SECURITY RISKS AND LOCKING DOWN WINDOWS ENDPOINTS

Technical White Paper

Published: May 2010

Table of Contents

Executive Summary

Personal computers and the Internet have completely revolutionized our lives in recent years. While individuals and businesses reap the benefits of Internet-connectivity, there are alarming levels of risks that are associated with access to the Internet. Because the Internet is inherently unsafe, organizations must take reasonable measures to protect their network systems from malicious software and external hackers. Most businesses protect their network servers, routers and other network devices by implementing firewalls and other mechanisms to safeguard their corporate data. However, the client operating systems, such as Windows desktop are not always locked down properly and pose one of the greatest risks to an organization's security.

While there are many challenges associated with securing network workstations, one of the most serious threat organizations face is when they use imaging software to mass-deploy desktop computers and use the same local Administrator password for the built-in Administrator account on all their client computers. This is a major security hole that poses serious security risk that is often overlooked. Organizations must find a way to plug this large gap and protect their valuable network assets.

In this white paper, we will examine some of the issues and concerns that organizations face when attempting to lock down their Windows desktops. We will discuss the costs associated with security attacks and take a closer look at some of the tools that are available that will aid organizations in implementing facets of desktop lockdown (controlling application privileges) and least user privilege (controlling local administrator accounts) to improve the security and manageability of desktop systems.

Costs Associated with Security Attacks

Attacks on network computers can be anywhere from a simple annoyance, such as a pop-up ad, to a highly dangerous takeover of an entire network by using a rootkit. The costs associated with such attacks can be astounding and the network downtime from security attacks can be substantial enough to cause a major blow to an organization's financial stability. Businesses are experiencing an alarming number of security attacks and the resulting financial loss is posing serious business threats, such as loss of revenue, business communications, intellectual property, data and source code, and loss of customers.

Risks Associated with Administrator Account

Microsoft Windows is by far the predominant operating system in use around the world today. It is common for organizations to give their users administrative privileges to their computer so they can perform day-to-day tasks. According to Microsoft, 90% of Windows software cannot be installed without administrative privileges and 70% of Windows software won't run unless the user is logged in with administrative credentials.[1] However, logging on to Windows computers with administrative privileges significantly increases the chances of computers becoming compromised because most malware requires administrative rights to cause damage. Granting administrative access to end users on their desktop workstations can not only be a security risk, it can also lead to incorrect configurations, which may in turn lead to downtime.

With so many risks associated with administrator account, what are some of the solutions or workarounds? To circumvent some of these problems, one solution that is used frequently is the *Principle of Least Privilege*. PC Magazine defines the principle of least privilege as "A basic principle in information security that holds that entities (people, processes, devices) should be assigned the fewest privileges consistent with their assigned duties and functions."[2]

Least-Privileged User Account in Windows XP

In Windows XP, Microsoft introduced the least-privileged user account (LUA) concept to implement the principle of least privilege. When discussing LUA, Microsoft refers to it as an "approach" because the LUA is not a specific account but rather an approach that includes best practices, tools and recommendations that encourage organizations to use non-administrative accounts to run Windows XP computers.

Despite the implementation of LUA approach, Windows XP does not offer an acceptable solution to organizations for securing the operating system or for managing the client desktops. Microsoft decided to try a different and much better approach in Windows Vista.

User Account Control in Windows Vista

In Windows Vista, Microsoft applied the principle of least privilege but with a slightly different twist. Because the model used in Windows Vista is different, Microsoft dropped the term LUA and replaced it with the new term User Account Control (UAC). This new approach to the principle of least privilege further enhances security. Microsoft realized that when users logon as local administrators, any application or malware that runs on that computer also have complete administrative privileges. This can potentially lead to creation of security holes in the system.

Microsoft focused on four major areas in Windows Vista where the principle of least privilege was applied:

1. User accounts
2. Web browsing
3. Services
4. Drivers

Unlike Windows XP, most users in Windows Vista can use a non-administrator account, which essentially is a least privilege user account, and run the operating system in a manner that doesn't limit them from doing their daily tasks. This ensures that users are not installing unapproved software or modifying the system configuration without following the corporate policies.

With Windows Vista, Microsoft has made significant improvements in implementing the principle of least privilege. However, experts agree that Microsoft doesn't go all the way to implement a complete least privilege solution. While UAC is a significant improvement and has several advantages, Microsoft points out the following facts about UAC in the TechNet article "The Long-Term Impact of User Account Control."[3]

- "UAC does not provide foolproof security."
- "UAC will not stop bad guys from stealing your personal data."
- "UAC was not designed to protect an application running with elevated privileges from all attacks by an application that runs with normal privileges in the same login session. While UAC does provide some weak process isolation, it was not a design goal for UAC to sandbox applications from each other."
- "UAC does not, nor is it intended to, stop malware."

The TechNet article points out the above facts not to minimize the value of UAC but to clarify some of the misconceptions about UAC. UAC is a useful set of features that should not be disabled. One major drawback of UAC is the way it is implemented, which can potentially discourage organizations from implementing it. Another disadvantage is that other than turning it on or off, it offers practically no configuration options at all.

User Account Control in Windows 7

Compared to Vista, the underlying technologies of UAC have remain relatively unchanged in Windows 7. The primary difference in Windows 7 UAC architecture is two new modes that the protected administrator account can use. The default behavior of UAC in Windows 7 prompts the user only when a non-Windows executable asks for elevation. In addition, some built-in Windows components can now benefit from an auto-elevation mechanism. The default administrator account is also disabled in Windows 7.

Although Windows 7 is moving to a more locked-down approach for the Administrator account, it does pose some problems for the applications that require administrative credentials for installation and execution.

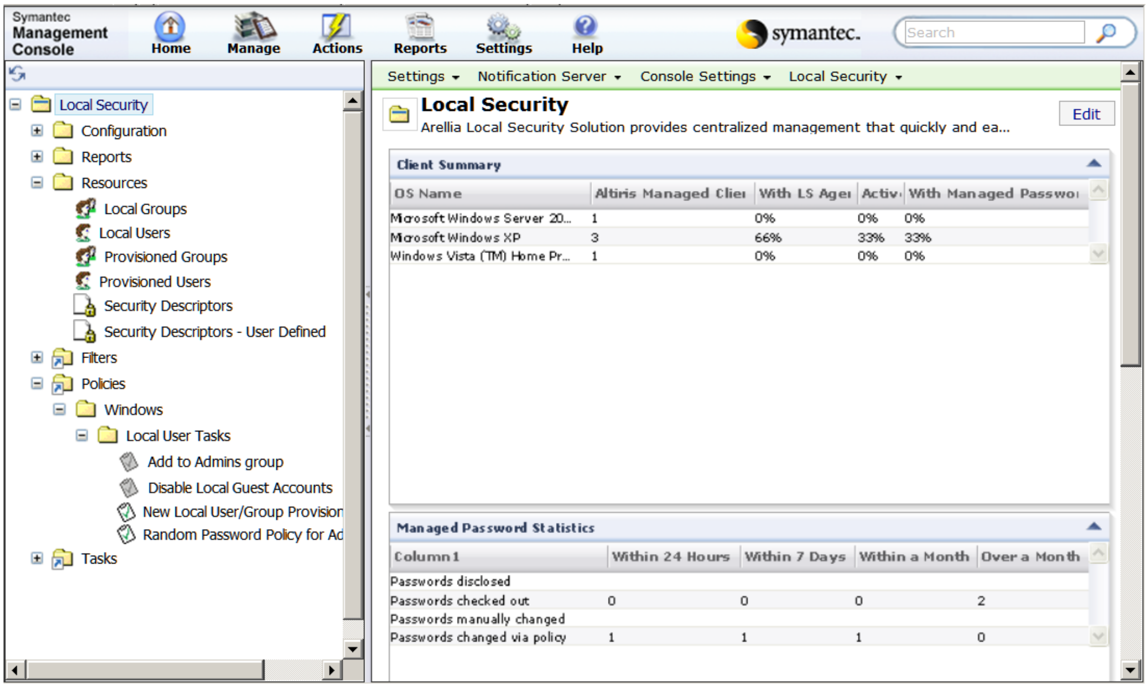
What is an Ideal Solution?

In order to achieve success, organizations are realizing that they must somehow find the right combination of the level of desktop lockdown and a security solution that is viable and realistic. Simply put, the key to minimizing the risks associated with malicious attacks is to implement a solution that provides efficient centralized management of local administrative users and groups, protection of administrative passwords, and better control of the execution of programs on workstations. An ideal solution should integrate with an organization's existing management system and should be flexible so you can avoid the "all or nothing" approach.

Arellia Solutions

The concepts of principle of least privilege have been implemented in Windows platform but fall short of being close to an ideal or complete solution. There are built-in tools in the operating system that help you achieve portions of what you want to achieve but not exactly what you want. In addition, there is no central console to manage all your user accounts and local group memberships, passwords for local administrators, and control of applications deployed across your entire network. These are helpful in implementing privilege management. While administrative accounts can be helpful in securing Windows platform, they also introduce risks because users logged in as administrators have unlimited privileges and can intentionally or inadvertently cause serious damage to their computers and potentially to the entire network.

Arellia looked at the bigger picture to address the overall need of the network administrators and business managers with a rather simple point of view. They asked simple questions. What do businesses want? What is missing in Windows platform? How can the gaps be filled easily and securely? What organizations want is a secure and well-managed environment that can be controlled centrally and integrated seamlessly in their existing environment. This led to the design of two solutions from Arellia called Local Security Solution and Application Control Solution.



Local Security

Arellia Local Security Solution provides centralized management that quickly and ea...

Client Summary

OS Name	Altiris Managed Clie	With LS Age	Activ	With Managed Passwo
Microsoft Windows Server 20...	1	0%	0%	0%
Microsoft Windows XP	3	66%	33%	33%
Windows Vista (TM) Home Pr...	1	0%	0%	0%

Managed Password Statistics

Column1	Within 24 Hours	Within 7 Days	Within a Month	Over a Month
Passwords disclosed				
Passwords checked out	0	0	0	2
Passwords manually changed				
Passwords changed via policy	1	1	1	0

Figure 1 - Password management portal

Local Security Solution and Application Control are designed to work seamlessly in an existing Windows environment and natively on the Symantec Management Platform. Together they offer much-needed relief for organizations and offer control from a central console. These two solutions address the reasons why so many organizations have failed to implement a desktop lockdown solution. Some of the key features from Arellia include:

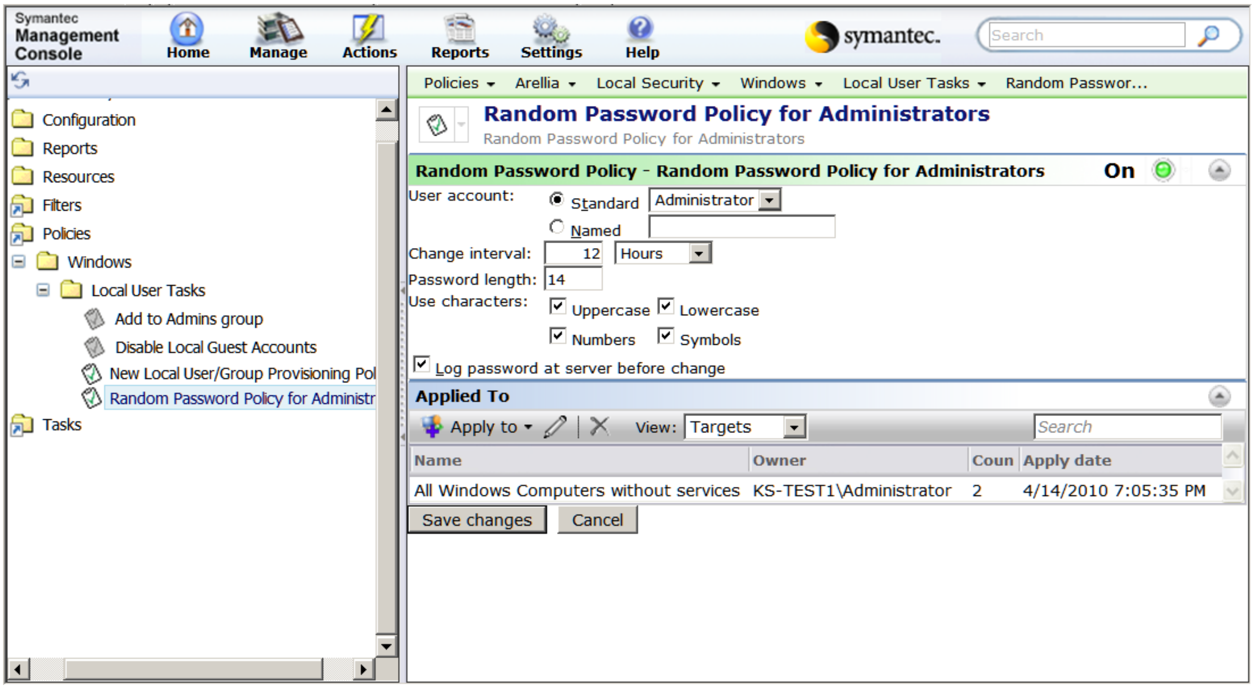
- Gain visibility and control over local users and groups
- Better manage local administrator account memberships
- Force password changes on administrator-defined schedules
- Randomize passwords based on strong password criteria
- Easily identify and track installed software
- Deny access to unauthorized or malicious software
- Protect against zero-day exploits
- Implement least-privilege security best practices

Benefits of Arellia Solutions

Arellia addresses several deficiencies and offers numerous benefits. For example, with Local Security Solution you have the ability to inventory and provision user and group accounts with specific rights. A reliable inventory and tracking method of local account and memberships ensures that you have a good understanding of the state of your individual systems, which minimizes security risks. Local Security Solution reduces 90% of the labor so you can avoid the costs associated with the manual configuration changes or scripting of local users and groups.[4]

Local Security Solution's implementation is policy-based which allows you to enforce security and management requirements through automated group memberships. This approach is beneficial to organizations because unauthorized users are less likely to be added maliciously or inadvertently to the administrative groups. It addresses one of the major challenges faced by businesses in locking down the desktops – better control of your local group account memberships.

Another major hurdle addressed by the Arellia solution is the issue of managing local administrative passwords. Many organizations have a tendency to use the same local administrator password on all their computers, especially in cases where imaging software is used to deploy computers. This poses a security risk. If one of your systems is compromised, it puts all the systems at risk. Local Security Solution enhances security by automating the cycling of administrative passwords. In addition, with Random Password policy you can generate random passwords based on strong password criteria automatically for a defined set of computers on administrator-defined schedules. Therefore, even if the password is compromised, the exposure will only last until the randomization period expires. Furthermore, the exposure will be limited to only one computer.



Random Password Policy for Administrators

Random Password Policy for Administrators

Random Password Policy - Random Password Policy for Administrators **On**

User account: ● Standard Administrator
○ Named

Change interval: 12 Hours

Password length: 14

Use characters: ☑ Uppercase ☑ Lowercase
☑ Numbers ☑ Symbols

☑ Log password at server before change

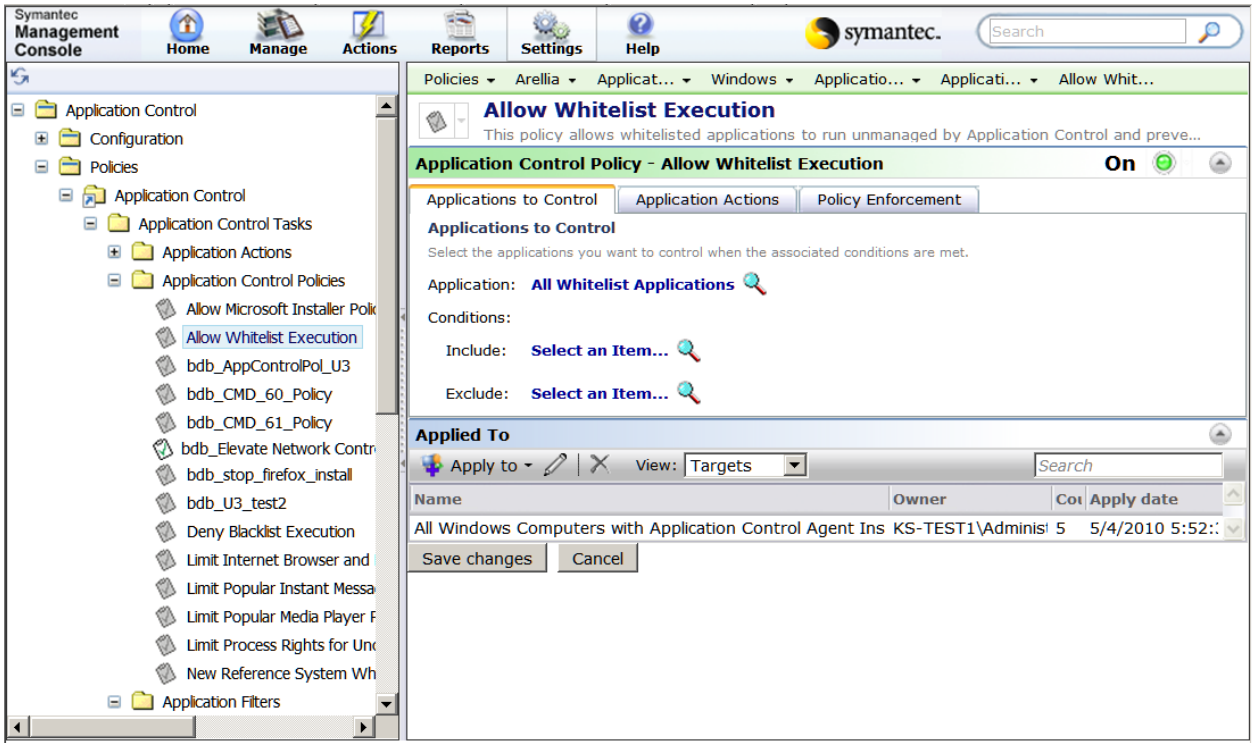
Applied To

Name	Owner	Coun	Apply date
All Windows Computers without services	KS-TEST1\Administrator	2	4/14/2010 7:05:35 PM

Figure 2 - Randomize password policy

Arellia Application Control Solution offers a policy-driven method for controlling applications running on managed computers.[5] It addresses the need for companies to better manage programs not only to improve security but also to lower the total cost of ownership by enhancing system integrity and manageability. Today, many businesses are concerned about malicious and unwanted software. They are also concerned about unlicensed software, shareware, freeware, and unapproved software on company computers.

Organizations of all sizes want to have control over the software that is executed on their computers. Application Control Solution addresses this need and offers you a mechanism to effectively control specific applications that are allowed to run on your network. This offers protection from malicious software, spyware and keyloggers. Known applications can be classified using specific criteria and execution of these applications may be allowed or denied based on these classifications.



Allow Whitelist Execution

This policy allows whitelisted applications to run unmanaged by Application Control and preve...

Application Control Policy - Allow Whitelist Execution On

Applications to Control

Select the applications you want to control when the associated conditions are met.

Application: **All Whitelist Applications**

Conditions:

Include: **Select an Item...**

Exclude: **Select an Item...**

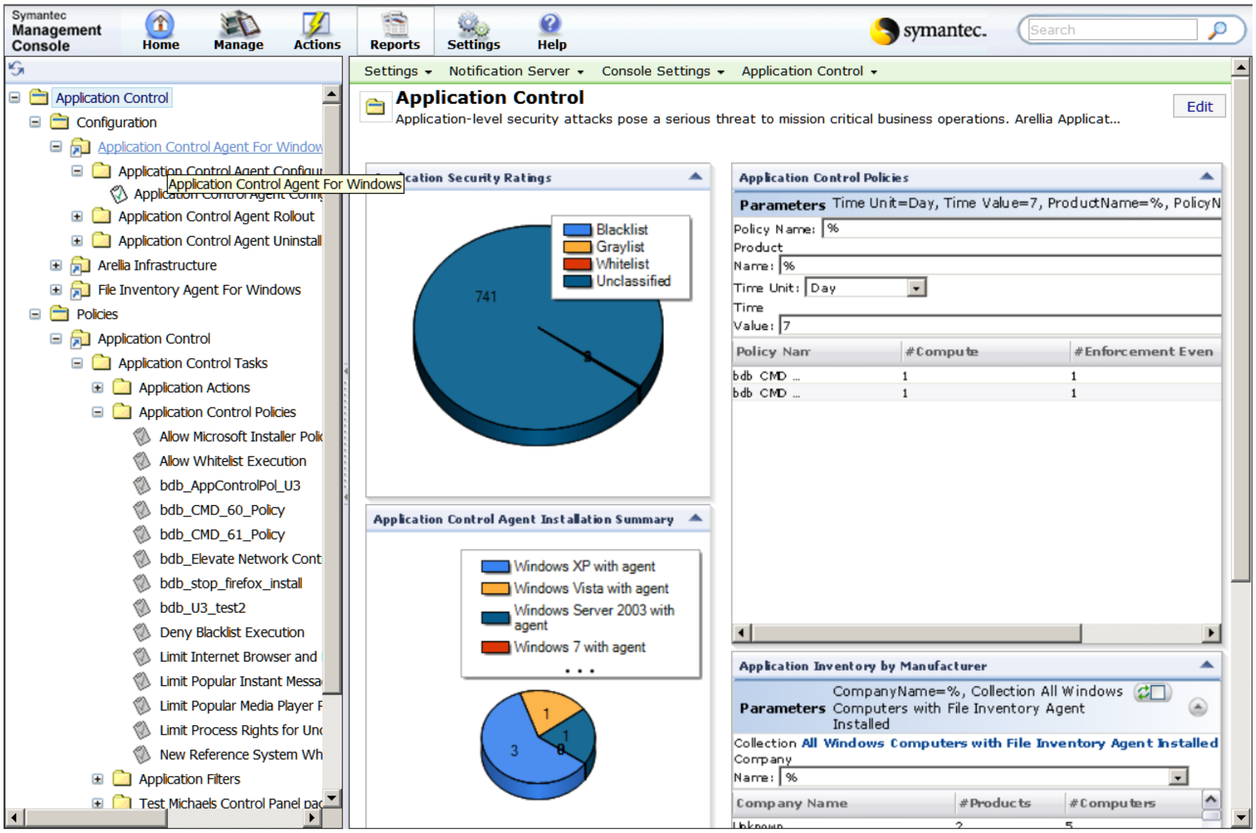
Applied To

Name	Owner	Coι	Apply date
All Windows Computers with Application Control Agent Ins	KS-TEST1\Adminis	5	5/4/2010 5:52::

Figure 3 - Manage application execution authorization list

Another useful feature in Application Control Solution is the ability to escalate or demote privileges per application. This allows programs to execute on user desktops without requiring administrative privileges for the entire computer, which minimizes security risks associated with running applications with administrative credentials. You can also deny Windows hooking to prevent certain types of attacks through privilege escalation. For example, you can limit the ability of malicious software to hook to the keyboard.

In addition to protecting network resources by having better control of installed software and improved security due to centralized management of local administrative accounts, the solutions offered by Arellia also helps organizations satisfy requirements for many industry regulations, such as Sarbanes-Oxley, HIPAA, FISMA, and Gramm-Leach-Bliley. With Arellia solutions you can generate compliance reports detailing all account-related differences between a previously established secure baseline system and a corresponding collection of existing systems.


Symantec Management Console
Home
Manage
Actions
Reports
Settings
Help
symantec.
Search
Settings ▾
Notification Server ▾
Console Settings ▾
Application Control ▾
Application Control
Configuration
Application Control Agent For Window
Application Control Agent Configur
Application Control Agent For Windows
Application Control Agent Config
Application Control Agent Rollout
Application Control Agent Uninstall
Arellia Infrastructure
File Inventory Agent For Windows
Policies
Application Control
Application Control Tasks
Application Actions
Application Control Policies
Allow Microsoft Installer Poli
Allow Whitelist Execution
bdb_AppControlPol_U3
bdb_CMD_60_Policy
bdb_CMD_61_Policy
bdb_Elevate Network Cont
bdb_stop_firefox_install
bdb_U3_test2
Deny Blacklist Execution
Limit Internet Browser and
Limit Popular Instant Messa
Limit Popular Media Player F
Limit Process Rights for Unc
New Reference System Wh
Application Filters
Test Michaels Control Panel pac
Edit
...cation Security Ratings
Blacklist
Graylist
Whitelist
Unclassified
741
2
Application Control Agent Installation Summary
Windows XP with agent
Windows Vista with agent
Windows Server 2003 with agent
Windows 7 with agent
1
3
1
0
Application Control Policies
Application Inventory by Manufacturer

Application Control

Application-level security attacks pose a serious threat to mission critical business operations. Arellia Applicat...

Parameters Time Unit=Day, Time Value=7, ProductName=%, PolicyN

Policy Name: %

Product Name: %

Time Unit: Day

Time Value: 7

Policy Nan	#Compute	#Enforcement Even
bdb CMD ...	1	1
bdb CMD ...	1	1

Parameters CompanyName=%, Collection All Windows Computers with File Inventory Agent Installed

Collection **All Windows Computers with File Inventory Agent Installed**

Company Name: %

Company Name	#Products	#Computers
Unknown	2	5

Figure 4 - Application Control management portal

Conclusion

Open systems, such as the Internet, offer numerous benefits but they also pose security threats that can be very costly to organizations. As a countermeasure, the principle of least privilege was introduced in the Windows platform. Windows XP Professional uses LUA approach that offers a rather limited implementation of least privilege management. Windows Vista offers a much better approach and is a major improvement over Windows XP Professional but the UAC is far from an ideal solution and has several limitations.

The Arellia solutions addresses some of the security concerns of open systems and the limitations in the Windows platform. In addition, it can also help businesses meet certain corporation and industry regulatory requirements. Arellia offers a solution that can be easily integrated into an existing management system to minimize security attacks on an organization's information assets. Another business concern addressed by Arellia solutions is the control of software that is executed on desktop computers. Unapproved and unlicensed software can cause major configuration and legal problems for organizations and can add to the total cost of ownership. With Arellia solutions you can not only inventory and keep track of applications running on your desktops, you can also effectively control execution or denial of specific programs.

Arellia offers excellent solutions that can not only improve security; they can also enhance system integrity and manageability which will result in lowering the total cost of ownership. An evaluation edition of the products offered by Arellia are available for download at http://portal.arellia.com/wiki/display/NS7Preview/Symantec+Installation+Manager.

References

[1] http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnlong/html/leastprivlh.asp

[2] http://www.pcmag.com/encyclopedia_term/0,2542,t=least+privilege&i=46010,00.asp

[3] http://www.microsoft.com/technet/technetmag/issues/2007/09/SecurityWatch/

[4] http://arellia.com/media/6765/arellia%20local%20security%20solution.pdf

[5] http://arellia.com/media/6726/arellia%20application%20control%20solution.pdf

About SeattlePro Enterprises

SeattlePro is a close-knit team of creative visionaries offering companies the guidance and education professionals need to stay competitive in today's market. SeattlePro provides custom on-site IT training, consulting, and authoring services for businesses to keep up with the rapid pace of technology. For more information on the services offered by SeattlePro visit www.seattlepro.com.

About the Author

Zubair is Microsoft MVP, a Microsoft Certified Trainer, and the founder of SeattlePro Enterprises, an IT training, consulting, and authoring business. He holds more than 25 industry certifications including MCT, MCSE, MCSA, MCDST, MCITP, MCTS, MCP+I, MCSA 2000/2003: Security, MCSE 2000/2003: Security, CNA, A+, Network+, Security+, CTT+ and CIW. His experience covers a wide range of spectrum: trainer, consultant, systems administrator, security architect, network engineer, author, technical editor, college instructor and public speaker.

Zubair teaches various Microsoft technologies and has written extensively on Microsoft products for several years. His specialties include network security, Windows operating systems, Active Directory, IIS, Terminal Services, and virtualization. His consulting engagements range from troubleshooting and designing networks for small to medium-sized companies to engineering network services for large enterprises with over 30,000 users. He excels in troubleshooting hardware and software problems and his real-world experience is one of his greatest strengths.

As a Microsoft-endorsed trainer, he has trained Microsoft Consulting Services (MCS) and Microsoft Product Support Services (PSS) technicians. In addition to writing Professor Windows columns for Microsoft TechNet, he has been involved in writing certification exam questions for Microsoft. Some of his other activities for the past decade at Microsoft include working as a Subject Matter Expert on various projects, teaching train-the-trainer courses, consulting for MCS, writing for TechNet Magazine, speaking at seminars and webinars, working with ISA Server group, writing white papers and case studies, doing technical reviews of Microsoft Learning courses, and more.

Zubair is known worldwide for his articles on Microsoft Technologies, written as a contributing editor and online columnist for Windows IT Pro Magazine and Microsoft Certified Professional (MCP) magazine. He writes "Windows Advisor" column for MCP Magazine and "Zubair's Security Zone" column for CertCities.com. He reviews technical books and articles for various publishers and has co-authored a book on Windows 2000 networking services. He also wrote "Microsoft ISA Server 2000" for Sams Publishing. All his publications are available at www.techgalaxy.net.

Microsoft has recognized him by presenting him the *Microsoft Most Valuable Professional (MVP) for Directory Services* award for inspiring excellence while helping people through his past recognized practical expertise and demonstrated willingness to share with peers in technical communities around the globe. In September 2009, he was recognized as the featured IT Pro of the Month on Microsoft's Web site. Zubair is also the founder of *Seattle* Windows Networking User Group. The User Group is sponsored by Microsoft and serves the greater Puget Sound IT community around Seattle and its suburbs.

Zubair was awarded a Bachelor of Science (B.S.) in Aeronautics and Astronautics Engineering from the University of Washington in Seattle. He also holds a B.S. in Mathematics. He taught at North Seattle Community College after he earned his Computer Information Systems (CIS) degree.