Release Notes for McAfee® VirusScan® Enterprise 8.7i

About this document

- Dat Version: 5381
- Engine Version: 5300.2777

Thank you for using VirusScan Enterprise software. This document contains important information about this release. We strongly recommend that you read the entire document.

CAUTION: *We do not support automatic upgrading of a pre-release version of the software. To upgrade to a production release of the software, you must first uninstall the existing version of the software.*

Beta product testing

The beta version of this product is available for use until the beta product license expires on November 30, 2008.

New features

New and updated features in the current release of the software:

Support for Microsoft Windows Server 2008

This release provides support for Windows Server 2008 (Longhorn).

Architectural changes

VirusScan Enterprise incorporates some significant architectural changes that affect the manner in which the VirusScan Enterprise 8.7i core components work. These changes result in greater security benefits to customers, including:

- **Better rootkit detection and cleaning without system restart** — Safe memory patching, better IRP repair support at the system core, and the ability to read locked files at the kernal level provide better rootkit detection and the ability to clean detections without restarting the system.
- **On-access scan performance improvements during system startup** — A new boot cache process improves on-access scan performance during system startup.
- **Greater self-protection** — The self-protection feature has been enhanced to protect against a wider range of mal-processes that can terminate McAfee processes. This provides greater VirusScan Enterprise self-protection and product stability.

Real-time malware protection

A new feature, **Heuristic network check for suspicious files**, provides customers with real-time detections for malware.

- This feature uses sensitivity levels that can be configured, based on your risk tolerance, to look for suspicious files on your endpoints that are running VirusScan Enterprise 8.7i.
- When enabled, this feature detects a suspicious program and sends a DNS request containing a fingerprint of the suspicious file to McAfee Avert Labs, which then communicates the appropriate action back to VirusScan Enterprise 8.7i.
- The real-time defense feature also provides protection for classes of malware for which signatures might not be available.
- This protection is in addition to the world-class DAT-based detection VirusScan Enterprise has always provided. The user experience remains the same and no additional client software is required.
- In this release, this feature is available only for on-demand scans and email scanning and is disabled by default. You must select a sensitivity level to enable the feature.

Performance improvements

These changes improve performance.

- New scan deferral options improve local control of on-demand scans, including the ability to defer scans when using battery power or during presentations. One option can be configured to allow end users to defer scheduled on-demand scans for the increment of time you specify. You can specify hourly increments up to twenty-four hours, or forever.
- Enhanced system throttling now includes registry and memory scanning in addition to file scanning.

Improved email scanner

The email scanner now supports double-byte and multi-byte languages. This improves detection reliability.

Buffer overflow protection exclusions by API

The ability to specify buffer overflow exclusions by API was removed from VirusScan Enterprise 8.5i, but has been reinstated for the VirusScan Enterprise 8.7i release. The API exclusion name is case-sensitive.

On-access scanner — Scan processes on enable

A new feature, **Scan processes on enable**, scans processes that are already running when the McShield service becomes enabled. When the McShield service starts, the scanner examines any process that is already running and any process as it is launched.

On-demand scan usability improvements

When initiating an on-demand right-click scan, you can now choose an action to take on items detected by the scan. These options are available:

- **Clean** — Report and clean the detection.
- **Continue** — Report the detection and continue scanning.

Known issues

Known issues in this release of the software are described below.

Installation

- **Issue**

  The current Detection Definition (DAT) is not preserved after upgrade to VirusScan® Enterprise 8.7i. When you select the **Preserve settings** option during an upgrade from an earlier version of VirusScan Enterprise to a later version, the current DAT version is not preserved. In this scenario, the current DAT version is removed during the uninstallation of the old product and the DAT version included in the new product build is installed.

- **Issue**

  The 64-bit version of Panda Antivirus 2008 is not removed during the VirusScan Enterprise installation. During the VirusScan Enterprise standalone product installation, the user is notified to manually remove the product. During silent installation, such as deployment via ePolicy Orchestrator, the VirusScan Enterprise installation fails with no notification. In either case, the user must manually uninstall the 64-bit version of Panda Antivirus 2008, then reinstall VirusScan Enterprise.

- **Issue**

  We do not recommend installing VirusScan Enterprise 8.7i on a system where the VirusScan for NetApp 7.1 Console is running. If you do, the VirusScan for NetApp 7.1 Console is disabled. This behavior is expected because of the impending release of VirusScan Enterprise for Storage, which is a replacement for VirusScan for NetApp 7.1.

- **Issue**

  To install the VirusScan Enterprise 8.7i Reporting .NAP file in ePolicy Orchestrator 3.6.1, complete these steps:

  1. Use the ePolicy Orchestrator Check-In Wizard to add the VSE870Reports.NAP file to the repository.
  2. If applicable, log out of the **Reporting** console.
  3. In the ePolicy Orchestrator installation directory, delete the *REPORTVERSIONS.SQL* file from the AVI directory.
  4. Log in to the **Reporting** console using *ePO Authentication*.
  5. Click **Y**

5. Click **Yes** to download the new reports.

Migrating policies and events in ePolicy Orchestrator

- **Issue**

  The Policy Migration tool (ePOPolicyMigration.exe) upgrades VirusScan Enterprise polices and tasks from an earlier version of VirusScan Enterprise. This tool runs only one time per server. If you have both the VirusScan Enterprise 8.0i .NAP file and the 8.5i .NAP or extension installed on the same server, you must choose whether to upgrade policies and tasks from VirusScan Enterprise 8.0i or 8.5i. You cannot upgrade both.

  Choose only one of these upgrade scenarios:

  - When upgrading VirusScan Enterprise 8.5i policies and tasks in ePolicy Orchestrator 3.6.1, first check in the .NAP file, then execute the Policy Migration tool on the server.
  - When upgrading VirusScan Enterprise 8.5i policies and tasks in ePolicy Orchestrator 4.0, first check in the extension, then execute the Policy Migration tool on the server.
  - When upgrading VirusScan Enterprise 8.0i policies and tasks, use the command-line option with the **force** switch as follows: **ePOPolicyMigration.exe /force80**

  NOTE: *You can upgrade more than one version of the VirusScan Enterprise software to a later version in ePolicy Orchestrator, but you can upgrade only one version of VirusScan Enterprise policies and tasks to a later version.*

- **Issue**

  Some Access Protection policies do not migrate when using ePOPolicyMigration.exe to migrate VirusScan Enterprise policies from an older version to a newer version of the product. See McAfee Support KnowledgeBase article 616156 for more information about this issue.

- **Issue**

  VirusScan Enterprise 8.7i events do not appear after migrating from ePolicy Orchestrator 3.6.1 to ePolicy Orchestrator 4.0. See McAfee Support KnowledgeBase article 616597 for more information about this issue.

Supported platforms and products

This version of VirusScan Enterprise supports Lotus Notes version 6.0x, 6.5, and 7.0x. See the VirusScan Enterprise 8.7i installation guide for information about supported operating systems.

Compatibility with other products

- **Issue**

  When VirusScan Enterprise 8.7i is installed on a system that is also protected by McAfee Network Access Control (McAfee NAC), a DAT compliance issue might occur if the DAT version included in VirusScan Enterprise 8.7i is older than the age configured in the McAfee NAC policy. If the DAT version exceeds this age, McAfee NAC quarantines the system until remediation steps are taken by the administrator or user. In most cases, remediation requires a restart.

  Both products are working as expected. There are two options to address this issue:
  - No change to McAfee NAC policies. The administrator can decide whether to install VirusScan Enterprise 8.7i with out-of-date DAT files and risk quarantining the system. For quarantined client systems that are managed by ePolicy Orchestrator, the administrator can still install VirusScan Enterprise 8.7i on the quarantined system and/or update the DAT file.
  - Run McAfee NAC in Audit mode. This allows client systems to be scanned and reported on, without risking quarantine from the DAT compliance issue. In this scenario, we recommend that all McAfee NAC policies be configured to run in Audit mode.

- **Issue**

  After installing VirusScan Enterprise 8.7i to a system where McAfee NAC 3.0 is installed, an infrequent failure might occur, preventing identification of McAfee services. You might see these symptoms:
  - A *specified driver is invalid* message is logged if you perform an update task before restarting.
  - A *driver failed to load* message is logged for one or both products.
  - The local system application event log contains event ID 5004.

  To resolve this issue, uninstall the failed product, restart the system, then reinstall the product.

- **Issue**

  NVIDIA® drivers might cause performance issues or system response failure. VirusScan Enterprise 8.7i might run at 100% CPU or cause the system to fail to respond when running on specified NVIDIA drivers. See KnowledgeBase articles 614212 and 65066 for more information about this issue.

- **Issue**

  When taking action on threatened items detected on an EMC filer, we recommend using only **Clean** and **Delete** action options. Do not use the **Deny access** action option. The implementation of the anti-virus protection between VirusScan Enterprise and EMC requires that a **Clean** or **Delete** action be taken to protect detected threats. **Deny access** does not take any action and allows the detected item to be accessed again.

Updating

- **Issue**

  The update task fails the first time after any system restart when running VirusScan Enterprise 8.7i on a system with Microsoft Windows 2000 Professional and Server operating systems. In this scenario, the update task fails the first time after every manual or scheduled system restart and might also occur when a manual update is performed after the system is left running for days. Subsequent update tasks are successfully performed in either case. If an update task fails in this scenario, start another update task or wait for the next scheduled task to be performed.

- **Issue**

  Update might fail when using a mirror repository that was created using VirusScan Enterprise 8.7i and a new installation of McAfee Agent version 4.0. In this scenario, the Sitelist.xml file is not found. This issue does not occur when upgrading the agent on an ePolicy Orchestrator-managed client computer from ePolicy Orchestrator agent 3.6.1 to McAfee Agent version 4.0.

  NOTE: *McAfee Agent was previously known as ePolicy Orchestrator agent.*

- **Issue**

  Failure to access the repository is not logged in the VirusScan Enterprise 8.7i update log, but the failure is logged in the McAfee Agent log. The default location of the McAfee Agent log is: <drive>:\Documents and Settings\All Users\Application Data\McAfee\Common Framework\ mcscript.log.

- **Issue**

  Silent update tasks performed from the command line still display the progress dialog box. The installation successfully completes, but the **Update in progress** dialog box appears when you run "setup.exe /q RUNAUTOUPDATESILENTLY=TRUE" from the command line.

- **Issue**

  We recommend using single-byte characters when naming folders for mirror site locations on localized systems. If you use double-byte or extended characters when naming folders for mirror site locations on localized systems, the folder name might change after specifying the folder name in the **Mirror Location** text box. This issue is in the McAfee Agent and expected to be fixed in a later version of the McAfee Agent.

- **Issue**

  Importing the Sitelist.xml file from the command line might fail. When you run "setup.exe CMASOURCEDIR="<drive>:\Documents and Settings\<username>\Desktop\" from the command line to install the product and import the Sitelist.xml file from the Desktop, the installation successfully completes but fails to import the Sitelist.xml file.

  To resolve this issue, use a Sitelist.xml file that was created by ePolicy Orchestrator agent 3.6.1. If the McAfee Agent 4.0 installation "upgraded" a previous installation of ePolicy Orchestrator agent 3.6.1, then it will produce a correct Sitelist.xml that can be imported by VirusScan Enterprise 8.7i.

Remote console

- **Issue**

  When using the remote console feature to open **Access Protection** properties on a system with Windows Server 2008, the time to open the connection might be slow and take up to several minutes.

Miscellaneous

- **Issue**

  When detections occur on 64-bit systems, event notifications might fail. See the activity log and the on-access scanner messages dialog box for information about detections.

- **Issue**

  Some customers have reported seeing VirusScan Statistics (VShield) crashing or disappearing from the system tray. See McAfee Support KnowledgeBase article 613892 for more information about this issue.

- **Issue**

  The McAfee email scanner for Lotus Notes does not use the **Quarantine Manager** to quarantine detected threats. Consequently, if you configured the email scanner first action to **Clean attachments** or **Delete attachments**, the original version of the detected threat is no longer available for recovery or restore after the clean or delete action is taken on the detection. If you want the original version of the detected threat to be available after the action is taken on the detection, we recommend that you set the first action to **Move attachments to a folder** and specify a quarantine folder. When this move action is enabled, the original detected threat is moved to the specified quarantine folder with the .VIR extension appended to the detection.

  NOTE: *If you enable the* ***Move attachments to a folder*** *option on client systems you should always have the on-access scanner enabled so those files may not inadvertently be accessed by a user.*

- **Issue**

  When running VirusScan Enterprise 8.7i on a system with Microsoft Windows Server 2008, the on-access scanner might fail to delete a detected file from a network shared folder. The on-access scanner's ability to delete a detected file is

not guaranteed on network file systems. In this case, if the detected file is not deleted, the file content is removed and the remaining file size is zero.

Where to find McAfee enterprise product information

The McAfee documentation is designed to provide you with the information you need during each phase of product implementation, from evaluating a new product to maintaining existing ones. Depending on the product, additional documents might be available. After a product is released additional information regarding the product is entered into the online Knowledgebase available on McAfee ServicePortal.

Installation Phase	Setup Phase	Maintenance Phase
Before, during, and after installation.	Getting up-and-running with the product.	Maintaining the software.
Release Notes • Known issues in the current release. • Issues resolved since the last release. • Last-minute changes to the product or its documentation.	*Product Guide* and *Online Help* • Setting up and customizing the software for your environment.	*Online Help* • Maintaining the software. • Reference information. • All information found in the product guide.
Installation Guide • Preparing for, installing and deploying software in a production environment.	*Online Help* • Managing and deploying products through ePolicy Orchestrator. • Detailed information about options in the product.	*Knowledgebase* (knowledge.mcafee.com) • Release notes and documentation. • Supplemental product information. • Workarounds to known issues.

Finding release notes and documentation for McAfee enterprise products

Use this task to go to the release notes and other product documentation for McAfee enterprise products.

1. Go to knowledge.mcafee.com and select Product Documentation under Useful links.
2. Select <Product Name> | <Product Version> and select the required document from the list of documents.

License attributions