Release Notes

FortiPAM 1.3.0

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

FORTINET®

August 9, 2024
FortiPAM 1.3.0 Release Notes
74-130-1014519-20240809

TABLE OF CONTENTS

Change log

Date	Change Description
2024-04-01	Initial release.
2024-04-02	Added bug 1007952 to Known issues on page 21.
2024-05-31	Updated Upgrade instructions on page 13.
2024-06-13	Added bug 998731 to Resolved issues on page 18.
2024-06-14	Added bug 1038568 to Known issues on page 21.
2024-08-07	Added bug 1030706 to Known issues on page 21.
2024-08-09	Updated description for bug 1030706 in Known issues on page 21.

FortiPAM 1.3.0 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, resolved issues, and known issues for FortiPAM 1.3.0, build 0862.

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 1.3.0 requires FortiClient 7.2.3 or above to offer the full set of functionalities.

For additional documentation, please visit:

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

Special notices

Disable live recording before downgrading to 1.1.x

Before downgrading from FortiPAM version 1.2.x to 1.1.x, disable *Live Recording* in the *Advanced* tab in *System > Settings*. Otherwise, you cannot replay videos on FortiPAM 1.1.x.

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>
```

Firefox extension not included in the installation package

The FortiPAM installation package does not include the *Fortinet Privileged Access Agent* for the Firefox browser.

You can download it on https://www.fortinet.com/support/product-downloads.

Allow pop up windows on Firefox

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

What' s new

FortiPAM version 1.3.0 includes the following enhancements:

985657- FortiPAM distributed architecture

FortiPAM now supports network gateway for distributed target deployment.

FortiPAM allows configuring a gateway, e.g., a FortiPAM, a FortiGate, or a FortiProxy device, when a target is not reachable directly from FortiPAM to proxy the connection to the target.

You can now add a gateway when configuring a target.

You can also add the gateway to a secret.

968457- Display 2FA status

FortiPAM now displays the 2FA status for a user in the *Two-factor Authentication* column in *User Management* > *User List*.

913565, 927433- Automated remote user provisioning

Before FortiPAM 1.3.0, all FortiPAM users were created manually by the administrator. Starting FortiPAM 1.3.0, FortiPAM allows you to automatically sync up users based on group membership without limiting the authentication protocol (LDAP, RADIUS, or SAML).

You can define a remote user auto provision rule in *User Management* > *Auto Provision Rules*.

Based on the predefined auto provision rules, remote users can be auto provisioned upon their first successful login without requiring the manual creation of a user in the system prior to login.

The auto provision rule includes information about the remote user group and users' role (access profile) on auto provision. The type of role depends on the user's group membership.

Based on the group, FortiPAM decides if the user can log in to FortiPAM and the type of permission the user is granted. Once the user logs in, the user is automatically created and listed in *User Management* > *User List*.

A new *Created By* column in *User List* tells you if the user was manually created or auto provisioned.

925187- Display ZTNA launch control inheritance settings for folders

When configuring permissions for a subfolder, in the *Permission* tab, with *Inherit ZTNA Control* enabled, ZTNA control settings from the parent folder are displayed.

883603- vTPM support for FortiPAM on GCP

FortiPAM supports vTPM on GCP.

961527- Logs extracted as JSON and CSV file

FortiPAM allows you to extract log files in JSON and CSV formats in addition to exporting logs as text files.

A new *Export* dropdown is available in the following locations in *Log & Report*:

- All the tabs in *Secret*
- The *Details* tab in *Events*
- *ZTNA* tab
- *SSH* tab
- *Antivirus* tab
- *Data Leak Prevention* tab

913157, 959127- New *Web Telnet* launcher

A new *Web Telnet* secret launcher is available.

957808- Password only viewable to the user checking out a secret

To ensure accountability, a secret password is only visible to the user with *Edit* or *Owner* permission for the secret the user is checking out.

Note that this is only valid when *Requires Checkout* is enabled in the *Secret Setting* pane when configuring the secret.

839929- Import remote LDAP users

To conveniently import LDAP users in bulk on FortiPAM, a new *Import* option is available in *User Management* > *User List*.

878661- New remote server option when creating a remote user

When configuring a remote user, you are no more required to select a remote user group in the *User Type* pane. Instead, if the remote user does not belong to a remote user group, you can select the remote server where the user resides in the *Choose a Remote Group where these users can be found or a Remote Server* dropdown in the *User Type* pane.

963099- Customizing replacement messages

A new *Replacement Messages* tab in *System* to customize replacement messages for FortiPAM.

975901, 963740- User deletion enhancements

You can delete users directly without deleting the references first.

If the deleted user alone owns resources not in the personal folder, e.g., secrets/folders in the public folder, targets, templates, user groups, or approved requests, etc., you can select a user who will own the resources once the user owning the resource is deleted.

A sponsor admin can delete members within its sponsored group.

964873- Approver minimum permission

A new *Minimum Permission* dropdown when creating an approval profile in *Secret Settings* > *Approval Profile*.

You can set up the minimum secret permission required by the approver to view/approve/deny the secret request.

920066- Approver group email notification for access requests

A new *Remote Group Email* option when creating an approval profile in *Secret Settings* > *Approval Profile*.

The option appears when you select at least one remote user group in *Approver Groups* when creating or editing an approval profile in *Secret Settings* > *Approval Profile*.

Enabling *Remote Group Email* ensures that members of an approver group receive email notification when an access request is sent for a secret where *Requires Approval to Launch Secret* is enabled and an approval profile is selected with at least one remote user group as an approver.

When *Remote Group Email* is enabled, a new *Trust Time* field appears. The *Trust Time* field controls how frequently the remote user needs to log in to FortiPAM to receive the approver email notification.

For example, when *Trust Time* is `5`, a remote user belonging to the remote user group selected in *Approver Groups* must have logged in to FortiPAM at least once within five days from the access request creation time to receive the approver email notification.

993481- Sync sender name across all emails

A new *Sender* field in the *Email Service* pane in *System* > *Settings*.

The *Sender* email address is the email address used to send emails.

942734- Log and video disk encryption

FortiPAM supports disk encryption to protect logs and videos.

A new *Disk Encryption* option in *Log & Report* > *Log Settings*.

964619- Immediate secret access on approval

When creating a secret access request in *Secrets* > *My Requests List* or directly from a secret in *Secrets* > *Secret List*, you can enable the *Start Upon Approval* option.

Enabling the *Start Upon Approval* option ensures that you can launch the secret once it is approved.

When *Start Upon Approval* is enabled, you see a new *Duration* option instead of the *Request Duration* option.

In the *Duration* option, specify the duration of time you need the secret access for (in minutes).

Note that the approver can still override when you get access to the secret and the duration of time you have access to the secret.

954620, 997420- Adjust the timezone for the secret access requestor and approver

When creating a secret access request in *Secrets* > *My Request List*, FortiPAM shows the local time of the requestor in the *New secret request* window.

When approving/denying a secret access request in *Secrets* > *Approval List*, time according to the approver's timezone is displayed by default in the *Approving secret request* window.

By clicking the *Enable Requestor Timezone* option, you can enable the requestor's timezone and display the requestor's local time in the *Approving secret request* window.

New *Enable/Disable Requestor Timezone* option and *Timezone* column in *Secrets* > *Approval List*.

877089- Secret list displays secret creation time

Secret List in *Secrets* includes a new *Creation Time* column that displays when a secret was created.

955024- Customize Email template for secret request

FortiPAM allows you to customize email templates for secret requests in *Secret Settings* > *Approval Email Template*.

When creating a new approval profile in *Secret Settings* > *Approval Profile*, you can assign a customized email template to the approval profile using the new *Customized Email Template* option.

950516- RDP auto token for FortiAuthenticator

FortiPAM supports RDP 2FA auto delivery when the FortiAuthenticator agent is running on remote Windows.

A new *RDP Auto TOTP* option available when *RDP Service* is enabled and the *RDP Security Level* is *TLS* in the *Service Setting* tab when creating or editing a secret in *Secrets* > *Secret List*.

A new *RDP Auto TOTP* option available when the *RDP Security Level* is *TLS* when creating or editing a secret policy in *Secret Settings* > *Policies*.

840054- Auto discovery of secrets

FortiPAM scans an environment to find accounts and other associated resources. Once the accounts and the resources are found, they can be automatically imported to FortiPAM for centralized management.

A new *Secret Discovery* option in the *Secret* tab when creating or editing a *Role* in *User Management* > *Role*.

893740- Increased secret capacity

FortiPAM can now support setting up a maximum of 50000 secrets in FortiPAM 1000G and up to 100000 in FortiPAM 3000G and the VM platform.

919801- Updating service account credentials

If a service running on a machine relies on a credential managed by FortiPAM, dependency updater feature offers the ability to update the service credential immediately after FortiPAM changes the credential. FortiPAM ensures that the service does not fail during authentication.

A new *Dependency Updater* tab in *Secret Settings*.

A new *Dependency* tab when creating or editing a secret.

It allows you to assign the secret to a target where the service defined in the selected dependency updater runs.

987061- Updated secret logs and active sessions GUI

In *Log & Report* > *Secret*:

- A new *Service Account* page is available where you can view logs related to service accounts.
- In the *Secrets* and the *Password Changers* pages, the following new columns are available:
  - *Secret Address*
  - *Gateway*

  Note that what the *Destination IP* column represents has changed. It is the next hop IP address. If the next hop is FortiPAM, this is the IP address of FortiPAM.
  - If the next hop is the actual target server, this is the IP address of the actual target server.
  - If the next hop is a gateway, this is the IP address of the gateway.

In *Monitoring* > *Active Sessions*:

- The following new columns are available:
  - *Gateway*
  - *Gateway Port*
  - *Gateway Name*

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.

When upgrading a FortiPAM instance, use the following CLI command to enable synchronizing the virtual IP address to the IP address of the external interface:

```
Example

 config firewall vip
  set intf-ip-sync enable
  set extintf "port1" #The interface connected to the source network
that receives the packets forwarded to the destination network.
 end
```

When installing a new FortiPAM instance, the synchronization happens automatically.

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

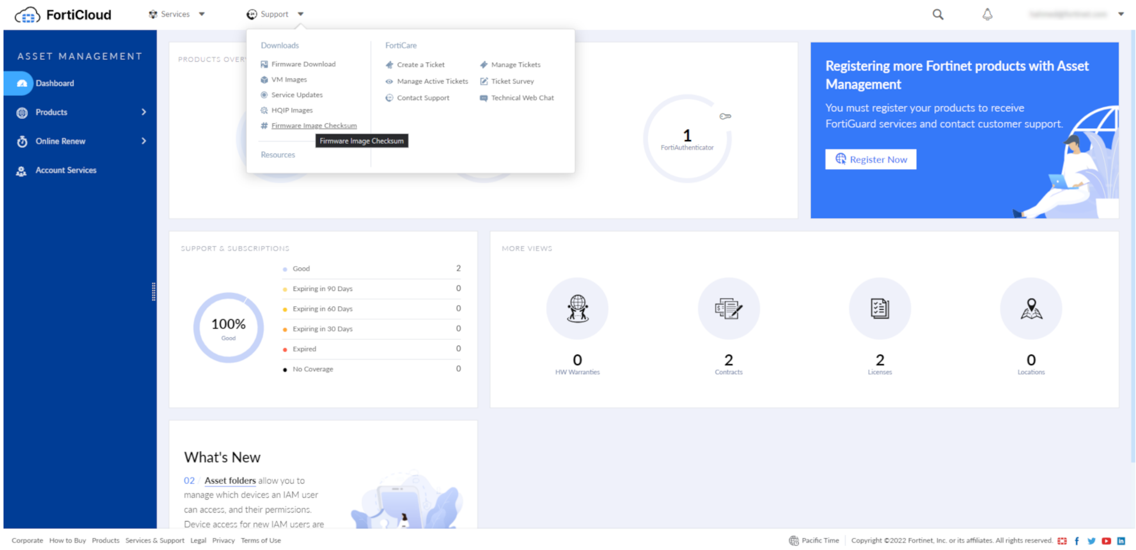
To verify the integrity of the firmware file, use a checksum tool to compute the firmware file’s MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

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 dropdrown, 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 1.1.2 and then upgrade to FortiPAM 1.3.0.
- From FortiPAM 1.1.x, you can directly upgrade to FortiPAM 1.3.0.
- From FortiPAM 1.2.0 to FortiPAM 1.3.0.

Product integration and support

FortiPAM 1.3.0 supports the following:

- Web browser support on page 16
- Virtualization software support on page 16
- Hardware support on page 16

Web browser support

FortiPAM version 1.3.0 supports the following web browsers:

- Microsoft Edge version 114
- Mozilla Firefox version 114

  Note: Mozilla Firefox is supported with some limitations.

- Google Chrome version 114

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

Virtualization software support

FortiPAM version 1.3.0 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 1.3.0 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.

Bug ID	Description
1014408	The web proxy launcher fails for certain passwords.
926156	Unable to move a folder in root to another folder under root folder in the GUI.
969403	When creating a target, the default *Target Only* template is not in the GUI.
988483	Selecting *Cancel* when editing proxy addreses returns a *Page Cannot be displayed* error.
998234	GUI error while canceling configuring some objects.
935427	TOTP auto delivery does not work during SSH launching to FortiProduct when 2FA is enabled.
877089	Added *Creation Time* on both CMDB of secrete database and in *Secret List* in the GUI.
967064	When manually modifying a secret credential, the *Credential History* should log it.
1010189	When *Force Proxy* is enabled in *Role*, it should save as *force proxy* instead of *allow-non-proxy*.
806403	Adding secret last access time and last hearbeat time/state in the list view.
986168	Only first entry shows up in *Secret Target* permission.
973188	Occasionally, unable to edit the secret configuration.
966357	Support non-PUSH based FortiToken 2FA
993603	ForitClient SSLVPN unable to make connection in the proxy-mode.
997420	Hide Time Display Setting - System.
798599	GUI displays last password change and verification status for a secret.
943210	Remote user (LDAP) login via SSH terminal not working in FortiPAM.
968457	GUI needs to show 2FA information in the *User Management* > *User List*.
925187	Inherited folder/secret ZTNA control should show up in details.
1005439	SAML- Enabling SP certificate and then disabling SP certificate on SP setting does not take effect without reboot.
1002390	Web RDP/VNC tab title typo when secret name has blank spaces.
952937	SSH filter does not work in WinSCP.

Bug ID	Description
938575	WAD session list cannot list two video sessions launching from same browser because the browser uses the same TCP connection.
930981	No group schedule option in the dropdown when editing a user schedule.
970915	DLP file size blocking associated with `.zip` file does not apply to WinSCP.
966933	Sponsor Admin unable view logs from FortiAnalyzer on FortiPAM,
981548	Sometimes, the password changer is triggered twice on a one day schedule.
961265	With *Web Proxy* enabled, failed to launch the web account secret which is using a non-standard `https` port, e.g., `8443`.
982710	*Launch Secret* not available on the secret page when disabling *Inherit Permission* on Firefox browser.
1002374	Authentication with 2FA failed when the remote server configured.
990692	Enhancement on the SSH filter log.
883599	FortiManager chaining.
993481	SMTP issues with Microsoft Office 365.
1004725	FortiPAM GUI: `Authorization failed: insufficient permissions!` for email 2FA LDAP user.
1015365	Add web proxy FQDN to VDOM exception.

Common Vulnerabilities and Exposures

Bug ID	CVE references
998731	FortiPAM 1.3.0 is no longer vulnerable to the following CVE-Reference(s): • CVE-2024-26010

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

Known issues

This section lists the known issues of this release, but is not a complete list. For inquiries about a particular bug, please contact Technical Support within the FortiCare portal.

Bug ID	Description
1002990	Web Account not responding after being idle for 10 minutes if recording is disabled.
1009075	Failed to launch Azure as the password cannot be filled. **Workaround**: **1.** Click *Submit*. **2.** Click the input box credential filler again. **3.** Click *Submit* again.
1014549	WebSSH TOTP for FortiProduct.
1003972	Fortinet Privileged Access Agent- MobaXterm Launch failure.
970315	Support importing secret target and secret from files.
1001231	The FortiPAM installation package does not include the *Fortinet Privileged Access Agent* for the Firefox browser. You can download it on https://www.fortinet.com/support/product-downloads.
970973	Soft RAID-10 is not supported.
969964	FortiAnalyzer log: Secret logs are not ordered by *Time* or *Token Id*.
971485	A disabled TOTP key could not be recovered from GUI except by providing the same shared key.
978393	Support AWS root and IAM users on *Web Proxy*.
970329	The standalone FortiClient requires the PC to reboot to start up after shutdown.
1007952	After changing the *Remote Group/Server* option when editing a SAML user from a SAML server to a SAML group, the *Force SAML Login* option is disabled.
1038568	Blank screen when live streaming or replaying recording using Web VNC on Mac OS.
1030706	If a secret is moved to a folder with policy that has ssh-filter/av-scan/dlp enabled, the resulting secret may not inherit from the folder correctly. If the configuration is not set correctly, try to make a backup of the secret before reboot to prevent loss.

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© 2024 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.