FortiPortal Release Notes

Version 4.2.0

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

January 2, 2018

FortiPortal 4.2.0 Release Notes

2nd Edition

TABLE OF CONTENTS

Change log

Date	Description
12/22/2017	Initial release
1/2/2018	Minor update

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 4.2.0, build 0178. It includes the following sections:

What's new

This release contains the following new features and enhancements.

- Support of FortiManager 5.6.0 and 5.4.4
- Proxy and flow-based inspection mode supported for data leak prevention sensors
- Support for the following:
  - FortiGate-100E
  - FortiGate-100EF
  - FortiGate-101E
  - FortiGate-140E
  - FortiGate-140E-POE
  - FortiGate-1500DT
  - FortiGate-2000E
  - FortiGate-200E
  - FortiGate-201E
  - FortiGate-2500E
  - FortiGate-3000D
  - FortiGate-3000D-DC
  - FortiGate-30E
  - FortiGate-3100D
  - FortiGate-3100D-DC
  - FortiGate-3800D
  - FortiGate-3800D-DC
  - FortiGate-3810D
  - FortiGate-3810D-DC
  - FortiGate-3815D
  - FortiGate-3815D-DC

- FortiGate-400D
- FortiGate-5001E
- FortiGate-50E
- FortiGate-51E
- FortiGate-52E
- FortiGate-600D
- FortiGate-60E
- FortiGate-61E
- FortiGate-700D
- FortiGate-7040E
- FortiGate-70D-POE
- FortiGate-800D
- FortiGate-80E
- FortiGate-80E-POE
- FortiGate-81E
- FortiGate-81E-POE
- FortiGate-900D
- FortiGate-90E
- FortiGate-91E
- FortiWiFi-30E
- FortiWiFi-30E-3G4G-INTL
- FortiWiFi-30E-3G4G-NAM
- FortiWiFi-50E-2R
- FortiWiFi-51E
- FortiWiFi-60E
- FortiWiFi-61E

FortiManager, FortiOS, and FortiAnalyzer 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 4.2.0 supports the following versions of Fortinet products:

- FortiManager, versions 5.2.x, 5.4.x, 5.6.0
- FortiOS, versions 5.2.x, 5.4.x, 5.6.0
- FortiAnalyzer, version 5.2.6 and 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

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:

- 5.5.57-MariaDB-1ubuntu0.14.04.1 (Ubuntu)
- 10.0.31-MariaDB-1~precise mariadb.org binary distribution

NOTE: The two 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 4.2.0 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.

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.
440932	IPS sensor signatures are not synced with FortiManager.
447503	Database logic does not handle VDOMs being moved to a new FortiGate.

Resolved issues

The following issues have been fixed in version 4.2.0. For inquiries about a particular issue, please contact Fortinet Customer Service & Support:

https://support.fortinet.com/

Table 2: Resolved issues

Bug ID	Description
452349	Editing an application sensor (*Policy & Objects* > *Objects* > *Security Profiles* > *Application Sensor*) does not work with FortiManager 5.6.
424191	When a new rating override is added to a new local FortiGuard category in a new web filter profile, the URL is wrong.
457764	When creating a web filter profile (*Policy & Objects* > *Objects* > *Security Profiles* > *Web Filter Profile*), you need to use the format in the most recent version of FortiManager.
453617	Using the REST API to add a domain to a new customer results in a 404 error message.
453614	You cannot use the GUI to edit a customer who was added using the REST API.
455374	You cannot use special characters in the Username field in *Admin* > *Settings* > *Email settings*.
452360	When creating an antivirus profile (*Policy & Objects* > *Objects* > *Security Profiles* > *Antivirus Profile* > *Create New*), the Detect Viruses buttons (Block or Monitor) are not displayed in the Create New Antivirus Filter Profile dialog box.
458435	After upgrading to FortiPortal 4.1.0, the system becomes unresponsive during IPSec phase 1.
448298	An IPS sensor (*Policy & Objects* > *Objects* > *Security Profiles* > *IPS Sensor*) created on FortiManager from FortiPortal cannot be edited.
458902	Unused ports are open.
448863	The collector does not accept logs that have been forwarded by FortiAnalyzer when there are double quotations marks around the value for the devid field. For example: devid="FGT90D0000000001"
436221	A wireless controller for a device managed by FortiManager is given a default IP address of 0.0.0.0, which cannot be changed.
463389	After upgrading from 4.1.1 to 4.1.2, the customer dashboard was not accessible.
461133	Older versions of TLS and SSL are available.

Bug ID	Description
457573	Apache Tomcat, Apache HTTP Server, OpenSSL, and OpenSSH upgrading needed.
458321	Cross-site scripting and improper access control issues need to be fixed.

Upgrade information

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

To upgrade from version 4.1.0 or later, you can upgrade directly to version 4.2.0.

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 13 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	4.1.2
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
4.1.1	4.2.0
4.1.2	4.2.0

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 15.
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 15.
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 15

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 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 14.
8. Select *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 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 *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, 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 14.
10. Select *OK*. The collector will upgrade. After the firmware is upgraded, the system will restart automatically.

FORTINET

High Performance Network Security