

FortiPortal Release Notes

Version 4.1.1

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



October 20, 2017

FortiPortal 4.1.1 Release Notes

1st Edition

TABLE OF CONTENTS

Change log	4
Introduction	5
What's new.....	5
FortiManager and optional device support	5
Additional compatibility resources.....	6
Hypervisor support.....	6
MySQL support.....	6
Web browser support.....	6
FortiPortal 4.1.1 software.....	6
Special notices	8
Special characters.....	8
Collector high-availability.....	8
Reconfiguring mySQL password on FortiPortal.....	8
Initial log-aggregation delay.....	8
SSID naming.....	8
Known issues	9
Resolved issues	10
Upgrade information	11
Upgrade procedures.....	12

Change log

Date	Description
10/20/2017	Initial release

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 for Managed Security Service Providers (MSSPs) as a virtual machine (VM) software solution that can be deployed on a hosted services infrastructure. This allows MSSPs to build highly customized private cloud services for their customers.

This document provides information about FortiPortal Version 4.1.1, build 0114. It includes the following sections:

- ["Special notices"](#) on page 8
- ["Known issues"](#) on page 9
- ["Resolved issues"](#) on page 10
- ["Upgrade information"](#) on page 11

What's new

FortiPortal Release Notes version 4.1.1, build 0114, is a patch release only. There are no new features and enhancements in this release. For more information, see ["Resolved issues"](#) on page 10 and ["Known issues"](#) on page 9.

FortiManager and optional device support

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

FortiPortal 4.1.1 supports the following versions of Fortinet products:

- FortiManager, Versions 5.0.8 to 5.2.9, 5.4.0 to 5.4.3
- FortiOS Versions 5.0, 5.2.1, 5.2.3, 5.2.4, 5.2.7, 5.2.8, 5.2.9, 5.4.0, 5.4.1, 5.4.2, 5.4.3, 5.4.4, 5.4.5
- FortiAnalyzer 5.0 or later

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

NOTE: Use FortiGate 5.2.3 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 version 5.5 or later
- KVM Version 2.6.x

MySQL 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
```

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 4.1.1 software

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

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. 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. 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.

An alternative option is to download the vApp file that will create the Portal, Collector, and MySQL database VM. The vApp file name is:

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

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. 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 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.

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

Defect ID	Description
0408255	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.
0424414	The Wildcard FQDN option for address objects need to be disabled for ADOM versions 5.4.X and earlier.
0440932	IPS Sensor signatures are not synced with FortiManager.

Resolved issues

The following issues have been fixed in version 4.1.1. For inquiries about a particular issue, please contact Fortinet Customer Service & Support:

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

Table 2: Resolved issues

Defect ID	Description
0453654	Passwords cannot contain special characters, such as the ones listed on http://www.degraeve.com/reference/specialcharacters.php or https://www.quackit.com/html/html_special_characters.cfm . Passwords can contain the following special characters: .-*@

Upgrade information

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

To upgrade from version 4.0.0 or later, you can upgrade directly to version 4.1.0.

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 4.1.0.

If you are upgrading from a version prior to version 4.0.0, refer to [Table 3](#) on page 11 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
3.1.2	3.2.0, 3.2.1, 3.2.2

Existing Version	Compatible Upgrade Version
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	4.1.0
4.0.1	4.1.0
4.0.2	4.1.0
4.0.3	4.1.0
4.0.4	4.1.0

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 (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 12.
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 13.
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 13



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

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. Click **OK**.
7. Once 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. Click the **FPC Admin** button 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, click the **Update** button beside the **Firmware Version**.
7. In the pop-up dialog, click **Choose File** and select the Portal `.out` file that you downloaded in Step 1 in "Upgrade procedures" on page 12.
8. Click **OK**. The Portal will upgrade. After the firmware is upgraded, the system will restart automatically.

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

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

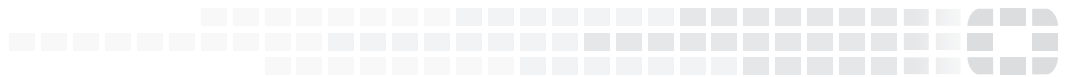
Upgrade the Collector

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 **Admin** 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, click the **Update** button beside the **Firmware Version**.
9. In the pop-up dialog, click **Choose File** and select the Collector `.out` file that you downloaded in Step 1 in "Upgrade procedures" on page 12.
10. Click **OK**. The Collector will upgrade. After the firmware is upgraded, the system will restart automatically.

FORTINET®

High Performance Network Security



Copyright© 2017 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.