Viewfinity Release Notes

These release notes apply to Viewfinity Application Control & Privilege Management 5.0 (GPO) Release 5.0.44.789

- Added new fix for behavior of Chrome v42.0.2311.152 or newer when the Configuration setting "Discovery Source URL" is turned on.
- Added Viewfinity Launcher tool installation to the SnapIn installation
- Fixed Policy Automation dialog on ActiveX installation if a specific ActiveX installation is Trusted by Publisher

These release notes apply to Viewfinity Application Control & Privilege Management 5.0 (GPO) Release 5.0.44.788

- Fixed behavior of Chrome v42.0.2311.152 or newer when the Configuration setting "Discovery Source URL" is turned on.
- Made the Configuration setting "Discovery Source URL" turned off by default.

These release notes apply to Viewfinity Application Control & Privilege Management 5.0 (GPO) Release 5.0.44.785

- Added a standalone tool (VF_Launcher) which allows starting applications "as different user" without specifying password.
- Added options to apply policies (elevate, block, start normal) by Publisher on local disks only. This option improves performance of when files are accessed on network drivers. There is an option to apply global change to all existing policies. Contact Viewfinity Support for more details
- Added option to Trusted Sources "Apply Policy to local drivers only" This option improves performance of when files are accessed on network drivers.
- Added option to apply Policies by Checksum on local disks only. This option improves performance of when files are accessed on network drivers.

- Fixed command "vf_agent.exe -RequestPolicies. In previous builds the command did not force policy update

These release notes apply to Viewfinity Application Control & Privilege Management 5.0 (GPO) Release 5.0.44.782

- Fixed freeze in IE when Viewfinty agent is present
- Improved visibility of "Script" icon when policy is active and deactivated.
- Added option for limited monitoring of network drives in case of slow file copy from network or losing connection to network driver. New setting is located under *Settings/General Setting/Network Shares Support*. Default option is "Full". Set this option to "Limited" in case of slow file copy from network is observed.
- Fixed issue of high CPU utilization when opening Internet Explorer. The issue was related to performance of resolving of environment variables
- Fixed not working "Refresh" under "Programs and Features"
- Improved handling of GPO XML files corruption. Provides to uses option to restore last good know xml file and option not to reset to original settings in case if non-critical xml file was corrupted.

These release notes apply to Viewfinity Application Control & Privilege Management 5.0 (GPO) Release 5.0.42.780

- Updated list of excluded Anti-Virus products in Settings, Files to be ignored always
- Fixed issue of saving files from browser to NAS when "Discover URL" setting is enabled
- Fixed issue of loading driver in a safe mode
- Fixed support of UNICODE languages
- Fixed definition of built in JAVA updater
- Fix potential freeze in agent
- Improved exclusion of network share based paths in "Files to be excluded always". Now path is ignored by driver.

These release notes apply to Viewfinity Application Control & Privilege Management 5.0 (GPO) Release 5.0.41.776

- Added popular COM objects in Pre-defined policies
- Removed "Trust" and "Block" shortcuts and Actions for the "Microsoft Windows" Publisher. It is not recommended to elevate or block "Microsoft Windows" digital signature

- Added support to "Files to be ignored always" to exclude by Viewfinity agent and driver. In previous versions ignore was applied only by agent
- Improved support of Terminal Servers
- Fixed slow execute of scripts from mapped drives
- Fixed handling on non-existing Domain Users in Policies which resulted in delayed connection to VPN clients.
- Fixed Revision History capturing. In previous version some events were not captured.
- Fixed agent behavior on simultaneous update and user logoff. Windows Error 7011
- Fixed removing of security ACLs from catroot by Viewfinity
- Fixed error message behavior on "Cancel" in Elevate user dialog
- Fixed handling of common (non-Policy) Dialogs such as "About" in order to avoid issue of replacing default dialog message from another GPO object.
  Note: Applicable to newly created GPO objects
- Added option to elevate installations from SCCM if installation option is performed Under user account. The option is available under General Settings, "Elevate SCCM for User Installations". The default setting is on.

These release notes apply to Viewfinity Application Control & Privilege Management 5.0 (GPO) Release 5.0.40.772

- Added support of UAC replacement in "Run Normally" Advanced Policy and Application Group
- Added UI dialogs and UAC suppress for Elevate If Necessary Policy per user type: Administrator or Standard User
- Added possibility to hide Viewfinity window icon in end-user dialogs
- Added customization of font in End-user Dialogs
- Fixed left-side alignment of End-user Dialogs
- Fixed End-user Dialog background color
- Added popular Antivirus products to "Files to be ignored always"
- Fixed ignoring of quotes in path of exclusions
- Fixed handling of URLs with UNICODE characters in MSIE
- Fixed upgrade/uninstall of Viewfinity Agent by limited (regular) User when Trust is applied
- Fixed possible error when opening Inbox or Policy Usage
- Fixed MSIE8 crash when Inbox is set to Elevate if necessary

These release notes apply to Viewfinity Application Control & Privilege Management 5.0 (GPO) Release 5.0.38.760

- Added integration with Check Point Threat Cloud and FireEye AX to Threat Detection section of Viewfinity management console. Applications from Inbox can be send for malware verification analysis to sandbox platforms of Check Point or FireEye
  Note: Integration with Check Point requires license of Check Point Threat Cloud (certificate key). Integration with FireEye requires existing installation of FireEye AX platform
- Added support for policy automation & policy usage events triggered by Windows 8 Apps
- Added option on the client Viewfinity taskbar icon not to cancel policy suspension after reboot/logoff
- Added warning on creation of a policy applying to core system processes such as explorer.exe, lsass.exe, smss.exe, winlogon.exe, svchost.exe, etc.

These release notes apply to Viewfinity Application Control & Privilege Management 5.0 (GPO) Release 5.0.37.751

- Added Event Offline Aggregation tool for Inbox.
  Note: install can be found on management snap-in PC as a separate installation in C:\Program Files\Viewfinity\Application Control & Privilege Management\Packages\ VFEventOfflineAggregationSetup.msi including user manual
- Improved "Microsoft Windows OS" Policy activation for better multi-GPO interoperability
- Fixed elevation of installations performed by SCCM with "Installation behavior" executed as "user" instead of "Install under "system" account
- Fixed issue with multiple GPOs corrupting user dialogs
- Fixed behavior of inherited process from cmd.exe/explorer (whether to elevate or not) when Trust All policy is used.

These release notes apply to Viewfinity Application Control & Privilege Management 5.0 (GPO) Release 5.0.36.746

- Added support of Windows 8 Applications for Block/Run policies.
- Added option to suppress notification page for elevation of web pages. Option can be found under End-User UI, Common UI settings, Web pages, Enable intro web page.
- Added advanced targeting option for default policies. Note: applies to Application Control product. New option can be found under Policies, Grey List, Default Policies wizards.
- Added End-user UI per user type (Admin/Standard) for Policy Automation / Policy Usage
- Fixed issue with with hidden UAC/Viewfinity dialog introduced by one of the Microsoft's updates

- Fixed native toolbar in elevated "Add/Remove Programs". In previous version some default options in Add/Remove Programs were missing.
- Fixed issue when application policy does not apply when there is "Trust All" and the application is ran from CMD

These release notes apply to Viewfinity Application Control & Privilege Management 5.0 (GPO) Release 5.0.34.737

- Added Threat Detection integrations with VirusTotal, NSRL, and PaloAlto
- Added option to protect modification of local administrator's group by administrator or elevated application. The option can be found under "Advanced" section of Agent Configuration: Protect administrative User Groups (default value "Off", "When turned on, administrative User Groups cannot be modified"). The following groups are protected from modifications when setting is set to ON:

  - Local Administrators (SID: S-1-5-32-544)
  - Power Users (SID: S-1-5-32-547)
  - Account Operators (SID: S-1-5-32-548)
  - Server Operators (SID: S-1-5-32-549)
  - Print Operators (SID: S-1-5-32-550)
  - Backup Operators (SID: S-1-5-32-551)
  - BUILTIN\Network Configuration Operators (SID: S-1-5-32-556)
  - BUILTIN\Hyper-V Administrators (SID: S-1-5-32-578)

- Added possibility to activate/deactivate separate Applications in Application Group. In previous version only whole application group could be activated/deactivated.
- Added possibility to move/assign applications (including Inbox events) to existing advanced policy
- Possibility to manage Policy Tree representation (Layout with turning on/off of the folders). Option is implemented under Policy pane, Layout, view. Option is available in Privilege Management license only
- Added various new security protection features.

These release notes apply to Viewfinity Application Control & Privilege Management 5.0 (GPO) Release 5.0.33.730

- One-time Run Authorization – added possibility to use various file parameters (digital signature, file description, virus total verification) in Request ID and to insert them in the email template
- Added ability to create Advanced Policy from Inbox (right click option)

- Added discovery of URL (from where a file was downloaded) as part of file history. URL can be found in Inbox, Source "Internet". Currently supported browsers: IE 8.0 and newer and Chrome

- Added VirusTotal Integration for file checksum (hash) and Source URL verification with external reputation service of Google. Verification option can be found in several places of UI including : Reputation score , Inbox Actions pane, right click on file

- Added setting to turn off collection of Agent trace under General Settings, Advanced, and "Collect of Agent Trace". Default is Yes

- Added configurable list of "well-known" Publishers used in Reputation. Setting can be found under: General Settings, Advanced, "Well Known" Publishers. By default 46 signatures of well-known vendors are entered.

- Added notification warning messages upon selection of default deny block policies

- Improved default behavior when there is "Trust All" policy and application or script is executed from command prompt. In previous version application executed from command prompt inherited policy of parent process which created problems with some installations

- Fixed misbehavior when third party application switches desktops and as result closing Viewfinity dialogs

These release notes apply to Viewfinity Application Control & Privilege Management 5.0 (GPO) Release 5.0.32.718

- Support of Viewfinity agent on Windows 8.1 operating system
- Added "Application Type" option in filter for advanced policies
- Added option not to send events from system users to Inbox . The setting is called "Report events triggered by service accounts". Events include the following accounts
  - Local System
  - Local Service
  - Network Service

  Default value is 'No'

- Added option to send Inbox/Policy Usage events once only in order to reduce amount of events in Inbox. The setting is called "Report launching of Applications once only ". If turned on, information about subsequent events for the same Application will not be

reported (including the event Count Information, End-user's Justification and possibly different command line arguments). Default value is 'No'

- Added option to send User Groups in Source/Pre-history . The setting is called "Report User Groups in events". It is recommended to turn off if Users triggering the events are usually belonging to numerous User Groups - the size of events may be shortened significantly. Note: if turned off the Trusted User/Group Policies defined for User Group will not affect events in Inbox. Default value is 'Yes'

- Added option to refresh Desktop on Policy update . If turned on, the Windows desktop of End-user will be forced to refresh on each Policy update. The setting is located under the "Viewfinity Icons" in "Common UI Settings" pane . The setting is called Refresh of Windows desktop on Policy update . Default value is 'Yes'

- Improved capturing of applications requiring administrative rights

- Improved Advanced Target browsing of users in user configurations on Windows 2003 or XP
- Improved reporting of various events in Inbox .

These release notes apply to Viewfinity Application Control & Privilege Management 5.0 (GPO) Release 5.0.31.712

- Added various filtering options to advanced policies such type of action, priority , active
- Added support to include sub-folders and files when creating Set Security Permissions policy for folders
- Improvements for creating end-user dialogs with text but no justification
- Added warning message when trust policy is created for MS Windows
- Improved End User messages when dialogs names length exceeded the box width.

These release notes apply to Viewfinity Application Control & Privilege Management 5.0 (GPO) Release 5.0.30.710

- Improved Agent tracing. Record events such as policy usage. Requires change in general settings pane
- Added column "Description" for Advanced Policies
- Fully supported Enhanced Protected Mode (EPM) in Internet Explorer 10
- Added .NET 3.5 to pre-requisites of GPO Editor Viewfinity Snap-in

These release notes apply to Viewfinity Application Control & Privilege Management 5.0 (GPO) Release 5.0.29.707

- Improved Viewfinity RSoP tool
- Improved compatibility of Internet Explorer 10 Enhanced Protected Mode and Viewfinity add-on for Internet Explorer
- Improved support for VBE scripts embedded in Policy.
- Improved visualization of expired Policies. In previous version there was no visual difference between expired and active policy
- UI Changes: replaced term "Rule" by "Action" where it was used
- Reputation of Applications signed by Microsoft is "High 10" always now.

These release notes apply to Viewfinity Application Control & Privilege Management 5.0 (GPO) Release 5.0.26.703

Improvements:

- Added "Copy" option for items in Event Details dialog in Inbox
- Added "Advanced Search" for items (e.g. Process) in Event Details dialog in Inbox
- Improved performance of Inbox
- Improved applying of Policy in User Configuration

These release notes apply to Viewfinity Application Control & Privilege Management 5.0 (GPO) Release 5.0.24.699

New Features

- Added "View By Source" in Inbox event details
- Added possibility to apply Trusted Publisher Policy to Applications installed by Apps signed by the Publisher
- Removed limitation not to apply Trusted Publisher Policy to Network Shares
- Changed the implementation of Windows Explorer Viewfinity add-on including Shell Extension policy and Viewfintiy Extended File attribute (note: if Agent is upgraded, a restart is needed to have the add-on working; the upgrade itself does not require restart)

Improvments:

- Policy Propagate Failed: 'Access is denied' when specifying user other than 'Current user'

- Very long justification is dropped along with email

- Unable to create Trusted publisher from aggregated view if event contains multiple publishers

- General Settings: 'Files to be ignored always': 'Location' cannot be deleted from an entry

- Microsoft dialog about computer restart appears for a few seconds during agent installation.

- New application events not collected to inbox on windows 8 for MSI installation

- Trust by Publisher for network share - CPU consuming in Explorer.exe