FortiCache 3.0
Release Notes

FortiCache 3.0 Release Notes

August 20, 2014

Revision 1

Technical Documentation	http://help.fortinet.com
Knowledge Base	http://kb.fortinet.com
Forums	https://support.fortinet.com/forums
Customer Service & Support	https://support.fortinet.com
Training	http://training.fortinet.com
FortiGuard Threat Research & Response	http://www.fortiguard.com
License Agreement	http://www.fortinet.com/doc/legal/EULA.pdf
Document Feedback	Email: techdocs@fortinet.com

Table of contents

Introduction

This document provides installation instructions and caveats, resolved issues, and known issues for FortiCache 3.0, build 0010. Please review all sections of this document prior to upgrading your device.

For additional documentation, please visit:

http://docs.fortinet.com/forticache/

Supported models

The following models are supported on FortiCache 3.0, build 0010.

Hardware & VM support

FortiCache 3.0 supports:

- FortiCache 400C
- FortiCache 1000C
- FortiCache 1000D
- FortiCache 3000C
- FortiCache 3000D
- FortiCache VM64

Special Notices

TFTP boot process

The TFTP boot process erases all current FortiCache configuration and replaces it with the factory default settings.

Monitor settings for web-based manager access

Fortinet recommends setting your monitor to a screen resolution of 1600x1200. This allows for all the objects in the Web-based Manager to be viewed properly without need for scrolling.

Before any upgrade

Save a copy of your FortiCache unit configuration prior to upgrading. *Go to System* > *Maintenance* > *Config* and select *Download Backup File* to backup the configuration.

After any upgrade

If you are using the Web-based Manager, clear your browser cache prior to login on the FortiCache to ensure the Web-based Manager screens are displayed properly

CVE-2014-0160 Statement

FortiCache 3.0 does not utilize a version of OpenSSL that is vulnerable to CVE-2014-0160.

What's new

FortiCache 3.0 is a major release designed to give greater feature parity with FortiOS. This release introduces features including:

System Enhancements

GUI Simplification: Option in the GUI to hide unused components.

Replacement messages: Ability to customize replacement pages with local branding.

Digital certificate support: Ability to make certificate signing requests to an external CA.

User Identity Based Policies: Improved user policies for identification of users and application of security policy.

Enhanced Logging Policy: Option to log all security events or all sessions

Centralized Management: Several system changes have been made to support centralized management. Contact your account manager for details of FortiCache Manager, centralized management console.

HTTPS Inspection

FortiCache 3.0 adds the ability to decrypt and inspect HTTPS traffic. This enables security (antivirus and web content filtering) and caching profiles to be applied to the requested content.

Web Content Filtering

Significant enhancements have been made to the Web Content Filtering including:

WCF Usage Quotas: Usage quotas can now be applied to Categories with Monitor, Warning and Authenticate Actions

Safe Search Enhancements: Added support for Yandex! To Safe Search Engine and Youtube education filtering.

Search keyword logging: Ability to log all keywords entered into supported search engines.

User Identification

AD Server Polling: FortiCache now supports polling of AD logon activity directly in addition to via an external FSSO Agent. FortiCache AD Server Polling is suitable for smaller requirements, whereas the external agent is more applicable to large deployments.

RADIUS Single-Sign-On: FortiCache supports user identification from external RADIUS sources via Accounting packets.

Logging

Logging Enhancements: Additional logging detail has been added and separated for convenience. New logs include

- Local Traffic Log
- Forward Traffic Log

- System logs – System
- Router
- Users
- WanOpt and Cache

Support for Webtrends logging format has been added (CLI only)

FortiAnalyzer Support: Native FortiAnalyzer support has been added to FortiCache 3.0. Extended HTTP-transaction logging now supports logging traffic-in/out and URL for each http request. Real time upload and encrypted transmission is now supported. Additional reports are now supported in the latest FortiAnalyzer release.

Upgrade instructions

Back up your configuration before beginning this procedure. Whilst no data loss should occur if the procedures below are correctly followed, it is recommended a full backup is made before proceeding.

For information on how to back up the FortiCache configuration, see the FortiCache Administration Guide.

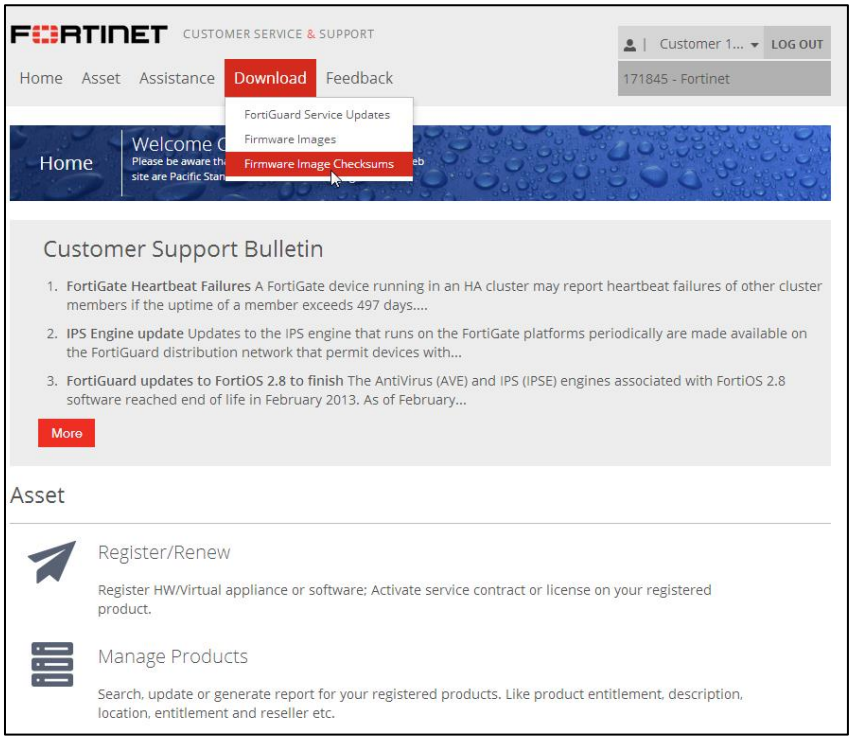
Image checksums

To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available from Fortinet Customer Service & Support:

https://support.fortinet.com

Figure 1: Customer Service & Support image checksum tool



After logging in to the web site, in the menus at the top of the page, click *Download*, then click *Firmware Image Checksums*.

Alternatively, near the bottom of the page, click the *Firmware Image Checksums* button. (The button appears only if one or more of your devices has a current support contract.) In the *File Name* field, enter the firmware image file name including its extension, then click *Get Checksum Code*.

Upgrading from previous releases

Whilst FortiCache 3.0 (build 0010) supports upgrade from previous releases, due to the significant feature changes, migration of configuration may not be fully supported and reconfiguration may be required. This will be resolved in a future patch release.

Firmware upgrade process

After backing up your configuration first, follow the following procedure to upgrade the firmware.

Before you can install FortiCache firmware, you must download the firmware package from the Customer Service & Support web site, then upload it from your computer to the FortiCache unit.

1. Log in to the Customer Service & Support web site at https://support.fortinet.com. In the Download section of the page, select the Firmware Images link to download the firmware.
2. To verify the integrity of the download, go back to the Download section of the login page, then click the Firmware Image Checksums link.
3. Log in to the FortiCache unit's Web-based Manager using the admin administrator account.
4. *Go to System > Dashboard > Status.*
5. In the System Information widget, in the Firmware Version row, select Update. The Firmware Upgrade or Downgrade dialog box opens.
6. In the Firmware section, select Choose File, and locate the upgrade package that you downloaded.
7. Select *OK* to upload the file to the FortiCache.

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, the following message is shown:

Wait until the unpacking, upgrade and reboot process completes (usually 3-5 minutes), then refresh the page.

Product Integration and Support

Web browser support

The following web browsers are supported by FortiCache 3.0:

- Microsoft Internet Explorer versions 8 to 11
- Mozilla Firefox versions 15 to 31
- Google Chrome versions 22 to 36

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

Virtualization software support

FortiCache 3.0 supports VMware ESXi / ESX 4.0, 4.1, 5.0, 5.1 and 5.5.

See Appendix A: FortiCache VM for more information.

Language Support

The following table lists FortiCache Language Support information.

Table 1: FortiCache Language Support

Language	Web-based Manger	Documentation
English	✓	✓
French (France)	✓	-
Spanish (Spain)	✓	-
Portuguese (Brazil)	✓	-
Korean	✓	-
Chinese (Simplified)	✓	-
Chinese (Traditional)	✓	-
Japanese	✓	-

To change the FortiCache language setting, go to *System > Admin > Settings, in View Settings> Language* and select the desired language on the drop-down menu

Resolved issues

The resolved issues listed below do not list every bug that has been corrected with this release. For inquires about a particular bug, please Fortinet Customer Service & Support:

https://support.fortinet.com

Table 2: Resolved issues

Bug ID	Description
0210223	Firewall Address Validation Failure
0217790	Support remote RADIUS authentication for webadmins
0250163	Support interface bypass in 3000D hardware
0247843	Bootloader TFTP upgrade fails
0241270	Transparent mode proxy should return the direct server error or timeout rather than '504' or '502' replacement message returned from FortiCache

Known issues

This section lists the known issues of this release, but is not a complete list. For inquires about a particular bug, please contact Fortinet Customer Service & Support:

https://support.fortinet.com

Table 3: Known issues

Bug ID	Description
0251710	Support upgrade config migration
0251719	Incorrect network hardware (VMXNet2) may be selected on VM ESXi install. **Workaround:** Power off the VM, delete the interface and recreate E1000 interfaces.