FortiPortal - Release Notes

Version 5.3.4

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

November 2, 2020
FortiPortal 5.3.4 Release Notes
37-534-653671-20201102

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-08-06	Initial release.
2020-08-21	Added bug 606424 to Resolved Issues on page 17.
2020-09-10	Added What's new on page 5.
2020-09-18	Updated Upgrade Information on page 12.
2020-11-02	Added FortiManager-FortiAnalyzer 6.2.6 to FortiManager, FortiOS, FortiAnalyzer, and FortiSandbox supported versions on page 6.

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 enterprises and managed security service providers (MSSP) to build highly customized private cloud services for their customers.

This document provides information about FortiPortal version 5.3.4, build 0313. It includes the following sections:

What's new

FortiPortal version 5.3.4, build 0313, is a patch release only. There are no new features and enhancements in this release. For more information, see Resolved Issues on page 17 and Known Issues on page 19.

Product Integration and Support

FortiPortal 5.3.4 supports some FortiManager, FortiOS, FortiAnalyzer, and FortiSandbox versions.

The section contains the following topics:

FortiManager, FortiOS, FortiAnalyzer, and FortiSandbox supported versions

The FortiPortal self-service interface for MSSP customers uses the FortiManager 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 5.3.4 supports the following product versions:

Product	Supported Versions	Recommended Version
FortiAnalyzer (for reports and analytics)	• 6.2.5 and 6.2.6 • 6.2.1 to 6.2.3 • 6.0.0 to 6.0.9	6.2.6
FortiAnalyzer (for reports)	• 6.2.5 and 6.2.6 • 6.2.1 to 6.2.3 • 6.0.0 to 6.0.9 • 5.6.7 to 5.6.11 • 5.6.0 to 5.6.5	6.2.6
FortiManager	• 6.2.5 and 6.2.6 • 6.2.1 to 6.2.3 • 6.0.0 to 6.0.9 • 5.6.7 to 5.6.11 • 5.6.0 to 5.6.5 • 5.4.0 to 5.4.6 • 5.2.10	6.2.6
FortiOS	FortiOS support is determined by FortiPortal support for FortiManager and FortiAnalyzer.	

Product	Supported Versions	Recommended Version
	FortiPortal supports specific versions of FortiManager and FortiAnalyzer, and FortiManager and FortiAnalyzer support specific versions of FortiOS. For supported FortiOS versions, refer to the release notes for the supported FortiManager and FortiAnalyzer versions on the Fortinet Docs Library.	
FortiSandbox	• 3.0.2	3.0.2

Use FortiGate 4.0.0 or later to get support for local APs.

If you are using FortiManager version 5.2.3 or later, you must ensure that the FortiManager user account (that you created for FortiPortal) 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
```

Also see:

- Additional compatibility resources on page 7
- Hypervisor support on page 7

Additional compatibility resources

Refer to the FortiOS, FortiManager, and FortiAnalyzer release notes on the Fortinet Docs Library for detailed compatibility information.

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

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

The MariaDB server versions do not require additional configuration, except for *Bind-Address* and *Grant Privileges*. See *FortiPortal Administration Guide* > *Upgrading FortiPortal software* on the Fortinet Docs Library.

Web browser support

The following web browsers are supported:

- Microsoft Internet Explorer (IE) Version 11
- Mozilla Firefox (up to) Version 79
- Google Chrome Version 84

Other (versions of the) browsers might also function but are not fully supported in this release.

FortiPortal 5.3.4 software

FortiPortal is delivered as virtual machine OVF/QCOW2 files for the VMware/KVM hypervisors.

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`
   OR
   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* on the Fortinet Docs Library.

Special Notices

This section contains the following:

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 collectors and collector databases 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

Upgrade Information

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

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

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 the following table to determine your upgrade path. Find your existing version in the *Existing Version* column of the table and determine the more recent versions 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.

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
3.2.0	3.2.1, 3.2.2, 4.0.0

Existing Version	Compatible Upgrade Version
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, 5.2.5, 5.3.0, 5.3.1, 5.3.2, 5.3.3, 5.3.4
5.1.1	5.2.0, 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.2.5, 5.3.0, 5.3.1, 5.3.2, 5.3.3, 5.3.4
5.1.2	5.2.0, 5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.2.5, 5.3.0, 5.3.1, 5.3.2, 5.3.3, 5.3.4
5.2.0	5.2.1, 5.2.2, 5.2.3, 5.2.4, 5.2.5, 5.3.0, 5.3.1, 5.3.2, 5.3.3, 5.3.4
5.2.1	5.2.2, 5.2.3, 5.2.4, 5.2.5, 5.3.0, 5.3.1, 5.3.2, 5.3.3, 5.3.4
5.2.2	5.2.3, 5.2.4, 5.2.5, 5.3.0, 5.3.1, 5.3.2, 5.3.3, 5.3.4
5.2.3	5.2.4, 5.2.5, 5.3.0, 5.3.1, 5.3.2, 5.3.3, 5.3.4
5.2.4	5.2.5, 5.3.2, 5.3.3, 5.3.4
5.3.0	5.3.1, 5.3.2, 5.3.3, 5.3.4
5.3.1	5.3.2, 5.3.3, 5.3.4
5.3.2	5.3.3, 5.3.4
5.3.3	5.3.4

Also see:

Performing a backup

To 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. Select *OK*.
7. After the backup is complete, right-click the virtual machine you backed up and go to *Power* > *Power On*.

You can use https://mysqlbackupftp.com to back up the portal and collector database.

Upgrading the portal

To 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 from the Fortinet Customer Service & Support website (https://support.fortinet.com/).
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.

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.*

Upgrading the collector

For a collector HA cluster, first upgrade the master and then the slaves. 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 from the Fortinet Customer Service & Support website (https://support.fortinet.com/).
10. Select *OK*. The collector will upgrade. After the firmware is upgraded, the system will restart automatically.

Upgrading to FortiPortal 5.3.4 and later if you are using a custom CSS file

If you are using a CSS file for a custom theme, back up the CSS file before upgrading to FortiPortal5.3.4.

This section focuses on significant changes in FortiPortal5.3.4 that affect using a custom CSS file as the color scheme when upgrading to version 5.3.4 and later. The following changes were made to the FortiPortal CSS:

- FortiPortal5.3.4 uses Bootstrap 4 style naming, grid system, table, button, and other styles.
- FortiPortal5.3.4 uses Font Awesome as the font for the entire web interface.

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 FortiPortal5.3.4)	CSS class in FortiPortal5.3.4 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')

Resolved Issues

The following issues have been fixed in 5.3.4. For inquires about a particular bug, please contact Fortinet Customer Service & Support.

Bug ID	Description
601571	When creating a customer, FortiPortal may partially create data on database when there is little disk space left on MySQL server.
603994	When changing a role's permission from read-only to read-write, the remote-auth-radius user still only can view.
608723	After FortiManager HA failover, FortiPortal may lose connectivity with FortiManager cluster.
612629	FortiPortal is unable to create or edit firewall policies if the policy package on FortiManager is a folder other than root.
618805	FortiPortal should block installation when device list is empty.
620175	DLP Sensor checkbox is mislabeled as properties.
621275	FortiPortal upgrades from 5.2.3 may fail.
625521	SD-WAN Rule should have four outgoing interface modes if ADOM version is 6.0 or higher.
630684	Permissions change in user role does not take effect immediately for remote SSO user authentication.
631169	After FortiManager HA failover and poll from FortiPortal, the status of HA master is incorrect.
631976	FortiPortal may prompt warning when accessing bandwidth field from *View* > *Source* > *Application* > *Bandwidth*.
634175	Download FortiPortal report fails when customer name contains allowed special characters.
637281	Assigned FortiToken should not be visible and selectable in user object.
641451	FortiPortal may not be able to save the changes on widgets.
642791	Letters with accent or extended characters are missing in FortiPortal reports.
643252	FortiManager may sporadically login to FortiAnalyzer with a 'null' user.
647435	FortiPortal gives error when creating user with multiple roles via API.
647625	A FortiPortal customer user cannot filter by site on dashboard.
649955	Changing the default dashboard settings from ALL to the first site.
650603	FortiPortal may prompt 500 error while loading Admin Roles.
641562	User may not be able to login using forgot password function generated passwords.
654305	FortiPortal may prompt an error when parsing FortiSandbox log records under Collector mode.

Bug ID	Description
606424	Application view reports incorrect bandwidth usage.

Known Issues

The following issues have been identified in FortiPortal 5.3.4. For inquires about a particular bug or to report a bug, please contact Fortinet Customer Service & Support.

Bug ID	Description
590535	FortiPortal cannot connect to the MySQL (8.0) server.
595541	The table element `role="presentation"` should be added to all tables.
649533	FortiGate may not be able to send logs to collector due to SSL connection error with OFTP.
629420	FortiPortal may prompt HTTP error 404 when there is unhanded HTTP error.
654241	FortiPortal may show database error HTTP 500 on "SQLGrammarException javax".