

## Viewfinity Privilege Management Support for FDCC and USGCB

---

### *FDCC and USGCB*

The Federal Desktop Core Configuration and U.S. Government Configuration Baseline constitute a list of security settings recommended by the National Institute of Standards and Technology for computers that are connected directly to the network of a United States government agency.

In March 2007 the Office of Management and Budget issued a memorandum instructing United States government agencies to develop plans for using the Microsoft Windows XP and Vista security configurations. Released in June 2008, FDCC Major Version 1.0 specifies 674 settings, while Major Version 1.1 (released October 31, 2008) has no new or changed settings, but only expands on reporting options.

In 2010, the USGCB was issued as a replacement to the Federal Desktop Core Configuration (FDCC) and provides the baseline settings that Federal agencies are required to implement for security and environmental reasons.

### *Complying with FDCC and USGCB*

Managing a security structure as defined by the USGCB and FDCC can be a daunting task for any government agency. There are processes and procedures that must be followed to the letter, and it's imperative that the mandate be implemented and managed. One of the key principles of robust security is removing the local user as a direct Administrator of the computer. However, removing local Administrator rights presents an issue all on its own, as end users require elevated rights to install applications, install drivers (such as printers and ActiveX controls), perform maintenance on the computer, and more.

### *Better Compliance Control through Privilege Management*

For departments that currently lock down desktops, or who are in the process of meeting these governmental guidelines, Viewfinity offers government agencies the ability to manage administrative rights so that the settings mandated by the USGCB and FDCC security list are not compromised due to functionality needs. Viewfinity Privilege Management features are integrated with Active Directory and allow agency administrators to establish flexible privilege elevation policies for applications and desktop functions that require administrator rights. Desktops continue to operate within the least privileges mode except for those functions flagged by the agency administrator for elevated privileges, such as:

- **Applications:** Elevate privileges to administrative rights per application, not per desktop
- **ActiveX:** Manage permissions for non-administrative users to install ActiveX applications
- **Printers:** Manage permissions for non-administrative users to install printers or perform application installations (optional)
- **Windows Services:** Raise privileges to perform specific administrative functions (Device Management, Disk Defragmenter, Manage Services and User Accounts & Shares)



## *Policy Management: Automating USGCB and FDCC Compliance Policies*

Viewfinity Privilege Management features offer IT departments new methods for enforcing USGDB and FDCC compliance policies on all its PC assets regardless of the endpoint client's location or connectivity status. Both officially supported applications and those installed by end users can be better managed and provisioned. Upon installation, they automatically become part of the pool of applications that are managed according to your predefined policies. Administrators can be assured that no matter what end users might be doing while working offsite, all established USGCD and FDCC compliance rules are continuously enforced.

Critical applications can be grouped by agency/work units or functional roles and then associated with groups of computers for which a set of policies should be applied. Enforcement criteria range from notification-only of certain application installation or usage to imposing security rules by blocking black listed applications. With our automated policy management, Viewfinity addresses the needs of both end users and IT. While ensuring desktop security, end users have the flexibility to install applications that normally are not allowed on government assets.

Viewfinity Privilege Management features provide the ability to restrict individual applications from operating on your network on a per-machine or per-group basis. Applications can be restricted entirely or simply hidden during working hours while still remaining available to the end user for home or travel use.

### **Flexible, Configurable Rules**

Rules are customizable by groups, by application, and even by time period as defined by your IT hierarchy and policies. Corresponding alerts are set to monitor desktops and notify system administrators, and for specific predetermined guidelines, take action in the event of any end user policy violation. This ensures that the time and investment made by IT departments setting USGCB and FDCC IT policies are enforced automatically in real-time, without intervention by IT staff.

## *Viewfinity FDCC Compliance Verification*

### **Activity Auditing**

Viewfinity supports real-time monitoring and recording of laptop, desktop and application events, providing the administrator with an auditable record of all changes being made on the laptop or desktop. Viewfinity's precise activity recording feature provides a picture of all meaningful user/application activity for every laptop and desktop. When an audit needs to be performed on a specific PC, our Activity Recording feature both expedites the process, as well as aiding in the interpretation of the results of information collected. The IT Administrator simply accesses the desktop activity journal for the specific end user and a record of all recent desktop activities appears.

### **USGCB and FDCC Policy Auditing**

A key component for USGCB and FDCC policy management is the ability to audit and report on the status of privilege management policies. Administrators should not have to go through the process of remotely connect to a PC to validate that a policy is in effect. Instead, IT needs centralized management capabilities to report on and review the status of policies to determine whether they have been successfully delivered and are activated.

## *Flexible Implementation Methodologies*

In support of the Federal Government's Apps.gov cloud initiative to move applications to the cloud, Viewfinity Privilege Management can be implemented through our SaaS/Cloud platform or via your on-premise servers as a private cloud, or as an extension to Group Policy, enabling policies to be managed through the standard Group Policy Management tools.

## *Privilege Management Functionality Components for USGCB and FDCC*

### **Elevate Privileges**

Certain Windows applications and desktop functions require local administrative privileges in order to run and function properly on a desktop or laptop. Granting Full Administrator Rights creates a less secure desktop environment and opens the door for malicious hackers and viruses, thus organizations consider the practice of granting Administrator Rights to standard users to be risky. It also breaches compliance regulations posed by these mandates, which stipulate that administrative rights cannot be granted to end users and may not be made available on federal desktops and laptops.

Viewfinity solves this problem by elevating administrative rights for certain processes or applications rather than at the user account level. When permissions are raised, the elevation is performed directly within the security token of the user account. The application or process is started using the current user credentials as opposed to using RUN AS which needs the Administrative account in order to raise privileges. The RUN AS method potentially introduces security risks and issues for changes that are written into current user registry.

All elevation rules are applied in a real time and do not require users to cycle through the log off/log on process. Viewfinity doesn't require desktops to be part of the domain or to be attached to the central network in order for privilege elevation policies to be delivered. Detailed reporting provides intelligence on all administrator privilege policies, including an audit trail report that provides confirmation that a policy has been delivered and activated on endpoint devices.

Elevate Privileges supports ActiveX Controls, printer installations, computer management functions, and applications requiring administrator rights for local, remote and mobile users. Policies are delivered as soon as the PC connects to the internet.



## Benefits and Features:

### Key Benefits of Elevate Privileges:

- Automates privilege management by bringing endpoints into full compliance with corporate software policies as soon as they connect to the Internet
- Ensures USGCB/FDCC, SOX, and HIPPA compliance through centralized control and regulation of PC administrative rights
- Increases user satisfaction by providing flexible application policies instead of completely blocking non-standard applications
- Prevents the use of applications that create security risks
- Reduces probability of malicious and virus attack on corporate laptops & desktops
- Eliminates security risks by attaching administrative rights to Windows applications and processes rather than adding users to the administrators group

### Key Features of Elevate Privileges:

- **ActiveX:** Manages permissions for non-administrative users to install ActiveX Controls
- **Printers:** Manages permissions for non-administrative users to install printers
- **Computer Management Functions:** Raises privileges to perform specific administrative functions (Device Management, Disk Defragmenter, Manage Services and User Accounts & Shares)
- **Applications:** Elevates administrative privileges for approved applications without compromising security on the PC (managed via central console, no desk-side visits required)
- **Remote/Mobile Clients:** Automatically delivers policy to remote clients as soon as the PC connects to the internet
- **Reports:** Confirms policy delivery status to ensure policies were applied

### Block Application

Each organization has list of known applications which they do not want installed on its desktops. In some cases, IT may want to permanently prevent users from installing certain applications, while for other applications, blocking the execution of an application maybe a temporary measure. In order to stop unwanted software installations, some organizations opt to completely lockdown its desktops. This approach can be unproductive for end users as it doesn't offer any flexibility for supporting non-standard requirements, such as the needs of traveling or remote users.

Using Viewfinity, the IT Administrator may establish policies that identify applications (by group if needed) that should be blocked from executing on agency desktops and laptops. For example, a particular division may have a specific policy that prohibits any Instant Messaging software from executing. Viewfinity automatically enforces this policy for division members of that AD group, ensuring that these PCs are intact with USGCB and FDCC compliance regulations. Policies can be set for multiple combinations software such as Skype, ICQ, Yahoo Messenger, AOL, etc. Policies can also be flagged to unblock usage of specific applications while the end user is not connected to the internal network.



## *Benefits and Features of Block Application:*

### *Key Benefits of Block Application:*

- Secures desktops & laptops by blocking execution of black listed software
- Easily implements policies on PCs located outside of your internal network
- Prevents the use of applications that create security risks
- Reduces the time IT spends maintaining a standard desktop image
- Manages and secures applications from a Central Management Console - no need for individual desk-side visits

### *Key Features of Block Application:*

- Allows logical grouping of business applications and sets protection policies based on business unit's common applications, roles, etc.
- Creates work and home profiles containing applications that can be activated / deactivated accordingly
- Provides flexible application lockdown and maintains standard application configurations used to rollback to protected state
- Provides flexible scheduler allowing applications to be block based on timeframe
- Ability to apply "block" policies based end user location (on/off ) corporate network

### **Policy Automation powered by Zero Touch Technology**

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. When an end-user tries to run a particular application or perform a task that requires elevated permissions, the Viewfinity Agent automatically detects this and opens a dialog box where the user can enter his business justification for using this particular application.

The Viewfinity agent automatically routes the request to the IT Administrator via the Viewfinity Console, or by way of a report or an email. The IT Administrator can approve and activate the policy and elevate the privilege on the fly. Prior to approval, the IT Administrator can review the business justification provided by the end user as well as information about applications or task from the computer/user that initiated the request. Information related to Applications, ActiveX, Administrative Task, Scripts, etc. is automatically collected during the Policy Automation process. Policies are automatically created without manual intervention.

### **Viewfinity Local Admin Discovery**

This complimentary tool identifies 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.

### **Pre-Discover Applications Requiring Elevated Permissions**

Silently gather information and monitor which applications, processes, and administrative actions will require administrative permission before users are removed from the local admin group. Our Application Admin Rights Analysis 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.

#### **Video Audit / Policy Audit**

A key component for policy management is the ability to audit and report on the status of privilege management policies. Administrators should not have to go through the process of remotely connect to a PC to validate that a policy is in effect. Instead, IT needs centralized management capabilities to report on and review the status of policies to determine whether they have been successfully delivered and are activated. During a corporate audit, it is critical to know which applications are running with elevated rights, which are blocked, and to monitor the administrator who is enforcing these rules.

*Screen recording per Application/Policy:* Automatically creates and stores a screen recorded video of user activity based upon a particular application or policy. IT Administrators can elect to record user actions based upon specific policies and/or applications. This feature has wide-spread usage and appeal considering the type of information that can be recorded and used for policy auditing purposes. For example, you can monitor a user session during which the user has elevated permissions to install an application or it can be used for monitoring suspicious user activity. Screen recordings can be stored locally or on a network share.

*Administrator's actions log and reporting:* When an admin creates a policy, there is a corresponding audit log that tracks the administrator's actions and activity. Senior IT management and audit teams gain a clear understand of which policies are being activated/deactivated, created, and removed by the IT team.

#### **Integration of policy reports with SCCM**

Viewfinity offers an add-on component which is deployed on SCCM server that reports privilege management policy usage status and information regarding privilege access request from end users. The SCCM agent can collect Viewfinity policy events such as policy usage, insufficient privileges to install applications or ActiveX, requests from users to perform Administrative tasks such as disk defragmentation or the ability to change power options, etc. All information collected is transferred to the SCCM server through the add-on component. The status of Viewfinity policies and privilege access requests are tracked through the SCCM Console. This helps IT administrators by providing general system management tasks and privilege access activity from one management console.

