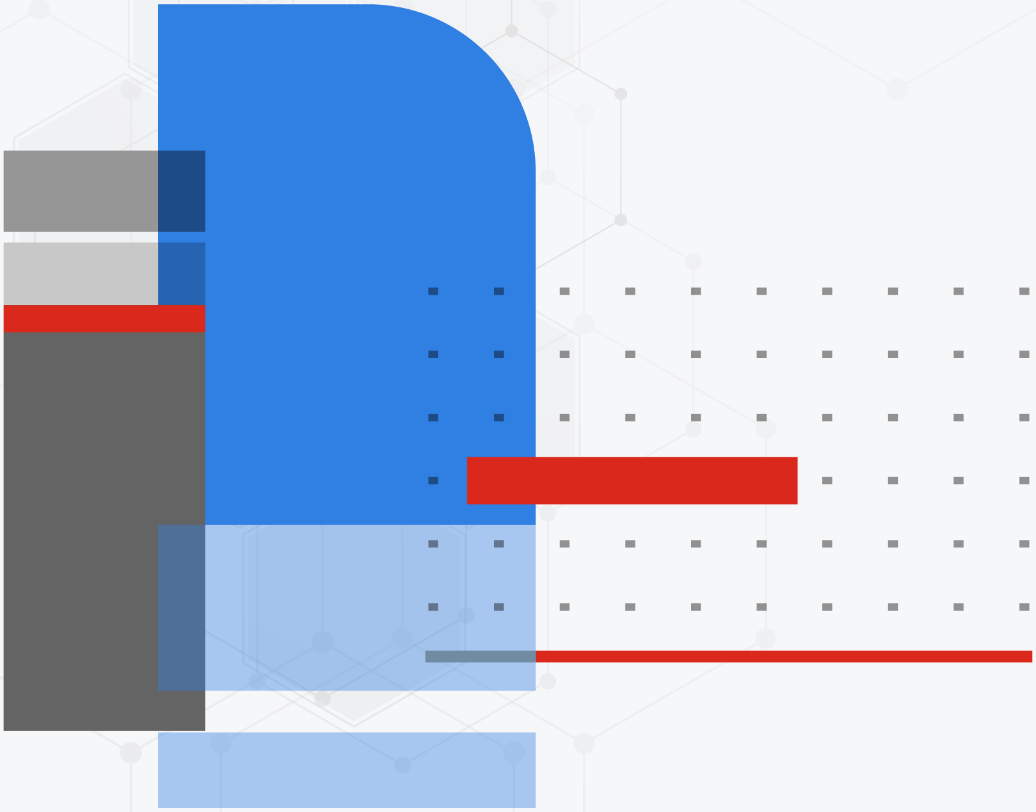
Release Notes

FortiPAM 1.2.0



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

April 18, 2024
FortiPAM 1.2.0 Release Notes
74-120-964688-20240418

TABLE OF CONTENTS

Change log

Date	Change Description
2023-12-15	Initial release.
2023-12-20	Updated Special notices on page 7.
2024-01-02	• Removed bug 965782 from Known issues on page 22. • Added bug 985832 to Known issues on page 22.
2024-01-03	Added bug 984506 to Known issues on page 22.
2024-01-04	Updated Special notices on page 7.
2024-01-05	Added bug 986168 to Known issues on page 22.
2024-01-08	Updated Special notices on page 7.
2024-02-16	Updated Configuration capacity for FortiPAM hardware appliances and VM on page 23.
2024-04-04	Updated What' s new on page 8.
2024-04-18	Updated What' s new on page 8.

FortiPAM 1.2.0 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, resolved issues, and known issues for FortiPAM 1.2.0, build 0697.

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 1.2.0 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>
```

Upgrading issue with standalone FortiClient

Native launchers fail after upgrading the standalone FortiClient from a previous version.

Workaround: You must uninstall the previous standalone version of FortiClient, reboot, install the standalone FortiClient 7.2.3, and then reboot again.

What' s new

FortiPAM version 1.2.0 includes the following enhancements:

883168- Display secret last launch time

FortiPAM displays the secret last launch time in *Secret* > *Secret List* in the new *Last Launch Time* column.

934741, 925399, 913558- Sponsored groups

Super administrators can now create sponsored groups in *User Management* > *Sponsored Groups*.

In addition, there is now a sponsor admin role. Sponsor admins are assigned to a sponsored group, and they can only access logs for their specific secrets. This includes creating, editing, and disabling users within their assigned sponsored group. The super administrator defines the maximum number of users for each sponsored group.

Multiple sponsor admins can be assigned to a single sponsored group.

893189, 954666- Secret targets now created separately and must include a classification tag

Secret targets are now created separately from secrets and secret templates. Each target can be assigned to multiple secrets, as needed.

Classification tags must be added to each target, classifying the target according to your needs.

When creating or editing a role in *User Management* > *Role*:

- You can now enable/disable editing secret targets in *Secrets* using the *Edit Secret Target* option in the *Secret* tab.
- You can now enable/disable editing the *Classification Tag* page in *Secret Settings* using the *Edit Classification Tag* option in the *Secret* tab.

890566- Regular expressions supported for the expect string in password changing procedures

When creating or editing a password changing procedure, set the *Type* to *Expect*. You can now select the method to interpret the expect string.

For the *Interpretation*, you can select one of the following:

- *Plain*: Interpret the expect string as a plain command.
- *Regex*: Interpret the expect string as a regular expression. For example, if the response is "`Current password:`", then all of "`Current`", "`password`", "`rent`" will succeed to match.

923627- New AntiVirus and DLP profile control in Role

When creating or editing a role in *User Management* > *Role*:

- You can now set access levels for the *AntiVirus* page in *Secret Settings* and the *AntiVirus* settings in the *ForitGuard License* page in *System* using the *Antivirus* option in the *System & Network* tab.
- You can also set access levels for the *Data Leak Prevention* and the *DLP File Pattern* pages in *Secret Settings* using the *Data Leak Prevention* option in the *System & Network* tab.

897591, 934000, 967356, 796667- New launchers and template supported

FortiPAM now includes the following four new secret launchers:

- *HeidiSQL*
- *SSMS* (Microsoft SQL Server Management Studio)
- *MobaXterm*
- *Xshell*

FortiPAM now includes the following two new secret templates:

- *HeidiSQL*
- *ESXi Web*

Also, FortiPAM now offers a new *ESXi Web* password changer.

885005- Favorite secrets related updates

To improve the user experience:

- Favorite secrets now appear on a new page instead of being listed in the tree menu on the left.
- You can now add/remove multiple secrets to/from the favorite list by selecting the secrets, right-clicking on any of the selected secrets, and then selecting either *Add/Remove Favorite*.
- By selecting a secret from the *Favorite Secrets* page, you can now (depending on how the secret is configured):
  - Launch the secret
  - Make a request to launch the secret/perform an automated task (job)
  - Check-out/check-in the secret
  - Edit
  - Remove the secret from the favorite list.

900367- Event filter profile

FortiPAM can retrieve specific logs for events that occurred during an RDP session from a target.

You can now create new event filter profiles in *Secret Settings* > *Event Filter Profile*.

When creating or editing a secret policy, a new *RDP Event Filter Status* dropdown is available. Once enabled you can enforce a particular event filter profile on the secret that resides in a folder where the policy applies.

When creating or editing a secret, a new *RDP Event Filter* option is available in the *Service Setting* tab, given that *RDP Service* is enabled. Enabling the *RDP Event filter* option allows you to then select and apply an event filter profile to the secret from the *RDP Event Filter Profile* dropdown.

Note that if *RDP Event Filter Status* is set as *Enable* or *Disable* in the secret policy, the *RDP Event Filter* option cannot be changed when configuring a secret that resides in a folder where this policy applies.

Only when *RDP Event Filter Status* is set to *Not Set* in the secret policy, you can set the *RDP Event Filter* option from within a secret.

Further, you can now set access levels for the *Event Filter Profile* page in *Secret Settings* using the *Event Filter Profile* option in the *Secret* tab when you create or edit a role in *User Management* > *Role*.

929608- Stackable seat license for hardware models

For FortiPAM 1000G and 3000G hardware models, you can update the licensed seat using the provided key if you purchase a new stackable seat license with additional seats from FortiCare.

930016- System settings GUI reorganization

System > *Settings* has been reorganized:

- The *PAM Settings* pane, previously available in the *General* tab, is now available in the *Advanced* tab.
  - A new *Live Recording* option in the *PAM Settings* pane.
- *User Password Policy*, *View Settings*, and *Email Service*, previously available in the *Advanced* tab, are now available in the *General* tab.
- A new *Other General Settings* pane in the *General* tab contains the following settings previously available in the *PAM Settings* pane:
  - *Login Disclaimer*
  - *GUI Session Timeout*
  - *Idle in/Force logout in*

883603- FortiPAM on Google Cloud Platform (GCP)

FortiPAM now supports GCP virtualization software.

937021- Setting up the minimum SSL/TLS version and port number for LDAPS password changer/verification

For LDAPS password changer and verification, the minimum SSL/TLS version and the target server port number used by LDAPS can be set using the following CLI commands, provided the secret has an associated target:

```
 config secret target
  edit target_name
   set ldaps-min-ssl-version {default | SSLv3 | TLSv1 | TLSv1.1 | TLSv1.2 | TLSv1.3}
   set ldaps-port <integer>
  end
end
```

897302- Button to generate a password for the secret

When creating a secret that requires a password, FortiPAM now offers a new *Generate* button to automatically generate a password for the secret following the password policy as set in Password policies.

860133- Bypass SSH command filter

Secret owners can now bypass the SSH command filter if the secret uses an SSH command filter. Secret owners can send otherwise prohibited commands (listed in the command filter profile) to targets.

The following new options are available in FortiPAM:

- When creating or editing a secret policy, a new *Bypass For Owner* option is available when *SSH Filter* is enabled.
- When creating or editing a secret, a new *Bypass for Owner* option is available when *SSH Service* and the *SSH Filter* options are enabled in the *Service Setting* tab.

Note that if *SSH Filter* is set as *Enable* or *Disable* in the secret policy, the *SSH Filter* option cannot be changed when configuring a secret that resides in a folder where this policy applies.

Only when *SSH Filter* is set to *Not Set* in the secret policy, you can set the *Bypass For Owner* option from within a secret.

943653- Display user location

FortiPAM displays the user location in *Monitoring* > *User Monitor* in the new *Location* column.

In *Monitoring* > *Active Sessions*, where the launched secret activities are displayed, FortiPAM now also displays the location from where the secret was launched in the new *Source Location* column.

Additionally, in *Monitoring* > *Active Sessions*:

The following new columns have been added:

- *Token ID*
- *Username*: Previously available as a widget on the top.

The *End Session(s)* button has been renamed to *Disconnect*, and the button is only available when you select a secret session.

923465- Customizing the report layout via GUI

You can now customize reports in the FortiPAM GUI by going to *Log & Report* > *Reports*, selecting *General*, and then going to the *Layout & Schedule* tab.

Note that the *Reports* tab in *Log & Report* has been reorganized:

- New *General* and *Secret Audit* pages.
- The *General* page contains the following tabs:
  - *Reports*: Display/generate audit reports to comply with audit requirements.
  - *Layout & Schedule*: Allows customization of reports and schedule generation of reports.

914109- Secret access audit report

You can now generate secret access audit reports by going to *Log & Report* > *Reports* and selecting *Secret Audit*.

945474- User group permission

When creating or editing a user group in *User Management* > *User Groups*, a new *Permission* tab allows you to set up access control for the user group.

Note that when creating or editing a user group in *User Management* > *User Groups*, a new *General* tab contains all the general settings.

904163- FortiPAM on Amazon Web Services (AWS)

FortiPAM now supports AWS virtualization software.

865796, 807856- Display logs stored on a FortiAnalyzer

When setting up FortiAnalyzer as the remote logging server in *Network* > *Fabric Connectors*, the following new option is available:

- Previously available non-editable *Upload option* has been replaced with a new *Upload option* that allows you to upload logs to FortiAnalyzer:
- *In real time*
- *Every minute*
- *Every 5 minutes*
- *More*

Logs stored on FortiAnalyzer can be viewed in *Log & Report* by selecting *FortiAnalyzer* as the source from the top-right.

Also, a new filter/time frame dropdown is available for the following tabs in *Log & Report* to filter logs by time:

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

Note that secret videos recorded in HA are not available from FortiAnalyzer.

876120, 948636, 951448- Web proxy for FortiPAM browser extensions

When accessing a target using the FortiPAM browser extension, the browser extension now sends the browser requests through the FortiPAM web proxy. This enhances security by not delivering credential information to the client.

FortiPAM now offers a new web proxy feature to dynamically operate on the web browser tab's PAC rule (on Google Chrome and Microsoft Edge) to successfully proxy the traffic to FortiPAM based on the configured domain. On Mozilla Firefox, FortiPAM sends the request to the web proxy instead.

Fortinet Privileged Access Agent 7.2.3 (browser extension) or above is required to support the web proxy feature.

FortiPAM scans the incoming web traffic and can replace the password.

The web proxy feature is supported on both extension only deployment and extension with FortiClient deployment.

To enable the web proxy feature, you must first enable the feature globally for the interface that handles incoming and outgoing traffic using the following CLI commands:

```
config system interface
 edit "port1"
  set explicit-web-proxy enable #must be enabled
 next
end
```

Alternatively, you can enable the feature by enabling *Explicit web proxy* for the interface that handles incoming and outgoing traffic.

When creating or editing a target in *Secrets* > *Target List*, given that the *Default Template* is *ESXi Web* or a custom template with the *URL* field and the *URL* field is filled in, the *Web Proxy* option can be enabled for the secret target from the *Advanced Web Setting* pane.

When creating or editing a secret in *Secrets* > *Secret List*, a new *Web Proxy* option is available in the *Secret Setting* pane if you enable and select a target for this secret that has *Web Proxy* set up.

Notes:

- The *Web Proxy* option is inherited from the secret target.
- When you edit the *Web Proxy* option, you are editing the *Web Proxy* option available from within the associated secret target.

912421- Display the last failed login time in the disclaimer

FortiPAM now displays the last failed login time in the disclaimer.

963856- New description column for secrets list

FortiPAM now displays a new *Description* column in *Secrets* > *Secret List*.

Note that the new *Description* column is not visible by default.

To display the new *Description* column, select *Configure Table* icon as you click the header for the left-most column, select *Description* and then click *Apply*.

958573, 960219- Deauthenticate a user and disconnect secret sessions

In *Monitoring* > *User Monitor*, the following new options are available in the *Terminate* dropdown when you select a user:

- *Deauthenticate User*
- *Disconnect Launched Sessions*
- *Deauthenticate & Disconnect*

In *Monitoring* > *Active Sessions*, you can terminate an active session by clicking *Disconnect the current secret session* as you live stream the session.

951931- New CA certificate download button

When you attempt to access a website using the web proxy feature, you may receive a warning about untrusted hosts on the web browser. To resolve this issue, you must download and install a CA certificate signed by FortiPAM.

When creating a secret with *Web Proxy* enabled, a new *Download CA Certificate* button on the top-right allows you to download the CA certificate.

Also, when there are multiple certificates that you need to install, a new *Download All CA Certificates* button is available instead.

When downloading multiple certificates, they are made available as a zip file named `CA-Certificates.zip`.

802577- Concurrent logins for a user

A concurrent session occurs when multiple users access FortiPAM using the same account from different locations or web browsers.

You can allow concurrent login sessions for a user account by enabling the new *Concurrent Log-on* option in the *General* tab in *System* > *Settings*.

By default, the new *Concurrent Log-on* option is disabled.

949813- View secret log from the Secret Details page

For FortiPAM users without administrative privileges, such as a *Sponsor Admin* who may want to check specific secret log and activity but does not have global log permission, FortiPAM now offers the following two new permissions when configuring a role in *User Management* > *Role*:

- *View Secret Log*- The user can see the secret modification history, launch activity logs, and SSH filter logs (for SSH launcher) in the *Secret Details* page when editing/viewing a secret in *Secrets* > *Secret List*.

  The following new tabs are available when editing/viewing a secret:

  - *Edit History*
  - *Activity*
  - *SSH Filter Log*
- *View Secret Video*- The user can view the secret launching video.

Notes:

- The *Sponsor Admin* user has *View Secret Log* and *View Secret Video* permissions by default.
- You must have at least *View* permission for the secret to see the new *Edit History*, *Activity*, and *SSH Filter Log* tabs.

850496- Over-the-shoulder monitoring

FortiPAM now allows administrators to monitor the user session and actions in real-time.

Prerequisites:

- *Fortinet Privileged Access Agent* 7.2.3 or above is required to support over-the-shoulder monitoring.
- When you launch a secret with *Session Recording* enabled, and given that *Live Recording* is enabled in the *Advanced* tab in *System* > *Settings*, you can monitor the user session in real-time.

You can terminate an active session by clicking *Disconnect the current secret session* as you live stream the session.

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

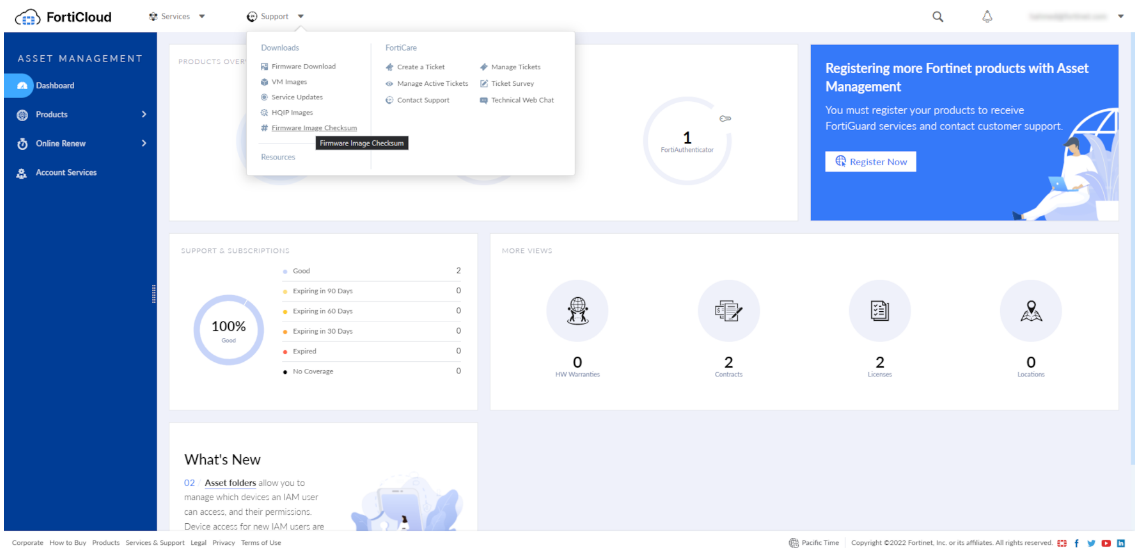
To verify the integrity of the firmware file, use a checksum tool to compute the firmware file’s MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

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.



Registering more Fortinet products with Asset Management

You must register your products to receive FortiGuard services and contact customer support.

Good	2
Expiring in 90 Days	0
Expiring in 60 Days	0
Expiring in 30 Days	0
Expired	0
No Coverage	0

What's New

02 / Asset folders allow you to manage which devices an IAM user can access, and their permissions. Device access for new IAM users are

Copyright ©2022 Fortinet, Inc. or its affiliates. All rights reserved.

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 1.1.x, you can directly upgrade to FortiPAM 1.2.0.

From FortiPAM 1.0.x, upgrade to FortiPAM 1.1.2 and then upgrade to FortiPAM 1.2.0.

Product integration and support

FortiPAM 1.2.0 supports the following:

- Web browser support on page 19
- Virtualization software support on page 19
- Hardware support on page 19

Web browser support

FortiPAM version 1.2.0 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 1.2.0 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 1.2.0 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
862980	Any updates to a secret for a user will trigger secret list reload warning for other users.
945205	WebSSH and password verification kex failed in a FortiSwitch 3032 V7.2.5.
949879	Failed launch native RDP on Windows 10 when connecting to a Windows 11 machine.
950094	GUI is missing maximum password retry, retry threshold, and account lockout warning.
962554	LDAPS fails to authenticate in the GUI with default settings.
950094	GUI is missing maximum password retry, retry threshold, and account lockout warning.

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
970973	Soft RAID-10 is not supported.
969403	When creating a target, the default *Target Only* template is not in the GUI.
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.
974134	Unable to log in to iDrac if *Web Proxy* is enabled.
975443	A new tagging feature added to FortiClient build 907 and above may cause the ZTNA feature not to work in FortiPAM.
978393	Support AWS root and IAM users on *Web Proxy*.
970329	The standalone FortiClient requires the PC to reboot to start up after shutdown.
982033	Native launchers fail after upgrading the standalone FortiClient from a previous version. For workaround, see *Native launchers failure* in Special notices on page 7.
982710	*Launch Secret* is not available on the *Secret Details* page when the *Inherit Permission* option is disabled on the Firefox browser. **Workaround**: Launch the secret from the *Secrets List* page using the *Launch Secret* option if the *Launch Secret* option is not available on the *Secret Details* page. Alternatively: • Use a different web browser (Chrome or Edge). • Enable *Inherit Permission* from the *Permission* tab when editing the folder where the secret resides. This option can also be enabled from the *Permission* tab of the *Secret Details* page.
985832	FortiPAM 1.2.0 does not support vTPM on GCP.
984506	The sponsor admin does not have secret and video log access enabled by default after upgrading from FortiPAM 1.1.2 to 1.2.0. **Workaround**: Rebooting the system enables *View Secret Log* and *View Secret Video* permissions for the sponsor admin.
986168	Only first entry shows up in *User Permission* for a secret target.

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	5000	10000	10000
Folder	2000	6000	6000
User	1000	3000	3000
Request	5000	10000	10000

www.fortinet.com