EVS Windows Update, EDR and Antivirus policies – EVS Applications

2022-09/1.0

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 CONTENT

INTRODUCTION

This document describes the policies applied to Windows stations running EVS applications in terms of Windows Updates deployment, Antivirus and Endpoint Detection and Response (EDR)[1].

As software updates and antivirus can have a dramatic impact on application performances and functionalities, the goal of this report is to show that specific AV solution have been tested against a set of EVS applications without issue.

WINDOWS UPDATES

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

It is recommended to activate the Windows Update as soon as the server is connected to a network (even with no internet access).

SUPPORTED UPDATE SCENARII

- 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.

[1] In this document, antivirus includes traditional AV solutions but also next generation EDR.

- 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 check the monthly security bulletin produced by EVS to validate Windows patches.
- EVS may refuse a request to apply a patch if it is deemed that it will cause problems with the software

HOW TO DEPLOY UPDATES

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

WSUS is a Windows Server role available in the Windows Server operating systems. It provides a single hub for Windows updates within an organization. WSUS allows companies not only to defer updates but also to selectively approve them, choose when they're delivered, and determine which individual devices or groups of devices receive them.

When you choose WSUS as your source for Windows updates, you use Group Policy to point Windows client devices to the WSUS server for their updates. From there, updates are periodically downloaded to the WSUS server and managed, approved, and deployed through the WSUS administration console or Group Policy, streamlining enterprise update management. *Always validate a patch before deployment!*

ANTIVIRUS SOFTWARE POLICY

Cybersecurity is becoming increasingly important in today's world. The traditional way of working with antivirus solutions is not enough for some customers. This is the reason why EVS decided to offer a new approach to cybersecurity and more precisely on EVS applications.

Due to the evolving nature of cyber threats, EVS applications supports now not only traditional antivirus clients but also next-generation Endpoint Detection and Response (EDR).

The following solutions are officialy supported:

- Windows Defender (recommended)
- Kaspersky Small Office Security Anti-virus
- Crowdstrike Falcon Prevent
- TrendMicro Server Protect
- McAfee EndPoint Security (Adaptive Threat Protection disabled).

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 recommended 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.

RECOMMENDED CONFIGURATION FOR ANTIVIRUS AND EDR SOLUTIONS

ANTI-VIRUS CONFIGURATION FOR MICROSOFT DEFENDER ON WINDOWS 10

With Microsoft Windows 10, to avoid low performance while transferring 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”

ANTI-VIRUS CONFIGURATION FOR KASPERSKY SMALL OFFICE SECURITY

- Settings:
  - Security level: Optimal,
  - Machine learning and signature analysis: Yes,
  - Heuristic analysis: Medium scan,
  - Scan technologies: iSwift: No,
  - iChecker: Yes,
  - Action on threat detection: Disinfect; delete if disinfection fails
- User type: Active user
- Component: Virus Scan

ANTI-VIRUS CONFIGURATION FOR CENTOS

- The following paths are excluded from scan:
  - /opt/evs
  - /var/log/EVSLogs
  - /dev/centos/storage
  - /etc/evs
  - /var/crash

OTHER SETTINGS

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 (outside production hours)

    - 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
- ATP (Advanced Threat Protection) is disabled
- All notifications are saved in logs (no user notification on screen)

Need more information? Visit our website: https://evs.com/services/cyber-security

DISCLAIMER