



## VIEWFINITY PRIVILEGE MANAGEMENT

---

### *Better Operations Control through Privilege Management*

Viewfinity Privilege Management offers IT Administrators a flexible approach for controlling its corporate desktop and laptop environment. With tighter, yet flexible control over the types of applications and privileges your distributed workforce are allowed, the more stable your desktop environment becomes. With this enhanced control over managing your environment, the number of end user support calls to the help desk are reduced. Through the use of automated policy settings, corporate guidelines can be established and applied for multiple dimensions of configurable, logical groupings: departments, applications, end users, connectivity status, time of day and more. Our group policies, combined with our privilege management features, offer a flexible yet secure approach to ensuring all your laptops and desktops automatically adhere to your corporate regulations.

Viewfinity offers the following Privilege Management features:

- Elevate Privileges
- Policy Management
- Application Lockdown
- Block Application/Whitelisting
- Activity Auditing
- Policy Auditing
- Support for FDCC, SOX, PCI Compliance and other desktop-level control procedures

### *Policy Management: Automating Compliance Policies*

Viewfinity Privilege Management features offer IT department's new methods for enforcing security and compliance policies on all its corporate PC assets regardless of the endpoint client's location or connectivity status. Both corporate 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 internal compliance rules are continuously enforced.

Business critical applications can be grouped by business 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 desktops security, end users have the flexibility to install applications that normally are not allowed on corporate 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 corporate 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 corporate IT policies are enforced automatically in real-time, without intervention by IT staff.

## *Corporate Compliance Adherence*

Management sets forth regulatory and corporate compliance objectives based on the risks and requirements of the business, and IT is responsible for enforcing these objectives through rules and policies. IT is also responsible for ensuring compliance with software licensing agreements, even on machines that are frequently outside of the corporate network. Due to limitations in available privilege management tools, enforcement tactics are often overly restrictive at the desktop-level in order to meet all compliance objectives set forth by the company.

An effective privilege management tool allows policies to be designed and enforced in a way that achieves the objectives of the company without creating unnecessary restrictions on the end user. This type of customization capability requires granular application-level enforcement and control on each individual desktop, with enough intelligence built-in so that the IT management process is automated and simplified as much as possible. For example, applications can be white listed by time slot whereby enabling/disabling access to certain applications during working hours or weekends.

By leveraging encapsulation, Viewfinity's Privilege Management features provide this type of application-level control and policy customization on the desktop. Many policies that formerly required complete lockdown can now be enforced without creating excessive limitations on the end user machine.

## *Privilege Management Functionality Components*

### **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 the Sarbanes-Oxley Act and HIPAA. Additionally, the US Government Federal Desktop Core Configuration (FDCC) mandate stipulates 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 corporate 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 Federal FDCC, SOX, HIPAA and FDCC 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
- Administrators can create policies that will execute scripts without needing to assign local administrator rights to the end user

### *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
- Identifies applications that require administrator rights before removing privileges

### **Block Application**

Each organization has list of known applications which they do not want installed on its corporate 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 may be 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 corporate desktops and laptops. For example, the Brokerage division has a specific policy that prohibits any Instant Messaging software from executing. Viewfinity automatically enforces this policy for members of the Brokerage group, ensuring that these PCs are intact with corporate 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 corporate 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 corporate 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
- Permits or blocks the use of child processes

**Application Lockdown**

Not all applications should be left completely unlocked to end user customization. In some cases, you may want to maintain a standard application configuration for all users. Our Application Lockdown feature provides the ability to set protection policies per application or group of applications, while still maintaining the capability to customize all other common desktop applications. With Application Lockdown you can prevent any unauthorized changes to files, registry keys, application settings and updates.

For example, the IT department can identify specific business-critical applications which should not be updated without following the appropriate change management process. If a change is detected to the configuration files, registry setting, dlls, or executables for any of these flagged applications, Viewfinity will automatically rollback the application to its protected state.



## *Benefits and Features of Flexible Application-Level Lockdown Policies:*

### *Key Benefits of Application Lockdown:*

- Automates management of privileges for applications deployed by both IT and by users
- Implements policies on PCs located outside of your corporate network
- Increases user satisfaction by providing flexible application policies instead of completely blocking non-standard applications
- Improves network and asset utilization by restricting the use of non business-critical applications during business hours
- Secures sensitive corporate assets such as critical applications and files while working offline
- Ensures business-critical applications are meeting corporate configuration standards

### *Key Features of Application Lockdown:*

- Allows logical grouping of business applications and sets protection policies based on business unit's common applications, roles, etc.
- Configures rules at a granular level; by time period, connectivity criteria (online or offline from the corporate network)
- 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
- Manages and secures applications from a Central Management Console - no need for individual desk-side visits

### **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.

### **Policy Auditing**

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.

