



**VIEWFINITY**

**Windows 7 and Desktop  
Lockdown with Privilege  
Management**

2011

## TABLE OF CONTENTS

<b>The Windows 7 Desktop Refresh and Security .....</b>	<b>3</b>
<b>Principle of Least Privilege and Windows Desktops.....</b>	<b>4</b>
<b>Benefits For Organizations when Users are Not Local Administrators.....</b>	<b>5</b>
Better Protection Against Malware.....	5
Tighter Control on Software Installations.....	6
Compliance with Regulatory Mandates and Industry Best Practices .....	6
Increased Data Security .....	6
<b>Common Challenges When Removing Local Administrator Rights .....</b>	<b>7</b>
Application Compatibility .....	7
User Self Service Application Installations.....	8
User Initiated System Maintenance Tasks.....	9
<b>Viewfinity Privilege Management Solutions .....</b>	<b>9</b>
Granular Control .....	9
Support for Remote and non AD Connected Systems.....	12
End-to-End Automated and Non-Disruptive Transition to Least Privileges.....	13
Centralized Policy Audit and Validation.....	14
Conclusion .....	15
<b>About the Author .....</b>	<b>16</b>

## The Windows 7 Desktop Refresh and Security

All organizations have to consider how to deploy Windows 7 over the next few years because Microsoft has announced the end of life dates for Windows XP support (see figure 1 below). The migration to Windows 7 provides an opportune event to re-evaluate desktop security standards and look for ways to more cost effectively provide secure and productive desktop computing environments.

<b>Windows XP Service Pack 3</b>	<b>Mainstream support ends</b>	<b>Extended support ends</b>
All editions	No longer supported	Tuesday, April 8, 2014
<b>Windows Vista Service Pack 2</b>	<b>Mainstream support ends</b>	<b>Extended support ends</b>
Business editions: Business Enterprise	Tuesday, April 10, 2012	Tuesday, April 11, 2017
Consumer editions: Home Basic Home Premium Ultimate	Tuesday, April 10, 2012	Not Applicable
<b>Windows 7</b>	<b>Mainstream support ends</b>	<b>Extended support ends</b>
Business editions: Professional Enterprise	Tuesday, January 13, 2015	Tuesday, January 14, 2020
Consumer editions: Starter Home Basic Home Premium Ultimate	Tuesday, January 13, 2015	Not Applicable

Figure 1

Source: [How long will Microsoft support XP, Vista, and Windows 7?](#)  
Ed Bott, ZDNet, August 2010

Studies have shown that a locked down environment is more cost effective to support because the end users are less likely to make unnecessary changes to the core system configuration. Implementing a locked down environment is also key in complying with various regulatory and compliance initiatives.

System Administrators can use the desktop refresh as a way to roll out changes in how security privileges are managed on the endpoint so that the local logged on user does not need to have local administrator rights.

If lockdown is done properly, that is, in conjunction with software that will help you manage privileges, the impact on user productivity should be nil and end users will have the ability to conduct business as usual. Essentially whatever privileges the end user requires to get his job done is managed through the software product and will seamlessly make available all required applications and desktop functions.

## Principle of Least Privilege and Windows Desktops

The principle of least privilege means that a module in a computing environment such as a user account should only have access to information and resources that are necessary to its legitimate purpose. (see [http://en.wikipedia.org/wiki/Principle\\_of\\_least\\_privilege](http://en.wikipedia.org/wiki/Principle_of_least_privilege))

The Department of Defense DOD-5200.28-STD “Orange Book” states “[The Principle of Least Privilege] requires that each subject in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks. The application of this principle limits the damage that can result from accident, error, or unauthorized use.”

Based upon the principle of least privilege, in a Windows desktop environment the locally logged on user will not have local administrative rights on the desktop. However many organizations have historically not followed the principle of least privilege when they deployed Windows XP or Windows Vista and have enabled the local user to have local administrator rights. Or many organizations have removed administrator rights for the majority of its end users but have allowed select groups or members to still have administrative privileges. This practice prevents an organization from meeting its compliance regulations and truly securing its desktop environment, which causes the entire network to be vulnerable.

This whitepaper highlights some of the key benefits to an organization when the users do not have local administrator rights. The paper will then discuss some of the most common challenges that organizations face when the local user no longer has local administrator rights. Finally, the paper will highlight how privilege management solutions from Viewfinity address the most common challenges organizations face when

removing local administrator rights from end users. Viewfinity Privilege Management allows organizations to manage user permissions at a very granular level after organizations have implemented a least privilege environment when moving to Windows 7.

## Benefits For Organizations when Users are Not Local Administrators

There are a number of benefits to organizations when users do not have local administrator rights on their desktop systems. Desktop management costs are reduced because the endpoint is more controlled, compliance objectives are met and your distributed desktop environment is more secure.

### Better Protection Against Malware

When the locally logged on user does not have local administrative rights, the programs and processes that the user runs do not have rights to modify core operating system files and settings. This reduces the surface area of an attack from malware. Malware that runs on the system in the context of the logged on user is not able to change core system settings. While this does not mean that the system doesn't need other security software such as firewall and anti-virus, removal of local admin rights does provide a more secure environment.

For example, there are many benefits when running the browser and mail client in a mode that does not have local admin rights. As users interact with web sites and data sources that are not necessarily trusted, malware that may be encountered is not as likely to be able to make unauthorized changes and introduce system instabilities.

Every month Microsoft releases a wide range of software updates (also known as patch Tuesday). Many of these updates are security related. A large percentage of software updates that are released by Microsoft every "patch Tuesday" have the following statement in the executive summary that describes the patch:

*"Users whose accounts are configured to have fewer user rights on the system could be less impacted than users who operate with administrative user rights." (As an example see <http://www.microsoft.com/technet/security/bulletin/ms10-053.msp>)*

Analysis of the patches released for Microsoft Office and Internet Explorer - processes that are typically run in the context of the logged on user - show that a very high percentage of the patches contain the above mentioned statement. The same is true for many of the patches associated with operating system provided applications such as media players and chat programs.

The analysis of the Microsoft patch data clearly shows that when the logged on user does not have local administrative rights, then it is more difficult for malware to attack a

system. Malware that is executed in the context of a non administrative user simply does not have the access to the system to make the changes that it could do if it were running with local administrator rights. If for no other reason than this analysis, organizations should remove local administrator rights from end users when moving to Windows 7.

### **Tighter Control on Software Installations**

When users do not have local administrative rights, it becomes more difficult for the users to install unauthorized software. Setup programs that modify core system files and registry settings cannot successfully complete if the user doesn't have the proper rights.

Unauthorized software may introduce system instabilities and conflicts. Unauthorized applications may introduce file system and registry changes that can impact other programs that run on the desktop. When this happens it leads to an increase in support calls to the help desk. Various third party reviews have consistently shown that there are fewer support calls when fewer changes are allowed on a system, thereby reducing desktop TCO and IT support costs.

Unauthorized software may also put an organization at risk from a software license compliance and software piracy perspective. If users are able to download and install any software at any time, then it becomes much more difficult for the organization to ensure that the software is properly licensed.

### **Compliance with Regulatory Mandates and Industry Best Practices**

Another reason to implement the principle of least privilege is to comply with various regulatory mandates. For example, the US Federal Government's Federal Desktop Core Configuration (FDCC) regulation requires users should not have administrator rights.

Sarbanes-Oxley, HIPAA, and various other standards provide best practices and requirements that include removal of administrator rights. Even if a given organization is not legally bound by one of these mandates, there is value in learning from the best practices that have been put in place by the various organizations. Organizations of all sizes and industries benefit from the set of security standards that have been generated over years of experience.

### **Increased Data Security**

When unauthorized software is installed or unauthorized changes are made to the system configuration, then it is more likely that additional ports may be opened on the system, firewall and anti-virus settings can be changed, access control settings can be changed, etc. These changes increase the risk of data being made accessible to people or processes that should not have access to such data. When users have less rights on the desktop, the information that is accessed on that system is more protected.

## Common Challenges When Removing Local Administrator Rights

An organization must consider the practical realities when removing local administrator rights from end users. In many organizations, local users have had administrative access on their desktop systems since PCs have been in use.

Many organizations use an operating system platform update (such as the move to Windows 7) as an event to evaluate a variety of desktop standards. There are a number of scenarios where the move to a locked down desktop may generate end user productivity issues.

### Application Compatibility

There are thousands and thousands of applications that have been written over the years that may not work properly when the logged on user does not have local administrator rights. Applications may assume read and write access to various locations in the file system or registry that are not accessible without administrator rights. Many of these legacy applications may not have been updated or available for use for a non-administrator user.

When an application tries to perform an operation that requires administrative level rights, Windows can allow the user to elevate the privilege through the User Account Control (UAC) mechanism. While UAC may work in some situations, it does not provide a solution that is appropriate for many use cases. For example, if a user that is not a local administrator encounters a UAC dialog, the user will need a local administrator password to enable the application to continue (see Figure 2 below). Since one of the key points of least privilege is that the user is not in the local administrator group, providing the user with the local administrator password is not a viable solution.

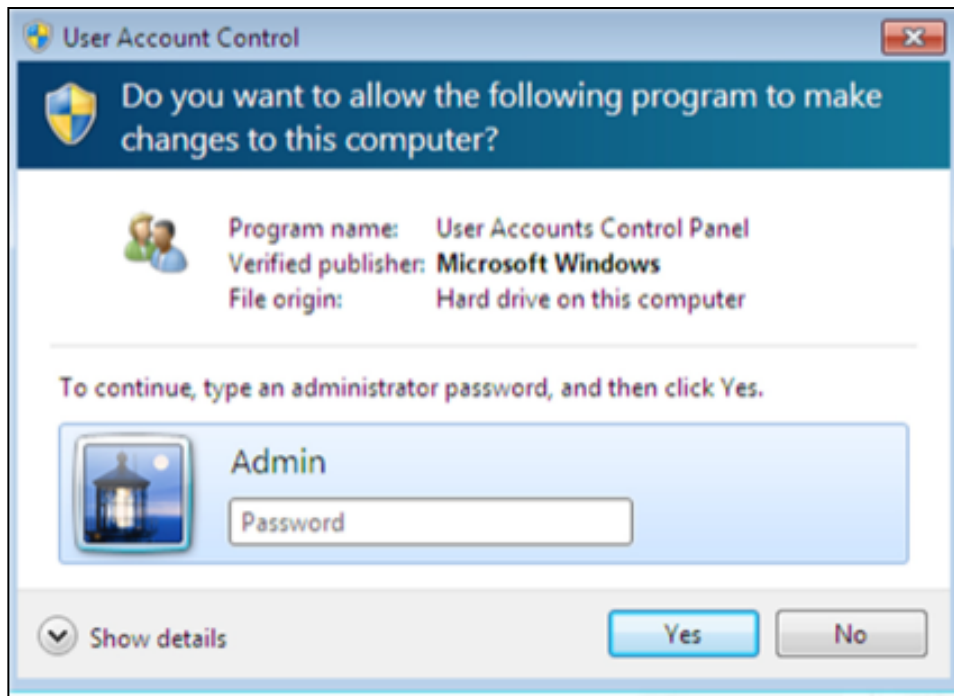


Figure 2

Applications can be configured to run in the context of an account other than the locally logged on user. However this presents many challenges in that the context used to access the HKEY\_CURRENT\_USER location in the registry will not be the same as the logged on user. Also, the location for the user profile data in the file system is not the same as the logged on user. Additionally, any process that is running as a separate security context will use that security for accessing resources that are off the local machine. For example if an application needs to access a file located on a network server, it doesn't use the ID of the logged on user, rather the ID of that application. This presents many challenges for controlling data access. Thus configuring applications to run with a different ID from that of the logged on user is not a good solution.

### User Self Service Application Installations

Most companies have sets of approved software that the user may install if it is required to do their job, however it is not part of the default set of applications that are actively installed on each computer by IT. Organizations need a way for users to install certain applications on demand without a call into the helpdesk. Often, these applications may require local administrative rights to be installed properly.

For example, many organizations have web portals or file shares with a range of available applications for anyone to use in the organization. The user on that endpoint needs to be able to install these applications from a known location without the user having local administrator rights.

## User Initiated System Maintenance Tasks

Many organizations may want users to be able run some system maintenance tasks that require administrator rights. This is especially true when you consider the large amounts of mobile and remote users that are not necessarily regularly logged onto the corporate network.

For example, an organization may want to allow end users to add certain hardware to the system such as printers and scanners. Some organizations may want end users to be able to change the time zone, system time, run disk management utilities, adjust application settings, or even stop and start certain services. Many of these system maintenance tasks require administrator rights.

Ideally organizations want to enable remote and mobile users to be able support themselves without having to provide the user with full administrator level access to the system.

## Viewfinity Privilege Management Solutions

Viewfinity Privilege Management enables enterprises to remove local administrator rights from the end user and manage permissions based on user role and the functionality they require to perform their job. By addressing these challenges, organizations can remove administrative privileges during its Windows 7 roll out with the confidence that applications and approved end user maintenance tasks will work as expected and not disrupt user productivity.

Viewfinity Privilege Management is implemented with an agent that runs on the desktop. (Note: consider incorporating the Viewfinity Agent into the standard operating system image in order to avoid deploying the agent after performing a migration.) The agent caches privilege policy settings from a Viewfinity server. The system administrator centrally defines the privilege management policies. Because the agent caches these policies on the endpoint, the endpoint does not need to be connected to the server to be able to enforce the privilege policies.

### Granular Control

A key benefit of Viewfinity Privilege Management is that it allows an organization to have very granular control on which processes are run with elevated rights. Privilege Management does not change the user identity used to run applications, rather it adjusts the rights for that instance of the application for that point in time.

For example, organizations are able to define policies that enable any application that is launched from a given network location to run with elevated rights. This allows the end user to successfully self-install software from a known corporate controlled software

repository. There is no UAC dialog that is presented to the user and the user simply runs through a standard installation process as if the user had local administrator rights.

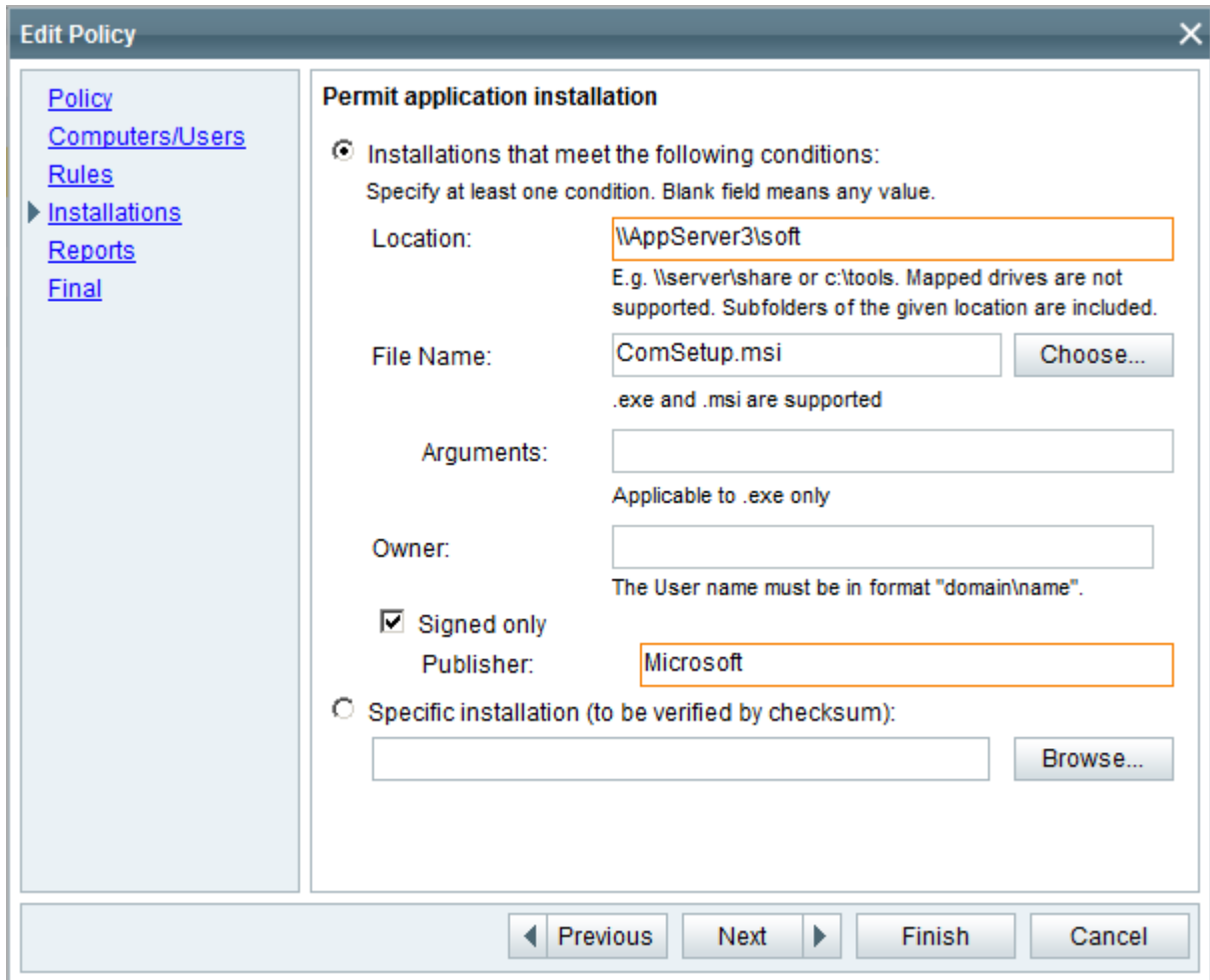


Figure 3 – Example of Viewfinity Privilege Management granular-level privilege elevation for applications

As another example, a company may have a legacy application that needs to have local administrator rights. When a user runs such an application, Viewfinity Privilege Management can adjust the privileges of the application when it starts up so that it can run. However this application is still running under the logged on user ID and all access to the current user profile settings work as expected. There is no UAC dialog that is presented to the user and the change in process rights is transparent to the end user.

Privilege Management also controls the privilege level of any child process. For example, a policy can be setup so that a legacy application can run with additional rights, but any child process reverts back to the default rights of the locally logged on user.

Another restriction imposed in least privilege environments is the inability for non-administrative users to install approved ActiveX controls. IT administrators may continue to operate endpoint devices in a least privileges mode and use Viewfinity

Privilege Management to grant administrative rights for installing ActiveX controls based on digital signature from a specific publisher, URL, or class ID.

**Edit Policy**

[Policy](#)  
[Computers/Users](#)  
[Rules](#)  
▶ [ActiveX](#)  
[Reports](#)  
[Final](#)

**Permit ActiveX control installation from Internet Explorer**

Any ActiveX control

ActiveX controls that meet the following conditions:  
Specify at least one condition. Blank field means any value.

Signed only

Publisher:

Source URL:

Installation Image Name:

MIME Type:   
e.g. "application/x-shockwave-flash"

Version:

Not older than  .  .  .

Not newer than  .  .  .

CLSID:   
e.g. {01234567-ABCD-1234-ABCD-0123456789AB}

◀ Previous    Next ▶    Finish    Cancel

Figure 4 – Example of Viewfinity Privilege Management granular-level privilege elevation for ActiveX controls

Viewfinity Privilege Management has granular controls for various administrative and maintenance tasks. Administrators can selectively choose which maintenance tasks are permitted and even which users or group of users can perform them.

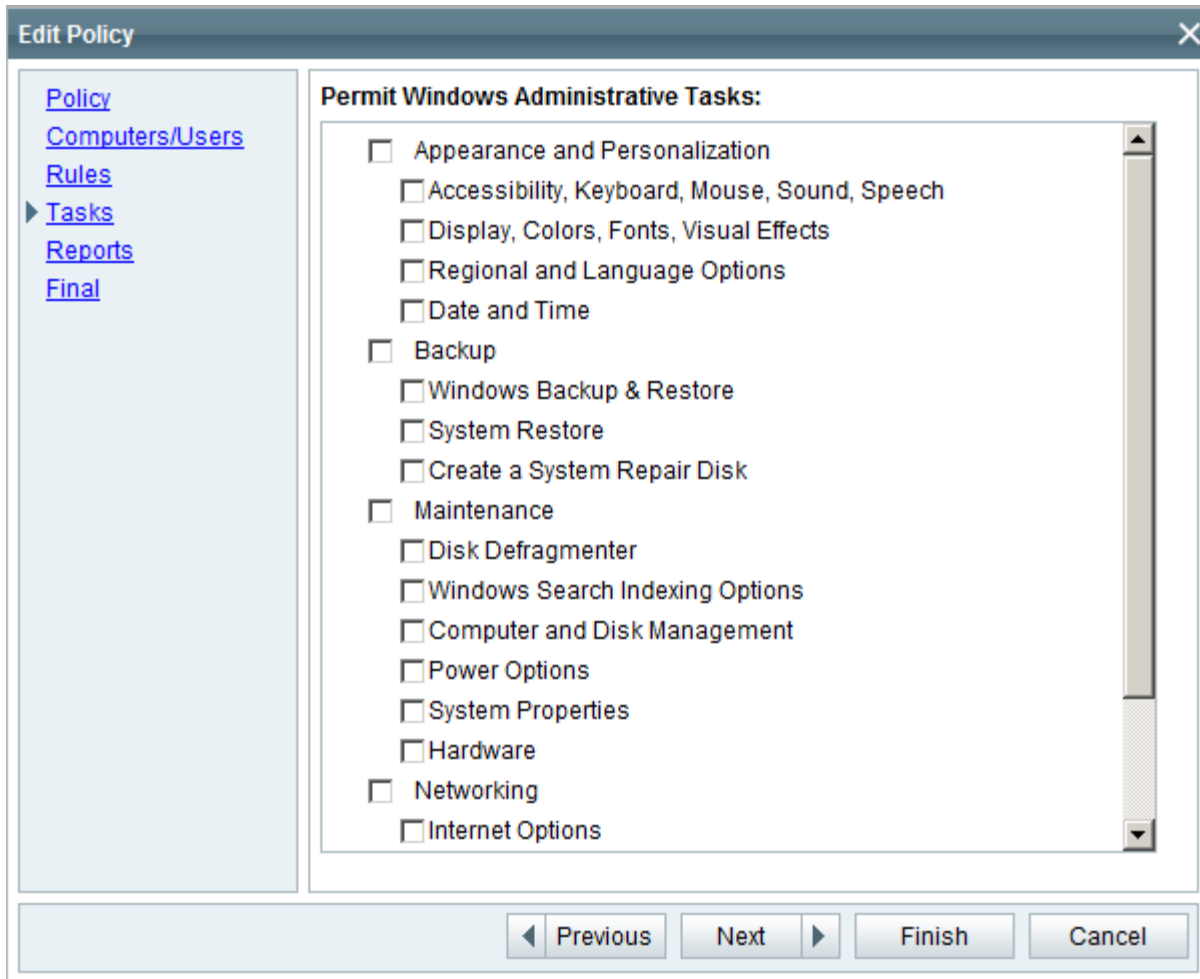


Figure 5 – Example of Viewfinity Privilege Management granular-level privilege elevation for Windows tasks

### Support for Remote and non AD Connected Systems

Viewfinity Privilege Management works just as well for systems that rarely connect to the corporate network as the systems that are inside the corporate firewall. There is a secure communications channel between the Viewfinity agent and the server. As a result, customers can configure a Viewfinity server so that it is accessible from any Internet connection.

Whenever the endpoint connects to the Internet, it is able to receive updated policies and provide feedback to the Viewfinity server. If the Viewfinity agent is not able to connect to the server, it still enforces policies based upon information that is cached on the endpoint.

Viewfinity Privilege Management works independent of an endpoint being connected to Active Directory. Because there is no reliance on AD Group Policy Objects (GPOs), Viewfinity privilege policies work on systems regardless of their state of connection to the directory or network. Policies are applied instantly without dependency on AD GPOs replication and there is no need for users to logoff or reboot their PCs in order for

policies to take effect. Viewfinity policies can be targeted not only to AD organization units, but also based upon any other group that the administrator wants to create within the Viewfinity console.

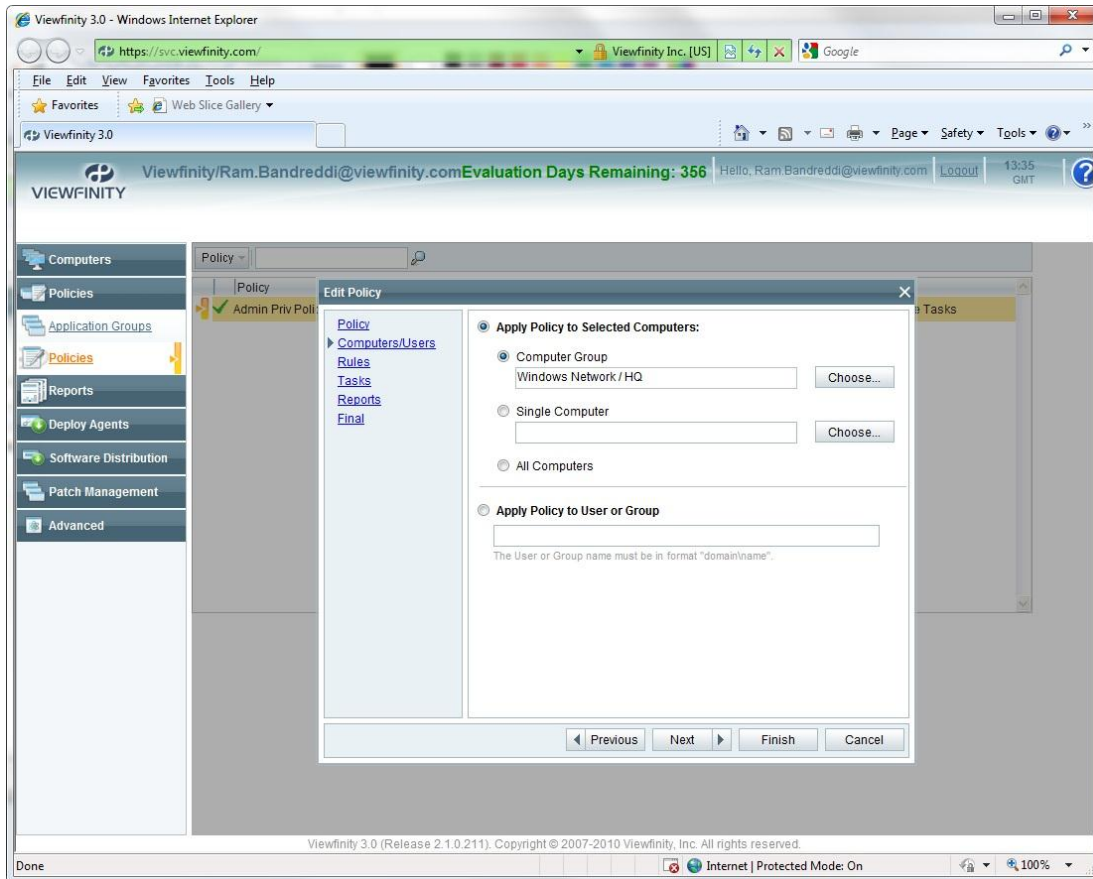


Figure 6 – Example of Viewfinity Privilege Management privilege elevation by user/group

## End-to-End Automated and Non-Disruptive Transition to Least Privileges

A project of this undertaking requires extensive analysis to determine user needs and prepare the environment. As organizations prepare their migration to Windows 7 with the goal to heighten IT security by moving to least privileges, our non-disruptive, automated method for moving to a least privileges environment provides an end-to-end best practice approach that helps enterprises reduce IT security risks.

### Pre-Discover Applications Requiring Elevated Permissions

Our Application Admin Rights Analysis silently gathers information and monitors which applications, processes, and administrative actions will require administrative permission before users are removed from the local admin group. This information is based on end user activity and is collected over a period of time to ensure all events are captured. Once the collection and analysis is completed, policies to elevate privileges can

be automatically created and prepared in advance so that when administrative rights are removed, the policies are in place to ensure a non-disruptive move to least privileges.

### **Discover User Accounts that Have Local Administrative Rights**

Viewfinity offers a free Local Admin Discovery tool that discovers user accounts and groups that are members of the local “Administrators” built-in user group on computers in your Windows domain. Having detailed information related to which users and groups have administrator rights on corporate desktops allows you to reassess who should have these rights. Once the analysis has been run, IT Administrators can take action, if needed, by removing the users or suspicious groups from the Administrators group.

### **Policy Automation For Exceptions to User Permission Needs**

While 90-95% of your privilege management needs and policies will be established and implemented well ahead of time, for those exceptions, and there are always exceptions, Viewfinity offers a method for IT administrators to streamline privilege elevation requests from end users.

Viewfinity’s Policy Automation is the automatic detection and capture of the need for elevated permissions, combined with the ability to create the appropriate policy and authorize the privilege elevation request on the fly. Automating the privilege elevation request process and creating the appropriate policies on-the-fly saves a great deal of time for both the IT Administrator and end-user.

### **Centralized Policy Audit and Validation**

The Viewfinity Privilege Management agent provides policy compliance data to the server so that the system administrator receives feedback in terms of how and when the privilege management is applied at the endpoints. This audit trail ensures that not only have policies been defined, but also that policies have been successfully delivered and applied. A journal is available which chronicles all policies and how they are being used by end users. General statistical trends regarding policy usage, such as the most frequently blocked applications and elevation privilege policies that are used the most, are available. Alerts can be created to inform the IT security team about actions taken that may cause servers to be less secure, such as removing the firewall software or disabling an anti-virus program.

This audit reporting offers critical insights and compliance validation that is not available with solutions that are based upon GPOs.

ACME		VIEWFINITY		
26-Aug-10 08:30:18 (GMT -04:00)				
Applied Elevate Privileges				
Active	Policy	Applied on	Application/Group	Rule
✓	<input checked="" type="checkbox"/> activex	All Computers	Application Independent	Permit ActiveX Installation
✓	<input checked="" type="checkbox"/> admin tasks	All Computers	Application Independent	Windows Administrative Tasks
Events for the period between 20-Aug-10 12:32:32 and 25-Aug-10 03:31:41				
Computer Name				Usage
<input checked="" type="checkbox"/> ALEX-XP2				4
Time	Type	Description	User	
20-Aug-10 12:32:32 (GMT -04:00)	Elevated Exe	"C:\WINDOWS\system32\rundll32.exe" /d C:\WINDOWS\system32\shell32.dll,Control_RunDLL timedate.cpl	DEMO\alex	
20-Aug-10 12:32:48 (GMT -04:00)	Elevated Exe	"C:\WINDOWS\system32\rundll32.exe" C:\WINDOWS\system32\shell32.dll,Control_RunDLL "C:\WINDOWS\system32\powercfg.cpl",Power Options	DEMO\alex	
23-Aug-10 22:28:13 (GMT -04:00)	Elevated Exe	"C:\WINDOWS\system32\rundll32.exe" /d C:\WINDOWS\system32\shell32.dll,Control_RunDLL timedate.cpl	DEMO\alex	
25-Aug-10 03:31:41 (GMT -04:00)	Elevated Exe	"C:\WINDOWS\system32\rundll32.exe" C:\WINDOWS\system32\shell32.dll,Control_RunDLL "C:\WINDOWS\system32\powercfg.cpl",Power Options	DEMO\alex	
<input checked="" type="checkbox"/> ALEX-W7				1
✓	<input checked="" type="checkbox"/> approved share	All Computers	Any Application	Install Applications
✓	<input checked="" type="checkbox"/> procmon	demo/finance	<input type="checkbox"/> procmon.exe	Elevated Privileges
✓	<input checked="" type="checkbox"/> shell	All Computers	Any Application	Shell Extensions

Figure7 – Example of Viewfinity Privilege Management policy audit reporting and validation

## Conclusion

With the Windows XP sunset date fast approaching, plans for Windows 7 migrations are in full swing. This has prompted most organizations to also re-assess their approach to PC lockdown. With the advanced privilege management capabilities offered by Viewfinity, enterprises have an alternative to the “all or nothing” approach to least privileges – because an “all or nothing” methodology prohibits organizations from meeting compliance, security and desktop operations goals. Viewfinity Privilege Management allows IT professionals to reach these objectives, without sacrificing user productivity or increasing support call volume, by providing granular, multi-level user permissions control. Endpoints are supported regardless of worker location as Viewfinity does not require laptops or desktops to be part of the Active Directory domain or to be directly connected to the corporate network in order to activate policies.

Finally, as you migrate to Windows 7, be prepared to manage and control administrative privileges by incorporating the Viewfinity Agent as part of the standard operating system image. This way you avoid having to separately deploy the agent after provisioning a new desktop or performing a migration.

## About the Author



### **Dwain Kinghorn** – *Partner at SageCreek*

Dwain's focus is to help companies align their product portfolio with their go to market and business requirements. Prior to SageCreek, Dwain was Vice President at Symantec Corporation and was in charge of the collaboration architecture to ensure multiple Symantec products work together. He was instrumental in the successful adoption of the Altiris platform at Symantec.

Dwain served as the CTO at Altiris from 2000 through the Symantec acquisition in 2007 and oversaw a development team that grew to over 500 people and an engineering budget in excess of \$50M. Dwain knows how to work with diverse teams across the world. He has a strong background in how to manage teams that consist of both employees and outsourced resources across the world. His leadership of the product teams was instrumental in Altiris' products receiving a large number of industry awards.

Dwain was instrumental in evaluating acquisition targets and has had a key role in the M&A process for many transactions. Dwain is a successful entrepreneur having started Computing Edge in 1994. Each year for 6 years Computing Edge experienced greater than 40% growth and each year the operation was profitable. Computing Edge was the recognized leader in solutions that extended Microsoft's management platform.

Prior to Computing Edge, Dwain worked at Microsoft in the Operating System division. Dwain graduated summa cum laude with a degree in Electrical and Computer Engineering.