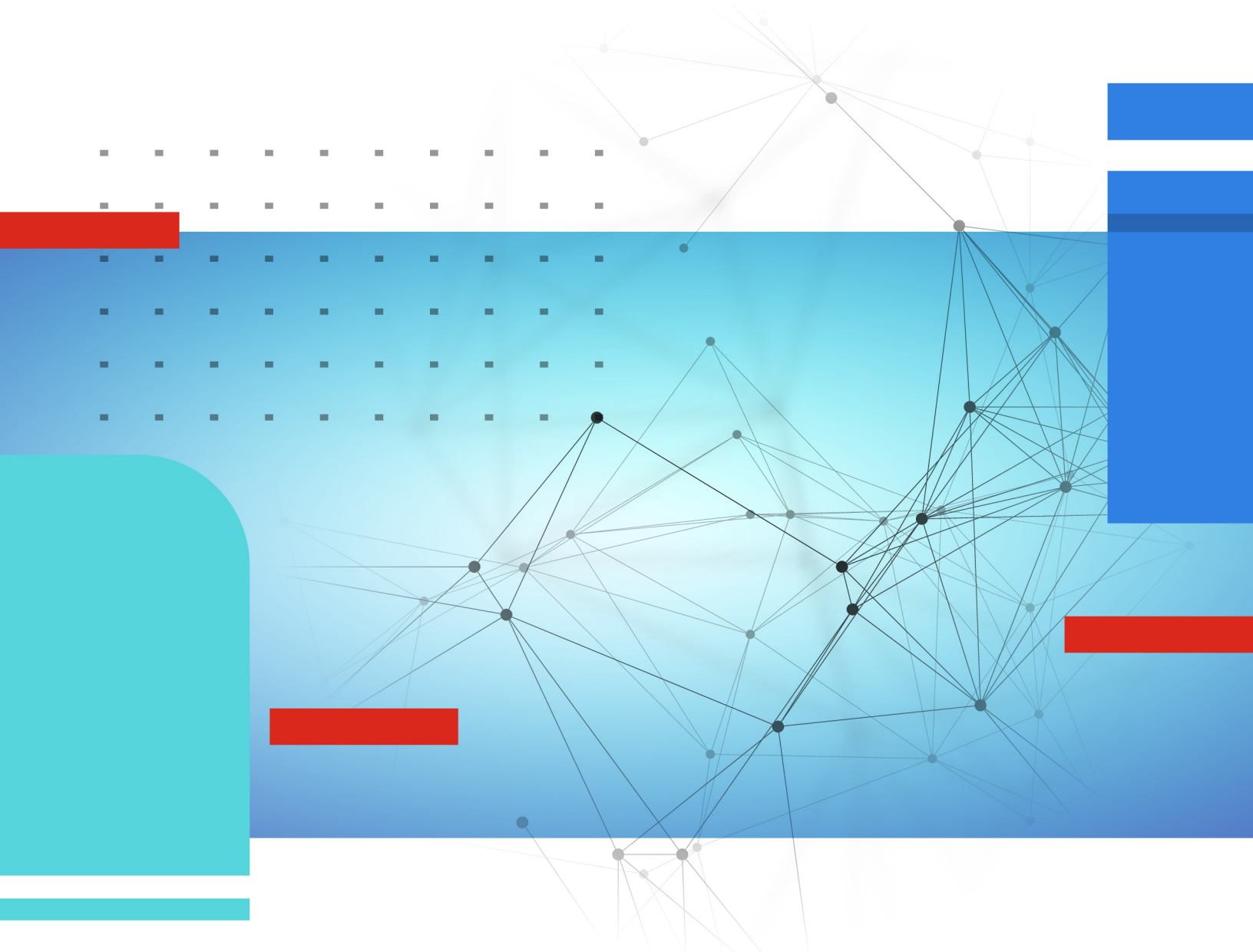
Release Notes

FortiPAM 1.4.3



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

January 8, 2026
FortiPAM 1.4.3 Release Notes
74-143-1178090-20260108

TABLE OF CONTENTS

Change log **4**
FortiPAM 1.4.3 release **5**
Special notices **6**
Do not enable server certificate validation 6
Allow pop up windows on Firefox 6
FortiPAM not compatible with FortiClient EMS 7.4.5 6
What' s new **7**
Upgrade instructions **8**
Upgrade paths 10
Product integration and support **11**
Web browser support 11
Virtualization software support 11
Hardware support 11
FortiPAM-VM **12**
Resolved issues **13**
Common Vulnerabilities and Exposures 14
Configuration capacity for FortiPAM hardware appliances and VM **15**

Change log

Date	Change Description
2025-07-16	Initial release.
2026-01-08	Updated Special notices on page 6.

FortiPAM 1.4.3 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, resolved issues, and known issues for FortiPAM 1.4.3, build 1146.

FortiPAM is a centralized credential management system within the Fortinet Security Fabric solution, designed to protect servers and network devices from cyberattacks.

FortiPAM delivers the following functionalities:

- **Credential vaulting**: Reduces the risk of credential leakage.
- **Privileged account access control**: Limits access to only authorized resources for users.
- **Privileged activity monitoring and recording**: Provides full-session video recordings.

FortiPAM 1.4.3 requires FortiClient 7.4.0 or above to offer the full set of functionalities.

For additional documentation, please visit:

https://docs.fortinet.com/product/fortipam/

Special notices

Do not enable server certificate validation

On the EMS, do not enable the server certificate validation for ZTNA.

Check *Endpoint Profiles > ZTNA Destinations* on the EMS to ensure that the certificate validation is disabled as shown below:

```
<disallow_invalid_server_certificate>0</disallow_invalid_server_certificate>
```

Allow pop up windows on Firefox

When launching web applications on the Firefox browser, allow pop up windows.

FortiPAM not compatible with FortiClient EMS 7.4.5

FortiPAM 1.4.3 is not compatible with FortiClient EMS version 7.4.5 GA.

What' s new

FortiPAM version 1.4.3 is a patch release. There are no new features. See Resolved issues on page 13 for more information.

Upgrade instructions

Back up your configuration before beginning this procedure. While no data loss should occur if the procedures below are correctly followed, it is recommended a full backup is made before proceeding with firmware upgrade.

For information on how to set up automated backup, see the Backup topic in the *FortiPAM Administration Guide* on the Fortinet Docs Library.

Before upgrading from FortiPAM 1.3.0 to 1.4.3, check *Policies* in *Secret Settings*.

If the *SSH Filter* is enabled, disable and reenable with the SSH filter profile.

Firmware upgrade process

Back up your configuration and then upgrade the firmware. Optionally, you can restore your configuration.

Before you can install FortiPAM firmware, you must download the firmware image from FortiCloud, then upload it from your computer to the FortiPAM device. See Upgrading the firmware.

To download the firmware image from FortiCloud:

1. Log into FortiCloud.
2. Go to *Support* > *Downloads*, and select *VM Images* from the dropdown list.
   The *VM Images* page opens.
3. In *Select Product*, select *Other*.
4. Click on the hyperlink that appears.
5. In *Select Product*, select *FortiPAM*.
6. Switch to the *Download* tab and go inside the correct image folder.
7. Click on *HTTPS* for the zip file you intend to download.
   The zip file is downloaded to your management computer.

Image checksums

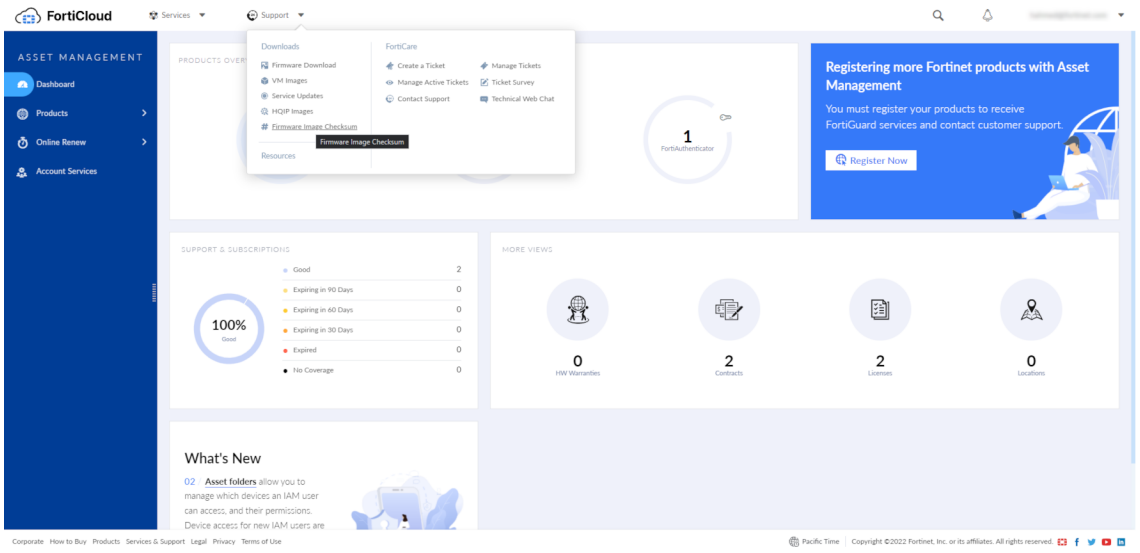
To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available on FortiCloud.

FortiCloud image checksum tool

After logging in to FortiCloud, in the menus at the top, click *Support*, then click *Firmware Image Checksum*.

In the *Image File Name* field, enter the firmware image file name, including its extension, then click *Get Checksum Code* to get the checksum code.



To backup your configuration manually:

1. In the user dropdown, go to *Configuration* > *Backup*.
   The *Backup System Configuration* window opens.
2. Select *Local PC* as the backup option.
3. Enable *Encryption*, enter and confirm password.
4. Click *OK*.
   The backup file is downloaded to your local computer.

To upgrade the firmware:

1. You can only upload a firmware when in maintenance mode.
   From the user dropdown, select *Activate Maintenance Mode* in *System*.
   a. Enter the maximum duration, in minutes.
   b. Enter a reason for activating the maintenance mode.
   c. Click *OK*.

   When in maintenance mode, select *Renew Maintenance Mode* in *System*, enter the new duration and reason and then click *OK* to renew the maintenance mode.

   When in maintenance mode, select *Deactivate Maintenance Mode* in *System* to deactivate the maintenance mode.

2. In the user dropdown, go to *System* > *Firmware*.
   The *Firmware Management* window opens.
3. Go to the *File Upload* tab:
   a. Select *Browse*, then locate the firmware image on your local computer.
   b. Click *Open*.

c. Click *Confirm and Backup Config*.
The firmware image uploads from your local computer to the FortiPAM device, which will then reboot. For a short period of time during this reboot, the FortiPAM device is offline and unavailable.

To restore the configuration manually:

1. You can only restore a configuration when in maintenance mode.
Repeat step 1 from Upgrading the firmware.
2. In the the user dropdown, go to *Configuration > Restore*.
The *Restore System Configuration window* opens.
3. Select *Local PC* as the option to restore from.
4. Select *Upload*:
   a. Locate the backup file on your local computer.
   b. Click *Open*.
   c. In *Password*, enter the encryption password for the backup file.
   d. Click *OK*.

When you restore the configuration from a backup file, any information changed since the backup will be lost. Any active sessions will be ended and must be restarted. You will have to log back in when the system reboots.

Upgrade paths

- From FortiPAM 1.0.x, upgrade to FortiPAM 1.1.x, upgrade to FortiPAM 1.2.0, and then upgrade to FortiPAM 1.4.3.
- From FortiPAM 1.1.x, upgrade to FortiPAM 1.2.0 and then upgrade to FortiPAM 1.4.3.
- From FortiPAM 1.2.0 upgrade to FortiPAM 1.4.3.
- From FortiPAM 1.3.0 upgrade to FortiPAM 1.4.3.

Product integration and support

FortiPAM 1.4.3 supports the following:

- Web browser support on page 11
- Virtualization software support on page 11
- Hardware support on page 11

Web browser support

FortiPAM version 1.4.3 supports the following web browsers:

- Microsoft Edge version 126
- Mozilla Firefox version 114

  Note: Mozilla Firefox is supported with some limitations.
- Google Chrome version 126

Other web browsers may function correctly but are not supported by Fortinet.

Virtualization software support

FortiPAM version 1.4.3 supports:

- VMware ESXi 6.5 and above
- Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0
- Microsoft Hyper-V
- Microsoft Azure
- GCP (Google Cloud Platform)
- AWS (Amazon Web Services)

Hardware support

FortiPAM 1.4.3 supports:

- FortiPAM 1000G
- FortiPAM 3000G

FortiPAM-VM

For information about FortiPAM-VM deployments and system requirements, see the FortiPAM virtualization Admin Guides on the Fortinet Docs Library.

Resolved issues

The resolved issues listed below may not list every bug that has been corrected with this release. For inquiries about a particular bug, please contact Technical Support within the FortiCare portal.

Secret/Launch

Bug ID	Description
1140540	Watchdog memory error in the password-change daemon.

User/Group

Bug ID	Description
1078236	Add API user to user group issue.

Others

Bug ID	Description
1112308, 1117737	Heap buffer overflow in websocket.
1120661	Integer Overflow on SSL-VPN VNC bookmark.
1121038	Weak authentication in WAD/GUI.
1092965	Format string vulnerability in FortiToken import.

Common Vulnerabilities and Exposures

Bug ID	CVE references
1130288	FortiPAM is no longer vulnerable to the following CVE-Reference(s): • CVE-2025-26466 • CVE-2025-26465
1092961	FortiPAM is no longer vulnerable to the following CVE-Reference(s): • CVE-2024-45324

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

Configuration capacity for FortiPAM hardware appliances and VM

The following table lists the maximum number of configuration objects per FortiPAM appliance that can be added to the configuration database for different FortiPAM hardware or VM models.

Features	FortiPAM 1000G	FortiPAM 3000G	FortiPAM-VM
Secret	50000	100000	100000
Target	5000	10000	10000
Folder	2000	6000	6000
User	1000	3000	3000
User group	2000	5000	5000
Request	5000	10000	10000

www.fortinet.com

Copyright© 2026 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 Chief Legal Officer, 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.