Using McAfee VirusScan® Enterprise with Asset Vision Professional

TI-DAT-VirusScanSetup
4-Nov-08

1 INTRODUCTION

1.1 Background

ABB recommends that a virus scanner is used on all Asset Vision Professional installations. McAfee VirusScan® Enterprise has been tested and qualified for this purpose.

This document describes how to configure VirusScan® so that it does not interfere with Asset Vision Professional's operation, and so that the impact on performance and reaction times is negligible.

Asset Vision Professional is subjected to comprehensive verification and quality assurance testing before the release of each version. The configuration settings described in this document have been verified in these tests.

Note that if and when a virus is found in a system, damage may already have been done. For mission critical systems it is therefore even more important to effectively prevent viruses from being introduced into the system than to run frequent virus scans.

The white paper *ABB IS Security Considerations for Automation Systems* (3BSE032547) provides general guidelines on how to protect a system from viruses and other malicious software.

1.2 Scope and software versions

McAfee VirusScan® Enterprise 8.5i has been qualified for use with the following versions of Asset Vision Professional:

- SV 5.0 (named as Asset Master)
- SV 5.0 SP2

Note that a particular installation of Asset Vision Professional may have been complemented with additional software from ABB or from a third party, which may require additional settings. For more information please refer to your ABB contact or to the third party, as relevant.

1.3 Upgrading from McAfee VirusScan® Enterprise 8.0i

When upgrading systems that have previously run with McAfee VirusScan® Enterprise 8.0i configured according to any of the documents 3BSE043205 or 3BSE045374, the "Preserve Settings" install option can be used.

1.4 VirusScan updates

Updated scan engine and virus definition files are tested as part of ABB's monthly Microsoft security update testing. Information about the latest scan engine and virus definition file versions that have been tested in this way is published together with the Microsoft security update test results (see *Microsoft Security Updates Validation Status for IIT System 800xA,* 3BSE041902).

ABB recommends that virus definition files are updated as they become available. However, except as described above, ABB does not specifically test new virus definition file versions.

1.5 Disable during Asset Vision Professional installation

Note that virus scanning must be disabled during installation of Asset Vision Professional software and updates. Refer to the installation guide for the relevant system version.

2 CONFIGURATION SETTINGS

2.1 Overview

McAfee VirusScan® Enterprise can be configured for on-access and on-demand virus scanning.

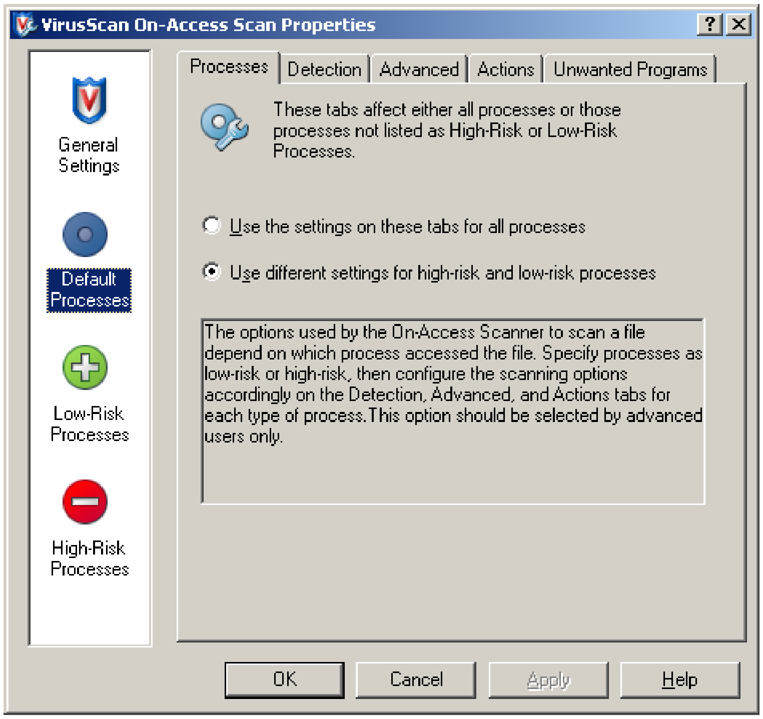
- On-access scanning is automatically activated at system startup and will check files as they are accessed. To prevent this from causing performance degradation, certain folders and files that are frequently accessed need to be excluded from on-access scanning.
- On-demand scanning can be configured to run cyclically at predetermined times or intervals, or be manually initiated. All files that are excluded from on-access scanning should be scanned on-demand at regular intervals. However, since this scanning will impact system performance and reaction times, it should be done when normal system activity is low.

This document describes the specific VirusScan configuration settings that need to be made. All other settings should be left at their defaults.

2.2 On-access scanning

2.2.1 Low and high risk processes

Under the tab “Processes”, select “Use different settings for low and high risk processes”:



These tabs affect either all processes or those processes not listed as High-Risk or Low-Risk Processes.

○ Use the settings on these tabs for all processes

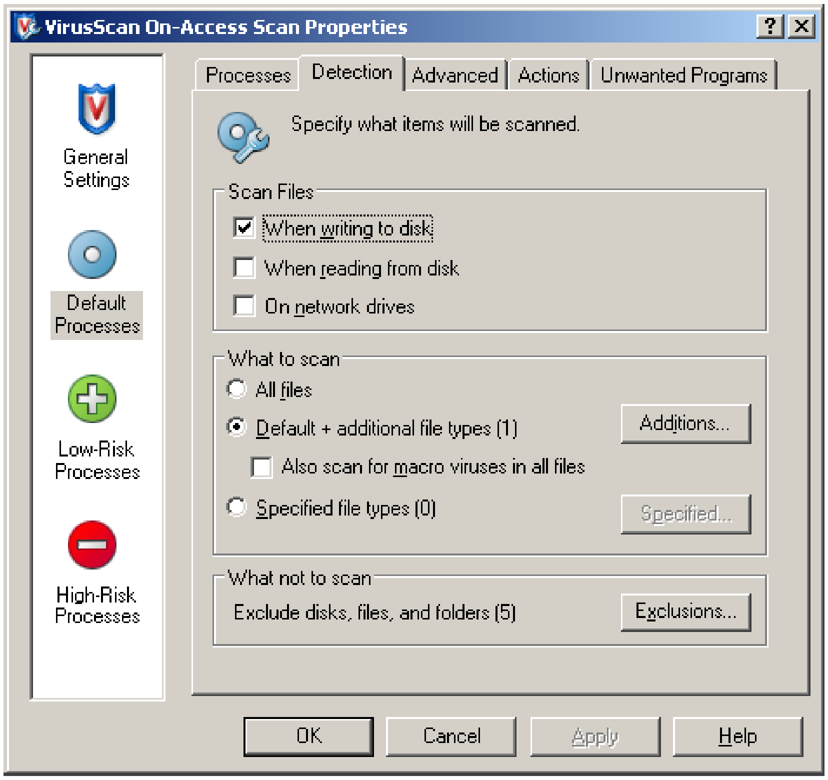
● Use different settings for high-risk and low-risk processes

The options used by the On-Access Scanner to scan a file depend on which process accessed the file. Specify processes as low-risk or high-risk, then configure the scanning options accordingly on the Detection, Advanced, and Actions tabs for each type of process.This option should be selected by advanced users only.

Figure 1 Select different settings for low and high risk processes

2.2.2 Settings for default processes

The settings to be used for default processes are shown in Figure 2.



Specify what items will be scanned.

Scan Files

- ☑ When writing to disk
- □ When reading from disk
- □ On network drives

What to scan

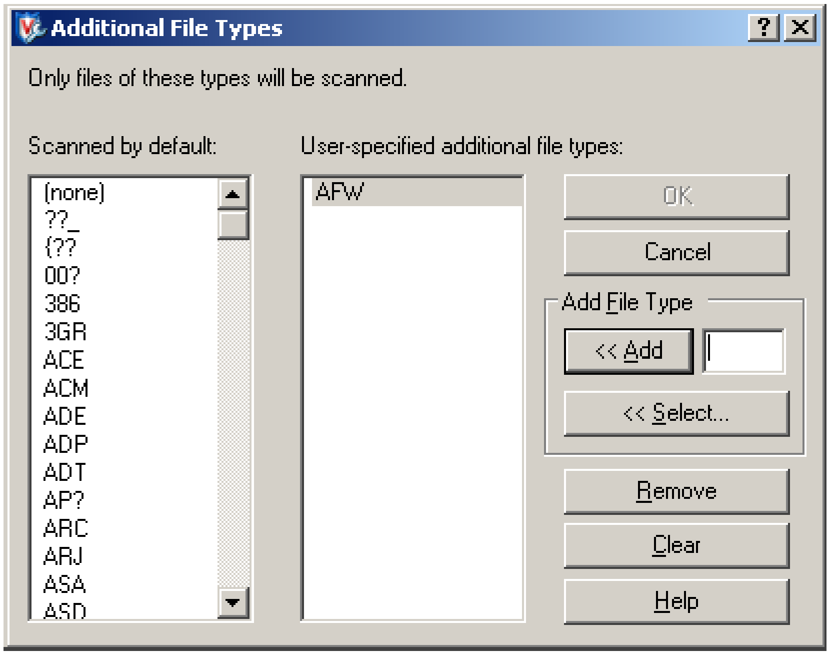
- ○ All files
- ● Default + additional file types (1)
  - □ Also scan for macro viruses in all files
- ○ Specified file types (0)

What not to scan

Exclude disks, files, and folders (5)

Figure 2 Settings for default processes

Click on “Additions …” and add the file type AFW to “User specified additional file types”:



Additional File Types

Only files of these types will be scanned.

Scanned by default:

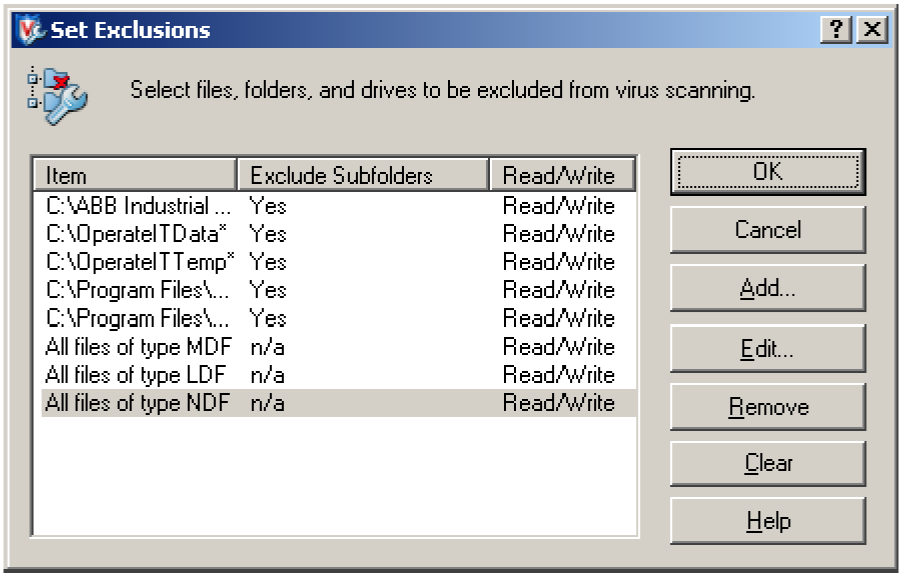
(none)
??_
{??
00?
386
3GR
ACE
ACM
ADE
ADP
ADT
AP?
ARC
ARJ
ASA
ASD

User-specified additional file types:

AFW

Figure 3 Add the file type AFW to the list of user-specified additional file types

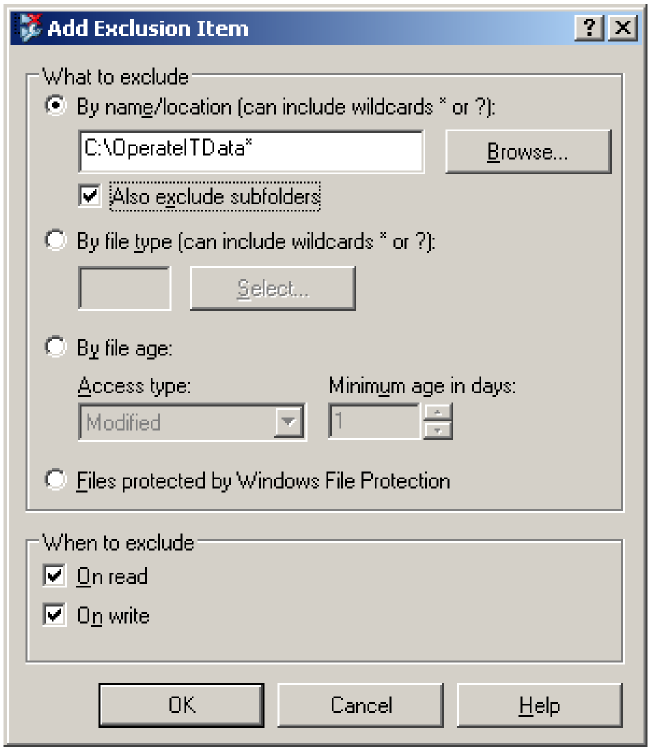
When you click on “Exclusions …” (see Figure 2), a list of the disks, files and folders that are excluded from on-access scanning is presented:


Set Exclusions
Select files, folders, and drives to be excluded from virus scanning.
OK
Cancel
Add...
Edit...
Remove
Clear
Help

Item	Exclude Subfolders	Read/Write
C:\ABB Industrial ...	Yes	Read/Write
C:\OperateITData*	Yes	Read/Write
C:\OperateITTemp*	Yes	Read/Write
C:\Program Files\...	Yes	Read/Write
C:\Program Files\...	Yes	Read/Write
All files of type MDF	n/a	Read/Write
All files of type LDF	n/a	Read/Write
All files of type NDF	n/a	Read/Write

Figure 4 List of folders, files, and file types excluded from on-access scanning

To add items to this list, click on “Add …” and fill in relevant folders, files, and file types as shown in Figure 5. The folders and file types that need to be excluded depend on the Asset Vision Professional version and which products are installed. A list is provided in chapter 3. For each item, select “Also exclude subfolders”, “On read”, and “On write”:



Add Exclusion Item

What to exclude

● By name/location (can include wildcards * or ?):

C:\OperateITData*

☑ Also exclude subfolders

○ By file type (can include wildcards * or ?):

○ By file age:

Access type: Modified

Minimum age in days: 1

○ Files protected by Windows File Protection

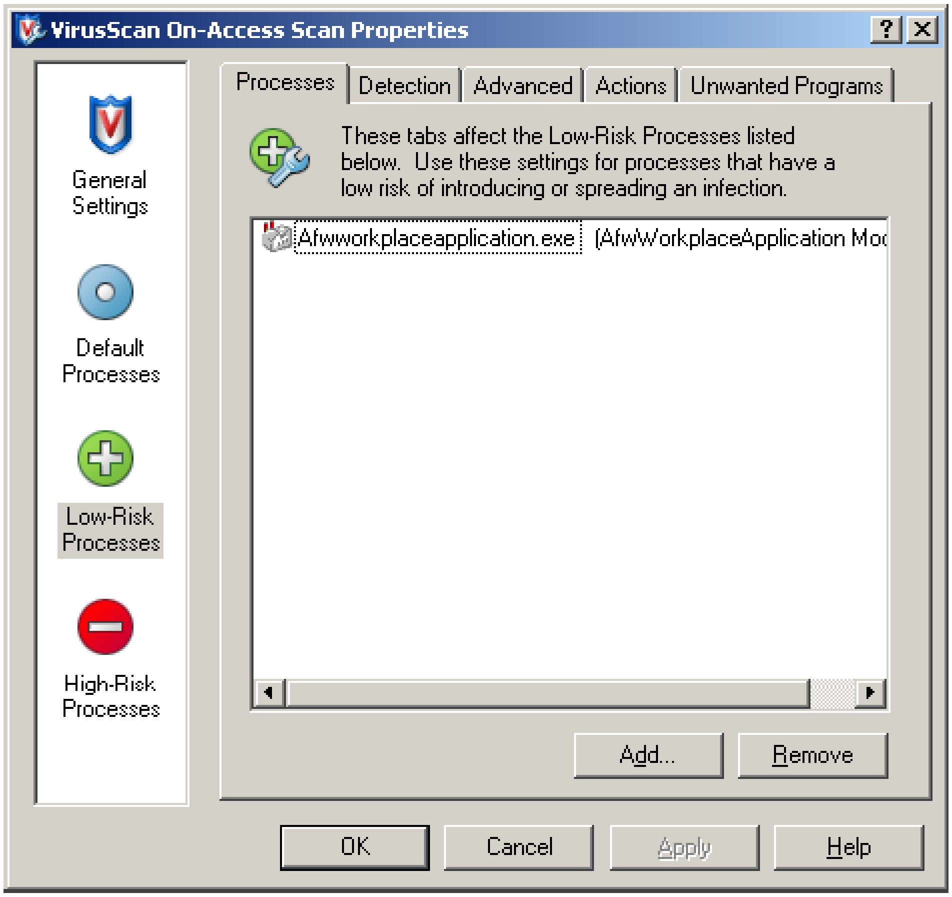
When to exclude

☑ On read

☑ On write

Figure 5 Adding a folder to exclude from on-access scanning

2.2.3 Settings for low risk processes
Add the 800xA system function Afwworkplaceapplication.exe to the list of low risk processes[1]:



These tabs affect the Low-Risk Processes listed below. Use these settings for processes that have a low risk of introducing or spreading an infection.

Afwworkplaceapplication.exe (AfwWorkplaceApplication Moc

Figure 6 Add Afwworkplaceapplication.exe to the list of low risk processes

Apply the same detection settings that were made for default processes also to low risk processes (see Figure 2). Apply the same folder and file type exclusion settings that were made for the default processes (see chapter 3) also to low risk processes. In addition, exclude the following folder:

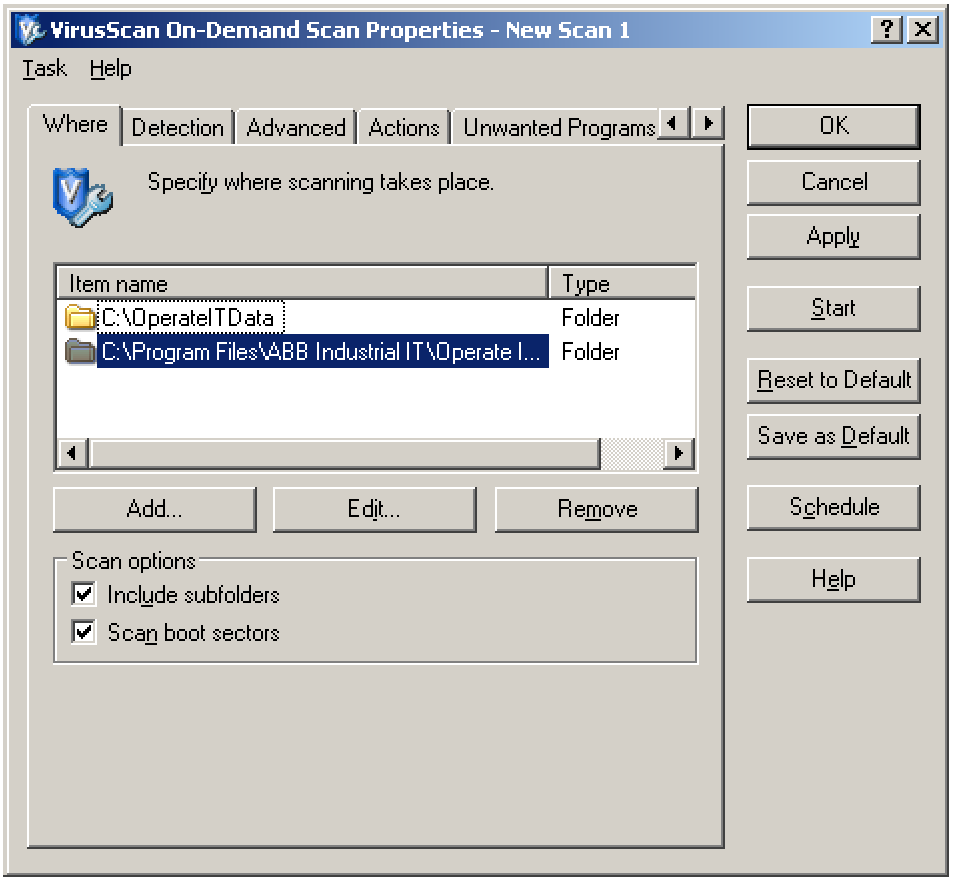
\Program Files\ABB Industrial IT\Operate IT\Process Portal A\bin

[1] Certain low risk processes may already be listed as defaults by McAfee. These can be left as is.

2.3 On-demand scanning

2.3.1 Configuring items to scan

The folders that are excluded from on-access scanning should be scanned regularly, either at scheduled intervals, or manually initiated. Since scanning these folders will impact system performance and reaction times, it should be done when normal system activity is low. In applications where it is not possible to select a regular time when on-demand scanning can be done without disturbing operation of the system, there should be procedures for manually initiating the scanning as often as practical. To configure on-demand scanning, right-click on the VirusScan icon in the system tray.Select “On-Demand Scan”, and click on the tab “Where”:



Specify where scanning takes place.

Item name	Type
C:\OperateITData	Folder
C:\Program Files\ABB Industrial IT\Operate I...	Folder

Scan options

☑ Include subfolders

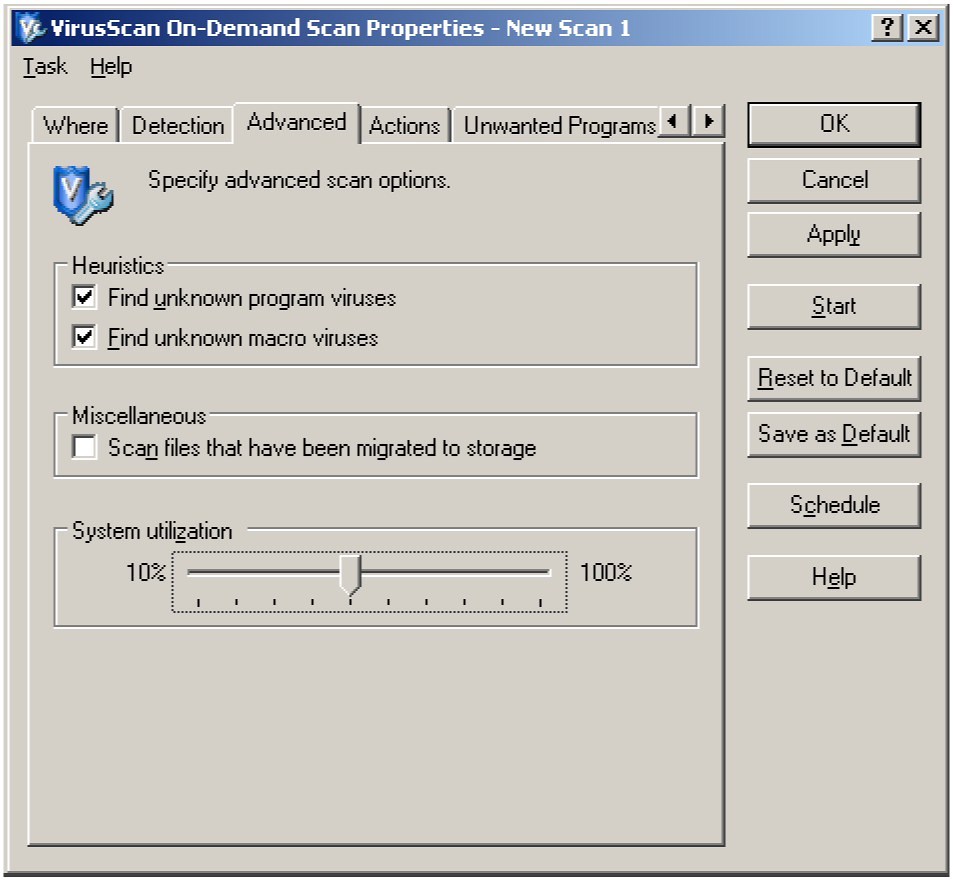
☑ Scan boot sectors

Figure 7 Configuring cyclic scanning

To add items for on-demand scanning, click on “Add”. All items excluded from on-access scanning should be added. Make sure that the scan options “Include subfolders” and “Scan boot sectors” are selected. To specify a schedule, click on “Schedule”.

2.3.2 Limiting the CPU utilization

It is possible to limit the share of available CPU capacity that is utilized by McAfee for on-demand scanning, as shown in Figure 8. After modifying this setting it is wise to run the scan once to ensure that it finishes within an acceptable amount of time.



VirusScan On-Demand Scan Properties - New Scan 1

Specify advanced scan options.

Heuristics

☑ Find unknown program viruses

☑ Find unknown macro viruses

Miscellaneous

☐ Scan files that have been migrated to storage

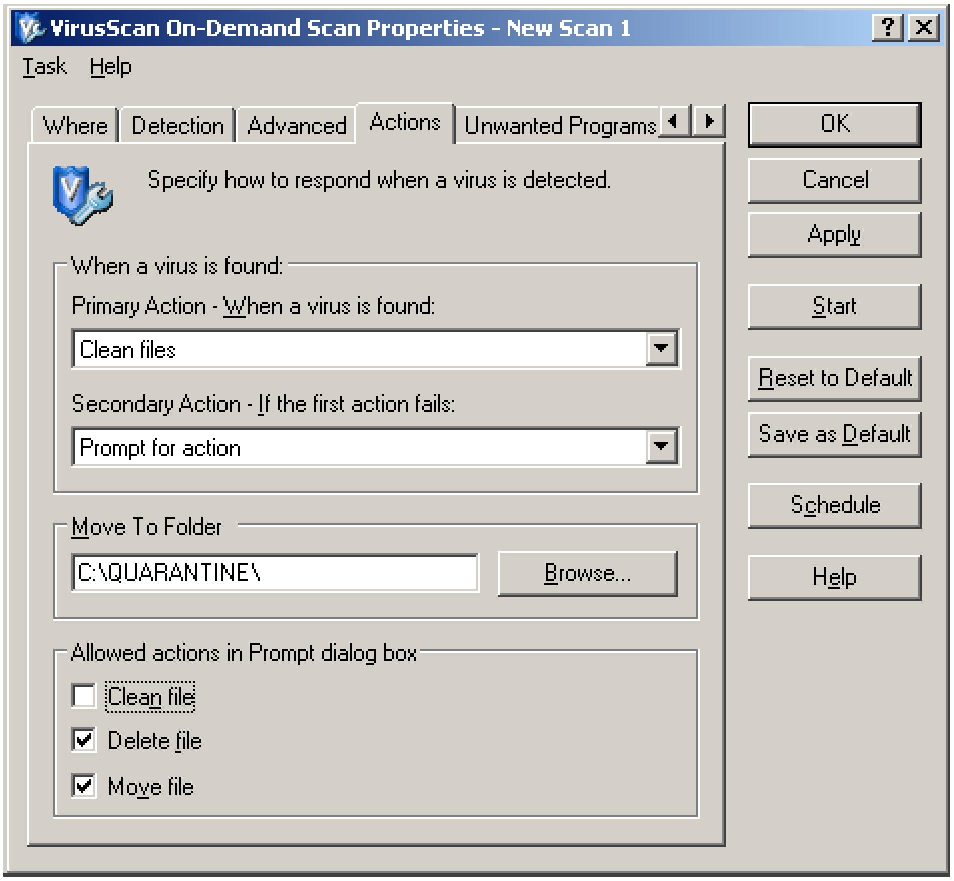
System utilization

10% — 100%

Figure 8 Limiting the CPU utilization

2.4 Handling of infected files

Automatically moving infected files to a separate quarantine folder, which is the default action when McAfee finds an infected file that it can't clean, might lead to system failure. Instead, manual action is required to ensure that the system is stopped in a controlled way. The settings shown in Figure 9 should be used:



Specify how to respond when a virus is detected.

When a virus is found:

Primary Action - When a virus is found: Clean files

Secondary Action - If the first action fails: Prompt for action

Move To Folder: C:\QUARANTINE\

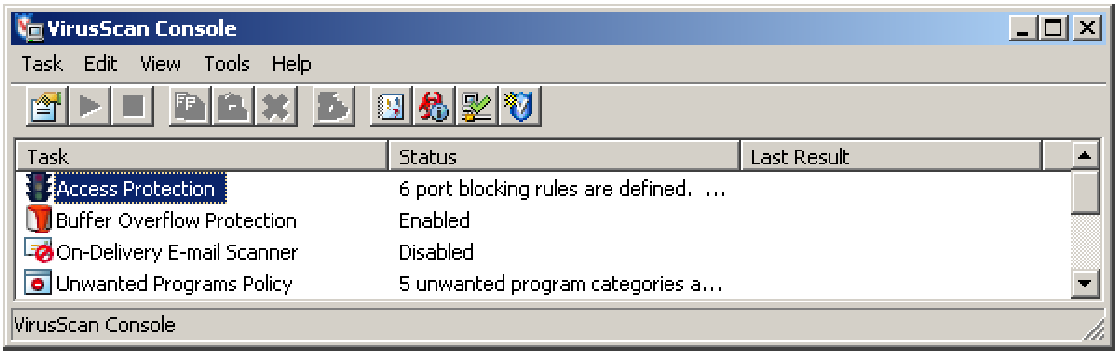
Allowed actions in Prompt dialog box

□ Clean file
☑ Delete file
☑ Move file

Figure 9 Configure the response to detected viruses

2.5 Access protection

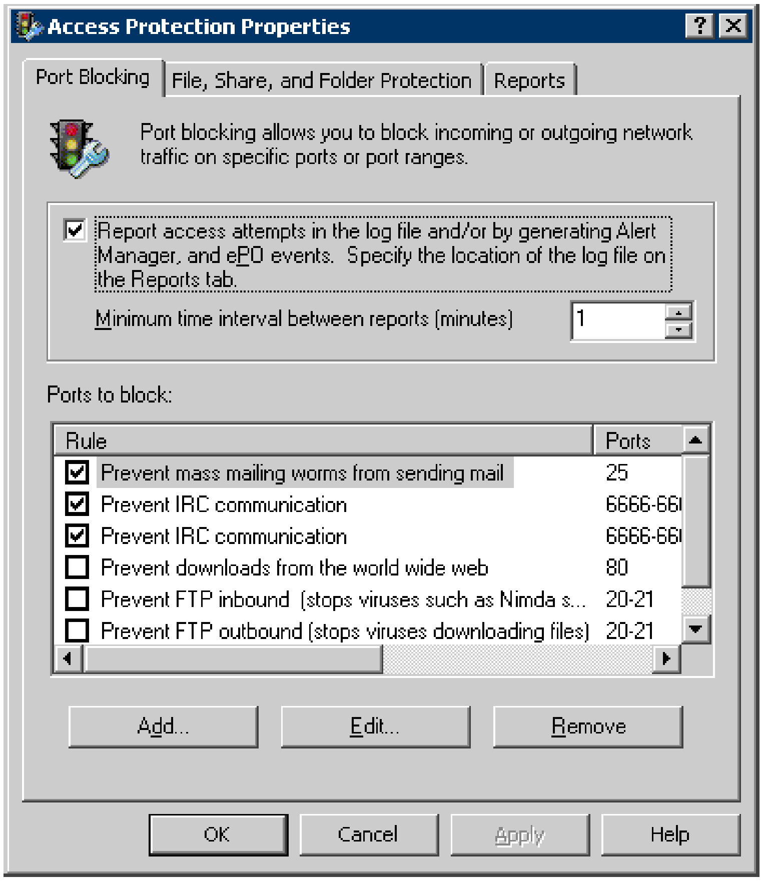
By default, VirusScan Enterprise blocks traffic on port 25, which is used by the SMS & e-mail Messaging function in Asset Vision Professional. In systems where this function is used, the process AdvMsgEngine.exe therefore needs to be added to the Excluded Processes list on the server where the Messenger Service runs (normally the Aspect Server). Open the VirusScan console, right-click on “Access Protection” and select “Properties”:



Task	Status	Last Result
Access Protection	6 port blocking rules are defined. ...	
Buffer Overflow Protection	Enabled	
On-Delivery E-mail Scanner	Disabled	
Unwanted Programs Policy	5 unwanted program categories a...	

Figure 10 VirusScan Console

Select the “Port blocking” tab, then select “Prevent mass mailing worms from sending mail” (Port 25) and click on “Edit…”:


Access Protection Properties
Port Blocking
File, Share, and Folder Protection
Reports
Add...
Edit...
Remove
OK
Cancel
Apply
Help

Port blocking allows you to block incoming or outgoing network traffic on specific ports or port ranges.

☑ Report access attempts in the log file and/or by generating Alert Manager, and ePO events. Specify the location of the log file on the Reports tab.

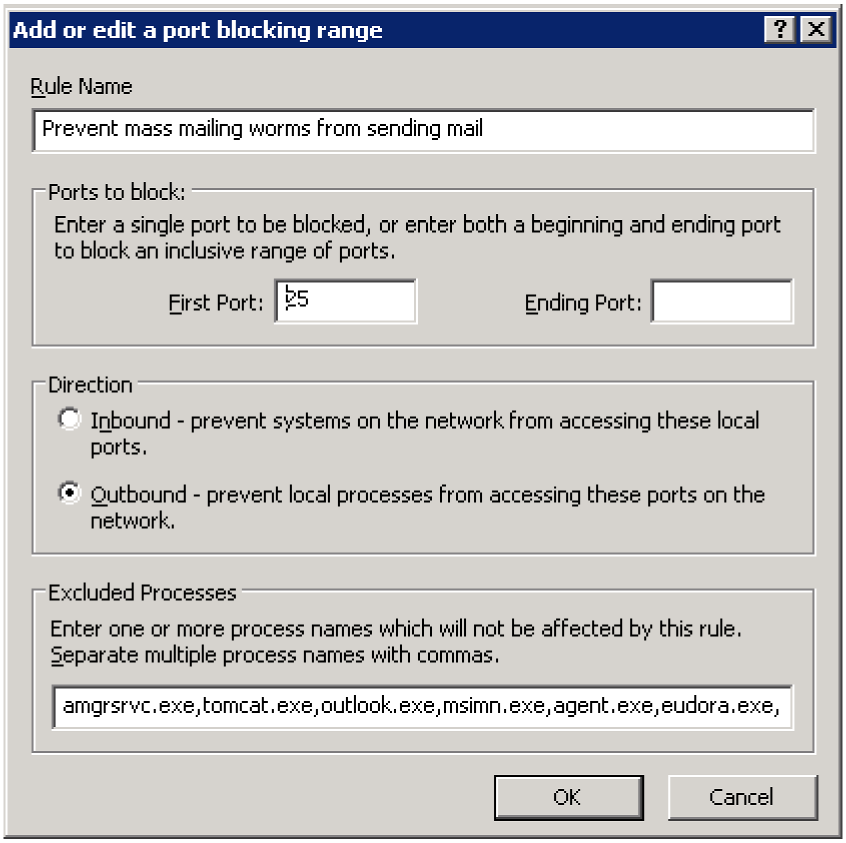
Minimum time interval between reports (minutes) 1

Ports to block:

Rule	Ports
☑ Prevent mass mailing worms from sending mail	25
☑ Prevent IRC communication	6666-66
☑ Prevent IRC communication	6666-66
□ Prevent downloads from the world wide web	80
□ Prevent FTP inbound (stops viruses such as Nimda s...	20-21
□ Prevent FTP outbound (stops viruses downloading files)	20-21

Figure 11 Access protection properties

In the “Excluded Processes” section, add AdvMsgEngine.exe to the list (separated by a comma):



Add or edit a port blocking range

Rule Name

Prevent mass mailing worms from sending mail

Ports to block:

Enter a single port to be blocked, or enter both a beginning and ending port to block an inclusive range of ports.

First Port: 25

Ending Port:

Direction

○ Inbound - prevent systems on the network from accessing these local ports.

● Outbound - prevent local processes from accessing these ports on the network.

Excluded Processes

Enter one or more process names which will not be affected by this rule. Separate multiple process names with commas.

amgrsrvc.exe,tomcat.exe,outlook.exe,msimn.exe,agent.exe,eudora.exe,

Figure 12 Add AdvMsgEngine.exe to the list of excluded processes

Click OK twice, and then close the VirusScan Console. SMS & e-mail Messaging can now send e-mails.

2.6 AutoUpdate

AutoUpdate is a feature that can be used to ensure that the latest McAfee virus definitions are downloaded and installed on every machine. However, this feature requires a direct connection between the automation system network and the Internet.

Enabling AutoUpdate on hosts connected to the automation system network is therefore not a standard practice. For a more secure and reliable deployment of virus definitions, a central management and update deployment host[2] can be set up on a corporate intranet. This allows a system administrator to have control over when updates are made, and an opportunity to test the updates before they are deployed. The white paper “IS Security Considerations for Automation Systems” (3BSE032547) provides general guidelines for how this could be arranged.

3 ITEMS TO BE EXCLUDED FROM ON-ACCESS SCANNING

The folders and file types that need to be excluded from on-access scanning depend on the Asset Vision Professional version.

3.1 Asset Master SV5.0 and Asset Vision Professional SV5.0 SP2

The following directories, files, and file types need to be excluded from on-access scanning:

Path or File Type
\OperateITData*
\OperateITTemp*
\Program Files\ABB Industrial IT\Operate IT\ Process Portal A\App Log\Asset Vision Professional File Types MDF, LDF, NDF
\ABB Industrial IT Data
\Engineer IT Data\Fieldbus Builder PH