



FortiPortal Release Notes

Version 5.2.0

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



March 28, 2019

FortiPortal 5.2.0 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..... | 8 |
| Hypervisor support..... | 8 |
| Database support..... | 8 |
| Web browser support..... | 9 |
| FortiPortal 5.2.0 software..... | 9 |
| Special notices | 10 |
| Special characters..... | 10 |
| Collector high-availability..... | 10 |
| Reconfiguring mySQL password on FortiPortal..... | 10 |
| Initial log-aggregation delay..... | 10 |
| SSID naming..... | 10 |
| Supported FortiManager API endpoints..... | 11 |
| Policy & Object endpoints..... | 11 |
| Device Manager endpoints..... | 11 |
| Known issues | 12 |
| Resolved issues | 13 |
| Common vulnerabilities and exposures..... | 14 |
| Upgrade information | 15 |
| Upgrade procedures..... | 17 |

Change log

| Date | Description |
|----------------|---|
| March 1, 2019 | Initial release for FortiPortal 5.2.0 |
| March 28, 2019 | Updated the FortiSandbox supported version and recommended version. |

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 5.2.0, build 0223. It includes the following sections:

- ["Special notices"](#) on page 10
- ["Known issues"](#) on page 12
- ["Resolved issues"](#) on page 13
- ["Upgrade information"](#) on page 15

What's new

This release contains the following new features and enhancements:

- You can incorporate FortiAnalyzer reporting directly into FortiPortal or collect FortiAnalyzer logs from collectors.
- You can now set up local, LDAP, RADIUS, and TACACS+ authentication for FortiPortal users.
- You can now use the FortiPortal API to hide objects and firewall rules for a customer.
- DHCP management
- WiFi management
- FortiSandbox 3000E (FSA3KE) is now supported.
- FortiManager 6.0.3 and 6.0.4 are now supported.
- FortiAnalyzer 6.0.3 and 6.0.4 are now supported.

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 5.2.0 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 | 6.0.4 |
| 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• 6.0.0• 6.0.1• 6.0.2• 6.0.3• 6.0.4 | 6.0.4 |

| 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 • 6.0.0 • 6.0.1 • 6.0.2 • 6.0.3 • 6.0.4 | 6.0.4 |
| FortiOS | <ul style="list-style-type: none"> • 5.6.0 • 5.6.1 • 5.6.2 • 5.6.3 • 5.6.4 • 5.6.5 • 5.6.6 • 5.6.7 • 5.6.8 • 6.0.0 • 6.0.1 • 6.0.2 • 6.0.3 • 6.0.4 | 6.0.0 |
| 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 5.2.0 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 |
|--------|--|
| 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. |

Resolved issues

The following issues have been fixed in version 5.2.0. For inquiries about a particular issue, please contact Fortinet Customer Service & Support:

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

Table 2: Resolved issues

| Bug ID | Description |
|-------------------|---|
| 415382 | A customer user with special characters in the first or last name cannot be edited. |
| 462017 | FortiPortal needs to use Apache Tomcat Server 9.0.12. |
| 487668 | The default FortiPortal SSL certificate needs to be updated. |
| 495623, 513743 | The 5.x OVF images for the portal server and collector server do not deploy in VMware ESXi 6.5.0. |
| 499035 | The status of application sensor categories configured on a FortiGate unit is not synchronized on a FortiPortal unit. |
| 501185 | The inspection mode of an object should not be changed from the value defined in the policy package. |
| 519922, 531071 | The pagination buttons overlap, making it difficult to select the correct button. |
| 520071 | When using a custom theme, the progress bar color needs to be changed. When there are more than 10 customers, the pagination needs to be fixed. |
| 522007 | When creating a new DHCP server, errors need to be displayed if mandatory fields are not filled or if IP or MAC addresses are incorrect. |
| 522255 | After FortiPortal unit is upgraded, the customer cannot view FortiAnalyzer reports in the <i>Customer > Reports</i> page. |
| 522566 | The <code>ftnt_fpc.log</code> is not listed in the drop-down list on the <i>Admin > System Log</i> page. Downloading a listed log file results in an error. |
| 523210 | After creating a web filter profile with a category that requires authentication in FortiManager, the category does not require authentication in FortiPortal. |
| 524985 | When single sign-on is enabled, some settings are not saved. |
| 526271 | Error messages do not mention that the feature is not supported in SD-WAN. |

| Bug ID | Description |
|--------|--|
| 526992 | The expand and collapse icons on the Wireless Networks page do not display correctly. |
| 528690 | When creating or editing a customer in the API, the value for the analyticsEnabled parameter is ignored. |
| 529265 | After an error in the installation log scheduler, the lock on the ADOM is not released. |
| 529316 | When devices are removed from FortiManager, the corresponding policy packages need to be automatically removed from FortiPortal. |
| 531183 | Creating a web filter profile object in FortiPortal with any FortiGuard category set to Authenticate causes an error. |
| 532544 | Error messages are need for incorrect input for fields in the <i>Admin > Settings</i> page. |
| 533346 | FortiPortal needs to allow longer names of services and applications for IPS rules. |
| 533349 | If an exception occurs in FortiPortal when polling for objects, all sessions in FortiManager should be logged out. |
| 537203 | The review tab is not displayed when there is a JavaScript error. |

Common vulnerabilities and exposures

FortiPortal 5.2.0 is no longer vulnerable to the following CVEs:

- CVE-2019-0190
- CVE-2018-17199
- CVE-2018-17189

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 15 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 |
| 5.1.1 | 5.2.0 |
| 5.1.2 | 5.2.0 |

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 17.
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 17.
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 18



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 17.
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 17.
10. Select *OK*. The collector will upgrade. After the firmware is upgraded, the system will restart automatically.



FORTINET

High Performance Network Security



Copyright© 2019 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.