

VirusScan Enterprise

VERSION 7.0



COPYRIGHT

© 2003 Networks Associates Technology, Inc. All Rights Reserved. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the written permission of Networks Associates Technology, Inc., or its suppliers or affiliate companies. To obtain this permission, write to the attention of the Network Associates legal department at: 3965 Freedom Circle, Santa Clara, California 95054, or call +1-972-308-9960.

TRADEMARK ATTRIBUTIONS

Active Firewall, Active Security, Active Security (in Katakana), ActiveHelp, ActiveShield, AntiVirus Anyware and design, Bomb Shelter, Certified Network Expert, Clean-Up, CleanUp Wizard, CNX, CNX Certification Certified Network Expert and design, Design (stylized N), Disk Minder, Distributed Sniffer System, Distributed Sniffer System (in Katakana), Dr Solomon's, Dr Solomon's label, Enterprise SecureCast, Enterprise SecureCast (in Katakana), Event Orchestrator, EZ SetUp, First Aid, ForceField, GMT, GroupShield, GroupShield (in Katakana), Guard Dog, HelpDesk, HomeGuard, Hunter, LANGuru, LANGuru (in Katakana), M and design, Magic Solutions, Magic Solutions (in Katakana), Magic University, MagicSpy, MagicTree, McAfee, McAfee (in Katakana), McAfee and design, McAfee.com, MultiMedia Cloaking, Net Tools, Net Tools (in Katakana), NetCrypto, NetScan, NetShield, NetStalker, Network Associates, NetXray, NotesGuard, Nuts & Bolts, Oil Change, PC Medic, PCNotary, PrimeSupport, Recoverkey, Recoverkey – International, Registry Wizard, ReportMagic, Router PM, Safe & Sound, SalesMagic, SecureCast, Service Level Manager, ServiceMagic, SmartDesk, Sniffer, Sniffer (in Hangul), Stalker, SupportMagic, TIS, TMEG, Total Network Security, Total Network Visibility, Total Network Visibility (in Katakana), Total Service Desk, Total Virus Defense, Trusted Mail, UnInstaller, Virex, Virus Forum, ViruScan, VirusScan, WebScan, WebShield, WebShield (in Katakana), WebSniffer, WebStalker, WebWall, Who's Watching Your Network, WinGauge, Your E-Business Defender, ZAC 2000, Zip Manager are registered trademarks of Network Associates, Inc. and/or its affiliates in the US and/or other countries. All other registered and unregistered trademarks in this document are the sole property of their respective owners.

This product includes or may include software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)

This product includes or may include cryptographic software written by Eric Young. (ey@cryptsoft.com)

LICENSE AGREEMENT

NOTICE TO ALL USERS: CAREFULLY READ THE APPROPRIATE LEGAL AGREEMENT CORRESPONDING TO THE LICENSE YOU PURCHASED, WHICH SETS FORTH THE GENERAL TERMS AND CONDITIONS FOR THE USE OF THE LICENSED SOFTWARE. IF YOU DO NOT KNOW WHICH TYPE OF LICENSE YOU HAVE ACQUIRED, PLEASE CONSULT THE SALES AND OTHER RELATED LICENSE GRANT OR PURCHASE ORDER DOCUMENTS THAT ACCOMPANIES YOUR SOFTWARE PACKAGING OR THAT YOU HAVE RECEIVED SEPARATELY AS PART OF THE PURCHASE (AS A BOOKLET, A FILE ON THE PRODUCT CD, OR A FILE AVAILABLE ON THE WEB SITE FROM WHICH YOU DOWNLOADED THE SOFTWARE PACKAGE). IF YOU DO NOT AGREE TO ALL OF THE TERMS SET FORTH IN THE AGREEMENT, DO NOT INSTALL THE SOFTWARE. IF APPLICABLE, YOU MAY RETURN THE PRODUCT TO NETWORK ASSOCIATES OR THE PLACE OF PURCHASE FOR A FULL REFUND.

Contents

| | |
|--|----------|
| Preface | 5 |
| Audience | 5 |
| Getting more information | 5 |
| Contacting McAfee and Network Associates | 7 |
| 1 New Features | 9 |
| Administration | 9 |
| One product for servers and workstations | 10 |
| Environment variables | 10 |
| Repairing corrupt installed VirusScan Enterprise files | 11 |
| Microsoft Windows Server 2003 support | 11 |
| Localized operating systems | 12 |
| Log files | 13 |
| AVERT samples | 14 |
| EMC Celerra and CAVA | 14 |
| Interface | 15 |
| Access to interface options | 15 |
| Right-click menus | 16 |
| EXTRA.DAT information in the About VirusScan Enterprise dialog box | 16 |
| Task status | 17 |
| Scanners | 18 |
| E-mail body scanning | 18 |
| MIME-encoded file scanning | 19 |
| Resuming an interrupted scan | 20 |
| Scan options for low-risk and high-risk processes | 21 |
| Secondary actions for scans | 22 |
| AutoUpdate 7.0 | 23 |
| HotFixes and service packs | 23 |
| Distributed update servers | 25 |
| Resuming an interrupted update | 26 |
| Update Now command | 27 |
| Multiple update tasks | 27 |

| | | |
|---------------------------------------|-------------------------|-----------|
| 2 | Changed Features | 27 |
| Administration | | 27 |
| CPU utilization | | 28 |
| Password protection | | 29 |
| Alerts by component | | 30 |
| Interface | | 31 |
| Start menu options | | 31 |
| Scanners and AutoUpdate | | 32 |
| What to scan and what not to scan | | 33 |
| Scheduled scan tasks and update tasks | | 35 |
| On-access scan messages | | 36 |
| Scan options in the user interface | | 37 |
| Archive and compressed file scanning | | 38 |
| Clean file scan cache | | 39 |
| 3 | Removed Features | 39 |
| Administration | | 39 |
| Operating system support | | 40 |
| Importing and exporting tasks | | 41 |
| Create Emergency Disk | | 41 |
| DMI alerts | | 41 |
| Performance counters | | 42 |
| Scanners and updates | | 42 |
| Internet Filter | | 42 |
| Download Scan | | 43 |
| Exclude action | | 43 |
| On-Demand Scan wizard | | 44 |
| AutoUpgrade | | 44 |

Preface

This Release Guide introduces McAfee VirusScan[®] Enterprise software version 7.0, and describes the following information:

- New features in this release of the software.
- Changed features in this release of the software.
- Removed features.

Audience

This information is intended primarily for two audiences:

- Network administrators who are responsible for the company's anti-virus and security program.
- Users who are responsible for updating virus definition (DAT) files on their workstation, or configuring the software's detection options.

Getting more information

Product Guide Product introduction and features, detailed instructions for configuring the software, information on deployment, recurring tasks, and operating procedures.

Available in an Adobe Acrobat .PDF file from either the product CD or the McAfee download site.

Installation Guide System requirements and instructions for installing and starting the software.

Available as a printed booklet that accompanies the product CD. Also available in an Adobe Acrobat .PDF file from either the product CD or the McAfee download site.

| | |
|----------------------------|---|
| Help | <p>Product information in the Help system that is accessed from within the application.</p> <ul style="list-style-type: none">■ The Help system provides high-level and detailed information. Access from either a Help menu option or Help button in the application.■ Context-sensitive (<i>What's This?</i>) Help provides brief descriptions of the selections in the application. Access by right-clicking on an option, pressing the [F1] control key, or dragging the question icon to an option. |
| Configuration Guide | <p><i>For use with ePolicy Orchestrator.</i> Procedures for installing, configuring, deploying, and managing your McAfee product through ePolicy Orchestrator management software.</p> <p>Available in an Adobe Acrobat .PDF file from either the product CD or the McAfee download site.</p> |
| Release Notes | <p><i>README file.</i> Product information, system requirements, resolved issues, any known issues, and last-minute additions or changes to the product or its documentation.</p> <p>Available as a .TXT file from either the product CD or the McAfee download site.</p> |
| Contact | <p>A list of phone numbers, street addresses, web addresses, and fax numbers for Network Associates offices in the United States and around the world. Also provides contact information for services and resources, including:</p> <ul style="list-style-type: none">■ Technical Support■ Customer Service■ Download Support■ AVERT Anti-Virus Emergency Response Team■ McAfee Beta Site■ On-Site Training■ Network Associates Offices Worldwide |

Contacting McAfee and Network Associates

| | |
|---|---|
| Technical Support | http://knowledge.nai.com |
| McAfee Beta Site | www.mcafeeb2b.com/beta/ |
| AVERT Anti-Virus Emergency Response Team | www.mcafeeb2b.com/naicommon/avert/default.asp |
| Download Site | www.mcafeeb2b.com/naicommon/download/ |
| DAT File Updates | www.mcafeeb2b.com/naicommon/download/dats/find.asp ftp://ftp.nai.com/pub/antivirus/datfiles/4.x |
| Product Upgrades | www.mcafeeb2b.com/naicommon/download/upgrade/login.asp Valid grant number required. Contact Network Associates Customer Service. |
| On-Site Training | www.mcafeeb2b.com/services/mcafee-training/default.asp |
| Network Associates Customer Service: | |
| E-mail | services_corporate_division@nai.com |
| Web | www.nai.com www.mcafeeb2b.com |
| US, Canada, and Latin America toll-free: | |
| Phone | +1-888-VIRUS NO or +1-888-847-8766 Monday – Friday, 8 a.m. – 8 p.m., Central Time |

For additional information on contacting Network Associates and McAfee — including toll-free numbers for other geographic areas — see the Contact file that accompanies this product release.

This release of VirusScan Enterprise 7.0 is designed for both servers and workstations, eliminating the need for two separate products.

This release of VirusScan Enterprise 7.0 introduces many new features. These can be divided into four categories:

- *Administration on page 9*
- *Interface on page 15*
- *Scanners on page 18*
- *AutoUpdate 7.0 on page 23*

Administration

The release of VirusScan Enterprise 7.0 introduces the following new administration features:

- *One product for servers and workstations on page 10*
- *Environment variables on page 10*
- *Repairing corrupt installed VirusScan Enterprise files on page 11*
- *Microsoft Windows Server 2003 support on page 11*
- *Localized operating systems on page 12*
- *Log files on page 13*
- *AVERT samples on page 14*
- *EMC Celerra and CAVA on page 14*

One product for servers and workstations

Previous release NetShield® 4.5 supported only file server configurations and VirusScan 4.5.1 supported only workstation configurations. This required the customer to manage multiple products.

Current release VirusScan Enterprise 7.0 supports both file servers and workstations in one product.

Benefits Having one product for file servers and workstations provides:

- More efficient use of resources during deployment and configuration.
- Consistent interface and features across configurations.
- More effective and efficient support.

Environment variables

Previous release You could not use environment variables in path names.

Current release You can use environment variables (for example, %WINDIR%) anywhere in a path name.

For example, environment variables can be used in the log file path and scan item path, among others.

NOTE

If, when configuring a scan task on a remote computer, you enter a variable that does not exist on the local computer, or does not have a compatible value, a message appears stating that the path name does not appear to be valid.

Benefits The ability to use environment variables in path names saves you time when configuring scan tasks on remote computers.

Repairing corrupt installed VirusScan Enterprise files

- Previous release** This feature was not available in either VirusScan 4.5.1 or NetShield 4.5.
- Current release** By using Microsoft Installer, you can use the **Repair** option in the installation wizard to repair any files that have been corrupted since the original installation.
- Benefits** This feature allows you to repair files or the registry without having to reinstall the software.

Microsoft Windows Server 2003 support

- Previous release** Not available in either NetShield 4.5 or VirusScan 4.5.1.
- Current release** VirusScan Enterprise 7.0 supports the Microsoft Server 2003 RC1 operating system (formerly known as Windows .NET RC1).
- Benefits** This provides another choice of server operating system.

Localized operating systems

Previous release The English language versions of VirusScan 4.5.1 and NetShield 4.5 would run on only the English language version of the operating system.

Current release The English language version of VirusScan Enterprise 7.0 runs on localized versions of supported operating systems.

Benefits This gives the product:

- Wider availability and flexibility.
- Compatibility with Microsoft multilingual user interfaces (MUIs).

Log files

Previous release

Log file size could be limited from one to 999KB (or you could choose not to limit the log file size). While configuring your log files, you could choose to include:

- **Virus detection**
- **Virus cleaning**
- **Infected file deletion**
- **Infected file move**
- **Session settings**
- **Session summary**
- **Date and time**
- **User name**

Current release

Log file size can be limited from one to 999MB (or you can choose not to limit the log file size). Virus detection, virus cleaning, infected file deletion, and infected file move information is logged automatically. When the log file reaches its limit, the first 20% of the file will be deleted to ensure logging data continues.

While configuring your log file, you can include the following optional information:

- **Session settings**
- **Session summary**
- **Failure to scan encrypted files**
This is a new feature for the log file.
- **User name**

Benefits

- Includes more information in the file and allows greater size of the file, if you choose to limit the size.
- Simplifies options of what to log.

AVERT samples

| | |
|-------------------------|--|
| Previous release | You could not submit a virus sample directly to AVERT through the user interface. |
| Current release | You can access the the AVERT WebImmune web site (www.webimmune.net) directly to submit a virus sample to AVERT. |
| Benefits | Direct access to the WebImmune web site. |
| Where to find | From the VirusScan Console , select Help Submit a Sample to AVERT . |

EMC Celerra and CAVA

| | |
|------------------------|---|
| Current release | <p>McAfee has integrated its VirusScan Enterprise technology with EMC's Celerra anti-virus solution, providing customers with comprehensive, easy-to-manage, enterprise-level anti-virus protection for their critical EMC network attached storage (NAS) resources. When a file is written and saved (scan on update), or first read (scan on read), the Celerra solution restricts access to that file until virus scanning has been performed by VirusScan.</p> <p>The Celerra anti-virus solution consolidates virus scanning on a scalable and low overhead configuration that protects business-critical information without impeding performance. The Celerra anti-virus solution consists of:</p> <ul style="list-style-type: none">■ VirusScan Enterprise 7.0 or NetShield 4.5■ The Celerra AntiVirus Agent (CAVA) 1.8.9 or later■ DART code 2.2.39 or later (DART 4.2 for scan on read) |
|------------------------|---|

NOTE

For Celerra NS600 hardware, DART code 5.0x and CAVA 2.2.4 are required as a minimum.

| | |
|-----------------|--|
| Benefits | Integration with other products offers you greater flexibility when configuring your network solution. |
|-----------------|--|

Interface

The release of VirusScan Enterprise 7.0 introduces the following new interface features:

- [Access to interface options on page 15](#)
- [Right-click menus on page 16](#)
- [EXTRA.DAT information in the About VirusScan Enterprise dialog box on page 16](#)
- [Task status on page 17](#)

Access to interface options

Previous release VirusScan 4.5.1 and NetShield 4.5 did not allow the administrator to limit user interface options for the end user.

Current release VirusScan Enterprise 7.0 allows you to:

- Show the system tray icon with all menu options.
- Show the system tray icon with minimal menu options.
- Hide the system tray icon, so that no menu options are available.

Benefits This feature allows you to:

- Configure the product for greater security by preventing users from turning off or altering the anti-virus protection on their workstation.
- Have complete control of user interface visibility.

Where to find Configure this feature on the **Display Options** tab of the **User Interface Options** dialog box. (From the **VirusScan Console**, select **Tools | User Interface Options**.)

Right-click menus

- Previous release** Both VirusScan 4.5.1 and NetShield 4.5 were unable to scan top-level virtual objects, such as **My Computer** and **My Documents**.
- Current release** Virus scanning of top-level virtual objects, such as **My Computer** and **My Documents**, is now available through right-click menus. Scanning from the right-click menus also scans files of any type.
- Benefits** Allows you to scan top-level virtual objects by right-clicking their icons and selecting **Scan for viruses** from the menu.

EXTRA.DAT information in the About VirusScan Enterprise dialog box

- Previous release** You could find the extra driver (EXTRA.DAT) information and the number of viruses detected by the EXTRA.DAT file only by searching the directory or the event log.
- Current release** The **About VirusScan Enterprise** dialog box contains:
- Information regarding the EXTRA.DAT file, if present.
 - The number of viruses detected by EXTRA.DAT, if present.
- Benefits**
- During an outbreak situation, you can see which computers have been updated, and whether the driver can detect the virus.
 - The EXTRA.DAT and license information (accessible from the dialog box) is reported to ePolicy Orchestrator.
- Where to find** Right-click the **VirusScan Enterprise** icon in the system tray and select **About VirusScan Enterprise**, or select **About** from the **Help** menu of the **VirusScan Console**.

Task status

- Previous release** When a scheduled task ran, you could view only the time at which the last task launched. You could not see whether the task was running.
- Current release** The **VirusScan Console** includes a **Status** column, which indicates the current status of all tasks.
- Benefits** Allows you to know whether a given task is currently running.
- Where to find** This information is available in the **Status** column of the **VirusScan Console**.

Scanners

The release of VirusScan Enterprise 7.0 introduces the following new scanning features:

- [E-mail body scanning on page 18](#)
- [MIME-encoded file scanning on page 19](#)
- [Resuming an interrupted scan on page 20](#)
- [Scan options for low-risk and high-risk processes on page 21](#)
- [Secondary actions for scans on page 22](#)

E-mail body scanning

| | |
|-------------------------|---|
| Previous release | Scanning the body of an e-mail message was not possible in either VirusScan 4.5.1 or NetShield 4.5. |
| Current release | <p>The On-Delivery Scanner and e-mail On-Demand Scanner now include body scanning for HTML-based script viruses. The scanner writes the body of a mail message to its own Temporary folder as a temporary file, then scans the file.</p> <p>Infected messages are embedded in a container e-mail message and moved to the intended recipient's infected folder in Microsoft Outlook. Another message is placed in the intended recipient's inbox, indicating that the original message has been sent to the infected folder.</p> |
| Benefits | Greater security with the e-mail scan features. |
| Where to find | <p>This option is located on the Advanced tab of the On-Delivery Scan Properties and On-Demand Scan Properties dialog boxes.</p> <p>The Infected folder is located in the Folder List pane of Microsoft Outlook.</p> |

MIME-encoded file scanning

Previous release MIME-encoded (multipurpose Internet mail extension) files were not scanned. The on-access scanner would scan the file only when the user tried to access the file, after the e-mail transport brought the infected file onto the system.

Current release All MIME-encoded files are scanned by all scanners when the **Decode MIME encoded files** option is selected.

This feature can be enabled or disabled.

The On-Delivery Scanner selects this option by default.

The On-Demand Scanner and On-Access Scanner do not select this option by default because some POP3 clients store all MIME e-mail messages in a combined form. So, if one file is infected, VirusScan Enterprise could delete all of the incoming messages.

Benefits Allows all scanners to detect infections inside files that are attached to incoming e-mail messages, before there is an attempt to access the file.

Provides greater security with earlier detection.

Where to find This configuration option (**Decode MIME encoded files**) is located on the **Advanced** tab of each of the scan feature's properties dialog boxes.

NOTE

In order to scan archives (for example, .ZIP) that are attached to an .EML file, the **Scan inside archives** option on this tab must also be selected.

Resuming an interrupted scan

| | |
|-------------------------|--|
| Previous release | Neither VirusScan 4.5.1 nor NetShield 4.5 allowed the resumption of a scan that had been interrupted. |
| Current release | <p>VirusScan Enterprise 7.0 allows the resumption of a scheduled scan if it is interrupted.</p> <p>You can configure your scan task properties to interrupt the task if it takes longer than a defined amount of time. When this happens, or if a scheduled scan is interrupted for any reason, the next time the task runs, it resumes from the point of interruption.</p> <p>When the scan task runs again, regardless of reason of the interruption, you are prompted to choose either to resume the scan or to start the scan from the beginning.</p> <p>Scheduled scans always resume since there is no user interface.</p> |
| Benefits | The ability to stop and resume a scan conserves resources, providing a higher degree of system efficiency. |
| Where to find | When you schedule a scan task (using the Schedule button in the VirusScan On-Demand Scan dialog box), select Enable , and select Stop the task if it runs for . Then enter the desired hours and minutes for the allowable amount of time to perform the scan before interruption. |

Scan options for low-risk and high-risk processes

Previous release In both VirusScan 4.5.1 and NetShield 4.5, scan policies were the same for all processes.

Current release The on-access scanner in VirusScan Enterprise 7.0 provides per-process configurations. You can configure what type of scanning to use for specific processes associated with specific applications. For example, you can configure the scanner to use lower security settings when scanning files accessed by applications known to be typically low-risk.

The options are:

- **Default Processes**

A list of processes, not defined as low-risk or high-risk, that use the same, configurable settings.

NOTE

You can apply these settings to all processes or to only those processes that are not defined as low-risk or high-risk.

- **Low-Risk Processes**

Custom configuration settings for low-risk processes.

- **High-Risk Processes**

Custom configuration settings for high-risk processes.

Benefits This feature allows greater administrative control by providing a flexible method for administrators to customize the scanning of processes to ensure maximum performance and risk mitigation.

Where to find This feature is located on the **VirusScan On-Access Scan Properties** dialog box, in the properties for **Low-Risk Processes** and **High-Risk Processes**.

Configure the settings for each set of processes on the **Detection**, **Advanced**, and **Actions** tabs on the respective sections (**Default Processes**, **Low-Risk Processes**, and **High-Risk Processes**) of the **VirusScan On-Access Scan Properties** dialog box.

Secondary actions for scans

- Previous release** In both VirusScan 4.5.1 and NetShield 4.5, you could not define a secondary action for the scanner to take if the selected action failed.
- Current release** VirusScan Enterprise 7.0 allows you to define a primary and secondary action for the scanner to take when it detects an infected file. If the primary action fails, VirusScan attempts the secondary action before prompting the user. If the secondary action fails, the error is logged and an alert is sent but the user is not prompted.
- Benefits** Having a predefined secondary action for infected files gives you greater control and fewer interruptions.
- Where to find** Define the primary and secondary actions for on-access scans on the **Actions** tab of the **VirusScan On-Access Scan Properties** dialog box for each option (**Default Processes**, **Low-Risk Processes**, and **High-Risk Processes**) in the list view of this dialog box.

AutoUpdate 7.0

The release of VirusScan Enterprise 7.0 introduces the following new update features:

- [HotFixes and service packs on page 23](#)
- [Distributed update servers on page 25](#)
- [Resuming an interrupted update on page 26](#)
- [Update Now command on page 27](#)
- [Multiple update tasks on page 27](#)

HotFixes and service packs

Previous release

With both NetShield 4.5 and VirusScan 4.5.1, you could use the AutoUpdate component to download:

- DAT files
- Scanning engines

Updates were retrieved from a UNC share, an FTP server, or a local path/mapped drive.

Current release

AutoUpdate 7.0 in VirusScan Enterprise 7.0 downloads the following:

- DAT files
- EXTRA.DAT files
- Scanning engines
- Service packs
- HotFixes

Updates are retrieved from a UNC share, FTP server, HTTP server, mapped drive, or local drive.

Benefits

- Improves update reliability.
- Simplifies the deployment of service packs, HotFixes, and EXTRA.DAT files for the most current software.
- Gives greater flexibility, by providing an additional download server type.

Where to find

You can schedule an update on the VirusScan Console by selecting **Task | New Update task**, or by scheduling the default AutoUpdate task in the VirusScan Console.

Distributed update servers

Previous release With both VirusScan 4.5.1 and NetShield 4.5, you could only update via an FTP server, a UNC share, or a local path/mapped drive.

VirusScan 4.5.1 allowed updating to a mirror site on a client computer. This allowed retrieving VirusScan software updates from a local client computer. However, this method had limitations because it had to be set up on a client computer instead of a server.

Current release A new companion utility, McAfee AutoUpdate Architect software version 1.0, allows you to configure and use distributed update servers. These are servers distributed on your network from which you can retrieve software updates.

VirusScan Enterprise 7.0 can update from a selection of internal servers and server types:

- HTTP servers.
- FTP servers (either passive or active).
- UNC share servers.
- Local drive.
- Mapped drive.

NOTE

With McAfee AutoUpdate Architect, VirusScan Enterprise 7.0 can communicate with the distributed update servers during an update, to determine which server provides the fastest download, and can update from that server. If none of the internal update servers are available, the AutoUpdate utility downloads from <ftp://ftp.nai.com/CommonUpdater>.

Benefits

- Conservation of bandwidth of both the local area network (LAN) and wide area network (WAN).
- Greater flexibility when choosing servers.
- Updates for both servers and workstations from local servers.

Where to find The AutoUpdate repository list can be configured through the Tools | Edit AutoUpdate Repository List menu from the VirusScan Console.

Resuming an interrupted update

- Previous release** Neither VirusScan 4.5.1 nor NetShield 4.5 allowed the resumption of an update task that had been interrupted.
- Current release** VirusScan Enterprise 7.0 allows the resumption of an update if it is interrupted.
- You can configure your update task properties to interrupt the task if it takes longer than a defined amount of time. When this happens, or if an update is interrupted for any reason, the next time the task runs, it resumes from the point of interruption.
- Benefits** Being able to stop and resume an update conserves resources, providing a higher degree of system efficiency.
- Where to find** When you schedule an update task (using the **Task | New Update task** command in the **VirusScan Console**), select **Enable**, and **Stop the task if it runs for**. Then enter the desired hours and minutes for the allowable amount of time to perform the update before interruption.

Update Now command

Previous release Having a single command to perform a comprehensive update was not available in NetShield 4.5 or VirusScan 4.5.1. Updating was only available by running a task from the console.

Current release VirusScan Enterprise 7.0 allows you to update the DAT files by clicking **Update Now**.

NOTE

Access to this feature is controlled by the administrator.

Benefits You can run an update more easily.

Where to find Right-click the **VirusScan** icon in the system tray and select **Update Now**, or open an existing update task and click **Update Now**, or select **Tools | New Update Task** in the **VirusScan Console**.

Multiple update tasks

Previous release In both VirusScan 4.5.1 and NetShield 4.5, you could schedule only one update task and one upgrade task.

Current release VirusScan Enterprise 7.0 allows you to create and schedule multiple update tasks in the **VirusScan Console**. (There are no upgrade tasks — upgrades are performed with update tasks.) You can configure separate update tasks for servers and workstations, each with its own options and schedule.

Benefits This allows you greater control over your enterprise environment.

Where to find In the **VirusScan Console**, select **Tools | New Update Task**.

While most features of the VirusScan 4.5.1 and NetShield 4.5 products were retained in VirusScan Enterprise 7.0, some features are now located in different areas of the product and require different actions to use them.

These can be divided into three categories:

- [Administration on page 27](#)
- [Interface on page 31](#)
- [Scanners and AutoUpdate on page 32](#)

Administration

The release of VirusScan Enterprise 7.0 includes the following changed administration features:

- [CPU utilization on page 28](#)
- [Password protection on page 29](#)
- [Alerts by component on page 30](#)

CPU utilization

| | |
|-------------------------|---|
| Previous release | <p>In NetShield 4.5, you could use the Scan priority slider to set the limit of CPU utilization that a scan task could use. However, there were five pre-set options only; you could not select a specific percentage of CPU utilization for scan tasks.</p> <p>VirusScan 4.5.1 did not include a feature in the user interface to define maximum CPU utilization. You had to change the value in the registry manually.</p> |
| Current release | <p>You can specify an allowable average percentage of CPU utilization for an on-demand scan. You can select from 10% to 100% utilization in increments of 10.</p> |
| Benefits | <p>You have more flexibility in configuring on-demand scans and more control of system resources.</p> |
| Where to find | <p>On the Advanced tab of the VirusScan On-Demand Scan Properties dialog box, under CPU utilization.</p> |

Password protection

Previous release In VirusScan 4.5.1, the security password did not apply to all options. Users still had control over some individual tabs and options.

Current release Password protection is now per task item. You can set or clear one password for access to specified VirusScan Enterprise features.

Password options are:

- **No password**
No password is set and all features and user interface are available.
- **Password protection for all items listed below**
Set a password that secures all the items listed on the **Password Options** tab of the **User Interface Options** dialog box.
- **Password protection for the selected items below**
Set a password and select which items you want password-protected.

Options of the following features can be password protected:

- On-Access Scan
- On-Demand Scan — Saved Tasks
- On-Demand Scan — Unsaved Tasks
- E-Mail Scan — On-Delivery
- E-Mail Scan — On-Demand
- AutoUpdate
- Alert Manager Client
- Console and Miscellaneous

If the password is set users must enter the password.

Administrators can lock or unlock the user interface by selecting **Tools | Unlock User Interface** from the **VirusScan Console** to access locked items.

Benefits Password protection offers better security by preventing administrators (or users with local administrator rights) without the password from configuring the product.

Where to find Set the password by selecting **Tools | User Interface Options** from the **VirusScan Console**.

Alerts by component

- Previous release** VirusScan 4.5.1 allowed the user who started an on-demand scan to choose whether an infection alerted the Alert Manager™ utility.
- Current release** VirusScan Enterprise 7.0 allows only administrators to set which VirusScan components generate alerts. Therefore, users cannot decide whether an alert is generated if a virus is detected on their computers.
- Benefits** Administrator-controlled alert generation allows better security. If administrators configure alerts to be sent to the Alert Manager, they can collect information by VirusScan Enterprise feature on all viruses found in the organization.
- Where to find** On the **Alert Manager Alerts** tab of the **Alert Properties** dialog box. (Select **Tools | Alerts** on the **VirusScan Console**.)

Interface

This release of VirusScan Enterprise 7.0 includes the following changed interface feature:

- [Start menu options on page 31](#)

Start menu options

Previous release

Previously, the **Start** menu shortcuts included:

- **Create Emergency Disk**
- **VirusScan**
- **VirusScan Alerting Configuration**
- **VirusScan Console**

Current release

In VirusScan Enterprise 7.0, the **Start** menu shortcuts include:

- **VirusScan Console**
- **VirusScan On-Access Scan**
- **VirusScan On-Demand Scan**
- **Alert Manager Configuration**
- **Alert Manager Messages**

NOTE

The Alert Manager shortcuts are present only if the Alert Manager software is installed.

Each shortcut launches its respective property dialog boxes, but does not launch scans.

Benefits

These shortcuts allow you quick access to all the property dialog boxes within VirusScan Enterprise 7.0, except the On-Delivery Scan.

Where to find

Select **Start | Programs | Network Associates**.

Scanners and AutoUpdate

This release of VirusScan Enterprise 7.0 includes the following scanning and updating changed features:

- *What to scan and what not to scan on page 33*
- *Scheduled scan tasks and update tasks on page 35*
- *On-access scan messages on page 36*
- *Scan options in the user interface on page 37*
- *Archive and compressed file scanning on page 38*
- *Clean file scan cache on page 39*

What to scan and what not to scan

Previous release

VirusScan 4.5.1 included different dialog boxes for on-access scans and on-demand scans when configuring which file types to scan.

In both NetShield 4.5 and VirusScan 4.5.1, you defined what not to scan on a separate **Exclusions** tab.

You could configure what to scan for on-access scans and on-demand scans with these options:

- **Default files**
- **All files**
- **User specified files**

In VirusScan 4.5.1, two lists of default file type were available, but not clearly separated on the interface. One list used defaults from the DAT files, and one used product defaults. You could not customize the DAT file type defaults, but you could customize the product file type defaults.

Current release

Configuring what to scan and what not to scan takes place on the same interface. Although the interfaces are nearly identical for both on-access scans and on-demand scans, you must set them up independently.

Selections of what to scan include:

- **All files**
- **Default + additional file types**
- **Specified file types**

Selections of what not to scan include:

- **Specific files, folders or drives**
- **File types**
- **File age**
- **Files protected by Windows File Protection**

VirusScan Enterprise 7.0 has a single list of default file types available. This list comes from the DAT files and cannot be customized. You can also add file types to the default list, or use a completely user-specified list of file types.

Changed Features

Benefits

- Easier configuration of what to include, and what not to include since they both take place on the same tab of the dialog boxes.
- A single list of default file types provides greater consistency.
- The ability to choose what not to scan provides greater administrative control.
- Greater administrative control since no one can customize the list of default file types.

Where to find

Located on the **Detection** tab of the **VirusScan On-Demand Scan** dialog box and on the **Detection** tab of the **Default Processes** or **All Processes** sections of the **VirusScan On-Access Scan Properties** dialog box.

Scheduled scan tasks and update tasks

| | |
|-------------------------|---|
| Previous release | <p>The options for configuring when to run a scheduled task were:</p> <ul style="list-style-type: none">■ Once■ At Startup■ Hourly■ Daily■ Weekly■ Monthly |
| Current release | <p>VirusScan Enterprise 7.0 provides greater flexibility for the existing options, and adds these new options:</p> <ul style="list-style-type: none">■ At Logon■ When Idle■ Run Immediately■ Run on Dialup |
| Benefits | <p>These task scheduling options provide greater flexibility when scheduling tasks.</p> |
| Where to find | <p>For on-demand scan tasks, click Schedule on the VirusScan On-Demand Scan Properties dialog box, then select the Schedule tab of the Schedule Settings dialog box.</p> <p>For update tasks, click Schedule on the VirusScan AutoUpdate Properties dialog box, then select the Schedule tab of the Schedule Settings dialog box.</p> |

On-access scan messages

- Previous release** VirusScan 4.5.1 included the **Prompt for Action** dialog box.
- If **Prompt for Action** was selected as the action for the scanner to take when it found an infected file, the **Prompt for Action** dialog box appeared, allowing users to decide what action to take on the virus when it was discovered.
- Current release** When the on-access scanner detects an infection, the **VirusScan On-Access Scan Message** dialog box appears with the infection details. If another infection is detected, it is added to the list pane. The **On-Access Scan Message** dialog box lists all infected files detected on the system. This dialog box provides the following information:
- **Name**
 - **In Folder**
 - **Detected As**
 - **Detection Type**
 - **Status**
Details what actions were attempted and if either action was successful.
 - **Date and Time**
 - **Application**
 - **Username**
Administrator only.
 - **Client ID**
Administrator only.
- The **On-Access Scan Message** dialog box lets you select an action with command buttons such as, **Delete** or **Move**. If a command is not available, the button is disabled.
- NOTE**
In a terminal server environment, this dialog box allows administrators the ability to act on all users' files, while users are restricted to acting on their own files.
- Benefits** Provides a higher level of detail for all current on-access scan messages.

Scan options in the user interface

- Previous release** VirusScan 4.5.1 had certain scan options that you could configure in the user interface:
- **Scan exit mode**
 - **Sound alert on infection**
 - **Custom message in the prompt dialog box**
- Current release** In VirusScan Enterprise 7.0:
- **Scan exit mode**
Can be set by an administrator with a registry key.
 - **Custom message in the prompt dialog box**
Can be set in the user interface on the **Messages** tab of the **On-Access Scan Properties** dialog box. This is for on-access scans only.
- Benefits** Gives administrators greater control over the scan options.

Archive and compressed file scanning

- Previous release** The McArchive utility performed scans on archives and compressed files, but was unable to scan all types of archive and compressed files. McArchive was also only able to scan one layer deep into directories contained within archives.
- Scanning archives and compressed files were controlled by the same options.
- Current release** VirusScan Enterprise 7.0 uses the latest scanning engine to scan archives and compressed files.
- Archive scanning and compressed file scanning are no longer controlled by the same setting, but are now configured separately.
- Benefits** The latest scanning engine supports a greater number of archive formats, scans more efficiently than McArchive, and is able to scan all layers contained within archives.

Clean file scan cache

Previous release

With VirusScan 4.5.1, you could not identify files that had already been scanned. Therefore, when a scan was performed, all files (according to the configuration) were rescanned.

NetShield 4.5 for Windows NT Server and VirusScan 4.5.1 for NT Workstation identified which files had already been scanned (and had not been modified since the last scan) by using a clean file scan cache. If a file was determined to be clean, its name and attributes was stored in the clean file scan cache. A file was not scanned again until its attributes changed.

However, the clean file scan cache was small for a file server, used excessive memory, and was located in the scanner.

Current release

VirusScan Enterprise 7.0 also identifies which files have already been scanned (and have not been modified since the last scan) by using a clean file scan cache.

However, the clean file scan cache:

- Uses less memory to store each file's attributes.
- Is larger (about 1,000,000 entries).
- Is located in a driver instead of the scanner.

Benefits

Scanning performance is faster and uses fewer system resources.

With the combination of VirusScan and NetShield, several features were removed. These can be divided into two categories:

- [Administration on page 39](#)
- [Scanners and updates on page 42](#)

Administration

The following administration features were removed for VirusScan Enterprise 7.0:

- [Operating system support on page 40](#)
- [Importing and exporting tasks on page 41](#)
- [Create Emergency Disk on page 41](#)
- [DMI alerts on page 41](#)
- [Performance counters on page 42](#)

Operating system support

- Previous release** VirusScan 4.5.1 supported *workstation* platforms running these Microsoft operating systems:
- Windows 95
 - Windows 98
 - Windows ME
 - Windows NT 4.0 Workstation
 - Windows 2000 Professional
 - Windows XP
- NetShield 4.5 supported *server* platforms running these Microsoft operating systems:
- Windows NT 4.0 Server and Terminal Server
 - Windows 2000 Server and Advanced Server
- Current release** VirusScan Enterprise 7.0 supports both *workstation* and *server* platforms running these Microsoft operating systems:
- Windows NT 4.0 Workstation, Server, and Terminal Server
 - Windows 2000 Professional, Server, and Advanced Server
 - Windows XP Home and Professional
 - Windows Server 2003 RC1 (formerly known as Windows .NET)
- Benefits** One product supporting both workstation and server platforms provides:
- Consistent features, functionality, and interface.
 - Easier maintenance and support.

Importing and exporting tasks

Previous release You could import and export tasks to and from a location outside the **VirusScan Console**.

Current release Tasks cannot be imported to, or exported from a location outside of the **VirusScan Console**.

The removal of this feature was necessary for compatibility issues.

Create Emergency Disk

Previous release VirusScan 4.5.1 allowed you to create an emergency disk at any time.

Current release This is not available through VirusScan Enterprise 7.0. However, you can use the CleanBoot™ 1.0 utility, located on the product CD, to create a boot disk.

DMI alerts

Previous release You could send a desktop management interface (DMI) alert independently of Alert Manager.

Current release Alert Manager generates all alerts.

DMI is not supported by the latest version of Alert Manager.

Benefits With Alert Manager generating all alerts, you have greater control over which events generate an alert.

Performance counters

- Previous release** Both VirusScan 4.5.1 and NetShield 4.5 installed the performance counters by default.
- Current release** The performance counter files are copied to the hard drive by default, but are not installed.
- The performance counters can be installed manually.

Scanners and updates

The following scanner and update features have been removed from VirusScan Enterprise 7.0:

- [Internet Filter on page 42](#)
- [Download Scan on page 43](#)
- [Exclude action on page 43](#)
- [On-Demand Scan wizard on page 44](#)
- [AutoUpgrade on page 44](#)

Internet Filter

- Previous release** The Internet Filter was based on an outdated model. The Internet Filter blocked Java applets, ActiveX scripts, URLs, and IP addresses.
- Current release** VirusScan Enterprise 7.0 does not block Java applets or ActiveX scripts, but its on-access scanning provides equivalent scanning protection against these threats.
- URL and IP address blocking functionality is not replaced.
- Benefits** Removing the Internet Filter provides better performance and more efficient use of system resources.

Download Scan

Previous release Through Download Scan, the user could select a different set of scan options for a collection of programs (for example, browsers, or POP3 clients) that are capable of introducing new infections to a protected system.

The administrator did not have the ability to set different scanning options for different processes.

Current release The scanning engine has been extended to allow users to set different scan options for three classes of processes:

- **Default**
- **Low-Risk**
- **High-Risk**

NOTE

For more information on using these features, see [Scan options for low-risk and high-risk processes on page 21](#).

- Benefits**
- Fewer components to manage and configure.
 - Greater administrative control.
 - More control when scanning different processes.

Exclude action

Previous release VirusScan 4.5.1 and NetShield 4.5 allowed users to access files that the scanner indicated were infected. This was done by selecting **Exclude** when defining what action to take on infected files.

Current release There is no **Exclude** action available.

Benefits Eliminating this option allows less access to infected files.

On-Demand Scan wizard

- Previous release** When setting up an on-demand scan, the user could work step-by-step through the scan task setup with a wizard.
- Current release** Users set up the on-demand scan with the tabs and options provided in the **VirusScan On-Demand Scan Properties** dialog box.

AutoUpgrade

- Previous release** The AutoUpgrade component was used to update DAT files and the engine. The AutoUpgrade component was used to update HotFixes and service packs.

- Current release** AutoUpdate downloads:

- DAT files
- EXTRA.DAT files
- Scanning engines
- HotFixes
- Service packs

NOTE

Although AutoUpdate downloads HotFixes and service packs to the client computer, they must be put on the server manually. The installation to the client computer will happen automatically when AutoUpdate executes.

- Benefits** Having one feature provide all updates, gives you a more efficient product.