Release Notes

FortiPAM 1.7.0

November 21, 2025
FortiPAM 1.7.0 Release Notes
74-170-1166987-20251121

TABLE OF CONTENTS

Change log

Date	Change Description
2025-08-05	Initial release.
2025-08-06	Updated Upgrade paths on page 18 and Language support on page 20.
2025-08-14	Updated What's new on page 9.
2025-09-05	Updated FortiPAM 1.7.0 release on page 6.
2025-11-21	Added Common Vulnerabilities and Exposures on page 24.

FortiPAM 1.7.0 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, resolved issues, and known issues for FortiPAM 1.7.0, build 1463.

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 1.7.0 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.

If FortiClient is installed on macOS, upgrade to FortiPAM 1.6.0

If FortiClient is installed on macOS, secret video recordings do not work with *Web SSH*, *Web RDP*, and *Web VNC* secret launchers.

Upgrade to FortiPAM 1.6.0 to resolve this issue.

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 1.7.0, 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 1.7.0, adjust the storage limit in the *Advanced* tab in *System > Settings*.

What's new

The following list contains new and expanded features added in FortiPAM 1.7.0.

Secret/Launch

1160995- Secret configuration page improvements

When creating a secret:

- The *Secret Setting*, *Service Setting* tabs have been merged into a single *Settings* tab.
- The *Permission* tab has been renamed to *Sharing*.
- *Credential History*, *Edit History*, *Secret Log* (previously *Activity*), *SSH Log* (previously *SSH Filter Log*) tabs now available under a new consolidated *Audit* tab.

1145871- Support MobaXterm-sftp

Starting FortiPAM 1.7.0, a new default launcher *MobaXterm-sftp* now available.

The *MobaXterm-sftp* launcher enables SFTP tab on the left of the SSH session console.

The SFTP tab allows you to upload/download files and perform directory operation directly within the session.

Prerequisites

Install `sshpass` package under mobaxterm packages.

Notes

- The *MobaXterm-sftp* launcher is not supported if the target Linux SSH server only allows keboard-interactive authentication.
- The *MobaXterm-sftp* launcher is not supported by secrets with TOTP settings enabled.
- If using the feature with an SSH profile, ensure to uncheck *SFTP* channel option in *Other Channels/Block Channel*.

1160286- AV/DLP support for secret file upload

In FortiPAM 1.7.0, AV/DLP support has been added for secret file upload to safeguard files stored on FortiPAM.

When creating a *File* type secret, new *Antivirus Scan* and *DLP Status* options are now available.

1173019- Support configurable SSH terminal types

In FortiPAM 1.7.0, new configurable SSH terminal type has been introduced:

```
config secret template
 set ssh-term {vanilla | xterm | vt100}
end
```

- `vanilla` : Minimal and legacy SSH terminal type and provides basic capabilities (default).
- `xterm`: Supports advanced features like color and cursor control.
- `vt100`: Supports simple text and cursor control for compatibility with older systems.

1173019- Default maximum delay for password changer increased

Starting FortiPAM 1.7.0, the default maximum delay for the password changer has been increased to 60000 ms (from 20000 ms).

1096117- Expose the configuration of strength of SSH encryption algorithms

Starting FortiPAM 1.7.0, when creating a secret with SSH service enabled, you can now set up the configuration strength for SSH encryption algorithms using the new *SSH Algorithm Negotiation* dropdown.

Additionally, a new *SSH Algorithm Negotiation* dropdown available when creating/editing a secret policy.

1138302- Target Auto Match/Create

Starting FortiPAM 1.6.0, FortiPAM allowed creating a secret without a target.

Starting FortiPAM 1.7.0, FortiPAM now simplifies secret creation by automatically matching the secret to a pre-exisiting target with the same address, domain, or URL. If no such target exists, a new target for the secret is automatically created.

When creating/editing a secret, a new *Auto Match/Create* option available in the *Target* dropdown.

⚠ The feature is only available when creating a secret using the GUI.

1134577- Native RDP connection diagnostics

Starting FortiPAM 1.7.0, for a failed RDP connection, FortiPAM now displays connection failure logs:

- Errors occur during the negotiation phase, for example, when the server requires NLA but FortiPAM is configured not to, or when FortiPAM requires NLA while the server does not support it.
- Errors produced during the TLS handshake phase.
- Errors during NLA authentication.
- Errors during protocol parsing.

1144521, 1119158- Two new default password changers

In FortiPAM 1.7.0, the following two new default password changers have been added:

- *PAN-OS (Palo Alto Networks)*
- *SSH Password For Root (Unix)*

1163064- Same IP address target with different gateway

Starting FortiPAM 1.7.0, you can create targets that have the same IP address but different gateways.

1149963- Discovery auto-onboarding

In FortiPAM 1.7.0, for Windows AD discovery type, FortiPAM supports account auto-onboarding where once the accounts have been discovered on the target windows AD server, the accounts are imported as secrets on FortiPAM automatically by preconfigured rules.

The following new options are available when creating a Windows AD discovery entry:

- *Account Filter*: *Legacy LDAP Search Base* and *LDAP Group Filter*.
- *Account Auto Onboarding*
  - *Folder Destination*: The folder that account secrets will be auto created into.
  - *Password Management*: The following two modes are supported:
    - *Manual*: The administrator enters the recently created secrets password.
      - *Synchronize*: In *Manual*, the administrator can choose whether to reset and synchronize the entered password to the remote Windows AD server.
  - *Random*: New secrets have their passwords randomly set by FortiPAM and synchronized to the remote server.
  - *Synchronize Password*
  - *Password*

1141928- Support OT application launchers

In FortiPAM 1.7.0, the following three new default TIA Portal based OT launchers are introduced:

- *TIA Portal*: For unprotected projects.
- *TIA Portal V16 Logon*: For password protected projects in the TIA Portal V16.
- *TIA Portal V19 Logon*: For password protected projects in the TIA Portal V19.

A new *TIA Project* default secret template is also available.

1134040- Renamed *Web Launcher* to *Web Browsing*

Starting FortiPAM 1.7.0, the *Web Launcher* secret launcher has been renamed to *Web Browsing*.

1184583- FortiClient script command

Starting FortiPAM 1.7.0, the following new options are available when creating a secret launcher for Windows:

- *Start FortiClient Session in Multiprocess Mode*
- *Full-screen Recording*

Start FortiClient Session in Multiprocess Mode and *Full-screen Recording* are only available with FortiClient 7.4.4 and above.

- *FortiClient Commands*

1113718- New *Radmin* launcher

Starting FortiPAM 1.7.0, a new *Radmin* secret launcher is available with *Type* as *Other client*.

Note: The launcher requires FortiClient support.

The *Radmin* launcher helps you pass credentials independently to FortiClient.

The *Radmin* secret launcher supports FortiClient commands allowing script executed by FortiClient to automate actions on the launched application including filling in the username and password.

Using the *Radmin* secret launcher, you can automatically enter username and password when a new credential prompt window appears during the secret session launch.

User/Group

1156215- Restrict user to only login through console

Starting FortiPAM 1.7.0, a new `login-restriction-console` CLI configuration command allows you to restrict user logins to FortiPAM through the console only, i.e., GUI, SSH, and other login methods are blocked.

```
config system admin
 edit "test_admin"
  set accprofile "Default Administrator"
  set login-restriction-console {enable | disable}
  next
end
```

Note:

- The configuration is only available in the CLI console.
- The configuration only applies to a local user with *Allow CLI Access* enabled in its user role.
- The configuration does not work with any MFA settings.
- The configuration is available to remedy scenarios where the *Default Administrator* is locked:
  - MFA was configured, but login fails due to network, firewall, or configuration issues.
  - Forgot password.

Always follow the best practices to avoid potential lockout issues.

1173026- Support for JWT authentication

FortiPAM supports creating a JWT user.

Starting FortiPAM 1.7.0, a new *JWT User* type is available in the *Configure Type* tab when creating a new user.

The following new options are available in the *Configure User Details* tab when creating a JWT user:

- *JWT Key*
- *JWT Claims*
- *Lease Duration*

A new *JWT Key Management* tab is available in *User Management*.

1182636- Increased maximum number of users configured on FortiPAM 1000G

Starting FortiPAM 1.7.0, the FortiPAM 1000G hardware device now supports configuring a maximum of 3000 users.

See Configuration capacity for FortiPAM hardware appliances and VM on page 26.

System/Log

1149017- Export the FortiPAM video to playable `webm` format

When *Remote Video Storage* is enabled, the original secret video files are backed up to a remote server using SFTP.

If *Live Recording* is enabled in the *Advanced* tab (*Video Setting* pane), the secret session video files are available in `.chk` format.

Note: The `.chk` file cannot be replayed.

FortiPAM now allows exporting the FortiPAM secret session video in a playable `webm` format.

With the introduction of the new feature, FortiPAM creates the secret session video as a `webm` file based on the `.chk` files.

The `webm` file is then backed up and can be replayed.

Limitation

`init.hdr` does not update after the launch session ends in the *Agentless* mode or when using extension only.

1082302- Associate SSH log with video

Starting FortiPAM 1.7.0, FortiPAM supports SSH log association with the secret session video playback.

When reviewing an SSH session:

- Users can click the command play button from the *Jump* column in the *SSH Event log* (left pane).
- The video playback (right pane) will automatically jump to the timestamp where that command was executed.

Secret configuration requirements:

- Create an SSH filter (in either *Deny* or *Allow* mode).

  Note: Ensure that the pattern you enter has *Log* enabled.
- When creating the secret that supports an SSH launcher, select *Enable SSH service* in the *Settings* tab, and select an *SSH Filter* profile.

  Also, ensure that *Session Recording* in enabled in the *Session Security* tab.

Note:

- Only commands with logging enabled in the SSH filter will be linked to the video.
- There may be a 1 - 2 second time difference between the log and the video timestamp.

Limitations

- In the agentless mode (for web based launchers, e.g., *Web SSH*), you cannot associate the SSH log to the video.

1166023- Secret audit report enhancements

Starting FortiPAM 1.7.0, when generating a secret audit report in *Log & Report > Reports*, new *Secret ID* and *Folder ID* columns are available.

Also, the complete folder path is displayed in the *Folder* column.

1096109- Support single-button global TLS version control

Starting FortiPAM 1.7.0:

- A new global *Minimum SSL Version* setting is available when editing system settings (*System > Settings*) in the *Security* pane.
- When editing an interface, a new *Minimum SSL Version* setting is available in the *Service Access Setting* pane.
- When creating or editing a secret target that uses an SQL template, a new *Minimum SSL Version* setting (in the *Advanced SQL Setting*) is available.
- When creating or editing a secret target that uses a template with *Domain* field, a new *Minimum SSL Version* setting (in the *Advanced RDP Setting*) is available.

1167148- Add video access audit logs

Starting FortiPAM 1.7.0, FortiPAM supports logging access over video, including playing/stopping video, etc.

Each time a user plays/stops/downloads a secret video, a log entry is generated.

The related logs are displayed in the following locations:

- *Audit > Secret Log* when you open the secret in *Secrets > Secrets*.
- *Log & Report > Secret Event & Video*.

Additionally, when using Over-the-shoulder monitoring (Live recording), the corresponding play/stop log is generated.

Others

1123018- Browser extension download directly

Starting FortiPAM 1.7.0, the *Integrity Check* tab has been renamed to *Client Software*.

After FortiPAM installation, you can find the FortiPAM Chrome and Edge extension: *Fortinet Privileged Access Agent* in *Secret Settings > Client Software*.

If a user launches a secret without the extension, the FortiPAM GUI prompts them to install the extension automatically.

If FortiPAM is in an air-gapped environment, you can remove/edit the default Chrome/ Edge extension.

You can also upload the Chrome/Edge extension to the FortiPAM local disk.

You can use the feature to save FortiClient and the native application to the FortiPAM disk or a remote URL.

When FortiClient and the native application are needed, the user is prompted to install them automatically.

Also, when creating/editing a launcher, the *Application Integrity Check* option has been renamed to *Client Software*.

1171798- FortiPAM on Nutanix

FortiPAM supports the Nutanix virtual environment.

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

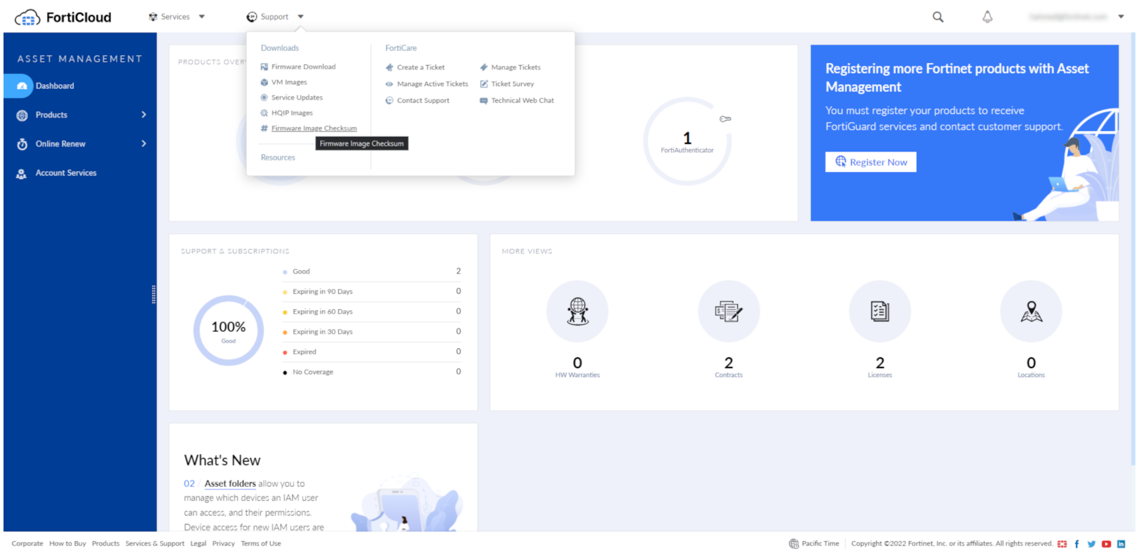
To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

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 1.5.x, upgrade to FortiPAM 1.7.0.
- From FortiPAM 1.6.x, upgrade to FortiPAM 1.7.0.

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 1.7.0 supports the following:

- Web browser support on page 19
- Virtualization software support on page 19
- Hardware support on page 20
- Language support on page 20

Web browser support

FortiPAM version 1.7.0 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 1.7.0 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)
- Alibaba Cloud
- Proxmox
- Nutanix

Hardware support

FortiPAM 1.7.0 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
1127370	Fails to connect Windows 7 Pro via native Remote-Desktop (Native and web RDP TLS version control).
1119158	Password changing for the 'root' user failed on an Oracle Linux 8.10.
1099202	*Target Only* template results in credential filler appearing in unrelated fields.
1154786	Issue with password change with FortiGate/FortiOS (Web) after upgrading to FortiPAM 1.6.0.
1158527	*Replace Web Credential on Proxy* not working with FortiMail.
1142480	Target system returns error authentication failed when enabling *Replace Web Credential*.
1147908	*Web SMB* not uses customized port.
1163918	Native RDP session present certificate errors on the remote desktop client when using a target server FQDN.
1158010	After 15 minutes secret requires reauthentication.
1129557	Add *Edit History* tab to the targets.
1163064	Unable to create targets with the same IP address and different gateways.
1127766	*Web SSH* cannot launch for role with only the secret folder read permission.
1045341	Random disconnections of *Web RDP* connection over FortiPAM.
1149309	Enabling session recording drops the admin session randomly.
1176924	No option to generate the password when secret template does not contain the *Target-Address* field.
1158456	*Web SSH* secret clipboard copy-paste is not working with multiple lines.
1159154	Target default permissoin enhancement.
1175121	Password changer issue after upgrading FortiGate supporting hash PBKDF2.
1178213	SSH discovery stuck at 9% and times out.

User/Group

Bug ID	Description
1144671	FortiPAM GUI cannot be reached after selecting DSA algorithm signed certificate.
1151887	Issue logging into the FortiPAM GUI with Microsoft Surface 7 and FortiToken.
1133443	Support renaming the remote CA.
1141791	Customized user role changes after editing comments.
1153375	The security answer input box prompt changes from token to answer.
1172630	FortiTokens no longer usable after shutting down the FortiPAM-VM.
1161866	Intermittent issues with external Login to FortiPAM.
1172148	Hide *Password Renewal* in the LDAP server.
1157030	After upgrading to 1.6.0, SAML is not working when accessing the FortiPAM from an FQDN.

System/Log

Bug ID	Description
1165860	Under the agentless mode, FortiPAMvideo end log does not display the source address.
1155877	Unable to configure a second GUI portal enabled interface from the GUI.
1174787	Old logs not displayed.
1185729	Expose ZTNA tags removal command on CLI.

Others

Bug ID	Description
1148124	Heap Overflow in FortiPAM -VM license uploading.
1153372	Support theme change on simple GUI.
1173150	sslvpnd crashed with signal 6.

Common Vulnerabilities and Exposures

Bug ID	CVE references
1187405	FortiPAM is no longer vulnerable to the following CVE-Reference(s): • CVE-2025-54821
1199742	FortiPAM is no longer vulnerable to the following CVE-Reference(s): • CVE-2025-61713

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.

Secret/Launch

Bug ID	Description
1139340	Native launcher, e.g., PuTTY, in the proxy mode asks for password in the first launch attempt when there is an invalid ZTNA destination rule in FortiClient 7.4.3.
1188815	After removing a secret from favorite Secrets, the secret still shows up until you refresh the browser.
1186845	Auto Password Verify/Change still shows ongoing in the GUI after disabling.
1180781	New default password changer for FortiGate 7.6.3.

User/Group

Bug ID	Description
1186599	FortiToken assigned during TPM enabled becomes invalid after disabling `private-data-encryption`.

System/Log

Bug ID	Description
1164912	The exported video file length is incorrect when generated using agentless or extension only.

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