Release Notes

FortiPAM 1.6.0

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

December 12, 2025
FortiPAM 1.6.0 Release Notes
74-160-1135298-20251212

TABLE OF CONTENTS

Change log

Date	Change Description
2025-04-28	Initial release.
2025-07-02	Updated Configuration capacity for FortiPAM hardware appliances and VM on page 27.
2025-08-06	Updated Language support on page 21.
2025-12-12	Added bug 1071180 Common Vulnerabilities and Exposures on page 25.

FortiPAM 1.6.0 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, resolved issues, and known issues for FortiPAM 1.6.0, build 1239.

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 1.6.0 requires FortiClient 7.4.0 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.

What' s new

The following list contains new and expanded features added in FortiPAM 1.6.0.

Secret/Launch

1096683- Maximum request time

When creating/editing an approval profile, you can now set the maximum time for which the requestor can request access to a secret using the new *Maximum Request Duration* option.

The maximum *Checkout Duration* is now `1440` minutes.

1087939, 1040854, 1007307- Support vCenter password changer

New *vCenter* secret template available.

New *Web API (vCenter)* password changer available.

1110389- Unidirectional file transmission control

Starting FortiPAM 1.6.0, FortiPAM supports unidirectional file transmission control:

- Upload file transmission from local to remote server.
- Download file transmission from remote server to local.
- Both upload/download file transmission between local and remote server.

Unidirection file transfer requires *WinSCP*, *Web SFTP*, or *Web SMB* launchers to perform unidirectional file transmission.

A new *transmission-direction (Match any file over certain direction)* option in the *Filter By* dropdown when creating or editing a DLP filter rule.

When *transmission-direction (Match any file over certain direction)* option in the *Filter By* dropdown is selected, a new *Direction* option is available.

The protocol is fixed to `http-get`, `http-post` and `ssh`.

1099960- Secret request exemption on schedule

FortiPAM 1.6.0 introduces secret access request exemption on schedule.

When assigning a schedule to an approval profile, the request can be exempted from the schedule.

This is often useful during working hours when there is no need to send an access request, while in non-working hours, it is required to request access.

A new *Request Exemption Schedule* option when creating or editing an approval profile in *Secret Settings > Approval Profile*.

When editing a secret that requires approval to launch the secret, a status message displays if the secret is within the request exemption duration.

1119989- Change the template and password changer name for FortiProduct

In the previous FortiPAM versions, we use FortiProduct template in most cases to indicate a Fortinet product. However, its built-in password changer does not support all the Fortinet products.

In FortiPAM 1.6.0, the names of some of the secret templates and password changers have been updated to clarify which Fortinet products are supported.

In FortiPAM 1.6.0, the following three secret templates have been renamed:

- *FortiProduct (Web)* to *FortiGate/FortiOS (Web)*
- *FortiProduct (SSH Password)* to *FortiGate/FortiOS (SSH Password)*
- *FortiProduct (SSH Key)* to *FortiGate/FortiOS (SSH Key)*

In FortiPAM 1.6.0, the following three password changers have been renamed:

- *Web API (FortiProduct)* to *Web API (FortiGate/OS)*
- *SSH Password (FortiProduct)* to *SSH Password (FortiGate/FortiOS)*
- *SSH Key (FortiProduct)* to *SSH Key (FortiGate/FortiOS)*

1103651- Native Key-value vault support

In 1.6.0, FortiPAM now supports storing key-value pairs.

A new *Key-Value Pairs* secret template is available to store custom key and its value.

A secret based on the *Key-Value Pairs* secret template is used for storage purposes only.

A maximum of 50 key-value pairs can be added to a secret.

A Key value pair secret supports 2 event subscriptions only.

1125550- Smart association

Starting 1.6.0, FortiPAM now supports smart association for secrets.

A new *Smart Association* option in the *Associated Secret* dropdown when creating a secret.

Enter an account prefix in the *Account Prefix* field.

When using *Smart Association*, FortiPAM:

- Combines the account prefix and the currently logged-in username to generate a new username.
- Looks into the secret database to search for any secret username that matches the generated username.
- When a matching secret is found, its credentials are used to launch the secret.

1109894- Support Viewer on *Web Launcher*

Before FortiPAM 1.6.0, the user with *View* permission cannot launch Web Launcher to access a website due to the possibility of password exposure.

A secret is often shared with *View* permission to others by the admin, resulting in unavailability of secret launch.

A new *Web Launcher Access* option is introduced under *Web Service* when creating/editing a secret.

- *Restricted*: Only the user that is allowed to view the credential to this secret is allowed to launch web launcher, i.e., the same behavior as before.
- *Any*: Anyone with permission to the secret is allowed to launch web launcher, i.e., even if a user with *View* permission can launch web launcher.

1103651- Secret creation GUI enhancements

Starting FortiPAM 1.6.0, when you select *Create* to create a new secret, a new *Select a Secret Template* page appears.

In the *Select a Secret Template* page, you can search for a specific secret template by name.

The templates are now displayed with their respective icons.

The templates are categorized and can be filtered by:

- *Unix-like*
- *FortiOS*
- *Cisco*
- *Windows*
- *ESXi*
- *Web*
- *Database*
- *Store Data*
- *Others*

By default, personal folder is selected when creating the secret. Click the folder path to change it.

Once the secret is created, you can still change the template being used by selecting the template, and from the *Convert Secret Template* window, select a new template from the dropdown.

Changing the secret template after creating the secret is a risky operation, ensure that important information used in the previous template are preserved in the new template.

1110651- *Initialization Command* is supported on both proxy and non-proxy mode

Initialization Commands for secret launchers now work on both the proxy and the non-proxy mode.

1123551- Password Reconciliation for Windows AD by LDAPs protocol

In FortiPAM 1.6.0, password reconciliation is introduced which lets the secret (base account) use another secret (reconcile account) to reset its password.

The reconcile account is used as the bind account to change the base account password. This can help secret to change password under the following two conditions:

- When the base secret does not have the right to change its own password.
- When the base secret password is out-of-sync with the target server.

A new *Password Reconciliation* option in the *Secret Setting* tab when creating/editing a secret.

Password Reconciliation contains the following two options:

- *Reconcile Account*: Use privileged account of the base account target as the reconcile account.
  A different secret can also be used as the *Reconcile Account*.
- *Reconciliation Activation Time*: Choose an activation point to trigger password reconciliation:
  - The password reconciliation happens directly instead of a password change.
  - After a password change failure.

The password reconciliation configuration influences manual password change, automatic password change, and password change during secret check in.

Note: When the *Reconcile Account* is set in *Secret Setting* tab, the user cannot manually change it in the pop-up window.

Password reconciliation is only supported for a password changer whose *Type* is *Active Directory LDAP*.

1102496, 1136165- Unix and FortiOS discovery

In FortiPAM 1.6.0, the following two new discovery types are supported in addition to the legacy *Active Directory* discovery type when creating or editing a discovery in *Secrets > Discovery*:

- *Unix*
- *FortiOS*

Unix and *FortiOS* discovery type can be supported as:

- Target only
- Account only
- Target and Account

Multiple IP ranges and ports:

- Support multiple IP ranges and ports
- Supports the SSH protocol exclusively
- Scanning and account discovery can be enabled or disabled for each IP range separately

Account filter rules:

For *Unix*: Choose to discover all accounts or only privileged accounts.

For *FortiOS*: Filter accounts based on FortiOS Access Profile, `super_admin`, `prof_admin`, etc.

Customized credentials:

Customized credentials are supported for Unix discovery type, including both target-only and target + account discovery.

1123606- Web Launcher via Service Gateway

Starting FortiPAM 1.6.0, *Web Launcher* can directly launch a secret via the service gateway.

When using the *Web Proxy* feature with a service gateway, the default IP address and the port for *Web Proxy* is the gateway address and port number `8080`.

To change the default values, go to the service gateway in *Network > Secret Gateway* on the central FortiPAM server, and use the new *Web Proxy Override* option (disabled by default).

The *Web Proxy Override* option allows you to set the gateway web proxy address and port.

If *Web Proxy Override* is disabled, it indicates if the gateway provides the web proxy feature. In this case, the IP address and the port for the gateway web proxy service is same as the address and the port of the gateway.

If *Web Proxy Override* is enabled, an additional gateway web proxy address is required (IP address or an FQDN). You can either configure the web proxy port or use the default value `8080`.

Note: The *Web Proxy Override* option only appears if the gateway *Type* is *Reverse*, and the *Mode* is *Service Gateway* or *On Demand*.

1126374- File storage

FortiPAM 1.6.0 supports storing files per secret, i.e., a secret can hold a single file.

The stored secret file can be downloaded based on the secret permission.

Also, download event subscription is supported.

To store a file in a secret, when creating a secret, select the new *File* template under *Store Data*.

The following new settings have been added to *System > Settings > Advanced*:

- *File Storage Limit*
- *File Storage Duration*
- *Maximum File Size*
- *Remove Out-of-Sync File*
- *Block File With No Extension*

1121780- Invite external user: One-time invitation

To enhance secure collaboration and controlled access, FortiPAM introduces a One-Time Invitation Feature that allows a secret owner to share a specific secret with an external user through a time-bound, single-use invite code.

Note: This feature is tightly governed by license seat availability and strict access policies to maintain security and compliance.

A new *Invite* button available when a secret owner opens the secret.

User/Group

1121726- JWT (JSON Web Token) integration with DevOps

For improved security when integrating FortiPAM with DevOps platform (such as, GitLab, Jenkins), JWT is introduced into FortiPAM 1.6.0.

It provides the following advantages:

- FortiPAM creates a dynamic token to GitLab or Jenkins. This ensures you are not required to save a permanent token for GitLab or Jenkins.
- After some time, the dynamic token expires for improved security.

In FortiPAM 1.6.0, the feature is only supported via the CLI console.

Use the following CLI commands to set up JWT authentication:

```
config secret jwt-key
 edit [xxx]
  set type jwks
  set jwks-url <gitlab jwks-url>
 next
end
```

```
config system api-user
 edit "jwt-user" #user name
  set type jwt
  set accprofile "pam_standard_user"
  set vdom "root"
  config claims
   edit "project_id"
    set value "2"
   next
   edit "iss"
    set value "gitlab214.fortipam.ca"
   next
   edit "project_path"
    set value "gitlab-instance-ff0dfc9a/robert_pj_001"
   next
  end
 next
end
```

See *JWT integration with DevOps* in the latest*FortiPAM Examples Guide*.

1131573- Simplified contractor user interface

In many real-world scenarios, external users such as technical contractors, auditors, and maintenance technicians require temporary and limited access to secrets within FortiPAM.

To support this, a new simplified UI is available for internal users with *Guest* role and external invited users.

System/Log

1112787- FortiPAM new languages support

Beginning FortiPAM 1.6.0, the FortiPAM GUI supports the following additional language:

- *Italian*

Administrators can configure the language setting for new or existing users when creating or editing a user.

Users can change their own language preferences at any time using the language dropdown in the banner.

1082596- CA certificate for web proxy

When launching a website with web proxy enabled, FortiPAM resigns the certificates of the HTTPs server with the default `Fortinet_CA_SSL` CA certificate.

Sometimes, customers need to use their own CA certificates instead of the default `Fortinet_CA_SSL` to avoid importing too many CA certificates to their Windows host.

Starting FortiPAM 1.6.0, you can now choose a CA certificate after enabling *Explicit Web Proxy* when editing an interface in *Network > Interfaces*.

1110282- FortiAnalyzer Cloud support

FortiAnalyzer Cloud is a remote logging server that keeps an additional copy of logs from FortiPAM.

A new *Cloud Logging* fabric connector available in *Network > Fabric Connectors*.

See*FortiAnalyzer Cloud as a logging server example* in the latest *FortiPAM Examples*.

1121839- Copy video file location

If a secret video file has been backed up to a remote storage and deleted from the FortiPAM local disk, you cannot replay the video. Such a video file displays as *Video not found*.

A right-click on *Video not found* displays the new *Copy Video URL* option.

Clicking *Copy Video URL* allows you to copy the folder location with the format `sftp_user_account@sftp_server_ip:/sftp_server_folders`, e.g., `sftp_user@10.59.112.254:./pam_vid/1884/64429111`.

If the video is in the FortiPAM local disk and recorded without livestreaming, the *Copy Video URL* option allows you to copy the video URL in the local disk, e.g., `https://10.59.112.16/wa_vid/1890/6943603/6943603.webm`.

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

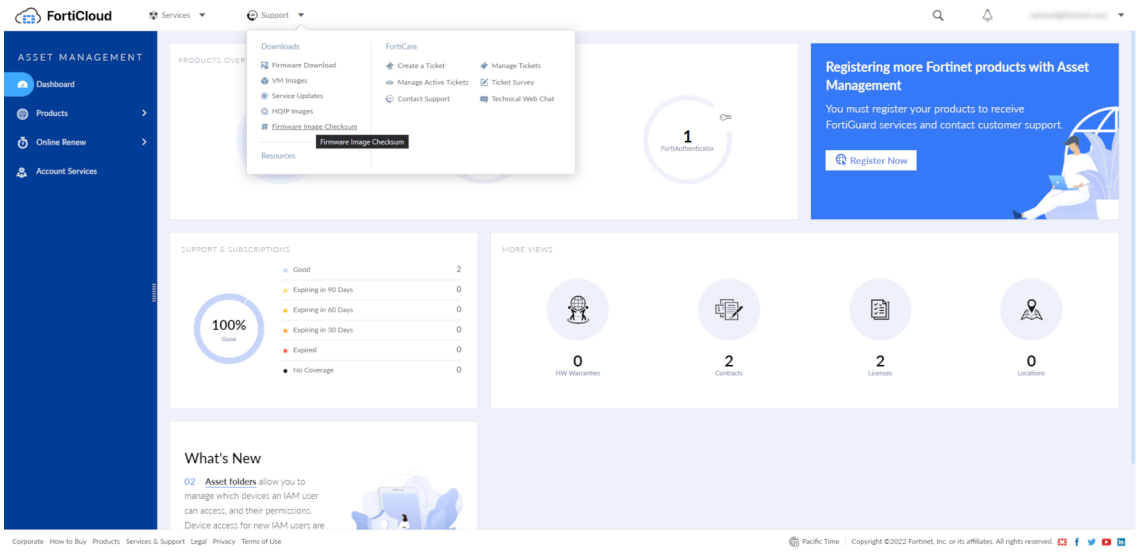
To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

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.

   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 1.4.x, upgrade to FortiPAM 1.6.0.
- From FortiPAM 1.5.x, upgrade to FortiPAM 1.6.0.

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 1.6.0 supports the following:

Web browser support

FortiPAM version 1.6.0 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 1.6.0 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

Hardware support

FortiPAM 1.6.0 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
1104861	Associated Secret does not work with Web-Proxy credentials replacement.
1111984	Occasionally, slow to launch `web_account` with `web_proxy` enable.
1123442, 1123005	Approval email does not have port in FQDN.
1121582	Automatic Password Change fails with FortiGate.
1128256	Fix approval Email with invalid token.
1130735	Logic of folder permission changed impacting secret permissions.
1110101	Loosen target domain restriction changes.
1125761	Using space in the application filter path breaks the path.
943426	Secret can not be deleted when there are requests referencing it.
1111605	SSMS fails to connect to SQLServer Express edition.
1120249	Unable to access secret using web launch and enabling SSO.
1099202	*Target Only* template results in credential filler appearing in unrelated fields.

User/Group

Bug ID	Description
1124133	Remove 2FA status check assert which causes wad crash.
942445	Add remote cert import feature in the GUI SAML configuration.
1146150	Resending the activation email for the 3rd party authenticator (all users getting QR code).
1140780	MFA bypass bug.
1143321	Dashboard displayed at the start page when Custom-Role is in use.
1141333	When deleting entry from the Restricted List, always deleted primary one.
1130835	Email approval not working.
1067329	When *Replace Web Credential* is enabled FortiPAM will randomly fail to proxy.

System/Log

Bug ID	Description
1118634	KVM video disk unavailable in rare case
1090570, 1117042	Redundant logs for web browsing with web-proxy enabled
1117515	ZTNA HTTPS deployment could not work with FOS 7.4 and higher version.
1113653	Enabling **private data encryption** breaks secret passwords.
1134290	Unable to view credentials in Glass Breaking mode.
1145017	Automation Stitch trigger with wrong condition on GUI.
1138555	SAML admin login failing when using group matching.

Others

Bug ID	Description
1116828	After enabling "GUI Portal" on port2, it failed to log in to FortiPAM due to incorrect firewall policy.
1007307	Issues with FortiVoice.
1134119	If FortiClient is installed on MacOS, upgrade your FortiPAM 1.6.0. See Special notices on page 7.
1121038	Weak authentication in wad/GUI.
1120661	Integer Overflow on SSL-VPN VNC bookmark.
1137498, 1138620	Add Ctrl/Shift+Insert and Ctrl+Shift+C/V support.
1127496	Replace Blacklist/Whilstlist terms.
1144380	Application Wad Signal 11.
1112308, 1117737	Heap buffer overflow in websocket.
1108888	Privilege escalation in Node.js websocket module.

Common Vulnerabilities and Exposures

Bug ID	CVE references
1130288	FortiPAM is no longer vulnerable to the following CVE-Reference(s): • CVE-2025-26466 • CVE-2025-26465
1071180	FortiPAM is no longer vulnerable to the following CVE-Reference(s): • CVE-2024-47570

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
1143226	Failed to launch VNC with Ubuntu version 22 with VNC Viewer. **Workaround** Create a customized launcher for Ubuntu 22 as below: • *Type*: VNC • *Executable Location*: `vncviewer.exe` • *Parameter*: `$HOST::$PORT -Quality=Medium`
1099202	Target Only template results in credential filler appearing in unrelated fields.

User/Group

Bug ID	Description
1134159	The GUI of "Trust Host" is incorrect for JWT User.

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
Gateway	256	256	256

www.fortinet.com