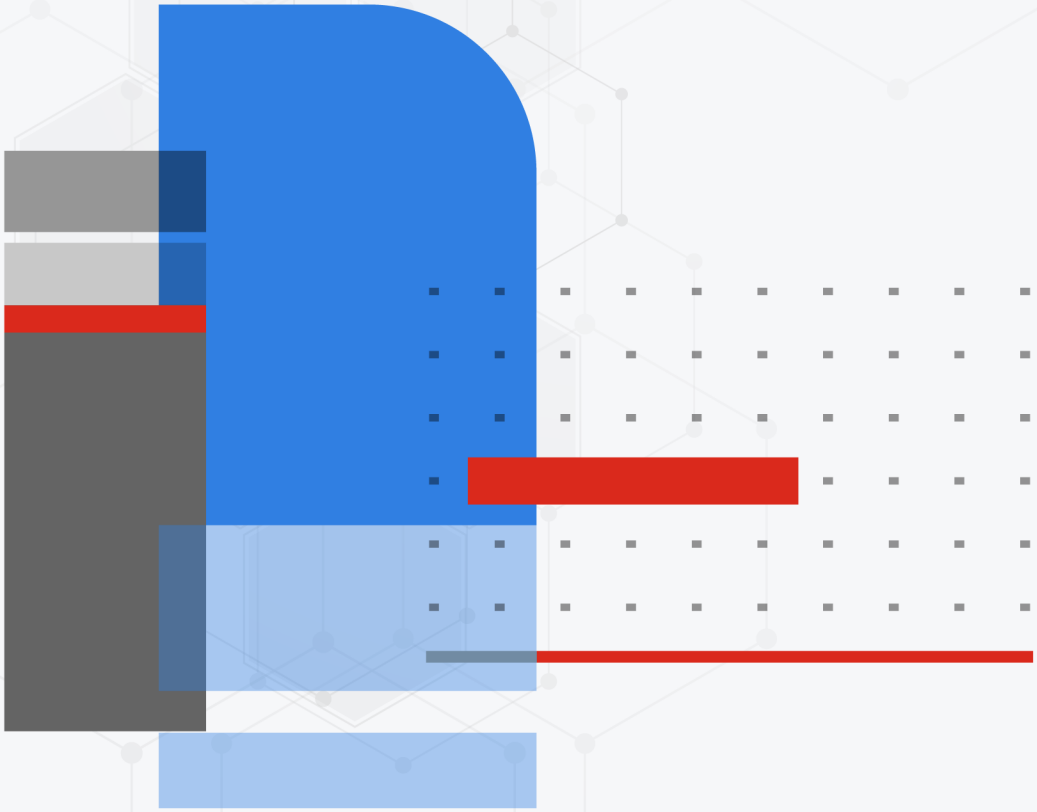
Release Notes

FortiPortal 7.2.7



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

FORTINET VIDEO LIBRARY
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

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

May 29, 2025
FortiPortal 7.2.7 Release Notes
37-727-1119045-20250529

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 7.2.7 software 8
Special Notices **9**
Port security requirements 9
Supported FortiManager API Endpoints 9
Requirements for Run Reports 10
Limitations with Scalable Cluster 10
SD-WAN Link Utilization widget with FortiAnalyzer 7.4.2 and later 10
Profile changes from previous version 11
Profile: Admin 11
Profile: Customer Admin 11
Profile: Customer Monitor 11
Profile: Web&Video Filters Admin 11
FortiPortal 6 features not implemented in FortiPortal 7.2.7 11
Scheduled backup password character restrictions 12
Limitation with install preview 12
Installing FortiPortal 7.2.7 ..... **13**
Installing on AWS or Azure 14
Upgrading FortiPortal **15**
Upgrading to 7.2.7 15
Upgrading AWS and Azure 16
Resolved Issues **17**
Common Vulnerabilities and Exposures 17
Known Issues **18**

Change Log

Date	Change Description
2025-01-30	Initial release.
2025-02-11	Updated Resolved Issues on page 17.
2025-02-10	Updated FortiManager, FortiOS, FortiAnalyzer, FortiAnalyzer BigData, and FortiSandbox supported versions on page 6 and ADOM supported versions on page 7.
2025-02-25	Updated Special Characters with Site Name.
2025-03-05	Removed Special Characters with Site Name.
2025-03-24	Added Port security requirements on page 9.
2025-04-29	Updated FortiManager, FortiOS, FortiAnalyzer, FortiAnalyzer BigData, and FortiSandbox supported versions on page 6.
2025-05-29	Updated FortiManager, FortiOS, FortiAnalyzer, FortiAnalyzer BigData, and FortiSandbox supported versions on page 6 and ADOM supported versions 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 7.2.7, build 1282. 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 7.2.7 on page 13
- Upgrading FortiPortal on page 15
- Resolved Issues on page 17
- Known Issues on page 18

What's new

This release contains the following new features and enhancements:

- APIs added to poll connected FortiManager and FortiAnalyzer devices.

System requirements

FortiPortal version 7.2.7 minimum system requirements:

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

Product Integration and Support

FortiPortal 7.2.7 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 7.2.7 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 7.2.7 supports the following product versions:

Product	Supported Versions
FortiAnalyzer	• 7.4.0 to 7.4.7 • 7.2.1 to 7.2.10 • 7.0.1 to 7.0.3, 7.0.5 to 7.0.13
FortiAnalyzer BigData	• 7.0.x
FortiManager	• 7.4.0 to 7.4.7 • 7.2.1 to 7.2.10 • 7.0.1 to 7.0.13
FortiOS	For FortiOS support, refer to the FortiManager or FortiAnalyzer release notes of the appropriate version in the Fortinet Docs Library.
FortiSandbox	• 3.0.2 to 4.4.7

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*. Configure it 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 7.2.7 supports the following FortiManager ADOM versions:

Product	Supported FortiManger Versions	Supported ADOM Versions		
		7.2	7.0	6.4
FortiManager	7.4.0 to 7.4.7	✓	✓	✓
	7.2.1 to 7.2.10	✓	✓	✓
	7.0.1 to 7.0.13		✓	✓

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
- KVM Version 2.6.x
- Nutanix AHV

Web browser support

The following web browsers are supported:

- 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 7.2.7 software

FortiPortal is delivered as a virtual machine.

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* > *7.2* > *7.2.7*.
6. Download the image files:
   - For KVM, download the latest QCOW2 file:
     FPC_VM64-v7.2.7-build1282-release-portal.qcow2
   - For VMWare, download the latest OVA file:
     FPC_VM64-v7.2.7-build1282-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:

- Port security requirements on page 9
- Supported FortiManager API Endpoints on page 9
- Requirements for Run Reports on page 10
- Limitations with Scalable Cluster on page 10
- SD-WAN Link Utilization widget with FortiAnalyzer 7.4.2 and later on page 10
- Profile changes from previous version on page 11
- FortiPortal 6 features not implemented in FortiPortal 7.2.7 on page 11
- Scheduled backup password character restrictions on page 12
- Limitation with install preview on page 12

Port security requirements

For security concerns, restrict public access to only HTTPS (port 443). All other ports, including port 22 (SSH) and ports required for scalable clusters (2379/2380, 6443, 8000, 7472/7946, 8472 (UDP), and 10250) must be restricted to internal access only.

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.

SD-WAN Link Utilization widget with FortiAnalyzer 7.4.2 and later

The *SD-WAN Link Utilization* in the *SD-WAN > Monitoring* page is removed for sites working with FortiAnalyzer 7.4.2 and later as the API is deprecated.

Profile changes from previous version

Following are the permission profile changes from FortiPortal 7.2.5.

Profile: Admin

No changes.

Profile: Customer Admin

Permission	Update	Notes
Miscellaneous > Allow CLI Preview	Added	Default: Disabled

Profile: Customer Monitor

Permission	Update	Notes
Miscellaneous > Allow CLI Preview	Added	Default: Disabled

Profile: Web&Video Filters Admin

Permission	Update	Notes
Miscellaneous > Allow CLI Preview	Added	Default: Disabled

FortiPortal 6 features not implemented in FortiPortal 7.2.7

The following features from FortiPortal 6 have not been implemented in FortiPortal 7.2.7:

- Zone/Interface/Dynamic Mapping
- Data Leak Prevention Profile
- Email Filter Profile
- DNS Filter Profile
- Advanced Attributes of LDAP Server

- Radius Server
- Tacacs Server
- Remote User
- DHCP Server Relay
- DHCP Server IPSEC

Scheduled backup password character restrictions

The password for a scheduled backup may contain the following characters:

- Alphanumeric letters (*0-9*, *a-z*, and *A-Z*).
- The following 12 special characters: *! @ # $ % ^ , . ? ~ - _*

Limitation with install preview

Due to a known FortiManager bug (1104703), the improved install preview features are only available with FortiManager 7.4 and 7.6. The traditional install preview approach is still available with earlier FortiManager versions.

Installing FortiPortal 7.2.7

To install FortiPortal 7.2.7:

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 are prompted to change the *admin* user password immediately.
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
   ```

   If needed, configure additional ports (`port2`, `port3`, etc.) in the same manner.
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 are required to change the web login password.

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

Installing on AWS or Azure

To install FortiPortal 7.2.7 on Amazon AWS:

1. Find the FortiPortal Managed Security Service Platform version 7.2.7 published on AWS Marketplace.
2. Deploy the platform according to the standard AWS processes and protocols, as described in the FortiPortal AWS Administration Guide.

To install FortiPortal 7.2.7 on Microsoft Azure:

1. Find the FortiPortal Managed Security Service Platform version 7.2.7 published on Azure Marketplace.
2. Deploy the platform according to the standard Azure processes and protocols, as described in the FortiPortal Azure Administration Guide.

Upgrading FortiPortal

Follow the instructions below to upgrade to FortiPortal 7.2.7.

To improve system security and reduce the chance of exploitation and breach, we recommend that you change the system encryption password after upgrading with the following CLI command:

```
config system encryption
    set password <new-password>
end
```

You can upgrade to 7.2.7 for both AWS and Azure platforms using the same OVA image as KVM and VMware.

If *Site* assertion attribute for remote SAML IdP authenticated customer users is not used (not present in the assertions from the IdP), but you want users to have access to all of their respective sites, the new CLI setting needs to be changed as follows after the upgrade is complete:

```
config system admin setting
    set remote-org-user-all-sites-access enable
end
```

Allow all sites is no longer enabled by default.

Upgrading to 7.2.7

You can upgrade from FortiPortal 7.0.12 or 7.2.6 to 7.2.7 through the FortiPortal dashboard using the *Upgrade Firmware* button and then upload the OVA file for the appropriate version.

Suggested upgrade path:

- 7.0.12 > 7.2.7
- 7.2.6 > 7.2.7

To upgrade to FortiPortal 7.2.7 from 7.0.12 or 7.2.6:

Repeat this upgrade procedure for each version in the upgrade path. Skipping versions is not recommended.

1. Save a backup of your existing FortiPortal system:
   a. Go to *Dashboard*.
   b. In the *System Information* pane, select the *System Backup* icon in *System Configuration* to save a backup file onto the local computer.

   For a scalable cluster, back up the primary node.
2. Download the appropriate OVA file for the version you are updating to. This image is available to download from the Fortinet Customer Service & Support website (https://support.fortinet.com/).
3. In the *System Information* pane, in *Version*, click the *Upload Firmware* icon, click *Choose File* and locate the downloaded OVA file on your local computer.
4. Click *Upload*.

Uploading a firmware image requires sufficient network bandwidth.

When upgrading a scalable cluster, the upgrade may take 10-20 minutes, or longer, depending on server performance.

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

Upgrading AWS and Azure

You can upgrade to 7.2.7 for both AWS and Azure platforms using the same image: FPC_VM64_AWS_AZURE-V7.2.7-build1282-release-Portal.ova.

Follow the standard upgrade procedure described on page Upgrading FortiPortal on page 15.

Resolved Issues

The following issues have been fixed in 7.2.7. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1108512	Incorrect French translations.
1107851	In FortiPortal on Azure, IP address is not displayed in `config system interface` > `show` command.
1107440	In FortiPortal on AWS, IP address is not displayed in `config system interface` > `show` command.

Common Vulnerabilities and Exposures

Visit https://fortiguard.com/psirt for more information.

Bug ID	CVE references
1118238	FortiPortal 7.2.7 is no longer vulnerable to the following CVE reference: CVE-2025-24470.

Known Issues

There are no known issues in FortiPortal 7.2.7.

www.fortinet.com