FortiPortal Release Notes

Version 5.3.0

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

November 22, 2019

FortiPortal 5.3.0 Release Notes

3rd Edition

TABLE OF CONTENTS

Change log

Date	Description
October 9, 2019	Initial release for FortiPortal 5.3.0
October 10, 2019	Updated the “FortiManager, FortiOS, FortiAnalyzer, and FortiSandbox supported versions” section.
November 22, 2019	Updated the “FortiManager, FortiOS, FortiAnalyzer, and FortiSandbox supported versions” section.

Introduction

FortiPortal is a self-service portal for FortiManager and a hosted security analytics management system for the FortiGate, FortiWifi, and FortiAP product lines. FortiPortal is available as a virtual machine (VM) software solution that can be deployed on a hosted services infrastructure. This allows MSSPs and Enterprises to build highly customized private cloud services for their customers.

This document provides information about FortiPortal version 5.3.0, build 0270. It includes the following sections:

What's new

This release contains the following new features and enhancements:

- You can now use the FortiPortal REST API to do the following:
  - Assign FortiAnalyzer reports to a customer or unassign them
  - List available FortiAnalyzer reports for a customer or change the report list
  - Add a FortiAnalyzer unit to FortiPortal or remove it
  - Update the information for an existing FortiAnalyzer
  - List all FortiAnalyzer units connected to FortiPortal or list detailed information about one FortiAnalyzer unit
  - List FortiAnalyzer report templates for a FortiAnalyzer unit.
- FortiAnalyzer 6.2.1 and 6.2.2 are now supported for both reports and analytics.
- FortiManager 6.2.1 and 6.2.2 are now supported.
- FortiOS 6.2.1 and 6.2.2 are now supported.
- You can now use a fully qualified domain name when you specify the database server with the `set server` command.
- You can now create and edit DNS filter profiles.
- FortiAnalyzer mode now supports the drill-down capability in the following dashboard widgets:
  - Top Countries
  - Top Threats
  - Top Sources
  - Top Destinations
  - Top Applications
- You can configure an SD-WAN for an ADOM.
- You can now monitor SD-WAN interfaces using a map view.
- You can now restore a custom theme after upgrading.

FortiManager, FortiOS, FortiAnalyzer, and FortiSandbox supported versions

FortiPortal's self-service interface for MSSP customers uses FortiManager's API for FortiGate firewall policy and IPsec VPN configuration.

FortiPortal optionally connects FortiGate wireless controllers for wireless analytics.

FortiPortal allows users to view FortiAnalyzer reports assigned to the MSSP customer.

FortiPortal 5.3.0 supports the following versions of Fortinet products:

Fortinet Product	Supported Versions	Recommended Version
FortiAnalyzer (for reports and analytics)	• 6.0.0 • 6.0.1 • 6.0.2 • 6.0.3 • 6.0.4 • 6.0.5 • 6.0.6 • 6.0.7 • 6.2.1 • 6.2.2	6.2.2

Fortinet Product	Supported Versions	Recommended Version
FortiAnalyzer (for reports)	• 5.6.0 • 5.6.1 • 5.6.2 • 5.6.3 • 5.6.4 • 5.6.5 • 5.6.7 • 5.6.8 • 5.6.9 • 5.6.10 • 6.0.0 • 6.0.1 • 6.0.2 • 6.0.3 • 6.0.4 • 6.0.5 • 6.0.6 • 6.0.7 • 6.2.1 • 6.2.2	6.2.2

Fortinet Product	Supported Versions	Recommended Version
FortiManager	• 5.2.10 • 5.4.0 • 5.4.1 • 5.4.2 • 5.4.3 • 5.4.4 • 5.4.5 • 5.4.6 • 5.6.0 • 5.6.1 • 5.6.2 • 5.6.3 • 5.6.4 • 5.6.5 • 5.6.6 • 5.6.7 • 5.6.8 • 5.6.9 • 5.6.10 • 6.0.0 • 6.0.1 • 6.0.2 • 6.0.3 • 6.0.4 • 6.0.5 • 6.0.6 • 6.0.7 • 6.2.1 • 6.2.2	6.2.2

Fortinet Product	Supported Versions	Recommended Version
FortiOS	• 5.2.x • 5.6.0 • 5.6.1 • 5.6.2 • 5.6.3 • 5.6.4 • 5.6.5 • 5.6.6 • 5.6.7 • 5.6.8 • 5.6.9 • 5.6.10 • 6.0.0 • 6.0.1 • 6.0.2 • 6.0.3 • 6.0.4 • 6.0.5 • 6.0.6 • 6.0.7 • 6.2.1 • 6.2.2	6.2.2
FortiSandbox	• 3.0.2	3.0.2

NOTE: Refer to FortiOS and FortiManager release notes for detailed compatibility information.

NOTE: Use FortiGate 4.0.0 or later to get support for local AP's.

NOTE: If you are using FortiManager version 5.2.3 or later, you must ensure that the FortiManager user account (that you created for FPC) has Remote Procedure Call (RPC) set to *read-write*.

In previous FortiManager releases, RPC was enabled by default. FortiManager version 5.2.3 introduced a new setting that you might need to configure as follows:

```
config system admin user
   get – lists all of the users (along with userids)
       - note the userid for the FPC user.
   edit <FPC userid>
      set rpc-permit read-write
```

Additional compatibility resources

For FortiAnalyzer and FortiManager compatibility with each FortiOS release, refer to the FortiManager Compatibility Chart:

http://docs.fortinet.com/d/fortimanager-compatibility

The respective release notes provide detailed compatibility information, including the hardware models supported and any product limitations.

Hypervisor support

The following hypervisor platforms are supported:

- VMware ESX Server versions 5.5, 6.0, 6.5, and 6.7
- KVM Version 2.6.x

Database support

The following MySQL versions are supported:

- MySQL 5.5.x
- MySQL 5.7.x

NOTE: If you are using MySQL 5.7.x, the following changes MUST be added to the `my.cnf` file:

```
sql_mode = STRICT_TRANS_TABLES,NO_ZERO_IN_DATE,NO_ZERO_DATE,ERROR_FOR_
DIVISION_BY_ZERO,NO_AUTO_CREATE_USER,NO_ENGINE_SUBSTITUTION
```

In addition, the following MariaDB server versions are supported:

- 10.2.X-MariaDB-10.2.X+maria~xenial-log mariadb.org binary distribution

NOTE: The MariaDB server versions do not require additional configuration, except for Bind-Address and Grant Privileges. See the “Upgrading FortiPortal software” chapter of the *FortiPortal Administration and User Guide*.

Web browser support

The following web browsers are supported:

- Microsoft Internet Explorer (IE) Version 11
- Mozilla Firefox (up to) Version 49
- Google Chrome Version 52

NOTE: Other (versions of the) browsers might also function but are not fully supported in this release.

FortiPortal 5.3.0 software

FortiPortal is delivered as virtual machine OVF/QCOW2 files for the VMware/KVM hypervisors.

Follow these steps to download the OVF files:

1. Navigate to the Fortinet Customer Service and Support website (https://support.fortinet.com/).
2. Select *Download* > *Firmware Images*.
3. In the Firmware Images page, select *FortiPortal*.

4. To use OpenStack KVM, download the latest QCOW2 files (one portal file and one collector file):

   `fpcvm64image-kvm-portal.qcow2.zip`

   `fpcvm64image-kvm-collector.qcow2.zip`

5. To use VMWare, download the latest OVF files (one portal file and one collector file):

   `fpcvm64imagePortal.out.ovf.zip`

   `fpcvm64imageCollector.out.ovf.zip`

If you are using VMWare, you can download one virtual application (vApp) file (instead of the above `.ovf` files) that contains the portal and collector VM information. The vApp file name is:

`fpcvm64imagevApp.out.ovf.zip`

When you install this `.ovf` file, the vSphere client will create the portal and collector VMs as a single cluster as well as an example MySQL VM.

Detailed installation instructions are included in the *FortiPortal Administration Guide*:

http://docs.fortinet.com/fpc/admin-guides

Special notices

Special characters

In earlier releases, you could include some special characters in controller names. For example, the following name would be valid:

```
Name'1/3
```

However, in release 2.4.0 and later, you cannot use special characters. Before upgrading to release 2.4.0, you must remove these special characters from existing names.

Collector high-availability

When using collectors in an HA configuration, you must reboot the slave collector(s) and collector database(s) before adding them to FortiPortal.

Reconfiguring mySQL password on FortiPortal

If you change the password for the FortiPortal user in the MySQL portal database, you need to update the configuration in the portal and collector(s):

```
config system sql
   set status remote
   set database-type mysql
   set password <mysql_password>
end
```

Initial log-aggregation delay

After FortiPortal starts to receive logs, there may be a delay of up to 15 minutes before the aggregated data appears on the dashboard.

SSID naming

The SSID name and interface name (which is configured on the FortiGate or FortiWireless Controller) needs to be the same for the FortiPortal to receive the data for this controller.

Supported FortiManager API endpoints

The following FortiManager API configuration endpoints are supported by FortiPortal.

Policy & Object endpoints

dynamic/interface

spamfilter/profile

webfilter/profile

dlp/sensor

antivirus/profile

ips/sensor

webfilter/ftgd-local-cat

webfilter/ftgd-local-rating

application/list

firewall/address

firewall/addrgrp

firewall/schedule/onetime

firewall/schedule/recurring

firewall/service/custom

firewall/service/group

firewall/vip

firewall/vipgrp

firewall/ippool

user/local

user/group

firewall/policy

reinstall/package

revision

Device Manager endpoints

vpn/ipsec/phase1-interface

vpn/ipsec/phase2-interface

router/static

Known issues

This section lists the known issues of this release. For inquiries about a particular issue, please contact Fortinet Customer Service & Support:

https://support.fortinet.com/

Table 1: Known issues

Bug ID	Description
588359	Selecting some permissions from the Available Permissions box in the Add Role form (*Admin* > *Roles* > *Add*) and moving them to the Selected Permissions box results in non-selected permissions being moved when you are using certain browsers such as Firefox 69.0.2 and Microsoft Edge 44.18362.387.0. **Workaround:** Use the Chrome, Chromium-based Edge, or Chromium-based Brave browser.
458423	When policies and objects have been imported from the FortiManager unit, the status is displayed as “Policy Package Uninstalled” in the *Policy & Objects* > *Policy* navigation pane. **Workaround:** Re-install the policy package to make the status show as “installed.”
424414	The Wildcard FQDN option for address objects need to be disabled for ADOM versions 5.4.X and earlier.
408255	With SSO enabled after upgrading from version 3.2.0 to 3.2.1, the default login page loads rather than the SSO login page.

Resolved issues

The following issues have been fixed in version 5.3.0. For inquiries about a particular issue, please contact Fortinet Customer Service & Support:

https://support.fortinet.com/

Table 2: Resolved issues

Bug ID	Description
468432	If a new customer does not have CustomerDashboard-Read-Write permission, the customer users cannot log in.
538660	The *Managed AP* > *Managed AP* tree on the WiFi tab displays a “Request failed with status code 500” error.
541752	Editing or creating a firewall policy in Internet Explorer 11 causes FortiPortal to stop responding.
549405	FortiPortal does not show any Central NAT policies after Central NAT has been configured on a FortiManager.
551229	When a new antivirus or web filter security profile is created, the customer admin cannot change the inspection mode.
555939	The default frequency in the dashboard and View tab need to match the defaults in FortiAnalyzer; the frequency selection options also need to match the options in FortiAnalyzer.
566993	When the language selected for the end user is French, the dashboard page does not display correctly.
572573	A customer user should be able to add FortiAnalyzer to FortiPortal without any problems, and the user should be able to see all report templates associated with FortiAnalyzer.
572712	When there are a lot of report templates in FortiAnalyzer, the report template page in *Devices* > *FortiAnalzyer*, as well as the customer report assignment page stop responding.
576243	Creating a rating override creates an audit log entry, but the FortiPortal API request does not retrieve the audit log entry.

Common vulnerabilities and exposures

FortiPortal 5.3.0 is no longer vulnerable to the following CVEs:

- CVE-2019-11477
- CVE-2019-11478
- CVE-2019-11479

Visit https://fortiguard.com/psirt for more information.

Upgrade information

This section provides instructions to upgrade FortiPortal from an earlier version to a more recent version.

NOTE: For FortiPortal 5.0 and later, you must download a new license file from https://support.fortinet.com/.

To upgrade from version 4.2.0 or later, you can upgrade directly to version 5.0.0.

To upgrade from version 3.2.2 or earlier, you must:

1. Perform a sequential set of upgrades to version 4.0.0.
2. Upgrade from version 4.0.0 to version 4.1.2.

If you are upgrading from a version prior to version 4.0.0, refer to Table 3 on page 17 to determine your upgrade path. Find your existing version in the *Existing Version* column of the table and determine the more recent version(s) to which you can upgrade in the *Compatible Upgrade Version* column. When you upgrade to a more recent version, repeat this process until you're running the most recent version.

Table 3: Upgrade path

Existing Version	Compatible Upgrade Version
2.1.0	2.1.1
2.1.1	2.2.0
2.2.0	2.2.1, 2.2.2, 2.3.0
2.2.1	2.2.2, 2.3.0
2.2.2	2.3.0
2.3.0	2.3.1
2.3.1	2.4.0, 2.4.1
2.4.0	2.4.1, 2.5.0, 3.0.0
2.4.1	2.5.0, 2.5.1, 3.0.0, 3.1.0
2.5.0	2.5.1, 3.0.0, 3.1.0
2.5.1	3.0.0, 3.1.0, 3.1.1, 3.1.2
3.0.0	3.1.0, 3.1.1, 3.1.2
3.1.0	3.1.1, 3.1.2, 3.2.0
3.1.1	3.1.2, 3.2.0

Existing Version	Compatible Upgrade Version
3.1.2	3.2.0, 3.2.1, 3.2.2
3.2.0	3.2.1, 3.2.2, 4.0.0
3.2.1	3.2.2, 4.0.0, 4.0.1
3.2.2	4.0.0, 4.0.1, 4.0.2, 4.0.3
4.0.0	4.1.2
4.0.1	4.1.2
4.0.2	4.1.2
4.0.3	4.1.2
4.0.4	4.1.2
4.1.0	4.2.0, 4.2.1, 4.2.2, 4.2.3, 4.2.4
4.1.1	4.2.0, 4.2.1, 4.2.2, 4.2.3, 4.2.4
4.1.2	4.2.0, 4.2.1, 4.2.2, 4.2.3, 4.2.4
4.2.0	5.0.3
4.2.1	5.0.3
4.2.2	5.0.3
4.2.3	5.0.3
4.2.4	5.0.0, 5.0.1, 5.0.2, 5.0.3
5.0.0	5.2.0
5.0.1	5.2.0
5.0.2	5.2.0
5.0.3	5.2.0
5.1.0	5.2.0, 5.2.1, 5.2.2, 5.2.3, 5.3.0
5.1.1	5.2.0, 5.2.1, 5.2.2, 5.2.3, 5.3.0
5.1.2	5.2.0, 5.2.1, 5.2.2, 5.2.3, 5.3.0

Existing Version	Compatible Upgrade Version
5.2.0	**5.2.1, 5.2.2, 5.2.3, 5.3.0**
5.2.1	**5.2.2, 5.2.3, 5.3.0**
5.2.2	**5.2.3, 5.3.0**
5.2.3	**5.3.0**

Upgrade procedures

Complete the following tasks to perform an upgrade:

1. From the Fortinet Customer Service & Support website (https://support.fortinet.com/), download the portal and/or collector build files for VMware (the `.out` files, not the `.ovf.zip` files) for the version to which you want to upgrade.
2. Perform a backup of the portal and collector MySQL database(s). For details, see "Perform a backup" on page 19.
3. To prevent the collectors from processing logs during the upgrade, shut down the collectors from the VM console.
4. *Restart the portal.* From the VM console, log in as admin and type `execute reboot`.
5. Upgrade the portal. For details, see "Upgrade the portal" on page 20.
6. Turn on the collector(s). For example, from the vSphere client, right-click the collector(s) and go to *Power > Power On*.
7. Upgrade the collector(s). For details, see "Upgrade the collector " on page 20

Do *not* turn off or restart the portal or collector(s) while upgrading. Doing so can cause a loss of data and otherwise harm the system.

Perform a backup

NOTE: You can use https://mysqlbackupftp.com to back up the portal and collector database.

1. You can export (or create a snapshot of) a VM for a backup. For example, for VMware, from the vSphere client, shut down the database VMs from the VM console. If you are using the sample MySQL database, log in as user `fpc`, get root privileges, type `sudo su`, and type `shutdown now`.
2. For VMware users, go to *File > Export > Export OVF Template* to export the VM.
3. For *Name*, set a name for the backup.
4. For *Directory*, select a directory from which you can restore the backup to vSphere.
5. Optionally, enter a *Description* for the backup.

6. Select *OK*.
7. After the backup is complete, right-click the virtual machine you backed up and go to *Power* > *Power On*.

Upgrade the portal

1. Log in to the portal using a service provider (administrator) account.
2. Select the *Admin* tab.
3. Select *FPC Admin* to open the administrator portal. The administrator portal opens in a new browser tab.
4. Log in to the administrator portal. The default user name is `admin`, and there is no default password.
5. Select the *System Settings* tab.
6. In the *System Information* widget, select the *Update* button beside the *Firmware Version*.
7. In the pop-up dialog, select *Choose File* and select the portal `.out` file that you downloaded in Step 1 in "Upgrade procedures" on page 19.
8. Select *OK*. The portal will upgrade. After the firmware is upgraded, the system will restart automatically.

Check that the version number in the *Admin* > *System Info* > *Version Information* > *Version* field in the FortiPortal administrative web interface matches the version number in the administrator portal (*System Settings* > *Dashboard* > *Firmware Version*). If these two numbers do not match, the portal has not finished upgrading. You must wait for the portal to finish upgrading before upgrading the collector.

NOTE: If you have a RADIUS server configured in an existing version, you must re-enter the RADIUS attributes after the portal upgrade is complete. For details, see the *FortiPortal Administration and User Guide*.

Upgrade the collector

For a collector HA cluster, first upgrade the master and then the slave(s). Repeat these steps for each collector:

1. Restart each collector, one at a time.
2. Log in to the portal using a service provider (administrator) account.
3. Select the *Devices* tab.
4. Select the *FPC Collectors* tab.
5. Click the IP address of the collector to open that collector's administrator portal. The administrator portal opens in a new browser tab.
6. Log in to the administrator portal. The default user name is `admin`, and there is no default password.
7. Go to *System Settings*.
8. In the *System Information* widget, select the *Update* button beside the *Firmware Version*.
9. In the pop-up dialog, select *Choose File* and select the collector `.out` file that you downloaded in Step 1 in "Upgrade procedures" on page 19.
10. Select *OK*. The collector will upgrade. After the firmware is upgraded, the system will restart automatically.

Upgrading to FortiPortal 5.3.0 if you are using a custom CSS file

NOTE: If you are using a CSS file for a custom theme, back up the CSS file before upgrading to FortiPortal 5.3.0.

This section focuses on significant changes in FortiPortal 5.3.0 that affect using a custom CSS file as the color scheme when upgrading to version 5.3.0. The following changes were made to the FortiPortal CSS:

- FortiPortal 5.3.0 uses Bootstrap 4 style naming, grid system, table, button, and other styles.
- FortiPortal 5.3.0 uses Font Awesome as the font for the entire web interface. **NOTE:** The Fontello font family is not supported.
- The button style has been changed and renamed. The previous `.flat_button` class will be deprecated in the future. Two new buttons, solid and hollow, have been added. Use `.fpc-btn` with `.btn.btn-primary` and `.btn.btn-outline-secondary`.
- Fortinet recommends using the `.btn.btn-primary.fpc-btn` class for general function buttons (such as *Submit*, *Save*, *OK*, *Yes*, and *Add*) and using the `.btn.btn-outline-secondary.fpc-btn` class for negative buttons (such as *Cancel* and *No*).
- The following CSS classes have been removed and will no longer be used:
  - .device_box_progress
  - .login-footer-text
  - .login-info-header
  - .login-header
  - .header-user-info
  - .ui-widget textarea
  - .ui-widget button
  - .menu_button_on_c
  - .menu_button_off_c
  - .sbHolder
  - .sbOptions
  - .settingsHeaderDiv
  - .myNavigation
- The header height has been reduced. The header logo ratio is the same, which prevents the image from overlapping the menu.

The following table describes major changes in CSS class names in the `place_holder_custom.css` file:

CSS class (before FortiPortal 5.3.0)	CSS class in FortiPortal 5.3.0
.login-header	.pub-temp-body .headerTopClass
.footerText	.footerText .footerText a
.login-footer-text	.pub-temp-body .footerText, .pub-temp-body .footerText a
#fpcfooterDiv a	.footerText a

CSS class (before FortiPortal 5.3.0)	CSS class in FortiPortal 5.3.0
.flat_button	.btn-primary.fpc-btn
.widget-header	.ui-dialog .ui-widget-header .modal-header
.ui-button	.btn-primary.fpc-btn
.ui-widget-content	.ui-state-default .ui-widget-content .ui-state-default:not('.fpc-btn')

FORTINET

High Performance Network Security