FortiDNS v1.0 MR3
Release Notes

FortiDNS v1.0 MR3 Release Notes

June 06, 2013

24-130-208911-20130606

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 4
Introduction 5
Supported models 5
Summary of enhancements 5
Special Notices 6
TFTP boot process 6
Monitor settings for Web-based Manager access 6
Before any upgrade 6
After any upgrade 6
Upgrade Information 7
Upgrading from FortiDNS v1.0 MR2 7
Upgrade procedure 7
Downgrading to previous versions 7
Product Integration and Support 8
Web browser support 8
Resolved Issues 9
Authentication 9
DHCP 9
DNS 10
Domain Query Protection (DQP) 10
Other 11
Web-based Manager 12
Known Issues 14
Firmware Image Checksums 15

Change Log

Date	Change Description
2013-06-06	Initial release.

Introduction

This document provides a summary of enhancements, support information, installation instructions, integration, resolved and known issues in FortiDNS v1.0 MR3 build 0175. Please review all sections of this document prior to upgrading your device.

This document includes the following sections:

- Special Notices
- Upgrade Information
- Product Integration and Support
- Resolved Issues
- Known Issues
- Firmware Image Checksums

Supported models

The following models are supported on FortiDNS v1.0 MR3:

FNS-400C, FNS-1000C, and FNS-3000D.

See http://docs.fortinet.com/fdns.html for additional documents on FortiDNS v1.0.

Summary of enhancements

The following is a list of enhancements in FortiDNS v1.0 MR3:

- Botnet protection: Added a new Botnet category to the FortiGuard Domain Query Protection Service. This category differs from the existing list as it uses a dynamically updated list of botnet member IP addresses supplied by FortiGuard (subject to valid license). When a DNS query resolves to one of those IP addresses, it can be blocked, redirected and/or logged.

Special Notices

TFTP boot process

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

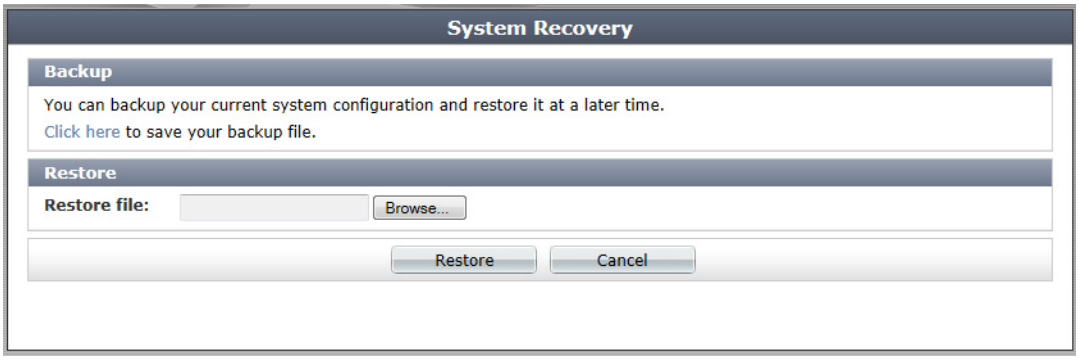
Monitor settings for Web-based Manager access

Fortinet recommends setting your monitor to a screen resolution of 1280x1024. This allows for all the objects in the Web-based Manager to be viewed properly.

Before any upgrade

Before any upgrade, save a copy of your FortiDNS unit configuration to your management computer. Go to *System* > *Maintenance* > *Config* and select *Click here* to backup the configuration.

Figure 1: System recovery window



After any upgrade

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

Upgrade Information

Upgrading from FortiDNS v1.0 MR2

FortiDNS v1.0 MR3 build 0175 officially supports upgrade from FortiDNS v1.0 MR2 build 0117 or later.

Upgrade procedure

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

1. Log in to the Customer Service & Support portal at https://support.fortinet.com.
2. In the *Download* section of the page, select the *Firmware Images* link to download the firmware.
3. To verify the integrity of the download, go back to the *Download* section of the login page, then select the *Firmware Image Checksums* link.
4. Log in to the FortiDNS unit's Web-based Manager using the *admin* administrator account.
5. Go to *System* > *Dashboard* > *Status*.
6. In the *System Information* widget, in the *Firmware Version* row, select *Upgrade*.

   The *Firmware Upgrade* or *Downgrade* window opens.

   Figure 2: Firmware upgrade or downgrade window

7. In the *Firmware* section select *Browse* and locate the upgrade package that you downloaded.
8. Select *OK* to upload the file to the FortiDNS.

   Your browser uploads the firmware file. The time required varies by the size of the file and the speed of your network connection.

Downgrading to previous versions

FortiDNS does not provide a full downgrade path. For those users who want to downgrade to an older FortiDNS firmware release, downgrade the system firmware via a TFTP server with the firmware burning procedure embedded within the FortiDNS system boot-up menu. All configuration will be lost after downgrading the device.

Product Integration and Support

Web browser support

The following web browsers are supported by FortiDNS v1.0 MR3:

- Microsoft Internet Explorer version 9
- Mozilla Firefox versions 20
- Google Chrome version 26

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

Resolved Issues

The resolved issues table below does not list every bug that has been corrected with FortiDNS v1.0 MR3 build 0175. For inquires about a particular bug, please contact Customer Service & Support.

Authentication

Table 1: Resolved authentication issues

Bug ID	Description
174209, 196359	Entering a large number of characters in the RADIUS server secret field causes an internal server error.
178770	Creating duplicate remote RADIUS servers should not be allowed.
189548	RADIUS authentication type uses PAP only regardless of the type selected.
189590	Include Fortinet CA in the FortiDNS firmware by default.
192655	When editing a remote RADIUS server, the secret is not saved properly.
192747	When editing a remote LDAP server, the password is not saved properly.
196484	An internal server error occurs when resetting the password with username.
196804	Secure LDAP authentication does not work.

DHCP

Table 2: Resolved DHCP issues

Bug ID	Description
167132	Shrink dhcp_page_render.js to mini version.
169723	Users should be able to clear the DHCP lease database.
178704	The default DHCP range type should be consistent.
189222	Removed table limits for DHCP options that are no longer defined at the device model level.
196057	A read-only user cannot view DHCP option set details.

DNS

Table 3: Resolved DNS issues

Bug ID	Description
177673	Domain redirection interface validation - currently in use interface.
188685, 190914	When starting the DNS service in the *DNS General Settings* page, an invalid syntax error is displayed.
194299, 194618	The DNS request summary widget's time period filter is broken.
197839, 197984	Failed to flush DNS cache.
197860, 198763	Non-ASCII DQP White/Blacklist domain causes a DNS synchronization error.

Domain Query Protection (DQP)

Table 4: Resolved DQP issues

Bug ID	Description
189630	Added a category filter for the DQP widget.
190303, 190305	Failed to delete a DQP server address or port address.
196049	Returned a *null* error when selecting *Update Now* for DQP if the user is read-only.
190307	DQP charts cannot be translated using Google Chrome.
190313	No return from button *Check for Update* without DQP server connection.
191771	Enable DQP update button feedback.
191887	DQP update polling (looking for last update date/time) needs to pass back DQP category counts.
192003	Zero domain blacklist popup in DQP widget using Internet Explorer.
192115	Spam URL is not displayed in the DQP widget.
192419	DQP update polling needs to trigger only on update.
193059, 194429, 192654	DQP update state should be displayed in the Web-based Manager.
193912	Bootup errors when DQP wants to clear the database.
194928	Abnormal DQP update behavior.
196377	Check memory before enabling DQP.

Table 4: Resolved DQP issues (continued)

Bug ID	Description
198892	One DQP update state is not handled by the Web-based Manager.
198951	Packet loss related DQP update issues.
197433	Botnet number is not updated after restoring the DQP version manually in the database.
197655	Time period does not work well in the DQP widget.
200889	Remove the time-stamp for a successful DQP update.
200407	DQP update failure not being handled in the Web-based Manager; failed to clear existing DQP data.

Other

Table 5: Other resolved issues

Bug ID	Description
158021, 165993	No validation performed on SNMP threshold form input fields.
160800	General setting forms lose state if any field fails validation.
178088, 196057	Assignment list does not show permission denied on submit for read-only users.
183705	The VLAN interface is not able to be removed if a global ACL list exists.
184304	Upgrade to Nominum Vantio 5.3.2.0.
187869	Changed the name field to client IP address in DNS audit logs & client.
188673	Unable to generate a netmask for SNMP IPv6 hosts.
189199	The incorrect year/month in the stored configuration file name.
189629	The number of items displayed in the audit log viewer is now configurable.
190020	Time period label issue.
190317	Multiple clicking *Check for Update* when fgd_dqp_poll is running.
190787	Upgrade to Nominum DCS 4.2.0.1
191217, 197525	Django Security Update.
193142	Issue with default system time & time zone.
193494	Need validation on the showing number setting.
193498	Wrong time period filtering in the second level if set period as week or month.
193767	Encrypted keys can be shown in SNMP configuration page.

Table 5: Other resolved issues (continued)

Bug ID	Description
194105	When the read-only settings is disabled, the user still has read-only rights.
194243	An error is displayed when deleting a VLAN.
194496	Stale PID files left on disk after reboot can prevent daemon launch.
195665	A removed VLAN interface is still visible.
196160	The free memory pop-up dialog box is not supported using Internet Explorer and Firefox.
197070	Prompt for user confirmation on reboot and shutdown.
197693	Time period does not work for *Blacklist* in the *Top Clients* widget.
197703	No-log blacklist entries also matching logged blacklist are logged.
202870	Reduce first boot time caused by license polling; no route to servers on first boot.
203246	Booting VM with no network interfaces results in startup errors.
203379	VLAN interface is removed in underlying system after reboot.
203752	Routes based on VLAN interface are removed in the underlying system after reboot.

Web-based Manager

Table 6: Resolved Web-based Manager issues

Bug ID	Description
194299, 194618	DNS request summary widgets time period filter is broken.
178089	Read-only user blacklist page expands to full ACL rule.
179135, 178438	Read-only users cannot use the Web-based Manager terminal console.
187868	Color issue with the titles in the DNS audit logs table.
188595	Stacked bar chart issue.
190508	The DQP widget is unable to handle a large number of logs entries.
190511	Suggest use 'K' as unit for the scalar in DQP widget.
190578, 190261, 190484	Sometimes the last number in DQP widget bar is omitted.
191356, 193640	Resolve client IPs to names in the *DNS Suspicious Clients* widget.

Table 6: Resolved Web-based Manager issues (continued)

Bug ID	Description
191607	DQP update logs should not show up in Web-based Manager logs.
191738	*Top Client* / *Top Domain* widgets reports incorrect time for data.
192423	Dashboard widget refresh prevents idle timeouts.
192810	Warn about unsupported browsers in the login page.
192887	Filter does not work if the number equal or bigger than 4294967296 in DNS audit log.
193033, 196298	Only one line is displayed in the CLI terminal widget using Google Chrome.
193621	Internal server error in the widget.
193630	Data in *Top Domains* and *Top Clients* widgets in not correct.
193633	*Top Client* and *Top Domain* widgets do not properly render measurement lines.
194189	Ordering issue in *Suspicious Domain* widget.
194195	An expired license is not displayed in the Web-based Manager.
194197	The limited LVP (DQP) list in license in not displayed.
194239	Display the total device RAM in the dashboard.
194602	No data in some widgets when DNS service is not running.
194611	The *DNS Statistics* widget displays incorrect information.
195318, 194088	Time labels are too close to the bottom in the *DNS Request Summary* widget.
195687	Race condition on session check.
196046, 196448	Incorrect behavior for service start when the license has expired.
200187	Internal server error when selecting *Blacklist* in the *Top Clients* widget.

Known Issues

There are no known issues that have been reported with FortiDNS v1.0 MR3 build 0175. 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 website located at https://support.fortinet.com. After logging in, click on *Download* > *Firmware Image Checksum*, enter the image file including the extension, and select *Get Checksum Code*.

Figure 3: Firmware image checksum tool