Release Notes

for FortiScan™ 4.0 MR3

Courtney Schwartz

Contributors:

Jianjun He
Ken Lin
Tom Mao
Idan Soen

Revision History

Date	Revision Number	Change Description
2012-03-21	Revision 1	Initial revision.
2012-03-26	Revision 2	Updated resolved issues list.
2012-04-02	Revision 3	Added supported web browser information.

FortiScan 4.0 MR 3 Release Notes

Revision 3

2 April 2012

Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.

Support will be provided to customers who have purchased a valid support contract. All registered customers with valid support contracts may enter their support tickets via the Fortinet Technical Support web site:

https://support.fortinet.com/

Contents

New features

These major new features and enhancements have been added since FortiScan 4.0 MR2 Patch 3. For configuration instructions, see the FortiScan Administration Guide.

- **GUI usability enhancements —** Scans that are agentless or agent-based are now categorized as such in the web UI. This simplifies use and clarifies scan prerequisites for deployments that are strictly agent-based, or strictly agentless. Other smaller items have also been streamlined for faster, easier configuration and use, such as the ability to search for a vulnerability without typing its “CVE-” prefix.
- **Possible vs. confirmed vulnerabilities** — Vulnerability scans now categorize and report potential vulnerabilities (that are impractical to confirm or situationally contingent).separately from confirmed vulnerabilities.
- **Import 3rd-party scan results** — FortiScan can now import vulnerability scan results from Nessus and Qualys.
- **Ordering/filtering by severity level** — You can now prioritize alerts based upon the severity level of the detected vulnerability. This helps you to focus on the most important issues.
- **Report error messages** — For troubleshooting, you can now differentiate when a report is still in progress or has terminated abnormally. When a report fails, a message is now created in *Events & Tickets* > *Error Events* > *General Events* or *Events & Tickets System Log* > *Historical*: “Scan job has terminated abnormally”.
- **Redesigned compliance report** — The compliance template has been redesigned.
- **VMware ESXi 5.0 support** — FortiScan-VM has been tested for compatibility with VMware vSphere ESXi 5.0.

System requirements

Upgrading to FortiScan 4.0 MR3 requires FortiScan 3.0 MR1 or later. (New installations do not require any prior installation.) ***If your appliance is running older software, you must first upgrade it to FortiScan 3.0 MR1 before upgrading it to FortiScan 4.0 MR3.***

Installing FortiScan-VM requires that you have already installed a supported virtual machine (VM) environment, sometimes called a hypervisor, such as VMware vSphere, Citrix XenServer, or Open Source Xen. For details, see the FortiScan-VM Install Guide.

The management computer that you use to access the web UI must have a compatible web browser, such as Microsoft Internet Explorer 8.0 or Mozilla Firefox 3.5 or greater.

FortiScan agents included with this release support the following host platforms:

- Windows XP (32-bit or 64-bit)
- Windows Vista (32-bit or 64-bit Enterprise or Business)
- Windows 7 (32-bit or 64-bit)
- Windows Server 2003 (32-bit or 64-bit)
- Windows Server 2008 (32-bit or 64-bit)
- Windows Server 2008 Release 2 (64-bit)
- Red Hat 9
- Red Hat Enterprise Server 3
- Red Hat Enterprise Server 4
- Red Hat Enterprise Server 5 (32-bit or 64-bit)
- Red Hat Enterprise Server 6 (32-bit or 64-bit)
- Fedora 13 (32-bit or 64-bit)
- Fedora 14 (32-bit or 64-bit)
- Fedora 15 (32-bit or 64-bit)
- CentOS 3
- CentOS 4
- CentOS 5
- Solaris Sparc 9
- Solaris Sparc 10
- Solaris 10 (x86 32-bit or 64-bit)

Upgrading

Upgrading differs from a new installation. Fortinet provides FortiScan software in three formats:

- `.out` — Use this for ***new physical appliance*** installations. Contains only the FortiScan appliance operating system.
- `.zip` or `.tgz` — Use this for ***new virtual appliance (VM)*** installations. Contains a deployable virtual machine package.
- `.pkg` — Use this for ***updates and adding the agent installers***. Contains the `.out` file, plus:
  - FortiScan agent softwareWindows application version of the push installer
  - Microsoft Installer and other software required by the agent
  - FortiScan Release Notes

Downloading the software

Before you can install FortiScan firmware, you must first download it.

There are two ways:

- Via the appliance, from the FDN
- Via your computer, from the Fortinet Technical Support web site

Via the appliance, from the FDN

FortiScan appliances periodically poll the Fortinet Distribution Network (FDN) for a list of new available firmware packages. If the appliance has a valid support license, when network traffic is low, the appliance automatically downloads the available firmware packages to its internal hard drive.

If you do not want to wait for the automatic download, you can initiate the download immediately.

To initiate the download

1. Log in to the FortiScan appliance's web UI using the admin administrator account. Other accounts may not have the required permissions.
2. From *Current ADOM*, select *Global*.
3. Go to *System* > *Dashboard* > *Status*.
4. In the *System Information* widget's *Firmware Version* row, click *Update*. The *Firmware Upgrade* dialog appears.

5 If new versions of FortiScan firmware were available at the time that the appliance last polled the FDN, new entries appear in the *Download Release Packages From FDN* section.

6 Click the *Download* icon to start downloading the new upgrade firmware immediately. The time required varies by the size of the file and the speed of your network connection.

7 Wait until the unpacking process completes, then refresh the page. The new firmware package will appear in the *Releases Available For Upgrade* section.

Via your computer, from Fortinet Technical Support

You can download a firmware release from the Fortinet Technical Support web site, then upload the package from your computer to the FortiScan appliance.

To download manually

1 Log in to the Fortinet Technical Support web site:

https://support.fortinet.com

2 In the Download section of the page, click the *Firmware Images* link to download the firmware (the `.pkg` file).

3 If you want to check the integrity of the download, go back to the *Download* section of the login page, then click the *Firmware Image Checksums* link.

4 Log in to the FortiScan appliance's web UI using the `admin` administrator account. Other accounts may not have the required permissions.

5 From *Current ADOM*, select *Global*.

6 Go to *System* > *Dashboard* > *Status*.

7 In the *System Information* widget's *Firmware Version* row, click *Update*. The *Firmware Update* dialog appears.

8 In the *Manually Upload a Release Package* section, click the *Browse* button and locate the `.pkg` file that you downloaded.

9 Click *OK* to upload the file to the appliance.

10 Your browser uploads the firmware file. The time required varies by the size of the file and the speed of your network connection. When the file transfer is complete, a message appears:

Manual release upload is complete. It will take a few minutes to unpack the uploaded release. Please wait.

11 Wait until the unpacking process completes (usually around 5 minutes), then refresh the page. The firmware package file name will appear in the *Releases Available For Upgrade* section.

Upgrading the appliance and agents

After you have downloaded the software, upgrade both your appliance and FortiScan agents.

> **Caution:** Before starting the upgrade process, back up your configuration and database. For detailed instructions, see the Administration Guide corresponding to your firmware.

To upgrade an existing installation

1. Log in to the FortiScan appliance's web UI using the `admin` administrator account. Other accounts may not have the required permissions.
2. From *Current ADOM*, select *Global*.
3. Go to *System* > *Dashboard* > *Status*.
4. In the *System Information* widget's *Firmware Version* row, click *Update*.

    > **Note:** After the system boots up, the FortiScan appliance will update its database to match structures required by the new firmware version. This could take up to half an hour. During this time, you will not be able to access asset information or perform actions on the assets.

    The *Firmware Update* dialog appears.In the *Releases Available for Upgrade* section, in the row corresponding to this release's firmware package, click the icon in the *Upgrade Firmware* column, and then click *OK* in the dialog that appears. The FortiScan appliance installs the firmware and restarts.
5. When upgrading from releases prior to FortiScan 4.0 MR 2, for each existing account whose *Role* is *Operator* or *Auditor,* the FortiScan appliance will automatically create an ADOM named after the account. All assets and asset groups assigned to the account will be added to its identically-named ADOM. Accounts whose *Role* is *Administrator* will be grouped into a default ADOM named `administrators`.
6. When the upgrade is successfully installed:
    - Clear your web browser's cache.
    - Log in to the web UI again.
7. If necessary, adjust the ADOMs that were configured during the upgrade.
8. Update each asset's FortiScan agent software. For more information, see the *FortiScan Administration Guide*.

Resolved issues

This release resolves the following issues in the previous releases, FortiScan 4.0 MR2 Patch 3 and earlier.

Bug ID	Description
127823	Registered FortiScan-3000C appliances could connect to the FDN, but could not get a trial license for the FortiGuard Vulnerability and Compliance Management service.
156766 164402	ADOM names and asset group names should not allow special characters that can enable a FortiScan administrator to execute XSS attacks.
156885	When restoring the configuration from a backup, in some cases, an ADOM's configuration might be missing or a remote network vulnerability scan might cease to function.
157031	On Windows XP, FortiScan did not detect Service Pack 1 for Microsoft Office 2007 when it was actually installed.
157042	Network vulnerability scan results compressed into a .zip file and delivered via email were empty.
157084	The *Email/Upload* option for report output did not work.
157906	In *Network Scan* > *Summary* > *Host Status*, after clicking the number of vulnerabilities detected for a host, the number displayed (*Affected Hosts*) was the total for all ADOMs, not the total the host in the ADOM currently being viewed.
158304	In the CLI, the command `execute reset_password` had no effect.
159589	FortiScan agent installation would fail on 64-bit Windows hosts that lack the .Net platform libraries.
160216	While the FortiScan-VM license was in the process of being validated, it would incorrectly display an error message indicating an invalid license: “Invalid Length.”
160388	In *Compliance* > *Audit Scan* > *Assessment Evaluation*, if the audit had multiple profiles, *# of Assets Evaluated* would contain the total number for all profiles, which could result in counting the same host multiple times.
161619	While running a scan, settings should not be editable because changes made during that time will not be kept. Some settings were incorrectly

editable, when they should have been greyed out.

162213 In *Report* > *Agent Scan* > *Scheduled*, clicking the link of a report to see its scheduled scans would not display any newly scheduled scans. Also, a newly scheduled scan would not run if its *Schedule Type* setting was not set to *Immediate*.

162816 Reports would sometimes terminate abnormally without an error message.

163565 When viewing a PCI DSS compliance report, links to the original report were sometimes broken.

164481 FortiScan-VM licenses would become invalid after entering the CLI command `execute factoryreset`.

164845 In the CLI in `config system interface`, after using the command `set allowaccess` to remove an administrative access method such as `http`, it could not be re-enabled. This could occur for any protocol except for `ping`.

165002 When viewing log messages, the last record was not visible.

165872 Adding a ticket for a policy violation alert would fail.

166380 If only the `admin` account existed and there were no other administrator accounts available to be assigned to a ticket, the ticket assignment would fail.

Known issues

The following are known issues in this release.

Bug ID	Description
131855	Agent-based scan result data and report remains for deleted assets.
165201	In Internet Explorer 9, in *System Log >Historical*, the page load progress indicator at the bottom of the page (i.e. 0.0%) never completes. **Note:** Internet Explorer 9 is ***not*** currently supported.