FortiScan v5.0 MR1 Patch Release 1

Release Notes

FortiScan v5.0 MR1 Patch Release 1 Release Notes

September 26, 2013

17-511-218717-20130926

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
2013-09-26	Initial release.

Introduction

This document provides a summary of enhancements, support information, and installation instructions in FortiScan v5.0 MR1 Patch Release 1 build 0315. Please review all sections in this document prior to upgrading your device. For more information on upgrading your FortiScan device, see the *FortiScan v5.0 MR1 Administration Guide* at http://docs.fortinet.com.

This document include the following sections:

Supported models

The following models are supported on FortiScan v5.0 MR1 Patch Release 1.

FortiScan

FSC-1000B, FSC-1000C, FSC-3000C, and FSC-3000D.

FortiScan VM

FSC-VM.

See http://docs.fortinet.com/fscan.html for additional documents on FortiScan v5.0 MR1.

Special Notices

Before any upgrade

To minimize any adverse impact your users and your network, plan the firmware upgrade during a maintenance window. This allows you to properly upgrade, test, and implement the firmware upgrade.

Save a copy of your FortiScan configuration prior to upgrading. To backup your FortiScan configuration, go to *System* > *Maintenance* > *Backup & Restore*. Select *Backup* and save the configuration file to your management computer.

In VMware environments, it is recommended that you take a *Snapshot* of the VM instance prior to upgrading. In the event of an issue with the firmware upgrade, use the *Snapshot Manager* to revert to the *Snapshot*. To create a *Snapshot*, right-click the VM instance and select *Snapshot* > *Take Snapshot*.

In Citrix XenServer environments, it is recommended that you take a Snapshot of the VM instance prior to upgrading. In the event of an issue with the firmware upgrade, use *Virtual Machines Snapshots* to revert to the *Snapshot*. To create a Snapshot, right-click the VM instance and select *Take a Snapshot*.

Open Source Xen does not natively support *Snapshots*. You can create a backup of LVM partitions with the *LVM Snapshots* feature and then restore this backup. You can also use Linux commands to backup and restore a virtual machine.

Upgrade Information

FortiScan firmware images

Fortinet provides FortiScan software in three formats:

- .out: Use this image for new FortiScan appliance installations. The file contains the FortiScan operating system.
- .zip or .tgz: Use this image for new FortiScan VM installations. This package contains the OVF and VMDk files.
- .pkg: Use this image for updating an existing installation. This package contains the .out file, push installer, Microsoft installer and other software required by the agent, and the FortiScan Release Notes.

Please review the Special Notices and Product Integration and Support chapters prior to upgrading. For more information on upgrading your FortiScan device, see the *FortiScan v5.0 MR1 Administration Guide* at http://docs.fortinet.com.

Upgrading from FortiScan v5.0 MR1

FortiScan v5.0 MR1 Patch Release 1 build 0315 officially supports upgrade from FortiScan v5.0 MR1 build 0310. Please upgrade to FortiScan v5.0 MR1 before upgrading to FortiScan v5.0 MR1 Patch Release 1. For more information, see the *FortiScan v5.0 MR1 Release Notes*.

General firmware upgrade steps

FortiScan periodically polls the FortiGuard Distribution Network (FDN) for a list of new firmware packages. If the device has a valid support contract, FortiScan automatically downloads the available firmware packages to its internal hard drive. Optionally you can select to manually upload a release package that you downloaded from the Customer Service & Support portal FTP directory.

The following table lists the general firmware upgrade steps.

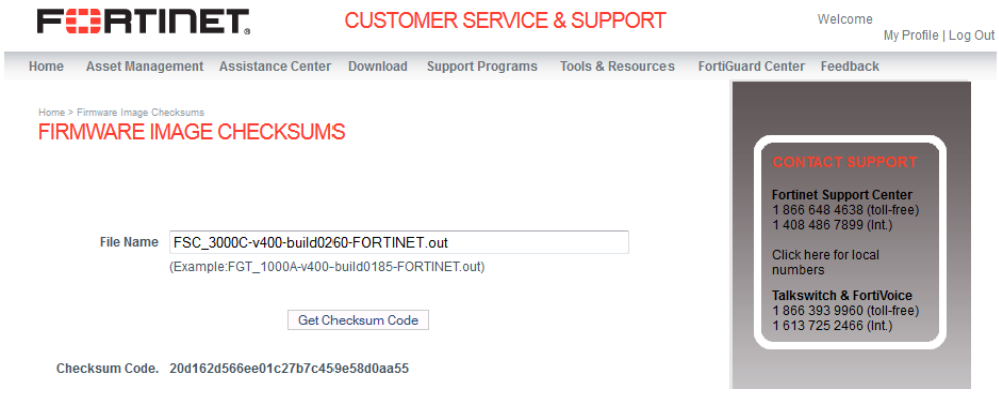
Table 1: Upgrade steps

Step 1	Prepare your FortiScan for upgrade.
Step 2	Backup your FortiScan system configuration. For FortiScan VM, take a *Snapshot* of the VM instance.
Step 3	Transfer the firmware image to your FortiScan device.
Step 4	Log into your FortiScan Web-based Manager to verify the upgrade was successful.

Step 1: Prepare your FortiScan for upgrade

1. Download the appropriate firmware image from the Customer Service & Support portal FTP directory.
2. To verify the integrity of the download, go back to the *Download* section of the login page, then select the *Firmware Image Checksums* link.

Figure 1: Firmware image checksums page



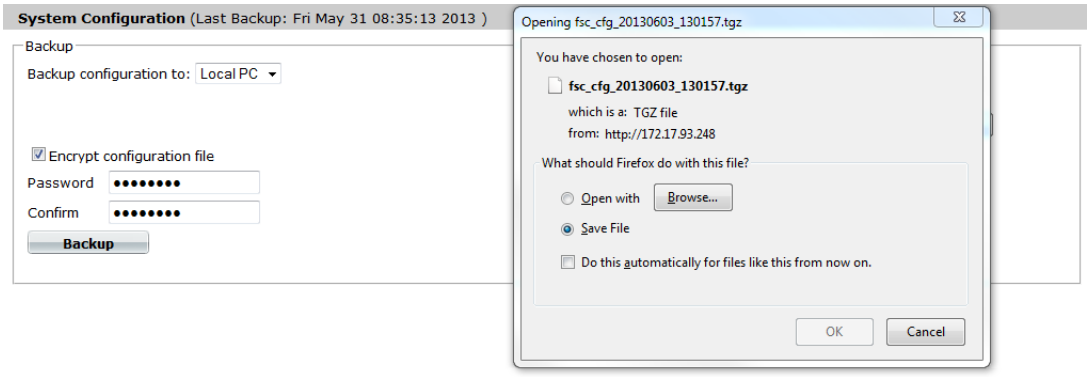
3. Enter the file name and select *Get Checksum Code* to get the firmware image checksum code. Compare this checksum with the checksum of the firmware image.

Step 2: Back up your FortiScan configuration

1. Go to *System* > *Maintenance* > *Backup & Restore*.
2. Select the checkbox to encrypt the configuration file and enter a password.
3. Select *Backup*. A backup dialog box opens and prompts you to save the file to your management computer.

   The *Backup* dialog box opens.

Figure 2: Backup dialog box

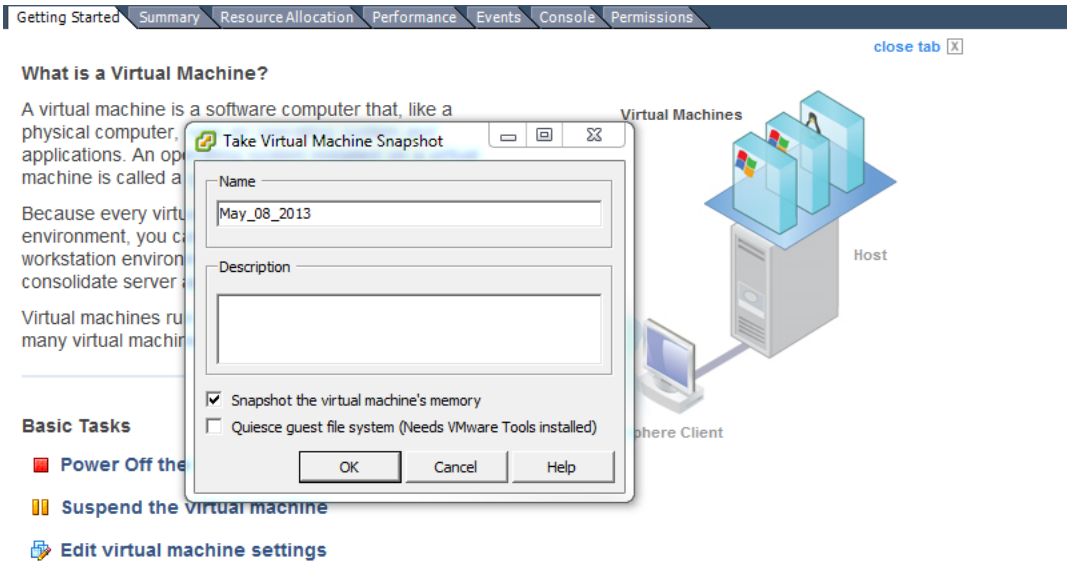


4. Select OK to save the backup file on your management computer.

When selecting to encrypt the backup configuration file, the same password used to encrypt the file will be required to restore this backup file to the FortiScan device.

5. In VM environments, it is recommended that you take a *Snapshot* of the VM instance. In the event of an issue with the firmware upgrade, use the *Snapshot Manager* to revert to the *Snapshot*. To create a *Snapshot*, right-click the VM instance and select *Snapshot* > *Take Snapshot*.

Figure 3: Snapshot of FortiScan VM (VMware)

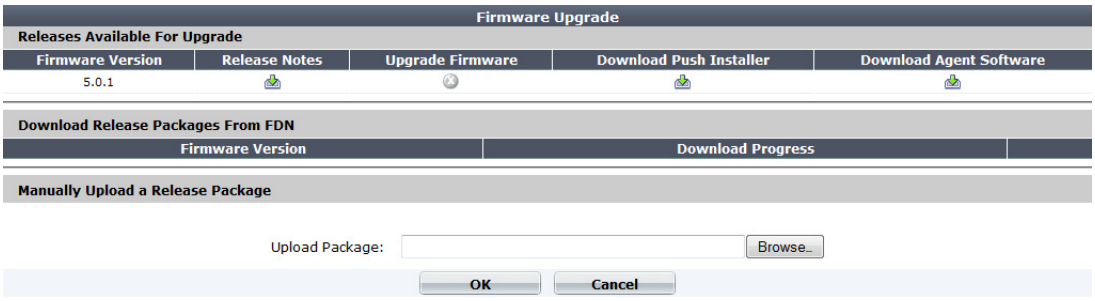


Step 3: Transfer the firmware image to your FortiScan device

1. Go to *System* > *Dashboard* > *Status*.
2. In the *System Information* widget, in the *Firmware Version* field, select *Update*.

   The *Firmware Upgrade* dialog box opens.

Figure 4: Firmware upgrade dialog box



3. Select *Browse* to locate the firmware package (`.pkg` file) that you downloaded from the Customer Service & Support portal and select *Open*.
4. Select *OK. Your* FortiScan will upload the firmware image and you will receive the confirmation message *Manual release upload is complete. It will take a few minutes to unpack the uploaded release. Please wai*t.

Step 4: Upgrade your device and agents

1. Select Return. You will see the package in the *Firmware Upgrade* page in the *Releases Available for Upgrade* section.
2. In the Upgrade Firmware column, select the upgrade icon and then select OK in the dialog box that appears. The FortiScan installs the firmware image and restarts.

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

All credentials are reset to default when the system is upgraded from v4.0 MR3 to v5.0.0 or later. These credentials must be reconfigured upon upgrade. These include the passwords configured for ADOMs, Asset Group, and individual assets.

3. When the upgrade is complete, clear your web browser cache and log in to the Web-based Manager.
4. Update each asset's FortiScan agent software. For more information, see the *FortiScan v5.0 MR1 Administration Guide*.

Downgrading to previous versions

Downgrading FortiScan to previous versions is not supported.

Product Integration and Support

Web browser support

FortiScan v5.0 MR1 Patch Release 1 supports the following web browsers:

- Microsoft Internet Explorer version 8
- Mozilla Firefox versions 3.5 to 9.0

Other web browsers may function correctly, but are not supported by Fortinet.

Virtualization software support

FortiScan v5.0 MR1 Patch Release 1 supports the following virtualization software:

- VMware ESX version 4.0 and 4.1
- VMware ESXi versions 4.0, 4.1, 5.0, and 5.1
- Citrix XenServer version 5.6
- Open Source Xen Hypervisor version 3.0.3

See "FortiScan VM" for more information.

Host platform support

FortiScan v5.0 MR1 Patch Release 1 supports the following host platforms:

- Microsoft Windows 8 (32-bit and 64-bit)
- Microsoft Windows 7 (32-bit and 64-bit)
- Microsoft Windows Vista (32-bit and 64-bit) (Enterprise/Business)
- Microsoft Windows XP (32-bit and 64-bit)
- Microsoft Windows Server 2012
- Microsoft Windows Server 2008 R2 (64-bit)
- Microsoft Windows Server 2008 (32-bit and 64-bit)
- Microsoft Windows Server 2003 (32-bit and 64-bit)
- Red Hat 9
- Red Hat Enterprise Server 6 (32-bit and 64-bit)
- Red Hat Enterprise Server 5 (32-bit and 64-bit)
- Red Hat Enterprise Server 4
- Red Hat Enterprise Server 3
- Fedora 15 (32-bit and 64-bit)
- Fedora 14 (32-bit and 64-bit)
- Fedora 13 (32-bit and 64-bit)
- CentOS 5
- CentOS 4

- CentOS 3
- Solaris 10 (x86 32-bit and 64-bit)
- Solaris Sparc 10
- Solaris Sparc 9

Resolved Issues

The resolved issues listed below do not list every bug that has been corrected with FortiScan v5.0 MR1 Patch Release 1 build 0315. For inquires about a particular bug, please contact Customer Service & Support.

Table 2: Resolved issues

Bug ID	Description
211425	FortiScan reflected XSS vulnerability.
216750	Vulnerability CVE-2010-0265 is not detected in Microsoft Windows XP and Vista.
217270	Network audit scan with Microsoft Windows benchmark fails.

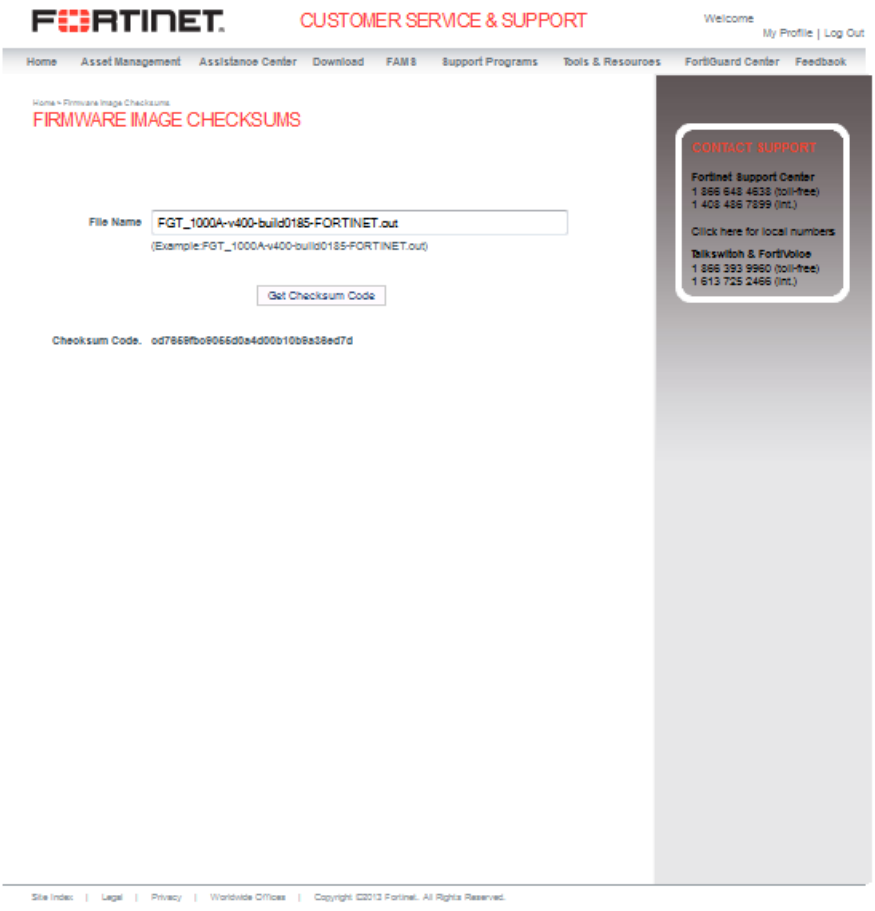
Known Issues

There are no known issues identified with FortiScan v5.0 MR1 Patch Release 1 build 0315. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Firmware Image Checksums

The MD5 checksums for all Fortinet software and firmware releases are available at the Customer Service & Support portal located at https://support.fortinet.com. After logging in, select *Download* > *Firmware Image Checksum*, enter the image file including the extension, and select *Get Checksum Code*.

Figure 5: Firmware image checksum tool



Appendix A: FortiScan VM

Licensing

Fortinet offers the FortiScan VM in a stackable license model. This model allows you to expand your VM solution as your environment expands. When configuring your FortiScan, ensure to configure hardware settings as outlined in Table 3 and consider future expansion needs.

Table 3: FortiScan VM license information

Technical Specification	VM-Base	VM-100	VM-1000	VM-5000	VM-20000
Hypervisor Support	VMware ESX versions 4.0 and 4.1 VMware ESXi versions 4.0, 4.1, 5.0, and 5.1 Citrix XenServer version 5.6 Open Source Xen Hypervisor version 3.0.3				
VM Form Factor	Open Virtualization Format (OVF)				
Administrative Domains (ADOMs)	10,000				
Virtual CPUs (Minimum / Maximum)	1 / Unlimited				
Virtual Network Interfaces (Minimum / Maximum)	1 / 4				
Virtual Memory (Minimum / Maximum)	1GB / Unlimited				
Virtual Storage (Minimum)	40GB				
Device Quota	200GB	+200GB	+1TB	+8TB	+16TB

FortiScan VM firmware

Fortinet provides FortiScan VM firmware images for VMware and Xen environments.

VMware

- `.pkg`: Download this 64-bit firmware image to upgrade your existing FortiScan VM installation.
- `.out.esx.zip`: Download this 64-bit package for a new FortiScan VM installation in a VMware ESX/ESXi environment.

Xen

- .out.citrix.zip: Download this 64-bit package for a new FortiScan VM installation in a Citrix XenServer environment.
- .out.xen.tgz: Download this 64-bit package for a new FortiScan VM installation in a Open Source Xen environment.