SECMON1

Information Security Guideline

User Application Hardening

THIS PAGE INTENTIONALLY LEFT BLANK

While useful for many business operations, applications like Flash, Java, Adobe Acrobat and certain features in Microsoft Office (e.g. OLE), can allow malware or intruders to enter your network. Disabling these applications and blocking online ads can remove any opportunity for adversaries to exploit these potentially disruptive tools. If your organisation uses these applications, you can restrict which users may access them.

In the SECMON1 blog post 'Security Overview - Information Security Essentials', we spoke about what application hardening is and why it is an essential security measure.

In this document we are going to provide some basic application hardening steps and provide you with some interesting and important links where you can educate yourself further on this topic and discuss other available options.

Implementation Guidance

Focus on hardening the configuration of applications used to interact with content from the Internet. For web browsers, disallow Adobe Flash (ideally uninstall it), ActiveX, Java, Silverlight and QuickTime for Windows. Whitelist trustworthy websites that require such web browser functionality for a specific business purpose. Note that some web browsers have an embedded version of Flash.

Ideally uninstall Flash, since simply disabling Flash in the web browser won't provide adequate protection.

Disallowing JavaScript, except for whitelisted websites (those that are known to be good ad trusted by you), is ideal though challenging due to the large number of websites that require such functionality for legitimate purposes, and is difficult to implement in a large-scale deployment.

Configure Microsoft Office to disable activation of object linking and embedding (OLE) packages; see Microsoft *Where's the macro? Malware authors are now using OLE embedding to deliver malicious files*.

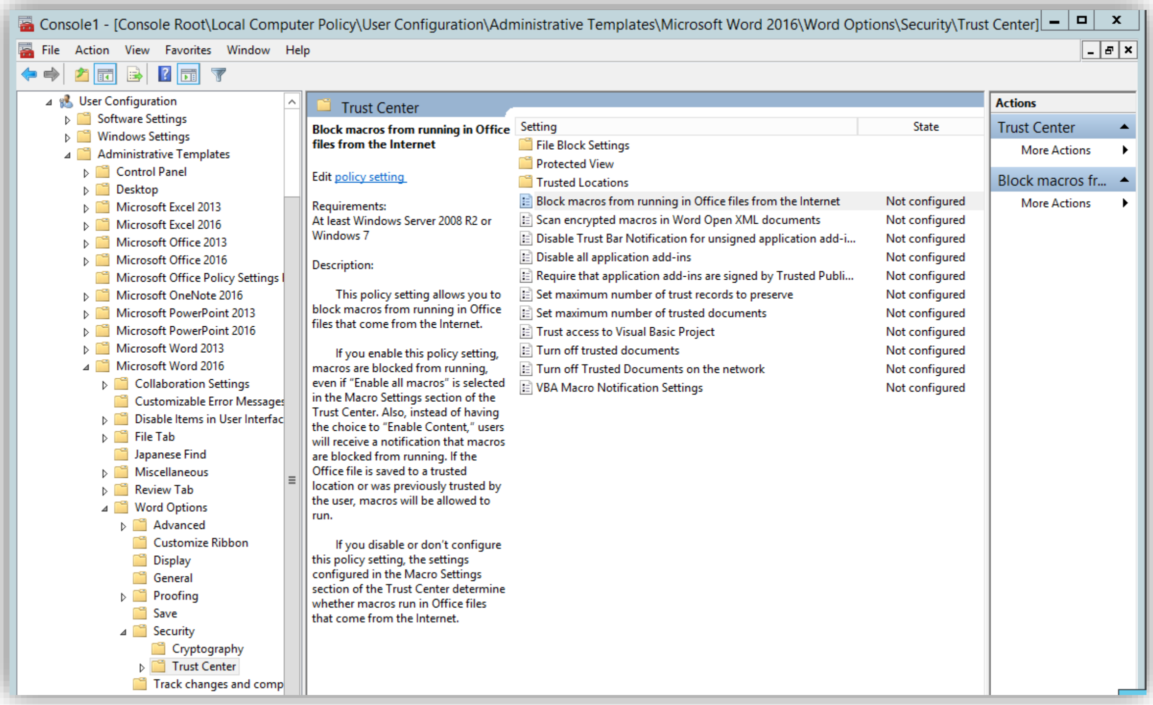
Further information

Further guidance, including applicability for non-Windows operating systems, is available at ASD Strategies to Mitigate Cyber Security Incidents.

How-To Guide

Using Group Policy for Hardening Microsoft Office 2013 via Server 2008

1. Download the Group Policy Administrative Templates for Microsoft Office 2013 here.
    a. Once downloaded, the ADMX and associated ADML files can be placed in **C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions** on the Domain Controller and they will be automatically loaded into the Group Policy Management Editor (gpmc.msc)
2. Either press the Windows logo key +R to open the **RUN** dialog box or click **Start**, click **All Programs**, click **Accessories**, then click **Run**.
3. Type **gpmc.msc** in the text box, and then click **OK** or press **ENTER**. This opens the **Group Policy Management Console/Editor**
4. In the **Group Policy Management Editor**, go to **User Configuration**
5. The directory structure should be similar to the screen below



Console1 - [Console Root\Local Computer Policy\User Configuration\Administrative Templates\Microsoft Word 2016\Word Options\Security\Trust Center]

Trust Center

Block macros from running in Office files from the Internet

Edit policy setting

Requirements:
At least Windows Server 2008 R2 or Windows 7

Description:

This policy setting allows you to block macros from running in Office files that come from the Internet.

If you enable this policy setting, macros are blocked from running, even if "Enable all macros" is selected in the Macro Settings section of the Trust Center. Also, instead of having the choice to "Enable Content," users will receive a notification that macros are blocked from running. If the Office file is saved to a trusted location or was previously trusted by the user, macros will be allowed to run.

If you disable or don't configure this policy setting, the settings configured in the Macro Settings section of the Trust Center determine whether macros run in Office files that come from the Internet.

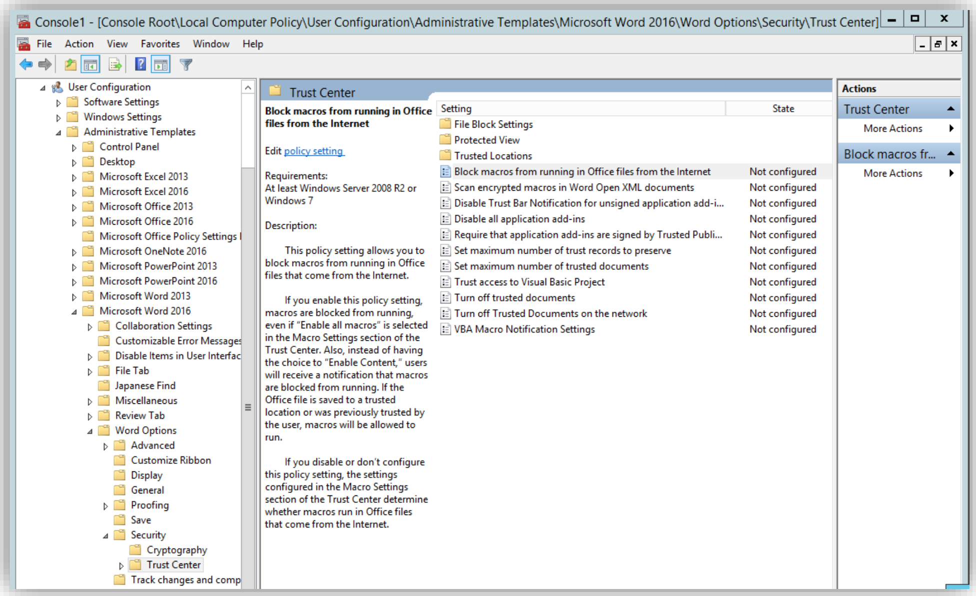
Setting	State
File Block Settings	
Protected View	
Trusted Locations	
Block macros from running in Office files from the Internet	Not configured
Scan encrypted macros in Word Open XML documents	Not configured
Disable Trust Bar Notification for unsigned application add-i...	Not configured
Disable all application add-ins	Not configured
Require that application add-ins are signed by Trusted Publi...	Not configured
Set maximum number of trust records to preserve	Not configured
Set maximum number of trusted documents	Not configured
Trust access to Visual Basic Project	Not configured
Turn off trusted documents	Not configured
Turn off Trusted Documents on the network	Not configured
VBA Macro Notification Settings	Not configured

For information on the different group policy settings you can configure, please go here.

Using Group Policy for Hardening Microsoft Office 2013 via Server 2012

1. Download the Group Policy Administrative Templates for Microsoft Office 2013 here.
    a. Once downloaded, the ADMX and associated ADML files can be placed in **C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions** on the Domain Controller and they will be automatically loaded into the Group Policy Management Editor (gpmc.msc)

2. On the **Start** screen, click the **Apps** arrow.
3. On the **Apps** screen, type **gpmc.msc** and then click **OK** or press **ENTER**
4. In the **Group Policy Management Editor**, go to **User Configuration**
5. The directory structure should be similar to the screen below



Console1 - [Console Root\Local Computer Policy\User Configuration\Administrative Templates\Microsoft Word 2016\Word Options\Security\Trust Center]

Block macros from running in Office files from the Internet

Edit policy setting

Requirements:
At least Windows Server 2008 R2 or Windows 7

Description:

This policy setting allows you to block macros from running in Office files that come from the Internet.

If you enable this policy setting, macros are blocked from running, even if "Enable all macros" is selected in the Macro Settings section of the Trust Center. Also, instead of having the choice to "Enable Content," users will receive a notification that macros are blocked from running. If the Office file is saved to a trusted location or was previously trusted by the user, macros will be allowed to run.

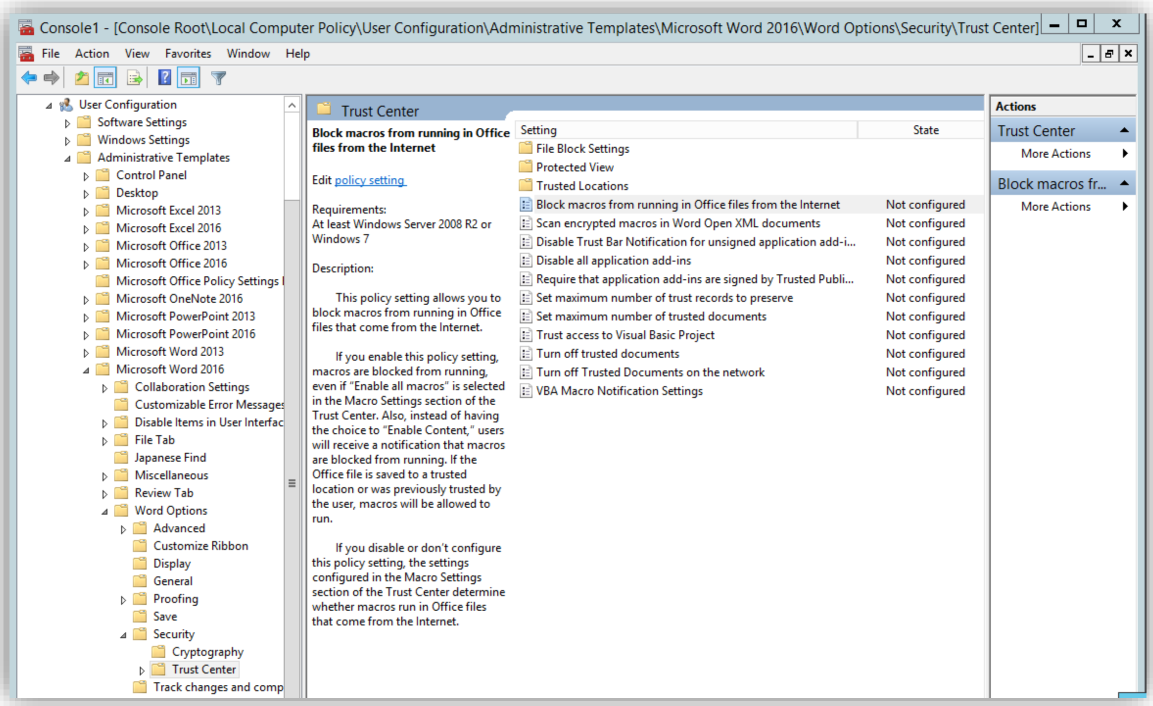
If you disable or don't configure this policy setting, the settings configured in the Macro Settings section of the Trust Center determine whether macros run in Office files that come from the Internet.

Setting	State
File Block Settings	
Protected View	
Trusted Locations	
Block macros from running in Office files from the Internet	Not configured
Scan encrypted macros in Word Open XML documents	Not configured
Disable Trust Bar Notification for unsigned application add-i...	Not configured
Disable all application add-ins	Not configured
Require that application add-ins are signed by Trusted Publi...	Not configured
Set maximum number of trust records to preserve	Not configured
Set maximum number of trusted documents	Not configured
Trust access to Visual Basic Project	Not configured
Turn off trusted documents	Not configured
Turn off Trusted Documents on the network	Not configured
VBA Macro Notification Settings	Not configured

For information on the different group policy settings you can configure, please go here.

Using Group Policy for Hardening Microsoft Office 2016 via Server 2008

1. Download the Group Policy Administrative Templates for Microsoft Office 2016 here.
    a. Once downloaded, the ADMX and associated ADML files can be placed in **C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions** on the Domain Controller and they will be automatically loaded into the Group Policy Management Editor (gpmc.msc)
2. Either press the Windows logo key +R to open the **RUN** dialog box or click **Start**, click **All Programs**, click **Accessories**, then click **Run**.
3. Type **gpmc.msc** in the text box, and then click **OK** or press **ENTER**. This opens the **Group Policy Management Console/Editor**
4. In the **Group Policy Management Editor**, go to **User Configuration**
5. The directory structure should be similar to the screen below



Block macros from running in Office files from the Internet

Edit policy setting

Requirements:
At least Windows Server 2008 R2 or Windows 7

Description:

This policy setting allows you to block macros from running in Office files that come from the Internet.

If you enable this policy setting, macros are blocked from running, even if "Enable all macros" is selected in the Macro Settings section of the Trust Center. Also, instead of having the choice to "Enable Content," users will receive a notification that macros are blocked from running. If the Office file is saved to a trusted location or was previously trusted by the user, macros will be allowed to run.

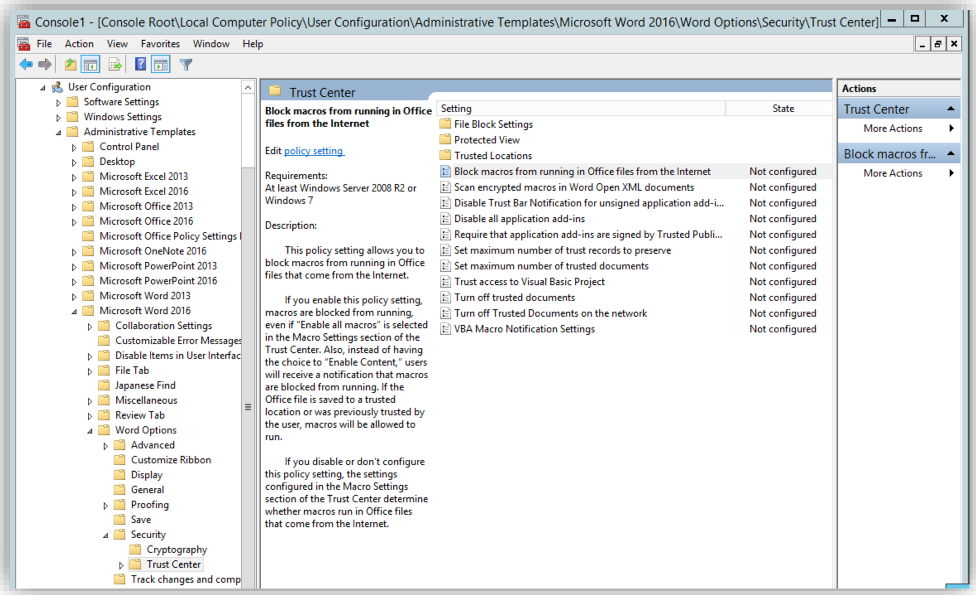
If you disable or don't configure this policy setting, the settings configured in the Macro Settings section of the Trust Center determine whether macros run in Office files that come from the Internet.

Setting	State
File Block Settings	
Protected View	
Trusted Locations	
Block macros from running in Office files from the Internet	Not configured
Scan encrypted macros in Word Open XML documents	Not configured
Disable Trust Bar Notification for unsigned application add-i...	Not configured
Disable all application add-ins	Not configured
Require that application add-ins are signed by Trusted Publi...	Not configured
Set maximum number of trust records to preserve	Not configured
Set maximum number of trusted documents	Not configured
Trust access to Visual Basic Project	Not configured
Turn off trusted documents	Not configured
Turn off Trusted Documents on the network	Not configured
VBA Macro Notification Settings	Not configured

For information on the different group policy settings you can configure, please go here.

Using Group Policy for Hardening Microsoft Office 2016 via Server 2012

6. Download the Group Policy Administrative Templates for Microsoft Office 2016 here.
   a. Once downloaded, the ADMX and associated ADML files can be placed in **C:\Windows\SYSVOL\domain\Policies\PolicyDefinitions** on the Domain Controller and they will be automatically loaded into the Group Policy Management Editor (gpmc.msc)
7. On the **Start** screen, click the **Apps** arrow.
8. On the **Apps** screen, type **gpmc.msc** and then click **OK** or press **ENTER**
9. In the **Group Policy Management Editor**, go to **User Configuration**
10. The directory structure should be similar to the screen below



Console1 - [Console Root\Local Computer Policy\User Configuration\Administrative Templates\Microsoft Word 2016\Word Options\Security\Trust Center]

Trust Center

Block macros from running in Office files from the Internet

Edit policy setting

Requirements:
At least Windows Server 2008 R2 or Windows 7

Description:

This policy setting allows you to block macros from running in Office files that come from the Internet.

If you enable this policy setting, macros are blocked from running, even if "Enable all macros" is selected in the Macro Settings section of the Trust Center. Also, instead of having the choice to "Enable Content," users will receive a notification that macros are blocked from running. If the Office file is saved to a trusted location or was previously trusted by the user, macros will be allowed to run.

If you disable or don't configure this policy setting, the settings configured in the Macro Settings section of the Trust Center determine whether macros run in Office files that come from the Internet.

Setting	State
File Block Settings	
Protected View	
Trusted Locations	
Block macros from running in Office files from the Internet	Not configured
Scan encrypted macros in Word Open XML documents	Not configured
Disable Trust Bar Notification for unsigned application add-i...	Not configured
Disable all application add-ins	Not configured
Require that application add-ins are signed by Trusted Publi...	Not configured
Set maximum number of trust records to preserve	Not configured
Set maximum number of trusted documents	Not configured
Trust access to Visual Basic Project	Not configured
Turn off trusted documents	Not configured
Turn off Trusted Documents on the network	Not configured
VBA Macro Notification Settings	Not configured

For information on the different group policy settings you can configure, please go here.

Minimising the Threat from Java-Based Intrusions

Java applications are widely used to perform necessary business functions. The Java platform consists of the Java Virtual Machine (JVM), which is installed on the host computer, and user applications that are written using the Java programming language. Java applications can be used in a web browser (applet) or launched outside the browser (Java Web Start application).

Software patches typically address security issues or add new features. Unfortunately, sometimes the updates to the JVM may cause compatibility issues with existing Java applications, which may stop working correctly. Organisations tend to avoid updating Java because of continued reliance on legacy applications, which opens their network up to security vulnerabilities. Patching is a recommended part of a defence-in-depth approach to security.

Exploitation of Java-based vulnerabilities in the JVM is mostly associated with visiting a malicious or compromised website or by opening an infected email or attachment. This can allow the adversary to gain the same level of access as the user or even higher (Administrator access).

How Can Java Be Used

1. Gather requirements and use cases for Java. Use cases need to address which applications need to be run and the degree of trust associated with each

    a. For example, a user interface for an internal database developed in-house would be necessary for database access and have a high level of trust. An application from the Internet to view video files will have both a low business use and a low trust level

2. Recommended mitigations against Java intrusions include, but are not limited to:
    a. Using Deployment Rule Sets to whitelist Java applications
    b. Applying security patches
    c. Permitting use of Java applications from trusted sources only
    d. Content filtering at the gateway
    e. Configuring separate browsers for internal and external use

Using Deployment Rule Sets to Whitelist Java Applications

Application whitelisting allows system administrators to control applications and the context in which they are run.

A security feature added in Oracle Java 7 Update 40 is Deployment Rule Sets, which allows administrators to whitelist Java applications based on attributes like location, file hash or signature hash. Deployment rules can be used to only permit Java applications from trusted sources, with greater control than other methods. Signature hash is a powerful way to identify and verify applications from trusted sources.

Deployment rules also allow administrators to specify the version of Java that is required to run any particular application. This can maintain compatibility of vital applications without compromising security. For example, an agency needs archived records from an old database that can only be accessed using a Java application that runs reliably on Java 5, but not any newer versions. A deployment rule is created that runs the legacy application in Java 5, but forces all other applications to run in the latest secure version.

Applying Security Patches

Install vendor-supplied Java security patches to protect systems against exploitation of known vulnerabilities. Many adversaries rely on unpatched software and can be stopped by installing security updates.

Please see the SECMON1 Guide to Patching Applications for more info.

Permitting Use of Java Applications from Trusted Sources Only

Allow Java applications to run only from trusted sources, such as the corporate intranet or absolutely trusted Internet domains (e.g., those of partners or suppliers).

Signed Java applications can run with a high privilege level by asking for user consent. Only trusted signing certificates should be entitled to this level of privilege.

Trusted domains can be configured in the Web browser, at the gateway or using Deployment Rule Sets (mentioned above).

a. Web browser-based controls work effectively when used with separate browsers (see information in the next section)
b. To control trusted domains at the gateway, consult your gateway vendor documentation. This can be used in conjunction with content filtering at the gateway (see information in section regarding Content Filtering at the Gateway)
c. Deployment Rule Sets are the most flexible way of configuring both trusted source and trusted code-signing certificates

Configuring Separate Browsers for Internal and External Use

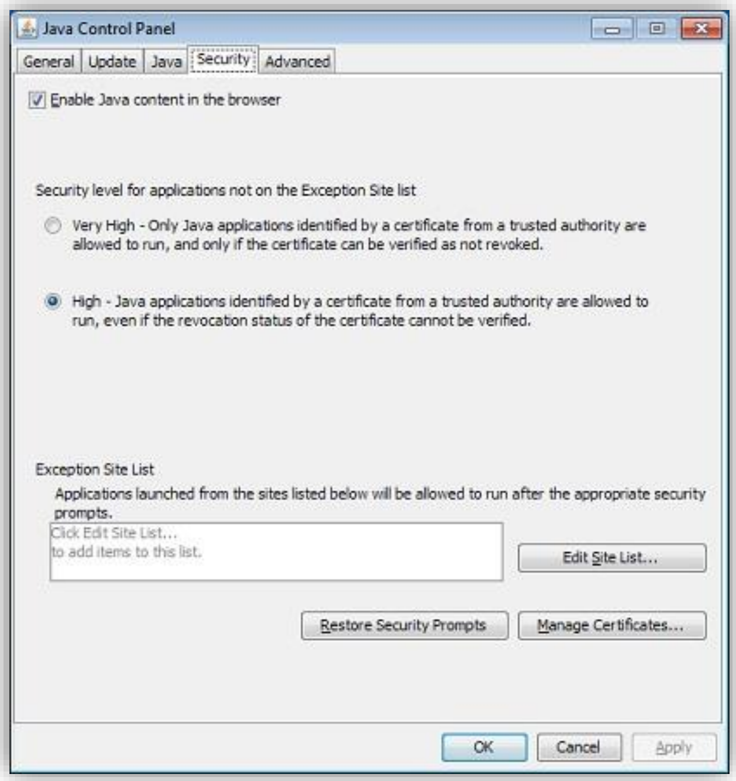
Different browsers can be configured for use with internal (intranet) and external (Internet) sites. Use of separate browsers is simple, but can effectively control use of Java applications.

You can configure the external browser to block or heavily restrict Java. If Java from external sites is required, then this browser should be configured to only allow Java from trusted sources. Untrusted websites should still be controlled or blocked.

Disabling Java Through the Java Control Panel

Directions to find the Java Control Panel for the different versions and different Windows operating systems can be found here.

Directions to find the Java Control Panel in Mac OS can be found here.



☑ Enable Java content in the browser

Security level for applications not on the Exception Site list

○ Very High - Only Java applications identified by a certificate from a trusted authority are allowed to run, and only if the certificate can be verified as not revoked.

● High - Java applications identified by a certificate from a trusted authority are allowed to run, even if the revocation status of the certificate cannot be verified.

Exception Site List

Applications launched from the sites listed below will be allowed to run after the appropriate security prompts.

Click Edit Site List...
to add items to this list.

Note: Screen shows Java Control Panel for Java 7 Update 11

1. In the Java Control Panel, click on the **Security** tab.
2. **Deselect** the check box for **Enable Java content in the browser**. This will disable the Java plug-in in the browser.
3. Click **Apply**. When the Windows User Account Control (UAC) dialog appears, allow permissions to make the changes.
4. Click **OK** in the Java Plug-in confirmation window.
5. Restart the browser for changes to take effect.

Disabling Java Content via Browser

1. Internet Explorer
   a. The only way to completely disable Java in Internet Explorer (IE) is to disable Java through the Java Control Panel (see instructions above)
2. Chrome
   a. Starting with Chrome version 42 (released April 2015), Chrome has disabled the standard way in which browsers support plugins. More info here.
3. Firefox
   a. From the Firefox menu, select **Tools**, then click the **Add-ons** option
   b. In the Add-ons Manager window, select **Plugins**

   c. Click **Java ™ Platform** plugin to select it
   d. Click **Disable** (if the button displays "Enable" then Java is already disabled)
4. Safari
   a. Choose Safari **Preferences**
   b. Choose the **Security** option
   c. Select **Allow Plug-ins**, then click on **Manage Website Settings**
   d. Click on the Java item, select **Block** from the pulldown list **When visiting other websites**
   e. Click **Done**, then close the Safari Preferences window

Content Filtering at the Gateway

Java content delivery can be controlled using a proxy or web content filtering device. Such devices can be configured to refuse outgoing requests for Java content, based on URL file extension or MIME type. Restriction of trusted sources can be implemented by creating exceptions for trusted domains. For example, a proxy can be configured to drop all requests for Java file extensions, unless the request is for the local intranet address range or all domains within a trusted domain, in which case the request will be allowed.

Some examples of web proxy devices come from vendors like Cisco and Symantec. Microsoft also has instructions for deploying a gateway server here.

Final Note

We at SECMON1 are available to review your application settings with you and advise on troubleshooting as well as potential improvements and solutions. We are also available to implement application hardening for your company.

Please feel free to visit our website at www.secmon1.com

You can also reach us by phone at 1300 410 900 or by e-mail at contact@secmon1.com