



Australian Government
Department of Defence
Intelligence and Security

PROTECT

CYBER SECURITY OPERATIONS CENTRE

JULY 2013

'Top 4' Strategies to Mitigate Targeted Cyber Intrusions

Mandatory Requirement Explained

Including technical implementation advice for a Windows environment



CONTENTS

- Introduction 3
 - Document scope..... 3
 - Context 3
- The scope of the mandatory requirement 4
- Steps to manage the top 4 mandatory requirement..... 5
 - Where are we now? 5
 - What do we need to do from here?..... 5
 - If necessary, consider ‘how can we get help with this?’ 5
- Compliance and reporting requirements explained..... 7
 - PSPF Reporting Requirements 7
 - Reporting compliance to ASD..... 7
- Technical Guide to implementing the Top 4 Strategies..... 9
 - Reading this Section 9
 - Assumptions 9
 - Mitigation One: Application Whitelisting..... 10
 - Mitigations Two and Three: General Patching Guidance 14
 - Mitigation Two: Patch Applications 16
 - Mitigation Three: Patch the Operating System..... 19
 - Mitigation Four: Minimise Administrative Privileges..... 20
- Implementation Notes:..... 25
 - Administrative Privileges Implementation Notes 25
 - AppLocker Implementation Notes 26
- A quick check of your agency's implementation status..... 40

(U) **LEGAL NOTICE:** THIS PUBLICATION HAS BEEN PRODUCED BY THE DEFENCE SIGNALS DIRECTORATE (DSD), ALSO KNOWN AS THE AUSTRALIAN SIGNALS DIRECTORATE (ASD). ALL REFERENCES TO ASD SHOULD BE TAKEN TO BE REFERENCES TO DSD.

INTRODUCTION

The Top 4 *Strategies to Mitigate Targeted Cyber Intrusions* (the Strategies) are the most effective security controls an organisation can implement at this point in time based on the our current visibility of the cyber threat environment. The Australian Signals Directorate (ASD), also known as the Defence Signals Directorate (DSD), assesses that implementing the Top 4 will mitigate at least 85% of the intrusion techniques that the Cyber Security Operations Centre (CSOC) responds to. For this reason, the Attorney-General's Department has updated the *Australian Government Protective Security Policy Framework* (PSPF) to require Australian government agencies to implement ICT protective security controls as detailed in the *Australian Government Information Security Manual* (ISM) to meet ASD's Top 4 Strategies.

DOCUMENT SCOPE

This document provides specific implementation information on the Top 4 Strategies, including:

- information on the scope of and steps to manage the mandatory requirement; and
- some technical guidance for IT system administrators to planning and implementing the Top 4 Strategies in a typical Windows environment.

This document focusses on implementing the Top 4 in a Windows environment, as the majority of government business is currently conducted using Windows operating systems.

For agencies seeking implementation advice for systems that use other operating environments, ASD recommends seeking advice from your agency systems integrator or vendor in the first instance. Additionally, ASD recommends conducting research using open source publications, forums and resources available on the operating system and how each of the Top 4 could be implemented.

If your agency finds it is not possible or feasible to implement the Top 4 in a non-windows environment, you should follow appropriate risk-management practices as outlined in the ISM.

CONTEXT

The document provides additional information on the implementation of some of the technical controls from the ISM related to the Top 4. The ISM contains a full spectrum of information security controls to help agencies secure their information and systems. More information on the mandatory Top 4 Strategies is contained in the *Mandatory Controls* chapter of the ISM, and the ISM more broadly.

THE SCOPE OF THE MANDATORY REQUIREMENT

Understanding the intent behind ASD's Strategies will help agencies understand the scope of this mandatory requirement. Applicability should be determined by the risks which agencies are trying to mitigate. The Strategies are directed at the most common cyber security threat being faced by the Australian government at this point in time: targeted cyber intrusions from the Internet to the workstation.

These intrusions purposefully target specific government agencies, seeking to gain access to the sensitive information they hold. This is different to other types of cyber security incidents. For example, Denial of Service attacks, which aim to prevent legitimate user access to online services.

Targeted cyber intrusions commonly use content-based attacks (i.e. email and web pages) which easily bypass perimeter defences, because they look like legitimate business traffic, to gain access to the workstation. From the workstation they spread, gaining access to other computing and network resources and the data they contain.

The Strategies were developed with this scenario in mind. They use a layered defence approach, primarily designed to protect the workstation and by extension the corporate network. *Priority for implementing these mandatory requirements should therefore be placed on Australian government systems that are able to receive emails or browse web content originating from a different security domain, particularly from the Internet.*

This document refers to 'high value' targets. This term refers to those in an organisation with ready access to key organisation information and staff who use Internet-facing systems. High value targets are often executive staff and their assistants, and public-facing staff who deal with human relations or Freedom of Information requests.

Other systems will benefit from implementing the Top 4 and Top 35 Strategies more broadly. However, ASD acknowledges there may be circumstances where the risks or business impact of implementing the Top 4 outweigh the benefit, and other security controls may have greater relevance.

In such circumstances, agencies should apply appropriate risk management practices as outlined in the ISM. It should also be noted that the intent of the Strategies is to make the job of cyber adversaries significantly harder. Implementing them will not, however, completely remove the risk to organisations.

STEPS TO MANAGE THE TOP 4 MANDATORY REQUIREMENT

The following can be used to guide your agency's planning and implementation of the new Top 4 mandatory requirement.

WHERE ARE WE NOW?

Firstly, assess the current status of the implementation of the Top 4 on your network. Developing an understanding of the security of your network will inform Top 4 implementation planning. For example, do you currently employ application whitelisting? If not, before purchasing new software, consider if existing software deployed on your system may already have functionality that would comply with the application whitelisting requirement once configured correctly.

If your agency has begun the process of implementing the Top 4, assess whether the maturity of your implementation is appropriate for your risk profile.¹ Different implementations of the Top 4 are stronger than others. Agencies should strive for the strongest implementation appropriate for their business environment.

WHAT DO WE NEED TO DO FROM HERE?

Next, conduct a threat and risk assessment and compare where your agency is and where you need to be. Determine which systems are within the scope of the Top 4 mandatory requirement and develop an implementation plan for each system. For systems not within scope of the Top 4 mandatory requirement, document these decisions and consider other technical controls to lower the associated risk.

Consideration also needs to be given to the resourcing required to achieve the Top 4 implementation, both in terms of staff and budget allocations.

IF NECESSARY, CONSIDER 'HOW CAN WE GET HELP WITH THIS?'

Finally, identify the available advice and assistance mechanisms. This document will be able to provide a good basis for implementation advice; however it will not cover every implementation scenario.

For configuration advice for specific software, your software vendor will likely be best placed to assist you.

¹ *DSD Top 4 Mitigation Strategies – Maturity Model*, Foresight Consulting, <http://www.foresightconsulting.com.au/resources/docs/T4MM.pdf>

Your agency could consider leveraging an Information security Registered Assessor to audit your system and provide feedback on the implementation of the Top 4. Private sector training is also likely to be available in the near future.

ASD can also provide advice to agencies. Additionally, ASD's OnSecure portal has forums that can be leveraged to liaise with other agencies on how they are implementing the Top 4.

COMPLIANCE AND REPORTING REQUIREMENTS EXPLAINED

This section gives an overview of the compliance and reporting requirements for the Top 4.

PSPF REPORTING REQUIREMENTS

The PSPF Mandatory Requirement GOV-7 requires agencies to: "undertake an annual security assessment against the mandatory requirements detailed within the PSPF, and report their compliance with the mandatory requirements to the relevant portfolio Minister".

ASD's Top 4 has been included as a component of mandatory requirement INFOSEC 4. Agencies need to capture their overall compliance with the Top 4 in a statement as part of the annual PSPF reporting process. This reporting should be incorporated with compliance reporting against other PSPF requirements and should be sent to:

- the relevant portfolio Minister(s)
- the Secretary of the Attorney-General's Department and
- the Auditor-General of the Australian National Audit Office; as per the guidance set out in the PSPF.

For further information regarding reporting requirements, consult the PSPF documentation which is available on the Attorney-General's Department's PSPF webpage, or check with your Agency Security Advisor (ASA).

As per the existing PSPF requirement, annual PSPF compliance reports are due to portfolio Ministers annually, starting in 2013. However, this does not mean that agencies are expected to have successfully implemented the Top 4 by this time. Agencies are best placed to determine appropriate timeframes for implementing the Top 4 as part of their implementation planning.

The key concept is that agencies use the PSPF compliance reporting process to inform their Portfolio Minister(s) as well as the Minister responsible for protective security and privacy (the Attorney-General) of progress against this mandatory requirement and rationale for non-compliance.

REPORTING COMPLIANCE TO ASD

It should be noted that Ministerial authorisation of the ISM's Mandatory Controls is intended to provide Ministers with oversight of decisions being made by their departments, rather than a new part of the system accreditation process. This reporting can be rolled into the broader PSPF reporting requirements.

There is an existing requirement for agencies to provide a copy of their ISM non-compliance reports to Director ASD. This will remain in place when the new mandatory requirements come into effect (ISM

control 0713). Reports can be submitted through the ASD Advice and Assistance email address: asd.assist@defence.gov.au.

In addition to the compliance reporting agencies provide to their portfolio Minister, ASD now has a responsibility to assess and report to Government on the performance of Australian government agency implementation of the Top 4.

To assist with this assessment process, ASD will request agencies complete an annual survey designed to measure how agencies are performing against the Top 4, and the Top 35 more broadly. This survey is based on self-assessment and requires agencies to disclose whether or not they have implemented the Top 4 to ASD. Agencies are also encouraged to provide feedback regarding their performance against the entire Top 35.

While the survey is not a means of assessing compliance with the ISM and related policies, the results of the survey will help ASD to provide agencies with tailored advice and assistance to improve their cyber security posture.

TECHNICAL GUIDE TO IMPLEMENTING THE TOP 4 STRATEGIES

Implementation of the Top 4 Strategies is likely to be technically complex. Appropriate planning will reduce both the short and long term costs of employing these techniques.

Organisations should consider beginning pre-deployment planning activities in the short term, to enable them to take advantage of the earliest possible opportunity to use these techniques in improving the security posture of their networks, systems and data.

READING THIS SECTION

This section provides planning, deployment and administrative guidance to system administrators or integrators to help ensure that implementation of the Strategies is carried out in such a way that provides a high level of security assurance, while taking into account the needs of and impact to system users. This in turn will reduce the requirement for user support once the changes have been carried out. It does not aim to provide any compliance information or high-level policy guidance. Such information is contained in the ISM.

ASSUMPTIONS

This section describes software and techniques available on a Microsoft Windows Active Directory domain consisting of Microsoft Windows 2008 R2 servers and Microsoft Windows 7 workstations. While the planning and implementation steps will be similar on other technology systems, agencies should research and take into account any differences which may exist. There may also be third-party solutions available for many of the issues discussed. Again, care and research is required to ensure these solutions are appropriate for any given environment.

MITIGATION ONE: APPLICATION WHITELISTING

Why Use Application Whitelisting?

Application whitelisting, if implemented correctly, can be an incredibly effective means of ensuring the security, stability and consistency of a computing environment. Unfortunately it is often misunderstood or poorly implemented, which can lead to an environment appearing more secure than it actually is. For further high-level information on the issues surrounding implementation of application whitelisting, see ASD's publication *Application Whitelisting Explained*.

Technology Selection

Microsoft introduced the AppLocker technology in Windows 7 as an integral component of the operating system. AppLocker has the advantage of being freely available with the operating system along with deployment and testing tools integrated with the operating system and Active Directory. While there are several other technologies available to implement application whitelisting in a Windows domain environment, this guidance will primarily focus on AppLocker. However, much of the following guidance will be applicable to other application whitelisting technologies, particularly the planning advice. Agencies should ensure any other technology used is properly researched and deployed.

Policy and Planning

Proper planning and pre-deployment activities are crucial to a successful deployment of application whitelisting technology. Many of the common concerns surrounding the technology, particularly those of an increased support burden, can be mitigated by properly assessing an organisation's environment to inform implementation design.

There are a number of decisions which need to be made before planning of the technical aspects of an AppLocker deployment can begin. These include:

What policies govern my implementation of application whitelisting? Application whitelisting can only be deployed in support of policy which defines applications which users are allowed to run, or can be expected to run, in the course of their duties. The technical implementation of application whitelisting needs to reflect these policies. It is important to note that in order for AppLocker to be correctly deployed, users must not be allowed local administrative privileges. This is a crucial requirement for application whitelisting to be effective.

Do all users need access to the same applications? While one consistent AppLocker configuration may be applicable for simple deployments and smaller organisations, larger organisations are likely to have several different computer configurations based upon user roles and responsibilities. AppLocker is capable of applying different restrictions based upon the Organisational Unit (OU) memberships of individuals and computers. For example, only Human Resource staff may require access to certain payroll applications while Web Team staff may require a suite of editing applications which are not licensed for use by other staff.

What executable content cannot be controlled with AppLocker? AppLocker can restrict execution of executables, libraries (DLLs) and scripts that are run under the Windows Scripting Host (VBScript, Jscript, batch files, .cmd files Windows PowerShell scripts). Other executables, for example Perl scripts, Java files or 16-bit DOS executables will need to be controlled using the settings of their host applications. For example, consider the security implications of macro security settings in Microsoft Word and Excel, if installed. In addition, there are methods by which ill-designed programs can bypass AppLocker restrictions², however a hotfix for these issues is available from Microsoft³.

Do I want to roll out incrementally, starting with a pilot group? For a homogenous environment, it may be possible to create and fully test an AppLocker configuration before applying it globally. For more complex environments, it may be preferable to deploy a test version first. For example, proposed AppLocker policies in Audit Only mode may be deployed to a pilot group containing staff from across different areas of the organisation. Audit Only mode logs events that application whitelisting would have blocked, had it been enabled. These logs can be collated and analysed to assess the effectiveness of the proposed design. Alternatively, AppLocker may be deployed to high value targets while testing is conducted on a broader deployment for staff with potentially more complex needs.

How will I create AppLocker rules? One of the simplest ways to generate AppLocker policies is using the Automatically Generate Rules wizard. This allows simple certificate and folder based rules to be set up on a reference computer, and then more specific rules can be generated based upon the software that is installed on that computer. This reference computer should be known to not be compromised. For organisations that use a limited number of Standard Operating Environment (SOE) builds, this may be a very effective rule generation mechanism. Alternatively, AppLocker rules may be created by hand. Either approach will require testing to ensure users are able to function normally under the newly secured environment.

How will I manage updates to AppLocker rules? When applications are updated, added to or removed from the operating environment the AppLocker rules for those applications may need to be updated. Consider how AppLocker updates can be added to existing change management or testing processes for the environment to ensure that users are not negatively impacted by any changes while ensuring AppLocker protections are fully effective.

What education will I provide users? Where can users seek help if an application is blocked or doesn't work as expected? What training will I provide support staff? Application whitelisting will impact on a user's ability to use their environment, especially if they are accustomed to executing programs which are not a part of their SOE. User education will ensure users are aware of the security context of the changes, as well as how to get support if applications do not work as expected. Similarly, support staff will need to be advised on how to handle such requests from users. AppLocker allows organisations to customise the error message displayed when an application is blocked to include a

² [http://technet.microsoft.com/en-us/library/ee844118\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ee844118(WS.10).aspx)

³ <http://support.microsoft.com/kb/2532445>

custom support link, which is an effective way to inform users of the policies and support processes applicable to the organisation.

How will I monitor and audit AppLocker logs? AppLocker logs should be monitored for unexpected policy results, particularly during the pilot and initial deployment stages. Consider aggregating all log messages to a central logging server, so that they can be analysed for any weaknesses. In addition, ongoing auditing of AppLocker logs should occur to ensure the environment continues to behave correctly.

Rule Creation

Rule creation can be performed either manually or automatically using a baseline SOE computer. The stages of rule creation differ between manual and automatic creation, and are as follows:

Configure All Software on Reference Computer. In order to effectively create automatic rules, all required software should be installed on the reference computer which is known to not be compromised. This allows the automatic generation process to create rules tailored to the specific operating environment. When creating rules manually, all necessary software for the environment should be installed so that the effectiveness of the rules, both in protecting the environment and allowing the appropriate software to function correctly, can be tested.

Confirm File-Level ACLs and Create Default Rules. A tool such as *accesschk*⁴ should be used to ensure that users cannot write to any directories which are intended for inclusion in the whitelist. This applies in two situations: where path-based rules are the preferred method of identifying whitelisted executables, or where default rules will be created for the Automatically Generate Rules process to build upon. While path-based rules are the easiest method to administer for identifying whitelisted executables, and require the lowest system overhead while in use, issues such as legacy applications which write into their own program directories need to be taken into account. Once ACLs are documented, appropriate rules can be created. Be sure to exclude any user-writable directories when using path-based rules.

At this point, it is also possible to configure which types of files should be subject to AppLocker approval. Library files (DLLs) should be included in enforcement as their exclusion is a significant security risk. Organisations should consider removing the LNK (Shortcut) file type from the list as this can have a significant and negative impact on user experience. If this file type is present in the list users will be unable to create and use their own links to files, folders and applications.

Automatically Generate Rules and Delete Excess Rules. At this point, the Automatically Generate Rules wizard should be run to generate customised rules for your environment. Once this is completed

⁴ <http://technet.microsoft.com/en-us/sysinternals/bb664922>

excess rules (including the Default Rules created earlier) should be deleted to ensure that more stringent enforcement using the specifically generated rules is applied.

Apply and Test Rules. Finally, the created rules are ready to be applied and tested. The Application Identity service is used by AppLocker to identify executables which should be allowed. Agencies must ensure that group policy is used to automatically start this service. Also ensure that the AppLocker Group Policy is applied to the appropriate OU. This should initially be applied to a test computer, followed by deployment (perhaps in Audit Only mode) to a pilot or test user group. Any exceptions or changes needed should be examined fully to ensure that they do not compromise the security of AppLocker as a whole.

Rule Maintenance

As computing environments change over time, AppLocker rules need to change with them in order to continue to be effective. Consider how AppLocker rule updates could be integrated in the change management process for your organisation to ensure that the rules are always up to date. This should include testing of the rules in conjunction with any changes made such as application installs, updates or operating system patches.

Consideration should be given to versioning policies, to ensure that policies are kept up-to-date and in-sync across the entire organisation. While Group Policy does not directly allow you to version policies, additional software such as the Advanced Group Policy Management feature from the Microsoft Desktop Optimization Pack⁵ can provide this functionality.

Conclusion: Application Whitelisting

In a well-designed and managed computing environment it is possible to identify every executable which should be allowed to run on a system. This means that any unidentified executable can be treated as suspicious at a minimum and should be prevented from running. The benefits of application whitelisting as a security approach are significant and can help organisations defeat known and unknown malicious intrusions. In addition, it can help administrators ensure that the computing environment remains in a known state, which in turn improves the stability and consistency of the environment.

⁵ <http://go.microsoft.com/fwlink/?LinkId=145013>

MITIGATIONS TWO AND THREE: GENERAL PATCHING GUIDANCE

This section covers advice which is applicable to both Mitigation Two: Patch Applications and Mitigation Three: Patch the Operating System.

It is important that patch management is considered a core function of IT management and is carried out in a timely and efficient manner. Patch management for operating systems and applications are closely related and the procedures followed should be similar. These procedures should be tightly integrated with corporate change management processes to ensure that they are effective and auditable across the entire organisation.

What to Patch?

Every server, workstation, network device, network appliance, mobile device, operating system and installed application needs to be kept up to date in order to ensure the security of an organisation's operating environment as a whole. A single unpatched machine significantly increases the attack surface of an organisation's environment, and this increase is multiplied as more machines are in a vulnerable or unknown state.

When to Patch?

Patch deployment timeframes should correspond to the level of risk associated with the vulnerability being patched. Patches associated with higher risk vulnerabilities should be deployed quicker than a patch addressing lower risk. For patches addressing extreme risk the deployment timeframe must be within 48 hours, as prescribed in the ISM.

ASD has observed many instances where unpatched vulnerabilities have been exploited in government systems. Historically speaking, many large-scale security incidents have occurred after patches for the exploited vulnerabilities were available. For example, the Zotob worm struck five days after the patch for the vulnerability was available⁶.

Priority in patching should be given to (in no particular order):

- Workstations used by employees most likely to be targeted by intrusions (or 'high value' targets)
- Internet-facing machines, such as web, email and remote access servers and data transfer machines
- Data transfer hosts
- Systems of critical business importance, such as Domain Controllers or financial database servers

⁶ <http://technet.microsoft.com/en-us/library/cc700845.aspx>

- Systems storing sensitive or classified data, such as file or HR database servers.

Testing and System Stability

A common concern of patching is that the system will no longer function as required. While it is possible for any patch to change the state of a system enough that it will function differently, it is important to weigh this risk against the risk of not patching a given system. Consideration should also be given to the pre-release testing which is performed by the operating system or application vendor. As discussed above, high-priority systems may demand patching sooner than others. This may necessitate less time spent testing a patch. Conversely, the decision may be made that certain systems are so critical that extensive testing is required before a patch can be deployed. Any decisions that are made need to be documented in the change management process, well understood and revisited in light of any new or increased threats to a given system. Change management documentation should provide concrete examples and clear guidance to those testing and deploying patches, so the patching procedure is clear for any given patch. Several approaches to patching are discussed in *Strategies to Mitigate Targeted Cyber Intrusions – Mitigation Details*⁷, such as deploying patches to a small number of systems initially and then rolling patches out to the rest of the organisation once stability has been verified over a pre-determined time period.

⁷ <http://www.dsd.gov.au/infosec/top-mitigations/top35mitigation-details.htm>

MITIGATION TWO: PATCH APPLICATIONS

Why Patch Applications?

An application is any software which is not part of the core operating system. Application patch management needs to be considered separately to the operating system primarily because it is likely to be significantly more challenging than operating system patching. Most applications will have unique patching methods and requirements. It is important to integrate these into a single process, both from a change management and a technical perspective.

Applications are a common exploitation vector for cyber intrusions for a number of reasons. The principal reason is that some applications (such as Adobe Flash Player or Microsoft Office) are present on the majority of systems and many organisations do not patch (or are not aware of) all applications on their systems.

Leaving applications unpatched will drastically increase the attack surface of the system and any interconnected system. Malicious intruders often take advantage of vulnerabilities in applications to gain a foothold on a network, which can be used to attack other systems from within the organisation's network.

Use Updated Software Versions

Agencies should avoid using versions of software which are outdated. Newer versions of software typically implement better protections against malicious behaviour and are often not vulnerable to older attacks. Examples in the *Microsoft Security Intelligence Report Volume 11*⁸ show that older versions of Microsoft Office are significantly more vulnerable to attack. Likewise, out-dated versions of Internet browsers and PDF viewing software are more vulnerable to attack.

The *Microsoft Security Intelligence Report Volume 11* also shows that newer versions of Internet Explorer provide significant security enhancements that proactively protect from many known vulnerabilities.

Patch Management

Organisations should patch every application on their systems, focussing on applications which interact with content from the Internet. This requires administrative staff to be aware of all applications present on their systems. Ways to achieve this are discussed in the previous section, Mitigation One: Application Whitelisting and also Mitigation Four: Minimise Administrative Privileges.

⁸ <http://www.microsoft.com/security/sir/archive/default.aspx>

Very few applications provide a means to manage patches at an enterprise level. The majority rely upon user intervention to patch, either through enabling automatic patches, agreeing to the installation of patches, or manually visiting the application website to download patches. This leads to a substantial delay between patch availability and install, if patches are installed at all.

Note that some applications do not provide security patches for old versions but rather require a new version to be installed.

Considerations

Applications should be patched as soon as possible in conjunction with change management and related testing procedures. While many of the same considerations also apply to patching of the operating system, there is one additional consideration for application patching: likelihood of exploit. Timely patching of applications substantially reduces the potential for attacks to compromise an organisation's computing environment and should be considered as important as timely operating system patching.

Further guidance on the update process for Microsoft products is available in the *Microsoft Security Update Guide*⁹.

Methodology

Creating a comprehensive patch management strategy for applications can be difficult, and depend on the specific applications, the patching methods they support and the patch management infrastructure available to the organisation. While centralised management of patching should always be the primary goal, alternative approaches such as application self-patching or forced application patching may also be considered.

Centralised Management

Centralised management of patches is a key enabler for securely deploying applications in your environment. Ideally, the selected solution for centralised patch management will allow the same fine-grained controls as those discussed in Mitigation Three: Patch the Operating System. It may be possible to use the same solution for both operating system and application patching, such as Microsoft's System Center Configuration Manager (SCCM)¹⁰. This reduces the administrative overhead associated with maintaining separate patching mechanisms for the operating system and applications. It also allows administrative staff to use similar procedures for testing and deploying both operating system and application patches.

⁹ <http://www.microsoft.com/security/msrc/whatwedo/securityguide.aspx>

¹⁰ <http://www.microsoft.com/systemcenter/en/us/configuration-manager/cm-software-update-management.aspx>

Application Self-Patching

Some applications are capable of detecting, obtaining and installing patches for themselves. They may also have the capability to run a corporately-controlled centralised patching service which is unique to the specific application. This may be an appropriate solution for patching some applications but there are several security considerations:

Administrative Privileges. If an application requires administrative privileges to execute patching, exploitation of that application could gain the attacker administrative level access to the system. It is very rare for an application to have the capability to patch itself without administrative privileges.

User Interaction. Patching methods need to be completely autonomous and should not rely on user action in order to be effective. If users are required to take action as part of the patching process, this may result in systems of an unknown patch level if some users fail to take the actions necessary to apply the patch.

Assurance. Allowing applications to patch themselves can lead to a state where the patch level of a given application on a given system cannot be determined. If administrators cannot determine the patch level of a given application across the organisation they will be unable to make meaningful threat and risk assessments for security issues effecting that environment. For example, if a security bulletin is released requiring a different mitigation method for software at different patch levels, administrative staff may need to apply multiple mitigations to ensure their environment is adequately protected.

Forced Application Patching

One technique historically used for patching is to force patching of applications, for example by running an update batch script during logon or after hours across multiple systems. While this may have been an appropriate solution when system architectures and applications were simpler, patching of a modern environment is too complex to be left to this kind of approach. Issues such as a mobile workforce, application whitelisting and systems with differing configurations can render such approaches partially effective at best, as well as potentially introducing instability into the environment. It is strongly recommended such patching instead be carried out in a centralised and organised fashion using patch management software.

MITIGATION THREE: PATCH THE OPERATING SYSTEM

Why Patch the Operating System?

The operating system is the core around which the entire computing environment is built. If it is not stable and secure other security considerations are, to a large extent, pointless. If the operating system is compromised, any action or information handled by that computer is at risk.

Use Updated Operating System Versions

As with application software, newer versions of operating systems include more protection against malicious behaviour. Upgrading to newer operating systems should be a high priority, particularly for computers which are running significantly out-of-date versions. In the *Microsoft Security Intelligence Report Volume 11*¹¹, data shows that desktop malware infection rates fall by a factor of ten between Windows XP with SP3 and Windows 7 64-bit with SP1 (1.09% and 0.11% respectively). This is primarily due to security features such as memory address space randomization (ASLR) and data execution prevention (DEP). Agencies should plan for and implement regular operating system upgrades for their computer systems.

Methodology

There are many tools available which are capable of providing patches to operating systems as well as monitoring and auditing their patch levels. Microsoft's primary tool for patching is the SCCM¹² which is built upon the framework of the Windows Server Update Services (WSUS). Unlike WSUS, SCCM is capable of managing a geographically diverse fleet of computing assets. Organisations are encouraged to investigate multiple tools capable of providing operating system patching in order to find the tool which most closely satisfies the requirements of their unique environment. When selecting an operating system patching tool, consideration should be given to the tool's ability to:

- Discover unknown/new devices in the environment and report on these discoveries
- Enumerate patch levels across all devices in the environment
- Patch different device types existent in the environment (especially all servers and workstations)
- Patch devices of different configuration (for example, with different deployed software packages)
- Provide for quick deployment of critical or emergency patches
- Provide assurance that all devices are patched and report on any devices which cannot be patched
- Deconflict between different patches which may apply to the same issue on the same device
- Provide for patching of devices in geographically diverse locations, if required.

¹¹ <http://www.microsoft.com/security/sir/archive/default.aspx>

¹² <http://www.microsoft.com/systemcenter/en/us/configuration-manager/cm-overview.aspx>

MITIGATION FOUR: MINIMISE ADMINISTRATIVE PRIVILEGES

Why Minimise Administrative Privileges?

Administrative privileges are designed to allow only trusted personnel to configure, manage and monitor computer systems. Accounts with administrative privileges on a system have the ability to make virtually any change to that system and to retrieve almost any information from it. Accounts with administrative privileges to a Windows domain typically have the ability to effect such changes or see such information from any system on that domain.

While these privileges are necessary for the ongoing administration of a system or network they introduce a number of potential points of weakness into that system. These include opportunities for users to make intentional or unintentional modifications with system-wide consequences and can provide a high-value target for malicious intruders.

The Windows 7 environment has greatly reduced the number of tasks which require local administrative privileges to carry out. Additionally, the controls for managing user access to the system offer extra granularity which allows administrative privileges to be more tightly focussed around tasks that administrators must carry out.

System Modification by Users

Some organisations allow users to obtain or execute software with administrative privileges in order to install custom software or to use legacy software which is not properly designed for their environment. While this may appear to be an easy way to reduce user support, it may actually allow the introduction of changes to a system which will require significantly more effort to correct.

Users are not typically trained in system administration and cannot be relied upon to avoid making changes which might damage the security or reliability of the system. If a user is able to delete or rename necessary system files, for example, they could cause issues which require significant administrative effort to correct.

Allowing users to install software can significantly increase the attack surface and administrative requirement of a system. In addition, this software may conflict with other software installed on the system which could be detrimental to the stability of that system.

Target for Malicious Intruders

Due to the powerful privileges an administrative account provides they are a primary target for malicious intruders. If a user with administrative privileges is able to browse the Internet or read email, for example, any drive-by malware or phishing campaign will have the potential to compromise the entire system. Security training for administrative users is not enough to prevent them being the source of a compromise.

Administrative accounts also typically have access to information like password hashes which can make infiltrating other systems in a network significantly easier. Further, a malicious intruder could modify the access permissions on those items that they desire access to in order to facilitate information gathering used to further penetrate and persist in that environment.

Separation of Privileges

Administrators should have access to multiple accounts with differing sets of privileges. These should require separate passwords to access. For example:

User Name	Account Type	Privilege level
jbloggs	User	Email and Internet access; access to data shares
admin_jbloggs	Administrator	No email or Internet access and access to only administrative network shares

A software developer who has a business requirement to install different software frameworks for testing might have accounts as per this example:

User Name	Account Type	Privilege level
jbloggs	User	Email and Internet access; access to data stores
dev_jbloggs	Developer	No email or Internet access and access to only software network shares. Software install privileges <i>only</i> on local workstation

Planning

Careful planning should be undertaken before removing administrative privileges for users. The planning and deployment steps required largely depend on a review of the reasons users have been allocated administrative privileges.

Privileges for System Administrators

While system administrators may require administrative privileges for their accounts these privileges do not need to be assigned to their day-to-day accounts. Any administrative privileges should be allocated to separate administrative accounts so that administrators have to make an explicit decision to take an action using those privileges. These administrative accounts should also have all external network access removed, such as email or Internet access.

Many administrative tasks may not actually require administrative privileges to undertake or may be undertaken with a limited subset of those privileges. For example, a Backup Administrator may simply require an account with Read access to the locations they need to back up, rather than administrative access to the system on which the data resides. Similarly, an Email Administrator will probably not require administrative privileges on any system other than the email server, and possibly not even on that system.

Privileges for Software Installation

Software installation and maintenance should be carried out in a central and managed fashion, rather than by users in an ad-hoc manner. The requirement for users to install their own software is often indicative of a policy deficit either in understanding the work environment needs of users, or a shortfall in managing user expectations of their work environment.

Privileges for Software Compatibility

Organisations often have a business requirement to use software which has not been updated by the manufacturer or is not compatible with their contemporary operating environment. While providing users with administrative privileges is commonly used as a workaround Microsoft has provided a number of more suitable techniques which can be used to ensure that these legacy products can be used in a safe manner. Tools such as the Microsoft Windows Application Compatibility Infrastructure (Shim Infrastructure)¹³ or Application Virtualization¹⁴ can be used to deploy legacy applications securely into a modern operating environment while still providing full functionality and privilege separation to users.

Logging and Auditing Administrative Privilege Use

When a large number of users within an organisation have administrative privileges it is virtually impossible to audit the actions taken using administrative credentials. The number of privileged actions performed will be greatly reduced once an organisation minimises the number of users who require administrative privileges and eliminates administrative privileges from the accounts of standard users. This reduction will make it easier for organisations to detect unauthorised, dangerous or inappropriate use of these credentials. As mentioned previously, administrative credentials are primary targets of malicious intruders looking to propagate and persist in a network. Good centralised logging, monitoring and auditing of these credentials can provide early warning that such activity might be occurring in an organisation's network.

This logging should extend to the creation of new accounts with administrative privileges as well as the addition of administrative privileges to existing accounts, modification of administrative privileges or the reactivation of disabled administrative accounts. These techniques are commonly used by malicious intruders to increase their privileges and level of access.

Remote Access

The ability for users connecting remotely to access administrative privileges, in any form, is a serious security risk for a system. This includes connecting as a non-administrative user before escalating

¹³ [http://technet.microsoft.com/en-us/library/dd837644\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/dd837644(WS.10).aspx)

¹⁴ <http://www.microsoft.com/windows/enterprise/products/mdop/app-v.aspx>

privileges during that session. Given the level of control administrative users have in an environment and the challenges inherent in securing a remote access solution, the potential productivity gains of remote administrative access are far outweighed by the security risks. Careful consideration needs to be given before such access is allowed, and if the risks are accepted by the organisation remote privileged access needs to be closely monitored and audited to catch any potential abuse or exploitation. Additional security measures such as multi-factor authentication, time-of-day restrictions and login location restrictions should also be seriously considered.

User Impact

As with any significant change to the computing environment, user impact must be closely managed. If users are accustomed to performing tasks using administrative privileges, for example installing or running their own software, then they will need to be educated on the requirement for and the restrictions imposed by the new privilege model. Change management and user support procedures will need to take into account the changes that users will see as necessary for their continued productive use of the environment. Pre-planning and assessment of applications commonly used or installed by users may provide insight into how to modify the user environment to minimise negative impact. For example, functionality provided by commonly installed applications could be replicated by existing or new corporately managed software, with the advantage that such software can be supported and updated across the organisation as discussed in Mitigations Two and Three of this document.

It is likely that different work units or areas within an organisation, particularly a large organisation, will use a unique set of applications. This will need to be considered during the planning phase, as these different environments could require additional planning to ensure that the changes do not have a negative impact on users' ability to perform work tasks.

Deployment

The ideal method of reducing administrative privileges within an organisation depends on the current scope of administrative credential deployment, the size of the organisation and the number of users or work groups with unique needs.

The introduction of a new Standard Operating Environment (SOE) is often the ideal time to carry out this deployment, especially if significant changes to the applications installed in the SOE are required, however the reduction of administrative privileges should not be delayed while agencies wait for a new SOE to be introduced.

Scope of Administrative Credential Deployment

In cases where system administrators are the only personnel in the organisation who have administrative credentials the transition can be relatively straightforward. In this scenario, the task would simply entail migration of these credentials to administration-only accounts and, once training and pre-deployment activities are completed, the transition should be fairly easy. System

administrators are more likely to understand the technical and security requirements of such changes and it will likely have a minimal impact on their day-to-day productivity.

A review should be undertaken of non-administrative users' administrative credentials of to determine the actions which need to be taken in each circumstance. Care should be taken to ensure that the new procedures regarding account activity separation are being followed and that the logging, monitoring and auditing regimes are working correctly.

Users and Groups with Unique Needs

If users or groups of users have unique or significantly different needs, a phased or pilot group-driven rollout model may be most suitable. In a phased rollout, users whose requirement for administrative privileges is low, or users who are high value targets, may have their privileges modified first. The agency gains an initial security benefit by doing this, which then allowing them to concentrate on users who have more complex operating environments.

Alternatively, a pilot group approach may be more appropriate. Volunteers or staff with a technical background from each of the groups with unique or similar requirements may have their environments modified first, in order to feed any suggestions or issues back to administrative staff. Once these issues have been overcome, changes can be rolled out to the entire organisation with a high degree of confidence that the negative impact on users will be minimal. The advantage of this approach is that any potential issues can be identified and dealt with before they impact on a significant portion of the user base.

Finally, there may be users whose requirements are significantly different from the majority of the user base and who require regular access to some form of administrative permissions. These users should have multiple accounts as discussed earlier. This will allow fine-grained control over the actions these users are permitted to take.

IMPLEMENTATION NOTES:

ADMINISTRATIVE PRIVILEGES IMPLEMENTATION NOTES

Limitation of Scope

Administrators are unlikely to require access to all computers in an organisation's environment. For example, while it may be appropriate for an email system administrator to have administrative privileges for an Exchange server, they are not likely to require the same access to desktop computers on the network. By placing devices into appropriate OUs within Active Directory (AD), placing administrators within appropriate Security Groups, and assigning the groups the appropriate permissions on the respective OUs, it is possible to tightly limit the scope and possible effect of any given account's privileges. This will ensure that not only is it possible to tightly track the allowed actions of any administrator but also that administrators cannot make inadvertent, accidental or unauthorised changes to the environment.

Delegation of Control

One available method for reducing staff requirements for wide-reaching or domain-level administrative privileges is delegating control of specific objects to users or groups. Broadly, this involves changing the Access Control Lists (ACLs) on objects within AD. Microsoft provides the Delegation of Control Wizard (DCW) to assist in what can be a complex task. This technique is sometimes called role-based administration.

The DCW comes with a built-in set of tasks, which are actually sets of permissions required to perform each specified task. This can be expanded to more than 70 common tasks with replacement of the **Delegwiz.inf** file¹⁵ or custom tasks can be created¹⁶.

Whether by using the DCW or manually assigning permissions to objects in AD, administrative staff can be provided with specifically targeted permissions which will allow them to carry out common tasks without requiring domain or local administrative privileges.

¹⁵ <http://technet.microsoft.com/en-us/library/cc772784.aspx>

¹⁶ <http://support.microsoft.com/kb/308404>

APPLocker IMPLEMENTATION NOTES

Executable Identification Methods

AppLocker can use three methods to identify executable files, each with their own pros and cons.

Path-Based Rules

These rules identify a specific location that contains executable files which are allowed to run. While these are the fastest and simplest rules to implement, care needs to be taken to ensure that users cannot write to any directory which is identified as allowed in a path-based rule, or any of their subdirectories. AppLocker implementations using path-based rules often overlook this requirement, failing to prevent execution to directories such as *C:\Windows\Temp*. This identification method is generally considered to be the least secure, as all files in a trusted path are allowed to execute.

Publisher-Based Rules

Rules which rely upon the certificate used to sign an executable are an intermediate step in terms of speed and complexity between path- and hash-based rules. These rules allow you to identify a publisher's code-signing certificate which you will use to identify allowed executables – Microsoft's code-signing certificate is a common one used to identify all Microsoft-signed executable files. This can be quicker and easier to maintain than a hash-based ruleset as multiple successive versions of a given file are often signed with the same certificate. This can make patching or updating of applications easier to manage than a hash-based ruleset.

While publisher-based rules are more secure than those which are path-based, it should be noted that code-signing certificates can be stolen or revoked. Consideration needs to be given to the security implications of trusting the veracity of any given certificate, especially over an extended period of time. Additionally, many executables (including executables provided as part of the Microsoft Windows operating system) are not signed, requiring path- or hash-based rules in order to run correctly.

Hash-Based Rules

Hash-based rules are the most specific form of rule, specifying that a specific executable file with a specific hash is allowed to execute. While this increases management overhead when an environment is patched or updated, hash generation and deployment can be incorporated into the testing and change management process in order to be carried out in a consistent manner. Hash-based rules are commonly used to cover gaps in, or for exceptions to, path- or publisher-based rules.

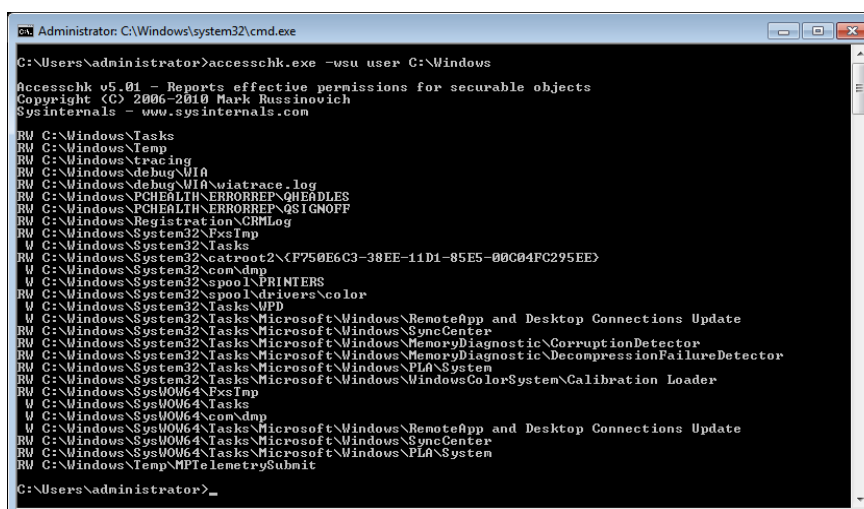
Hash-based rules are the most secure, as they give a high level of assurance that only the specifically identified file is allowed to execute.

Certificate-Based Rules

While certificate-based rules are supported by AppLocker, they can be circumvented if a certificate in a code-signing chain is stolen and used in an intrusion, as occurred in July 2012.¹⁷

Using *accesschk* to Test Permissions

The *accesschk* utility¹⁸ can be used to enumerate permissions for any user on a given directory and its subdirectories. The below example illustrates the process for using *accesschk* to find administrator and user permissions on files and folders within *C:\Windows* and *C:\Program Files* on a Windows 7 workstation with Microsoft Office and Adobe Reader 9 installed:



```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\administrator>accesschk.exe -usu user C:\Windows
Accesschk v5.01 - Reports effective permissions for securable objects
Copyright (C) 2006-2010 Mark Russinovich
Sysinternals - www.sysinternals.com

RW C:\Windows\Tasks
RW C:\Windows\Temp
RW C:\Windows\tracing
RW C:\Windows\debug\MIa
RW C:\Windows\debug\MIa\wiatrace.log
RW C:\Windows\PCHEALTH\ERRORREP\QHEADLES
RW C:\Windows\PCHEALTH\ERRORREP\QSIGNOFF
RW C:\Windows\Registration\CRLLog
RW C:\Windows\System32\ExsImp
W C:\Windows\System32\Tasks
RW C:\Windows\System32\catroot2\F750E6C3-38EE-11D1-85E5-00C04FC295EE
W C:\Windows\System32\comNdp
W C:\Windows\System32\pool\PRINTERS
RW C:\Windows\System32\pool\drivers\color
W C:\Windows\System32\Tasks\MPD
W C:\Windows\System32\Tasks\Microsoft\Windows\RemoteApp and Desktop Connections Update
RW C:\Windows\System32\Tasks\Microsoft\Windows\SyncCenter
RW C:\Windows\System32\Tasks\Microsoft\Windows\MemoryDiagnostic\CorruptionDetector
RW C:\Windows\System32\Tasks\Microsoft\Windows\MemoryDiagnostic\DecompressionFailureDetector
RW C:\Windows\System32\Tasks\Microsoft\Windows\PLA\System
RW C:\Windows\System32\Tasks\Microsoft\Windows\WindowsColorSystem\Calibration Loader
RW C:\Windows\SysMOW64\ExsImp
W C:\Windows\SysMOW64\Tasks
W C:\Windows\SysMOW64\comNdp
W C:\Windows\SysMOW64\Tasks\Microsoft\Windows\RemoteApp and Desktop Connections Update
RW C:\Windows\SysMOW64\Tasks\Microsoft\Windows\SyncCenter
RW C:\Windows\SysMOW64\Tasks\Microsoft\Windows\PLA\System
RW C:\Windows\Temp\MPTelemetrySubnit
C:\Users\administrator>
```

¹⁷ <http://blog.bit9.com/2013/02/25/bit9-security-incident-update/>

¹⁸ <http://www.microsoft.com/technet/sysinternals/Utilities/AccessChk.msp>

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\administrator>accesschk.exe -usu user "C:\Program Files"
Accesschk v5.01 - Reports effective permissions for securable objects
Copyright (C) 2006-2010 Mark Russinovich
Sysinternals - www.sysinternals.com
No matching objects found.

C:\Users\administrator>accesschk.exe -usu user "C:\Program Files (x86)"
Accesschk v5.01 - Reports effective permissions for securable objects
Copyright (C) 2006-2010 Mark Russinovich
Sysinternals - www.sysinternals.com
No matching objects found.

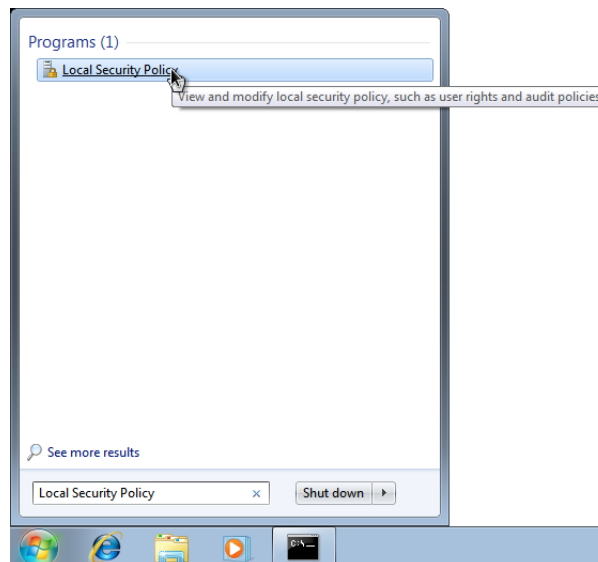
C:\Users\administrator>
```

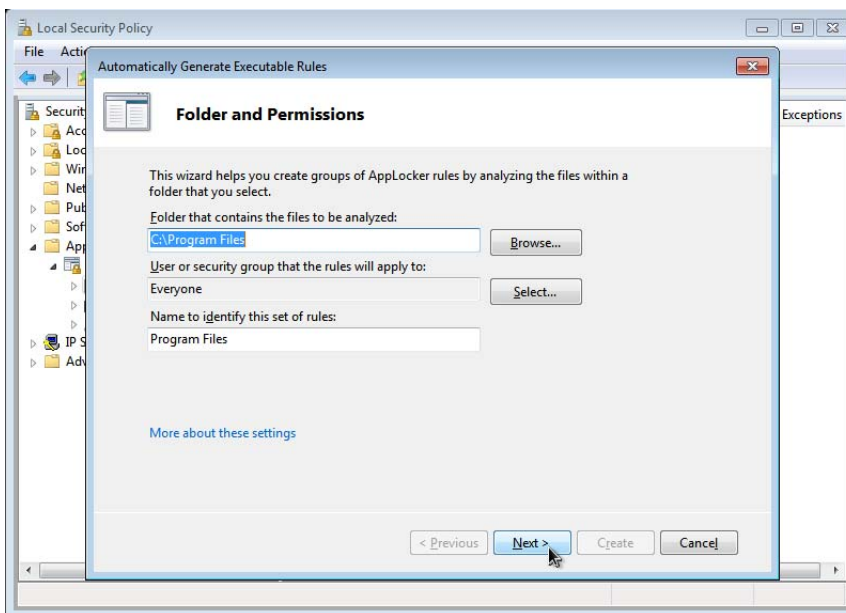
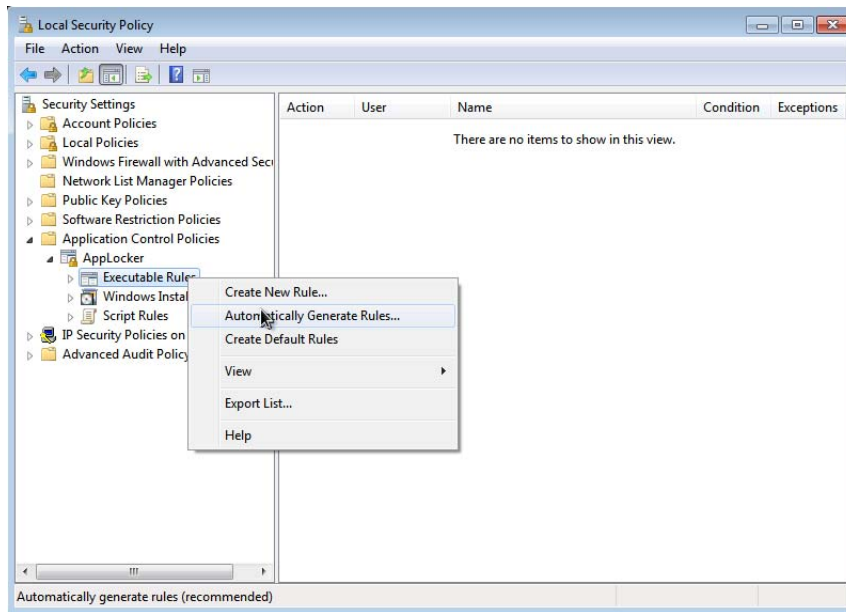
All files and folders listed here are writeable or readable and writable (W or RW in the first column, respectively). In a path-based ruleset, if including *C:\Windows* as an allowed directory, these locations would need to be explicitly blocked using AppLocker. This will be further detailed in the next section.

How to Enable AppLocker

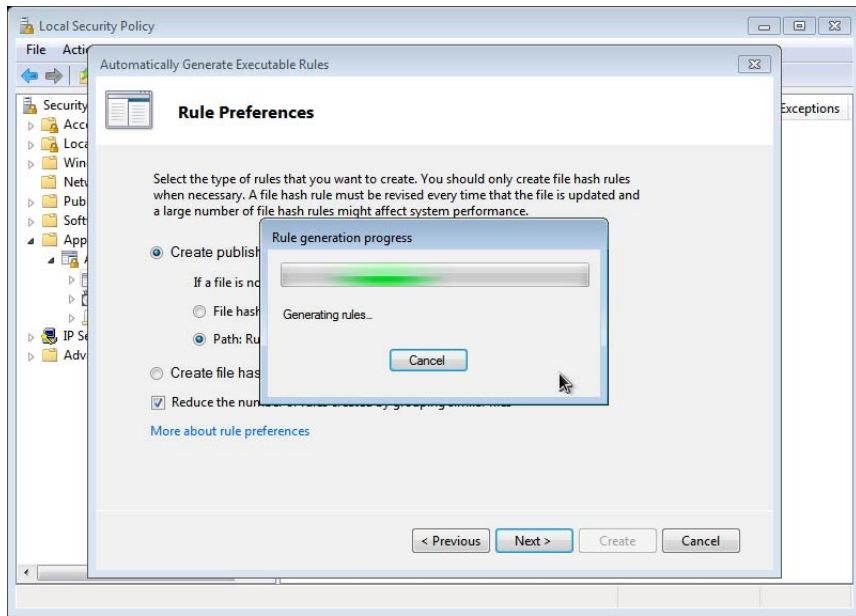
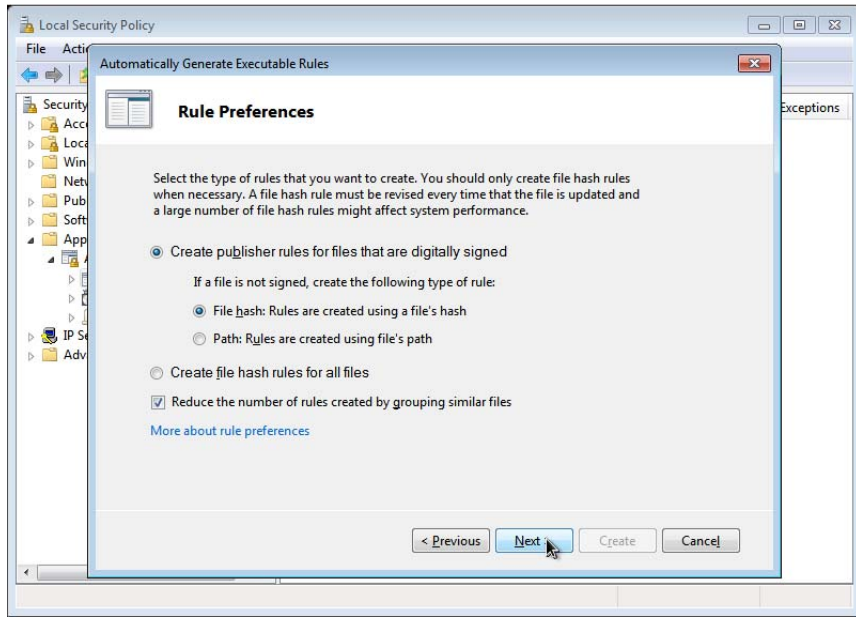
Below are example steps to use a reference computer to automatically generate AppLocker rules for 64-bit Windows 7 computers within a Server 2008 R2 domain.

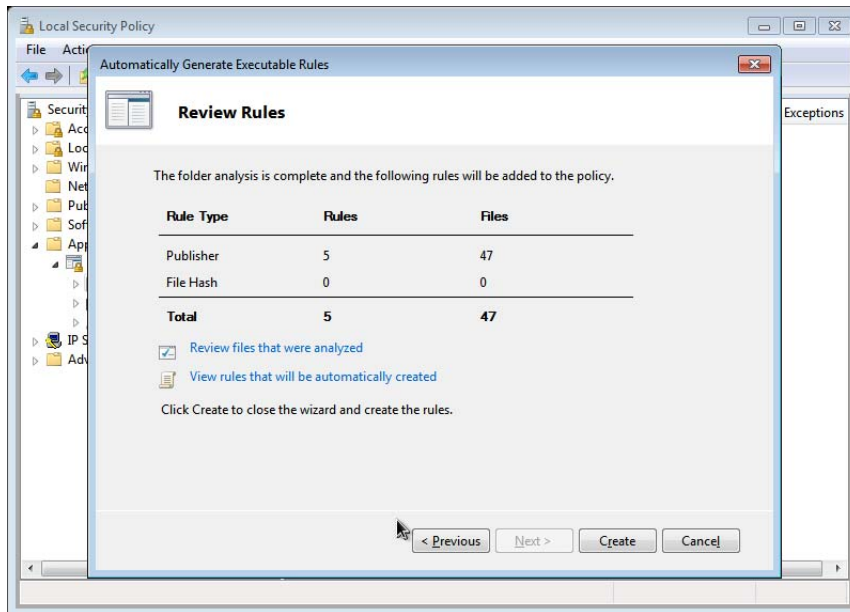
The Local Security Policy MMC snap-in can be used to complete the rule generation wizard:



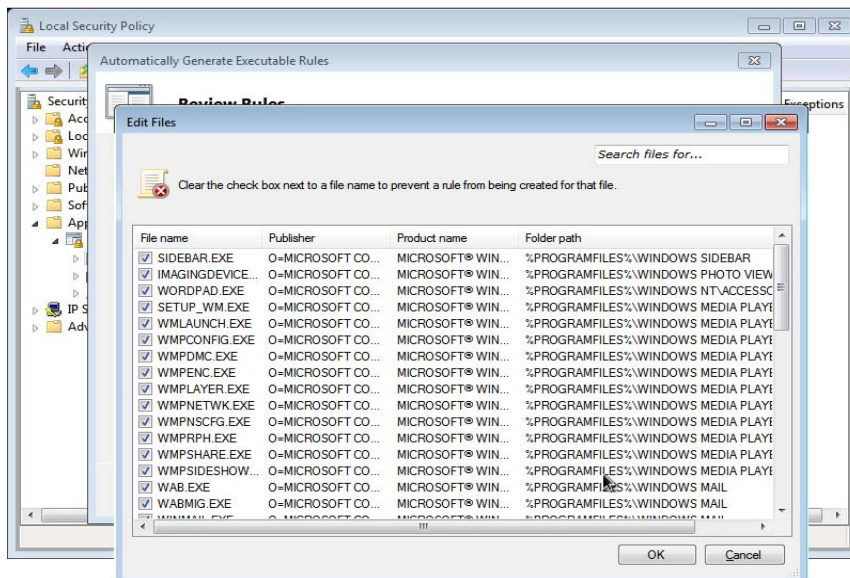


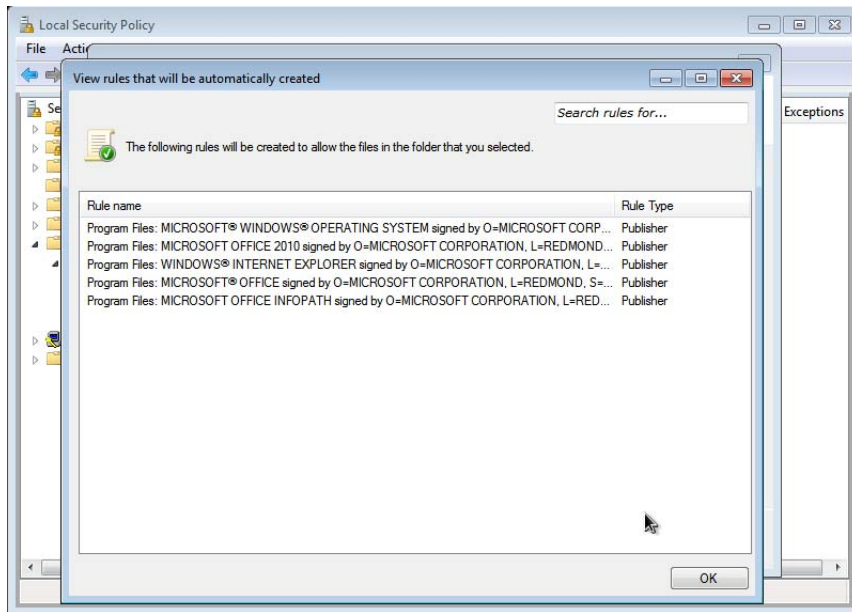
Note that in this instance you are choosing to create signature- or hash-based rules. First, create some rules for the Program Files directory:



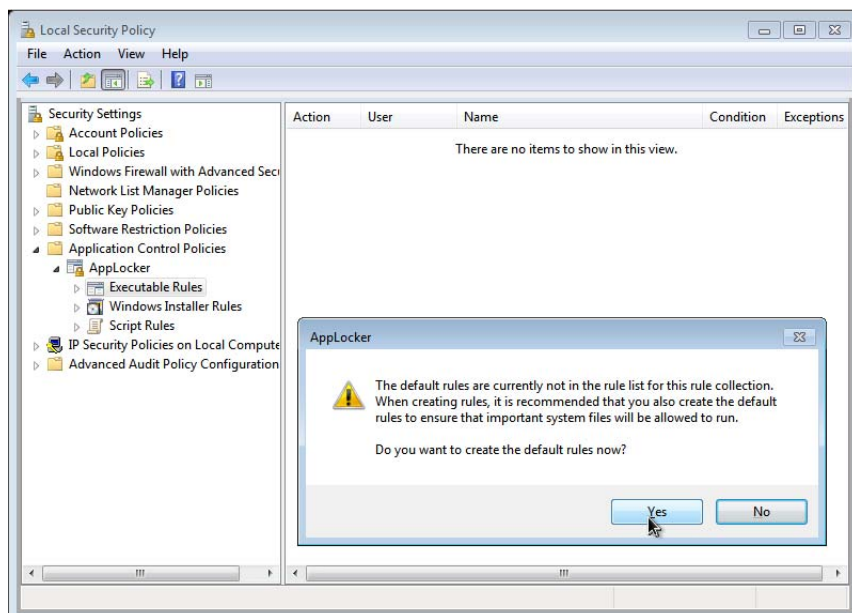


From here you can view the rules that were generated, as well as any errors encountered. Errors may occur for transient files or files that are being written to at the time of the scan. Any files you don't want rules created for can be deselected via the 'Review files that were analysed' link.

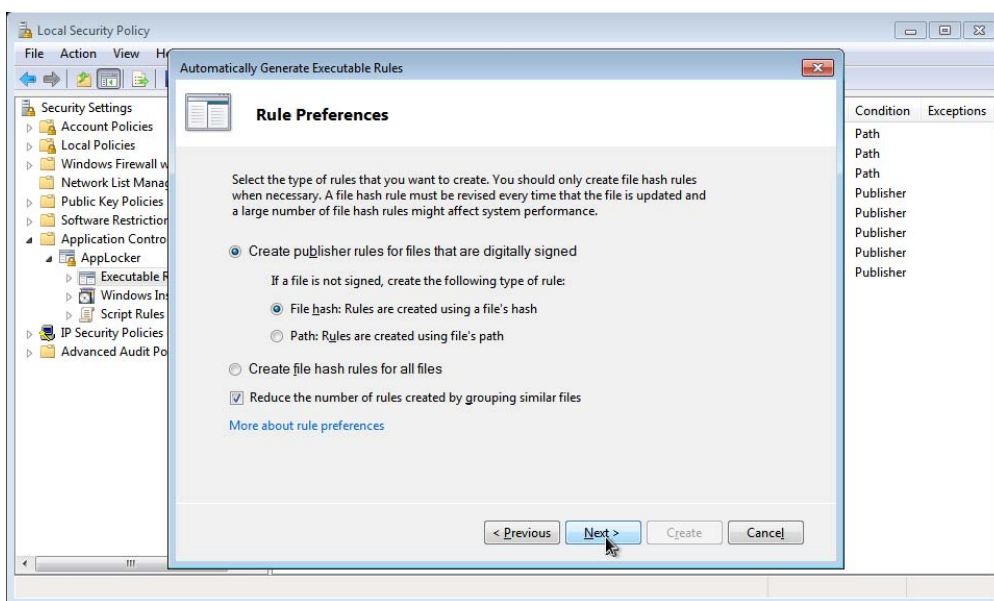
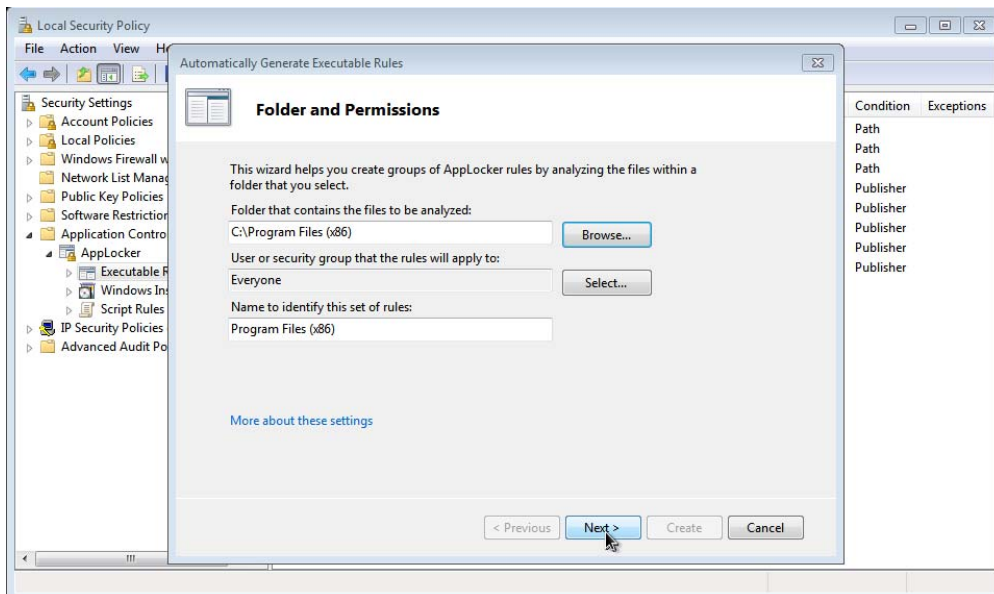


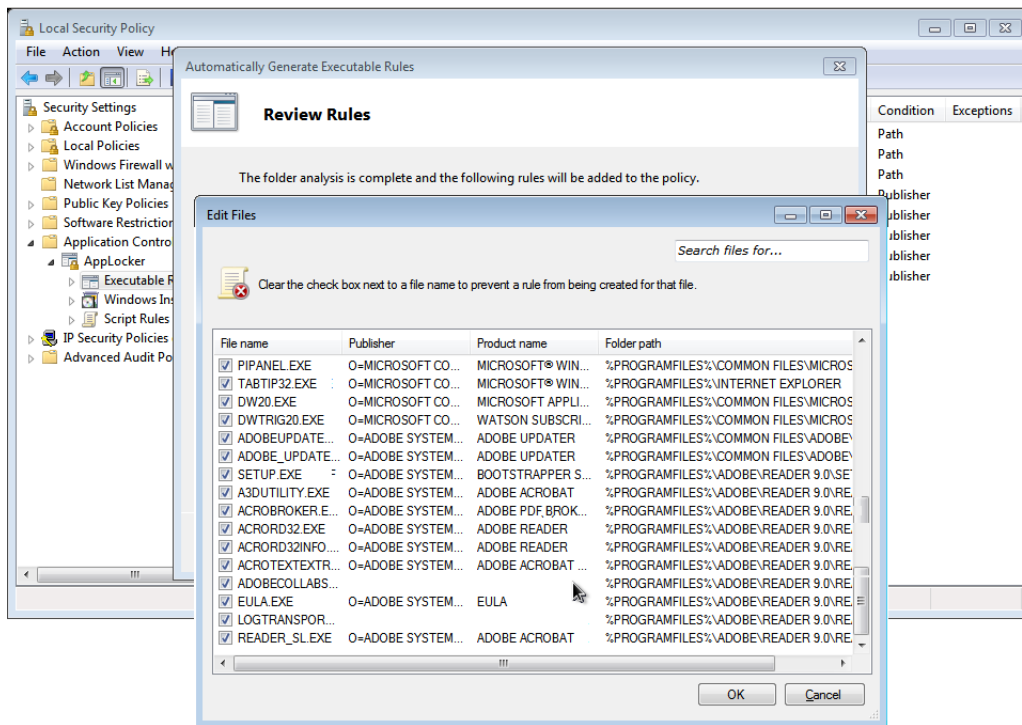
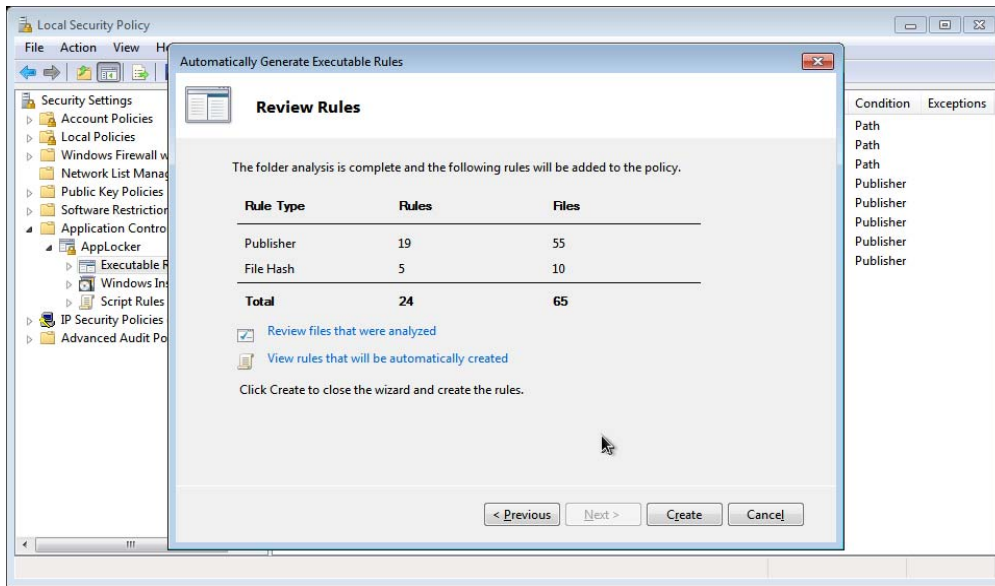


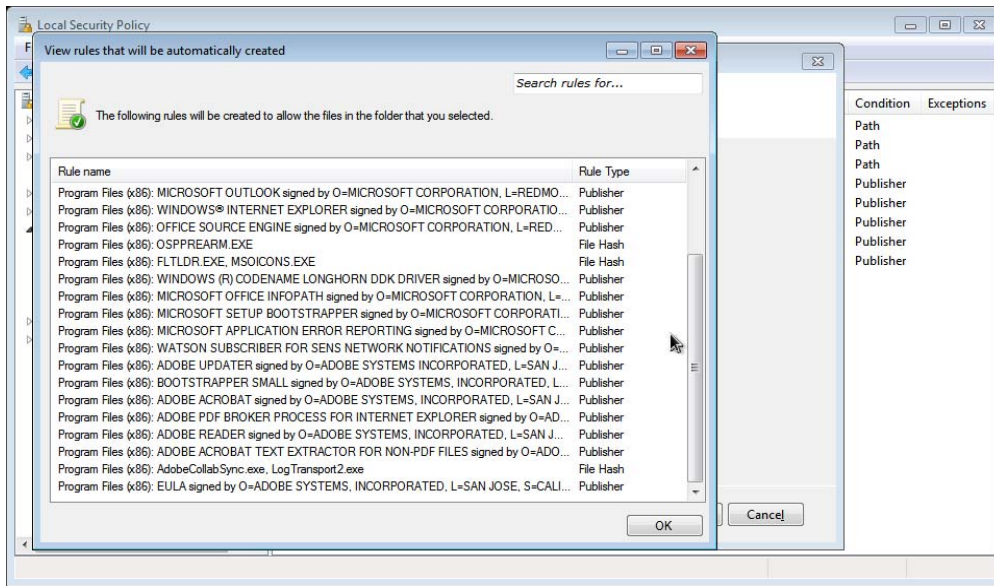
Click 'Create' to create the automatically-generated rules. If this is the first rule in this ruleset, you will be prompted to create a default set of rules. This will cover Microsoft Windows executables and directories. This will create several path-based rules which you can later edit.



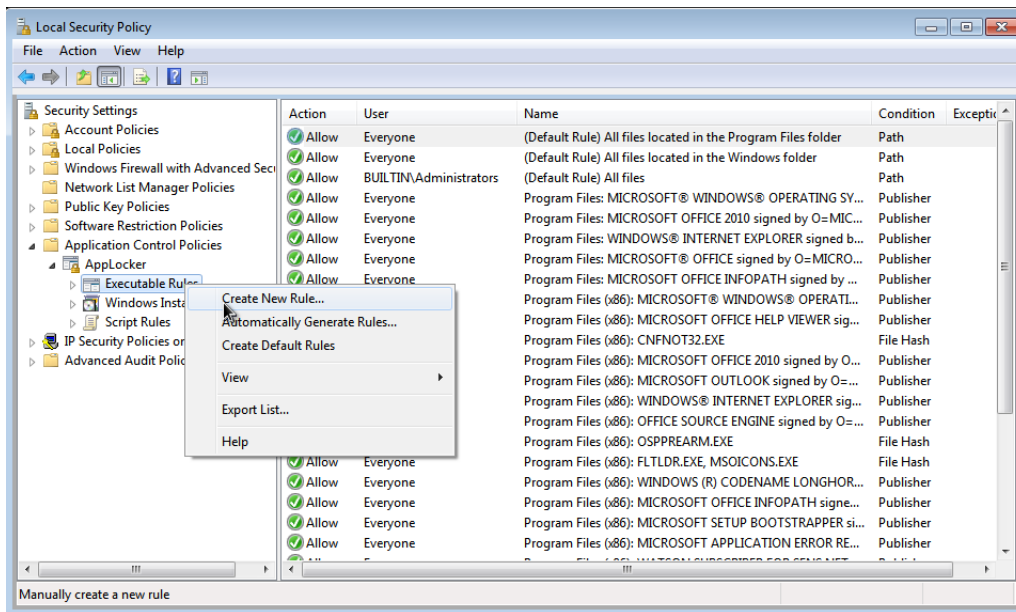
Next, as this is 64-bit Windows 7, you carry out the same steps for *Program Files (x86)*:

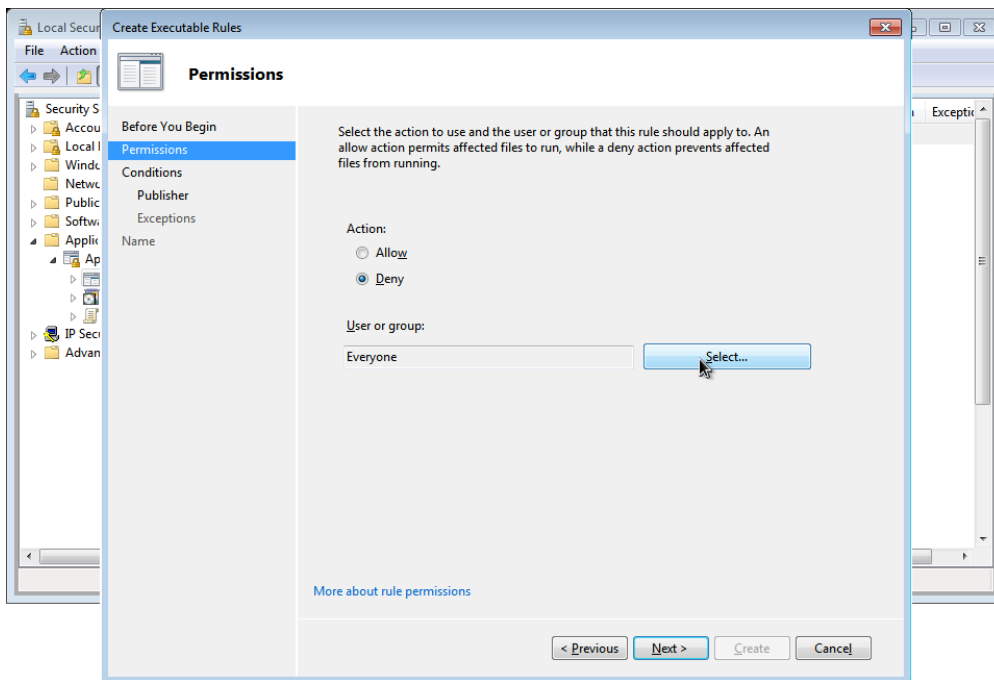
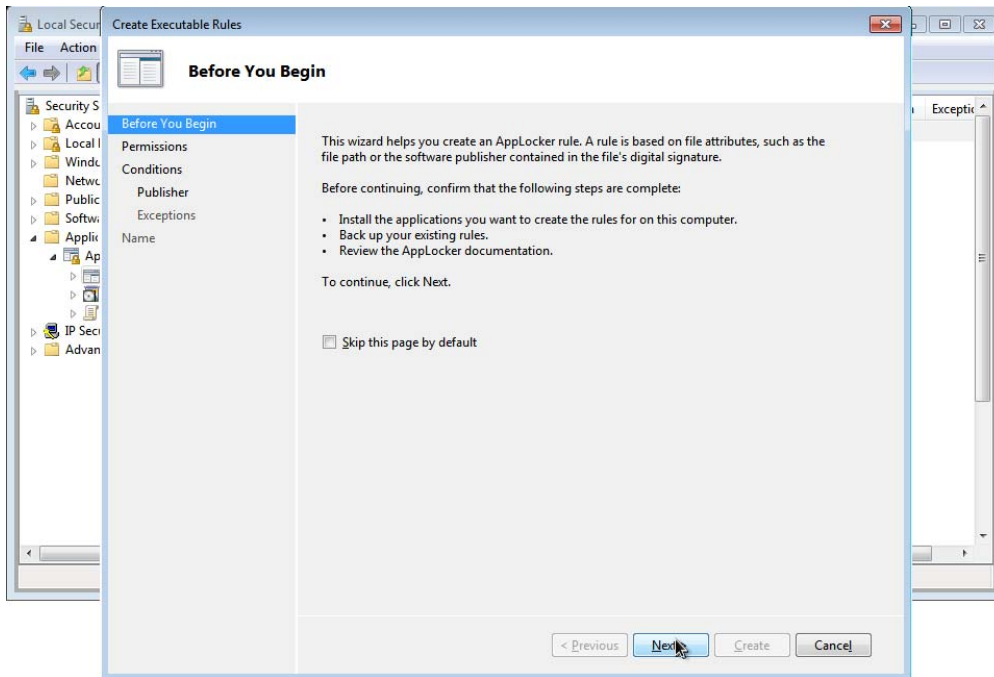


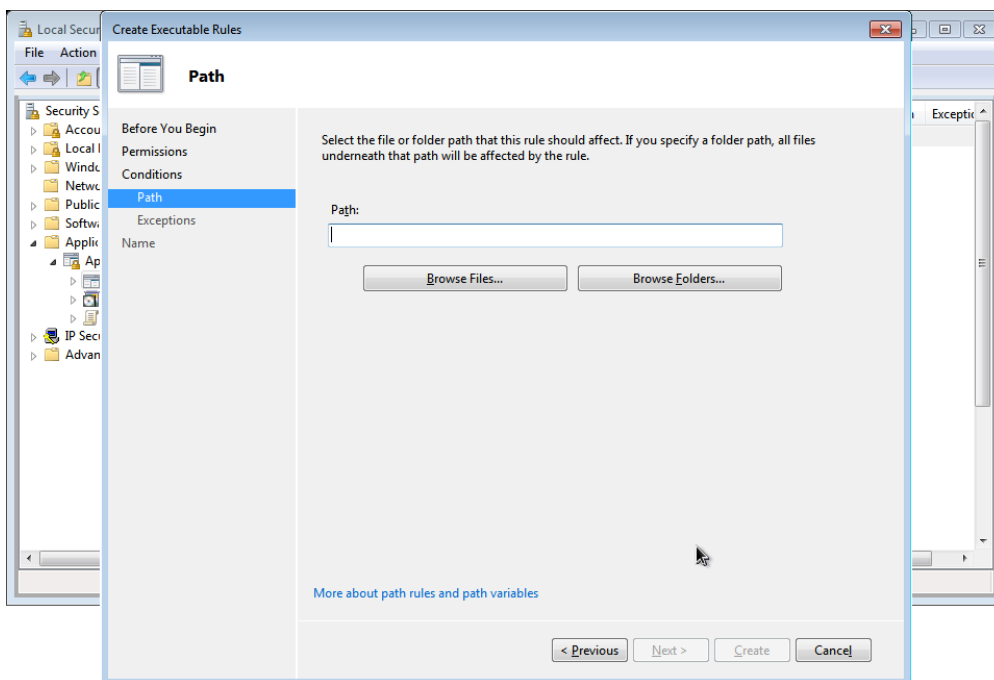
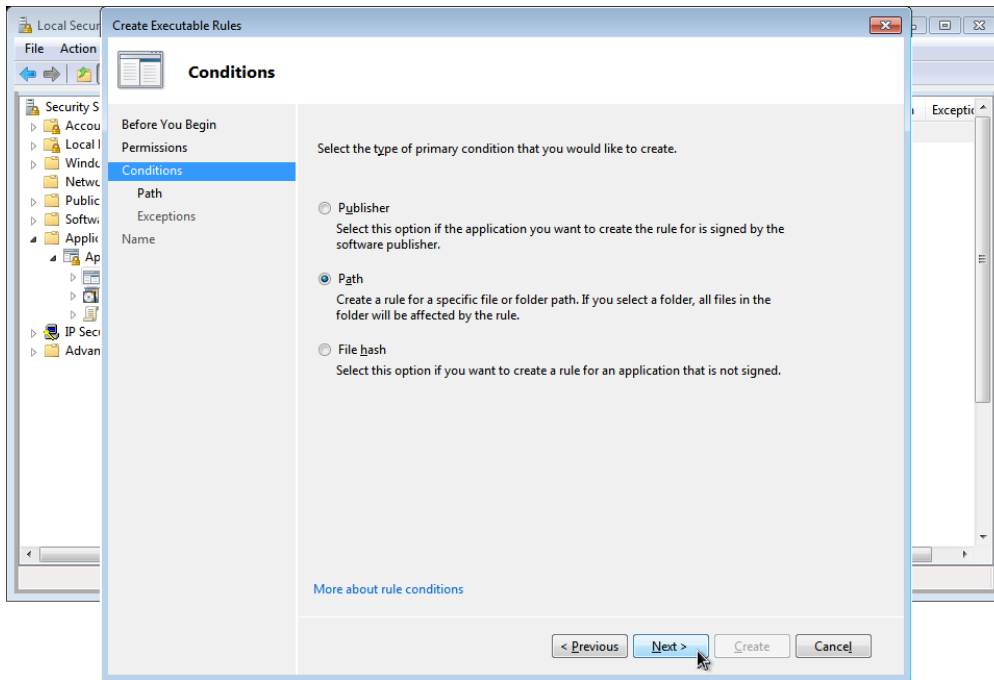




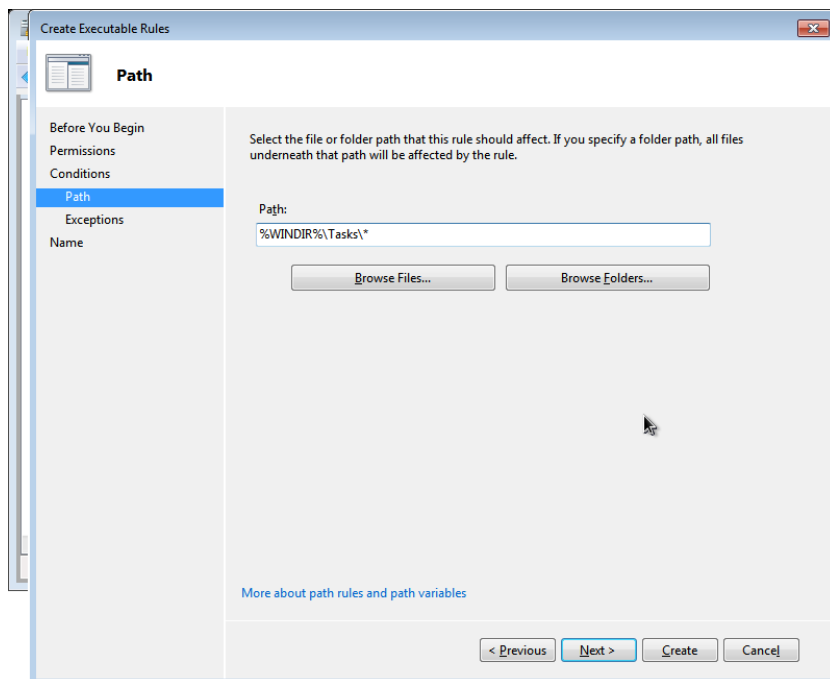
You now have a set of rules which was generated based upon software currently installed on this computer. There is one more change required: you need to create Deny rules for the writable directories you discovered using *accesschk*.



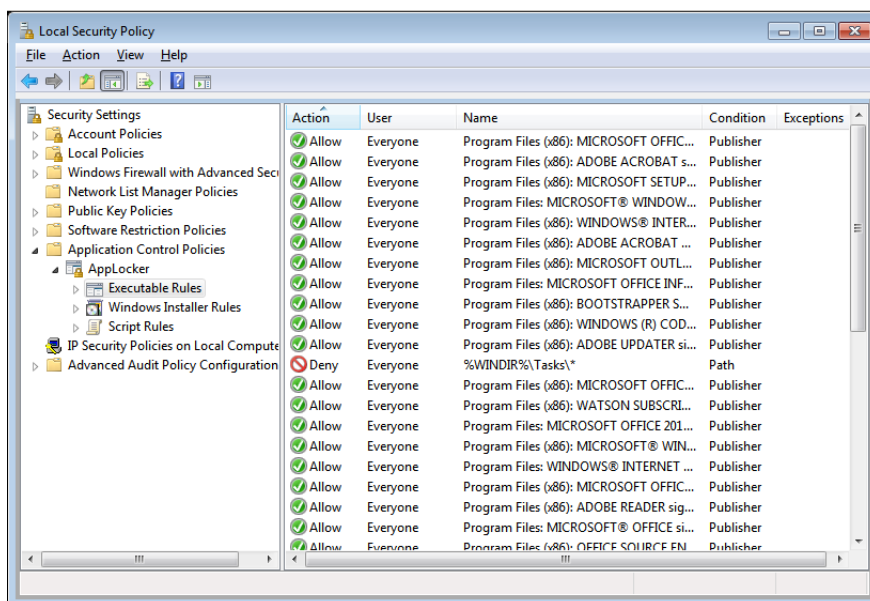




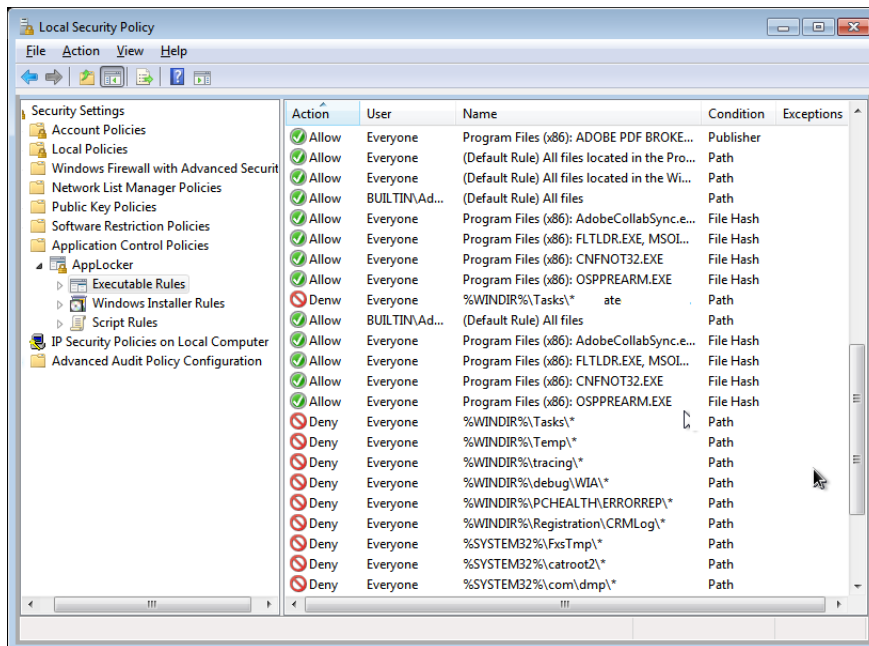
Here you need to enter one of the writable paths discovered in the previous section:



You now have a path Deny rule in place.



You need to do the same for all other writeable paths identified via **accesschk**. Note that you can group paths together to reduce the total volume of rules used:



A QUICK CHECK OF YOUR AGENCY'S IMPLEMENTATION STATUS

The following guidance is intended for agency admins to conduct a quick check of their agency's implementation status. This section outlines some system commands that agency IT administrators can run on Microsoft Windows systems to make an initial assessment of the Top 4 strategies have been implemented on that system, and does not constitute an exhaustive system audit.

Application Whitelisting

1. Run a command prompt

Start Menu -> cmd.exe

2. Check that you can run Microsoft's calculator application

```
c: \wi ndows\system32\cal c. exe
```

3. Check if application whitelisting prevents unapproved programs from being run from your h:\

```
copy /b c: \wi ndows\system32\cal c. exe + c: \wi ndows\system32\cal c. exe h: \cal c2. exe  
h: \cal c2
```

4. Check if application whitelisting prevents unapproved programs from being run from your user profile's temp directory

```
copy /b c: \wi ndows\system32\cal c. exe + c: \wi ndows\system32\cal c. exe  
%temp%\cal c2. exe  
%temp%\cal c2
```

5. Check if application whitelisting prevents unapproved programs from being run from permitted directories that incorrectly enable the user to write/execute programs from e.g. c:\windows\temp

```
copy /b c: \wi ndows\system32\cal c. exe + c: \wi ndows\system32\cal c. exe  
c: \wi ndows\temp\cal c2. exe  
c: \wi ndows\temp\cal c2
```

6. Check if application whitelisting prevents unapproved .dll software libraries from being run from your h:\

```
copy /b c: \wi ndows\system32\shel l 32. dl l + c: \wi ndows\system32\shel l 32. dl l  
h: \shel l 32x. dl l  
rundl l 32 h: \shel l 32x. dl l , Shel l AboutA
```

7. Check if application whitelisting prevents unapproved .dll software libraries from being run from your user profile's temp directory


```
copy /b c:\windows\system32\shell32.dll + c:\windows\system32\shell32.dll
%temp%\shell32x.dll
```

```
rundll32 %temp%\shell32x.dll, ShellAboutA
```

8. Check if application whitelisting prevents unapproved .dll software libraries from being run from permitted directories that incorrectly enable the user to write/execute programs from e.g. c:\windows\temp

```
copy /b c:\windows\system32\shell32.dll + c:\windows\system32\shell32.dll
c:\windows\temp\shell32x.dll
```

```
rundll32 c:\windows\temp\shell32x.dll, ShellAboutA
```

9. For completeness, the following command can be run from c:\windows and c:\program files to identify any directories where users have permission to write to and execute from, noting that the Microsoft accesschk.exe program is more suitable than cacls

```
cacls . /c /t > h:\cacls.txt
```

```
notepad h:\cacls.txt
```

look for users:f or users:c or generic_write

Patching Applications

1. Preferably ask the system/network administrator if there is existing patch deployment infrastructure in place e.g. Microsoft WSUS or System Centre.
2. Determine which applications are installed and their version

```
wmic product list > product.txt
```

```
notepad product.txt
```

3. Alternatively, manually check the versions of Adobe Reader, web browser(s) such as Internet Explorer and Firefox, Microsoft Office, and java (by using a command prompt to run `java -version`)

Patching Operating Systems

1. Preferably ask the system/network administrator if there is existing patch deployment infrastructure in place e.g. Microsoft WSUS or System Centre.
2. Determine which patches are installed and the date when they were installed

```
wmic qfe list > qfe.txt
```

```
notepad qfe.txt
```

3. Internet resources such as <http://go.microsoft.com/fwlink/?LinkID=245778> or <http://kbupdate.info> provide details of each KB update and when it was released by Microsoft.

Minimising Local/Admin Privileges

1. Check if the current user is part of a local/domain administrator group or power user group
`gpresult /r`
2. On a domain controller, check how many users are part of Domain Admin and similar elevated groups, noting that business context is necessary to determine if this number is justified.