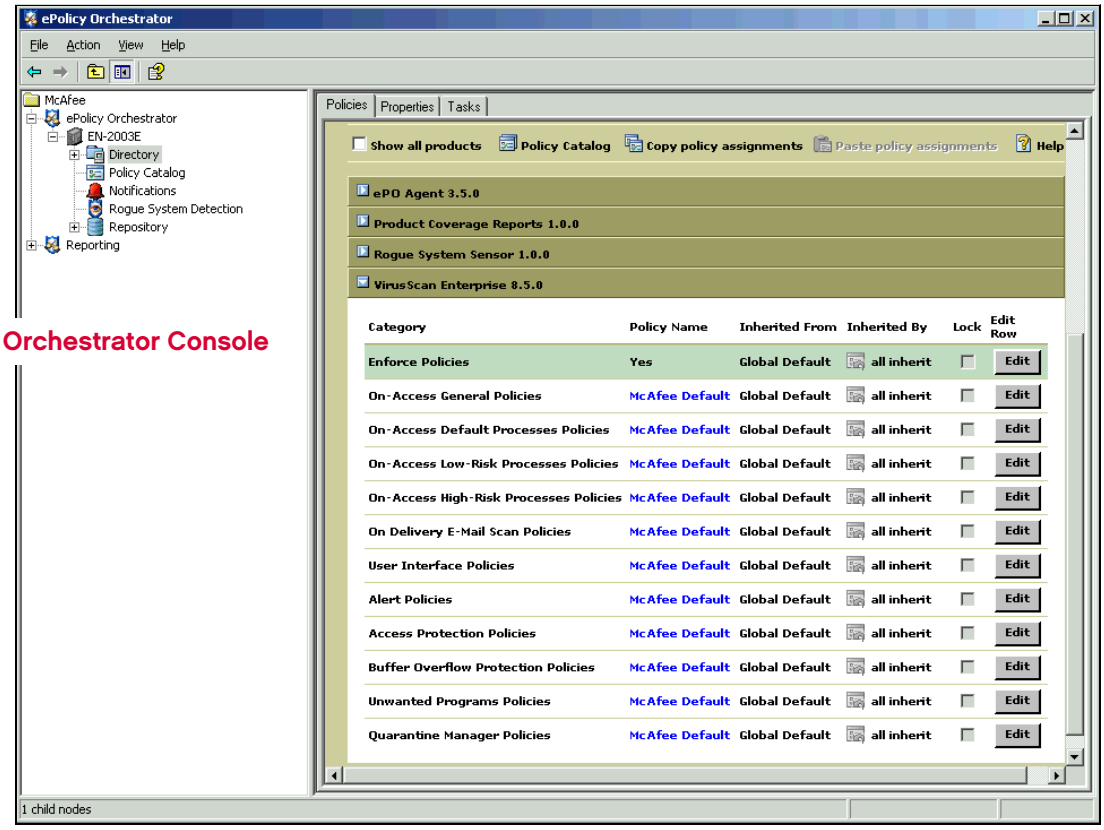
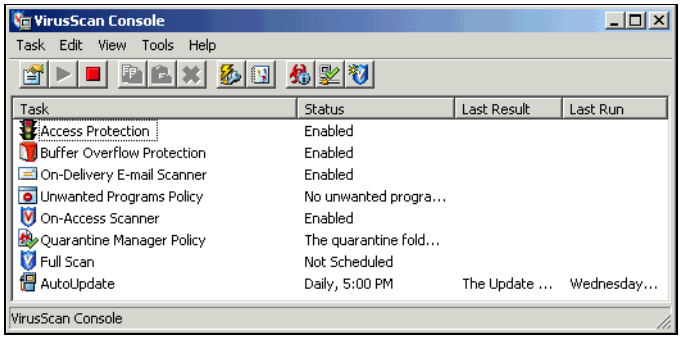
McAfee® VirusScan® Enterprise version 8.5*i* Quick Reference Card

VirusScan Enterprise integrates advanced anti-virus, firewall, and intrusion prevention technologies to protect your environment from malware, access violations, buffer overflow exploits, and blended attacks. It features advanced outbreak management responses to reduce the damage and costs of outbreaks.

Configure and manage VirusScan Enterprise via McAfee ePolicy Orchestrator® or from the VirusScan Console.



ePolicy Orchestrator Console



VirusScan Console

Features

VirusScan Enterprise 8.5*i*

Each feature plays a part in protecting your environment from potential threats.

Feature	Function
Access Protection	Uses access protection rules to protect your computer from access violations that can cause unwanted changes in your environment. Rules are categorized by the type of protection they provide; standard, maximum, and outbreak.
Alerts	Specifies which features receive messages when detections occur and if applicable, you can configure McAfee Alert Manager™.
AutoUpdate	Gets automatic updates of detection definition (DAT) files, scanning engine, and product upgrades according to the schedule you set. Use the Update Now option to perform immediate updates.
Buffer Overflow Protection	Prevents exploited buffer overflows from executing arbitrary code on your computer. This feature is not supported on 64-bit operating systems.
E-mail Scanners	Uses on-delivery or on-demand scans to examine e-mail messages, attachments, and public folders in Microsoft Outlook or Lotus Notes e-mail clients, then takes action on potential threats.
On-Access Scanner	Examines files as they are opened, copied, or saved and other scan items as they are accessed, then takes action on potential threats. Blocks connections from remote computers with potential threats in shared folders.
On-Demand Scanner	Uses scheduled or immediate scans to examine selected files, folders, and drives, then takes action on potential threats.
Quarantine Manager Policy	Specifies the length of time to keep quarantined items. Manages quarantined items by allowing the user to delete, rescan, restore, and check quarantined items for false positives.
ScriptScan	Examines JavaScript and VBScript scripts that are executed by the Scripting Host, then prevents unwanted scripts from executing.
Unwanted Programs Policy	Examines your computer for potentially unwanted programs, then takes action on potential threats.
User Interface Options	Restricts access and specifies password protection for the user interface. Specifies the preferred console language.

AntiSpyware Enterprise Module 8.5

The AntiSpyware Enterprise Module can be purchased to add on to VirusScan Enterprise. The module uses VirusScan Enterprise technology to extend its ability to detect and block adware, spyware, and other potentially unwanted programs before they threaten your environment.

Feature	Function
Access Protection	Provides additional sets of anti-spyware standard and maximums protection rules to protect the system.
E-mail Scanners	Provides additional protection against adware, spyware and other unwanted programs.
On-Access Scanner	Adds the ability to examine cookies in the cookies folder and files running in memory. Provides additional protection against adware, spyware and other unwanted programs.
On-Demand Scanner	Adds the ability to examine the registry and cookies in the cookies folder. Provides additional protection against adware, spyware and other unwanted programs.

Tasks

What to do first

When VirusScan Enterprise is installed, it is preconfigured to use the DAT files and scanning engine that were packaged with the product. Take these actions before you use the product to protect your environment:

1. Establish security

Set **User Interface Options** to password protect features, control which system tray icons are visible, and specify the preferred language for the console.

2. Update DAT files and scanning engine

Get the most current DAT files and scanning engine, then configure update tasks to get regular updates:

- Perform an immediate **AutoUpdate** or **Update Now** task to get the most current DAT files and scanning engine.
- Create and configure **AutoUpdate** tasks.
- If you don't want to use the McAfee default update site, you can configure the **AutoUpdate Repository List** to specify sites from which you retrieve updates.

McAfee provides daily DAT updates to ensure that your desktops and file servers have the most up-to-date detection and prevention.

3. Configure all other features

- Access Protection
- Buffer Overflow Protection
- Unwanted Programs Policy
- On-Access Scanner
- On-Demand Scan Tasks
- E-mail Scanner
- Quarantine Manager Policy
- Alerts

When using ePolicy Orchestrator to manage the product, you can configure separate policies for servers and workstations.

What to do next

After initially configuring the product, perform these tasks:

1. Monitor activity

Review alerts, logs, scan statistics, quarantined items, and if applicable, ePolicy Orchestrator reports, to determine:

- What was detected.
- What actions were taken.

2. Evaluate protection

Evaluate detection activity to determine:

- If potential threats were detected.
- If appropriate action was taken on detections.

3. Submit samples to Avert® Labs

Submit samples of false positives or potential threats that were not detected to Avert Labs WebImmune for analysis:

https:/ /www.webimmune.net/default.asp

4. Adjust configuration settings

If necessary, fine tune your configuration settings. For example:

- Access Protection:

  Edit rules to specify inclusions for items that you want to detect.

  Edit rules to specify exclusions for items that you legitimately use.

  Create new rules as necessary.

- Buffer Overflow Protection

  Create exclusions for detected processes that you legitimately use.

- Unwanted Programs Policy:

  Create exclusions for detected programs that you legitimately use.

- On-Access, On-Demand, and E-mail Scanners:

  Specify additional items that you want to detect.

  Create exclusions for detected items that you legitimately use.

  Adjust actions as necessary.

Information

Getting information

Where to go for threat information, product documentation, and technical support.

Threat Center

McAfee Avert® Labs helps you maintain the highest possible level of security. 100 researchers in 14 countries continuously monitor the latest threats and provide remediation, so that you can stay ahead of the latest threats and respond quickly to emergencies.

http://www.mcafee.com/us/threat_center/default.asp

Documentation

Product documentation is available in PDF format at:

http://www.mcafee.com/us/enterprise/downloads/index.html

VirusScan Enterprise 8.5*i*

Release Notes, Product Guide, Installation Guide, Configuration Guide, and Quick Reference Card.

AntiSpyware Enterprise Module 8.5

Release Notes and Product Guide.

ePolicy Orchestrator® 3.5 or later

Release Notes, Product Guide, Installation Guide, Hardware Sizing and Bandwidth Usage Guide, Reporting Guide, Walkthrough Guide, and Quick Reference Card.

ProtectionPilot® 1.5 or later

Release Notes, Product Guide, and Installation Guide.

Enterprise Support

Customer Care for the business user. Access websites for customer service and technical support.

http://www.mcafee.com/us/enterprise/support/index.html

VirusScan Enterprise About dialog box

License and product information.