New Zealand

National Cyber Security Centre

Application Whitelisting

With

Microsoft Applocker

June 2012 V1.0.5

Application Whitelisting with Microsoft Applocker

Cyber Security Plan

As outlined in the New Zealand Cyber Security Plan (CSP), crown entities are currently working to adopt the top 4 of the top 35 mitigations identified by the Australian Defence Signals Directorate's (DSD) research into reported incidents. Full details of the top 35 mitigation strategies can be found here: http://www.dsd.gov.au/infosec/top35mitigationstrategies.htm

Specifically, the top 4 threat mitigation strategies being implemented in the first phase of the CSP are:

- Patching all applications employed by agencies.
- Patching operating system vulnerabilities
- Minimising users with administrative account privileges on networks
- Application whitelisting to prevent the execution of unauthorised programmes.

Application whitelisting is one of the best available protections against malware. This document aims to outline how this affordable, highly efficient anti-malware protection can be utilised whilst maintaining minimal oversight costs.

Disclaimer

The use of Applocker is not NCSC or GCSB policy. This document is intended as a reference / guideline for configuration and management of Applocker. NCSC accepts no liability or responsibility to any person or organisation as a consequence of any loss or any other issues that may arise while using this document. The users of this document are recommended to use a test environment which is able to be recovered or rebuilt in the unlikely event of issues.

While this publication is accurate to the best of our knowledge, NCSC does not accept any responsibility for errors or omissions. You are advised to ensure that you have the most current information available. NCSC will not be liable for any loss or damage caused, arising from or in connection with the use of information contained in this publication. Any reference in this publication to any commercial product, process or service does not constitute or imply its endorsement or recommendation by NCSC. Views and opinions in this publication may not be used for advertising or product endorsement purposes.

Overview

The origins of Software Restriction Policies date back to Server 2000 and XP: "*Software Restriction Policies (SRP), in Windows XP and Windows Vista, gave IT administrators a mechanism to define and enforce application control policies. However, SRP could become a management burden in a very dynamic desktop environment where applications were installed and updated on a constant basis because the application control policies predominantly used hash rules. With hash rules, a new hash rule needs to be created every time an application is updated.*" [1]

The US National Security Agency (NSA) produced a guide on general application whitelisting using SRP in 2010. The NSA guide is available here: http://www.nsa.gov/ia/_files/os/win2k/Application_Whitelisting_Using_SRP.pdf

Initial adoption of whitelisting by using SRP was limited, as initial versions required significant effort to maintain whitelisted applications and patching requirements.

Applocker is a revision of earlier versions of SRP, and was released as a new feature available in Windows 7 Enterprise, Windows 7 Ultimate, and server 2008R2, and was designed to streamline application whitelisting.

Applocker – An Overview

Applocker provides a "4x3" approach to protection. It can be set to protect four primary file types; executable, script, DLL file types and Microsoft Install (MSI) files, and is capable of providing three protection types; Signed, Hashes and Path protections.

[1] http:/technet.microsoft.com/en-us/library/dd548340(v=ws.10).aspx

File types:

- Executable
- Script
- DLL
- Microsoft Install Files (MSI)

Protection types:

- Signed(Primary feature)
- Hashes
- Path

Important: By default DLL protection is not enabled - it must be enabled manually upon setup. Enabling DLL protection is pivotal in realising the security gains of whitelisting, as a significant portion of the malicious code found in the cyber environment, is distributed as DLL.

Limitations

There are some limitations to Applocker, as whitelisting is performed while loading controlled files from media (such as disk) to memory, but does not perform whitelisting protection when injecting controlled files directly into memory, as is often seen during exploitation.

Applocker Management Tools

Applocker employs standard Microsoft management tools which many system administrators will be familiar with:

- Group Edit; gpedit.msc which is used to manage the rules
- Event viewer; eventvwr.msc which is used to monitor logs

As an additional streamlining practise, it is also recommended that system administrators configure event logs to be sent to a Syslog server to allow centralised log management and alerting.

While this publication is accurate to the best of our knowledge, NCSC does not accept any responsibility for errors or omissions. You are advised to ensure that you have the most current information available. NCSC will not be liable for any loss or damage caused, arising from or in connection with the use of information contained in this publication. Any reference in this publication to any commercial product, process or service does not constitute or imply its endorsement or recommendation by NCSC. Views and opinions in this publication may not be used for advertising or product endorsement purposes.

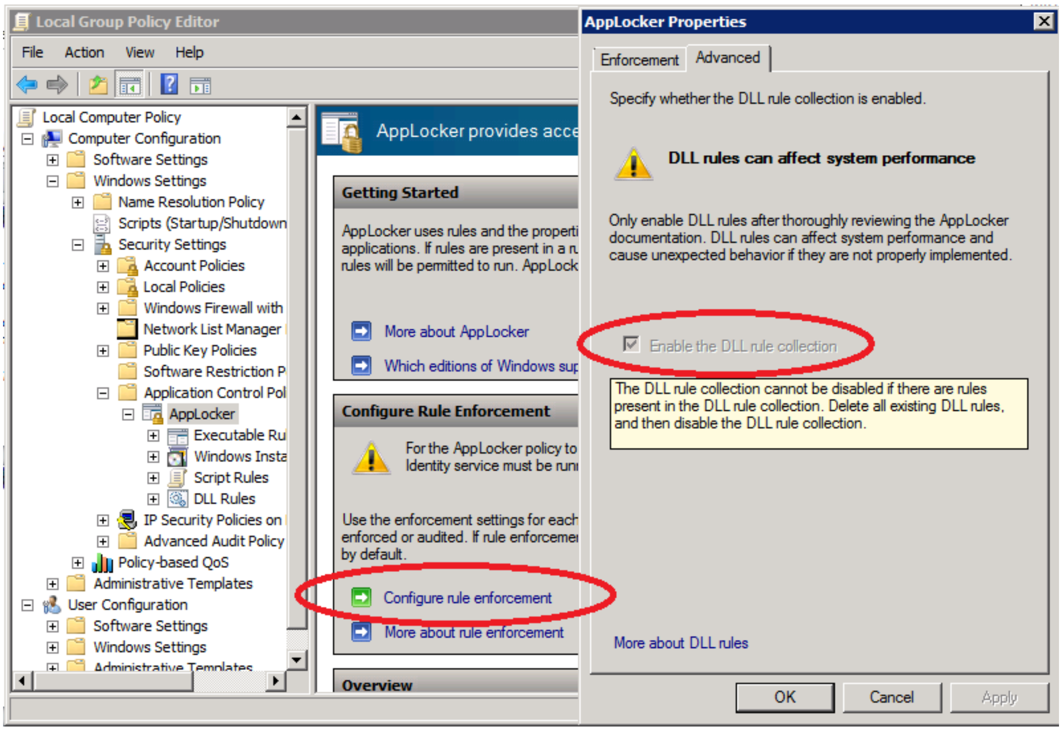
Getting Started

This section will demonstrate an example of how a set up and configure Applocker.

Step 1 - Enabling DLL Protection

To recognise the protection benefits offered by Applocker, it is important as a first step to enable DLL protection. To do so;

1. Start gpedit (Start/(in search) gpedit.msc). *You will need administrator rights to run gpedit* (Ctrl right-click and select run as Administrator).
2. Navigate to “Computer Configuration/Windows Settings/Security Settings/Application Control Policies/Applocker/Configure rule enforcement”. *This will open the “Applocker Properties” window.*
3. Select the “Advanced” tab.
4. Select “Enable DLL rule collection”.
5. Click “Apply”.



AppLocker uses rules and the properti applications. If rules are present in a ru rules will be permitted to run. AppLock

For the AppLocker policy to Identity service must be runi

Use the enforcement settings for each enforced or audited. If rule enforceme by default.

Specify whether the DLL rule collection is enabled.

DLL rules can affect system performance

Only enable DLL rules after thoroughly reviewing the AppLocker documentation. DLL rules can affect system performance and cause unexpected behavior if they are not properly implemented.

☑ Enable the DLL rule collection

The DLL rule collection cannot be disabled if there are rules present in the DLL rule collection. Delete all existing DLL rules, and then disable the DLL rule collection.

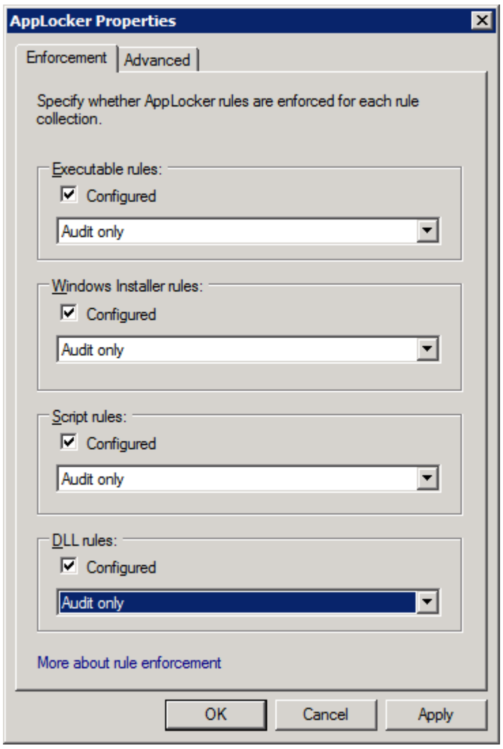
Step 2 - Enable Enforcement

Following on from the previous step, whilst in Applocker Properties, auditing should be enabled;

1. Select the tab Enforcement

   For all rule types, enable "Configured"
2. Select "Audit only"

   For all rule types, select Audit only.
3. Click OK to apply and close the Properties.



Specify whether AppLocker rules are enforced for each rule collection.

Executable rules:
☑ Configured
Audit only

Windows Installer rules:
☑ Configured
Audit only

Script rules:
☑ Configured
Audit only

DLL rules:
☑ Configured
Audit only

The above picture shows an example of enabled rule sets configured for Audit only.

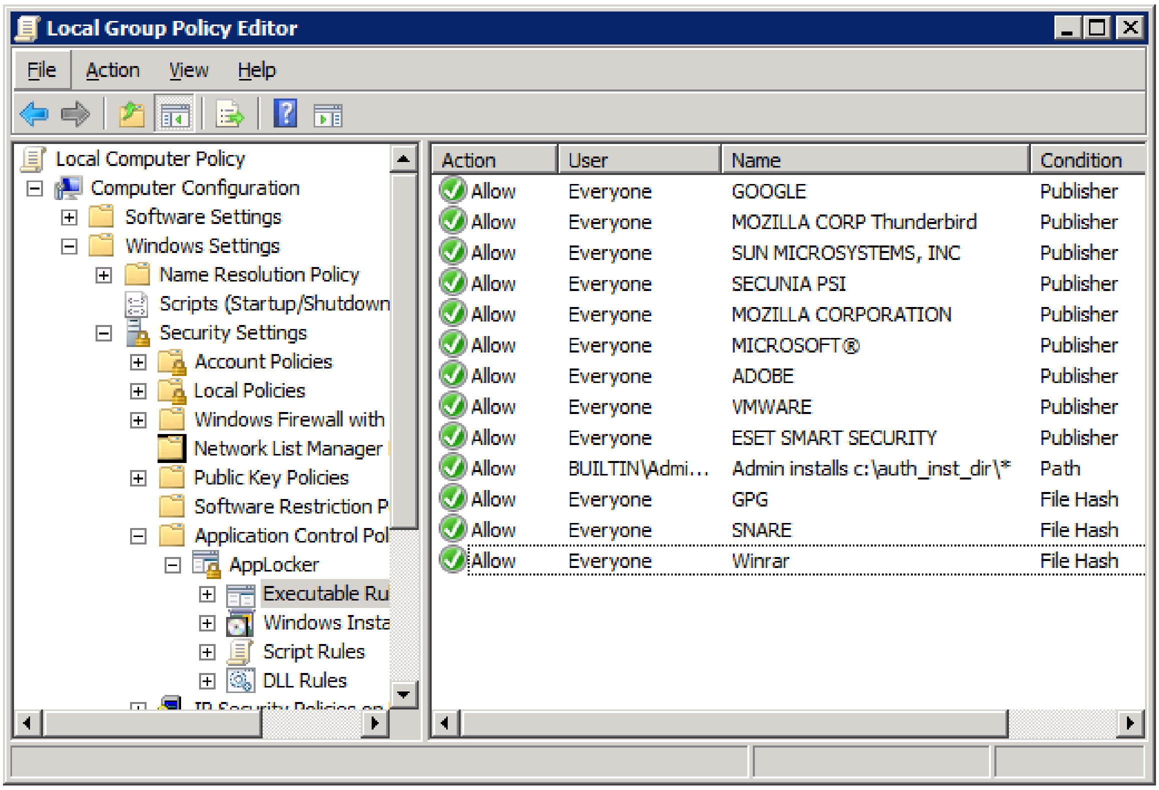
Important:: You should always start with Audit and test your rules before fully enabling enforcement or you may lock yourself out of Windows.

Example of Executable Rules

This section aims to provide an easy to implement and administer Applocker configuration, which will focus on approved software publishers rather than approved/whitelisted individual applications. As a result, most of the rule examples provided are geared towards whitelisting rules by "publisher".

The example below demonstrates a whitelisting setup focused on a publisher oriented rule set:

While this publication is accurate to the best of our knowledge, NCSC does not accept any responsibility for errors or omissions. You are advised to ensure that you have the most current information available. NCSC will not be liable for any loss or damage caused, arising from or in connection with the use of information contained in this publication. Any reference in this publication to any commercial product, process or service does not constitute or imply its endorsement or recommendation by NCSC. Views and opinions in this publication may not be used for advertising or product endorsement purposes.



Action	User	Name	Condition
Allow	Everyone	GOOGLE	Publisher
Allow	Everyone	MOZILLA CORP Thunderbird	Publisher
Allow	Everyone	SUN MICROSYSTEMS, INC	Publisher
Allow	Everyone	SECUNIA PSI	Publisher
Allow	Everyone	MOZILLA CORPORATION	Publisher
Allow	Everyone	MICROSOFT®	Publisher
Allow	Everyone	ADOBE	Publisher
Allow	Everyone	VMWARE	Publisher
Allow	Everyone	ESET SMART SECURITY	Publisher
Allow	BUILTIN\Admi...	Admin installs c:\auth_inst_dir\*	Path
Allow	Everyone	GPG	File Hash
Allow	Everyone	SNARE	File Hash
Allow	Everyone	Winrar	File Hash

Automatic Rule Creation

To minimize the risk of missing individual applications it is recommended, when setting up rules, to use the automatically find and create rules option.

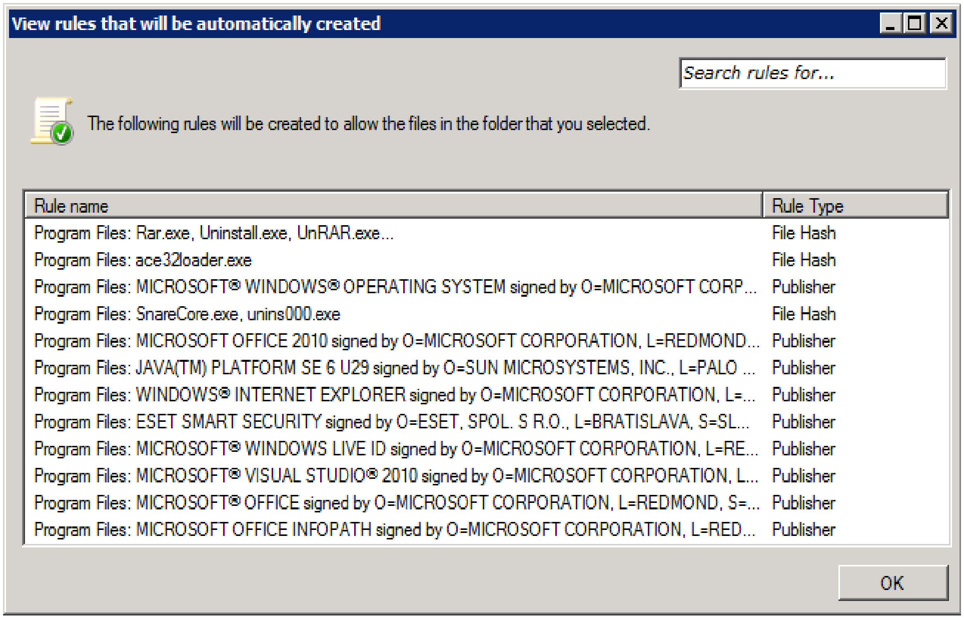
Important: Do not create the default rules - the default rules are set to allow anything in the system folder and program folders to be executed, including possible malicious software.

1. Select “Executable Rules” under Applocker in gpedit.msc.
2. Right click and select “Automatically generate rules”.
3. In “Folder and permissions”, select your system folder.
4. In rule preferences, base the rules on “Publisher” and “File Hash” (file hash is used for unsigned files).

While this publication is accurate to the best of our knowledge, NCSC does not accept any responsibility for errors or omissions. You are advised to ensure that you have the most current information available. NCSC will not be liable for any loss or damage caused, arising from or in connection with the use of information contained in this publication. Any reference in this publication to any commercial product, process or service does not constitute or imply its endorsement or recommendation by NCSC. Views and opinions in this publication may not be used for advertising or product endorsement purposes.

5. Select “Reduce number of rules”.
6. Review and select “Create”.
7. Repeat the process for each directory where applications are installed. Typical directories to generate rules for include:
   c:\windows , c:\program files, and c:\program files(x86).

The picture above shows an example of discovered programs.



View rules that will be automatically created

Search rules for...

The following rules will be created to allow the files in the folder that you selected.

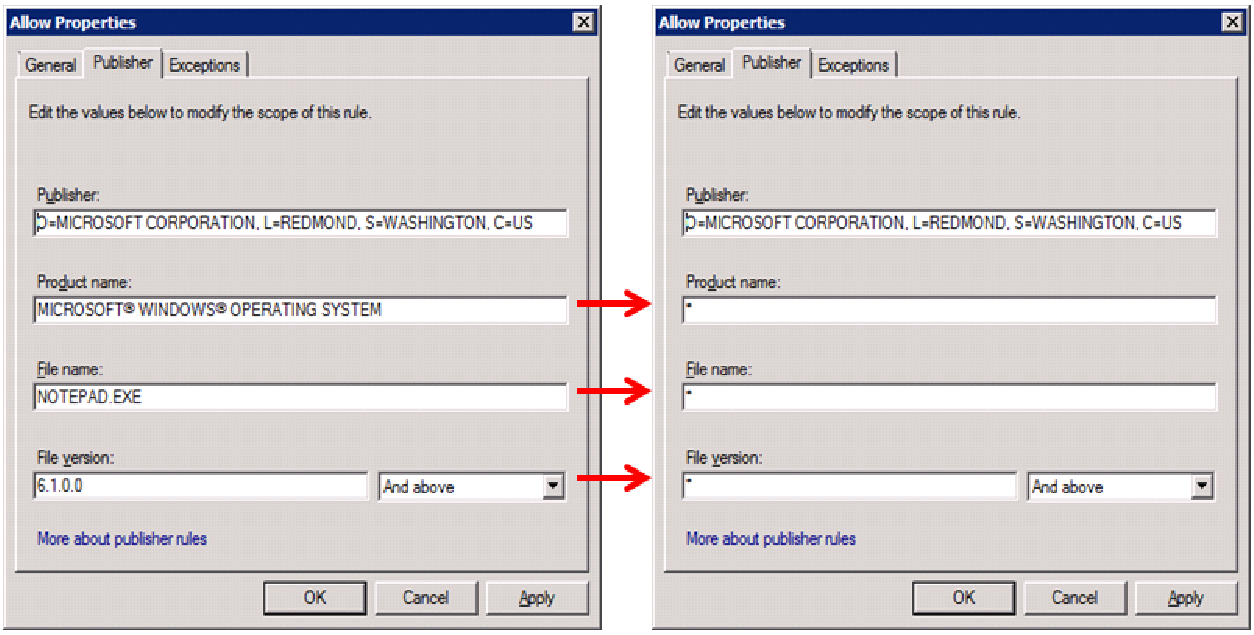
Rule name	Rule Type
Program Files: Rar.exe, Uninstall.exe, UnRAR.exe...	File Hash
Program Files: ace32loader.exe	File Hash
Program Files: MICROSOFT® WINDOWS® OPERATING SYSTEM signed by O=MICROSOFT CORP...	Publisher
Program Files: SnareCore.exe, unins000.exe	File Hash
Program Files: MICROSOFT OFFICE 2010 signed by O=MICROSOFT CORPORATION, L=REDMOND...	Publisher
Program Files: JAVA(TM) PLATFORM SE 6 U29 signed by O=SUN MICROSYSTEMS, INC., L=PALO ...	Publisher
Program Files: WINDOWS® INTERNET EXPLORER signed by O=MICROSOFT CORPORATION, L=...	Publisher
Program Files: ESET SMART SECURITY signed by O=ESET, SPOL. S R.O., L=BRATISLAVA, S=SL...	Publisher
Program Files: MICROSOFT® WINDOWS LIVE ID signed by O=MICROSOFT CORPORATION, L=RE...	Publisher
Program Files: MICROSOFT® VISUAL STUDIO® 2010 signed by O=MICROSOFT CORPORATION, L...	Publisher
Program Files: MICROSOFT® OFFICE signed by O=MICROSOFT CORPORATION, L=REDMOND, S=...	Publisher
Program Files: MICROSOFT OFFICE INFOPATH signed by O=MICROSOFT CORPORATION, L=RED...	Publisher

Edit and Consolidate Rules

To minimise the number of rules when whitelisting applications by publisher, it is possible to create one rule for each publisher and change all fields except the publisher to a wildcard, *, which allows any applications signed by approved publisher to run. Delete any duplicate rules for the same publisher.

Note: Some publishers may use more than one Certificate. If that is the case, you will need multiple rules for that publisher.

The picture below shows an example where a single application rule has been changed to a publisher rule.



Allow Properties

General | Publisher | Exceptions

Edit the values below to modify the scope of this rule.

Publisher: O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US

Product name: MICROSOFT® WINDOWS® OPERATING SYSTEM

File name: NOTEPAD.EXE

File version: 6.1.0.0 And above

More about publisher rules

OK Cancel Apply

Allow Properties

General | Publisher | Exceptions

Edit the values below to modify the scope of this rule.

Publisher: O=MICROSOFT CORPORATION, L=REDMOND, S=WASHINGTON, C=US

Product name: *

File name: *

File version: * And above

More about publisher rules

OK Cancel Apply

Rule creation for DLL, Scripts and MSI

For DLL files - repeat the process as for EXE files.

For Scripts - perform a risk review.

Allowing scripts can introduce an element of risk to systems, so it is recognisable that whitelisting should be thoroughly considered. The list below contains some of the key issues which should be considered:

- What damage could a malicious script cause?
- What scripts are safe to run?
- In what locations can scripts run?

While this publication is accurate to the best of our knowledge, NCSC does not accept any responsibility for errors or omissions. You are advised to ensure that you have the most current information available. NCSC will not be liable for any loss or damage caused, arising from or in connection with the use of information contained in this publication. Any reference in this publication to any commercial product, process or service does not constitute or imply its endorsement or recommendation by NCSC. Views and opinions in this publication may not be used for advertising or product endorsement purposes.

- Who can write/create scripts in whitelisted locations?
- What type of whitelisting should be used (signed, path, hash)?
- Other risks/considerations?

Note: Some programs do use scripts as part of their operation. A typical script that should be whitelisted is the Logon Script.

For MSI (and exe installers) – specify who can install.

By limiting the MSI installation privileges this setup will provide better protection and minimise the risk, of a malicious script or an exploit with administrator privileges, installing software.

1. Create a safe location such file share or somewhere on a local drive.
2. Create a rule allowing a specific administrator to install files from this location. Keep this account disabled and only enable it when you need to install software.

Review and Test

Before going live with a rule set defined in Applocker, it is essential that systems administrators review and test the Applocker rules.

1. "Review" all rules
2. Ensure "Enforcement" is set to log
3. **Start Applocker by starting the service "Application identity".**
4. **Configure the service "Application identity" to automatically start.**
5. Start/Stop applications, services and reboot the system.
6. Frequently review the logs with event viewer to check for issues (see the next chapter for details). If Applocker indicates that it is blocking "unknown" applications, DLLs & scripts, assess each instance for appropriateness and create new rules as required.

While this publication is accurate to the best of our knowledge, NCSC does not accept any responsibility for errors or omissions. You are advised to ensure that you have the most current information available. NCSC will not be liable for any loss or damage caused, arising from or in connection with the use of information contained in this publication. Any reference in this publication to any commercial product, process or service does not constitute or imply its endorsement or recommendation by NCSC. Views and opinions in this publication may not be used for advertising or product endorsement purposes.

7. Windows uses hidden file system mounts in the system folder. You may get errors/warnings for missing files that “don’t exist”. If this happens, search for the file, typically located somewhere else in the system folder.
8. Create new rules only as required.
9. Repeat the review process until there are no errors or warnings.

Note: Not all software vendors call dll files .dll.

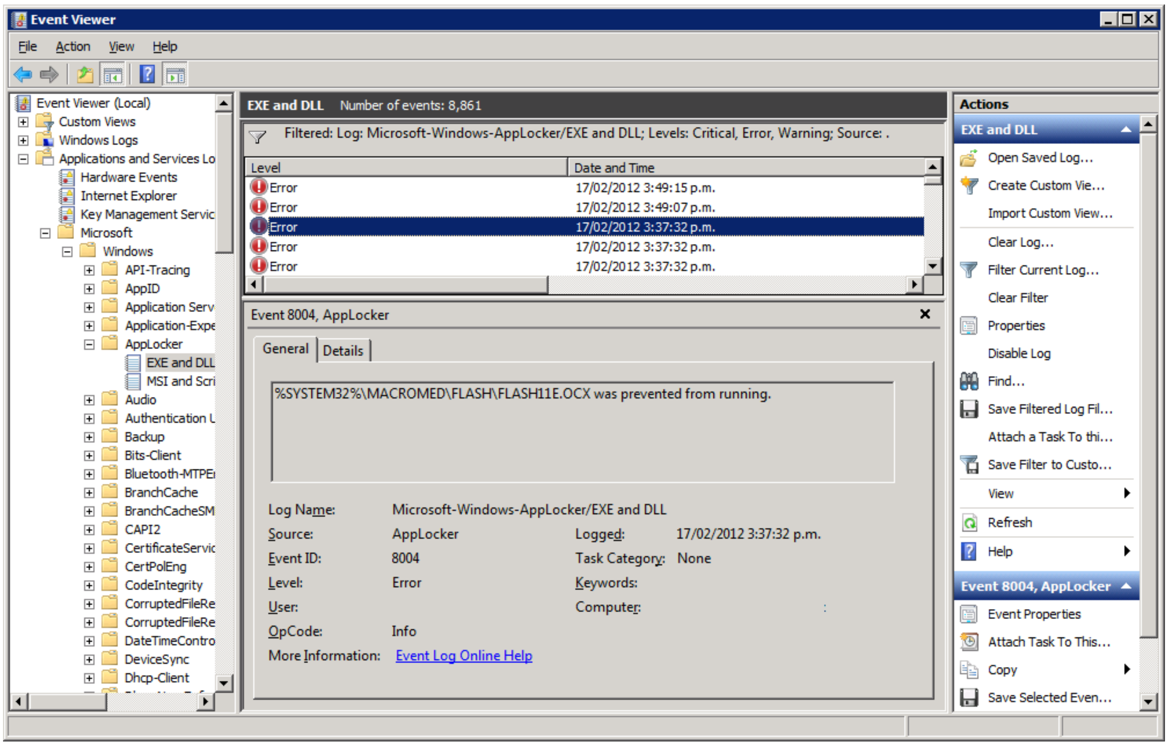
Important: Be mindful of malware when setting up Applocker. If unsure about a particular application, script or DLL, check with the software provider or Microsoft. If you are checking for information on the Internet, be conscious of malicious websites providing false information about the legitimacy of files. Some sites are also injecting drive by malware.

Log review

Use “Event Viewer” to review the logs. Start event viewer and navigate to “Application and Services Logs/Microsoft/Applocker”. Under Applocker there are two groupings, “EXE and DLL”, and “MSI and Scripts”. Apply a filter using “Filter Current Log…” to only display Critical, Error, and Warning events.

The picture below shows an example of event viewer displaying a DLL being blocked. Note the extension of the file.

While this publication is accurate to the best of our knowledge, NCSC does not accept any responsibility for errors or omissions. You are advised to ensure that you have the most current information available. NCSC will not be liable for any loss or damage caused, arising from or in connection with the use of information contained in this publication. Any reference in this publication to any commercial product, process or service does not constitute or imply its endorsement or recommendation by NCSC. Views and opinions in this publication may not be used for advertising or product endorsement purposes.



EXE and DLL Number of events: 8,861

Filtered: Log: Microsoft-Windows-AppLocker/EXE and DLL; Levels: Critical, Error, Warning; Source: .

Level	Date and Time
Error	17/02/2012 3:49:15 p.m.
Error	17/02/2012 3:49:07 p.m.
Error	17/02/2012 3:37:32 p.m.
Error	17/02/2012 3:37:32 p.m.
Error	17/02/2012 3:37:32 p.m.

Event 8004, AppLocker

%SYSTEM32%\MACROMED\FLASH\FLASH11E.OCX was prevented from running.

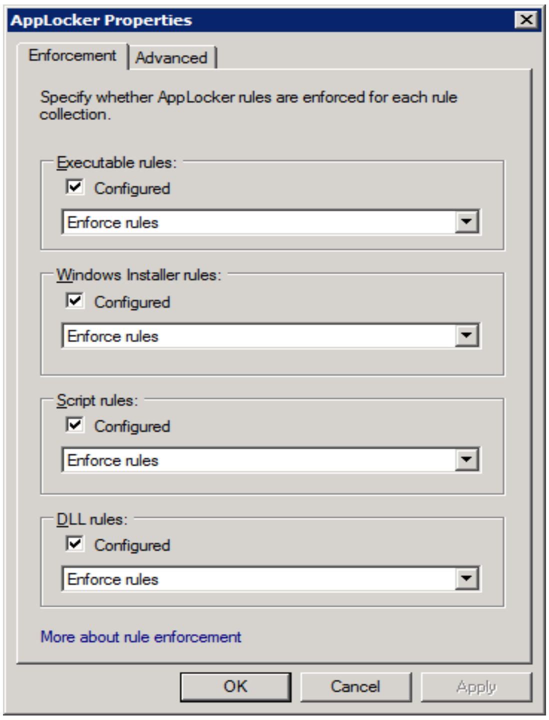
Log Name:	Microsoft-Windows-AppLocker/EXE and DLL		
Source:	AppLocker	Logged:	17/02/2012 3:37:32 p.m.
Event ID:	8004	Task Category:	None
Level:	Error	Keywords:	
User:		Computer:	
OpCode:	Info		
More Information:	Event Log Online Help		

Going Active

Once rules have been reviewed and there are no more warnings or errors, Applocker whitelisting can go active. Prior to doing so, make sure you have backups and/or the capability to perform a roll back just in case Windows is unable to start.

To go active/live:

1. Open Applocker “configure rule enforcement” to get the Applocker Properties.
2. Change rule enforcement to Enforce rules and click OK.
3. Reboot.
4. Review the Applocker logs.
5. Create more rules as required.



AppLocker Properties

Specify whether AppLocker rules are enforced for each rule collection.

Executable rules:
☑ Configured
Enforce rules

Windows Installer rules:
☑ Configured
Enforce rules

Script rules:
☑ Configured
Enforce rules

DLL rules:
☑ Configured
Enforce rules

The picture above shows the Applocker Properties set to “Enforce rules”.

Other information

Some important points to remember are:

- In “Active Directory”
  - Restrict access to Applocker rules (It is important to limit who can review and create rules for Applocker).
  - Ensure SCCM/WSUS can deploy patches.
- Never access the internet from an account that has administrator rights.
- If possible use application virtualization such as App-V or similar in combination with Applocker.
- Always use an up-to-date anti-virus solution.

While this publication is accurate to the best of our knowledge, NCSC does not accept any responsibility for errors or omissions. You are advised to ensure that you have the most current information available. NCSC will not be liable for any loss or damage caused, arising from or in connection with the use of information contained in this publication. Any reference in this publication to any commercial product, process or service does not constitute or imply its endorsement or recommendation by NCSC. Views and opinions in this publication may not be used for advertising or product endorsement purposes.

- Always use a properly configured firewall. A desktop/laptop can be part of “Active Directory” with a firewall blocking all incoming traffic (patching/remote management may need specific rules).
- Disable or uninstall any unnecessary services.
- Disable sharing and NetBios protocols.
- Enable Data Execution Prevention (DEP) for all programs.
- Set User Account Control (UAC) settings to highest level.
- Disable remote assistance and remote desktop connections (unless required for remote support in a corporate environment).
- Disable Autorun.
- If possible use sandbox capable/enabled applications that access the Internet.

Contact Information

Contact and other information about NCSC can be found on our website http://www.ncsc.govt.nz