UI. True (default): User is online False: Opposite of the above		

75	Browser_Urlbar_Restrict_Typed (Browser Urlbar Restrict Typed)	N/A	N/A
	Returns only results that have been typed		
76	Network_Idn_Blacklist_Chars (Network Idn Blacklist Chars)	N/A	N/A
	If a domain name contains any of the characters in this preferences value, display the domain in punycode, overriding network.IDN_show_punycodeand network.IDN.whitelist (see bug 301694). See here for a complete list of characters in the default preference. Note: Firefox 1.5 and above only.		
77	Network_Http_Version (Network Http Version)	N/A	N/A
	Determines which HTTP version to use. Default value is 1.1.		
78	Privacy_Item_Cookies (Privacy Item Cookies)	Similar semantics can be achieved by modifying multiple settings at different zones	Similar semantics can be achieved by modifying multiple settings
	True: Delete all cookies when using the Clear Private Data feature (Firefox 1.5 and above only) False (default): Opposite of the above Note: This can be changed via Tools ? Options ? Privacy ? Settings... (Firefox 1.5) or Tools ? Options ? Privacy / Private Data ? Settings... (Firefox 2.0 and above).		
79	Browser_Underline_Anchors (Browser Underline Anchors)	N/A	N/A
	Determines default text-decoration of anchor elements. True (default): Underlines links False: Opposite of above Note: In Firefox, this can be changed via Tools ? Options ? Content ? Fonts & Colors ? Underline links		
80	Browser_Link_Open_Newwindow_Restriction (Browser Link Open Newwindow Restriction)	N/A	N/A
	Firefox and SeaMonkey only. Source: The Burning Edge. 0 (Default in Firefox 1.0.x and SeaMonkey): Force all new windows opened by JavaScript into tabs. 1: Let all windows opened by JavaScript open in new windows. (Default behavior in IE.) 2 (Default in Firefox 1.5 and above): Catch new windows opened by JavaScript that do not have specific values set (how large the window should be, whether it should have a status bar, etc.) This is useful because some popups are legitimate - it really is useful to be able to see both the popup and the original window at the same time. However, most advertising popups also open in new windows with values set, so beware.		
81	Bidi_Support (Bidi Support)	N/A	N/A
	Select provider of bi-directional support 1 (default): Mozilla 2: OS 3: Disable		

82	Network_Standard_-Url_Encode_Utf8 (Network Standard Url Encode Utf8)	N/A	N/A
	Determines how URLs are encoded and sent True: Always encode and send URLs as UTF-8 False (default in Firefox 1.0.x): Opposite of the above Note: This was True for a short time before Firefox 1.5, causing trouble with some international websites (see bug 284474)		
83	View_Source_Editor_-Path (View Source Editor Path)	N/A	N/A
	Path to the external editor to use for View Source when view_source. editor. external is True. If the path doesnt exist or isnt a program, the internal viewer will always be used.		
84	Network_Proxy_-Failover_Timeout (Network Proxy Failover Timeout)	N/A	N/A
	Determines how long to wait until re-contacting an unresponsive proxy server. Default value is 1800 (30 minutes).		
85	Network_Http_Pipelining (Network Http Pipelining)	N/A	N/A
	Determines whether to use HTTP/1.1 pipelining. True: Enable pipelining False (default): Disable pipelining Note: Pipelining is not well-supported by some servers and proxies. Things may break - use with caution.		
86	Network_Automatic_-Ntlm_Auth_Allow_-Proxies (Network Automatic Ntlm Auth Allow Proxies)	N/A	N/A
	Enable automatic use of the operating systems NTLM implementation to silently authenticate the user with their Windows domain logon with proxy servers. (See Integrated Authentication for more information) True (default): Automatically authenticate with proxy servers False: Prompt for authentication		
87	Network_Http_Proxy_-Version (Network Http Proxy Version)	N/A	N/A
	Determines which HTTP version to use when a proxy server is configured. Default value is 1.1, though 1.0 is recommended for some finnicky proxies (such as the Junkbuster proxy).		

88	Extensions_Dss_Switch-pending (Extensions Dss Switchpending)	N/A	N/A
	True: Non-dynamic theme switch pending a browser restart False (default): Opposite of the above		
89	Profile_Manage_Only_-At_Launch (Profile Manage Only At Launch)	N/A	N/A
	True: Only show the Profile Manager at program launch False (default): Show Profile Manager at any time via menus Note: In Firefox, there is no UI to access the Profile Manager from within the browser		
90	Dom_Allow_Scripts_-To_Close_Windows (Dom Allow Scripts To Close Windows)	N/A	N/A
	Determines which close() operations are legal. True: Any script may close any window False (default): Only windows opened via script may be closed via close().		
91	Network_Negotiate_-Auth_Trusted_Uris (Network Negotiate Auth Trusted Uris)	N/A	N/A
	A comma-and-space-delimited list of sites that are permitted to engage in SPNEGO authentication with the browser. (See Integrated Authenticationfor more information.) Default value is an empty string.		
92	Xpinstall_Whitelist_Add (Xpinstall Whitelist Add)	Similar semantics can be achieved by modifying multiple settings at different zones	Similar semantics can be achieved by modifying multiple settings
	A comma-separated list of sites to automatically add to the extensions whitelist. Default value is update.mozilla.org,addons.mozilla.org but is cleared as soon as the values are added to the whitelist		
93	Network_Negotiate_-Auth_Using_Native_-Gsslib (Network Negotiate Auth Using Native Gsslib)	N/A	N/A
	True (default): Use the GSS lib that comes standard with the host operating system False: Use the GSSAPI library specified in network.negotiate-auth.gsslib.		
94	Network_Dnscache-expiration (Network Dnscacheexpiration)	N/A	N/A
	Determines the maximum number of seconds to cache resolved DNS entries. Default value is 60.		

95	Dom_Popup_Allowed_Events (Dom Popup Allowed Events)	N/A	N/A
	A space-separated list of the events that are allowed to create popups. Default value is change click dblclick mouseup reset submit. A presumably complete list of events from mozilla/content/events/src/nsDOMEvent.cpp:		
96	Privacy_Popups_Usecustom (Privacy Popups Usecustom)	N/A	N/A
	Seemingly unused.		
97	Xpinstall_Enabled (Xpinstall Enabled)	Similar semantics can be achieved by modifying multiple settings at different zones	Similar semantics can be achieved by modifying multiple settings
	True (default): Enables the XPInstall system (i.e., allows extensions to be installed) False: Opposite of the above Note: In Firefox 1.0.x, this can be changed in Tools ? Options ? Web Features ? Allow web sites to install software (UI removed in Firefox 1.5).		
98	Dom_Disable_Image_Src_Set (Dom Disable Image Src Set)	N/A	N/A
	Determines whether scripts may change the .src member of image objects (effectively, whether images can be changed via JavaScript) True: Scripts may not modify .src of images False (default): Opposite of above Note: In Mozilla Suite, this can be changed via Edit ? Preferences ? Advanced ? Scripts & Plug-ins ? Allow scripts to: Change images and, in Firefox 1.0.x, via Tools ? Options ? Web Features ? Enable JavaScript / Advanced ? Allow scripts to: Change images. This option has been removed from the UI in Firefox 1.5 [2]		
99	Dom_Min_Background_Timeout_Value (Dom Min Background Timeout Value)	N/A	N/A
	See the Inactive tabs section of the window.setTimeout methods help.		
100	Security_Xpconnect_Plugin_Unrestricted (Security Xpconnect Plugin Unrestricted)	N/A	N/A
	True (default): Allow scripting of plugins by untrusted scripts False: Opposite of the above		

101	Browser_Cache_Memory_Enable (Browser Cache Memory Enable)	N/A	N/A
	True (default): Use memory cache, up to capacity specified in browser.cache.memory.capacity (if set); otherwise, use a percentage of physical RAM (see bug 105344) False: Disable memory cache (same effect as setting browser.cache.memory.capacity to 0)		
102	Network_Cookie_Lifetime_Days (Network Cookie Lifetime Days)	Similar semantics can be achieved by modifying multiple settings at different zones	N/A
	Determines the number of days to keep cookies if network.cookie.lifetimePolicy is 3. Default value is 90.		
103	Network_Http_Max_Connections (Network Http Max Connections)	N/A	Similar semantics can be achieved by modifying multiple settings
	Determines the maximum number of simultaneous HTTP connections. Default value is 30. Valid values are between 1 and 65535 inclusive.		
104	Network_Http_Request_Max_Start_Delay (Network Http Request Max Start Delay)	N/A	N/A
	Determines amount of time (in seconds) to suspend pending requests, before spawning a new connection, once the limit on the number of persistent connections per host (network.http.max-persistent-connections-per-server) has been reached. However, a new connection will not be created if max-connections (network.http.max-connections) or max-connections-per-server (network.http.max-connections-per-server) has also been reached. Default value is 10.		
105	Network_Negotiate_Auth_Allow_Proxies (Network Negotiate Auth Allow Proxies)	Similar semantics can be achieved by modifying multiple settings at different zones	N/A
	True (default): Allow SPNEGO by default when challenged by a proxy server. (See Integrated Authentication and bug 266485 for more information.) False: Opposite of the above		
106	Browser_Popups_Showpopupblocker (Browser Popups Showpopupblocker)	N/A	N/A
	True (default): Show an icon in the status bar when a popup has been blocked. False: Do not show an icon in the status bar when a popup has been blocked.		

107	Network_Http_Sendrefererheader (Network Http Sendrefererheader)	N/A	N/A
	Determines when to send the Referer HTTP header. 0: Never send the referring URL 1: Send only on clicked links 2 (default): Send for links and images		
108	Browser_Dom_Window_Dump_Enabled (Browser Dom Window Dump Enabled)	N/A	N/A
	True: Enable JavaScript dump() output False: Opposite of the above		
109	Network_Http_Default_Socket_Type (Network Http Default Socket Type)	N/A	N/A
	Determines the socket type to be used for normal HTTP traffic. Default value is an empty string, indicating a normal TCP/IP socket type.		
110	Browser_Cache_Disk_Cache_Ssl (Browser Cache Disk Cache Ssl)	N/A	N/A
	True (default): Cache content received via SSL False: Do not cache content received via SSL Note: See bug 531801 for more information		
111	Network_Dns_Ipv4onlydomains (Network Dns Ipv4onlydomains)	N/A	N/A
	A comma-separated list of domains for which DNS lookups are for IPv4 addresses only (see bug 68796). Default value is .doubleclick.net.		
112	Network_Cookie_Prefsmigrated (Network Cookie Prefsmigrated)	N/A	N/A
	Indicates whether some cookie preferences - previously stored in deprecated preferences - have been migrated to current preferences. True: Consult current preferences for cookie prefs False (default): Read deprecated preferences, update current preferences, then set this preference to true		