



FortiPortal Release Notes

Version 5.3.2

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



March 2, 2020

FortiPortal 5.3.2 Release Notes

2nd Edition

TABLE OF CONTENTS

Change log	4
Introduction	5
What's new.....	5
FortiManager, FortiOS, FortiAnalyzer, and FortiSandbox supported versions.....	5
Additional compatibility resources.....	9
Hypervisor support.....	9
Database support.....	9
Web browser support.....	9
FortiPortal 5.3.2 software.....	9
Special notices	11
Special characters.....	11
Collector high-availability.....	11
Reconfiguring MySQL password on FortiPortal.....	11
Initial log-aggregation delay.....	11
SSID naming.....	11
Supported FortiManager API endpoints.....	12
Policy & Object endpoints.....	12
Device Manager endpoints.....	12
Known issues	13
Resolved issues	14
Upgrade information	16
Perform a backup.....	18
Upgrade the portal.....	18
Upgrade the collector.....	19
Upgrading to FortiPortal 5.3.0 and later if you are using a custom CSS file.....	19

Change log

Date	Description
January 8, 2020	Initial release for FortiPortal 5.3.2
March 2, 2020	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 5.3.2, build 0288. It includes the following sections:

- ["Special notices"](#) on page 11
- ["Known issues"](#) on page 13
- ["Resolved issues"](#) on page 14
- ["Upgrade information"](#) on page 16

What's new

This release contains the following new features and enhancements:

- You can now use the FortiPortal REST API to assign one or more FortiAnalyzer reports to a specific customer.
- A Refresh button is now available on the Policy & Objects > Policy page for customer users with read-only permissions.
- You can now specify names for policies.
- You can now specify which customers will receive which system notifications.

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 5.3.2 supports the following versions of Fortinet products:

Fortinet Product	Supported Versions	Recommended Version
FortiAnalyzer (for reports and analytics)	<ul style="list-style-type: none"> • 6.0.0 • 6.0.1 • 6.0.2 • 6.0.3 • 6.0.4 • 6.0.5 • 6.0.6 • 6.0.7 • 6.0.8 • 6.2.1 • 6.2.2 	6.2.2
FortiAnalyzer (for reports)	<ul style="list-style-type: none"> • 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 • 5.6.11 • 6.0.0 • 6.0.1 • 6.0.2 • 6.0.3 • 6.0.4 • 6.0.5 • 6.0.6 • 6.0.7 • 6.0.8 • 6.2.1 • 6.2.2 	6.2.2

Fortinet Product	Supported Versions	Recommended Version
FortiManager	<ul style="list-style-type: none">• 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• 5.6.11• 6.0.0• 6.0.1• 6.0.2• 6.0.3• 6.0.4• 6.0.5• 6.0.6• 6.0.7• 6.0.8• 6.2.1• 6.2.2	6.2.2

Fortinet Product	Supported Versions	Recommended Version
FortiOS	<ul style="list-style-type: none"> • 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 • 5.6.11 • 6.0.0 • 6.0.1 • 6.0.2 • 6.0.3 • 6.0.4 • 6.0.5 • 6.0.6 • 6.0.7 • 6.0.8 • 6.2.1 • 6.2.2 	6.2.2
FortiSandbox	<ul style="list-style-type: none"> • 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 5.3.2 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
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.
424414	The Wildcard FQDN option for address objects need to be disabled for ADOM versions 5.4.X and earlier.
458423	When policies and objects have been imported from the FortiManager unit, the status is displayed as "Policy Package Uninstalled" in the <i>Policy & Objects > Policy</i> navigation pane. Workaround: Re-install the policy package to make the status show as "installed."
530216	Nested virtual IP groups are not displayed when editing the firewall policy.
592068	The FortiPortal collector database grows bigger than the configured size and ignores the global retention policy.
595541	The table element <code>role="presentation"</code> should be added to all tables.
598674	Upgrading to FortiPortal 5.2.4 failed with a new FortiPortal environment.

Resolved issues

The following issues have been fixed in version 5.3.2. For inquiries about a particular issue, please contact Fortinet Customer Service & Support:

<https://support.fortinet.com/>

Table 2: Resolved issues

Bug ID	Description
472796	A "Possible database integrity problem detected during scheduled verification. Please check manually" error is displayed in the Alert Message Console, but the database is hosted externally.
565264	Customer policies are not listed in FortiPortal, even when daily polling is configured.
567833	FortiPortal will not install a security profile with the proxy mode different from the policy package.
570866	The Top Traffic by Customer and Top Customer for Sandbox widgets should not be displayed in the dashboard in FortiAnalyzer mode.
576219	The password and settings for a restricted local user account cannot be changed.
576297	Some logs are not displayed in <i>FortiView > Session</i> .
581186	After selecting <i>Refresh</i> , no policies are listed on the <i>Policy & Objects > Policy</i> page.
581204, 583125	A firewall is not displayed on the <i>Policy & Objects > Objects</i> page.
582276	The review report is missing columns.
583917	When logging in as a remote service provider user with RADIUS, the user cannot edit the firewall policy.
586218	When editing a firewall policy, you cannot see or select ISDB objects.
587135	The response of the <code>/customers/{cid}/availablefzreports</code> API endpoint needs to be improved.
588359	Selecting some permissions from the Available Permissions box in the Add Role form (<i>Admin > Roles > Add</i>) 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.
588420	When the ADOM version is 6.2 or higher, the Cost field does not need to be displayed in the Create New Interface Member or Edit Interface Member forms.
588504	The customer FortiPortal in Collector mode points to the slave FortiGate in HA mode.

Bug ID	Description
589124	The favicon and css requests need to be cached.
590642	Selecting the Refresh button in the Policy & Objects > Policy page causes an “Error: 500” to be displayed.
592002	Creating a new application override for an existing application sensor causes the session to stop responding.
592230	When FortiPortal reports are emailed, sometimes there are random numbers added to the report name, or the report cannot be opened.
592402	After upgrading to FortiPortal 5.3.0, a test account cannot be deleted.
592617	A “[500]JSONObject[“webfilter ftgd-local-cat”] not found” error is displayed when trying to create or edit a web filter profile.
592720	The SD-WAN > Monitoring page shows all health checks for a device as failing when only one health check has failed.
593673	When an SD-WAN template has multiple performance SLAs defined but only some of they are being used in the SD-WAN rule, the SD-WAN > Monitoring page displays the unused SLAs as failing in red.
593807	A FortiPortal collector does not accept logs from an FG-100F unit because of an internal error.
593904	The Installation tab on the Policy & Objects > Policy page should be a button instead at the top level of the page.
594156	After changing from Collector mode to FortiAnalyzer mode, FortiPortal does not show data from FortiAnalyzer.
594560	When editing an existing IPsec Phase 1 or IPsec Phase 2 configuration, all of the Diffie-Hellman Groups are selected instead of the previously partially selected groups.
594947	After switching from Collector mode to FortiAnalyzer mode, most of the generated FortiPortal PDF reports are no longer listed in the FortiPortal GUI.
595661	The customer end user does not see any policies or objects.
596399	The Build Number field on the Admin > System Info page should indicate whether the build is interim or GA.
596839	No policies are listed under the Policy tab and Objects tab, and the HA cluster is labeled as standalone.

Upgrade information

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

NOTE: Before upgrading FortiPortal, back up the portal database. If the upgrade fails, you can restore the portal database from the backup.

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 16 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

Existing Version	Compatible Upgrade Version
3.1.1	3.1.2, 3.2.0
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, 5.2.4, 5.3.0, 5.3.1, 5.3.2
5.1.1	5.2.0, 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.3.0, 5.3.1, 5.3.2

Existing Version	Compatible Upgrade Version
5.1.2	5.2.0, 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.3.0, 5.3.1, 5.3.2
5.2.0	5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.3.0, 5.3.1, 5.3.2
5.2.1	5.2.2, 5.2.3, 5.2.4, 5.3.0, 5.3.1, 5.3.2
5.2.2	5.2.3, 5.2.4, 5.3.0, 5.3.1, 5.3.2
5.2.3	5.2.4, 5.3.0, 5.3.1, 5.3.2
5.3.0	5.3.1, 5.3.2
5.3.1	5.3.2

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 information" on page 16.
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 information](#)" on page 16.
10. Select *OK*. The collector will upgrade. After the firmware is upgraded, the system will restart automatically.

Upgrading to FortiPortal 5.3.0 and later 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 and later. 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 and later
.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
.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



Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features, or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. 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.