FortiPortal - Release Notes

Version 6.0.1

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 18, 2020
FortiPortal 6.0.1 Release Notes
37-601-670634-20201118

TABLE OF CONTENTS

Change Log

Date	Change Description
2020-10-22	Initial release.
2020-10-26	Added FortiManager-FortiAnalyzer 6.2.1 to 6.2.3, 6.2.5 to 6.2.6, and 6.0.9 to FortiManager, FortiOS, FortiAnalyzer, and FortiSandbox supported versions on page 6.
2020-11-18	Added FortiAnalyzer 6.4.3 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 6.0.1, build 0127. It includes the following sections:

What's new

This release contains the following new features and enhancements:

- New log types in *View* > *Log View*: Antivirus, Application Control, Web Filter, DNS, and Event.
- New Top Threats and Secure SD-WAN monitors display top threats and SD-WAN monitoring information respectively.
- New *Search by URL* filter in *Objects* > *Security Profiles* > *Web Filter Profile* that allows you to search URLs.
- In *Admin* > *Settings*, if you select RADIUS as the remote server, the *Authentication Protocol* dropdown allows you to choose between CHAP or PAP authentication protocols.

Product Integration and Support

FortiPortal 6.0.1 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 6.0.1 supports the following product versions:

Product	Supported Versions	Recommended Version
FortiAnalyzer (for reports and analytics)	• 6.4.1 to 6.4.3 • 6.2.1 to 6.2.3 and 6.2.5 to 6.2.6 • 6.0.9	6.4.3
FortiAnalyzer (for reports)	• 6.4.1 to 6.4.3 • 6.2.1 to 6.2.3 and 6.2.5 to 6.2.6 • 6.0.9	6.4.3
FortiManager	• 6.4.1 and 6.4.2 • 6.2.1 to 6.2.3 and 6.2.5 to 6.2.6 • 6.0.9	6.4.2
FortiOS	FortiOS support is determined by FortiPortal support for FortiManager and FortiAnalyzer. FortiPortal supports specific versions of FortiManager and FortiAnalyzer, and FortiManager and FortiAnalyzer support specific versions of FortiOS.	

Product	Supported Versions	Recommended Version
	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

If you are using FortiManager, 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
- MySQL 8.0.0

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 82
- Google Chrome Version 86

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

FortiPortal 6.0.1 software

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

To download the image files:

1. Log in to the Fortinet Customer Service and Support website at https://support.fortinet.com/.
2. Go to *Download > Firmware Images*.
3. In the *Select Product* list, select *FortiPortal*.
   The *Release Notes* tab for FortiPortal is displayed.
4. Click the *Download* tab.
   The *Image File Path* and *Image Folders/Files* sections are displayed.
5. In the *Image Folders/Files* section, go to *v6.00 > 6.0 > 6.0.1*.

6. Download the image files for the hypervisor you are using:
   - For OpenStack KVM, download the latest QCOW2 files:
     FPC_VM64-v6.0.1-build0127-release-portal.qcow2.zip
     FPC_VM64-v6.0.1-build0127-release-portal.out
   - For VMWare, download the latest OVF files:
     FPC_VM64-v6.0.1-build0127-release-portal.out.ovf.zip
     FPC_VM64-v6.0.1-build0127-release-portal.out

   The .zip files are used for installation, and the .out files are used for upgrade.

Detailed installation instructions are included in the *FortiPortal Administration Guide* on the Fortinet Docs Library.

Special Notices

This section contains the following:

FortiPortal 6.0.0 and later requirements

FortiPortal 6.0.0 supports only FortiAnalyzer mode. Collector mode is not supported. If you are using FortiPortal in Collector mode, you must migrate to FortiAnalyzer mode before upgrading to FortiPortal 6.0.0. See Migrating to FortiAnalyzer mode on page 14.

FortiPortal 6.0.0 features require a license. See Uploading licenses on page 15.

Special Characters with Site Name

When a site name contain special characters, FortiPortal may fail to display the policy page and install policy changes to FortiManager.

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:

```
config system sql
   set status remote
   set database-type mysql
   set password <mysql_password>
end
```

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

Theme Settings after Upgrade from 5.3

Due to major technical design changes in 6.0, users need to reconfigure FortiPortal theme settings after upgrade.

For information on updating custom CSS files after upgrade, see Updating custom CSS files after upgrade on page 15.

Enabling SNMP agent on FortiPortal

In FortiPortal 6.0.0, you can no longer configure the SNMP agent on `https://<portal_IP_address>:4443`.

To enable SNMP agent:

Enter the following commands in the CLI console:

```
config system snmp sysinfo
   set status enable
end
```

Upgrade Information

You can upgrade FortiPortal 5.3.3 or later directly to 6.0.0.

To upgrade from earlier versions of FortiPortal to 5.3.3, see Upgrade paths on page 17.

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

For FortiPortal 6.0.0 and later, you must ensure you are running FortiPortal in Analyzer mode. Collector mode is not supported in FortiPortal 6.0.0 and later. In addition, FortiPortal 6.0.0 and later requires a license.

How you upgrade from FortiPortal 5.3.3 to 6.0.0, depends on whether you are using Collector mode.

If you are using FortiPortal 5.3.3 in FortiAnalyzer mode, use the following upgrade process:

1. Back up FortiPortal 5.3.3. See Performing a backup on page 13.
2. Upgrade FortiPortal. See Upgrading the portal on page 14.
3. Apply the license. See Uploading licenses on page 15.
4. If required, update any custom CSS files. See Updating custom CSS files after upgrade on page 15.

If you are using FortiPortal 5.3.3 in Collector mode, use the following upgrade process:

1. Back up FortiPortal 5.3.3. See Performing a backup on page 13.
2. Migrate from Collector mode to FortiAnalyzer mode. See Migrating to FortiAnalyzer mode on page 14.
3. Upgrade FortiPortal. See Upgrading the portal on page 14.
4. Apply the license. See Uploading licenses on page 15.
5. If required, update any custom CSS files. See Updating custom CSS files after upgrade on page 15.

Performing a backup

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`.

To perform a backup:

1. For VMware users, go to *File* > *Export* > *Export OVF Template* to export the VM.
2. For *Name*, set a name for the backup.
3. For *Directory*, select a directory from which you can restore the backup to vSphere.
4. Optionally, enter a *Description* for the backup.
5. Select *OK*.
6. 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 database.

Migrating to FortiAnalyzer mode

FortiPortal 5.3.3 and earlier supported the following modes:

- Collector mode
- FortiAnalyzer mode

However FortiPortal 6.0.0 and later supports only FortiAnalyzer mode.

If you are using FortiPortal 5.3.3 in Collector mode, you must migrate to FortiAnalyzer mode before upgrading to FortiPortal 6.0.0 and later. If you are already using FortiAnalyzer mode, you can skip this step.

All logs and reports are lost after migrating from Collector mode to FortiAnalyzer mode. If you want to retain copies of logs and reports, back up the files before you migrate to FortiAnalyzer mode.

To migrate to FortiAnalyzer mode:

1. In FortiPortal 5.3.3, go to *Admin* > *Settings*, and select *FortiAnalyzer*.
   FortiPortal switches from Collector mode to FortiAnalyzer mode.

Upgrading the portal

Before you can upgrade the portal, you need to download the image file.

To download the image files:

1. Log in to the Fortinet Customer Service and Support website at https://support.fortinet.com/.
2. Go to *Download* > *Firmware Images*.
3. In the *Select Product* list, select *FortiPortal*.
   The *Release Notes* tab for FortiPortal is displayed.
4. Click the *Download* tab.
   The *Image File Path* and *Image Folders/Files* sections are displayed.
5. In the *Image Folders/Files* section, go to *v6.00* > *6.0* > *6.0.1*.
6. Download the image files for the hypervisor you are using:
   - For OpenStack KVM, download the latest QCOW2 files:
     FPC_VM64-v6.0.1-build0127-release-portal.qcow2.zip
     FPC_VM64-v6.0.1-build0127-release-portal.out

- For VMWare, download the latest OVF files:
  FPC_VM64-v6.0.1-build0127-release-portal.out.ovf.zip
  FPC_VM64-v6.0.1-build0127-release-portal.out

The .zip files are used for installation, and the .out files are used for upgrade.

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.

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.*

Uploading licenses

FortiPortal 6.0.0 and later requires a license. If FortiPortal is already licensed, FortiPortal can connect to FortiGuard to retrieve the latest license.

You can also manually download the license file and upload it to FortiPortal.

To manually download and upload FortiPortal licenses:

1. Log in to the Fortinet Customer Service & Support site (https://support.fortinet.com/), and download the license file.
2. In FortiPortal, go to *Admin* > *System Info*, and click *Upload License*.

Updating custom CSS files after upgrade

If you are using a CSS file for a custom theme, back up the CSS file before upgrading to FortiPortal6.0.1.

This section focuses on significant changes in FortiPortal6.0.1 that affect using a custom CSS file as the color scheme when upgrading to version 6.0.1 and later.

The following CSS classes have been removed and will no longer be used:

- `.pub-temp-body.footerText`
- `.pub-temp-body.footerText a`
- `.login-page a`
- `#sidemenu ul a`
- `.form-control,label`

The following table describes major changes in CSS class names in the `place_holder_custom.css` file:

CSS class (before FortiPortal 6.0.0)	CSS class in FortiPortal 6.0.0 and later
.headerTopClass	.fpc-header
.header .btn-link	.fpc-header a, .fpc-header .brand-title, .fpc-header .btn-link
.footerTopClass	.fpc-footer
.footerText, .footerText a	.fpc-footer, .fpc-footer a
#sidemenu	.side-nav .nav, .popover-submenu .popover .popover-body
#sidemenu ul a.active	.side-nav .nav .lv1:hover, .side-nav .nav .active
.nav-tabs .nav-link.active:before	.nav-tabs .nav-link.active:before, .nav-tabs .nav-link:hover:before
.btn-primary.fpc-btn	.btn-primary
.btn-primary.fpc-btn:hover, .btn-primary.fpc-btn:active	.btn-primary:hover, .btn-primary:active, .btn-primary.active, .btn-primary:not(:disabled):active
.btn-outline-secondary.fpc-btn	.btn-outline-primary
a, a:hover	set color as body's color
.text-primary	set color as body's color
login-page .login-modal-form .input-group .input-icon	set background as .login-page
.login-page .login-modal-form .input-group input, .login-page .login-modal-form .input-group input:focus	set border-color as .login-page
.login-page .login-modal-header,	set color as body's color

CSS class (before FortiPortal 6.0.0)	CSS class in FortiPortal 6.0.0 and later
.login-page .login-modal-header .login-service-name	
.modal .modal-content:before	set background color on modal's top bar
.sweet-alert:before	set background color on modal's top bar
.ui-dialog .ui-dialog-titlebar > span:first-child::before	set background color on modal's top bar
.nav-tabs .nav-link.active	set border color on nav

The following table identifies renamed items in the `place_holder_custom.css` file:

Name (before FortiPortal 6.0.0)	Name in FortiPortal 6.0.0 and later
.headerTopClass	.fpc-header
.header .btn-link	.fpc-header a, .fpc-header .brand-title, .fpc-header .btn-link
.footerTopClass	.fpc-footer
.footerText, .footerText a	.fpc-footer, .fpc-footer a
#sidemenu	.side-nav .nav, .popover-submenu .popover .popover-body
#sidemenu ul a.active	.side-nav .nav .lv1:hover, .side-nav .nav .active
.nav-tabs .nav-link.active:before	.nav-tabs .nav-link.active:before, .nav-tabs .nav-link:hover:before
.btn-primary.fpc-btn	.btn-primary
.btn-primary.fpc-btn:hover .btn-primary.fpc-btn:active	.btn-primary:hover, .btn-primary:active, .btn-primary.active, .btn-primary:not(:disabled):active
.btn-outline-secondary.fpc-btn	.btn-outline-primary

Upgrade paths

The following table identifies the supported FortiPortal upgrade paths. 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
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

Existing Version	Compatible Upgrade Version
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, 6.0.0
5.3.4, 6.0.0	6.0.1

Resolved Issues

The following issues have been fixed in 6.0.1. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
630521	When adding a site, FortiPortal may prompt an incorrect warning to detach devices.
646597	FortiPortal is missing the Internet Service input option in *SDWAN Template* > *SDWAN Rule*.
646625	After changing the destination from Address to Internet Service, the SDWAN rule cannot be saved.
646541	Signatures displayed in the IPS Sensor may be displayed multiple times.
646608	FortiPortal may not be able to display details for the Sandbox log.
646928	*Review* tab does not display information if the source or destination address are set as IPv6 addresses or Internet Service.
619997	When creating a static route with SD-WAN interface, users should not be required to default a gateway.
647209	When listing the devices from FortiManager, the device name may overlap with another field if the device name is too long.
666768	Device filter may not work for the SD-WAN Monitor or the Table view.
666677	FortiPortal is missing column option to sort entries under SD-WAN Monitor or Table view.
663423	API call fpc/api/customers/<cust_id>/installs/<install_id> may result in 500 error.
663094	FortiPortal may return "Certificate Unknown" when connecting to the SMTP server with STARTTLS.
663081	FortiPortal API does not include the "Device Manager" property required to configure tab permissions.
662155	FortiPortal may show unexpected collector log messages.
659480	Under the customer configuration, in the "Policy Tab Permissions" section, the option for "DoS Policy" is listed twice.
659391	Top Countries dashboard widget may show incorrect data.
657952	Remote Server IP Address does not allow Domain Names for RADIUS.
653655	Searching radius roles is not working on the *Admin* > *Settings* tab.
649955	A customer user cannot filter by site on the dashboard.
641451	FortiPortal may not be able to save the changes on dashboard widgets.
590535	FortiPortal cannot connect to MySQL 8.0.

Known Issues

The following issues have been identified in FortiPortal 6.0.1. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
613938	When creating a new WiFi SSID, it saves without any error, but no new SSID is created.
614500	SD-WAN template is not showing the rule Criteria or the default rule.
615927	User cannot update per-device SD-WAN configuration for *Performance SLA > Packet size value*.
624315	Only one device shows for devices at the same location in the SD-WAN map.
626378	Rating and Proxy option settings changed when Web filter object created from FortiManager and edited on FortiPortal.
631340	Timestamps in FortiPortal may not be uniform across the system.
634040	If a FortiManager has been added with the correct password, then even if it is changed to a wrong password, the poll will still succeed.
637515	FortiPortal shows error when SD-WAN drill down view is not able to find SLA or interface logs.
641532	FortiPortal cannot show the *Policy* tab when the site name contains special characters.
645186	When a policy package name contains a special character, FortiPortal cannot install the policy package.
646551	Right click menu for FortiGuard Categories in the DNS filter profile shows invalid actions.
646920	User cannot create a policy with only IPv6 Addresses on a FortiGate 6.4 device.
620619	Installation fails when a DNS profile is created from FortiPortal.
671520	Port forwarding configuration is missing for VIP.
671133	User can only select one IPS signature at a time and it becomes read-only IPS Sensor.
672124	SD-WAN Performance Status widget may not poll data based on the specified time interval.
642048	After upgrade, FortiPortal may lose connection to all FortiManager or FortiAnalyzer units. **Workaround**: Please reboot the FortiPortal.