Release Notes

FortiPortal 7.4.9

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

TABLE OF CONTENTS

Change Log

Date	Change Description
2026-03-12	Initial release.

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 7.4.9, build 2176. 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 7.4.9 on page 12
- Upgrading FortiPortal on page 13
- Known Issues on page 16

What's new

This release contains the following new features and enhancements:

- Browsing LDAP server
- Firewall policy per-column filtering
- FortiClient EMS security posture tags: new rule types
- NTP server authentication
- Policy object tooltips
- Reliable syslog with TCP and TLS
- Sending logs in CEF format
- Support for organization site alias
- Switch VLAN per-device mapping

For more information, see the FortiPortal New Features Guide.

System requirements

FortiPortal version 7.4.9 minimum system requirements:

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

Product Integration and Support

FortiPortal 7.4.9 supports some FortiManager, FortiOS, FortiAnalyzer, FortiAnalyzer BigData, and FortiSandbox versions.

This section contains the following topics:

FortiManager, FortiAnalyzer, FortiAnalyzer BigData, FortiClient EMS, FortiOS, 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 7.4.9 supports the following product versions:

Product	Supported Versions
FortiAnalyzer	7.6.0 to 7.6.6 7.4.0 to 7.4.10 7.2.1 to 7.2.12 7.0.1 to 7.0.3, 7.0.5 to 7.0.16
FortiAnalyzer BigData	7.0.x
FortiManager	7.6.0 to 7.6.6 7.4.0 to 7.4.10 7.2.1 to 7.2.12 7.0.1 to 7.0.16
FortiClient EMS	7.2.3 to 7.2.14 7.4.0 to 7.4.5

Product	Supported Versions
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

FortiPortal 7.4.9 supports the following FortiManager ADOM versions:

Product	Supported FortiManger Versions	Supported ADOM Versions			
		7.6	7.4	7.2	7.0
FortiManager	7.6.0 to 7.6.6	✓	✓	✓	✓
	7.4.0 to 7.4.8		✓	✓	✓
	7.2.1 to 7.2.12			✓	✓
	7.0.1 to 7.0.16				✓

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

Web browser support

The following web browsers are supported:

- Mozilla Firefox version 103 and later
- Google Chrome version 103 and later

> Other browsers and browser versions might also function but are not fully supported in this release.

FortiPortal 7.4.9 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 > 7.4 > 7.4.9*.
6. Download the image files:
   - For KVM, download the latest QCOW2 file:
     FPC_VM64-v7.4.9-build2176-release-portal.qcow2
   - For VMWare, download the latest OVA file:
     FPC_VM64-v7.4.9-build2176-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:

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.

FortiPortal 6 features not implemented in FortiPortal 7.4.9

The following features from FortiPortal 6 have not been implemented in FortiPortal 7.4.9:

- Zone/Interface/Dynamic Mapping
- Data Leak Prevention Profile
- Advanced Attributes of LDAP Server
- Tacacs Server
- DHCP Server IPSEC

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 7.4.9

To install FortiPortal 7.4.9:

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.

Upgrading FortiPortal

Follow the instructions below to upgrade to FortiPortal 7.4.9.

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
```

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.

Suggested upgrade paths

Upgrading from 7.4 branch

- 7.4.8 > 7.4.9

Upgrading from 7.2 branch

- 7.2.8 > 7.4.9

Upgrading to 7.4.9

You can upgrade from the versions noted in Suggested upgrade paths on page 13 through the FortiPortal dashboard using the *Upgrade Firmware* button and then upload the OVA file for the appropriate version.

To upgrade to FortiPortal 7.4.9:

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 FortiPortal, which then reboots.

Upgrading AWS, Azure, and GCP

You can upgrade to 7.4.9 for AWS, Azure, and GCP platforms using the same image: FPC_VM64_AWS_AZURE-GCP-V7.4.9-build2176-release-Portal.ova.

Follow the standard upgrade procedure described on page Upgrading FortiPortal on page 13.

Resolved Issues

The following issues have been fixed in 7.4.9. For inquires about a particular bug, please contact Customer Service & Support.

Bug ID	Description
1181513	GUI language is wrong for SSO users from Germany.
1187304	Notification badge shows incorrect count compared to notification list.
1221739	Generated packet capture files are corrupted.
1228303	SD-WAN *Monitoring* page shows implicit instead of actual SD-WAN rules.
1230498	AP profiles of FortiAP devices are not displayed in AP profiles WiFi configuration.
1230533	Unable to download reports due to "Device array can't be empty" error.
1236261	Logs in *Insights > Logs* do not show all values shown in FortiAnalyzer.
1237879	Updating trunk port on a switch template gives invalid trunk member error when multiple trunks are defined.

Known Issues

The following issues have been identified in FortiPortal 7.4.9. For inquires about a particular bug or to report a bug, please contact Customer Service & Support.

Bug ID	Description
1207145	FortiPortal uses port 443 to check FortiManager health when FortiManager HA cluster uses another port, which leads to *Unhealthy* status.
1228821	Confusing messages in policy installation logs.
1233055	SNMPv3 produces inconsistent values.
1257835	"Create failed" error when adding FortiManager Cloud.
1263253	*Managed Endpoint* page is blank when Root/Computer Workgroup objects are added for FortiClient EMS.

FORTINET

www.fortinet.com