Configure advanced IE settings with Group Policy

In this article, I will show you the advanced security settings in IE and do so to best configure them.

In this article, I will show you the advanced security settings in IE and do so to best configure them.

In addition to Microsoft's advancements to IE, such as UAC, Protected Mode, integrity levels, . it seems that there are still misconfiguration for IE, especially after a horrific month of IE. . Not only misconfiguration, there are still some clutter related to Advanced Security advanced security settings available in IE. In this article we will show you what the Advanced Security settings mean and give you a few ways to best configure them.

Where to find advanced security settings

There is some confusion about the security settings in IE that we alluded to, so we will clarify what is still unclear to you. The security settings we talked about are below the **Tools - Internet Options menu** within IE. When you open the Internet Options dialog box, you can click on the **Advanced** tab. Under the Advanced tab, you can scroll down until you see the **Security** option, as shown in Figure 1 below.

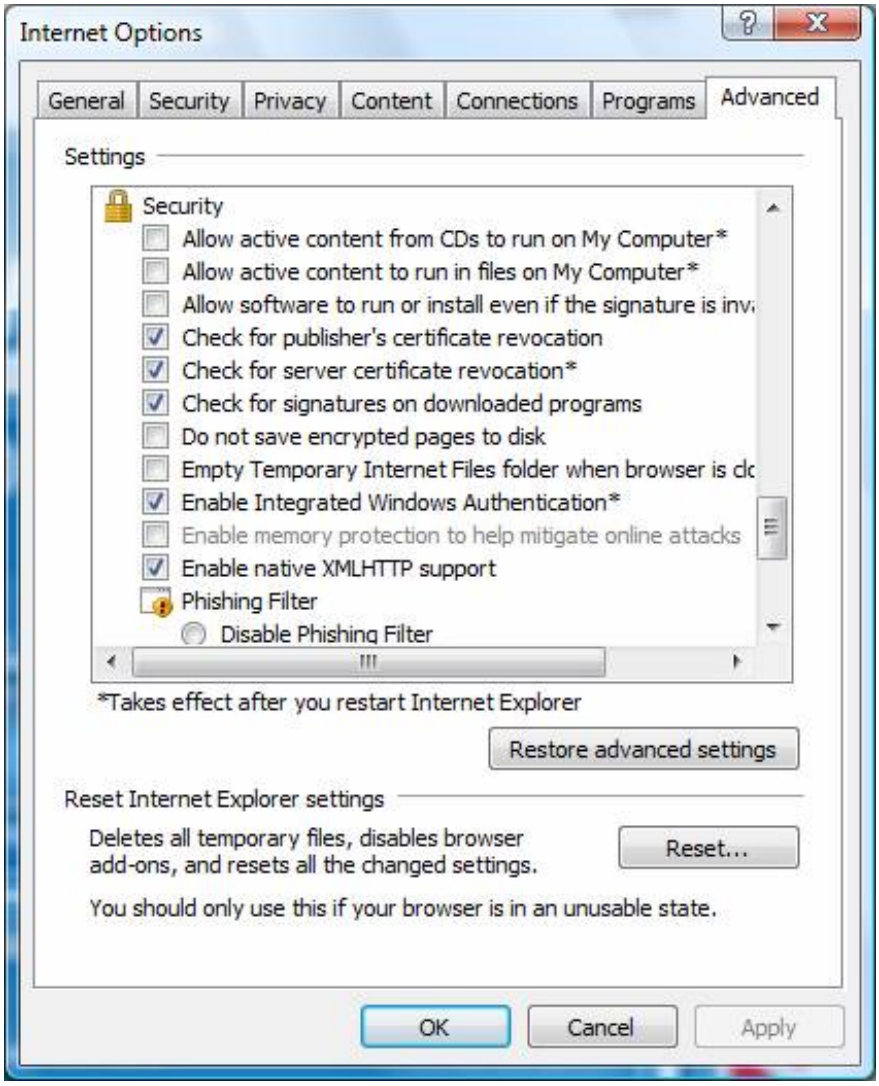

Figure 1: Advanced Security settings for Internet Explorer

Here is a set of settings that we will cover in this article.

Advanced IE settings in GPO

These Advanced Security settings for IE are also introduced in many IE versions through the use of Group Policy. Supported versions of IE include 5, 6, 7 and 8.

For you to access this IE Advanced Security settings using GPO, you need to have Group Policy Preferences (GPP) available. For this feature you must use Windows Server 2008, Vista SP1, 7, or Windows Server 2008 R2.

Once you have installed the GPMC version correctly to be able to view the GPP, you will need to enter the correct policy to install these advanced security settings. To access this policy, you will enter the **User ConfigurationPreferencesControl Panel SettingsInternet Explorer** . From here, you can add policies to all appropriate IE versions.

Specific security settings

Enables content activation from CDs to run on the computer

Content activation includes ActiveX controls and browser add-ons used by many websites. These programs are often locked because they may be malfunctioning or an attacker can perform computer name tasks without your knowledge.

Default: Not selected
Encourage: Do not choose

Enable content activation to run in files on your computer

Just like the previous setup, except from files instead of CDs

Default: Not selected
Encourage: Do not choose

Allows the software to run or install even without a valid signature

Signatures can be combined with certain applications or settings, bind them to the manufacturer. This will keep the app or 'correct' setting and help you detect if the application or installation is fake.

Default: Not selected
Encourage: Do not choose

Check the issuer's certificate cancellation

Usually a certificate needs to be awakened by a private key or expired certificate. This setting will check the certificate on the wake up list before allowing it to be used.

Default certificates: Select
Promotion: Select

Check server certificate revocation

Default: Select
Encourage: Choose

Check the signature on the download program

Usually a certificate needs to be awakened because the private key is compromised or expired. This setting will check the certificate of wake up list before allowing it to be used.

Default: Select
Encourage: Choose

Do not save encrypted pages to disk

If data from an HTTPS website connection is saved on your disk, this is an issue an attacker can take advantage of to access data through the data stored in the Temporary Internet folder. Obviously, it will be more efficient and faster to save this data to disk for later access to the website. However, not storing this encrypted data is safer than allowing it to be saved.

Default: Not selected
Encourage: Choose

Delete the folder containing the temporary files when closing the browser

The directory of temporary files for IE contains a lot of data from the sites you visit. This information is cached on your disk for faster access later if you visit the page again. Even so, worms, viruses and malicious software can also be saved with good website data. Therefore, deleting all files in a certain period is a safer security measure than saving them.

Default: Not selected
Encourage: Choose

Enable DOM storage

Archive DOM (Document Object Model) is designed to provide an easier, safer, and larger way to store information in cookies. DOM is used for programs such as JavaScript to provide dynamic websites and distribute custom web pages to users. This behavior should not be allowed unless the DOM stored for the task on the Internet.

Default: Select
Encourage: Do not choose

Enable authentication of integrated windows

Forcing IE to use Kerberos or NTLM authentication instead of using Basic, Digest or anonymous authentication.

Default: Select
Encourage: Choose

Enable memory protection to help mitigate online attacks
Whether these controls, whether IE uses DEP (Data Execution Protection) or not, will help you protect your computer against applications that have a 'sickness' that can harm your computer.

Default: Not selected
Encourage: Choose

Enable original xmlhttp support

Today is used by many companies as a standard to provide dynamic control of data through multiple websites.

Default: Select
Encourage: Choose

Fake filter

Phishing Filter will break the ability to navigate to and download from known sites that may contain malicious content. It also helps you avoid fake websites and online fraud. The filter collects the website with a list of phony sites that have been reported, collates software downloads with a list of malware, helping you avoid visiting sites that may lead to identity theft.

Default: Disable automatic website checking
Encourage: Enable automatic website checking

Use ssl 2.0

When you connect to a commercial website, such as a bank website or an online sales website, Internet Explorer will use a secure connection (connecting using Secure Sockets Layer (SSL) technology.)) to encrypt the session. This encryption is based on a certificate to provide Internet Explorer with the information needed for secure communication with the website. Certificates also identify the website, its owner or company.

Default: Not selected
Encourage: Do not choose

Use ssl 3.0

Similar to using SSL 2.0, however this is newer technology.

Default: Select
Encourage: Choose

Use tls 1.0

TLS (Transport Layer Security) 1.0 is used when visiting SSL websites to protect and encrypt data and connect.

Default: Select
Encourage: Choose

Use tls 1.1

TLS (Transport Layer Security) 1.1 is used when visiting SSL websites to protect and encrypt data and connect. Only allowed on the condition that you know those websites support this TLS version.

Default: Not selected
Encourage: Do not choose

Use tls 1.2

TLS (Transport Layer Security) 1.2 is used when visiting SSL websites to protect and encrypt data and connect. Allow only if you know websites that support this TLS version.

Default: Not selected
Encourage: Do not choose

Warning about certificate type errors

Provide alerts when certificate for a website

Default: Select
Encourage: Choose

Warning if there is a change between security and non-security mode

If a website has both HTTP and HTTPS links, or you are taken from an HTTPS site to an unsafe site or HTTP, then you will be warned.

Default: Not selected
Encourage: Choose

Warning if POST is sent indirectly to an area that does not allow posting

Warning if you are working on a form on the Internet can send you to a different address than the address hosting the form. This will prevent your information or browser from being sent to an unsafe site.

Default: Select
Encourage: Choose

Conclude

Advanced Security for IE security features are very detailed and can help you protect your desktops as well as the entire network, avoiding attacks and security holes. Using them correctly can make your computer safer from a machine that lacks security and safety measures. Leverage Group Policy can configure these settings for

versions 5, 6, 7, and 8, making this solution effective.

You finished reading the article "**Configure advanced IE settings with Group Policy**" edited by the **TipsMake** team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.
