EVS Windows update and Antivirus policies

Rules applied to EVS applications

2017-10-18

Corporate
+32 4 361 7000

North & Latin America
+1 973 575 7811

Asia & Pacific
+852 2914 2501

Other regional offices
www.evs.com/contact

TABLE OF CONTENTS

INTRODUCTION

This document describes the policies applied to Windows stations running EVS applications in terms of Windows Updates deployment and Antivirus.

As software updates and antivirus can have a dramatic impact on application performances and functionalities, these two aspects must follow the rules described below.

WINDOWS UPDATES

DEFAULT CONFIGURATION ON EVS HARDWARE

To avoid unmanaged windows patch deployement, the Windows Update service is disabled by default on EVS hardwares running a Windows operating system

SUPPORTED UPDATE SCENARIOS

UPDATE FILTERS

- Only security and critical updates can be deployed on an EVS station
- No .Net Framework updates or patches can be deployed without prior EVS validation
- No Windows Service packs can be deployed without prior EVS validation
- No updates can be applied to EVS management station without EVS agreement

DEPLOYMENT RULES

- Deployment of updates should be controlled or done manually. No automatic update are permitted
- Windows Update service cannot be configured to automatically deploy updates coming from the Windows Update Internet Service
- EVS support or project management must be notified at least 10 days before the update
- The customer must provide a definite list of all windows updates they wish to apply, to be assessed by EVS
- EVS may refuse a request to apply a patch if it is deemed that it will cause problems with the software

HOW TO DEPLOY UPDATE

MANUALLY DEPLOY FIXES

- Set Windows Update service to manual start-up
- Start Windows Update service
- Run the fixes installation files manually
- Restart the station if needed
- Set Windows Update service to disable

CONNECT TO A WSUS (WINDOWS SERVER UPDATE SERVICES)

- Configure the Windows Update intranet server in the Group policies
- Start Windows Update Service
- Manage the deployment with the WSUS

ANTIVIRUS SOFTWARE POLICY

For products running Windows 7, Kaspersky is the only antivirus software validated by EVS to guarantee the proper operation of its products.

For products running Windows 10, Microsoft Windows Defender is the only antivirus software validated by EVS to guarantee the proper operation of its products.

EVS recognises that there are other antivirus products available, and that customers may have a prefered vendor.

If customer do not want to use Kaspersky antivirus on Windows 7, EVS recommends to upgrade to windows 10, providing a clean state of the system. Contact your EVS representative for the conditions.

If such an upgrade is not feasible, uninstall procedures are provided by Kaspersky. These procedures go beyond a standard uninstall. The most recent procedure can be found at https://support.kaspersky.com/common/service/1464. It must be noted that EVS did not validate this approach. EVS cannot guarantee that the uninstallation will be successful. EVS cannot guarantee that the system will behave as desired after having applied this procedure.

Where a customer installs a third party antivirus product, EVS stronly recommends that it is tested thoroughly by the customer. In larger installations, it should be tested on a customers test system, or on a contained part of the larger system before deployment to the entire system.

EVS will not be responsible for the installation and configuration of the third party antivirus software, but it can offer advice to the customer on suggested configurations. Below you can find an example configuration of the antivirus software that EVS would deploy. It can be used as a guideline for the customer to install, configure and test their prefered antivirus product.

If a Site Acceptance Test, as part of a project, is passed with third party antivirus software installed, EVS will support the third party antivirus software, but it is not considered as validated.

EVS support will request for any antivirus product to be disabled or uninstalled first if they feel it is interupting in the day-to-day operation of the products, suspected to cause an issue, or interfering in the investigation of an open support-case. EVS will not continue with a support case until this request has been fullfilled.

ANTI-VIRUS CONFIGURATION FOR MICROSOFT DEFENDER ON WINDOWS 10 OS

With Microsoft Windows 10, to avoid low performance while transfering files from a local network, the group policy must be edited.

- From the start menu, run “gpedit.msc”
- Browse the “Local Computer Policy” tree to “Computer Configuration > Administrative Templates > Windows Components > Windows Defender > Scan”
- Disable the following policies
  - “Run full scan on mapped network drives”
  - “Scan network files”

TYPICAL ANTI-VIRUS CONFIGURATION FOR NON-KASPERSKY ANTI-VIRUS FOR WINDOWS 7 OS

As a reference, here is the typical configuration applied to the antivirus used on EVS hardwares. We strongly recommend to follow the same kind of configuration would another antivirus be installed on stations where EVS applications are used.

- The firewall component and the port monitoring component should be disabled.
- The NDIS drivers should not be installed.
- Antivirus engine starts on computer start-up.
- Objects to detect: Viruses and worms, Trojan programs, Malicious Tools, Adware, Auto-Diallers, Packed files that may cause harm, Multi-packed files
- The following objects are excluded from scan (trusted zone):
- **EVS Applications and Files**
  - Video files: *.avci, *.avi, *.dnx, *.dv, *.imx, *.imx, *.m2t, *.m2v, *.mov, *.mp4, *.mpg, *.mpv, *.mxf, *.prores
  - Audio files: *.aud, *.m2a, *.pcm, *.mp3, *.wav
  - Miscellaneous files : *.bmp, *.dif, *.gho, *.ghs, *.ini, *.jar, *.jpeg, *.jpg, *.km, *.kmt, *.ldf, *.mdf, *.ndf, *.plst, *.tga, *.tiff, *.xml

- **Windows and Backoffice applications**
  - %SYSTEMDRIVE%\Pagefile.sys *
  - %SYSTEMDRIVE%\System Volume Information\catalog.wci *
  - %SystemRoot%\system32\MsDtc\msdtc.log *
  - %SystemRoot%\system32\inetsrv\* *
  - %SystemRoot%\IIS Temporary Compressed Files* *
  - %SystemDrive%\inetpub\temp\IIS Temporary Compressed Files* *

- %SystemDrive%\inetpub\logs\logfiles\w3svc\* *
  - wsusscan.cab *
  - wsusscn2.cab *
  - %ProgramFiles%\EVS Broadcast Equipment\ *
  - %ProgramFiles(x86)%\EVS Broadcast Equipment\ *
  - %ProgramFiles%\EVS Avid Tools\ *
  - %ProgramFiles(x86)%\EVS Avid Tools\ *

- Scan is activated for all removable drives and all hard drives with the following options:
  - Heuristic Analysis: light scan
  - Scan only new and changed files
  - Scan embedded OLE objects
  - Scan mode: smart mode
- Action on threat detection: select action automatically (no user intervention requested)
- Scheduled tasks:
  - Update: manually (to be set by the customers, outside operation hours)
  - Full scan: manually
  - Critical Areas Scan: after application start-up, Security level = high, Scan scope: System Memory, Start-up Objects, Disk boot sectors
  - Custom scan: manually
  - Idle scan: disabled
  - Action on removable drive connection: Quick scan
- Self-Defense is disabled
- All notifications are saved in logs (no user notification on screen)

Remark : This configuration is also in place for default Antivirus provided by EVS on Windows 7 OS.