

VIEWFINITY PRIVILEGE MANAGEMENT SUPPORT FOR FDCC

FDCC

The Federal Desktop Core Configuration is 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.

Complying with FDCC

Managing a security structure as defined by the 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 FDCC Control through Privilege Management

For departments that currently lock down desktops, or who are in the process of meeting the FDCC guidelines, Viewfinity offers government agencies the ability to manage administrative rights so that the settings mandated by the 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 FDCC Compliance Policies

Viewfinity Privilege Management features offer IT departments new methods for enforcing 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 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 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.

FDCC Policy Auditing

A key component for 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.

Privilege Management Functionality Components for 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 the FDCC mandate, which 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 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 Federal FDCC, SOX, HIPPA 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

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 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

