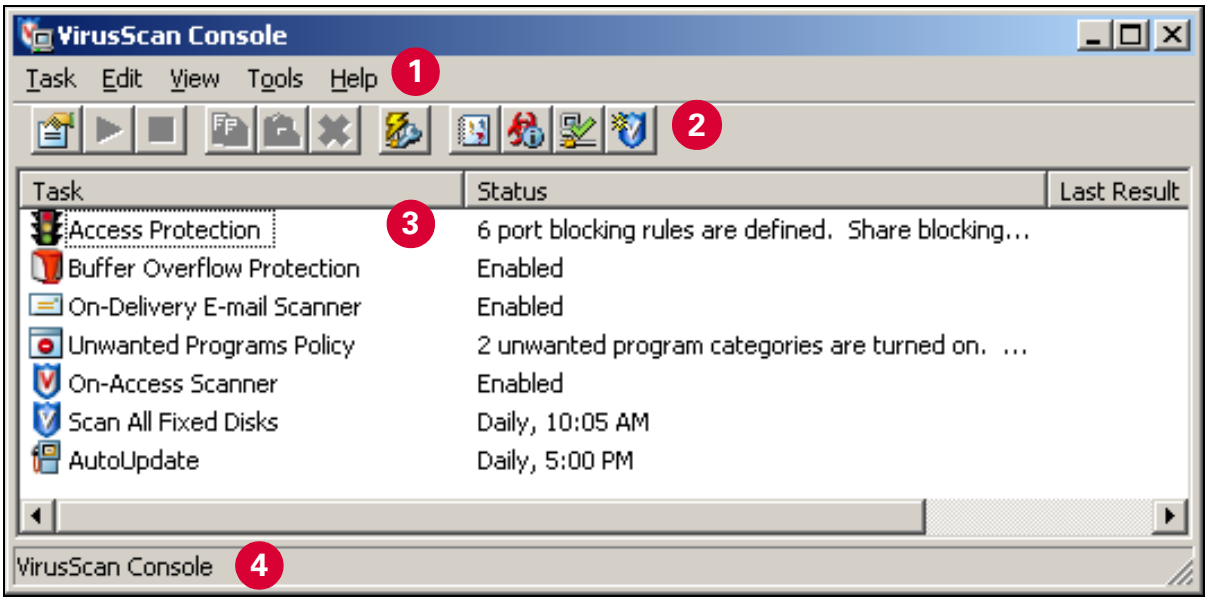
VirusScan® Enterprise version 8.0*i* Quick Reference Card

VirusScan Enterprise 8.0 integrates elements of intrusion protection and firewall technology with the product's powerful scanning capabilities to offer protection from viruses, worms, Trojan horses, and potentially unwanted code and programs.

VirusScan Console

1 **Menu bar** — Use the menu items to create tasks, configure properties, and access additional information.

- **Task** — Create and configure tasks such as scanning for threats or updating the DAT files.
- **Edit** — Copy, paste, delete, or rename the selected task.
- **View** — Display the Toolbar and/or Status bar and refresh the display.
- **Tools** — Configure user interface options, lock or unlock user interface security, enable the error reporting service, configure alerts, access the event viewier, open a remote console, import or edit the repository list, and roll back the DAT files.
- **Help** — Access online Help topics, the Virus Information Library, the Submit a Sample web site, and the Technical Support web site. You can also repair the product installation and view the About dialog box to see copyright information and which versions of the product, license, definition files, scanning engine, extra driver, and patch are installed.



2 **Toolbar** — Use the icons to access commonly used features. For example, connect to a computer, create a new on-demand scan task, display the properties of the selected task, start or stop the selected task, open the event viewer, or configure alerting options.

3 **Task list** — Displays the default tasks and any new tasks that you create as well as the status and last result for each task.

4 **Status bar** — Displays the status of the current activity.

First things to do after installing VirusScan Enterprise

We recommend that you take the following actions immediately after installing VirusScan Enterprise and before you deploy the product.

1. Establish security

Set display and password security for VirusScan Enterprise features.

To configure security options, select **User Interface Options** from the **Tools** menu in the **VirusScan Console**.

2. Update VirusScan Enterprise

Create and configure scheduled AutoUpdate tasks to keep your product, DAT files, scanning engine, and patches up-to-date. These tasks specify which items to update, when updates are performed, and which executables to run after update. You can also configure the repository list to specify the download sites from which updates are retrieved.

To configure an AutoUpdate task, open its property pages in the **VirusScan Console**.

To create a new update task, select **New Update Task** from the **Task** menu in the **VirusScan Console**.

To configure the **AutoUpdate Repository List**, select **Edit AutoUpdate Repository List** from the **Tools** menu in the **VirusScan Console.**

View the **About** dialog box to see which versions of the product, license, definition files, scanning engine, extra driver, and patch are currently installed.

To do this, select **About** from the **Help** menu in the **VirusScan Console**.

3. Prevent intrusions

Configure these features to prevent intrusions:

Buffer Overflow Protection

Block exploited buffer overflows from executing code on your computer.

Buffer Overflow Protection detects code starting to run from data in a heap or stack and prevents that code from running. It does not stop data from being written to the heap or stack. Do not rely on the exploited application remaining stable after being exploited, even if Buffer Overflow Protection stops the exploited code from running.

To configure **Buffer Overflow Protection**, open its property pages in the **VirusScan Console**.

VirusScan Enterprise protects against buffer overflows for approximately 30 of the most commonly used and exploited software applications and Microsoft Windows services. These protected applications are defined in a separate Buffer Overflow Protection Definitions (DAT) file that can be downloaded along with the Virus Definitions file during regular updates.

Access Protection

Restrict access to inbound and outbound ports as well as files, shares, and folders.

To configure **Access Protection**, open its property pages in the **VirusScan Console**.

VirusScan Enterprise comes with a number of pre-configured rules for both **Port Blocking** and **File, Share, and Folder Protection**. It is important that you review each of these rules to verify that they do not restrict access to ports, processes, programs, files, shares, or folders used by your business.

On the **Port Blocking** tab, we recommend that you:

- **Ensure that access to your e-mail client is not blocked**. For example, there is a default Port Blocking rule; Prevent mass mailing worms from sending mail, that is configured to prevent outbound processes from accessing port 25 on the network. Be sure to add your e-mail client to the **Excluded Processes** whitelist so that access is not blocked.
- **Ensure that access to any IRC communication processes you use are not blocked**. For example, there are two default Port Blocking rules that block inbound and outbound access to port 6666 through 6669. Be sure to add any IRC processes that you use to the **Excluded Processes** whitelist so that access is not blocked.

On the **File, Share, and Folder** tab, many of the pre-configured rules are set to **Warning mode**. We recommend that you use these rules in **Warning mode** for a short time, then review the log file to help determine whether to change these rules to one of the blocking modes.

Unwanted Programs Policy

Detect and take action on potentially unwanted programs, such as spyware, adware, dialers, jokes, etc.

To configure the **Unwanted Programs Policy**, open its property pages in the **VirusScan Console**. The policy you configure is enabled by default in each of the scanner's property pages. After configuring the **Unwanted Programs Policy**, go to each of the scanner's respective property pages and specify which actions you want the scanner to take when it detects an unwanted program.

You can select whole categories of programs or specific files in those categories from a pre-defined list. The pre-defined list comes from the current DAT file; the actions that can be taken on the detected program are determined by the DAT file just as they are for viruses.

For example, if you detect a program and have the primary action set to **Clean**, the DAT file attempts to clean the program using information contained in the DAT file. If the DAT file does not contain the information necessary to clean the program, the first action fails and the secondary action is taken. If you select **Delete** as the action, only the file defined as unwanted is deleted and modified registry keys may be left intact.

First things to do after installing VirusScan Enterprise (continued)

4. Detect intrusions

Configure these features to detect and take action on intrusions:

On-access scanner

Configure the **On-Access Scanner** to provide continuous, real-time scanning of files and processes as they are accessed and take action on any detections.

The per-process scanning capabilities allow you to classify specific processes as default, low-risk, or high-risk processes, then scan those processes based on the specified configuration for each type.

To determine which risk to assign to a process, follow these guidelines:

- **Decide why you want to have different scanning policies:**

  When balancing performance against risk, the two most common reasons are: 1) to scan some processes more thoroughly than the default scanning policy, and 2) to scan some processes less thoroughly than the default scanning policy based on risk and impact on performance. For example, backup applications.

- **Decide which processes are low-risk and high-risk:**

  Low-risk processes typically have a lower possibility of spreading or introducing a virus. These can be processes that access a lot of files, but do so in a way that has a lower risk of spreading viruses. For example, backup applications and compiling processes.

  High-risk processes typically have a higher possibility of spreading or introducing a virus. For example, processes that launch other processes such as Microsoft Windows Explorer or the command prompt, processes that execute scripts or macros such as WINWORD or CSCRIPT, and processes used for downloading from the Internet such as browsers, instant messengers, and mail clients.

  Default processes are any processes not defined as low-risk or high-risk processes.

When configuring the **On-Access Scanner**, you can also configure the options on these tabs:

- **ScriptScan** allows you to scan for JavaScript and VBScript scripts that are executed by the Windows Scripting Host. For example, Internet Explorer web page scripts.
- **Blocking** allows you to block connections from remote computers that have infected files in a shared folder, for a specified amount of time.
- **Unwanted Programs** allows you to specify which actions to take when an unwanted program is detected by the on-access scanner.

To configure the **On-Access Scanner**, open its property pages in the **VirusScan Console**.

On-demand scan tasks

Create and configure scheduled scan tasks to scan files and processes and take action on any detections.

When configuring an on-demand scan task, you can also configure the options on the **Unwanted Programs** tab to specify which actions to take when an unwanted program is detected by an on-demand scan.

To configure an on-demand scan task, open its property pages in the **VirusScan Console**.

To create a new on-demand task, select **New On-Demand Scan Task** from the **Task** menu in the **VirusScan Console**.

To perform an immediate scan task, right-click the VShield icon in the system tray and select **On-Demand Scan**.

E-mail scanners

Configure the **On-Delivery E-mail Scanner** and the **On-Demand E-mail Scanner** to scan Lotus Notes e-mail clients or MAPI-based e-mail clients such as Microsoft Outlook and take action on any detections. The **On-Delivery E-mail Scanner** scans e-mail as it is delivered and the **On-Demand E-mail Scanner** scans e-mail as required from within the e-mail client.

To configure the **On-Delivery E-mail Scanner**, open its property pages in the **VirusScan Console**.

To configure the **On-Demand E-mail Scanner**, open its property pages from within the e-mail client.

When configuring either the **On-Delivery E-mail Scanner** or the **On-Demand E-mail Scanner**, you can also configure the options on the **Unwanted Programs** tab to specify which actions to take when an unwanted program is detected by the e-mail scanner.

Alerts

Specify how and when you are notified when a detection occurs.

To configure **Alerts**, select it from the **Tools** menu in the **VirusScan Console**.

Getting information

Product documentation

The product documentation which provides release notes, installation, and configuration information is available in PDF format on the product CD and also on the McAfee download web site.

Links from the VirusScan Console

The **Help** menu in the **VirusScan Console** provides links to some useful resources:

Help Topics

Select **Help Topics** from the **Help** menu to access the online Help topics for the product.

Virus Information LIbrary

Select **Virus Information** from the **Help** menu to access the McAfee Anti-Virus & Vulnerability Emergency Response Team (AVERT) Virus Information Library. This web site has detailed information on where viruses come from, how they infect your system, and how to remove them.

In addition to genuine viruses, the Virus Information Library contains useful information on virus hoaxes, such as those virus warning that you receive via e-mail. A *Virtual Card For You* and *SULFNBK* are two of the best-known hoaxes, but there are many others. Next time you receive a well-meaning virus warning, view our hoax page before you pass the message on to your friends.

Submit a Sample

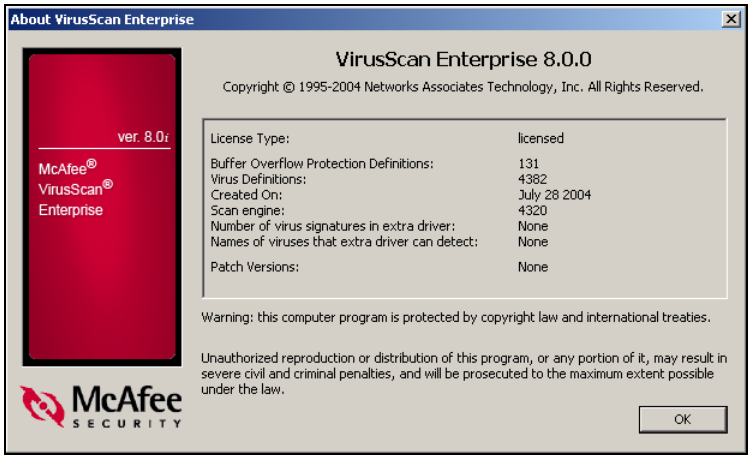
Select **Submit a Sample** from the **Help** menu to access the McAfee AVERT WebImmune web site. If you have a suspicious file that you believe contains a virus, or experience a system condition that might result from an infection, McAfee recommends that you send a sample to its anti-virus research team for analysis. Submission not only initiates an analysis, but a real-time fix, if warranted.

Technical Support

Select **Technical Support** from the **Help** menu to access the McAfee PrimeSupport KnowledgeCenter Service Portal web site. Browse this site to view frequently asked questions (FAQs), documentation, and perform a guided knowledge search.

About

Select **About** from the **Help** menu to see which versions of the product, license, definition files, scanning engine, extra driver, and patch are installed.



Copyright © 2004 Networks Associates Technology, Inc. All Rights Reserved.

Document Build 02-EN

NAI-102-0012-1