

FortiPortal Release Notes

version 3.1.0

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>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

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



Friday, October 07, 2016

FortiPortal version 3.1.0 Release Notes

Change Log

| Date | Change Description |
|------------|---|
| 2016-09-30 | FortiPortal 3.1.0 release. |
| 2016-10-07 | Added release 3.1.0 to product support matrix |

TABLE OF CONTENTS

| | |
|--|-----------|
| Change Log | 3 |
| Introduction | 5 |
| What's New in FortiPortal v3.1.0..... | 5 |
| Supported models..... | 5 |
| Special Notices | 7 |
| Special Characters..... | 7 |
| Collector High-Availability..... | 7 |
| Reconfiguring MySQL Password on FortiPortal..... | 7 |
| Initial Log-Aggregation Delay..... | 7 |
| SSID Naming..... | 7 |
| Upgrade Information | 8 |
| Upgrade Procedure..... | 8 |
| Product Integration and Support | 10 |
| Firmware Compatibility Matrix..... | 10 |
| Notes..... | 10 |
| Additional Compatibility Resources..... | 11 |
| Hypervisor Support..... | 11 |
| Web Browser Support..... | 11 |
| Resolved Issues | 12 |

Introduction

This document provides information about the FortiPortal version 3.1.0 release, and includes the following sections:

- [Special Notices](#)
- [Upgrade Information](#)
- [Product Integration and Support](#)
- [Resolved Issues](#)
- [Known Issues](#)

What's New in FortiPortal v3.1.0

This release contains the following additional features:

- REST API.

The Fortinet document library at <http://docs.fortinet.com/fpc> provides additional information about the FortiPortal product.

Supported models

The FortiPortal product is delivered as virtual machine OVF files for the VMware hypervisor.

You can download the OVF files from the Fortinet customer support site:

1. Navigate to the Fortinet customer support site(<https://support.fortinet.com>)
2. Select **Download > Firmware Images**
3. In the Firmware Images page, select **FortiPortal**
4. For easy MySQL deployment, download the latest OVF file for MySQL :
 - mysql.ovf.zip
5. To use OpenStack KVM, download the latest QCOW2 files (one portal file, one collector file):
 - fpcvm64image-kvm-portal.qcow2.zip
 - fpcvm64image-kvm-collector.qcow2.zip
6. To use VMWare, download the latest OVF files (one portal file, 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. When you install this OVF file, vSphere will create the Portal and Collector VMs as a single cluster.

The vApp file name is as follows:

- fpcvm64imagevApp.out.ovf.zip

An alternative option is to download the vApp file that will create portal, collector and MySQL database VMs:

- `fpcvm64imagevApp-mysql.out.ovf.zip`

Installation instructions are included in the [FortiPortal Admin Guide](#).

Special Notices

Special Characters

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

```
Name '1/3
```

However, In release 2.4.0 and later, you must not use these characters. Prior to upgrading to release 2.4.0, you must remove these special characters from existing names.

In release 2.4.0 or later, if an entry has a name containing a special character, you will not be able to edit the entry (but you can delete it).

Collector High-Availability

When using collectors in HA configuration, note the following points:

- You must reboot the slave collector and collector database before adding either of them to the 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 FortiPortal portal and collector:

```
config system sql
  set status remote
  set database-type mysql
  set password <fpc portal db mySQL password>
end
```

Initial Log-Aggregation Delay

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

SSID Naming

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.

Upgrade Information

2.4.1, 2.5, 2.5.1 or 3.0 releases

FortiPortal version 3.1.0 supports software upgrade from release 2.4.1, 2.5.0, 2.5.1 and 3.0.0.

To upgrade from an earlier release, perform a sequential set of upgrades up to release 2.4.0, starting at your current release:

- a. 2.1.1 → 2.2.0
- b. 2.2.0 → 2.2.1
- c. 2.2.1 → 2.2.2
- d. 2.2.2 → 2.3.0
- e. 2.3.0 → 2.4.0
- f. 2.4.0 → 2.4.1

For example, to upgrade from Version 2.1.1, start at step (a). To upgrade from version 2.2.2, start at step (d).

Upgrade Procedure

Perform the following actions prior to the upgrade:

- Perform a backup of the MySQL database VMs (Portal and Collector DB)
- Ensure that the Collector VM's are powered off
- Ensure that the Portal and Collector database VM's are running
- Ensure that the Portal VM is running
- Download the latest portal and collector build files (the .out files, not the .ovf.zip files)

Upgrade the Portal

1. Log in to the FortiPortal Admin Portal
2. From the **Admin** tab, click the **FPC Admin** button to open the portal admin web UI. The portal admin web UI opens in a new browser tab, and presents a login page.
3. Log in to the portal admin web UI
4. On the **System settings** page, in the **System Information** panel, click the **Update** button beside the **Firmware Version**.
5. In the pop-up dialog, click Choose File and select the portal .out file that you downloaded. The portal will upgrade and then perform a restart.

Upgrade the Collector

Note: for a Collector HA cluster, upgrade the master first, followed by the slave collector.

Repeat this set of steps for each collector:

1. Log in to the FortiPortal Admin Portal
2. From the **Admin** tab, click the **FPC Collectors** tab.

3. Click the IP address of the collector to open the collector Admin web UI.
The collector admin web UI opens in a new browser tab, and presents a login page.
4. Log in to the portal admin web UI.
5. On the **System settings** page, in the **System Information** panel, click the **Update** button beside the **Firmware Version**.
6. In the pop-up dialog, click Choose File and select the collector.out file that you downloaded.
The collector will upgrade and then perform a restart.

Product Integration and Support

FortiPortal version 3.1.0 supports the following versions of Fortinet products:

- FortiManager, versions 5.0.8 to 5.2.4, and version 5.4.0
- FortiOS 5.0, 5.2.1, 5.2.3 or 5.2.4, and version 5.4.0
- FortiAnalyzer 5.0 or later

Firmware Compatibility Matrix

The following table displays the Fortinet product firmware versions that are compatible with each version of FortiPortal.

| FortiOS | FortiAP | Compatible firmware versions | | |
|------------------|---------------------------|-----------------------------------|----------------|--|
| | | FortiManager | FortiAnalyzer | FortiPortal |
| 5.0.4 to 5.0.10 | 5.0 | 5.0.8 to 5.2.4 | 5.0.8 to 5.2.7 | 2.2.x, 2.3.x |
| 5.0.11 to 5.0.13 | 5.0 | 5.0.11 5.2.2 to 5.2.4 | 5.0.8 to 5.2.7 | 2.2.x, 2.3.x |
| 5.2.1 | 5.0.8 5.2.1 | 5.0.8 to 5.2.4 | 5.0.8 to 5.2.7 | 2.2.x, 2.3.x, 2.4.x, 2.5.x, 3.0.0, 3.1.0 |
| 5.2.3 | 5.0.9 5.2.3 and later | 5.0.10 to 5.2.4 (except 5.2.0) | 5.0.8 to 5.2.7 | 2.2.x, 2.3.x, 2.4.x, 2.5.x, 3.0.0, 3.1.0 |
| 5.2.4 | 5.0.9 5.2.4 and later | 5.2.3 to 5.2.7 | 5.0.8 to 5.2.7 | 2.2.x, 2.3.x, 2.4.x, 2.5.x, 3.0.0, 3.1.0 |
| 5.4.0 | 5.0.10 5.2.5 and later | 5.4.0 | 5.4.0 | 2.4.x, 2.5.x, 3.0.0, 3.1.0 |

Notes

1. Refer to FortiOS and FortiManager release notes for detailed compatibility information.
2. Use Fortigate 5.2.3 or later to get support for local AP's.
3. FortiManager 5.4.0 does not support the policy move capability.

Additional Compatibility Resources

Refer to the following document for the FortiAnalyzer compatibility with each FortiOS release:

[Fortianalyzer Compatibility Chart](#)

Refer to the following document for the FortiManager compatibility with each FortiOS release:

[FortiManager Compatibility Chart](#)

The FortiManager and FortiAnalyzer release notes for each release provide detailed compatibility information, including the hardware models supported, and any product limitations.

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 may 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
```

Hypervisor Support

The following Hypervisors are supported:

- VMware ESX Server version 5.5 or later
- KVM version 2.6.x

Web Browser Support

The following browser versions are supported:

- Microsoft Internet Explorer version 11
- Mozilla Firefox: up to version 45
- Google Chrome version 52

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

Resolved Issues

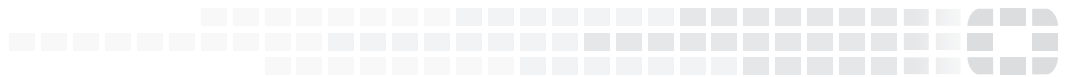
The FortiPortal version 3.1.0 release includes the following resolved issues:

Resolved issues

| Defect ID | Description |
|-----------|-------------|
|-----------|-------------|



High Performance Network Security



Copyright© 2016 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.