Privilege Management Deployment & Best Practices
**Table of Contents**

ENDPOINT LOCKDOWN REQUIRES PRIVILEGE MANAGEMENT CAPABILITIES  
BEST PRACTICES FOR IMPLEMENTING A PRIVILEGE MANAGEMENT PRODUCT  
STUDY YOUR ENVIRONMENT AND DEFINE ORGANIZATIONAL NEEDS  
DISCOVER USER ACCOUNTS THAT HAVE LOCAL ADMINISTRATIVE RIGHTS  
TESTING IN A LAB  
TRUSTED SOURCES  
PILOT  
PRE-DISCOVER APPLICATIONS REQUIRING ELEVATED PERMISSIONS  
PREPARING FOR THE DEPLOYMENT STAGE  
POLICY AUTOMATION FOR EXCEPTIONS TO USER PERMISSION NEEDS  
VIEWFINITY PRIVILEGE MANAGEMENT DEPLOYMENT OVERVIEW  
VIEWFINITY COMPONENTS  
VIEWFINITY DEPLOYMENT TIME LINE AND DELIVERABLES
**Endpoint Lockdown Requires Privilege Management Capabilities**

There are a number of use cases where organizations may want end users to be able to perform operations that generally require administrative level access to the system.

For example, organizations may want to allow users to install certain ActiveX controls. They may want to allow anyone to be able to install and configure new printers on a system. A traveling user may want to be able to install certain applications without having to be connected to the corporate network. Mobile/remote users may need to perform particular system level tasks on their own. Certain applications may need to run with elevated rights to be able to function as expected.

In all of these cases, a privilege management system adds value. A privilege management system balances the rigidity of locking down systems with the realities of user customization needs on the endpoint. It helps ensure that the right applications run with the proper privilege levels, and provides the system administrator with the validation to ensure that endpoints match an approved configuration standard.

**Best Practices for Implementing a Privilege Management Product**

A project of this undertaking requires extensive analysis to determine user needs and prepare the environment. As organizations work 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 Advanced Persistent Threat risks.

**Study Your Environment and Define Organizational Needs**

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

Different divisions of your organization have different rights on desktops. This can vary by individual user or a group of users. Even within the same division, a hierarchy of employees may exist and the rights can differ.

**Questions to consider:**

- Do you know how many users in your organization have administrative rights?
- Had you decided who among your users will have (if at all) administrative rights?
Having detailed information related to which users and groups have administrative 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.

**Best Practice:**
- Perform a scan to discover how many users have administrative rights
- Plan to remove administrative rights from as many endpoints/users as possible

**Testing in a Lab**

Best practices dictate that testing start in a completely controlled environment. For this stage several days should be allocated. We suggest testing on computers which will contain standard images used for deployment in your organization. Start by installing the Viewfinity Administrative Console on one of the computers. Next, install the Viewfinity agent on computers with standard images and then run our privilege management software in discovery mode. This will kick off our Application Admin Rights Analysis and will silently gather information that identifies which applications, processes, and administrative actions will require administrative permissions. Having this information before users are removed from the local administrator group is key during the preparation phase.

The initial analysis should start by testing basic features and manual policies. It is extremely important to understand that your environment may likely contain hundreds of thousands of endpoints and many hundreds of applications. It is for this reason precisely that automated tools are necessary to help you accurately identify which applications, etc. will require privilege elevation policies. 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.

During the initial stages, it is important to test the reporting capabilities of the software solution. Knowing what information you’ll need to analyze and take action on will help you define reports -- this exercise will save time in the future. After several days of lab testing, most policies that will be needed in production can automatically be created. This is because the information needed to create the policies is based on actual end user activity that has been collected over a period of
time. Once the collection and analysis is completed, policies to elevate privileges are automatically created. This advance preparation ensures that when administrative rights are removed, all policies are in place, ensuring a non-disruptive move to least privileges.

**Trusted sources**

During lab testing we suggested that you establish major policies based on Viewfinity Trusted Sources. The Viewfinity Administrator can define Trusted Vendors. Scenarios include:

- Trusted vendors - any software signed by this vendor and requiring administrative rights will be elevated.
- Trusted share - any software residing on this share will be available for standard user to install; and other options of Trusted Sources (see our manual for additional details).

Using our Trusted Sources approach will dramatically decrease the need for additional policies in a standard OS image environment.

**Pilot**

The pilot project should start with a selection of typical end user computers. It is important to include computers of end users who have administrative rights and end users who are standard users. Factors for choosing the right computer include: typical OS platforms, departments (ranging from the simple environment of a teller’s computer to a complicated environment such as that of a software engineer), physical location, location in the AD forests, users who are not members of the domain, users who are located outside of corporate firewalls. You can study the implications of the policies in action, alter them, and expand where appropriate. Survey and monitor participants to capture data that supports the need for elevated rights for those employees that are using work-related applications that require administrator rights. We suggest choosing 20-40 end users for the pilot. The process should begin from the monitoring/discovery mode, i.e. you should not change any user rights or activity during the initial discovery and creation of policies phase.
Pre-Discover Applications Requiring Elevated Permissions

**Best Practice:**

- Prior to removing administrative rights, include a group of users who require administrative rights and enable the discovery process. This process will analyze user activity and compile a list of applications based on user activity that require administrator rights;
- After the list of applications is collected, analyze the results and generate policies;
- To elevate access to specific application/version, create an Elevate Privileges policy;
- To elevate all applications from specific vendor or product create a Trusted Sources policy.

Below is an example of silently discovered applications which required administrative rights. From this screen, policies can automatically be generated.

We recommend 10-14 days for the discovery stage. The results show the following:

- The list of applications discovered by the Viewfinity software which require administrative rights
- Events include application type (EXE, MSI, COM, ActiveX, etc.) product name, request date, business justification, and a count of specific requests
• Collected events are classified by users account type: Standard Users and Administrators.
• By highlighting a specific event policy, it can be automatically approved.
• Identical events from multiple computers are automatically combined and presented as a single event. This aggregation of events identifies trends in your organization related to applications that should be considered for elevation policies.

Questions to consider:
Choose a common model for each department (ranging from support required for a call center to support needed for developers), for instance:
• End-users do not have administrative rights but some applications / system tasks will need elevated privileges using the software solution;
• End-users who do have administrative rights but some applications / system tasks are forbidden;
• Endpoints are completely locked down / then only carefully chosen applications can be used (whitelisting).

Preparing for the deployment stage

In preparation for full deployment of the Viewfinity product, it is suggested that administrators and project planners of the solution will be trained by the vendor. The vendor should be involved in launch preparations, the overall test plan, the success criteria, and during the review of the initial policies developed during the pilot phase prior to a mass deployment of agents. While 90% 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. We strongly recommend having a clear method for collecting feedback and communicating between end users and the personnel performing the deployment.

Policy Automation for Exceptions to User Permission Needs

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.
If a user attempts to launch an application that requires administrative rights, Viewfinity automatically detects that the application requires administrative rights. To easily support this situation, you can enable our end-user justification dialog which is used to collect justification from end users when requesting elevated rights.

**Best Practice:**
- Edit End-User messages by displaying custom messages, logos, URLs, (multiple languages are supported);
- End-User requests and justification messages can be configured to record and enter a help desk ticket as long as the help desk system accepts tickets in email format.

**Viewfinity Privilege Management Deployment Overview**

Viewfinity Privilege Management features are integrated with Active Directory Group Policies and allow IT administrators to establish flexible privilege elevation policies for applications and desktop functions requiring administrator rights. Desktops continue to operate within the least privileges mode except for those functions flagged for elevated privileges, such as the ability to run applications requiring administrator rights, printer installations, ActiveX controls, and more. Additionally, Viewfinity Privilege Management uses the same common rules and features to allow you to black-list prohibited or harmful applications, effectively blocking them even when the users have administrative rights.

**Viewfinity Components**

Viewfinity Privilege Management is intended to work on multiple clients, using a domain-distributed group policy.

**The Viewfinity Agent** needs to be deployed to each client intended for policy management.

Supported platforms
- Windows XP SP3
- Windows Vista SP1
- Windows 7
- Windows 7 x64
- Windows Server 2003 SP3
- Windows Server x64 2003 SP3
- Windows Server 2008
- Windows Server x64 2008
- Windows Server x64 2008 R2

Viewfinity agents can be deployed using a GPO software deployment policy or by using an existing software delivery method such as SCCM or a similar tool. Viewfinity agents have a very light footprint on Operating System performance due to the following characteristics: 25-30MB disk space, 3-5MB RAM and less than 1% of CPU load.

**The Viewfinity GPO Editor** (Administrator Console) is required to manage Viewfinity policies, discover applications requiring administrative rights, and report on the status of policies.

Required components
- Microsoft MMC 3.0
- Microsoft .NET Framework 3.5 SP1
- Internet Explorer 8 and up
- Microsoft Report Viewer 2010
**Viewfinity Deployment Time Line and Deliverables**

In addition to Viewfinity providing consulting services in order to optimize timelines and execution, Viewfinity will need to engage with SME’s responsible for the following:

1) System Engineer responsible for Group Policy Objects (GPO) management
2) Application Deployment Expert

<table>
<thead>
<tr>
<th>Deployment Phase</th>
<th>Proposed Time Line</th>
<th>Client resource requirement &amp; approximate time required</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Testing in Lab</strong></td>
<td>Week 1 (5 days)</td>
<td>GPO System Engineer 10 hours</td>
</tr>
<tr>
<td>• Set Scope of the Project</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Test on 5-10 standard desktops</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Discover Users with Admin Rights</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Discover Applications</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Create Policies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Remove Admin Rights</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Report Status of Policies</td>
<td></td>
<td></td>
</tr>
<tr>
<td>• Success Criteria</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

| **Pilot Testing**                      | Week 2 (5 days)    | GPO System Engineer 20 hours                           |
| • Identify Pilot Users from multiple BU|                    | Application Deployment Expert 2-5 hours                |
| • Train Administrators from pilot BUs  |                    |                                                        |
| • Deploy Agents (20-40 desktops)      |                    |                                                        |
| • Discover Users with Admin rights    |                    |                                                        |
| • Discover Applications              |                    |                                                        |
| • Create Policies                     |                    |                                                        |
| • Remove Admin Rights                 |                    |                                                        |
| • Report Status of Policies           |                    |                                                        |
| • Success Criteria                    |                    |                                                        |

| **Viewfinity Product Training for IT Staff** | Week 3 (2 days) | IT Staff - 2 days of training |
| • Viewfinity will provide training sessions for IT Administrators and GPO Engineers | | |

| **Production Deployment**               | Weeks 4 and 5 (10 days) | GPO System Engineer 30 hours |
| • Deploy Viewfinity Agent to production desktops | | Application Deployment Expert 7-9 hours |
| • Deploy Viewfinity GPO Editor           | | |
| • Discover Applications                 | | |
| • Create Policies                        | | |
| • Report Status of Policies              | | |
| • Remove Admin Rights                    | | |

| **Post Deployment Support**             | Week 6 (5 days)       | GPO System Engineer 16 hours                           |
| • Create ad-hoc policies                | |                                                        |
| • Address deployment issues             | |                                                        |
| • Transfer Knowledge                    | |                                                        |
| • Use Admin Discovery tool to identify remaining presence of Admin Rights | | |
| • Generate policy reports               | |                                                        |