FortiScan™

Version 4.0 MR2 Patch 3

Release Notes

Revision History

Date	Revision Number	Change Description
2011-10-24	Revision 1	Initial revision.
2011-10-27	Revision 2	Added support for Fedora 15.
2011-10-28	Revision 3	Added resolved issues.
2011-10-28	Revision 4	Sorted resolved issues.

FortiScan 4.0 MR2 Patch 3 Release Notes

Revision 4

28 October 2011

Performance metrics contained herein were attained in internal lab tests under ideal conditions. Network variables, different network environments and other conditions may affect performance results, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding contract 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. Certain Fortinet products are licensed under U.S. Patent No. 5,623,600.

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

This section highlights the major new features and enhancements added since FortiScan 4.0 MR1. For configuration instructions, see the *FortiScan Administration Guide*.

- **FortiScan-VM** — FortiScan is now available as a virtual appliance that can be deployed in virtual machine environments such as VMware vSphere, Citrix XenServer, and the open source Citrix Hypervisor. For VM-specific installation instructions, see the *FortiScan-VM Install Guide*.
- **Administrative domains (ADOMs)** — Assets are now separated into ADOMs for better administration. Users other than default `admin` administrator must be assigned to an ADOM. All asset-related operations can only be performed within that asset's ADOM. When upgrading from firmware prior to FortiScan 4.0 MR2, 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`. After the upgrade, if necessary, you can adjust each account's ADOM assignment and/or each asset's ADOM assignment.
- **Support for assets with identical IP addresses** — Assets on different network segments that use the same IP address space are now supported as long as each asset belongs to a different ADOM.
- **Change to asset filter usage** — Asset filters no longer apply to each individual administrator. Instead, they apply to each individual ADOM. Asset filters define which assets are included in the ADOM. Accounts assigned to an ADOM can affect assets allowed by the ADOM's asset filter, and can use with the network vulnerability scanner (*Network Scan* menu) with any range of IP addresses allowed by the ADOM's asset filter.
- **System settings enhancements** — Configuration of system settings is now more granular. Some settings apply to whole appliance, while others are configured separately for each individual ADOM or asset group.
- **Remediation ticketing** — You can now track vulnerabilities and assign them to specific administrator accounts for remediation, receiving alerts based upon completion status and deadlines.
- **Manually adding assets** — In addition to adding assets by discovering them via a discovery scan, you can now add assets manually either through the web UI or by uploading a file.
- **Sharing benchmarks, policies, and templates between ADOMs** — You can now specify whether newly created OVAL benchmarks, policies, and remediation templates are visible to other ADOMs.
- **Change to Operator role privileges** — Administrators whose *Role* is *Operator* can now use the network vulnerability scanner (Network Scan menu).

System requirements

Upgrading to FortiScan 4.0 MR2 Patch 3 requires FortiScan 3.0 MR1 or later. (New installations do not require any prior installation.) ***If your appliance is running an earlier software release, you must first upgrade it to FortiScan 3.0 MR1 before upgrading it to FortiScan 4.0 MR2 Patch 3.***

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*.

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

- Windows 2000
- 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 software
  - Windows 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:

- **Automatically 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.

- **Manually from Fortinet Technical Support** — You can download a firmware release from:

  https://support.fortinet.com/

  then upload the package to the FortiScan appliance.

  To download manually:

  1. Download the firmware (the `.pkg` file) from the Fortinet Technical Support web site, https://support.fortinet.com.
  2. Log in to the FortiScan appliance's web UI using the `admin` administrator account. Other accounts may not have the required permissions.
  3. From *Current ADOM*, select *Global*.
  4. Go to *System* > *Dashboard* > *Status.*
  5. In the *System Information* widget's *Firmware Version* row, click *Update*. The *Firmware Update* dialog appears.
  6. In the *Manually Upload a Release Package* section, click the *Browse* button and locate the `.pkg` file that you downloaded.
  7. Click *OK* to upload the file to the appliance.
  8. 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 upload release complete. It will take a few minutes to
        unpack the uploaded release. Please wait.”
     ```

  9. 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*. The *Firmware Update* dialog appears.

5. In the *Releases Available for Upgrade* section, in the row corresponding to the FortiScan 4.0 MR 2 Patch 3 firmware package, click the icon in the *Upgrade Firmware* column, then click *OK* in the dialog that appears. The FortiScan appliance installs the firmware and restarts.

   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.

   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:
   - Ping the FortiScan appliance to verify connectivity.
   - Clear your web browser’s cache.
   - Log in to the web UI.

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 Install Guide*.

Resolved issues

This release resolves the following issues in the previous releases, FortiScan 4.0 MR2 Patch 1 and earlier.

Bug ID	Description
152463 154010	FortiScan-VM trial is now low-encryption, suitable for download in countries subject to export controls on encryption strength. To support this, the agent installers now include .NET 4.0 when installing the agent on Windows assets.
154532	On FortiScan-VM with FortiGuard VCM package version 1.215, remote network vulnerability scans failed to complete and generate a report. To solve this, you can upgrade either the firmware with the package, or just the package.
154582	The MSI installers for 32-bit and 64-bit hosts of the FortiScan agent have been combined to simplify deployment.
154597	On FortiScan-VM, with some network configurations, route confusion could occur. To prevent this, by default, port2, port3, and port3 are now disabled.
155516	FortiScan-VM now includes agent installers. Now, no upload of the .pkg firmware file is required during installation.

Known issues

There are no known issues.