

Release Notes for
McAfee(R) VirusScan (R) Enterprise
Version 8.5i plus Patch
Copyright (C) 2007 McAfee, Inc.
All Rights Reserved

=====
- DAT Version: 4893
- Engine Version: 5100.194
=====

Thank you for using VirusScan(R) Enterprise software. This file contains important information regarding this release. We strongly recommend that you read the entire document.

IMPORTANT:

McAfee does not support automatic upgrading of a pre-release version of the software. To upgrade to a later beta release, a release candidate, or a production release of the software, you must first uninstall the existing version of the software.

WHAT'S IN THIS FILE

- Introduction
- Product License
- Installation & System Requirements
- Testing Your Installation
- Resolved Issues
- Known Issues
 - Installing, Upgrading, and Uninstalling
 - Language Support
 - Compatibility with Other Products
 - Alert Manager(TM)
 - AntiSpyware Enterprise Standalone
 - ePolicy Orchestrator(R)
 - ePolicy Orchestrator Agent
 - McAfee Installation Designer(TM)
 - Microsoft Windows Vista
 - PreScan
 - ProtectionPilot(TM)
 - GroupShield(TM)
 - Spy Sweeper
 - Access Protection
 - Adding File Type Extensions
 - AutoUpdate
 - Buffer Overflow Protection
 - E-mail Scanning
 - On-Delivery E-mail Scanning
 - Lotus Notes Scanning
 - Help File
 - Log File Format
 - Mirror Tasks
 - Preserving Settings

- Unwanted Programs Policy
- Documentation
- Participating in the McAfee Beta Program
- Contact Information
- Copyright & Trademark Attributions
- License & Patent Information

INTRODUCTION

McAfee VirusScan Enterprise protects your desktop and file servers from a wide range of threats, including viruses, worms, Trojan horses, and potentially unwanted code and programs. This version provides these new or improved features:

- Support for 64-bit operating systems.

NOTE:

These features or products are not supported on 64-bit operating systems:

- Buffer Overflow Protection.
- Scanning of Lotus Notes databases.
- Alert Manager 4.7.1.
- Support for Microsoft windows Vista operating systems.
- Quarantine Manager Policy. Configure a policy to manage quarantined items. Before the on-access or on-demand scanner cleans or deletes a file, it creates a backup copy of the original file and registry value in the quarantine directory. These backed-up items can be automatically deleted after a specified number of days. You can also selectively restore, delete, and rescan quarantined items.
- 5100 series scanning engine. This product release provides these engine enhancements:
 - Component engine updates. Allows for updating new engine features between major engine releases. The engine version, displayed in the VirusScan Enterprise "About" dialog box, shows both the engine series and the latest incremental update version. For example, 5100.0194.
 - Two versions of the 5100 series engine; a 32-bit version and a 64-bit version. The VirusScan Enterprise About dialog box displays the 32-bit engine version number and if the 64-bit engine is used, it also displays the 64-bit engine version number.
 - Detection of rootkits in memory. The on-demand scanner can be configured to scan system memory for installed rootkits. Rootkits conceal running processes and files or system data, and are a threat if an intruder uses the rootkit to

maintain access to a system without the user's knowledge.

- Enhanced Access Protection. This feature prevents unwanted changes by restricting access to specified ports, files and folders, shares, registry keys and values. The rules have been enhanced to expand exclusion capability and provide better protection:
 - Access Protection rule configuration options include "Processes to include" and "Processes to exclude." See the Access Protection section of the VirusScan Enterprise Product Guide for details.
 - Rules have been separated into Anti-virus, Common, Outbreak, and User-defined categories.
 - Protection levels. When you install the product, you choose whether to enable "Standard Protection" or "Maximum Protection" rules as the default.
 - Standard Protection. Anti-virus and common rules that protect some critical settings and files from modification, but generally allow installation and execution of legitimate software.
 - Maximum Protection. Anti-virus and common rules that protect most critical settings and files from modification. These rules provide more protection, but might also prevent you from installing software. If you are prevented from installing legitimate software, we recommend that you disable the Access Protection feature before installing software, then enable it again after installation.

You can change which rules are enabled and disabled after VirusScan Enterprise is installed.

PRODUCT LICENSE

These time limits apply to these VirusScan Enterprise 8.5i product licenses:

- The Beta 4 license expires on December 31, 2006.
- The Evaluation license expires 90 days after installing the evaluation version of the product.

INSTALLATION AND SYSTEM REQUIREMENTS

Please see the product documentation for complete information on installation and system requirements.

TESTING YOUR INSTALLATION

You can test the operation of the software by running the EICAR Standard AntiVirus Test File on any computer where you have installed the software. The EICAR Standard AntiVirus Test File is a combined effort by anti-virus vendors throughout the world to implement one standard by which customers can verify their anti-virus installations.

To test your installation:

1. Copy the following line into its own file, making sure you do not include any spaces or line breaks. Save the file with the name EICAR.COM.

```
X50!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

The file size will be 68 or 70 bytes.

2. Start your anti-virus software and allow it to scan the directory that contains EICAR.COM.

When your software scans this file, it will report finding the EICAR test file.

3. Delete the file when you have finished testing your installation to avoid alarming unsuspecting users.

IMPORTANT:

Please note that this file is NOT A VIRUS.

For more information on the EICAR test file, visit:

<http://www.eicar.org>

RESOLVED ISSUES

The following list describes issues from the previous release of this software product that have been resolved with this current release.

1. **ISSUE:**
When you upgrade from VirusScan Enterprise 7.1 or 8.0i to version 8.5i and choose to preserve settings, previously created console tasks do not display in the VirusScan console.

RESOLUTION:

The VirusScan Enterprise installation package has been updated to properly initialize previously created console tasks so they display

in the VirusScan console when preserving settings during the product upgrade.

2. ISSUE:

When you upgrade from VirusScan Enterprise 7.1 or 8.0i to version 8.5i, the older version of the Check Point .DLL is not automatically upgraded. This results in failures as noted in the Check Point VPN compliance reports.

RESOLUTION:

The VirusScan Enterprise installation package has been updated to unregister the older Check Point .DLL before upgrading to the new version of the Check Point .DLL that is included in the VirusScan Enterprise 8.5i installation package.

3. ISSUE:

When you use McAfee Installation Designer 8.5 to create a custom installation package that includes a VirusScan Enterprise 8.5i Patch, then attempt to install the package, the installation fails.

RESOLUTION:

The VirusScan Enterprise installation executable has been updated to increase the buffer size of the code that handles Patch installation.

4. ISSUE:

When you upgrade to VirusScan Enterprise 8.5i in ePolicy Orchestrator, the ePolicy Orchestrator migration tool did not properly port over access protection exclusions.

RESOLUTION:

The ePolicy Orchestrator migration tool has been updated to no longer place quotes around the entire exclusion string when porting over access protection exclusions.

5. ISSUE:

When you upgrade to VirusScan Enterprise 8.5i in ePolicy Orchestrator, the ePolicy Orchestrator migration tool did not properly port over on-demand scan tasks.

RESOLUTION:

The ePolicy Orchestrator migration tool has been updated to solve SQL script issues so that on-demand tasks are properly ported over.

6. ISSUE:

When installing VirusScan Enterprise, the Universal Uninstaller program removes non-McAfee anti-virus products from your system. The Universal Uninstaller program included in the VirusScan Enterprise 8.5i installation package did not remove the most current versions of non-McAfee anti-virus products.

RESOLUTION:

New scripts have been added to the Universal
Page 5

Uninstaller program to support removal of newer versions of non-McAfee anti-virus products.

NOTE:

Some 64-bit versions of non-McAfee anti-virus products may not be removed due to security rights on the operating system.

7. ISSUE:

A runtime error occurs when users without administrative rights run on-demand scan tasks.

RESOLUTION:

A new version of the ePolicy Orchestrator Agent is included with this release to resolve this issue.

KNOWN ISSUES

INSTALLING, UPGRADING, AND UNINSTALLING

1. To install the VirusScan Enterprise product using MSIEXEC.EXE, complete these steps:

- a. Extract the .MSI and other files by entering this command at the command prompt:

```
SETUP.EXE -nos_ne [-nos_o"<output path>"]
```

NOTES:

The -nos_ne command extracts the setup files from the SETUP.EXE, but does not execute the SETUP.EXE or delete the setup files.

The -nos_o"<output path>" command specifies the folder to which you want to extract the setup files.

If you do not specify the output path, the files are extracted to the user profile's "Temp" folder.

- b. Ensure that any competitor's products are removed including previous versions of McAfee VirusScan and VirusScan Enterprise.
- c. To inject localized strings into the MSI before installing the product, enter this command at the command prompt:

```
"setupvse.exe /IMPORTMSISTRINGS"
```

- d. Run MSIEXEC.EXE by entering this command at the command prompt:

```
"msiexec.exe /i vse850.msi"
```

2. When installing Buffer Overflow Protection, these limitations apply:

Readme_EN.txt

- If Buffer Overflow Protection is installed on a computer that already has the McAfee Enterecept or Host Intrusion Prevention agent installed on it, the Buffer Overflow Protection feature is disabled in the VirusScan Console.

NOTE:

The McAfee Enterecept or Host Intrusion Prevention products provide more complete coverage, so they take precedence over the Buffer Overflow Protection feature in VirusScan Enterprise.

- Buffer Overflow Protection cannot be installed on 64-bit or Microsoft windows Vista operating systems.

3. When installing VirusScan Enterprise 8.5i via the command line, the property for choosing "Standard Protection" or "Maximum Protection" is "PROTECTIONTYPE." Standard Protection is installed by default. To silently install Maximum Protection rules, use this command:

```
Setup.exe PROTECTIONTYPE=Maximum /q
```

This command-line property is not documented in the VirusScan Enterprise 8.5i Installation Guide.

4. This release supports deployment using Administration Installation Points (AIP). However, you must run SETUPVSE.EXE from the AIP to perform upgrades or to uninstall other anti-virus software.

To create an AIP, type "setup.exe /a" at the command prompt. A wizard appears to take you through the process of creating the AIP. When the AIP is created, all of the necessary files in the compressed (.ZIP) file are also copied to the AIP. These files are:

- SETUPVSE.EXE
- MSISTRINGS.BIN
- SETUP.INI
- UNINST.DLL
- UNINST.INI
- VSE850.MSI
- WINDOWSINSTALLER-KB893803-V2-X86.EXE

Since these files are automatically copied to the AIP, the administrator does not need to manually copy the files.

NOTE:

If you deploy VirusScan Enterprise via Active Directory group policies, which install using MSIEXEC.EXE, you must remove any existing anti-virus products prior to installing VirusScan Enterprise.

5. When silently over-installing the Computer Associates eTrust Antivirus program, the action is not completely silent. The Computer Associates eTrust Antivirus program displays a message box stating that a restart is needed with an "OK" button. Once you click "OK", the over-installation continues normally. This problem is a known Computer Associates problem referenced on the Computer Associates' web site under article Q019636. The web site provides a downloadable file that fixes this problem. The problem references Computer Associates eTrust Antivirus version 6.0, but the fix also works for version 7.0.

LANGUAGE SUPPORT

1. The language displayed in the update task progress dialog box and the "Edit AutoUpdate Repository List" dialog box does not match the preferred language in the VirusScan Console. Setting the preferred language in the console to another language does not fix this issue because the AutoUpdate task and related dialog boxes retain the system language.

When using ePolicy Orchestrator to manage VirusScan Enterprise 8.5i, you can correct this issue by checking the ePolicy Orchestrator Agent language pack in and deploying it to client computers.

2. The language displayed when accessing right-click scan and the Microsoft Outlook or Lotus Notes On-Demand Scan Properties dialog box does not match the preferred language in the VirusScan Console. Setting the preferred language in the console to another language does not fix this issue because these features retain the system language. See KB Article 1935692 for information about displayed language.
3. VirusScan Enterprise 8.5i user interface text may appear to be corrupted when viewing an Asian version of the product on an operating system that does not have Asian fonts installed. To correct the issue, install Asian fonts on the operating system.

COMPATIBILITY WITH OTHER PRODUCTS

Alert Manager

1. VirusScan Enterprise 8.5i can only send alerts to Alert Manager 4.7.x. It cannot send alerts to earlier versions of Alert Manager.

Furthermore, VirusScan Enterprise 8.5i cannot be installed on a computer where an Alert Manager version earlier than 4.7.x is already installed. If you are installing VirusScan Enterprise onto

a system where Alert Manager 4.5 or 4.6 is installed, you should also install Alert Manager 4.7.x, which automatically replaces the older version of Alert Manager.

However, also note that Alert Manager 4.7.x can receive alerts from earlier versions of NetShield and VirusScan. You can configure earlier versions of these software programs to send alerts to an installation of Alert Manager 4.7.x.

AntiSpyware Enterprise Standalone

1. When using ePolicy Orchestrator to install VirusScan Enterprise 8.5i over AntiSpyware Enterprise Standalone 8.5, you must restart the client computer after VirusScan Enterprise is installed.

ePolicy Orchestrator

1. This version of VirusScan Enterprise 8.5i is compatible with ePolicy Orchestrator version 3.5.0 or later. The ePolicy Orchestrator Agent version 3.6 or later must be deployed to client computers before you deploy VirusScan Enterprise.
2. If you are using ePolicy Orchestrator 3.5 or 3.6 to manage the VirusScan Enterprise beta release, you must add the most current ePolicy Orchestrator Agent NAP file (CMA360.NAP) to the ePolicy Orchestrator repository, then deploy it to client computers before you deploy the VirusScan Enterprise 8.5i product.

NOTE:

The CMA360.NAP file is available from the McAfee download web site.

3. This version of VirusScan Enterprise 8.5i provides two .NAP files that must be added to the ePolicy Orchestrator repository. These files are included in the VirusScan Enterprise 8.5i installation package and can be found in the location where you downloaded the files:
 - VSE850.NAP.
 - VSE850REPORTS.NAP. This file is an extended reports .NAP file.
4. To install the VSE850REPORTS.NAP file to the repository:
 - a. Use the ePolicy Orchestrator Check-In wizard to add the VSE850Reports.NAP file to the repository.
 - b. If applicable, log out of the Reporting

console.

- c. In the ePolicy Orchestrator installation directory, delete REPORTVERSIONS.SQL file from the AVI directory.
- d. Log in to the Reporting Console using "ePO Authentication."
- e. Click "Yes" to download the new reports.

NOTE:

Repeat steps b through e for every computer running the remote ePolicy Orchestrator Console.

5. To preserve settings when upgrading to VirusScan Enterprise 8.5i, run the "ePOPolicyMigration.exe" file that is included in the installation package.
 - a. Add the VSE850.NAP file to the ePolicy Orchestrator repository.
 - b. Run the ePOPolicyMigration.exe on the server where ePolicy Orchestrator is installed.
6. If you are using Microsoft SQL Server version 7.0 with ePolicy Orchestrator 3.5 or later, on-demand scan tasks are not preserved when you run ePOPolicyMigration.exe. You must have Microsoft SQL Server version 2000 or later installed to preserve on-demand scan tasks.
7. ePolicy Orchestrator reports are affected by an issue where DAT and engine version numbers display in different formats. The version number format varies depending on which ePolicy Orchestrator agent is being used, which product the system property is collected from, and whether ePolicy Orchestrator converts the format when it reads the property. For example,

DAT version may be displayed in any of these formats:

- 4.0.4841
- 4841.000
- 4841

Engine version may be displayed in either of these formats:

- 5.1.0002
- 5100.0194

This difference in formats affects any ePolicy Orchestrator reports or queries that compare the DAT and/or engine values, such as the Compliance Issues and DAT/Engine Coverage reports. For example, a computer with a DAT system property of 4.0.4841 fails compliance when compared to systems with the 4841.000 DAT file because ePolicy Orchestrator doesn't recognize the versions to be the same.

This issue has been fixed in ePolicy Orchestrator 3.5 Patch 7 or later and ePolicy Orchestrator 3.6 Patch 4 or later.

If you are using ePolicy Orchestrator 3.5 or 3.6.0, you can use report filters to select DAT and engine version numbers that match. For example, to ascertain compliance of computers with the 4841 DAT file, you must run the Compliance Issues report with a filter for 4.0.4841, then run it again with a filter for 4841.000, then once again with a filter for 4841 if that format is used as well. See the ePolicy Orchestrator documentation and KB Article 5263068 for more information.

NOTE:

You cannot filter the Compliance Issues report to display compliance with the 64-bit engine property. All computers with the 64-bit engine are also reported as computers with a 32-bit engine.

8. When you check a new DAT file that contains changes to access protection rules into the ePolicy Orchestrator repository, the changed rules do not appear in the Access Protection Policies. You must install ePolicy Orchestrator 3.6.0 Patch 2a or later to resolve this issue.
9. A replicated repository may be blocked if the Access Protection Properties for the "Prevent remote creation/modification of executable and configuration files" rule are set to "Block." The rule is set to "Report" by default.
10. A replicated repository may become corrupted when replicating via UNC from an ePolicy Orchestrator server to a server that has this file blocking rule enabled in the Access Protection Properties:

"Prevent remote creation/modification of executable and configuration files"

When this rule is set to "Block", some file replications are blocked because the ePolicy Orchestrator server remotely opens the files for write access and modifies their contents in the same way that a share-hopping worm performs.

If you plan to replicate a repository via UNC from an ePolicy Orchestrator server, be certain to disable file blocking rules on the target server before you perform the replication.

11. The ePolicy Orchestrator compliance baseline does not recalculate compliance when you remove items from the repository.

For example, when you check VirusScan Enterprise 8.5i into the ePolicy Orchestrator repository,

Readme_EN.txt

it is flagged as the new compliance baseline for the environment. All computers with VirusScan Enterprise versions earlier than 8.5i are flagged as non-compliant. However, if you remove VirusScan Enterprise 8.5i from the repository, rather than recalculate compliance, the compliance baseline remains at version 8.5i. The compliance baseline only increases incrementally, even if you re-check VirusScan Enterprise 8.0i into the repository.

12. The English description for VirusScan Enterprise 8.5i may not be available in the ePolicy Orchestrator Repository under Managed Products | Windows | VirusScan Enterprise | 8.5.0 depending on the order in which you installed the two VirusScan Enterprise 8.5i .NAP files.
 - If you installed the VSE850.NAP to the Repository before you installed the VSE850REPORTS.NAP, the English description is not available.
 - If you installed the VSE850REPORTS.NAP before you installed the VSE850.NAP, the English description is available.

ePolicy Orchestrator Agent

1. If you are using ePolicy Orchestrator to manage VirusScan Enterprise 8.5i, you must also use ePolicy Orchestrator Agent version 3.6 or later.

NOTE:

Do not push an ePolicy Orchestrator Agent version 3.5.x to a system where VirusScan Enterprise was installed by a third party deployment tool or local installation.

2. Unrelated error message in agent log. When using ePolicy Orchestrator to install VirusScan Enterprise on client computers from, you may receive an unrelated error message in the agent log. The message states "Can't get the installed language for VIRUSSCAN8600." This message is misleading; it should state that the version of the currently installed ePolicy Orchestrator agent is not supported with this version of VirusScan Enterprise. VirusScan Enterprise 8.5i requires ePolicy Orchestrator Agent version 3.6 or later.

McAfee Installation Designer

1. This version of VirusScan Enterprise 8.5i is compatible with McAfee Installation Designer version 8.5 or later. It is not compatible with earlier versions.

Microsoft windows Vista

1. Before remotely connecting to a computer with the windows Vista operating system, you must complete these steps:
 - a. From the computer with the windows Vista operating system, modify the windows Firewall settings to allow "Remote Service Management" as follows:
 - From the "Start" menu, select "Control Panel | Security | Windows Firewall | Change settings"
 - On the "User Account Control" dialog box, click "Continue."
 - On the "Exception" tab, select "Remote Service Management" on the "Program or port" list.
 - b. Start the "Remote Registry" service on the target computer with the Microsoft windows Vista operating system, before remotely connecting to it. To start the "Remote Registry" service:
 - From the "Start" menu, select "Control Panel | Administrative Tools | Services."
 - If the "User Account Control" dialog box is available, click "Continue."
 - Ensure the status of the "Remote Registry" service is "Started." If necessary, start the service.

We recommend that you stop the "Remote Registry" service on windows Vista after completing the remote configuration.

2. When using the "Browse" option to connect to a remote console with the windows Vista operating system, the list of computers does not display for a long period of time or at all. If the list does appear, you can select a computer, but the "OK" button is disabled so the connection cannot be made.

You can make a remote connection to the console of other computers by specifying the full computer name or the IP address of the computer to which you want to remotely connect.

3. When running update or mirror tasks from the VirusScan Console on a system using windows Vista, the task progress dialog box does not display while the task is running. However, the task completes successfully. You can view information about the task in the activity log.
4. When a connection is blocked in a share folder on a computer with the windows Vista operating system, the blocked connection cannot be unblocked using the "Unblock All Connections Now" button in the On-Access Scan Statistics

dialog box. The "Unblock All Connections Now" button is disabled in this scenario.

The blocked connection will be unblocked after the default time out.

5. Buffer Overflow Protection is not supported on Microsoft Windows Vista operating systems.

PreScan

1. McAfee PreScan 1.0 Service Pack 1 or earlier versions are not compatible with VirusScan Enterprise 8.5. Refer to KB Articles KB4095245 and KB7675743 for more details.

ProtectionPilot

1. This version of VirusScan Enterprise 8.5i is compatible with ProtectionPilot version 1.5 or later. It is not compatible with earlier versions.

GroupShield

1. If you plan to use GroupShield in addition to VirusScan Enterprise 8.5i and Alert Manager 4.7.1, be certain to install GroupShield before you install Alert Manager. This installation sequence is required to ensure alerting works correctly.

Spy Sweeper

1. Spy Sweeper. If you are using Spy Sweeper to scan the VirusScan Enterprise installation folder, a false detection occurs when it detects BHO.DLL. This file is not spyware; it is a component of ScriptScan that is installed as part of VirusScan Enterprise.

ACCESS PROTECTION

1. On a dual boot system, the "Prevent Windows Process spoofing" rule may return a false alarm on the windows files from other windows installations.
2. The "Prevent McAfee services from being stopped" feature is not supported on 64-bit operating systems.
3. If you have unexpected issues with blocked accesses, review the actions set for access protection rules. For example, if the "Prevent remote creation/modification of executable and configuration files" rule is set to "Block", you are prevented from replicating the ePolicy

Orchestrator repository.

ADDING FILE TYPE EXTENSIONS

1. If you are using wildcards to specify file type extensions in either the Additional File Types or Specified File Types dialog boxes, you cannot use an asterisk (*) as the wildcard. You must use a question mark (?) as the wildcard when specifying file type extensions in these scenarios.

AUTOUPDATE

1. Updating from a mapped drive only works if you are logged on when the update occurs and you have at least read rights to that mapped drive location. If no one is logged on to the system, or if you are logged on but do not have at least read rights to the mapped location, the update fails.
2. When editing the repository list to use a UNC path, the "Edit AutoUpdate Repository List" dialog box does not validate that the path entered is a valid UNC share before accepting it. Be sure that you enter a valid UNC server, share, and path name. Entering an invalid UNC path could cause problems when updating from this location.
3. If you are using content scanning and filtering software on your network, you may experience some problems with updating. This can occur if your content filtering software modifies a McAfee update package.

BUFFER OVERFLOW PROTECTION

1. When the Sasser worm or any other malware that uses MS04-011 infects your system, the infection may result in an exploited buffer overflow. The Buffer Overflow Protection feature can detect and prevent the buffer overflow code from executing on your computer. Although the execution of malicious code is prevented, the actual buffer overflow is not stopped. If a buffer overflow occurs as a result of the Sasser worm, the LSASS.EXE becomes unstable and the computer automatically restarts.
2. The Buffer Overflow Protection feature is not supported on 64-bit or Microsoft Windows Vista operating systems.
3. The Buffer Overflow Protection feature cannot be installed on a system that already has the Cisco Security Agent installed on it.

E-MAIL SCANNING

On-Delivery E-mail Scanning

4. When Microsoft Outlook is configured to deliver new e-mail to a personal folder and rules are used to move e-mails, the on-delivery scanner may not detect infected e-mails. We do not recommend that you configure Microsoft Outlook to deliver new e-mails to a personal folder if you use rules to move e-mails to other folders in Microsoft Outlook.

Lotus Notes Scanning

1. Lotus Notes Scanning is not supported on Microsoft Vista operating systems.
2. If you exclude the "Lotus Notes E-mail Scanner" feature when you use the Setup utility to perform a custom installation of VirusScan Enterprise, you cannot use the Setup utility to later add the "Lotus Notes E-mail Scanner" feature. You must install Lotus Notes manually.
3. Prompting for a password from other Notes-based programs reduces security. When accessing a local database on Windows 2000 Server, Windows 2003 Server, or Windows XP, the user is prompted for a password. When the user types the password, the text search dialog is initiated and the password is inserted into the text search dialog instead of being inserted into the password dialog. The password dialog box is not completely modal. Selecting the dialog box again allows the user to input the password.

When using Lotus Client Release version 6 or later, we recommend that you prevent prompts for passwords as follows:

- a. From Lotus Notes, select File | Preferences | Security | User Security | Dialog.
- b. Select "Don't prompt for a password from other Notes-based programs (reduces security)."

NOTE:

This option is not available on other versions of the Lotus Client.

4. Notes Scanner appears to slow Lotus Notes down significantly when using VPN. For each note item the user accesses, Lotus Notes reads it then the Notes scanner reads it a second time. Users do not realize that each item is accessed twice so they perceive performance is twice as slow, when in fact it is normal.

HELP FILE

1. The Help file is provided as a downloadable file. Download it automatically the first time you access "Help" from VirusScan Enterprise. Click "Help" in any dialog box or select it from the "Tools" menu in the VirusScan Console.

If you are using ePolicy Orchestrator to manage VirusScan Enterprise, the Help file must be present in the ePolicy Orchestrator repository before it can be deployed to client computers. The Help file is available in VirusScan Enterprise product package that is available on the McAfee download web site and the product CD.

LOG FILE FORMAT

1. The default format for the log files is Unicode UTF8 except when installing Virus Enterprise 8.5i on Windows NT operating systems. The default format for log files on Windows NT operating systems is ANSI.

MIRROR TASKS

1. If you are using a VirusScan Enterprise 8.5i mirror task to mirror the NAIFTP site, the task may fail in two ways.
 - First, the task does not mirror 100% of the files on the FTP site. For example, if a file is missing on the NAIFTP site, the task does not replicate anything other than the "current" folder.
 - Second, if you configured the schedule to do so, it will execute the task again, but will not execute any programs that were specified to run after successful completion of the task.

NOTE:

If the scheduled mirror task is manually executed in this scenario, the programs that are specified to run after successful completion of the task will run.

We recommend that you use McAfee AutoUpdate Architect to create a task to mirror the NAIFTP site.

PRESERVING SETTINGS

1. Settings can be preserved when upgrading VirusScan Enterprise from an earlier version to version 8.5i:
 - When using the VirusScan Enterprise Setup utility to install the product, select the "Preserve Settings" option. See the VirusScan

Readme_EN.txt

Enterprise Installation Guide for details.

- When using ePolicy Orchestrator, run the "ePOPolicyMigration.exe" file that is included in the installation package.
 - Add the VSE850.NAP file to the ePolicy Orchestrator repository.
 - Run the ePOPolicyMigration.exe on the server where ePolicy Orchestrator is installed.
- 2. The path to the previous product's installation directory is not preserved even though you select the "Preserve Settings" option. VirusScan Enterprise 8.5i is installed to %Program Files%\McAfee\VirusScan by default unless a different installation path is specified.

UNWANTED PROGRAMS POLICY

1. wildcards are not supported when configuring user-defined unwanted programs.

DOCUMENTATION

Documentation is included on the product CD and/or is available with a valid grant number from the McAfee download site:

<https://secure.nai.com/us/forms/downloads/upgrades/login.asp>

NOTE:

Unless otherwise noted, product documentation comes as Adobe Acrobat .PDF files. The product CD includes the latest version of Acrobat Reader, or you can download any version from the Adobe web site:

<http://www.adobe.com/products/acrobat/readstep2.html>

STANDARD DOCUMENTATION

This product includes the following documentation set:

- Installation Guide
System requirements and instructions for installing and starting the software.
- Product Guide
Introduction to the product and its features; detailed instructions for configuring the software; information on deployment, recurring tasks, and operating procedures.
- Help

Readme_EN.txt

High-level and detailed information accessed from the software application: Help menu and/or Help button for page-level help.

- Configuration Guide
For use with ePolicy Orchestrator(R) management software. Procedures for deploying and managing supported products through the ePolicy Orchestrator management software.
- Release Notes (this ReadMe file)
- LICENSE Agreement
The McAfee License Agreement booklet that includes all of the license types you can purchase for your product. The License Agreement presents general terms and conditions for use of the licensed product.

ADDITIONAL DOCUMENTATION

- Quick Reference Card
A handy card with information on basic product features, routine tasks that you perform often, and critical tasks that you perform occasionally. A printed card accompanies the product CD.

SUPPLEMENTAL DOCUMENTATION

- ePolicy Orchestrator(R) 3.5 or later version documentation set.
- ProtectionPilot(TM) 1.5 documentation set.
- McAfee Installation Designer(TM) 8.5 documentation set.
- Alert Manager(TM) 4.7.1 documentation set.

PARTICIPATING IN THE MCAFEE BETA PROGRAM

To download new beta software or to read about the latest beta information, visit the McAfee beta web site located at:

<http://www.mcafeesecurity.com/us/downloads/beta/mcafeebetahome.htm>

To submit beta feedback on any McAfee product, send e-mail to:

mcafee_beta@mcafee.com

McAfee is devoted to providing solutions based on your input.

CONTACT INFORMATION

THREAT CENTER: Avert(R) Labs

Home Page

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

Avert Labs Threat Library

<http://vil.nai.com/>

Avert WebImmune & Submit a Sample (Logon
credentials required)

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

Avert DAT Notification Service

http://vil.nai.com/vil/signup_DAT_notification.aspx

DOWNLOAD SITE

Home Page

<http://www.mcafee.com/us/downloads/>

Security Updates (Click "Check for updates")

- Enterprise:

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

- Small & Medium Business:

<http://www.mcafee.com/us/smb/downloads/index.html>

Anti-Spam Rules File and Engine Updates

<ftp://ftp.mcafee.com/spamdefs/1.x/>

Product Upgrades (Valid grant number required)

- Enterprise:

https://mcafee.com/apps/downloads/my_products/login.asp

- Small & Medium Business:

<http://www.mcafee.com/us/smb/downloads/index.html> (Click "Login")

HotFix and Patch Releases for Security
Vulnerabilities (Available to the public)

- Enterprise:

http://www.mcafee.com/apps/downloads/security_updates/hotfixes.asp?region=us&segment=enterprise

- Small & Medium Business:

http://www.mcafee.com/apps/downloads/security_updates/hotfixes.asp?region=us&segment=smb

HotFix and Patch Releases for Products
(ServicePortal account and valid grant number
required)

http://mysupport.mcafee.com/eservice_enu/start.swe

SOFTWARE & HARDWARE TECHNICAL SUPPORT

Home Page

<http://www.mcafee.com/us/support>

Knowledge Search

<http://knowledge.mcafee.com/>

MCAfee Technical Support ServicePortal (Logon
credentials required)

https://mysupport.mcafee.com/eservice_enu/start.swe

CUSTOMER SERVICE

- Web: <http://www.mcafee.com/us/support/index.html>
<http://www.mcafee.com/us/about/contact/index.html>
- Phone: +1-888-VIRUS NO or +1-888-847-8766
Monday-Friday, 8am-8pm, Central Time
US, Canada, and Latin America
toll-free

MCAFFEE BETA PROGRAM

- Enterprise:
<http://www.mcafee.com/us/enterprise/downloads/beta/index.html>
- Small & Medium Business:
<http://www.mcafee.com/us/smb/downloads/beta/index.html>
- Submit Beta Feedback:
mcafee_beta@mcafee.com

PROFESSIONAL SERVICES

- Enterprise:
<http://www.mcafee.com/us/enterprise/services/index.html>
- Small & Medium Business:
<http://www.mcafee.com/us/smb/services/index.html>

COPYRIGHT AND TRADEMARK ATTRIBUTIONS

Copyright (C) 2007 McAfee, 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 McAfee, Inc., or its suppliers or affiliate companies.

TRADEMARKS

ACTIVE FIREWALL, ACTIVE SECURITY, ACTIVESECURITY (AND IN KATAKANA), ACTIVESHIELD, CLEAN-UP, DESIGN (STYLIZED E), DESIGN (STYLIZED N), ENTERCEPT, EPOLICY ORCHESTRATOR, FIRST AID, FOUNDSTONE, GROUPSHIELD, GROUPSHIELD (AND IN KATAKANA), INTRUSHIELD, INTRUSION PREVENTION THROUGH INNOVATION, MCAFFEE, MCAFFEE (AND IN KATAKANA), MCAFFEE AND DESIGN, MCAFFEE.COM, MCAFFEE VIRUSSCAN, NET TOOLS, NET TOOLS (AND IN KATAKANA), NETSCAN, NETSHIELD, NUTS & BOLTS, OIL CHANGE, PRIMESUPPORT, SPAMKILLER, THREATSCAN, TOTAL VIRUS DEFENSE, VIREX, VIRUS FORUM, VIRUSCAN, VIRUSSCAN, VIRUSSCAN (AND IN KATAKANA), WEBSCAN, WEBSHIELD, WEBSHIELD (AND IN KATAKANA) are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other

countries. The color red in connection with security is distinctive of McAfee brand products. All other registered and unregistered trademarks herein are the sole property of their respective owners.

LICENSE & PATENT INFORMATION

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 MCAFEE OR THE PLACE OF PURCHASE FOR A FULL REFUND.

LICENSE ATTRIBUTIONS

This product includes or may include:

- * Software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).
- * Cryptographic software written by Eric A. Young and software written by Tim J. Hudson. * Some software programs that are licensed (or sublicensed) to the user under the GNU General Public License (GPL) or other similar Free Software licenses which, among other rights, permit the user to copy, modify and redistribute certain programs, or portions thereof, and have access to the source code. The GPL requires that for any software covered under the GPL, which is distributed to someone in an executable binary format, that the source code also be made available to those users. For any such software covered under the GPL, the source code is made available on this CD. If any Free Software licenses require that McAfee provide rights to use, copy or modify a software program that are broader than the rights granted in this agreement, then such rights shall take precedence over the rights and restrictions herein. * Software originally written by Henry Spencer, Copyright 1992, 1993, 1994, 1997 Henry Spencer. * Software originally written by Robert Nordier, Copyright (C) 1996-7 Robert Nordier.
- * Software written by Douglas W. Sauder. * Software developed by the Apache Software Foundation (<http://www.apache.org/>). A copy of the license agreement for this software can be found at www.apache.org/licenses/LICENSE-2.0.txt.
- * International Components for Unicode ("ICU") Copyright (C) 1995-2002 International Business

Machines Corporation and others. * Software developed by CrystalClear Software, Inc., Copyright (C) 2000 CrystalClear Software, Inc. * FEAD(R) Optimizer(R) technology, Copyright Netopsystems AG, Berlin, Germany. * Outside In(R) Viewer Technology (C) 1992-2001 Stellent Chicago, Inc. and/or Outside In(R) HTML Export, (C) 2001 Stellent Chicago, Inc. * Software copyrighted by Thai Open Source Software Center Ltd. and Clark Cooper, (C) 1998, 1999, 2000. * Software copyrighted by Expat maintainers. * Software copyrighted by The Regents of the University of California, (C) 1996, 1989, 1998-2000. * Software copyrighted by Gunnar Ritter. * Software copyrighted by Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, California 95054, U.S.A., (C) 2003. * Software copyrighted by Gisle Aas. (C) 1995-2003. * Software copyrighted by Michael A. Chase, (C) 1999-2000. * Software copyrighted by Neil Winton, (C) 1995-1996. * Software copyrighted by RSA Data Security, Inc., (C) 1990-1992. * Software copyrighted by Sean M. Burke, (C) 1999, 2000. * Software copyrighted by Martijn Koster, (C) 1995. * Software copyrighted by Brad Appleton, (C) 1996-1999. * Software copyrighted by Michael G. Schwern, (C) 2001. * Software copyrighted by Graham Barr, (C) 1998. * Software copyrighted by Larry Wall and Clark Cooper, (C) 1998-2000. * Software copyrighted by Frodo Looijaard, (C) 1997. * Software copyrighted by the Python Software Foundation, Copyright (C) 2001, 2002, 2003. A copy of the license agreement for this software can be found at www.python.org. * Software copyrighted by Beman Dawes, (C) 1994-1999, 2002. * Software written by Andrew Lumsdaine, Lie-Quan Lee, Jeremy G. Siek (C) 1997-2000 University of Notre Dame. * Software copyrighted by Simone Bordet & Marco Cravero, (C) 2002. * Software copyrighted by Stephen Purcell, (C) 2001. * Software developed by the Indiana University Extreme! Lab (<http://www.extreme.indiana.edu/>). * Software copyrighted by International Business Machines Corporation and others, (C) 1995-2003. * Software developed by the University of California, Berkeley and its contributors. * Software developed by Ralf S. Engelschall <rse@engelschall.com> for use in the mod_ssl project (<http://www.modssl.org/>). * Software copyrighted by Kevlin Henney, (C) 2000-2002. * Software copyrighted by Peter Dimov and Multi Media Ltd. (C) 2001, 2002. * Software copyrighted by David Abrahams, (C) 2001, 2002. See <http://www.boost.org/libs/bind/bind.html> for documentation. * Software copyrighted by Steve Cleary, Beman Dawes, Howard Hinnant & John Maddock, (C) 2000. * Software copyrighted by Boost.org, (C) 1999-2002. * Software copyrighted by Nicolai M. Josuttis, (C) 1999. * Software copyrighted by Jeremy siek, (C) 1999-2001. * Software copyrighted by Daryle Walker, (C) 2001. * Software copyrighted by Chuck Allison and Jeremy siek, (C) 2001, 2002. * Software copyrighted by Samuel Krempf, (C) 2001. See <http://www.boost.org> for updates, documentation, and revision history. * Software copyrighted by Doug Gregor (gregod@cs.rpi.edu), (C) 2001, 2002. * Software copyrighted by Cadenza New Zealand Ltd.,

Readme_EN.txt

(C) 2000. * Software copyrighted by Jens Maurer,
(C) 2000, 2001. * Software copyrighted by Jaakko
Järvi (jaakko.jarvi@cs.utu.fi), (C) 1999, 2000.
* Software copyrighted by Ronald Garcia, (C) 2002.
* Software copyrighted by David Abrahams, Jeremy
Siek, and Daryle walker, (C) 1999-2001. * Software
copyrighted by Stephen Cleary (shammah@voyager.net),
(C) 2000. * Software copyrighted by Housemarque Oy
<<http://www.housemarque.com>>, (C) 2001. * Software
copyrighted by Paul Moore, (C) 1999. * Software
copyrighted by Dr. John Maddock, (C) 1998-2002.
* Software copyrighted by Greg Colvin and Beman
Dawes, (C) 1998, 1999. * Software copyrighted by
Peter Dimov, (C) 2001, 2002. * Software copyrighted
by Jeremy Siek and John R. Bandela, (C) 2001.
* Software copyrighted by Joerg Walter and Mathias
Koch, (C) 2000-2002. * Software copyrighted by
Carnegie Mellon University (C) 1989, 1991, 1992.
* Software copyrighted by Cambridge Broadband Ltd.,
(C) 2001-2003. * Software copyrighted by Sparta,
Inc., (C) 2003-2004. * Software copyrighted by
Cisco, Inc and Information Network Center of Beijing
University of Posts and Telecommunications, (C)
2004. * Software copyrighted by Simon Josefsson, (C)
2003. * Software copyrighted by Thomas Jacob, (C)
2003-2004. * Software copyrighted by Advanced
Software Engineering Limited, (C) 2004. * Software
copyrighted by Todd C. Miller, (C) 1998. * Software
copyrighted by The Regents of the University of
California, (C) 1990, 1993, with code derived from
software contributed to Berkeley by Chris Torek.

PATENTS

Protected by US Patents 6,006,035; 6,029,256;
6,035,423; 6,151,643; 6,230,288; 6,266,811;
6,269,456; 6,457,076; 6,496,875; 6,542,943;
6,594,686; 6,611,925; 6,622,150; 6,668,289;
6,697,950; 6,735,700; 6,748,534; 6,763,403;
6,763,466; 6,775,780; 6,851,058; 6,886,099;
6,898,712; 6,928,555; 6,931,540; 6,938,161;
6,944,775; 6,963,978; 6,968,461; 6,971,023;
6,973,577; 6,973,578.

DBN-008-EN

V3.1.4