Using McAfee VirusScan® Enterprise with System 800xA

Summary

ABB recommends that a virus scanner is used on all System 800xA servers and workplaces. McAfee VirusScan® Enterprise has been tested and qualified for this purpose.

This document describes how to configure VirusScan to ensure that it does not interfere with the 800xA system's operation, and that the impact on performance and reaction times is negligible.

Contents

NOTICE

This document and parts hereof must not be reproduced or copied without written permission from ABB and the contents hereof must not be imparted to a third party nor used for any unauthorized purpose.

The information in this document is subject to change without notice, and should not be construed as a commitment by ABB. ABB provides no warranty, express or implied, for the information contained in this document, and assumes no responsibility for the information contained in this document or for any errors that may appear in this document.

The purpose of this document is to describe certain configuration settings. The described measures are not necessarily complete or effective for all applications and installations.

In no event shall ABB be liable for direct, indirect, special, incidental or consequential damages of any nature or kind arising from the use of this document, nor shall ABB be liable for incidental or consequential damages arising from use of any software or hardware described in this document.

The software described in this document is furnished under a license and may be used, copied, or disclosed only in accordance with the terms of such license.

1 Introduction

1.1 Background

ABB recommends that a virus scanner is used on all System 800xA servers and workplaces. McAfee VirusScan® Enterprise has been tested and qualified for this purpose.

This document describes how to configure VirusScan® such that it does not interfere with the 800xA system's operation, and such that the impact on performance and reaction times is negligible.

System 800xA is subjected to comprehensive verification and quality assurance testing before the release of each system 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 *Security for Industrial Automation and Control Systems* [1] provides general guidelines on how to protect a system from viruses and other malicious software.

It is strongly recommended that you establish a security policy for your System 800xA installation. The policy should include plans for how to recover from disasters such as computer failure or a virus infection.

1.2 Supported Software Versions

McAfee VirusScan® Enterprise 8.8 with Patch 4[1] has been qualified for use with System 800xA version 5.1.

Note that a particular installation of System 800xA 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 VirusScan Updates

McAfee VirusScan patches and scan engine and virus definition file updates are tested as part of ABB's monthly third party security update testing. Information about the latest patch level, scan engine, and virus definition file versions that have been tested in this way is published together with security update test results in the document *System 800xA - Third Party Security Updates Validation Status* [2].

ABB also verifies DAT updates on a daily basis, on the latest version of System 800xA. The results of these tests are published in the document *System 800xA daily verification of McAfee updates* [3]. ABB recommends waiting with updating to a new DAT version until the test result has been published in that document

Note that SuperDAT's should not be used for regular updating of virus definitions, since that may update not only the DAT files, but also the scan engine. A new scan engine version should not be installed until it has been tested by ABB as described above.

1.4 Disable Virus Scanning during System 800xA Installation

Virus scanning must be disabled during installation of System 800xA software and updates. Refer to the installation guide for the relevant system version.

---

[1] Patch 4 requires additional configuration settings compared to earlier versions and patches, see chapter 6.

1.5 Related Documents

1. Security for Industrial Automation and Control Systems, 3BSE032547
2. System 800xA - Third Party Security Updates Validation Status, 3BSE041902
3. System 800xA daily verification of McAfee and Symantec updates, 9ARD107543-002
4. Installing and Configuring McAfee ePO Server with System 800xA, 9ARD107543-005
5. How to choose antivirus software to run on computers that are running SQL Server, http://support.microsoft.com/kb/309422.
6. Virus scanning recommendations for enterprise computers that are running currently supported versions of Windows, http://support.microsoft.com/kb/822158.

2 Installing McAfee Virus Scan Enterprise

To install McAfee VirusScan, double click on SetupVSE.exe and accept any Windows security messages. Select Next to proceed and accept the License terms & conditions.

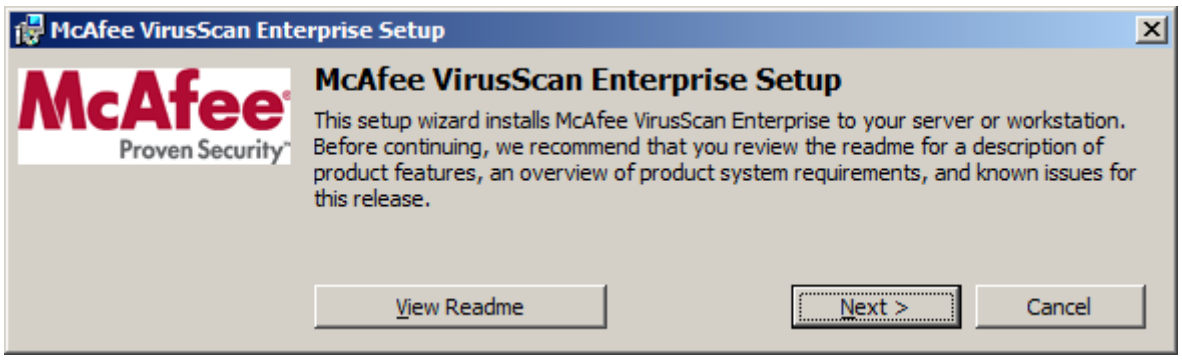

Figure 1 VirusScan setup start screen. Click on Next

Select Setup Type Typical, and click on Next:

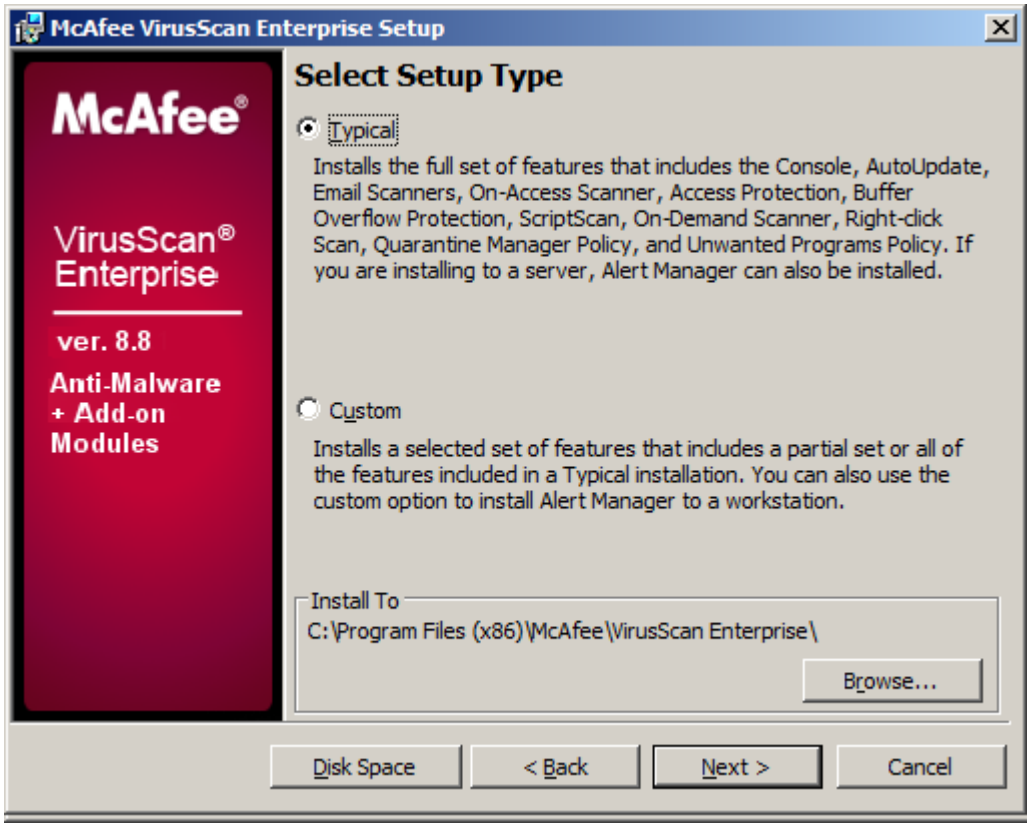

Figure 2 Select setup type Typical

Select Standard Protection for Access Protection Level to avoid conflicts with any 800xA software, and click on Next:

Figure 3 Select standard protection level

Click on Install to complete the installation:

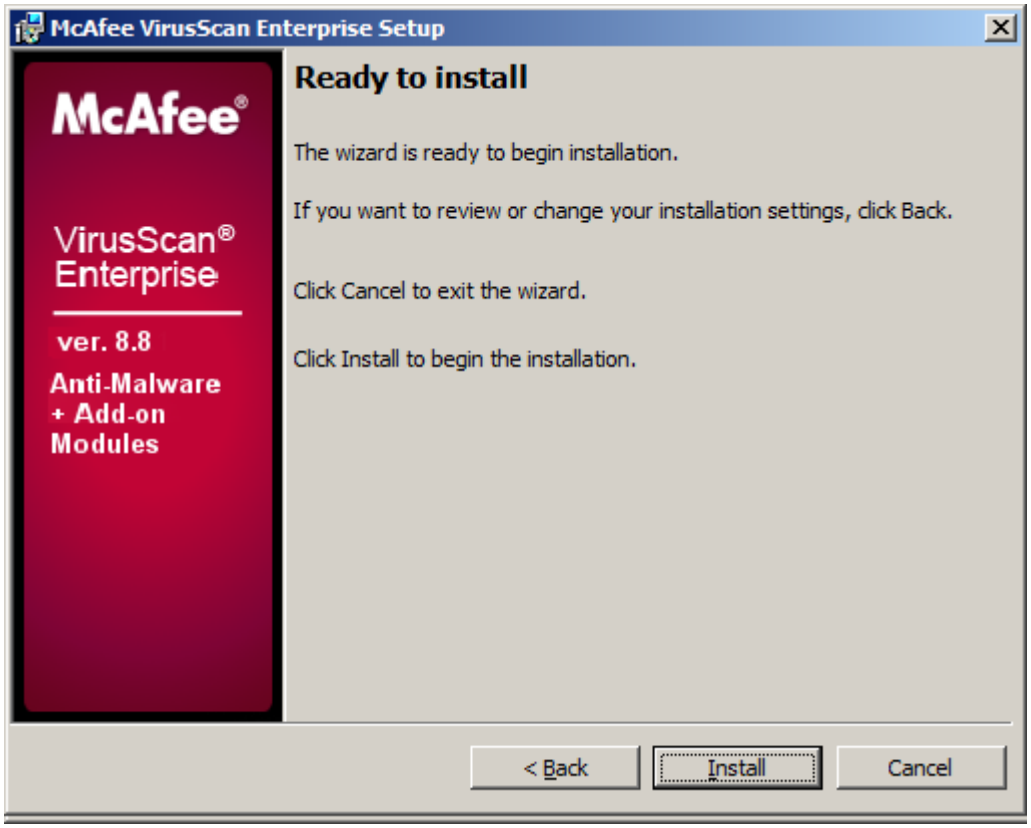

Figure 4 Click on Install to proceed with the installation

Click on Finish and reboot the system to complete the installation.

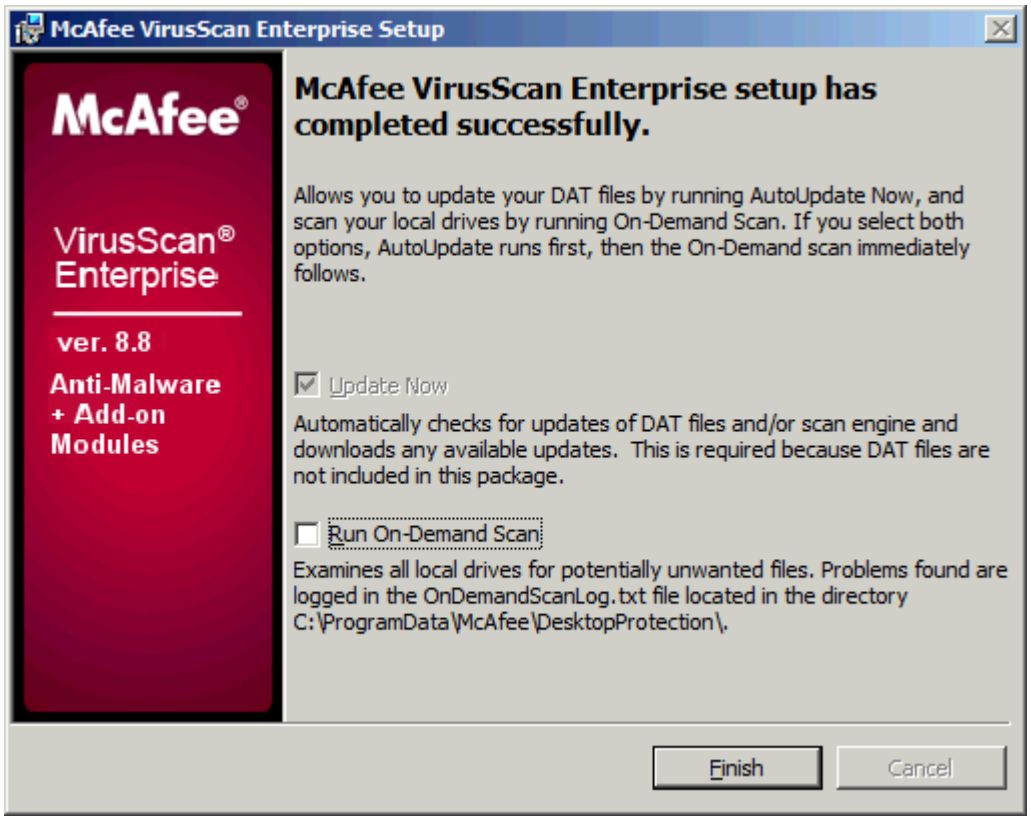

Figure 5 Click on Finnish

3 Configure Virus Scanning

3.1 Overview

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

- On-access scanning is automatically activated at system start-up 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 folders and files (with certain exceptions, see below)) 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.

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

NOTE: Some VirusScan configuration settings may require that the computer is restarted for the changes to take effect. Refer to McAfee's user documentation and help texts.

3.2 On-access Scanning

3.2.1 General Settings

Under the tab “General”, deselect “Processes on enable”.

Under “Heuristic network check for suspicious files”, select “Sensitivity level” Disabled[1].

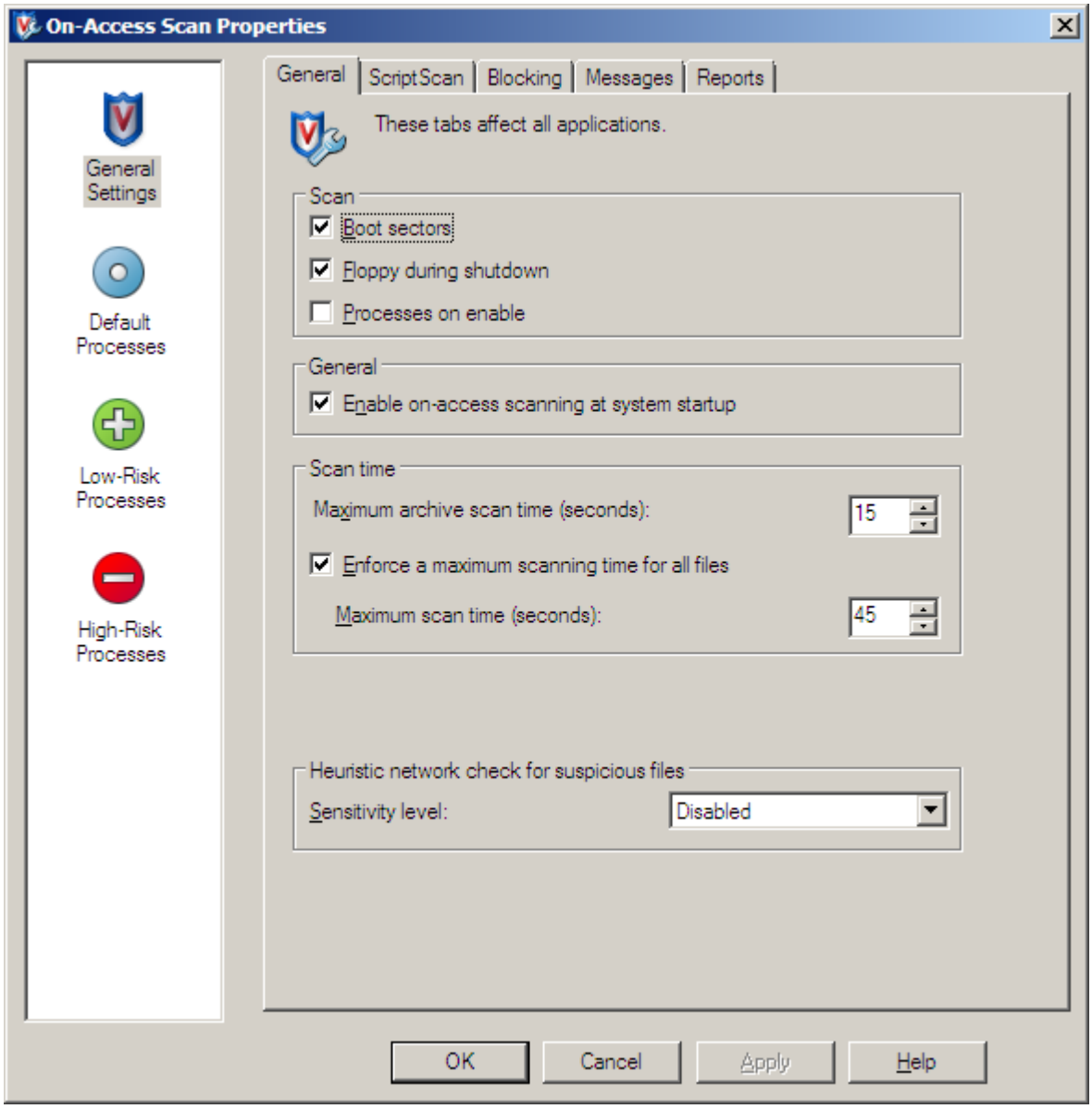

Figure 6 Deselect “Processes on enable” and select suitable maximum scan times

[1] If enabled, when this feature detects a suspicious file it will send a DNS request containing a fingerprint of the suspicious file to McAfee Avert Labs, which then communicates the appropriate action back to VirusScan Enterprise. This behavior may cause problems in an 800xA system.

Under the tab “Messages”, in “Actions available to user”, clear the selection in “Delete files” check box

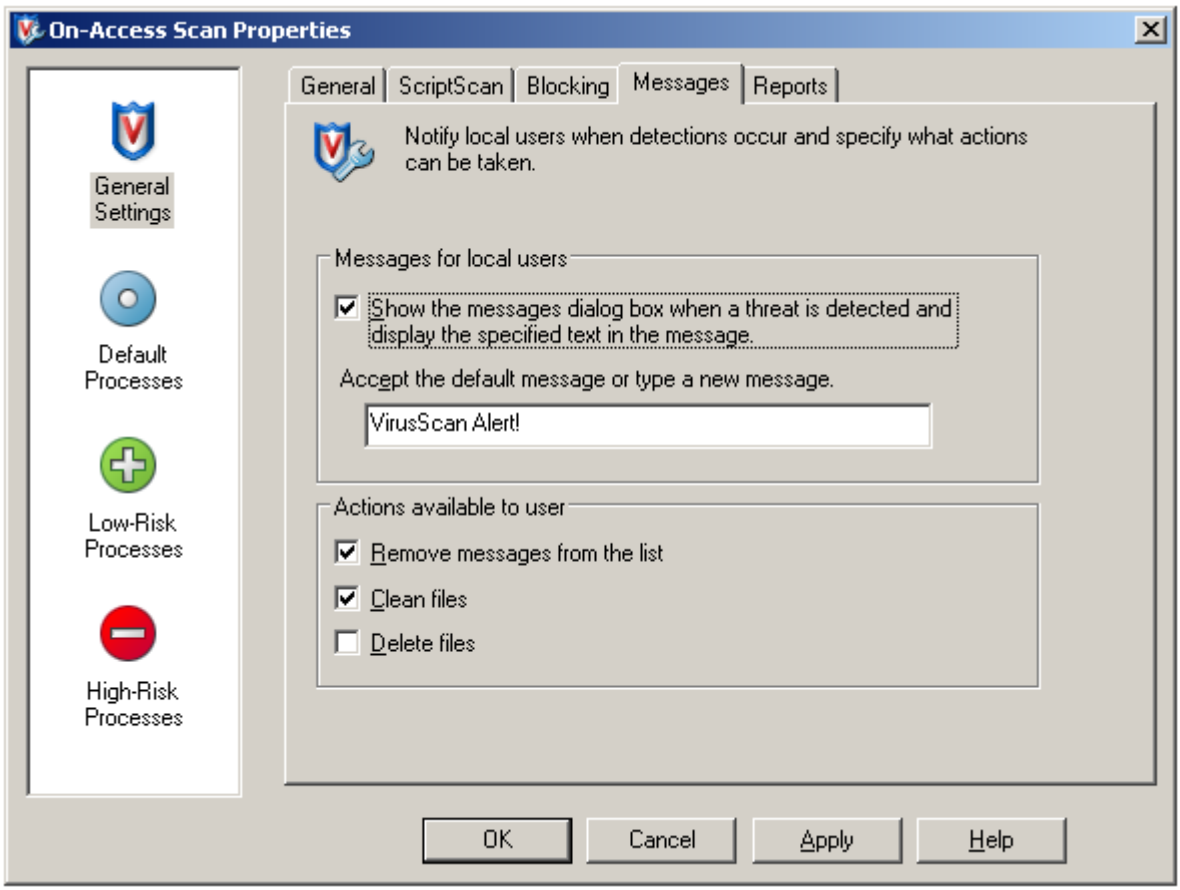

Figure 7 Deselect “Delete files” from “Actions available to user”.

3.2.2 Settings for Default Processes

Under the tab “Processes” select “Configure different settings for high-risk, low-risk, and default Processes”:

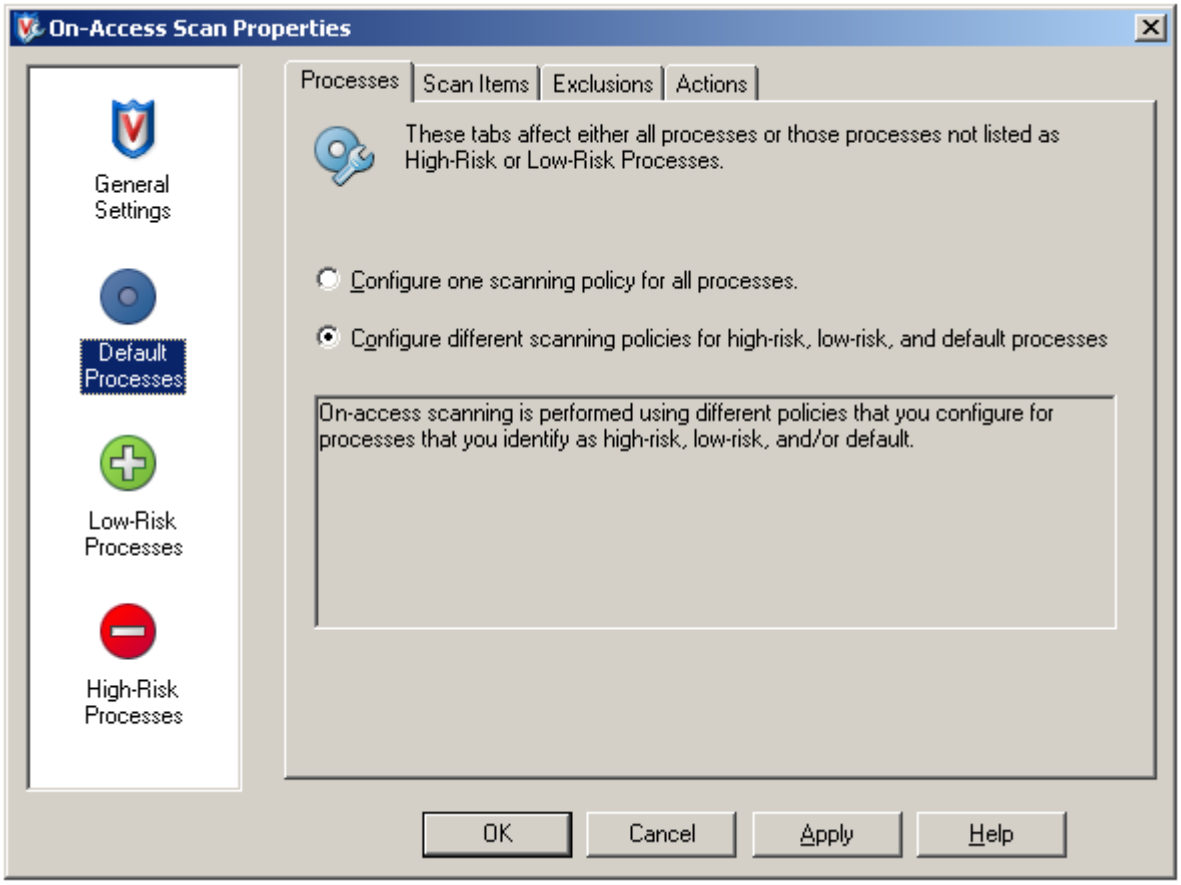

Figure 8 Select “Configure different settings for high-risk, low-risk, and default Processes”

The settings for default processes are shown in Figure 9.

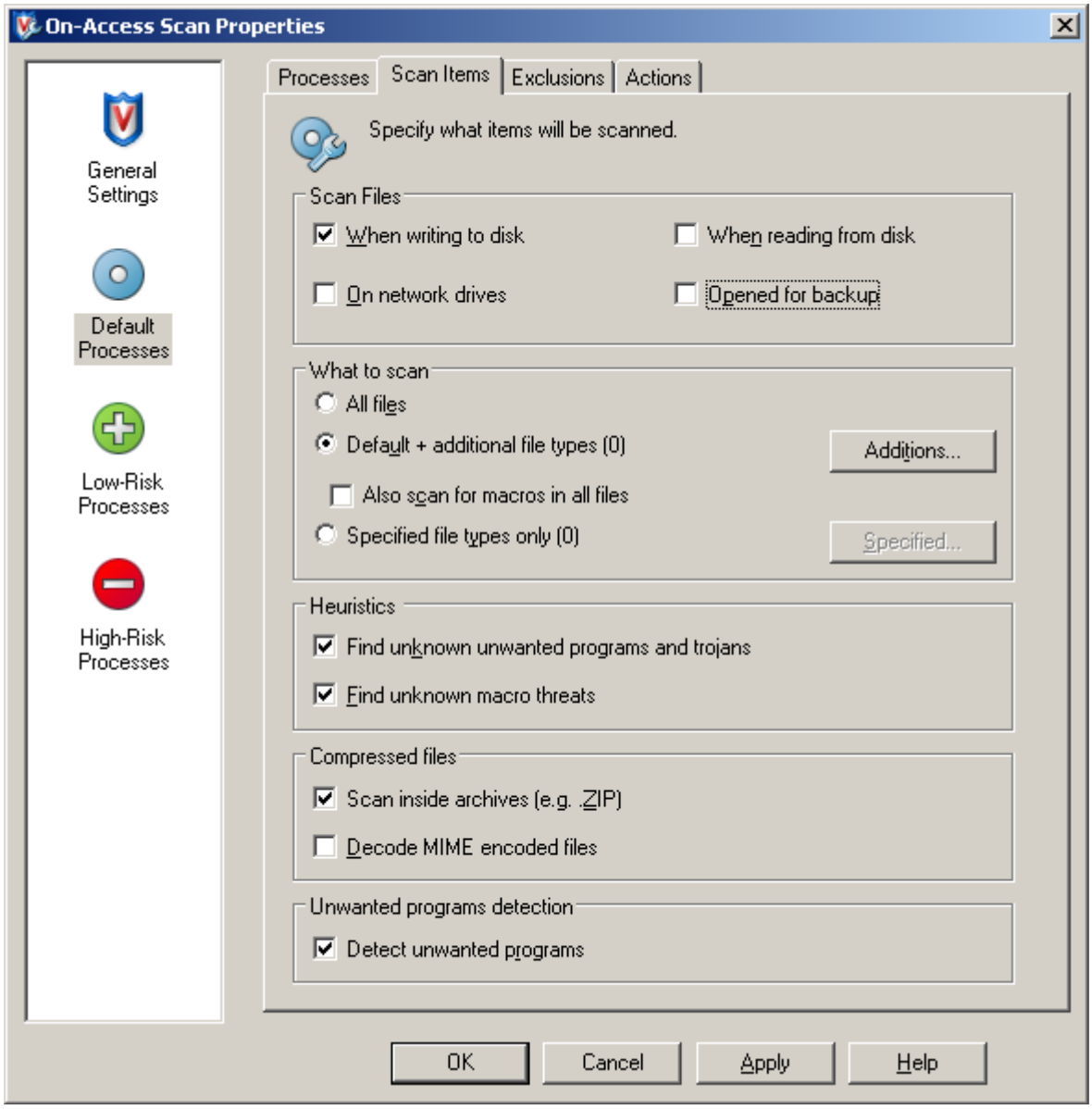

Figure 9 Settings for default processes

Click “Additions” and add the file type AFW to “User specified additional file types”, see Figure 10.

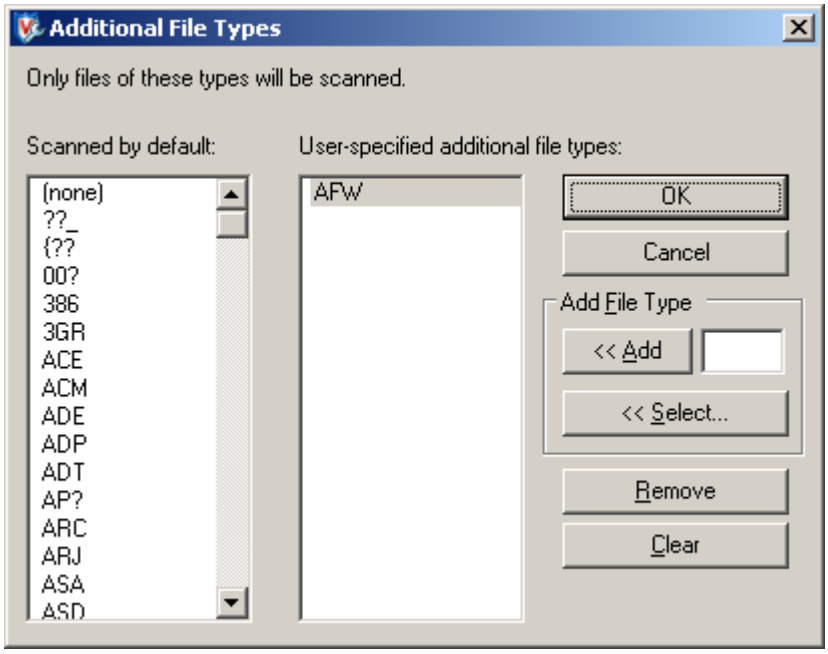

Figure 10 Add the file type AFW to the list of user-specified additional file types

Click OK, then select the tab “Exclusions”, and click “Exclusions”. A list of disks, files and folders that are excluded from on-access scanning is displayed.

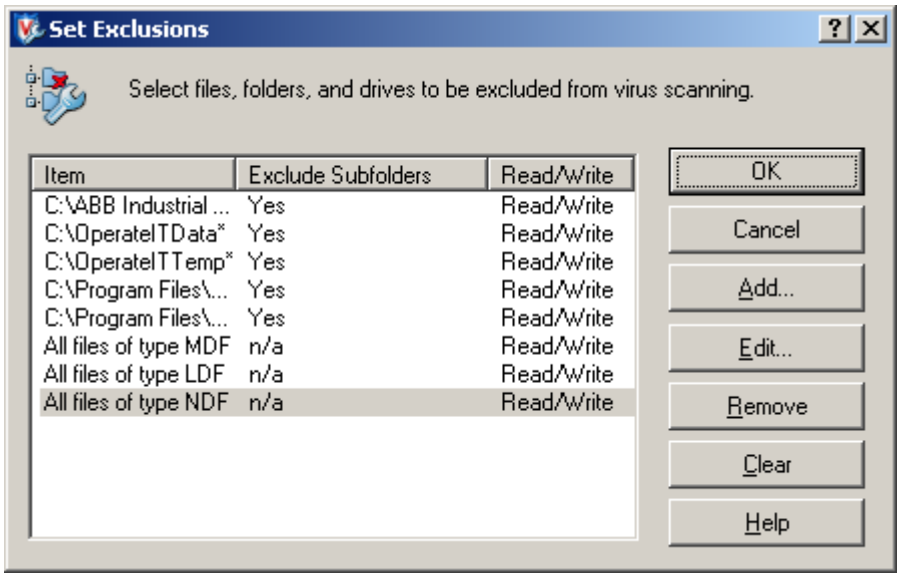

Figure 11 List of folders, files, and file types excluded from on-access scanning. See chapter 9 for information on what items to exclude.

To add items to this list, click “Add” and fill in relevant folders, files, and file types as shown in Figure 12. The items that need to be excluded depend on the 800xA system version and which 800xA products are installed, see chapter 9.

The file types LDF, MDF, and NDF are related to SQL Server and should be excluded from scanning. Scanning these files may under certain circumstances cause a deadlock, see Microsoft KB309422 [5].

For each item that is added, select “Also exclude subfolders”, “On read”, and “On write”, as shown in Figure 12.

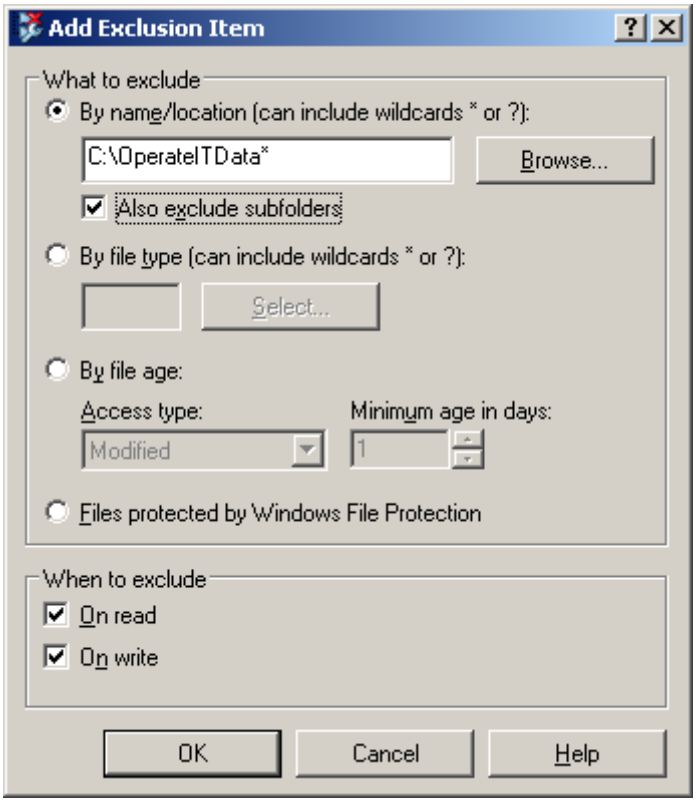

Figure 12 Adding an item to exclude from on-access scanning

Select the tab “Actions” and do the settings shown in Figure 13:

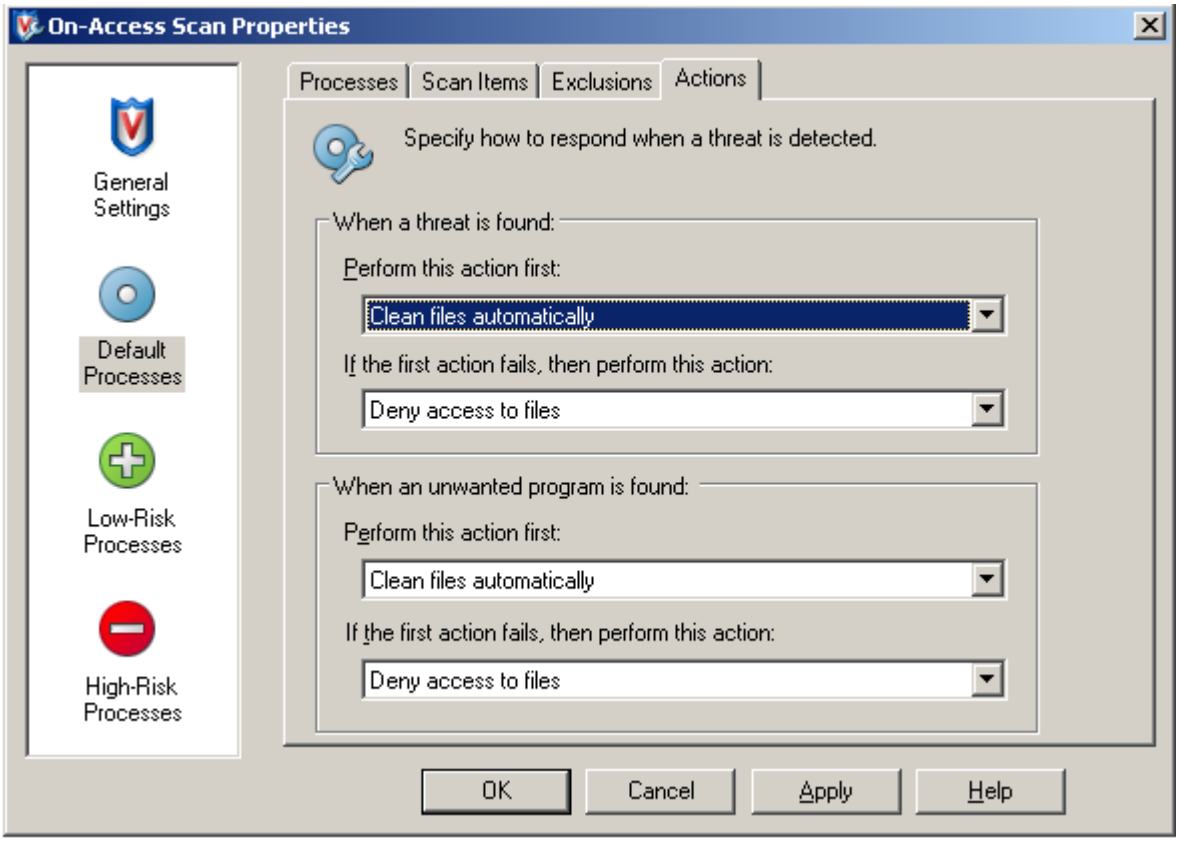

Figure 13 Action settings for On-Access scanning

3.2.3 Settings for Low Risk Processes

Add the 800xA system function Afwworkplaceapplication.exe to the list of low risk processes. Certain low risk processes may already be listed as defaults by McAfee. These can be left as is.

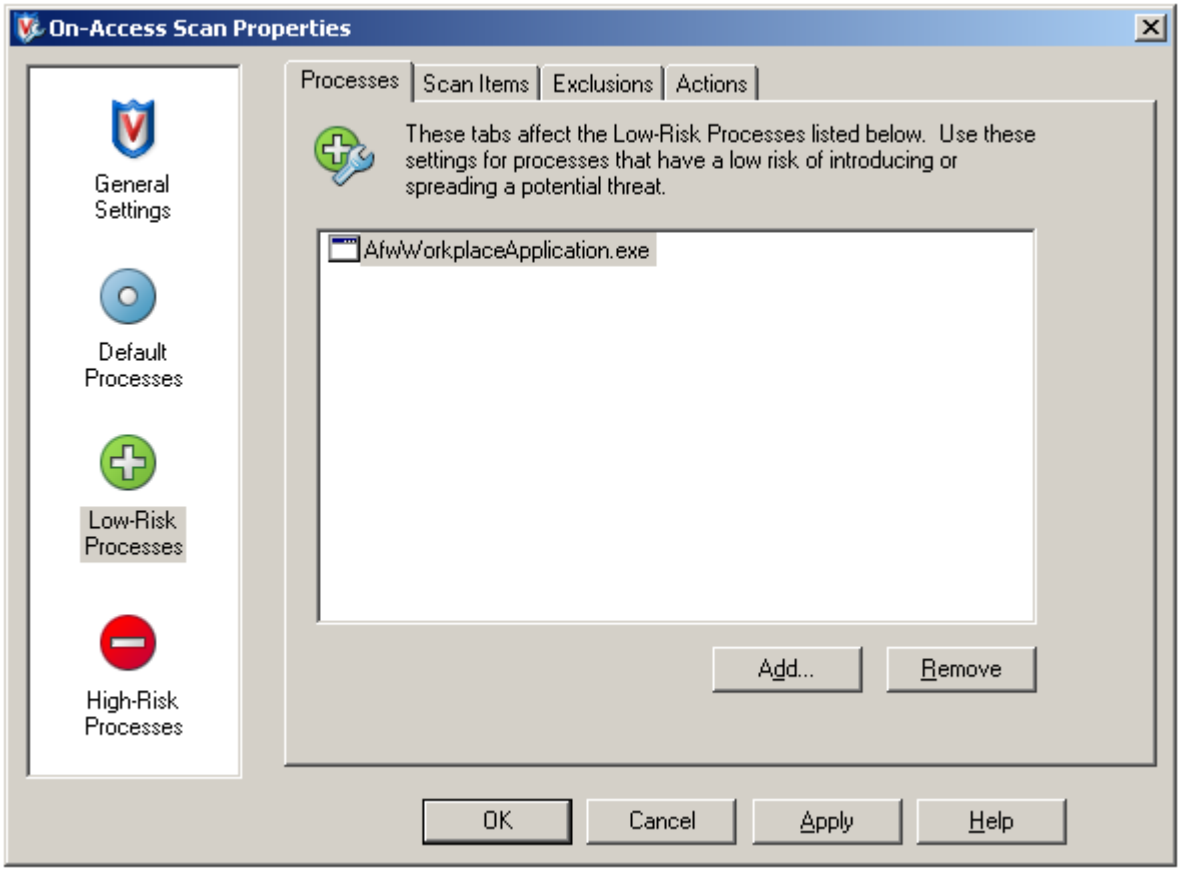

Figure 14 Add Afwworkplaceapplication.exe to the list of low risk processes

Select the tab “Scan Items” and apply the same settings that were done for default processes also to low risk processes (see Figure 9).

Select the tab “Exclusions”, click “Add”, and fill in relevant folders, files, and file types. The items that need to be excluded depend on the 800xA system version and which 800xA products are installed, see chapter 9.

The file types LDF, MDF, and NDF are related to SQL Server and should be excluded from scanning. Scanning these files may under certain circumstances cause a deadlock, see Microsoft KB309422 [5].

Select the tab “Actions” and apply the same settings that were done for default processes also to low risk processes.

3.2.4 Settings for High risk processes

Apply the same “Scan Items” settings that were done for default processes also to high risk processes (see Figure 9).

Select the tab “Exclusions” and apply the same settings that were done for the default processes also to high risk processes.

Select the tab “Actions” and apply the same settings that were done for default processes also to high risk processes.

3.3 On-demand Scanning

All folders and files should be scanned regularly, either at scheduled intervals or manually initiated, also those that are excluded from on-access scanning (with certain exceptions, see below). Note that this scanning will impact system performance and reaction times. It should therefore 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 the VirusScan icon in the system tray. Select “On-Demand Scan”, and click the tab “Scan Locations”:

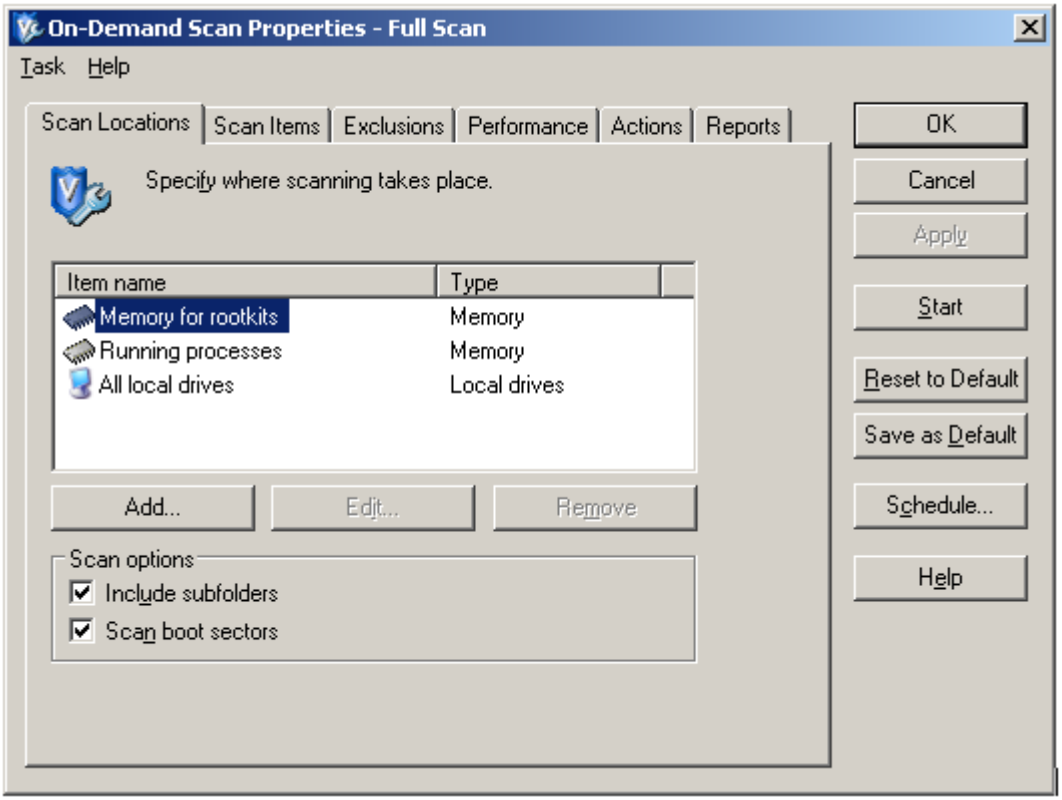

Figure 15 Configuring on-demand scanning (Note: the figure does not necessarily show all files that need to be included, see below)

The default setting for on-demand scanning is to include all local drives. To remove locations, click “Remove”, to add items, click on “Add”.

NOTE: All local folders and files should be covered by on-demand scanning, also those that are excluded from on-access scanning (except file types MDF, LDF, and NDF, see below).

Ensure that the scan options “Include subfolders” and “Scan boot sectors” are selected.

To specify a schedule, click “Schedule”.

Select the tab “Scan Items” and make the selections shown in Figure 16:

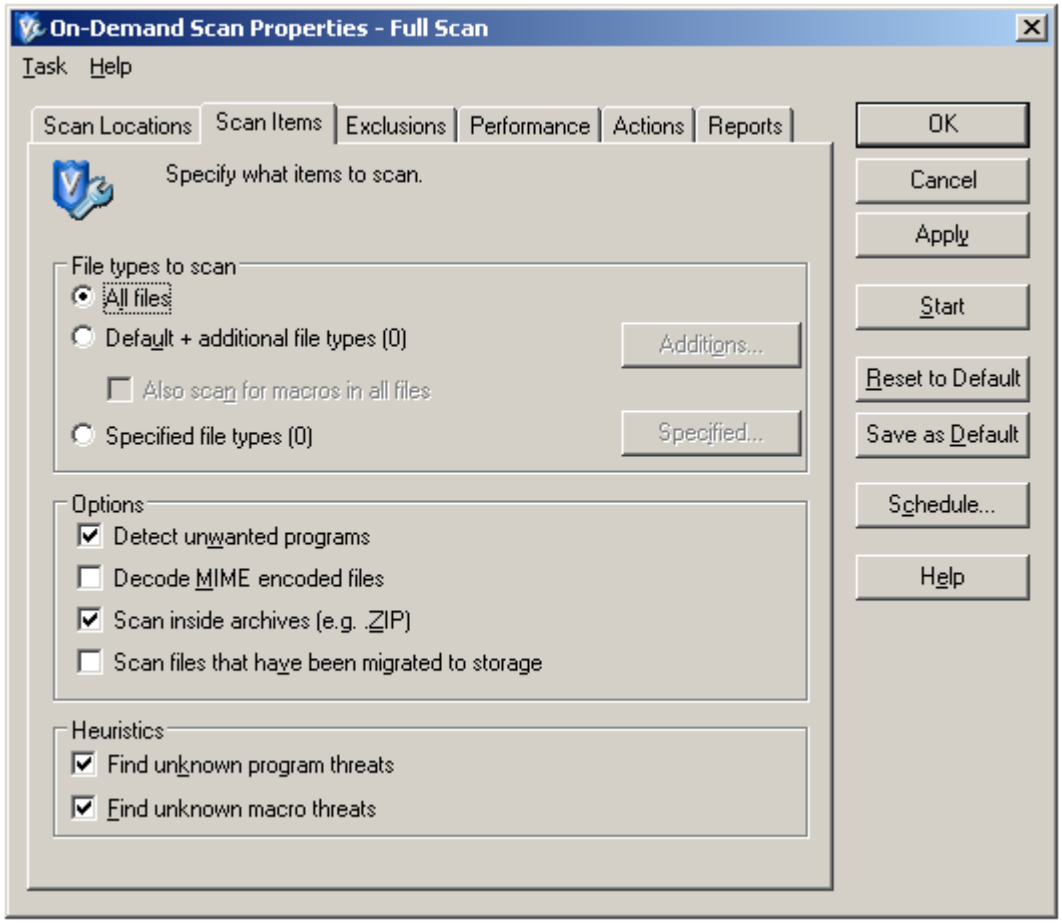

Figure 16 Scan Items settings for On-Demand scanning

Select the tab “Exclusions”, click “Exclusions …” and add the file types LDF, MDF, and NDF. These file types are related to SQL Server and should be excluded also from on-demand scanning. Scanning these files may under certain circumstances cause a deadlock, see Microsoft KB309422 [5].

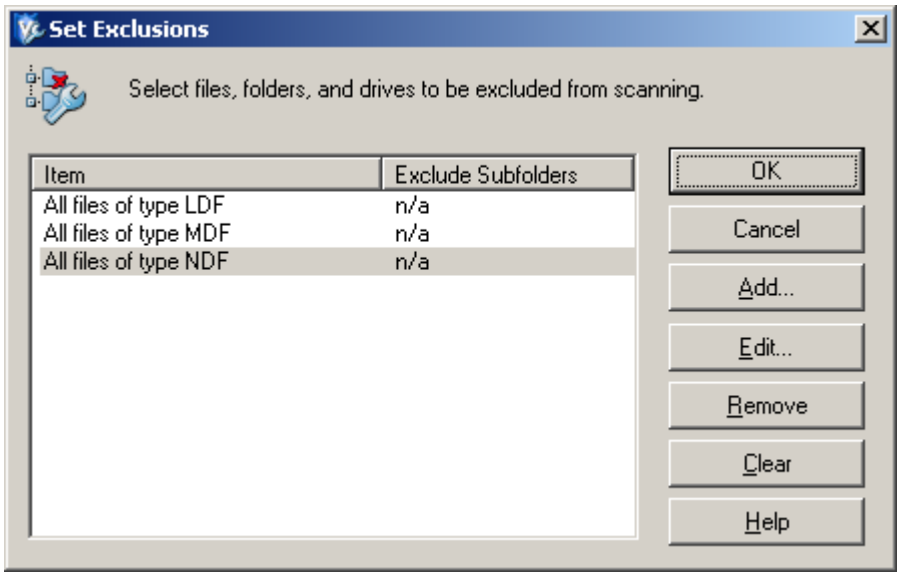

Figure 17 Exclude file types LDF, MDF, and NDF

Select the tab “Performance” to limit the performance impact from on-demand scanning, as shown in Figure 18.

NOTE: The optimal value for this setting is installation specific and depends on many factors, including the system configuration and load, the application, and the operating conditions during the on-demand scanning. The value shown in Figure 18 is intended as guidance only. Try out a value that allows the scanning to finish within an acceptable amount of time while keeping the impact on system performance and reaction times at a level that is tolerable.

Under “Heuristic network check for suspicious files”, select “Sensitivity level” Disabled [1].

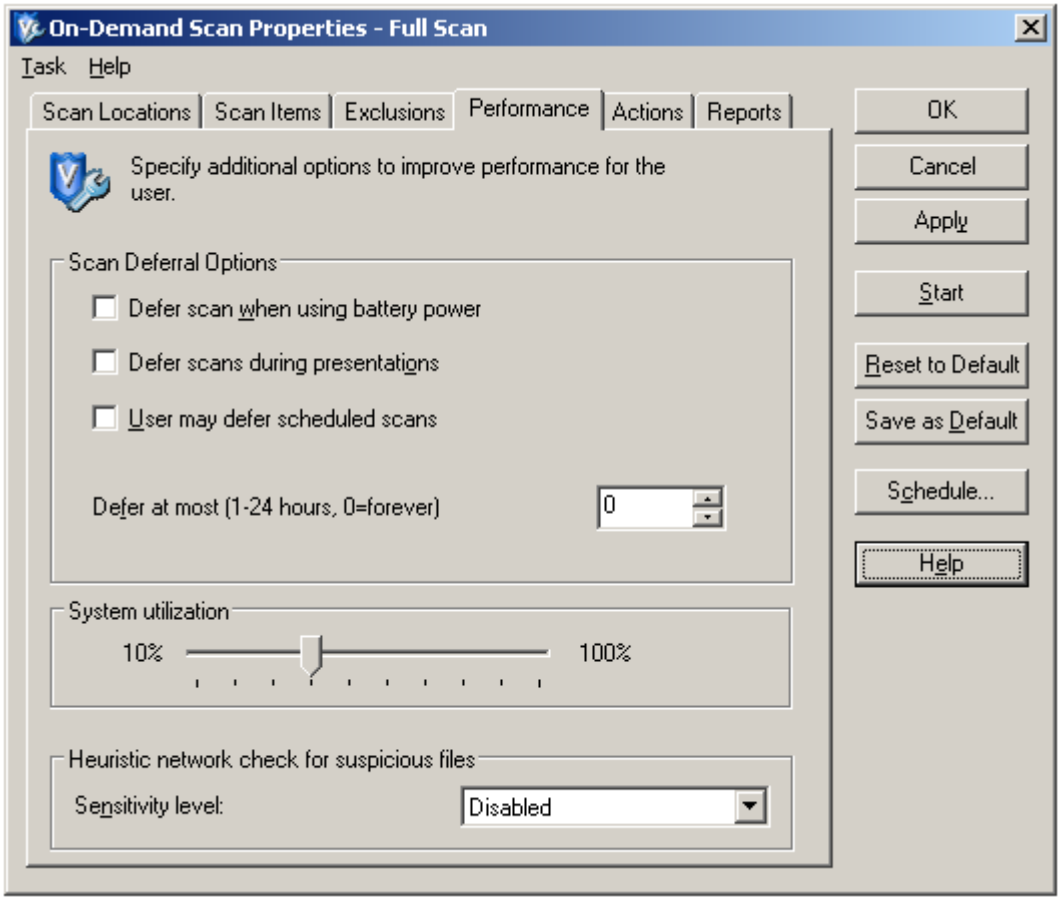

Figure 18 Limiting the CPU utilization

[1] If enabled, when this feature detects a suspicious file it will send a DNS request containing a fingerprint of the suspicious file to McAfee Avert Labs, which then communicates the appropriate action back to VirusScan Enterprise 8.7i. This behavior may cause problems in an 800xA system.

Select the tab “Actions” and make the settings shown in Figure 19:

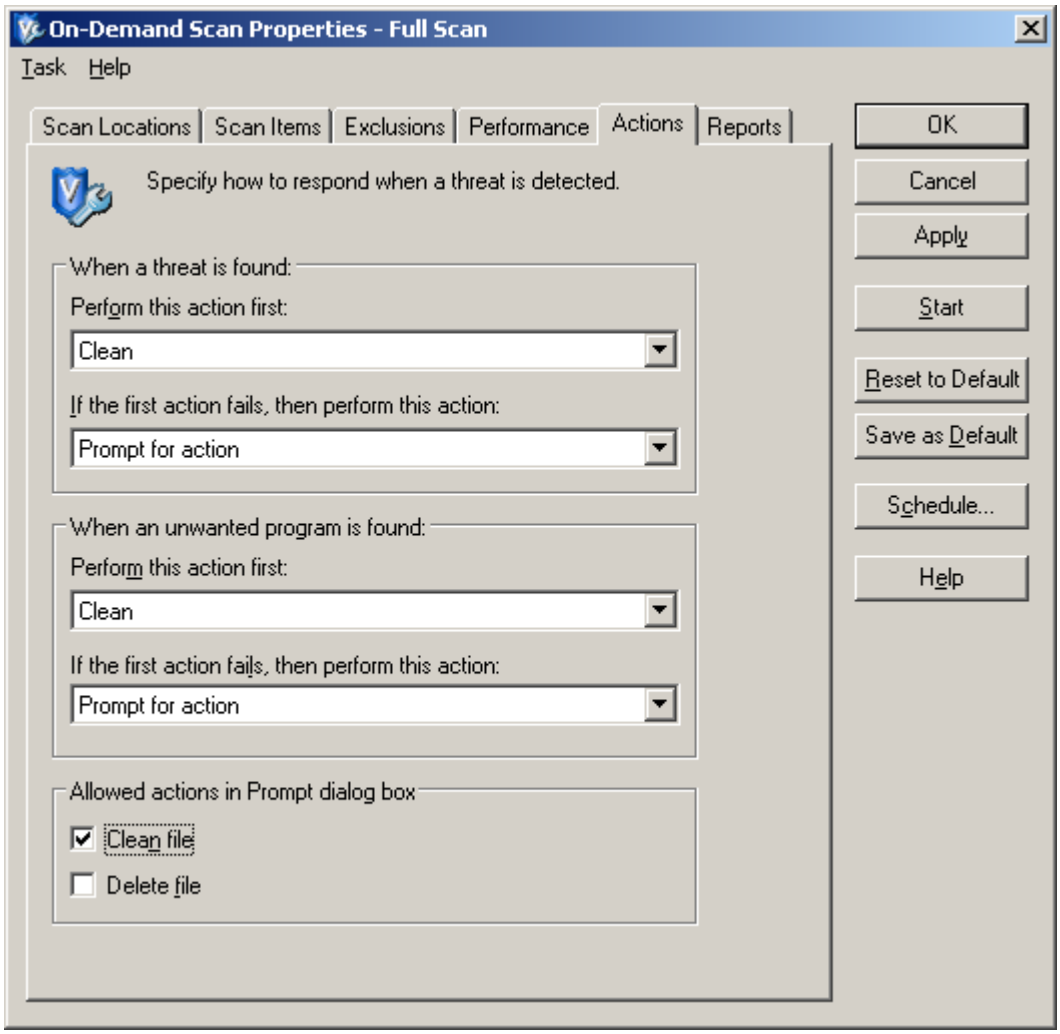

Figure 19 Action settings for On-Demand scanning

3.4 Additional Settings for Windows Domain Controller

In order to avoid serious performance problems due to file locking, McAfee and Microsoft provide recommendations regarding exclusions for computers that run the Windows Server domain controller. In an 800xA system this applies to Domain Servers or, in configurations where Aspect and Domain Server functions are combined in the same server, to Aspect Servers. The exclusions need to be made for on-demand as well as on-access scanning. For information about recommended exclusions, please refer to the Microsoft knowledge base article KB822158 [6].

4 Recovery from a Virus Infection

The security policy for the 800xA installation should include procedures for recovery from a virus infection, and these procedures should be well known by all operating personnel.

On-demand scanning includes 800xA system files. Automatically deleting or moving these files could lead to system malfunction or failure. Instead, manual action is required as described below.

There is no simple way to determine which files can be safely moved or deleted without causing problems in the 800xA system. Hence, if VirusScan reports an infected file that can't be cleaned, the following procedure is recommended:

1. If the infected node is critical for the operation of the system, stop the system in a controlled way. Nodes that are critical should be clearly identified in the security policy (examples are non-redundant Aspect or Connectivity Servers, however, this is highly application dependent).
2. Disconnect the infected node from all networks.
3. Restore the infected node from a disk image if available, or re-install from scratch (see "Node Replacement" in the user manual "Maintenance").
4. Run a complete virus scan to verify that the node is no longer infected.
5. Reconnect the node to the network and restart it.

Note that if a virus is found on one node, it is likely that also other nodes are infected. An on-demand scanning of all nodes is therefore recommended.

5 Configure Access Protection

By default, VirusScan Enterprise blocks traffic on port 25, which is used by the SMS & e-mail Messaging function in System 800xA. 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”:

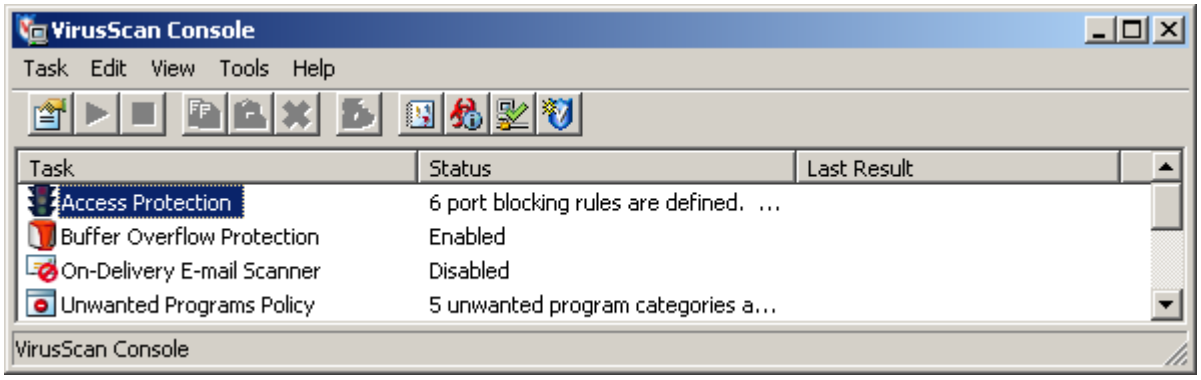

Figure 20 VirusScan Console

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

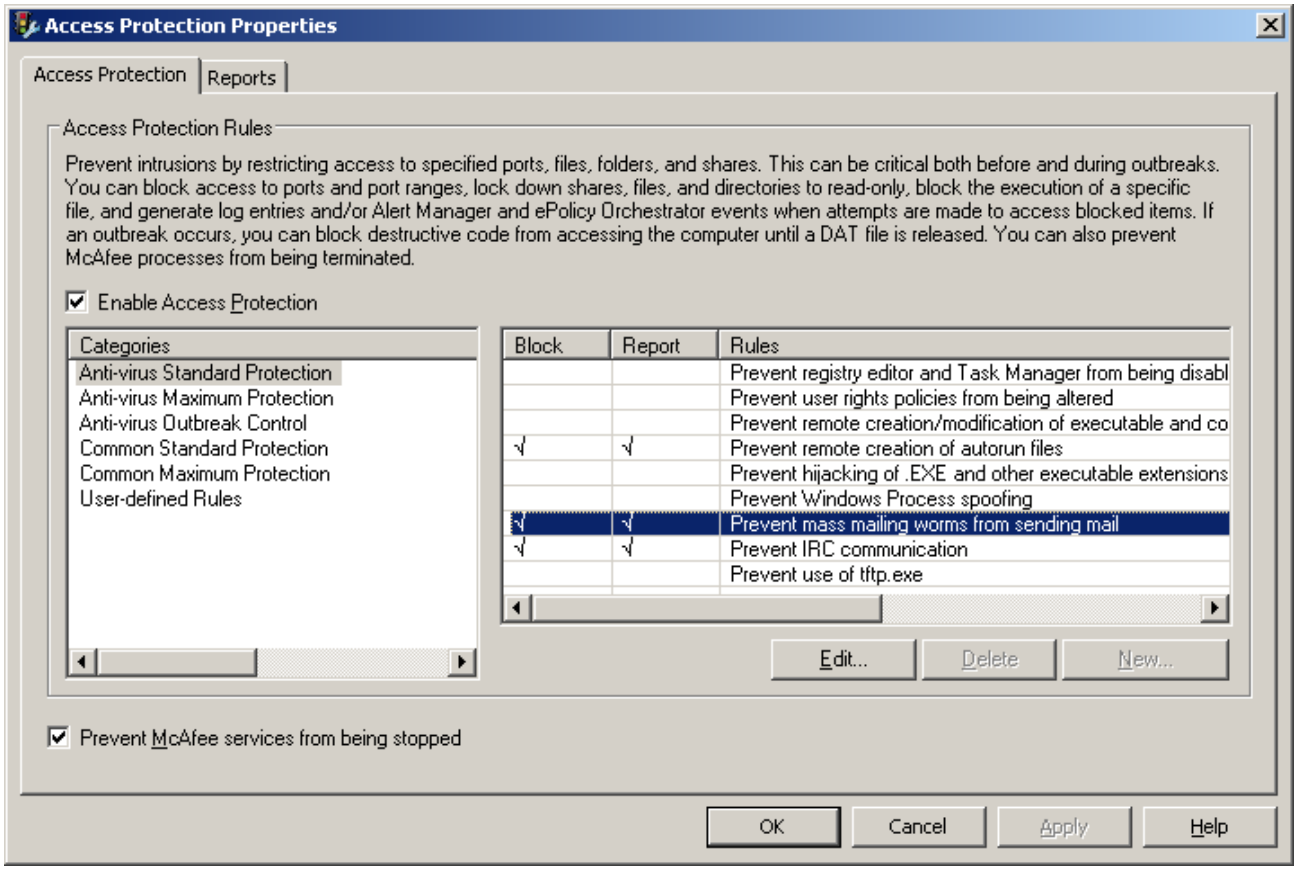

Figure 21 Access protection properties

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

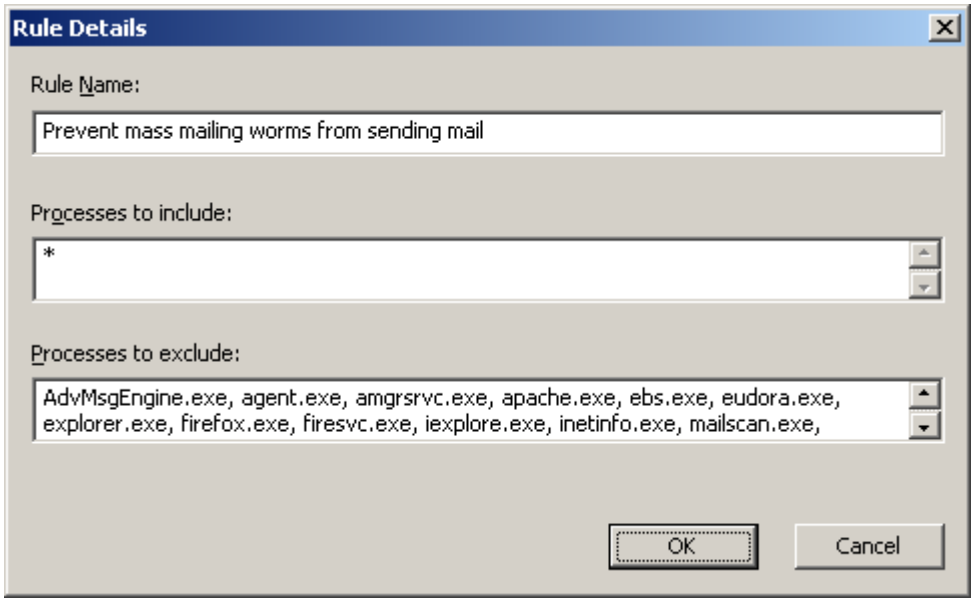

Figure 22 Add AdvMsgEngine.exe to the list of excluded processes

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

6 Configure Buffer Overflow Protection

For VirusScan 8.8 with Patch 4 installed on 32-bit versions of the operating system, the file EXCEL.EXE needs to be excluded from buffer overflow protection:

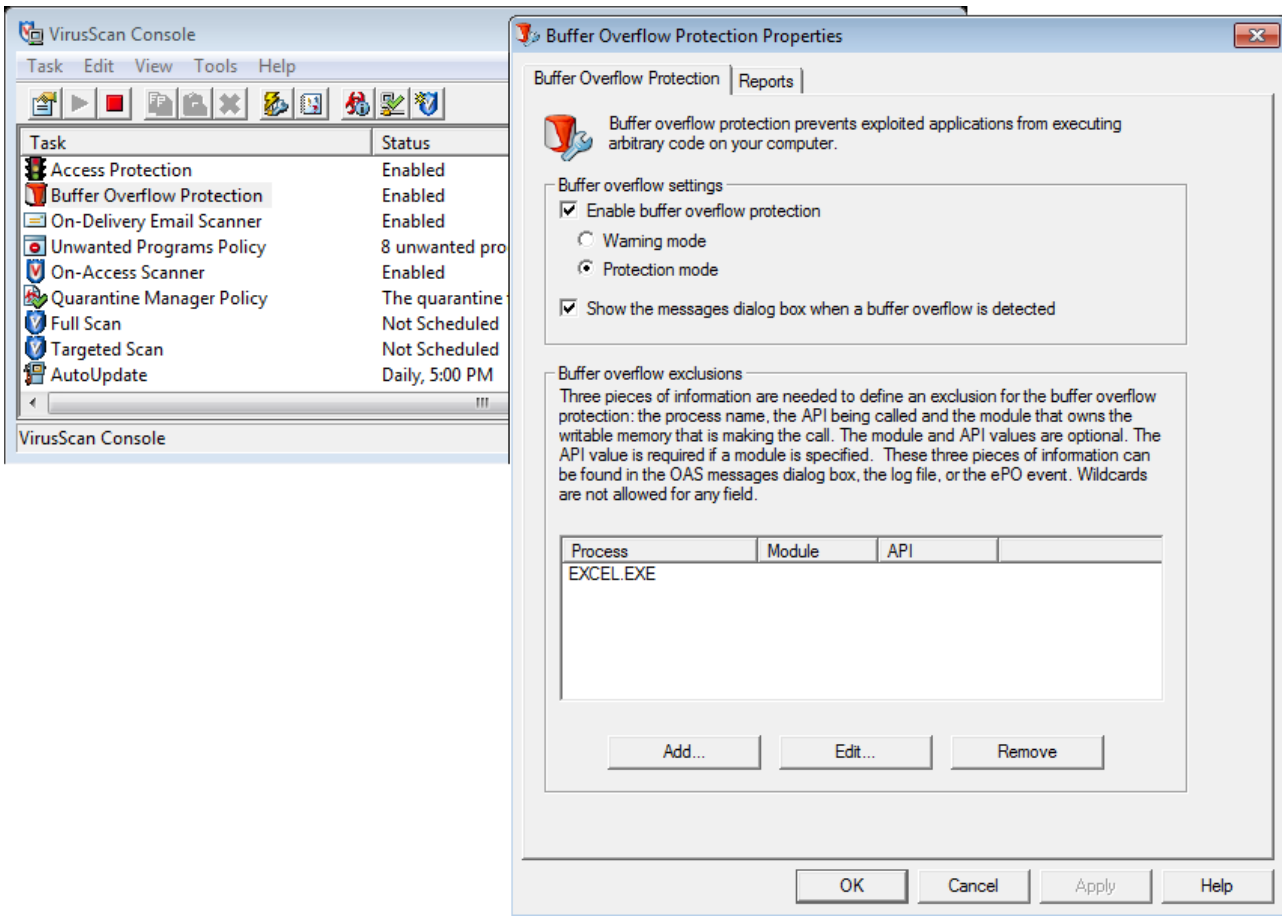

Figure 23 Exclude EXCEL.EXE from buffer overflow protection on 32-bit operating systems.

7 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, violating good security practices described e.g. in [1]. Enabling AutoUpdate on hosts connected to the automation system network is therefore not recommended.

8 McAfee ePolicy Orchestrator

For central management of all McAfee VirusScan installations in a system, and for secure and reliable deployment of virus definitions, a central management and update deployment host can be set up. McAfee ePolicy Orchestrator (ePO) can be used for this purpose. The document “Installing and Configuring McAfee ePO Server with System 800xA” [4] describes how to configure and manage VirusScan® Enterprise using ePolicy Orchestrator.

See also section 1.3 regarding VirusScan updates.

9 Exclude from On-Access Scanning

The folders and file types that need to be excluded from on-access scanning depend on the 800xA system version and which 800xA products are installed, as described in this chapter.

NOTE: Read the full document before applying the settings described in this chapter.

NOTE: Exclusions from on access scanning can be stated without any drive letter, in which case they will apply to all drives where the path is found. However, when configuring items to be scanned on demand, the full path including drive letter must be specified.

9.1 System 800xA version 5.1 (64 bit)

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

Product	Path or File type
800xA Base System	<drive>:\OperateITData*\ (for all disks where it exists) <drive>:\OperateITTemp*\ <drive>:\ProgramData\ABB\ \Program Files(x86)\ABB Industrial IT\Operate IT\Process Portal A\bin\ (for low risk processes only) File types MDF, LDF, NDF (exclude also from on-demand scanning)
Control IT	<drive>:\ABB Industrial IT Data\
Information Manager	<drive>:\HsData\ (for all disks where it exists) <drive>:\oracle\admin\ <drive>:\oracle\oradata\
Batch Management	<drive>:\Program Files(x86)\ABB Industrial IT\Operate IT\Produce IT\Batch\bin\
Foundation Fieldbus Device Integration	<drive>:\ABB Industrial IT Data\ <drive>:\Program Files(x86)\ABB Industrial IT\Engineer IT\Fieldbus Builder FF\log\
Profibus & HART Device Management	<drive>:\Engineer IT Data\Fieldbus Builder PH\

9.2 System 800xA version 5.1 (32 bit)

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

Product	Path or File type
800xA Base System	<drive>:\OperateITData*\ (for all disks where it exists) <drive>:\OperateITTemp*\ <drive>:\ProgramData\ABB\ \Program Files\ABB Industrial IT\Operate IT\Process Portal A\bin\ (for low risk processes only) File types MDF, LDF, NDF (exclude also from on-demand scanning)
Control IT	<drive>:\ABB Industrial IT Data\
Information Manager	<drive>:\HsData\ (for all disks where it exists) <drive>:\oracle\admin\ <drive>:\oracle\oradata\
Batch Management	<drive>:\Program Files\ABB Industrial IT\Operate IT\Produce IT\Batch\bin\
Foundation Fieldbus Device Integration	<drive>:\ABB Industrial IT Data\ <drive>:\Program Files\ABB Industrial IT\Engineer IT\Fieldbus Builder FF\log\
Profibus & HART Device Management	<drive>:\Engineer IT Data\Fieldbus Builder PH\

The following files need to be excluded from buffer overflow protection:

Product	File
-	EXCEL.EXE

10 Settings Summary

The following tables summarize configuration settings. They can be used as checklists to verify that all settings have been done correctly. Table headings refer to the respective configuration views and tabs, with references to the relevant sections in this document.

Installation Options (chapter 2)		
Step	**Setting**	✓
Select Setup Type	Typical	
Select Access Protection Level	Standard Protection	

On-Access Scan Properties, General Settings (section 3.2.1)				
Tab	**Alternatives**		**Setting**	✓
General	Scan	Boot Sectors	Enabled	
		Floppy during shutdown	Enabled	
		Processes on enable	Disabled	
	General	Enable On-access scanning on system start up	Enabled	
	Scan Time	Maximum Archive Scan time (seconds)	15	
		Enforce a maximum scanning time for all files	Enabled	
		Maximum scan time (seconds)	45	
	Heuristic network check for suspicious files	Sensitivity level	Disabled	
Messages	Actions available to user	Delete files	Disabled	

On-Access Scan Properties, Default Processes (section 3.2.2)				
Tab	**Alternatives**		**Setting**	✓
Processes	Configure different scanning policies for high-risk, low-risk, and default processes		Selected	
Scan Items	Scan Files	When writing to disk	Enabled	
		When reading from disk	Disabled	
		On network drives	Disabled	
		Opened for backup	Disabled	
	What to scan	Default + additional file types	Selected	
		Additional file types	AFW	
	Heuristics	Find unknown unwanted programs and trojans	Enabled	
		Find unknown macro threats	Enabled	
	Compressed files	Scan inside archives	Enabled	
		Decode MIME encoded files	Disabled	
	Unwanted programs detection	Detect unwanted programs	Enabled	
Exclusions	Exclude	Files and folders as specified in chapter 6	-	
Actions	When a threat is found	Perform this action first	Clean files automatically	
		If the first action fails, then perform this action	Deny access to files	
	When an unwanted program is found	Perform this action first	Clean files automatically	
		If the first action fails, then perform this action	Deny access to files	

On-Access Scan Properties, Low-Risk Processes (section 3.2.3)				
Tab	**Alternatives**		**Setting**	✓
Processes	Add	AfwWorkplaceApplication.exe	-	
Scan Items	Scan Files	When writing to disk	Enabled	
		When reading from disk	Disabled	
		On network drives	Disabled	
		Opened for backup	Disabled	
	What to scan	Default + additional file types	Selected	
		Additional file types	AFW	
	Heuristics	Find unknown unwanted programs and trojans	Enabled	
		Find unknown macro threats	Enabled	
	Compressed files	Scan inside archives	Enabled	
		Decode MIME encoded files	Disabled	
	Unwanted programs	Detect unwanted programs	Enabled	
Exclusions	Exclude	Files and folders as specified in chapter 9	-	
Actions	When a threat is found	Perform this action first	Clean files automatically	
		If the first action fails, then perform this action	Deny access to files	
	When an unwanted program is found	Perform this action first	Clean files automatically	
		If the first action fails, then perform this action	Deny access to files	

On-Access Scan Properties, High-Risk Processes (section 3.2.4)				
Tab	**Alternatives**		**Setting**	✓
Processes	-		-	
Scan Items	Scan Files	When writing to disk	Enabled	
		When reading from disk	Disabled	
		On network drives	Disabled	
		Opened for backup	Disabled	
	What to scan	Default + additional file types	Selected	
		Additional file types	AFW	
	Heuristics	Find unknown unwanted programs and trojans	Enabled	
		Find unknown macro threats	Enabled	
	Compressed files	Scan inside archives	Enabled	
		Decode MIME encoded files	Disabled	
	Unwanted programs	Detect unwanted programs	Enabled	
Exclusions	Exclude	Files and folders specified in chapter 9	-	
Actions	When a threat is found	Perform this action first	Clean files automatically	
		If the first action fails, then perform this action	Deny access to files	
	When an unwanted program is found	Perform this action first	Clean files automatically	
		If the first action fails, then perform this action	Deny access to files	

On-Demand Scan Properties – Full Scan (section 3.3)				
Tab	**Alternatives**		**Setting**	✓
Scan Locations	Specify where scanning takes place	Memory for Rootkits	Selected	
		Running processes	Selected	
		All local drives	Selected	
	Scan options	Include subfolders	Enabled	
		Scan boot sectors	Enabled	
Scan Items	File types to scan	All files	Selected	
	Options	Detect unwanted programs	Enabled	
		Decode MIME encoded files	Disabled	
		Scan inside archives	Enabled	
		Scan files that have been migrated to storage	Disabled	
	Heuristics	Find unknown program threats	Enabled	
		Find unknown macro threats	Enabled	
Exclusions	Exclude	Exclude file types LDF, MDF, and NDF	-	
Performance	Scan deferral options	Defer scan when using battery power	Disabled	
		Defer scans during presentations	Disabled	
		User may defer scans	Disabled	
	System utilization	Try out a value that allows scanning to finish within an acceptable amount of time while keeping the impact on system performance and reaction times at a level that is tolerable. The value stated here is for guidance only.	30%	
	Heuristic network check	Sensitivity level	Disabled	
Actions	When a threat is found	Perform this action first	Clean	
		If the first action fails, then perform this action	Prompt for action	
	When an unwanted program is found	Perform this action first	Clean	
		If the first action fails, then perform this action	Prompt for action	
	Allowed actions in Prompt dialog box	Clean file	Enabled	
		Delete file	Disabled	

Access Protection Properties (section 5)			
Rule	**Processes to exclude**		✓
Prevent mass mailing worms from sending mail	AdvMsgEngine.exe	-	

Buffer Overflow Protection (section 6)			
VirusScan 8.8 with Patch 4 installed on 32 bit operating systems	**Processes to exclude**		✓
	EXCEL.exe	-	

REVISION

Rev. ind.	Section	Description	Date Dept./Init.
-		New document.	2007-03-13 PAPR/XA/A TP
A	1.2	Added SV3.1 to the list of 800xA system versions.	2007-04-18 PAPR/XA/A TP
	3.4	Added section about additional exclusions for computers running Windows domain controller.	
	9	Added a section for 800xA version 3.1 In the Information Manager sections, added note about excluding the folder \HsData for all disks where it exists.	
B	1.1	Added recommendation to establish a security policy.	2008-10-09 PAPR/XA/A TP
	1.2	Updated the recommended VirusScan version to 8.5i with Patch 4 installed.	
	3	Updated figures to reflect the appearance of VirusScan 8.5i.	
	3.2.2	Added recommendation to exempt file types MDF, LDF, and NDF from on-access scanning.	
	3.3	Clarified that this chapter relates to on-demand scanning. Added recommendation to scan inside archives during on-demand scanning. Emphasized that all files excluded from on-access scanning should be added. Added recommendation to exclude file types MDF, LDF, and NDF from on-demand scanning.	
	4	Added recommendation that the security policy should include procedures for recovery from virus infections. Added recommended recovery procedure when VirusScan detects an infected file that it can't clean.	
C	3.2.3	Removed stale link to McAfee knowledge base	2008-11-12 PAPR/XA/A TP
D	1	Removed information about upgrading from VirusScan 8.0i	2009-02-27 PAPR/XA/A TP
	1.4	Added reference to the document "Microsoft Security Updates Validation Status for IIT System 800xA" (3BSE041902) for information on qualified VirusScan patch level	
	3.3	Modified the recommendation for on-demand scanning to include the alternative to scan all local drives	
E	All	Updated and restructured the document to reflect changes and new features in VirusScan 8.7i.	2010-03-04 PAPR/XA/A TP
	1.2	Changed recommended VirusScan version to 8.7i with patch 2.	
	1.3	Added recommendation to not use SuperDATs for regular virus definition updates.	
	3.1	Added note to the fact that some VirusScan configuration settings require that the computer is restarted for the changes to take effect.	
F	1.3	Added recommendation to test virus definition file updates that have not been verified by ABB, before introducing them in a production system.	2010-05-02 PAPR/XA/A TP
G	1.2	Added version 5.1 to the list of System 800xA versions	2010-06-28 PAPR/XAA TP
	9	Added section for System 800xA version 5.1 Added note about need to state full path for items to scan on demand Added exclusions for Batch Management	
H	1.3	Replaced recommendation to test DAT updates with a reference to the document *System 800xA daily verification of McAfee updates*, 9ARD107543-002	2011-03-18 PAPR/XAA TP
	4	Added reference to the user manual "Maintenance"	
I	9	Clarified that the listed exclusions are additional to those mentioned in chapter 3.	2011-08-18 PAPR/XAA TP
J	1.2	Changed the recommended VirusScan version to 8.8 with patch 1. Changed supported System 800xA versions to 4.1, 5.0, and 5.1	2012-04-03 PAPR/XAA TP
	1.3	Changed recommendation "delay DAT updates by 48 hours" to "wait with updating to a new DAT version until the test result has been published"	
	3.4	Added the need to install the hotfix VSE880HF625756 for Windows 2000 Server users	

Rev. ind.	Section	Description	Date Dept./Init.
	9	Removed sections for System 800xA 3.1 and 4.0 Updated exclusions for Foundation Fieldbus Device Integration	
K	1.2	Moved information about need to install a McAfee hotfix for Windows 2000 Server to here, and updated the hotfix reference information.	2012-05-16 PAPR/XAA TP
	3.4	Added that the additional settings for Windows Domain Controller need to be made for on-demand as well as on-access scanning	
	9	Corrected the path for Batch Management exclusions	
L	1.2	Changed supported System 800xA versions to 5.0 and 5.1 Changed the recommended VirusScan version to 8.8 with Patch 2	2012-11-12 PAPR/XAA TP
	3.3	Changed the recommendation for on-demand scanning to always include all folders and files except file types LDF, MDF, and NDF	
	8	Added a chapter on McAfee ePO	
	9	Added a section for System 800xA 5.1 64-bit	
	10	Added a Settings Summary chapter	
M	1.2	Removed System 800xA versions to 5.0 from the list of supported versions. Changed the recommended VirusScan version to 8.8 with Patch 4.	2014-09-10 PAPR/XAA TP
	2	Added the chapter “Installing McAfee Virus Scan Enterprise” Added that “Access Protection Level” shall be set to “Standard Protection”	
	6	Added chapter on configuration of Buffer Overflow Protection	
	9	Removed section for System 800xA version 5.0	
	10	Added table for Install Options. Added table for Buffer Overflow Protection.	