

Release Notes

FortiPortal 7.0.1



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/training-certification>

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



September 6, 2022

FortiPortal 7.0.1 Release Notes

37-701-827174-20220906

TABLE OF CONTENTS

Change Log	4
Introduction	5
What's new	5
System requirements	5
Product Integration and Support	6
FortiManager, FortiOS, FortiAnalyzer, FortiAnalyzer BigData, and FortiSandbox supported versions	6
ADOM supported versions	7
Additional compatibility resources	7
Hypervisor support	7
Web browser support	8
FortiPortal 7.0.1 software	8
Special Notices	9
Special Characters with Site Name	9
Supported FortiManager API Endpoints	9
Requirements for Run Reports	10
Limitations with Scalable Cluster	10
Installing FortiPortal 7.0.1	11
Upgrade Information	12
Resolved Issues	13
Known Issues	14

Change Log

Date	Change Description
2022-08-04	Initial release.
2022-08-30	Updated Installing FortiPortal 7.0.1 on page 11.
2022-09-06	Update Hypervisor support on page 7.

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 7.0.1, build 0084. It includes the following sections:

- [What's new on page 5](#)
- [System requirements on page 5](#)
- [Product Integration and Support on page 6](#)
- [Special Notices on page 9](#)
- [Installing FortiPortal 7.0.1 on page 11](#)
- [Upgrade Information on page 12](#)
- [Resolved Issues on page 13](#)
- [Known Issues on page 14](#)

What's new

FortiPortal version 7.0.1, build 0084, is a patch release only. There are no new features and enhancements in this release. For more information, see [Resolved Issues on page 13](#) and [Known Issues on page 14](#).

System requirements

FortiPortal version 7.0.1 minimum system requirements:

- 4 CPUs
- 16 GB RAM
- 12 GB free disk space

Product Integration and Support

FortiPortal 7.0.1 supports some FortiManager, FortiOS, FortiAnalyzer, FortiAnalyzer BigData, and FortiSandbox versions.

This section contains the following topics:

- [FortiManager, FortiOS, FortiAnalyzer, FortiAnalyzer BigData, and FortiSandbox supported versions on page 6](#)
- [Web browser support on page 8](#)
- [FortiPortal 7.0.1 software on page 8](#)

FortiManager, FortiOS, FortiAnalyzer, FortiAnalyzer BigData, 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 7.0.1 supports the following product versions:

Product	Supported Versions	Recommended Version
FortiAnalyzer	<ul style="list-style-type: none">• 7.0.1 to 7.0.3• 6.4.1 to 6.4.8	7.0.3
FortiAnalyzer BigData	<ul style="list-style-type: none">• 7.0.x	7.0.2
FortiManager	<ul style="list-style-type: none">• 7.0.1 to 7.0.4• 6.4.1 to 6.4.8	7.0.3
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	<ul style="list-style-type: none">• 3.0.2	3.0.2



You must ensure that the FortiManager and the FortiAnalyzer user accounts (that you created for FortiPortal) have *Remote Procedure Call (RPC)* set to *read-write*. In previous FortiManager-FortiAnalyzer releases, RPC was enabled by default. FortiManager-FortiAnalyzer 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 7.0.1 supports the following FortiManager ADOM versions:

Product	Supported FortiManger Versions	Supported ADOM Versions	
		7.0	6.4
FortiManager	7.0.1 to 7.0.4	✓	✓
	6.4.1 to 6.4.8		✓

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 6.0, 6.5, 6.7, and 7.0

Web browser support

The following web browsers are supported:

- Microsoft Internet Explorer (IE) Version 11
- Mozilla Firefox (up to) Version 103
- Google Chrome Version 103



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

FortiPortal 7.0.1 software

FortiPortal is delivered as a virtual machine for the VMware hypervisor.

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 *v7.00 > 7.0 > 7.0.1*.
6. Download the image files for VMWare:
 - FPC_VM64-v7.0.1-build0084-release-portal.ova

Detailed installation instructions are included in the *FortiPortal Administration Guide* on the [Fortinet Docs Library](#).

Special Notices

This section contains the following:

- [Special Characters with Site Name on page 9](#)
- [Supported FortiManager API Endpoints on page 9](#)
- [Requirements for Run Reports on page 10](#)
- [Limitations with Scalable Cluster on page 10](#)

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.

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

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.

Limitations with Scalable Cluster

Due to known technical limitations, FortiPortal Scalable Cluster is subject to the following caveats:

- When the primary unit is down, it may take several minutes before the cluster resumes responding.
- When joining multiple secondary units to a cluster, please join the units in sequential order.
- When multiple units are shutdown, please power-on units in sequential order when resuming service.

Installing FortiPortal 7.0.1

To install FortiPortal 7.0.1:

1. Deploy the VMware FortiPortal image file on a hypervisor.



Make sure the network interface is connected to a reachable network adapter.

2. Once the FortiPortal instance is booted up, log in with the default username `admin` and password `portal1234`. You can change the password by entering the following commands in the CLI console:

```
config system admin user
edit admin
set password
Old password: xxxxxx
New password: yyyyyy
Retype password: yyyyyy
end
```

3. In the CLI console, enter the following commands to configure the IP address for the instance:

```
config system interface
edit port1
set ip x.x.x.x/x.x.x.x
end
```

4. In the CLI console, enter the following commands to configure the default route for the instance:

```
config system route
edit 1
set device port1
set gateway x.x.x.x
end
```

5. Optionally, in the CLI console, enter the following commands to configure the DNS for the instance:

```
config system dns
set primary x.x.x.x
set secondary y.y.y.y
end
```

6. Optionally, in the CLI console, enter the following commands to configure the NTP for the instance:

```
config system ntp
config ntpserver
edit 1
set server x.x.x.x or <hostname>
end
```

7. Connect to FortiPortal via the web interface using the configured IP address. The default web login username and password are `spuser` and `test12345`, respectively. Upon login, you may change the web login credential.



The login credentials are separated between web UI and console/SSH.

Upgrade Information

You can upgrade from FortiPortal 7.0.0 to 7.0.1.



Upgrading FortiPortal 6.0.x and below to 7.0.x is not supported yet.

To upgrade FortiPortal to the latest version, [Back up FortiPortal configuration on page 12](#) and then [Upgrade FortiPortal on page 12](#).

Back up FortiPortal configuration

To back up FortiPortal configuration:

1. Go to *Dashboard*.
2. In the *System Information* pane, select the *System Backup* (📄) icon in *System Configuration* to save a backup file onto the local computer.

Upgrade FortiPortal

To upgrade FortiPortal:

1. Go to *Dashboard*.
 2. In *System Information* pane, select the icon (📄) in *Version*.
 3. In the *Firmware Management* pane, select *Choose File* and locate the firmware image on your local computer.
 4. Select *Upload*.
-



Uploading a firmware image requires sufficient network bandwidth.

The firmware image uploads from your local computer to the FortiPortal, which will then reboot.



Do not log in until FortiPortal has completely restarted.

Resolved Issues

The following issues have been fixed in 7.0.1. For inquiries about a particular bug, please contact Customer Service & Support.

Bug ID	Description
765816	Increased memory size to 16 GB.
748739	<ul style="list-style-type: none">• User may not be able to configure the remote syslog server.• Log files may not be rolling.

Known Issues

The following issues have been identified in FortiPortal 7.0.1. For inquiries about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
788989	Session timeout may not function correctly.
806414	The top 10 charts may display only top 5 entries in <i>Insight > Health</i> .
809079	Types LDAP, Radius, and TACACS+ might be missing in User object.
817026	VIP/VIP Groups may show up in "IPv4 Destination Address" dropdown when user is editing a policy.
817455	The detailed content of the change may not be available in Audit log.
817796	When user tries to edit an address, the "Static route configuration" may be shown as disabled with FortiManager 7.0.4.
818750	Sorting by "VLAN" may not work correctly in <i>Switch Monitoring > Clients</i> page.
819143	No audit log may be generated for SD-WAN templates related changes.
819964	User may not be able to run reports on FortiPortal with FortiAnalyzer 7.0.4.
821517	The signature list in IPS profile may not be updating accordingly if user changes severity/target/protocol.
822563	When the primary node in an HA cluster is down, operations may be slow.



www.fortinet.com

Copyright© 2022 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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. 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.