Release Notes

FortiPAM 1.8.3

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

June 8, 2026
FortiPAM 1.8.3 Release Notes
74-183-1301468-20260608

TABLE OF CONTENTS

Change log

Date	Change Description
2026-06-08	Initial release.

FortiPAM 1.8.3 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, resolved issues, and known issues for FortiPAM 1.8.3, build 1702.

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 1.8.3 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

If "server certificate validation" of FortiClient is enabled by EMS

If server certificate validation is enabled in FortiClient by EMS, make sure that the certificate in the FortiPAM GUI can be validated by FortiClient.

Use one of the following two options:

- **Option 1**: The FortiPAM GUI certificate is signed by the public certificate authority (CA).
- **Option 2**: The CA certificate for the FortiPAM GUI is pushed to FortiClient by the EMS, or is manually installed in the Windows certificate store.

To configure the FortiPAM GUI certificate, see Editing an interface in the latest *FortiPAM Administration Guide*.

To verify whether server certificate validation is enabled in FortiClient, go to *Endpoint Profiles > ZTNA Destinations* and check the following setting:

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

A value of `0` indicates that server certificate validation is disabled.

Allow pop up windows on Firefox

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

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 1.8.3, 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 1.8.3, adjust the storage limit in the *Advanced* tab in *System > Settings*.

What's new

FortiPAM version 1.8.3 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

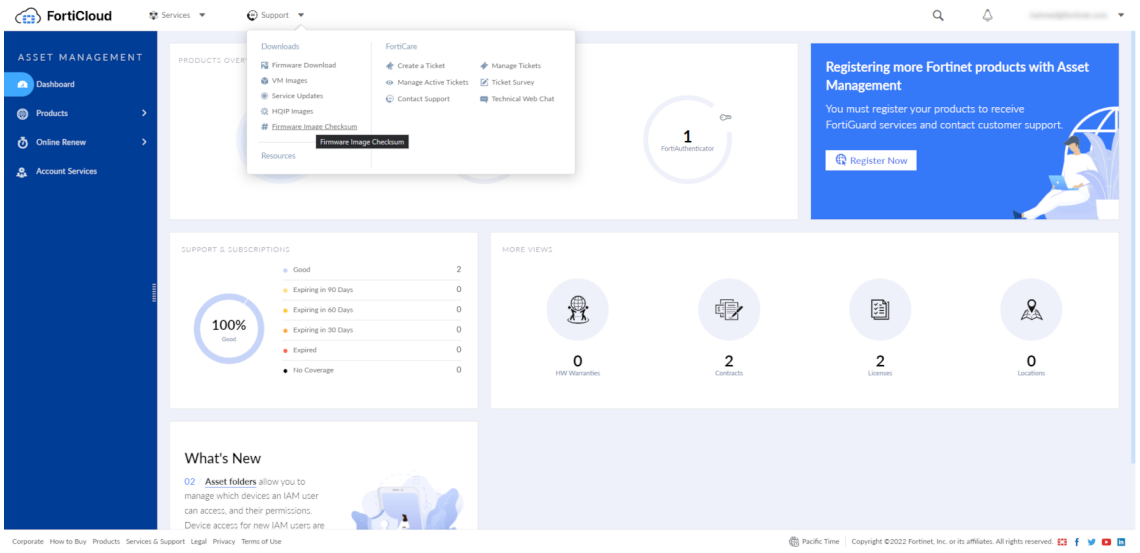
To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

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

Use the following table to verify the list of compatible upgrade paths:

From	To
1.6.x	1.8.3
1.7.x	1.8.3
1.8.0	1.8.3

Product integration and support

FortiPAM 1.8.3 supports the following:

Web browser support

FortiPAM version 1.8.3 supports the following web browsers:

Google Chrome version 135
Microsoft Edge version 135
Mozilla Firefox version 137
 Mozilla Firefox is supported with some limitations.

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

Virtualization software support

FortiPAM version 1.8.3 supports:

Alibaba Cloud
AWS (Amazon Web Services)
GCP (Google Cloud Platform)
Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0
Microsoft Azure

Microsoft Hyper-V
Nutanix
OCI (Oracle Cloud Infrastructure)
Proxmox
VMware ESXi 6.5 and above

Hardware support

FortiPAM 1.8.3 supports the following FortiPAM hardware models:

FortiPAM 1000G
FortiPAM 1100G
FortiPAM 3000G

Language support

The FortiPAM GUI can be displayed in the following languages:

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

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
1293456	Approved Email template received by the requestor is misaligned.
1287429	Cannot add 32nd secret as favorite.
1294312	Disable auto match/create for Targets with specific role assigned.
1276453	Domain field does not accept domains starting with a number.
1273260	Secret Password Changer fails for Azure AD web-api password changer.
1274827	API return code when querying target might be incorrect.
1270351	Session not ending when secret is checked in.

User/Group

Bug ID	Description
1055670	Forced to use "Message-Authenticator" in RADIUS message.

System/Log

Bug ID	Description
1273123	Issue with Expanding Disk Space for Video Recordings on FortiPAM in AWS.
1263843	Updating/deleting the EMS tag causes HA to go out of sync.
1267271	Incorrect disk usage calculation sends FortiPAM into conserve mode.

Others

Bug ID	Description
1281645	Add more video module traces.

Bug ID	Description
1279383	Fix buffer overflow.
1275950	Wrong API return code for `/api/v2/utility/id`.
1296451	Downgrade from build 1747 to build 1698 causes GUI access failure.

Migration from FortiSRA to FortiPAM

In version 1.8.0, FortiSRA is merged into FortiPAM.

Starting FortiPAM 1.8.0:

1. The previous FortiSRA default administrator will have the full Super Administrator role, including the ability to launch secrets.
2. With `SKU-591`, an extra seat is added for free.
   For example, when the purchased license seat quantity is 20, then 21 users can be enabled.
   For HA, if a node has 10 licensed seats and the other has 5 users, the primary node can have 16 users enabled.

Upgrade path for FortiSRA:

1. Upgrade FortiSRA from 1.6.x to 1.7.2 using the FortiSRA image.
2. Upgrade FortiSRA from 1.7.2 to FortiPAM 1.8.0 using the FortiPAM 1.8.0 image.

After migration from FortiSRA to FortiPAM, the original FortiSRA administrator becomes a regular administrator on FortiPAM with the ability to create/edit/launch secrets.
This is a free administrator account.

After migration from FortiSRA to FortiPAM, native launchers are automatically created and added to the default templates.
If you do not want to display the native launchers, remove them from the following default templates:

- *Unix Account (SSH Password)*, *VNC Server*, *FortiGate/FortiOS (SSH Key)*,*FortiGate/FortiOS (Web)*, *Machine*, *Windows Domain Account*, etc.

After migration from FortiSRA to FortiPAM, the GUI can report the `Configuration can contain errors` warning.
Run:

```
diag debug config-error-log read
```

Output:

```
"end" @ global.system.replacemsg.auth.auth-sra-login-page:failed command (error -
56)
 "end" @ global.system.replacemsg.auth.auth-sra-token-page:failed command (error -
56)
 "end" @ global.system.replacemsg.auth.auth-sra-passchg-page:failed command (error
-56)
```

The above output is harmless to your system.
Run the following command to clear the output:

```
diag debug config-error-log clear
```

After you migrate from FortiSRA to FortiPAM, you can no longer downgrade back to FortiSRA.

Ensure that you create a snapshot of your FortiSRA before the migration to FortiPAM.

If the FortiSRA license is expired, FortiSRA license may not be available.

If using a new FortiPAM license to replace an expired FortiSRA license, the following must be performed:

Fabric connectors (EMS, FortiAnalyzer)	Reconfigure EMS and FortiAnalyzer to accept FortiPAM connection request
Users with local mobile 2FA	Disable/re-enable 2FA
Users with FortiToken Cloud 2FA	Disable/re-enable 2FA

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 1100G	FortiPAM 3000G	FortiPAM-VM
Secret	50000	50000	100000	100000
Target	5000	5000	10000	10000
Folder	2000	2000	6000	6000
User	3000	3000	3000	3000
User group	2000	2000	5000	5000
Request	5000	5000	10000	10000
Gateway	256	256	256	256

www.fortinet.com