

Configuring Anti-Virus Software on Intellex

Overview

Intellex is a video security system designed and optimized for the Microsoft Windows 2000 platform. It is vulnerable to newly created worms and exploits that attack any of the underlying operating system's previously undocumented flaws. Some administrators may choose to include a virus scanning program such as Symantec Antivirus / McAfee VirusScan / CA Etrust Antivirus, etc.

This document:

- Guides an administrator through a generic configuration for an antivirus program, while trying to reduce the impact on the Intellex's overall performance.
- Presents configuration options for common virus scanners.

Performance Impact

- The Intellex is finely tuned for performance, and any additional software put on the machine will have an impact.
- Intellex handles copious amounts of video (as well as the compression of that video) every second and writes to the hard disk 24 hours a day, 7 days a week.
- Once you install or configure a virus scanning utility, you may find that your Intellex is not performing adequately (lags in the database, slow network performance, etc.). If this is the case, you may need to re-evaluate your virus scanner's configuration or consider removing the virus scanning software altogether.
- Other strategies to protect your system without using a virus scanner are also feasible. These are described later in this document.

Key Features to Disable In Any Virus Scanning Software

Network Drive Monitoring/Scanning

- Scanning a network drive is CPU- and network-intensive, as it must deal with a lot of data through the local network interface to read each file from another system.
- Intellex is often serving Network Client users remotely, so by scanning a network drive, you are flooding the Intellex's subnet with network traffic. Congesting the network will degrade the throughput to the Intellex's clients.
- You should scan the networked drive with another system that is not running Intellex.

Key Features to Modify In Any Virus Scanning Software

- 1 Exclude scanning of file extensions AVI, DAT, NDX, TMP in both real-time and scheduled scans.
 - Intellex maintains a large (> 20 MB) database in a file named MASTER.NDX.
 - Intellex writes its image captures in 20,480 KB files with a filename format of IMGxxxx.AVI.
 - Intellex writes temporary files as CACHExxxx.TMP before it commits to writing an AVI file.
 - Intellex writes TRKxxxx.DAT files to its alarm directory.
 - Any scheduled (or real-time) scanning of these files hampers Intellex performance because these files are so large (> 20 MB).

- Real-time scanning is CPU- and I/O-intensive, just like Intellex. If your virus scanner allows you to exclude the specified extensions, configure it accordingly. However, if your virus software does not allow real-time exclusions based on extensions, you should disable this feature.

2 Set CPU usage to the lowest setting.

Most virus scanners allow you to adjust a scanner's CPU priority. Adjust it as low as possible to avoid competing with Intellex.

Best Practices

- Scan when you do not expect missing video frames to be an issue.

If Intellex does not have the resources to write to the disk or the resources to compress its video data in memory, it may drop video frames. If you must run a virus scanning program, determine a time when losing frames is acceptable.

- Disable any software firewall that is included in your virus scanner.

Software firewalls can be very CPU-intensive and have an adverse effect on both hard disk and network I/O. Since Intellex heavily taxes these resources, NOT installing a software firewall on the Intellex machine is strongly recommended. A hardware firewall sitting between the Intellex and the corporate network is recommended.

Strategies to Reduce Intellex Virus Vulnerabilities Without Installing a Virus Scanner

- Keep Intellex servers or farms on their own subnet with a hardware firewall between them and your corporate network. (A software firewall on the Intellex will affect CPU and network performance.)
- Configure firewalls only to allow inbound and outbound Network Client traffic (default ports are 5000, 5001, and 5003). In addition, enable outbound web traffic only to the Microsoft update sites. Opening other system ports for various administration tasks (SMS/SNMP) is NOT recommended.
- Notify your network administrator to keep the Intellex machine patched with the latest Microsoft Windows updates. American Dynamics routinely reviews these updates. Go to <http://americandynamics.net> for recommendations on which to install and which can be safely ignored. Check for possible updates from another computer on the corporate network, not from the Intellex machine itself. If updates are required, be sure to download them directly from Microsoft.
- Do not use the Intellex for web browsing, E-mail, or anything outside the scope of what it was designed to do. Installing or using third party software that was not shipped with Intellex can lead to performance degradation and compromise the unit's security.
- Do not allow mapping of network drives to or from the Intellex. This reduces performance and exposes the Intellex to attack.
- The server and messenger services are not used by Intellex and are disabled. Enabling these increases vulnerability to attack.

Virus Software Configuration Options

CA Etrust Antivirus

Modify Real-time scanning

- 1 Go to real-time monitor options > selection > regular files.

- 2 Select all except the specified extensions.
- 3 Edit the list, adding TMP, DAT, AVI, and NDX.

Low CPU Usage

- 1 Go to schedule new scan job.
- 2 Click schedule tab, then CPU usage low.

Network Drives

Do not allow any scheduled jobs to scan a network drive.

Exclude File Extensions

- 1 Go to schedule a new scan job, and click selection tab.
- 2 From the regular files section, select all except the specified extensions.
- 3 Edit the list, making sure to include TMP, DAT, AVI and NDX.

Scheduled Scans

Schedule scans only during low usage when losing video frames is not critical.

Norton Antivirus Corporate Edition

Modify Real-time scanning

- 1 Go to configure file system realtime protection > file types > select > extensions.
- 2 Remove TMP, DAT, AVI, and NDX.

Low CPU Usage

On a scheduled scan:

- 1 Select options.
- 2 Set CPU utilization to low.

Network Drives

Do not allow any scheduled jobs to scan a network drive.

Exclude File Extensions

On a scheduled scan:

- 1 From options, select exclusions.
- 2 Select check file for exclusion before scanning.
- 3 Add *.tmp, *.dat, *.avi, *.ndx extensions to the exclusions.

Scheduled Scans

Schedule scans only during low usage when losing video frames is not critical.

McAfee Antivirus

Modify Real-time scanning

- 1 Go to on-access scan properties > all processes > detection > exclusions > by file type.
- 2 Add TMP, DAT, AVI, and NDX.

Low CPU Usage

On a scheduled disk scan, select 10% system utilization.

Network Drives

Do not allow any scheduled jobs to scan a network drive.

Exclude File Extensions

On a scheduled scan:

- 1** From detection, select exclusions.
- 2** Add *.tmp, *.dat, *.avi, *.ndx extensions to the exclusions.

Scheduled Scans

Schedule scans only during low usage when losing video frames is not critical.