Recommended Antivirus Configuration

Table of Contents

Recommended Antivirus Configuration

Introduction

Today, computer systems are constantly under siege by various rogue software applications. These programs (viruses, worms, malware, etc.) can cause the computer operation to slow down, expose secure data, damage data, and\or extend through corporate networks. Often, best practices alone cannot always guarantee healthy machines and companies must look toward antivirus software packages for protection.

Antivirus software is often used to help prevent such localized attacks. These applications monitor network transfers, data storage drives, changes to the operating system configuration, and running applications. However, in doing their job, they provide the unfortunate side effect of slowing down the computer system. Antivirus can also cause instability in reliable software applications.

ITW EAE applications, with their need to control machine hardware and handle high speed communication to external devices, can often be affected by antivirus and other software depending on the product, configuration, and system resource requirements.

Though ITW EAE attempts to test our software product under real-world conditions, it is impossible to test against every known antivirus application and configuration. Consequently, we provide this document as a guideline for how to configure antivirus software running on ITW EAE equipment.

Recommended Antivirus Configuration

Auto Scans

Most antivirus applications include the ability to schedule or manually initiate a full computer scan. ITW EAE recommends disabling the auto or scheduled run of this scan and include a manually initiated scan as part of our company's equipment preventive maintenance procedures.

The process of scanning a computer requires extensive hard drive access and CPU time, both of which are required by the ITW EAE applications while running in production environments. ***At no time, should a virus scan be attempted while the machine is running production.***

USB Drives/Devices

Depending on the installed hardware options and your corporate environment, it is best to enable scanning of all local drives including removable drives such as USB hard drives and memory sticks. Often USB memory sticks can be the carrier of malicious software since they tend to be connected to numerous machines in the corporate environment.

Realize that scanning large capacity drives often consumes considerable system resources. It is best to use an alternate machine to scan these devices prior to connecting them to ITW EAE equipment.

ITW EAE recommends that you try and restrict the use of USB devices to times when the machine is not running production.

Auto Updates/Virus Definitions

As with the auto scan feature, enabling this feature during production could cause undesirable effects due to the resource needs of the antivirus software while the ITW EAE software has access. It is recommended that definitions be updated weekly, during the PM cycle, or at machine startup\shutdown to minimize undesirable side effects.

Recommended Antivirus Configuration

Real-Time Scan /Filters /Exceptions

Most Windows based antivirus applications have the ability run in the background, monitoring the file system known in real-time. The purpose is to validate files when they are accessed or created. ITW EAE recommends that this feature be enabled only when the antivirus application supports filters or exceptions to the monitoring. Considerable file access occurs while running ITW EAE equipment in production mode. Since scanning these files would affect system performance, you should enable exceptions to the following directories and registry keys depending on the product.

CAMALOT Dispensers

Folders:

C:\Benchmark	
C:\BenchmarkLogs	
C:\BenchmarkTemp	
C:\CAMFiles	
C:\CAMTemp	
C:\Inspection	
C:\Program Files\CAMALOT	***(Windows XP & 7 32-bit Only)***
C:\Program Files (x86)\CAMALOT	***(Windows 7 64-bit Only)***
C:\Program Files\Speedline	***(Windows XP & 7 32-bit Only)***
C:\Program Files (x86)\Speedline	***(Windows 7 64-bit Only)***
C:\VisionTemp	

Registry Keys:

HKLM\SOFTWARE\Speedline\Benchmark for Dispensers

MPM Printers (for Edison see next section)

Folders:

C:\Benchmark	
C:\BenchmarkLogs	
C:\BenchmarkTemp	
C:\Inspection	
C:\Program Files\Speedline	***(Windows XP Only)***
C:\Program Files (x86)\Speedline	***(Windows 7 64-bit Only)***
C:\VisionTemp	

Registry Keys:

HKLM\SOFTWARE\Speedline\Benchmark for Printers

Recommended Antivirus Configuration

Intueri (Edison Products)
Folders:
C:\MPM
Registry Keys:
HKLM\SOFTWARE\MPM\Intueri

NOTE: Include folders containing Machine Process Programs, Recipes and Data logs in this Folder Exception List.

Desktop Applications/Web Browsing /Email

The computers used in ITW EAE equipment are considered machine controllers and as such are not intended to support the practices of a general-purpose computer configured for internet web browsing, desktop or email applications, unless the application is specifically approved by ITW EAE in conjunction with the operation of the equipment.

Best Practice/Safe Computing

The best approach to maintaining a clean computer environment is to establish a best practice or safe computing policy for your employees.

- Use a dedicated USB memory stick for file transfers and make sure you scan if often. Do not allow operators to use the memory stick to load unknown software or transfer media unrelated to the machine functions. Scan devices before connecting to ITW EAE equipment on a secondary machine with up to date antivirus software.
- Disable screen savers and slideshow applications.
- Develop a backup and recovery process before you need it.
- Keep antivirus definitions up to date on all computers.
- Minimize the amount of software your corporate IT department installs as these can also affect machine performance. Often corporate IT departments will require all networked computers to adhere to their policies and be permitted to run monitoring tools\utilities. Software inventory programs that run in the background can use considerable CPU time and effect machine operation. If such software is required, determine if it can be executed manually during a PM period.