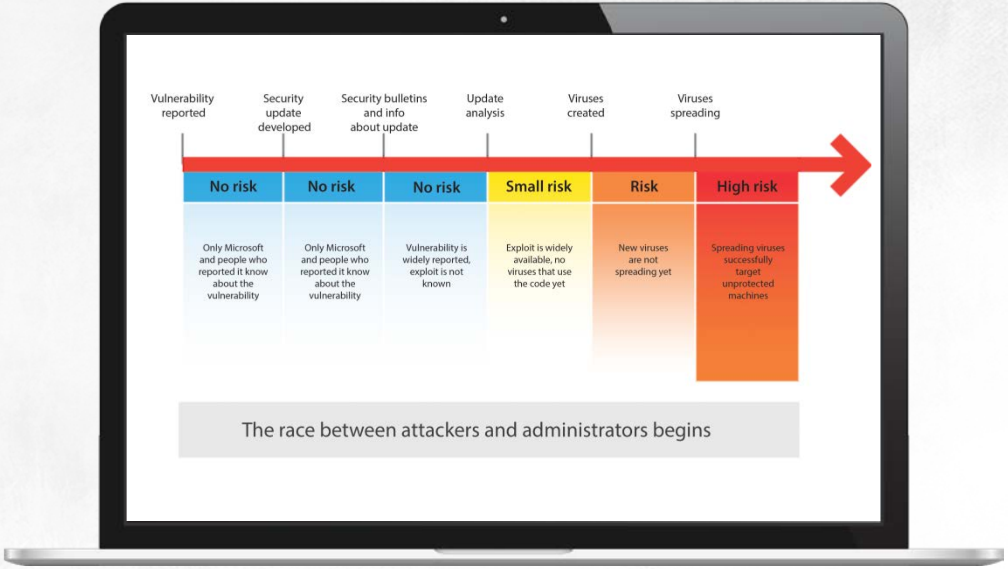
Managing Applications

Software updates

Software vendors develop and release updates to fix discovered security problems in their products and protect their clients. This solution however has its flaws:

- Because security fixes are publically available, also attackers get them
- On-and-off security update installation you do on your own is time-consuming and incomplete


Vulnerability reported
Security update developed
Security bulletins and info about update
Update analysis
Viruses created
Viruses spreading
No risk
No risk
No risk
Small risk
Risk
High risk
Only Microsoft and people who reported it know about the vulnerability
Only Microsoft and people who reported it know about the vulnerability
Vulnerability is widely reported, exploit is not known
Exploit is widely available, no viruses that use the code yet
New viruses are not spreading yet
Spreading viruses successfully target unprotected machines
The race between attackers and administrators begins

Software updates

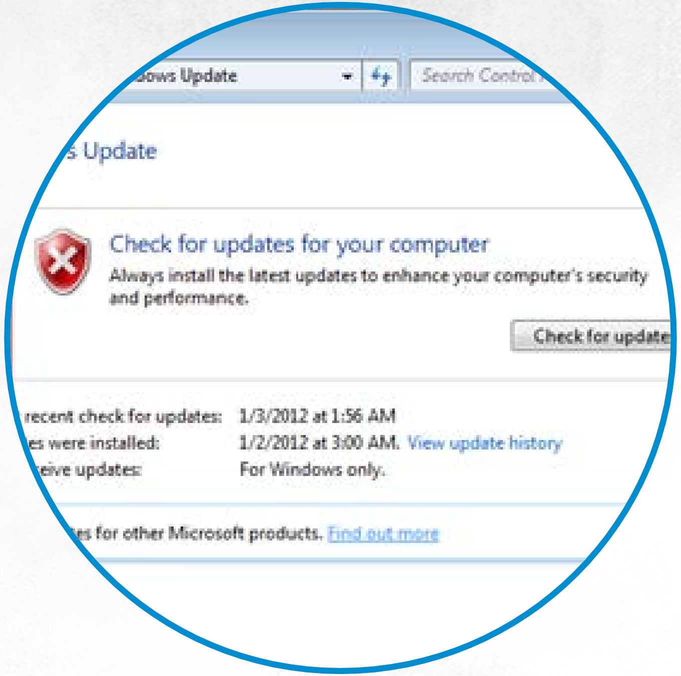
Depending on the size of your system, here is the software you should pick to automate Microsoft software updates:

- Microsoft Update for home PCs
- Microsoft Update for small enterprise systems that don’t have a Windows server
- Windows Server Update Services for enterprise systems with at least one Windows 2000 (or newer) server
- System Center Configuration Manager for enterprises that have adopted a policy of full control over all software updates

Software updates

Microsoft Update

You can update Windows and several dozen other Microsoft applications and additional OS components manually, or the process can be automated



Check for updates for your computer

Always install the latest updates to enhance your computer's security and performance.

recent check for updates: 1/3/2012 at 1:56 AM

es were installed: 1/2/2012 at 3:00 AM. View update history

eive updates: For Windows only.

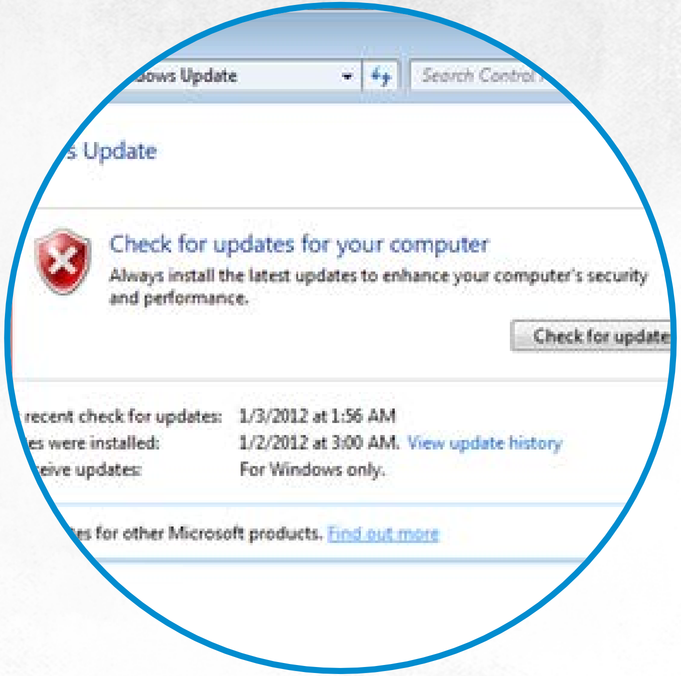
es for other Microsoft products. Find out more

Software updates

Microsoft Update

Here’s how it works:

- Every 17-22 hours the program checks for new updates (the schedule is changeable to avoid a situation where computers worldwide connect to a Microsoft Update server at the same time)
- The MU server is verified, and signatures for available updates are downloaded
- The program searches for missing updates (not installed in the local host)
- Depending on the settings:
    - Users are notified about new available updates
    - Updates are automatically downloaded
    - Updates are automatically downloaded and installed
- System registry logs information about installed updates



s Update

Check for updates for your computer

Always install the latest updates to enhance your computer's security and performance.

recent check for updates: 1/3/2012 at 1:56 AM

es were installed: 1/2/2012 at 3:00 AM. View update history

eive updates: For Windows only.

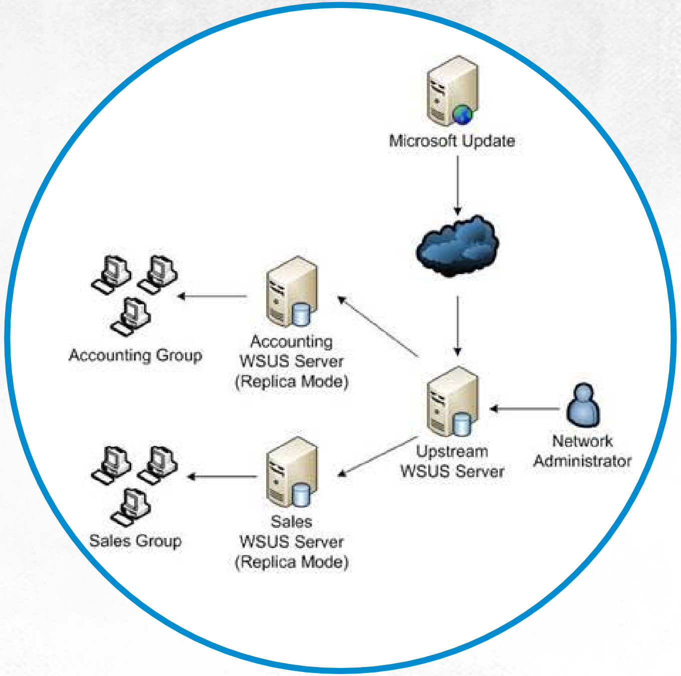
es for other Microsoft products. Find out more

Software updates

Microsoft Update

WSUS is a feature of Windows Server 2008 and you don’t need to pay more to deploy it

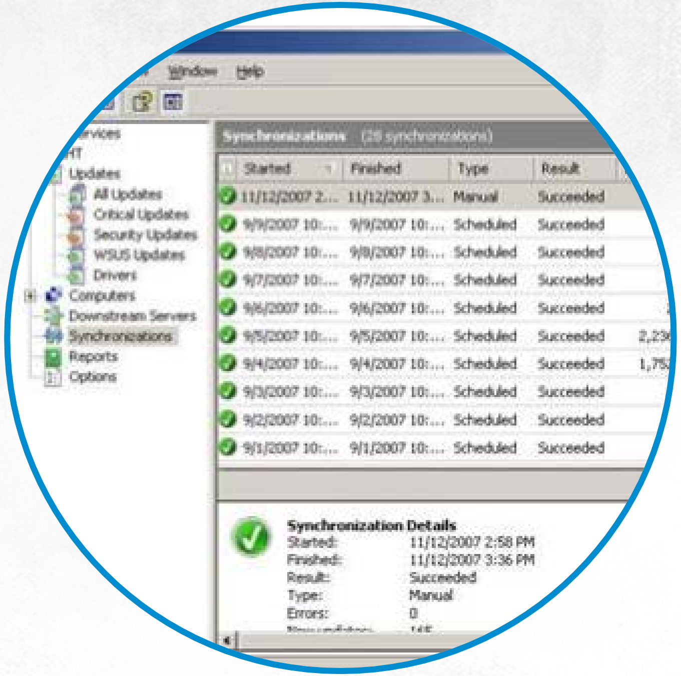
You can simply give WSUS the role of a local Microsoft Update server. When you do this, your individual client computers will not need to download updates multiple times from the Internet



Software updates

Microsoft Update

WSUS, however, is capable of much more. It can allow you to create automatic update policies on selected computers, check for missing updates, notify administrators about available updates and keep track of software update state on selected computers thanks to a built-in report feature



Synchronizations (28 synchronizations)

Started	Finished	Type	Result	
11/12/2007 2...	11/12/2007 3...	Manual	Succeeded	
9/9/2007 10:...	9/9/2007 10:...	Scheduled	Succeeded	
9/8/2007 10:...	9/8/2007 10:...	Scheduled	Succeeded	
9/7/2007 10:...	9/7/2007 10:...	Scheduled	Succeeded	
9/6/2007 10:...	9/6/2007 10:...	Scheduled	Succeeded	2
9/5/2007 10:...	9/5/2007 10:...	Scheduled	Succeeded	2,23
9/4/2007 10:...	9/4/2007 10:...	Scheduled	Succeeded	1,75
9/3/2007 10:...	9/3/2007 10:...	Scheduled	Succeeded	
9/2/2007 10:...	9/2/2007 10:...	Scheduled	Succeeded	
9/1/2007 10:...	9/1/2007 10:...	Scheduled	Succeeded	

Synchronization Details

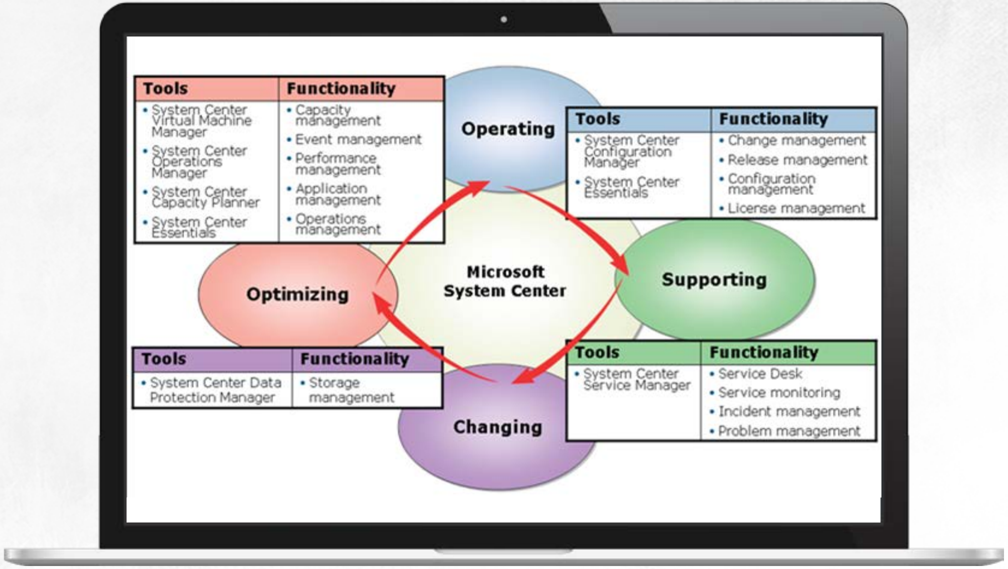
Started:	11/12/2007 2:58 PM
Finished:	11/12/2007 3:36 PM
Result:	Succeeded
Type:	Manual
Errors:	0

Software updates

System Center Configuration Manager

SCCM audits and manages remote computers
It can allow you to:

- Check their hardware and software configurations
- Manage computers in a workstation
- Keep track of installed software
- Report collected information
- Load and start software
- Distribute updates for OS and third-party applications



Tools	Functionality
System Center Virtual Machine Manager System Center Operations Manager System Center Capacity Planner System Center Essentials	Capacity management Event management Performance management Application management Operations management

Tools	Functionality
System Center Configuration Manager System Center Essentials	Change management Release management Configuration management License management

Tools	Functionality
System Center Data Protection Manager	Storage management

Tools	Functionality
System Center Service Manager	Service Desk Service monitoring Incident management Problem management

Block programs from starting

As the threat of users inadvertently running malware grew bigger, a new strategy of defence had to be shaped

Windows XP features a mechanism called software restriction policies. This function allows administrators to decide which programs and scripts may be started by users

Windows 7 Enterprise and Ultimate administrators can use the overhauled (with streamlined settings and more flexibility) equivalent of software restriction policies: application control policies

Administrators can use application control policies to do a variety of tasks, like control users downloading programs from the Internet, fight worms, block the execution of unsigned scripts, prevent the installation and start of banned programs and decide which users are able to modify trusted software vendors list

Block programs from starting

But if these mechanisms are to really prevent users from potentially running malicious programs, either deliberately or accidentally, you need to **set them to block the running of all programs and then create exceptions allowing some programs**

If you only set them to block selected programs, this is much like trying to block selected ports or packets in a firewall. It is hardy possible to block each and every malicious packet, and likewise it is not possible to block all programs by identifying them

Block programs from starting

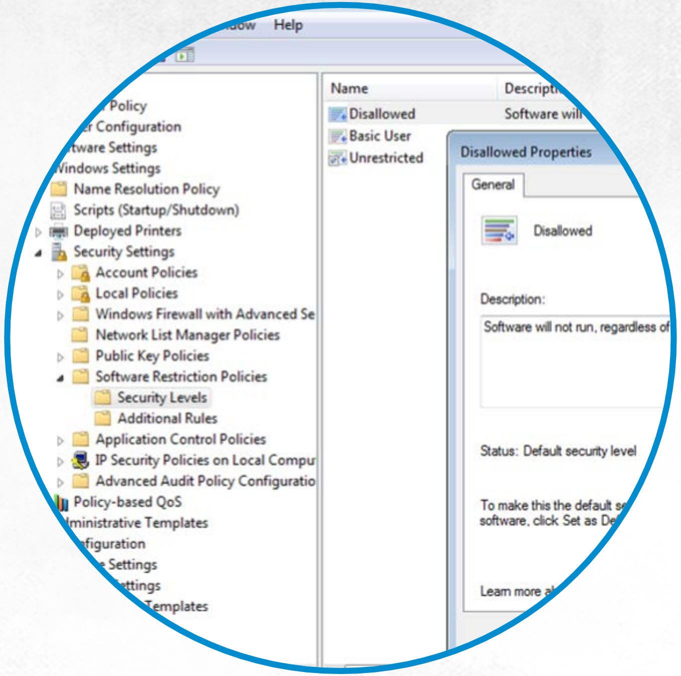
Software restriction policies

Three elements:

- Default security level
- Four types of rules that identify software (certificate, hash, Internet zone and path rules)
- Additional configuration options

Software restriction policies rules are applied in the following order of precedence:

- Hash rule
- Certificate rule
- Path rule
- Internet zone rule
- Default security level 'rule'



Description:

Software will not run, regardless of

Status: Default security level

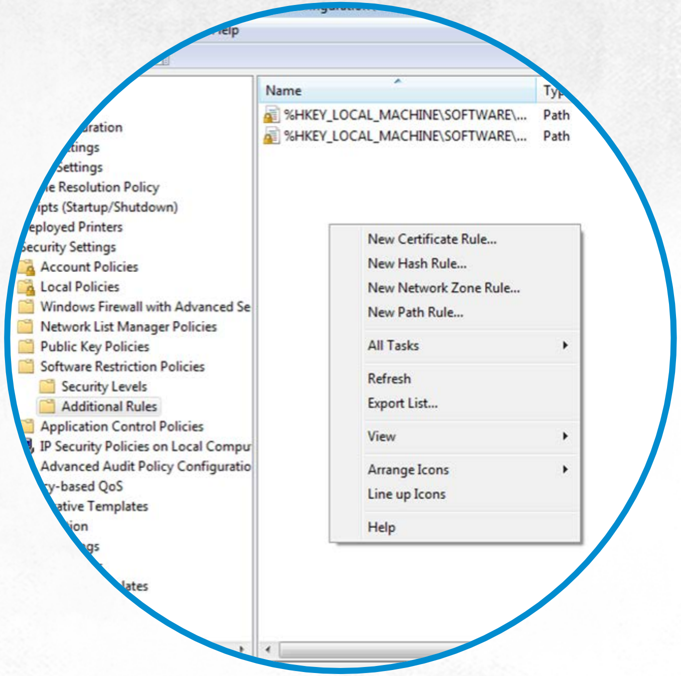
To make this the default se software, click Set as De

Learn more a

Block programs from starting

Software restriction policies

When a first rule can be applied to a launched file, other rules are skipped



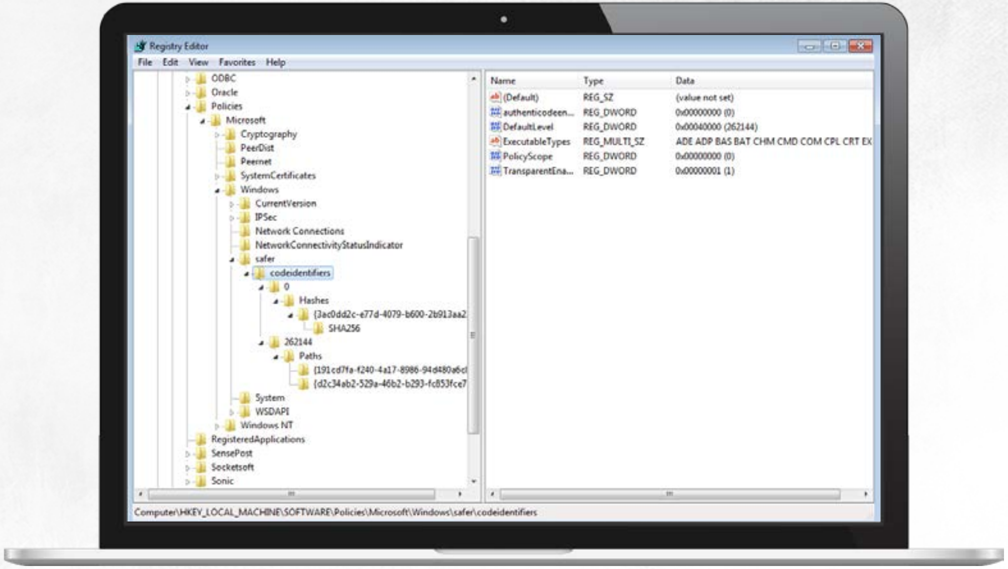
Name	Typ
%HKEY_LOCAL_MACHINE\SOFTWARE\...	Path
%HKEY_LOCAL_MACHINE\SOFTWARE\...	Path

Block programs from starting

Software restriction policies

Before a program or script can be launched, Windows will check if software restriction policies allow it to be started. This applies to among others:

- Win API CreateProcess
- Ntdll.dll
- Command line
- Script environment



```
ODBC
Oracle
Policies
    Microsoft
        Cryptography
        PeerDist
        Peernet
        SystemCertificates
        Windows
            CurrentVersion
            IPSec
            Network Connections
            NetworkConnectivityStatusIndicator
            safer
                codeidentifiers
                    0
                        Hashes
                            {3ac0dd2c-e77d-4079-b600-2b913aa2
                                SHA256
                    262144
                        Paths
                            {191cd7fa-f240-4a17-8986-94d480a6cl
                            {d2c34ab2-529a-46b2-b293-fc853fce7
            System
            WSDAPI
        Windows NT
RegisteredApplications
SensePost
Socketsoft
Sonic
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
authenticodeen...	REG_DWORD	0x00000000 (0)
DefaultLevel	REG_DWORD	0x00040000 (262144)
ExecutableTypes	REG_MULTI_SZ	ADE ADP BAS BAT CHM CMD COM CPL CRT EX
PolicyScope	REG_DWORD	0x00000000 (0)
TransparentEna...	REG_DWORD	0x00000001 (1)

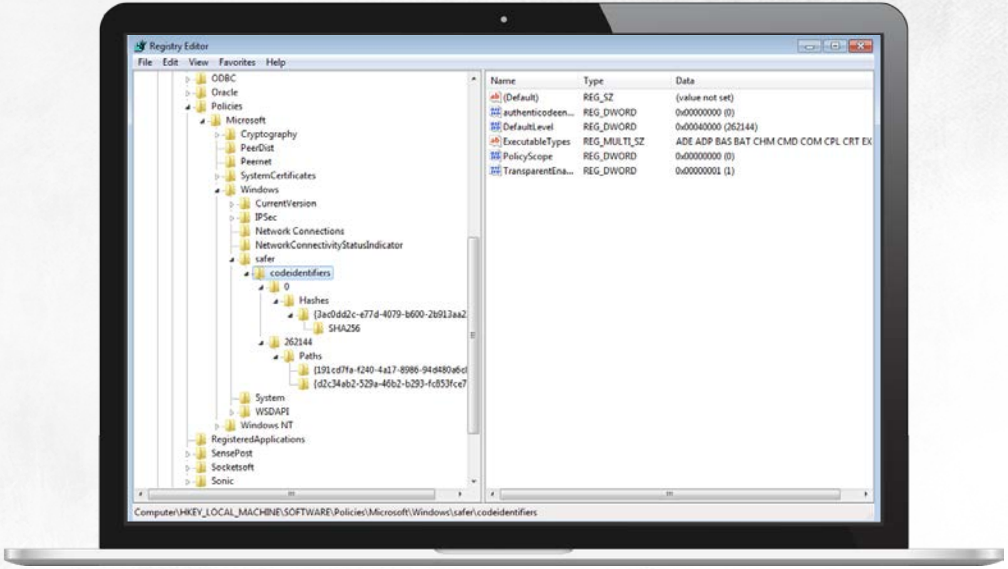
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers

Block programs from starting

Software restriction policies

The key is read:
HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Safer\CodeIdentifiers\TransparentEnabled

If the policies are active, the system checks if the file to be started is covered under one rule saved in the CodeIdentifiers key. If it is, it checks if the file is allowed to be run



```
ODBC
Oracle
Policies
  Microsoft
    Cryptography
    PeerDist
    Peernet
    SystemCertificates
    Windows
      CurrentVersion
      IPSec
      Network Connections
      NetworkConnectivityStatusIndicator
      safer
        codeidentifiers
          0
            Hashes
              {3ac0dd2c-e77d-4079-b600-2b913aa2
                SHA256
          262144
            Paths
              {191cd7fa-f240-4a17-8986-94d480a6c
              {d2c34ab2-529a-46b2-b293-fc853fce7
      System
      WSDAPI
    Windows NT
RegisteredApplications
SensePost
Socketsoft
Sonic
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
authenticodeen...	REG_DWORD	0x00000000 (0)
DefaultLevel	REG_DWORD	0x00040000 (262144)
ExecutableTypes	REG_MULTI_SZ	ADE ADP BAS BAT CHM CMD COM CPL CRT EX
PolicyScope	REG_DWORD	0x00000000 (0)
TransparentEna...	REG_DWORD	0x00000001 (1)

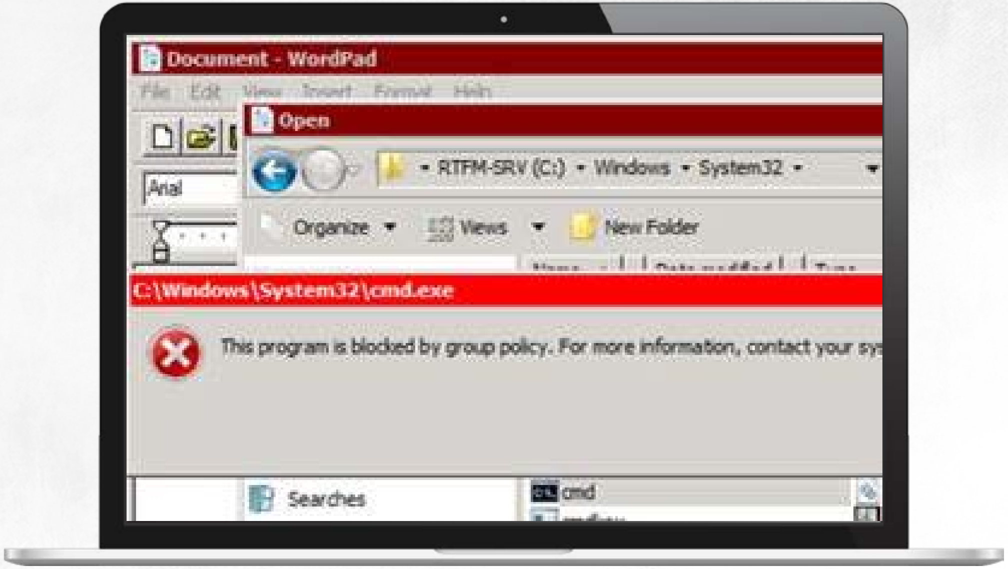
Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\safer\codeidentifiers

Block programs from starting

Software restriction policies

This mechanism can only be circumvented if you can make the launched file not fit any of your defined rules, which, depending on the used rule type, will require a user to:

- Change file name or location for path rules
- Change file content for hash rules
- Assign the website from which a file will be downloaded to a different Internet Explorer zone for Internet zone rules
- Delete and/or sign file with a different certificate for certificate rules



Document - WordPad
File Edit View Insert Format Help
Open
Arial
▸ RTFM-SRV (C:) ▸ Windows ▸ System32 ▸
Organize ▾
Views ▾
New Folder
Searches
cmd

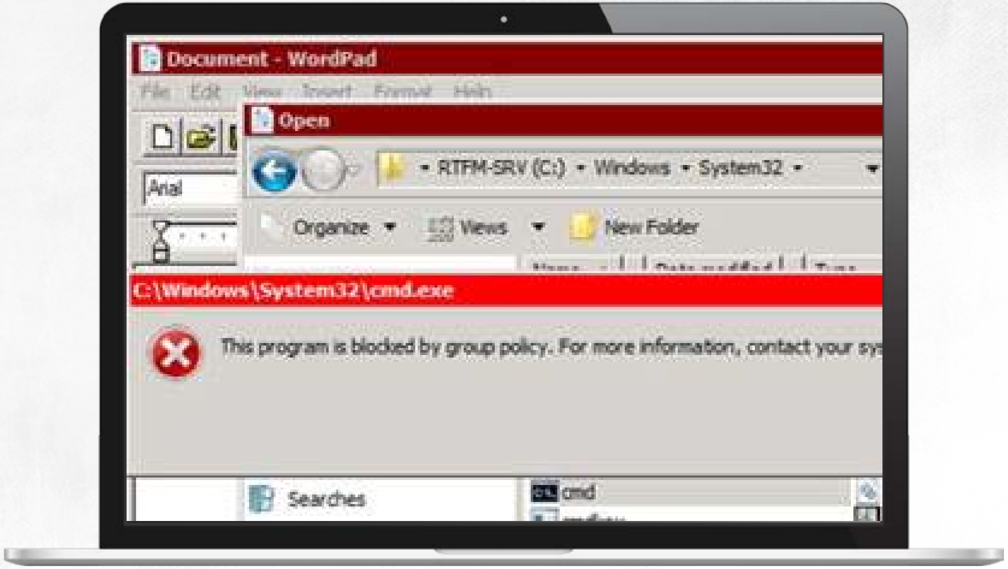
C:\Windows\System32\cmd.exe

This program is blocked by group policy. For more information, contact your sys

Block programs from starting

Software restriction policies

This bypassing will only work if the default software security rule allows all programs to be run


Document - WordPad
File Edit View Insert Format Help
Open
Arial
RTFM-SRV (C:) ▸ Windows ▸ System32 ▸
Organize ▾
Views ▾
New Folder
Searches
cmd

C:\Windows\System32\cmd.exe

This program is blocked by group policy. For more information, contact your sys

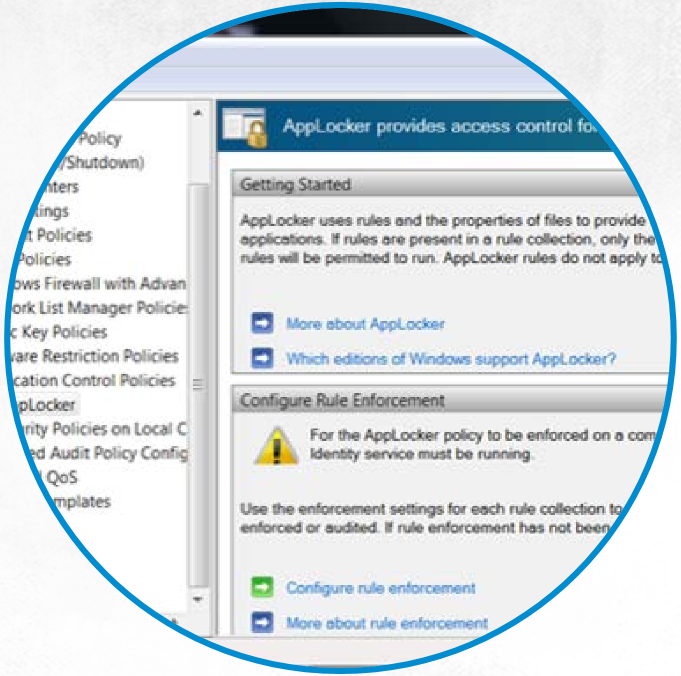
Block programs from starting

Application control policies

Application control policies describe and identify application based on one of the three rules: path rule, file hash rule and publisher rule

Application control policies rules may apply to:

- Executables
- MSI installer files
- Scripts
- DLLs and ActiveX controls



Policy
/Shutdown)
nters
tings
t Policies
Policies
ows Firewall with Advan
ork List Manager Policie
c Key Policies
vare Restriction Policies
cation Control Policies
pLocker
rity Policies on Local C
ed Audit Policy Config
l QoS
mplates

AppLocker provides access control fo

Getting Started

AppLocker uses rules and the properties of files to provide applications. If rules are present in a rule collection, only the rules will be permitted to run. AppLocker rules do not apply to

More about AppLocker

Which editions of Windows support AppLocker?

Configure Rule Enforcement

For the AppLocker policy to be enforced on a com Identity service must be running.

Use the enforcement settings for each rule collection to enforced or audited. If rule enforcement has not been

Configure rule enforcement

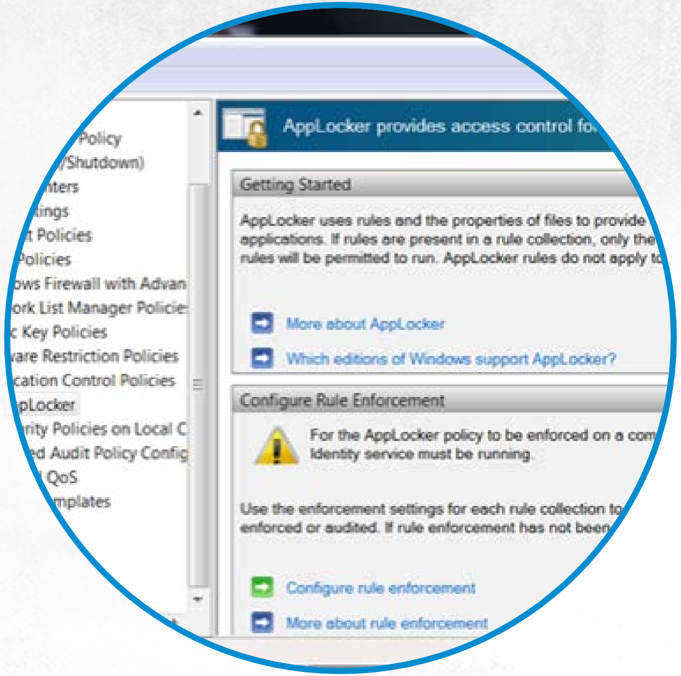
More about rule enforcement

Block programs from starting

Application control policies

The task of an administrator is to draw up a whitelist of allowed programs, and, optionally, create a blacklist of blocked applications that contains exceptions

To use application control policies, you need to start AppID Service



AppLocker provides access control fo

Getting Started

AppLocker uses rules and the properties of files to provide applications. If rules are present in a rule collection, only the rules will be permitted to run. AppLocker rules do not apply to

More about AppLocker

Which editions of Windows support AppLocker?

Configure Rule Enforcement

For the AppLocker policy to be enforced on a com Identity service must be running.

Use the enforcement settings for each rule collection to enforced or audited. If rule enforcement has not been

Configure rule enforcement

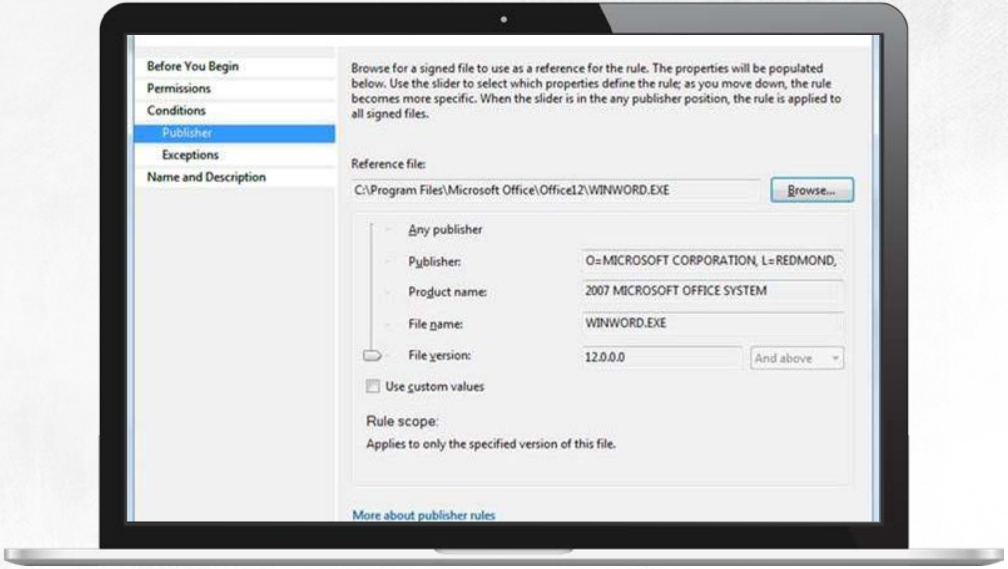
More about rule enforcement

Block programs from starting

Application control policies

Creating default rules ensures the system will run smoothly: three rules that allow all users to run programs stored in the Program Files folder and its subfolders, allowing them to run OS components (files stored in the system folder) and rules that allow the local administrator group to run all programs regardless of where they are stored

Publisher rules may be broadened and contain exceptions



Browse for a signed file to use as a reference for the rule. The properties will be populated below. Use the slider to select which properties define the rule; as you move down, the rule becomes more specific. When the slider is in the any publisher position, the rule is applied to all signed files.

Reference file:
C:\Program Files\Microsoft Office\Office12\WINWORD.EXE

Any publisher
Publisher: O=MICROSOFT CORPORATION, L=REDMOND,
Product name: 2007 MICROSOFT OFFICE SYSTEM
File name: WINWORD.EXE
File version: 12.0.0.0 And above

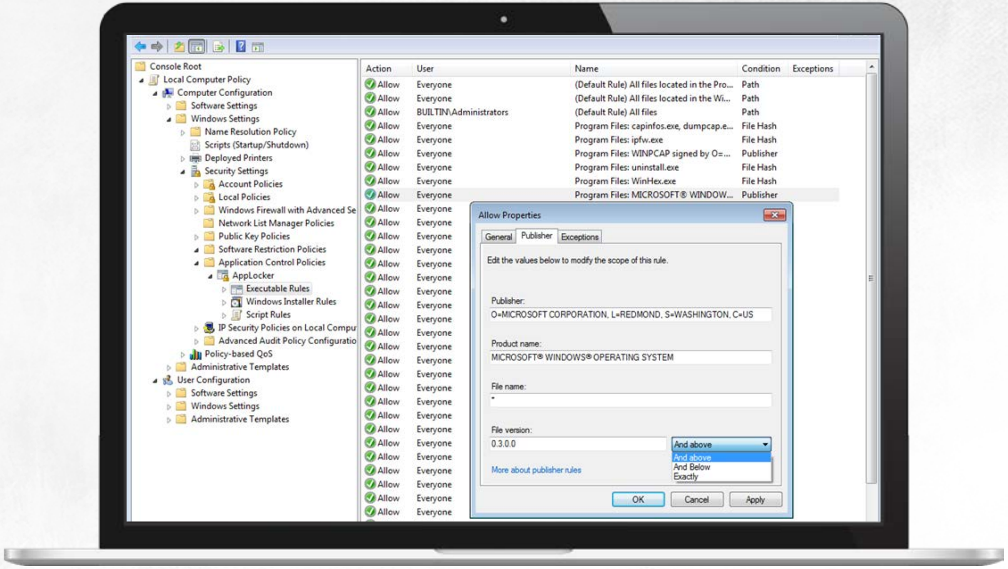
□ Use custom values

Rule scope:
Applies to only the specified version of this file.

Block programs from starting

Application control policies

Automatic rule generator for programs in a selected folder is a wizard that can simplify configuration and make it quicker to do



Action	User	Name	Condition	Exceptions
Allow	Everyone	(Default Rule) All files located in the Pro...	Path	
Allow	Everyone	(Default Rule) All files located in the Wi...	Path	
Allow	BUILTIN\Administrators	(Default Rule) All files	Path	
Allow	Everyone	Program Files: capinfos.exe, dumpcap.e...	File Hash	
Allow	Everyone	Program Files: ipfw.exe	File Hash	
Allow	Everyone	Program Files: WINPCAP signed by O=...	Publisher	
Allow	Everyone	Program Files: uninstall.exe	File Hash	
Allow	Everyone	Program Files: WinHex.exe	File Hash	
Allow	Everyone	Program Files: MICROSOFT® WINDOW...	Publisher	
Allow	Everyone			
Allow	Everyone			
Allow	Everyone			
Allow	Everyone			
Allow	Everyone			
Allow	Everyone			
Allow	Everyone			
Allow	Everyone			
Allow	Everyone			
Allow	Everyone			
Allow	Everyone			
Allow	Everyone			
Allow	Everyone			
Allow	Everyone			
Allow	Everyone			
Allow	Everyone			
Allow	Everyone			
Allow	Everyone			
Allow	Everyone			
Allow	Everyone			
Allow	Everyone			
Allow	Everyone			
Allow	Everyone			

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:
*

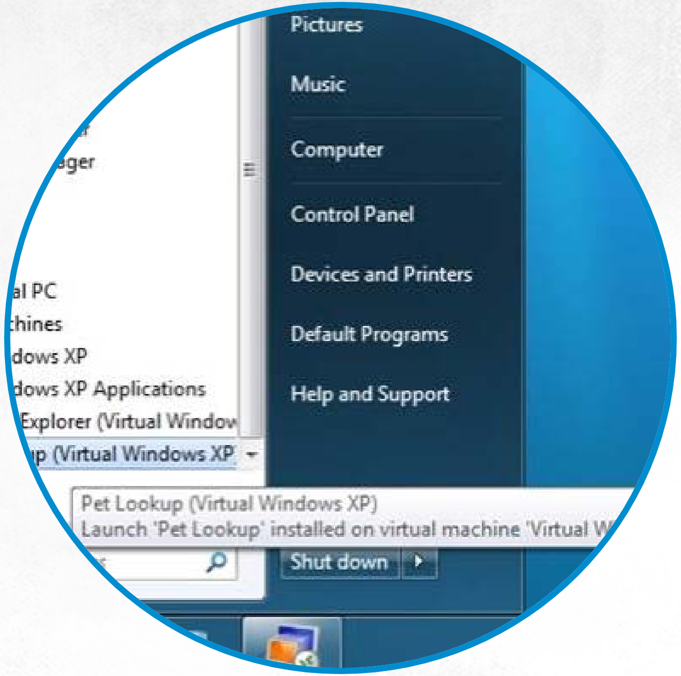
File version:
0.3.0.0 And above

Isolating programs

If regardless of an application being a potential hazard it has to be used in a system, the only protective measure is isolating the program

You can isolate a program from the rest of the system by:

- Running it on a dedicated non-domain host
- Running it on a virtual OS
- Running it in a sandbox (an isolated OS environment)



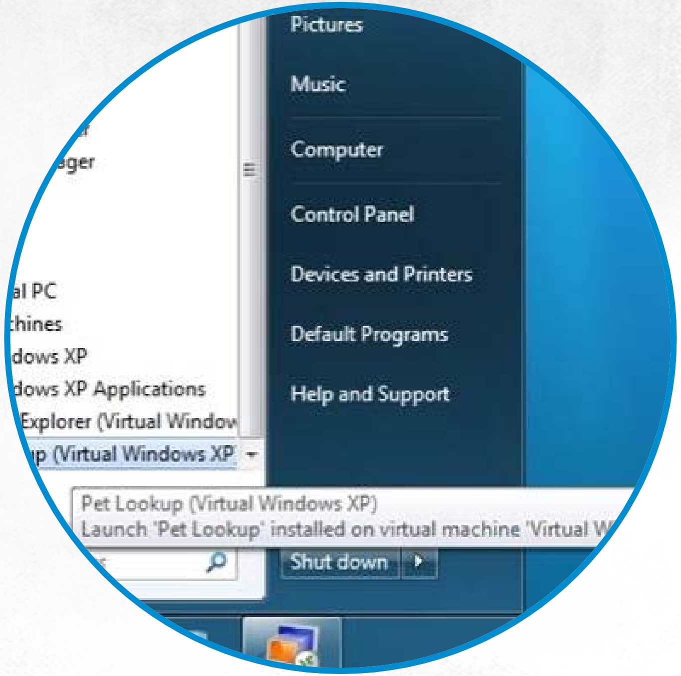
Pet Lookup (Virtual Windows XP)
Launch 'Pet Lookup' installed on virtual machine 'Virtual W

Isolating programs

XP Mode uses 256 MB of RAM by default and communicates with other hosts through a NAT network that uses a Windows 7 system as the server and is hibernated when turned off

Disable the host system integration function

Virtualised software is accessed directly from the host system

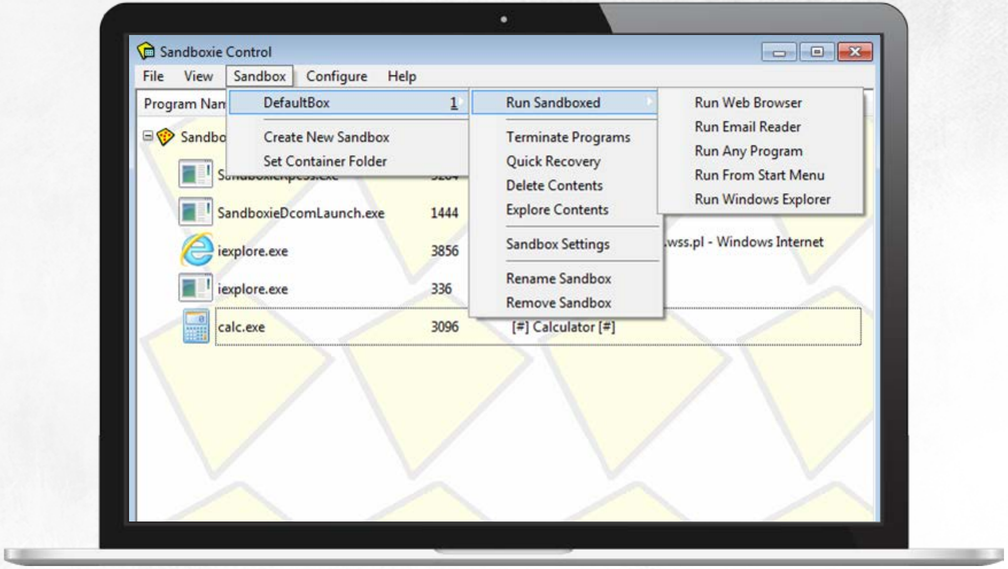


Pet Lookup (Virtual Windows XP)
Launch 'Pet Lookup' installed on virtual machine 'Virtual W

Isolating programs

To isolate programs, you can run them in a sandbox. To do this, install sandboxing software, for example Sandboxie

Sandboxie controls the operation of applications run in the sandbox mode by capturing all attempts to communicate with system resources and by saving them in a special isolated environment



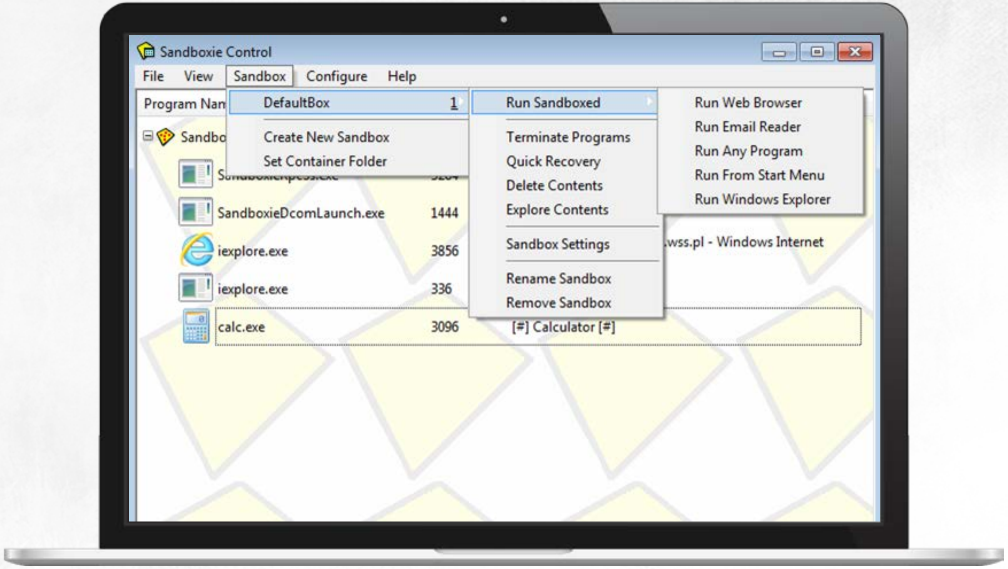
```
SandboxieDcomLaunch.exe   1444
iexplore.exe              3856   .wss.pl - Windows Internet
iexplore.exe              336
calc.exe                  3096   [#] Calculator [#]
```

Isolating programs

Using sandboxed applications does not differ from using them in the standard mode, running directly in the OS: all users have to do is to open them from Sandboxie

Sandboxie may also be used to monitor program activity in addition to isolating them

Sandboxing programs also offers another crucial benefit: you can quickly delete any setting changes made



SandboxieDcomLaunch.exe 1444
iexplore.exe 3856 .wss.pl - Windows Internet
iexplore.exe 336
calc.exe 3096 [#] Calculator [#]

THANKS

IT SECURITY ACADEMY

www.SecAcademy.com