

Getting Started Guide

FortiPortal 7.0.0



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



July 20, 2022

FortiPortal 7.0.0 Getting Started Guide

37-700-735201-20220718

TABLE OF CONTENTS

Change Log	4
Overview	5
Contact Us	5
Preparing FortiManager and FortiAnalyzer	6
Deploying and configuring FortiPortal	8
Installation on VMware	8
Downloading virtual machine image files	8
Installing FortiPortal VMs	8
Starting the VM	9
Logging in to the portal	9
Configuring the portal	10
Configuring a scalable cluster	11

Change Log

Date	Change Description
2022-07-04	Initial release.
2022-07-18	Updated Installation on VMware on page 8 . Updated Configuring the portal on page 10 . Added Configuring a scalable cluster on page 11 .

Overview

This guide will walk you through the setup and initialization of your FortiPortal VM. For detailed step-by-step instructions, please see the *FortiPortal Administration Guide*.

Contact Us

For assistance in setting up your VM, please visit <https://support.fortinet.com/>.

Preparing FortiManager and FortiAnalyzer

FortiPortal interacts with FortiManager and FortiAnalyzer. For specific setup configurations, please consult the [FortiPortal Administration Guide](#) to optimize CPU usage and memory sizes. Fortinet also recommends contacting your Fortinet Systems Engineer for assistance.

To configure FortiManager to work with FortiPortal:

1. *The ADOM mode must be enabled for FortiManager to work with FortiPortal.* If needed, enable ADOMs and the advanced adom-mode on FortiManager so that you can add VDOMs on the same physical device to different ADOMs. For example:

```
config system global
  set adom-status enable
  set adom-mode advanced
  y
end
```

2. Create a portal user with read-and-write permission:

```
config system admin user
  edit fpc
    set profileid Super_User
    set adom all_adoms
    set policy-package all_policy_packages
    set password fortinet
    set rpc-permit read-write
  next
end
```

3. *The workspace mode must be enabled for FortiManager to work with FortiPortal.*

```
config system global
  set workspace-mode normal
end
```

4. In FortiManager, go to the root of the ADOM and then go to *System Settings > Network*; enable the *Web Service* option for the administrative access for the system network management interface.
5. Add your FortiManager device using the JSON port. You must poll FortiManager to see the device list. For more information about adding FortiManagers to the portal, see the [FortiPortal Administration Guide](#).

To configure FortiAnalyzer to work with FortiPortal:

1. The ADOM mode must be enabled for FortiAnalyzer to work with FortiPortal. You must enable the interface permission `webservice` on FortiAnalyzer for the portal-facing interface.
2. You must allow remote procedure calls. Create an admin user for portal:

```
config system admin user
  edit <user_name>
```

```
set profileid Super_User
set rpc-permit read-write
end
```

Deploying and configuring FortiPortal

FortiPortal software provides a self-service management interface for organizations (or any organization that uses FortiManager to manage security instances) to monitor and configure security instances without direct FortiManager access. FortiPortal is a web application and runs on virtual machines.

This chapter covers the following topics:

- [Installation on VMware on page 8](#)
- [Logging in to the portal on page 9](#)
- [Configuring the portal on page 10](#)
- [Configuring a scalable cluster on page 11](#)

Installation on VMware

This chapter assumes some familiarity with the VMware vSphere Client terminology.

All VM instances run on VMware ESXi Server versions 5.5, 6.0, 6.5, 6.7, and 7.0.

Before deploying your FortiPortal using VMware, install the [VMware vSphere Client](#) on the management computer.

Downloading virtual machine image files

To download the VM files:

1. Go to [FortiCloud](#) and log in to your account.
2. Go to *Support > Downloads > Firmware Download*.
3. Select FortiPortal.
4. Click the *Download* tab.
5. Extract the package to a local folder on the management computer.

Installing FortiPortal VMs

The first time you start the portal, you will have access only through the console window of your VM server environment. After you configure the initial parameters, you can access FortiPortal through the web-based portal.

Deploying a VM instance

To deploy a VM instance:

1. Launch the VMware vSphere client.
2. Enter the IP address or host name of your VMware server.
3. In the inventory menu, select the physical server where you will install the VM.

4. Select *File > Deploy OVF Template* to launch the OVF Template wizard. The wizard will guide you through a series of deployment steps.
5. *Source*: Use the Browse function to locate the OVF file that you downloaded.
6. *OVF Template Details*: This page displays the following information: FortiPortal version, size of the download, and application size on disk.
Click *Next*.
7. *End-user License Agreement*: Accept the end-user license agreement and click *Next*.
8. *Name and Location*: Enter a name for this virtual machine, select a location from the location inventory, and click *Next*.
9. *Storage*: Select the destination storage for the virtual machine files and click *Next*.
10. *Disk Format*: This page displays the storage device that you selected in the previous step, along with available space. Select *Thin Provision* and click *Next*.
11. *Network Mapping*: Select the destination network to map to the source network in your OVF and click *Next*.
12. *Ready to Complete*: Review the deployment settings. Select *Back* to make any changes. When ready, click *Finish*.

Configuring VM hardware settings

To configure the VM settings:

1. Select the newly created VM in the inventory list and go to *Getting started > Edit virtual machine settings*.
2. Adjust the VM CPU, memory, and storage settings and click *Save*. The following are the **minimum** requirements:
 - CPU: 4
 - Memory: 16 GB
 - Hard drive: 12 GB

For more information about sizing, please consult "[Appendix A - Sizing](#)" in the *FortiPortal Administration Guide*.

Starting the VM

To start the virtual machine:

1. In the inventory list, right-click the FortiPortal VM that you just deployed and click *Power On*.
2. Right-click on the instance and click *Open Console* to see the login prompt.

Logging in to the portal

Use the default user name and password to log in to the portal.

Component	Default User Name	Default password
Console/SSH	admin	portal1234
Portal GUI	spuser	test12345



The login credentials are separated between the portal GUI and console/SSH.

Configuring the portal

- Before you can access the portal GUI, you must configure the VM port1 with an IP address and administrative access using the CLI console.

- Log in to the console using the default console/SSH credentials.
- To change the admin password using the CLI:

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

- In the CLI console, enter the following commands to configure the IP address and netmask:

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

- 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
```

- Optionally, in the CLI console, enter the following commands to configure the DNS servers for the instance:

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

- Optionally, in the CLI console, enter the following commands to configure the NTP server for the instance:

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



The NTP source should be the same for all portal VMs to synchronize the log time stamps across all devices.

- Connect to FortiPortal via the GUI using the configured IP address and the default portal GUI credentials. After logging in and successfully uploading the license file, you may change the login credentials.
- Upload the license file. Go to *System > Settings > General*, and click *Upload* in *Upload License*.

4. After the license is uploaded, check that the license status is valid and the number of devices allowed is correct in the *Dashboard*.



The individual portal VM does not have a serial number.

Configuring a scalable cluster



Use this feature only if you are certain that a FortiPortal cluster is required. Once a cluster has been set up it cannot be deleted.

When a FortiPortal instance is used to set up a new cluster or a FortiPortal instance joins an existing cluster, the FortiPortal instance can no longer be a standalone FortiPortal.

A cluster consists of a primary unit and two or more standby secondary units. A minimum of three units is required to set up a cluster. If the primary unit becomes unavailable, one of the standby secondaries will become the new primary.

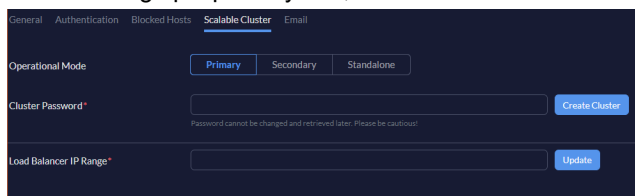
The following roles are available:

- *Standalone*: The FortiPortal is independent of a high-availability cluster. This is the default setting. Use it if you intend to keep the FortiPortal instance independent of a cluster.
- *Primary*: The FortiPortal is the primary in a high-availability cluster.
- *Secondary*: The FortiPortal is a secondary in a high-availability cluster.

To set up a FortiPortal cluster:

1. Prepare your system for the cluster.
 - a. If the *Certificate Information* and *Upload License* related options in *System > Settings* need to be updated, the options should be updated in the primary unit before setting up the cluster.
 - b. If the firmware, restore, and backup options in the *Dashboard* need to be updated, the options should be updated in the primary unit before setting up a cluster.
2. Set up the primary instance.
 - a. Log in to the primary FortiPortal instance.
 - b. Go to *System > Settings > Scalable Cluster*.

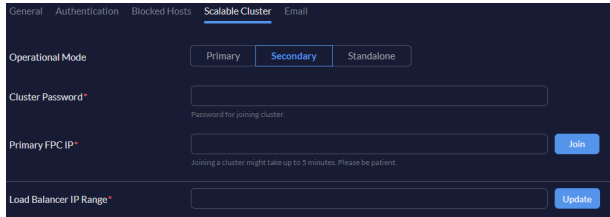
When setting up a primary unit, the *Scalable Cluster* tab looks like the following:



- c. In the *Operational Mode* field, select *Primary*.
- d. In the *Cluster Password* field, set a password for the cluster. This password cannot be retrieved or changed once it is set.
- e. Click *Create Cluster*.

3. Set up two or more secondary units.
 - a. Log in to another FortiPortal instance.
 - b. Go to *System > Settings > Scalable Cluster*.

When setting up a secondary unit, the *Scalable Cluster* tab looks like the following:



The screenshot shows the 'Scalable Cluster' configuration page in FortiPortal. At the top, there are tabs for 'General', 'Authentication', 'Blocked Hosts', 'Scalable Cluster', and 'Email'. The 'Operational Mode' section has three radio buttons: 'Primary', 'Secondary' (which is selected), and 'Standalone'. Below this is the 'Cluster Password' field with a placeholder text 'Password for joining cluster'. The 'Primary FPC IP' field is empty, and there is a 'Join' button next to it. Below that is the 'Load Balancer IP Range' field with an 'Update' button. A small note at the bottom of the form says 'Joining a cluster might take up to 5 minutes. Please be patient.'

- c. In the *Operational Mode* field, select *Secondary*.
 - d. In the *Cluster Password* field, enter the cluster password you set on the primary instance.
 - e. In the *Primary FPC IP* field, enter the IP address of the primary instance.
 - f. Click *Join*.
 - g. Repeat step 3 to add additional secondary instances to the cluster.
4. Configure the load balancer (optional).
 - a. Log in to one of the FortiPortal instances in the cluster.
 - b. Go to *System > Settings > Scalable Cluster*.
 - c. In the *Load Balancer IP Range* field, enter an IP address in the same subnet as the cluster instances. This IP should be one that is not assigned to any devices.
 - d. Click *Update*.

The load balancer IP configuration is automatically applied across all instances of the cluster.



After upgrading a FortiPortal instance, you must set the load balancer IP address again.



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.