Release Notes

FortiPAM 1.7.1

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

November 19, 2025
FortiPAM 1.7.1 Release Notes
74-171-1215070-20251119

TABLE OF CONTENTS

Change log

Date	Change Description
2025-10-27	Initial release.
2025-11-19	Updated Upgrade instructions on page 9.

FortiPAM 1.7.1 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, resolved issues, and known issues for FortiPAM 1.7.1, build 1467.

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 1.7.1 requires FortiClient 7.4.3 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.

HA and DR essential

Setting up High Availability (HA) and Disaster Recovery (DR) are essential for system protection. This is important in case of power outages or other unexpected events.

With the introduction of the new floating license feature, HA and DR setups are affordable and flexible.

Web proxy CA certificate

When launching public websites, FortiPAM uses the selected CA certificate to re-sign the public websites.

When launching private websites, FortiPAM will use untrusted CA to re-sign the private websites.

Client software

Before upgrading to FortiPAM 1.7.1, check if there is a software in *Secret Settings > Client Software*. If yes, reduce the *Video Storage Limit* / *File Storage Limit* (in the *Advanced* tab in *System > Settings*) to allow uploading software from a USB disk (`/data2/pkg`) to the video disk.

After upgrading to FortiPAM 1.7.1, adjust the storage limit in the *Advanced* tab in *System > Settings*.

What's new

FortiPAM version 1.7.1 is a patch release. There are no new features.

See Resolved issues on page 15 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.

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

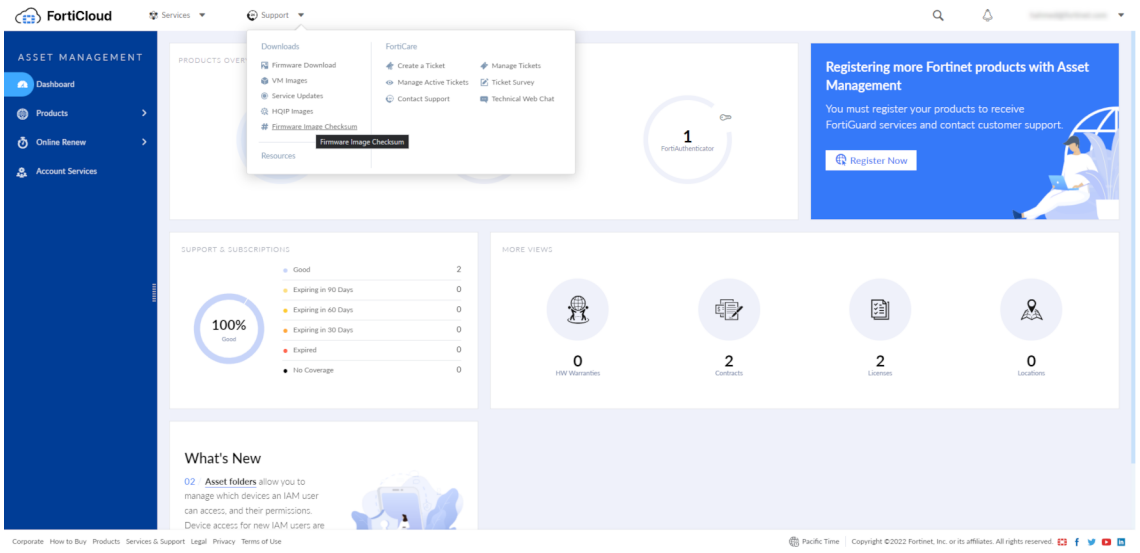
To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

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.

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.

Once the configuration is restored, select *Deactivate Maintenance Mode* in *System* to deactivate the maintenance mode.

Upgrade paths

- From FortiPAM 1.5.x, upgrade to FortiPAM 1.7.1.
- From FortiPAM 1.6.x, upgrade to FortiPAM 1.7.1.

If the web proxy CA certificate has been configured on a previous version, e.g., 1.5.x or 1.4.x, the CA certificate is still in the FortiPAM configuration after the upgrade. However, the CA certificate is not selected for web proxy.

Go to the interface being used in *Network > Interfaces* and select the CA certificate from the *CA certificate* dropdown in *Explicit Web Proxy*.

Product integration and support

FortiPAM 1.7.1 supports the following:

Web browser support

FortiPAM version 1.7.1 supports the following web browsers:

- Microsoft Edge version 135
- Mozilla Firefox version 137

  Note: Mozilla Firefox is supported with some limitations.

- Google Chrome version 135

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

Virtualization software support

FortiPAM version 1.7.1 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)
- Alibaba Cloud
- Proxmox
- Nutanix

Hardware support

FortiPAM 1.7.1 supports:

- FortiPAM 1000G
- FortiPAM 3000G

Language support

The FortiPAM GUI can be displayed in the following languages:

- English
- French
- Spanish
- German
- Portuguese
- Japanese
- Chinese (Simplified)
- Chinese (Traditional)
- Korean
- Italian
- Arabic

For more information on changing the language in the GUI, see the FortiPAM Administration Guide.

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
1094925	Launching sessions dropping over SSL VPN - `FortiPAM freezes periodically.`
1195492	Displays the wrong approver in the log for email link approval.
1195003	Error- `Cannot set Allow View For Web Launcher Cred Replacement`
1212330	`LIST` secret permission causes the secret page to not load.
1211000	Secret approvals unable to send emails when using approval groups rather than users.
1210740	Unable to change the password changer in a new template in *Secret Settings*.
1214261	Approval learning failed on rename.

User/Group

Bug ID	Description
1157030	After upgrading to 1.6.0, SAML is not working when accessing FortiPAM from FQDN.
1193170	SAML SSO login looping redirects indefinitely.
1216736	Trust host not learned for API user.

System/Log

Bug ID	Description
1184705	Video upload timed out randomly causing session disconnections (FortiClient-based).

Others

Bug ID	Description
1184604	FortiPAM 3000G disks randomly turn to unavailable.
1208346	Lost connectivity to the FortiPAM GUI WAD crashes.
1167792	Neutrino UI inconsistency - FortiPAM login page.
1207203	Path traversal in CLI.
1207243	Path traversal in FortiCron.
1209421	Security Best Practice: CLI `libedit` code has potential buffer overlow in `term_alloc`.
1189650	Require configuring migration tool to migrate FortiSRA to FortiPAM.

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	3000	3000	3000
User group	2000	5000	5000
Request	5000	10000	10000
Gateway	256	256	256

www.fortinet.com