FortiPortal - Release Notes

Version 6.0.4

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://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

FORTINET®

June 10, 2021
FortiPortal 6.0.4 Release Notes
37-604-717665-20210610

TABLE OF CONTENTS

Change Log

Date	Change Description
2021-05-19	Initial release.
2021-06-10	Added FortiManager-FortiAnalyzer 6.0.11 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 6.0.4, build 0240. It includes the following sections:

- Product Integration and Support on page 6
- Special Notices on page 10
- Upgrade Information on page 13
- Known Issues on page 22

What's new

This release contains the following new features and enhancements:

- New *Last N Minutes/Hours/Days/Months* time ranges added to *Insights, Log View, Monitors*, and *Reports*.
- Per-device view associated with a site available in *SD-WAN > Monitoring*.
- A new *Device Health* tab available in *Dashboard*. It displays the managed devices status summary.
- A new *SD-WAN Monitoring* tab (*SD-WAN > Monitoring*) that consolidates SD-WAN related information from *View > Monitors > Secure SD-WAN* and *Device Manager > SD-WAN > Monitoring*.
- FortiPortal now allows you to give an alias for ADOM/Device/VDOM in *Add/Edit Customer* and *Add/Edit Site* dialogs to prevent customers from knowing the MSSP configuration when they access devices from dropdown menus.
- Performance improvements in SD-WAN monitoring.

Product Integration and Support

FortiPortal 6.0.4 supports some FortiManager, FortiOS, FortiAnalyzer, and FortiSandbox versions.

The section contains the following topics:

- FortiManager, FortiOS, FortiAnalyzer, and FortiSandbox supported versions on page 6
- Database Support on page 8
- Web browser support on page 8
- FortiPortal 6.0.4 software on page 8

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 6.0.4 supports the following product versions:

Product	Supported Versions	Recommended Version
FortiAnalyzer	• 6.4.1 to 6.4.5 • 6.2.1 to 6.2.3 and 6.2.5 to 6.2.8 • 6.0.9 to 6.0.11	6.4.5
FortiManager	• 6.4.1 to 6.4.5 • 6.2.1 to 6.2.3 and 6.2.5 to 6.2.8 • 6.0.9 to 6.0.11	6.4.5
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. 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:

- ADOM supported versions on page 7
- Additional compatibility resources on page 7
- Hypervisor support on page 7

ADOM supported versions

FortiPortal 6.0.4 supports the following FortiManager ADOM versions:

Product	Supported FortiManger Versions	Supported ADOM Versions			
		6.4	6.2	6.0	5.6
FortiManager	6.4.1 to 6.4.5	✓	✓	✓	✓
	6.2.1 to 6.2.3 and 6.2.5 to 6.2.8		✓	✓	✓
	6.0.9 to 6.0.11			✓	✓

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 85
- Google Chrome Version 88

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

FortiPortal 6.0.4 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* > *6.0.4*.
6. Download the image files for the hypervisor you are using:
   - For OpenStack KVM, download the latest QCOW2 files:
     FPC_VM64-v6.0.4-build0240-release-portal.qcow2.zip
     FPC_VM64-v6.0.4-build0240-release-portal.out
   - For VMWare, download the latest OVF files:
     FPC_VM64-v6.0.4-build0240-release-portal.out.ovf.zip
     FPC_VM64-v6.0.4-build0240-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 on page 10
- Special Characters with Site Name on page 10
- Reconfiguring MySQL password on FortiPortal on page 10
- SSID Naming on page 11
- Supported FortiManager API Endpoints on page 11
- Theme Settings after Upgrade from 5.3 on page 11
- Enabling SNMP agent on FortiPortal on page 12
- Requirements for Run Reports on page 12
- Moving an SD-WAN rule on page 12

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
```

Requirements for Run Reports

To successfully run a report in FortiPortal, the following requirements must be met:

1. All FortiAnalyzer units on FortiPortal must have a version higher than 6.4.2.
2. All the devices within a site must belong to the same ADOM on the same FortiAnalyzer.

Moving an SD-WAN rule

Due to technical limitation on FortiManager 6.4.3 or earlier, a FortiPortal user must save configurations first after a rule is moved, otherwise FortiPortal may not save the order of the rules when other actions such as creating and editing rules are combined.

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 18.

FortiPortal does not support database downgrade. Before upgrading FortiPortal, take a snapshot of the portal database server and 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.

To backup and restore using the CLI:

Use the following CLI commands to backup and restore the configuration:

- execute backup all-settings {ftp | scp | sftp} <server ip> <path/filename> <username> <password>
- execute restore all-settings {ftp | scp | sftp} <server ip> <path/filename> <username> <password>

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 > 6.0.4*.
6. Download the image files for the hypervisor you are using:
   - For OpenStack KVM, download the latest QCOW2 files:
     FPC_VM64-v6.0.4-build0240-release-portal.qcow2.zip
     FPC_VM64-v6.0.4-build0240-release-portal.out
   - For VMWare, download the latest OVF files:
     FPC_VM64-v6.0.4-build0240-release-portal.out.ovf.zip
     FPC_VM64-v6.0.4-build0240-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 FortiPortal6.0.4.

This section focuses on significant changes in FortiPortal6.0.4 that affect using a custom CSS file as the color scheme when upgrading to version 6.0.4 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,	set border-color as .login-page

CSS class (before FortiPortal 6.0.0)	CSS class in FortiPortal 6.0.0 and later
.login-page .login-modal-form .input-group input:focus	
.login-page .login-modal-header, .login-page .login-modal-header .login-service-name	set color as body's color
.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

Existing Version	Compatible Upgrade Version
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, 6.0.0
5.3.4, 6.0.0	6.0.1
5.3.5, 6.0.0 - 6.0.1	6.0.2
5.3.5, 6.0.0 - 6.0.2	6.0.3
5.3.5, 6.0.0 - 6.0.3	6.0.4

Resolved Issues

The following issues have been fixed in 6.0.4. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
703113	*System Notifications* can only be assigned to the first 100 customers.
685721	Customer User with Read-Only permission can run report.
703764	FortiPortal shows error while loading SD-WAN Monitoring in *Device Manager*.
624315	Only one device shows for multiple devices at the same location in SD-WAN map.
707169	SD-WAN color-coding can be mismatched.
706246	Inconsistencies between the FortiPortal Monitor graphs and FortiAnalyzer FortiView graphs.
701595	Run Report settings is reset when reporting period is changed.
697838	User can still run reports even though the permission has been taken away.
696107	User with read-only role is not able to view web filer profile when FortiManager ADOM is locked.
700549	There may be some French translation issues in the *Run Reports* window.
696857	Uploaded images within the size limit should be shown properly in the preview.
695432	User passwords may be hashed with SHA-1.
697209	FortiPortal should show a readable timestamp under *Policy* > *Revision Backup*.
697207	There may be multiple issues with the action settings under *Objects* > *Security Profiles* > *Web filter Profile* > *FortiGuard Categories*.
646551	Right-click menu for FortiGuard Categories in DNS filter profile may show invalid actions.
701609	Changing role type resets role permissions.
702240	Source code shows up when the user visits the backup login page when SSO is disabled.
706554	*Top Sources* and *Top destinations* widgets on customer's *Dashboard* > *Insights* tab show 'invalid' for entries with MAC addresses.
707779	FortiPortal may show warning message on *Security Profiles* object which is not same as package setting.
708918	Security Profiles with special characters not showing correctly on FortiPortal.
709201	IPS Signatures may be lost within IPS sensor profile.
641532	FortiPortal may not display policy package with certain characters.

Bug ID	Description
711284	FortiPortal may return error message stating query did not return unique result when a single ADOM on FortiManager contains three VDOMs from the same device.
697224	*Policy* dropdown does not display the dropdown when clicking the arrow.

Known Issues

The following issues have been identified in FortiPortal 6.0.4. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
719097	Device name should be replaced with an alias in the *Authorized Access Points* widget in *Dashboard* > *Insights*.
719091	Policy Hits widget does not show alias.
718303	In the provider portal, pages that list devices should show VDOM alias.
613938	When creating a new WiFi SSID, it saves without any error, but no new SSID is created.
624315	FortiPortal should show healthy or unhealthy device percentage when multiple devices are at the same location.
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.
646920	User cannot create policy with only IPv6 addresses on a FortiGate 6.4 device.
642048	After an upgrade, FortiPortal may lose connection to all FortiManager or FortiAnalyzer units. **Workaround:** Please reboot the FortiPortal.
684426	When devices belong to two FortiAnalyzer units, the generated report for those units cannot be shown on FortiPortal.
681210	Rogue AP page is empty or stuck.
680943	Application and Filter Overrides cannot be moved up or down.
680939	IPS signature and filer entries cannot be reordered.
680859	The color of address object is not shown in the policy list.
684813	FortiPortal may not list all the available interfaces as it lack normalization interface support.
720135	*Run Reports* may return an error if a customer has no ADOM filter selected.