

Release Notes for McAfee® VirusScan® Enterprise for Storage 1.0.2

- [About this document](#)
- [Product license](#)
- [New features and other product notes](#)
- [Known issues](#)
- [Upgrade instructions](#)
- [Where to find McAfee enterprise product information](#)
- [License attributions](#)

About this document

Thank you for using McAfee® VirusScan® Enterprise for Storage. 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.

Product license

These time limits apply to these McAfee® VirusScan® Enterprise for Storage product licenses:

- The Evaluation license expires 90 days after installing the evaluation version of the product.

New features and other product notes

New and updated features in the current release of the software are described below:

- This release supports McAfee VirusScan Enterprise 8.8.
- McAfee VirusScan Enterprise for Storage 1.0.2 can now be managed using ePolicy Orchestrator 4.6.
- This product is an upgrade for McAfee VirusScan Enterprise for Storage 1.0.
- Support for Artemis (Heuristic network check for suspicious files) — Looks for suspicious programs and DLLs running on the client systems. When the real-time malware defense detects a suspicious program, it sends a DNS request.

By default, Artemis settings from VirusScan Enterprise On-Access Scan will be used.

If you intend to configure different Artemis settings for Storage:

1. Go to the Registry Editor.
2. Navigate to the following path:

For NetApp	HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\VSES\NetApp
For ICAP	HKEY_LOCAL_MACHINE\SOFTWARE\McAfee\VSES\ICAP

3. Configure the following DWORD values:

DWORD Value name	Value data
ArtemisEnabled	0 or 1

ArtemisLevel	0 to 4	• 0 — Disable • 1 — Enable
		• 0 — Very low • 1 — Low • 2 — Medium • 3 — High • 4 — Very high

4. From the Services console, restart the **McAfee VirusScan Enterprise for Storage** service.

- You can now Check-in the McAfee VirusScan Enterprise for Storage 1.0.2 Help extension in ePolicy Orchestrator 4.5 and 4.6.

Known issues

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

- **Issue**

The ePolicy Orchestrator Migration tool might fail to migrate the existing policies and tasks from an ePolicy Orchestrator server that uses Windows NT authentication for ePolicy Orchestrator access. In some cases the ePolicy Orchestrator Migration tool needs to pass the SQL administrator password as a parameter for the ePolicy Orchestrator Migration tool.

Workaround:

Run ePOPolicyMigration.exe from the command line, and add the /PASSWORD switch and the SQL administrator password.

For example, type: [path]

```
\epopolicymigration.exe /vses /password=sql_admin_password
```

- **Issue**

The firewall in McAfee Host Intrusion Prevention may block communication on the ICAP communication port set by default in McAfee VirusScan Enterprise for Storage (port 1344). To resolve the conflict, change the port used by VirusScan Enterprise for Storage in the properties. Alternatively, see the Host Intrusion Prevention documentation for details about configuring the Host Intrusion firewall to allow communication on the port used by ICAP.

- **Issue**

When using McAfee VirusScan Enterprise for Storage's ICAP AV Scanner with Sun StorageTek 5320 you might encounter these known issues:

- Sun StorageTek 5320 sends two scan requests to the ICAP AV Scanner for each file copied or accessed from a Network Share on the StorageTek 5320.
- When copying or accessing large files (about 1GB or larger) from a Windows OS to a Network Share on the StorageTek 5320, the user might see an error message stating that the Network Share is no longer available.

These issues have been communicated to Sun and are known issues. Please contact Sun for further information.

- **Issue**

When detection alerts are sent to Alert Manager from McAfee VirusScan Enterprise for Storage, the alert message might incorrectly state that OAS (On Access Scanning) denied access to the file. The AV scanner name is properly shown in these messages, you might consider customizing this message by removing the reference to the OAS scanner.

- **Issue**

When files are accessed on the NetApp Filer from the Scan Server the NetApp Filer will not request those files to be scanned.

This issue has been communicated to NetApp and is a known issue. Please contact NetApp for further information.

- **Issue**

The VirusScan Enterprise **Repair** feature will not repair the files for the McAfee VirusScan Enterprise for Storage product. If repair is needed to the McAfee VirusScan Enterprise for Storage product, rerun the installer and select **Repair** during the re-installation. A KB article exists explaining the repair feature for VirusScan Enterprise: KB60029

- **Issue**

If you enable or disable alerts for VirusScan Enterprise for Storage, or change any of the additional alerting options using the VirusScan Console you need to restart the VirusScan Enterprise for Storage service for the changes to take effect.

- **Issue**

After the localization was completed for the VirusScan Enterprise for Storage Product Guide, ePolicy Orchestrator 4.0 extension Help, and VirusScan Console Help the following "How scanning of ICAP servers works" section was added.

This section describes how VirusScan Enterprise for Storage scans Internet Content Adaptation Protocol (ICAP) servers.

NOTE: In the following example, the ICAP client is a Network Attached Storage (NAS) device.

The following process occurs when an ICAP client requests a file scan by VirusScan Enterprise for Storage:

1. The ICAP client contacts VirusScan Enterprise for Storage and requests that a specific file be scanned.
2. The file is transferred to a temporary location on the computer running VirusScan Enterprise for Storage, where it is scanned.
3. If the file is found to be a threat, the action taken depends on the following VirusScan Enterprise for Storage configuration:
 - If **Clean files automatically** is selected, any threats found cause an attempt to clean the file.
 - If the file is successfully cleaned, VirusScan Enterprise for Storage notifies the ICAP client that the file was a threat and was successfully cleaned, and VirusScan Enterprise for Storage returns the cleaned file to the ICAP client.
 - If unable to successfully clean the file, VirusScan Enterprise for Storage follows the ICAP standard by replacing the file with an HTML message stating that the original file is a threat and that it was unable to clean the file.
 - If **Continue scanning** is selected, VirusScan Enterprise for Storage notifies the ICAP client that the file is a threat and the ICAP client then blocks access to this file.

- **Issue**

The installation section of the *VirusScan Enterprise for Storage, Product Guide* contains simple instructions for installing the VirusScan Enterprise for Storage software module. However, there may be times when you want to install the product from the command-line with different parameters to change the default behavior. The following section provides the basic format for the command-line operation and also some common parameters.

- Installing locally from command-line:
`setup.exe /S /v"<command-line options>"`
- Installing from ePO Deployment task (input in the command-line form field):
`/v"<command-line options>"`

Where <command-line options> is a space-delimited set of valid MSI flags. For example:

- `/qn` — silent install
- `/quiet` — same as `/qn`
- `INSTALLDIR=<Path to a Directory>` — alternative installation directory

- /l*v <Path to a LogFile> — log the installation activity to the following location

- **Issue**

After the localization was completed for the *VirusScan Enterprise for Storage Product Guide*, ePolicy Orchestrator 4.0 extension Help, and VirusScan Console Help the following sections were modified:

- Managing the list of file types scanned — replaced step 1 with the following text:
 1. Start NetApp configuration using either of the following:
 - From ePolicy Orchestrator 4.0, select **Systems | Policy Catalog**, select **VirusScan Enterprise for Storage 1.0.2** from the **Product** drop-down list, select **NetApp Policies** in the **Category** drop-down, select **edit** from the **Actions** column of the display, and select the **Scan Items** tab.
- Configuring the list of ICAP file types scanned — replaced step 1 with the following text:
 1. Start ICAP configuration using either of the following:
 - From ePolicy Orchestrator 4.0, select **Systems | Policy Catalog**, select **VirusScan Enterprise for Storage 1.0.2** from the **Product** drop-down list, select **NetApp Policies** in the **Category** drop-down, select **edit** from the **Actions** column of the display, and select the **Scan Items** tab.

- **Issue**

If you perform a repair install of VirusScan Enterprise it causes the strings.bin file to return to the original version that is not compatible with VirusScan Enterprise for Storage.

The workaround is to perform a repair install of VirusScan Enterprise for Storage by running the setup.exe again and choose the **Repair** option. This causes the strings.bin file to be updated to the version compatible with VirusScan Enterprise for Storage.

- **Issue**

The installation log (VSESTOSetup.log) for the VirusScan Enterprise for Storage is stored in [current user]%temp%, where [current user] refers to the user performing the installation.

Upgrade instructions

Use this task to upgrade VirusScan Enterprise for Storage 1.0 to VirusScan Enterprise for Storage 1.0.2.

Task

1. On the computer where VirusScan Enterprise for Storage 1.0 is installed, install VirusScan Enterprise 8.8.

NOTE: This will not uninstall VirusScan Enterprise for Storage 1.0. The product will stop working; however all the settings will be saved.
2. Install McAfee VirusScan Enterprise for Storage 1.0.2.

NOTE: After installing the Storage 1.0.2 extension file, ensure to run the policy migration tool (ePOPolicyMigration.exe) on the ePolicy Orchestrator server to migrate your VirusScan Enterprise for Storage 1.0 policies.

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. <i>Release Notes</i> • Known issues in the current release. • Issues resolved since the last release. • Last-minute changes to the product or its documentation. <i>Product Guide</i> • Preparing for, installing and deploying software in a production environment.	Getting up-and-running with the product. <i>Product Guide and Online Help</i> • Setting up and customizing the software for your environment. <i>Online Help</i> • Managing and deploying products through ePolicy Orchestrator. • Detailed information about options in the product.	Maintaining the software. <i>Online Help</i> • Maintaining the software. • Reference information. • All information found in the product guide. <i>Knowledgebase</i> (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

COPYRIGHT

Copyright © 2011 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.

TRADEMARK ATTRIBUTIONS

AVERT, EPO, EPOLICY ORCHESTRATOR, FOUNDSTONE, GROUPSHIELD, INTRUSHIELD, LINUXSHIELD, MAX (MCAFEE SECURITYALLIANCE EXCHANGE), MCAFEE, NETSHIELD, PORTALSHIELD, PREVENTSYS, SECURITYALLIANCE, SITEADVISOR, TOTAL PROTECTION, VIRUSSCAN, WEBSHIELD are registered trademarks or trademarks of McAfee, Inc. and/or its affiliates in the US and/or other countries. McAfee 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 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 ACCOMPANY 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 WEBSITE 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.