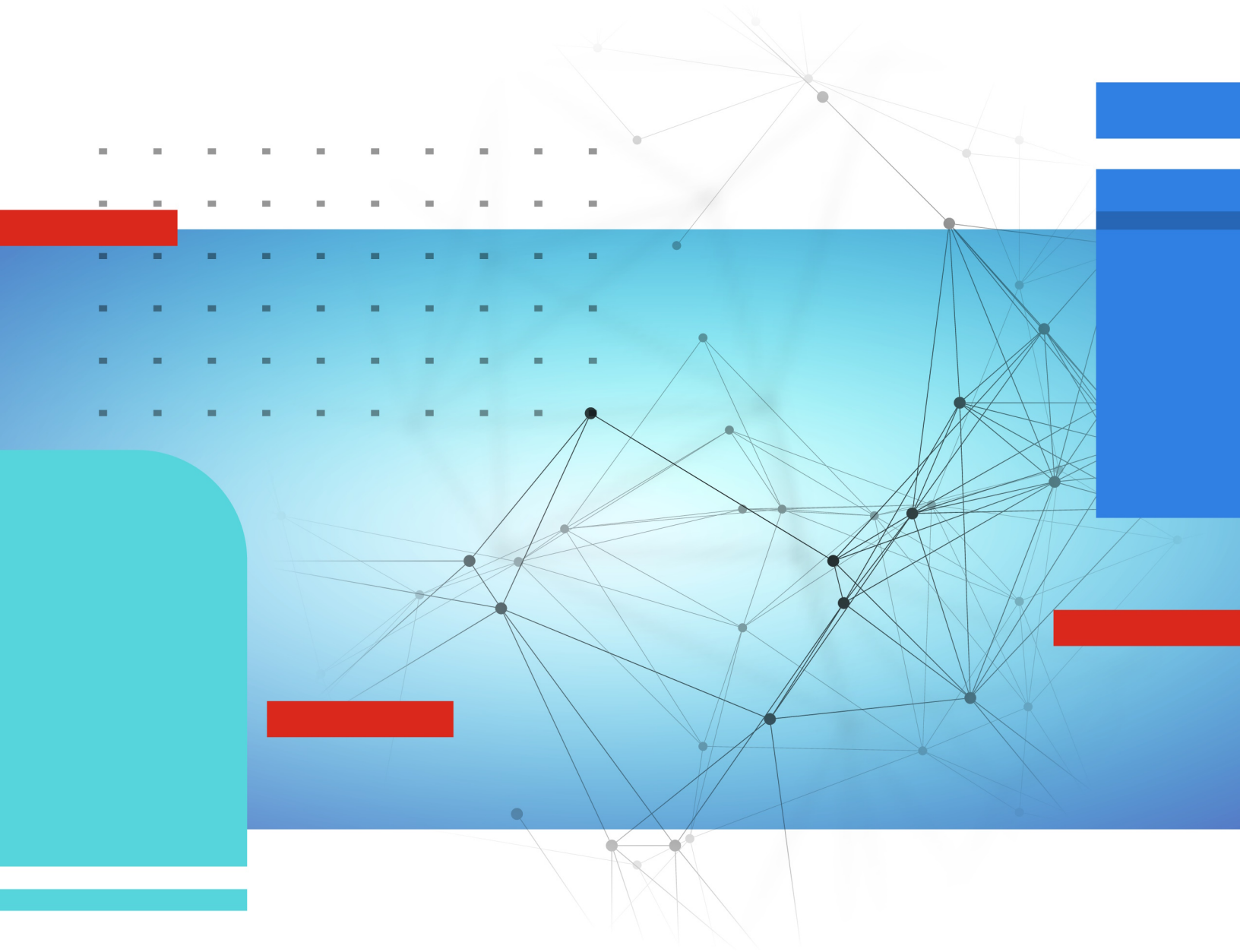
Release Notes

FortiPAM 1.4.0



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

August 13, 2024
FortiPAM 1.4.0 Release Notes
74-140-1056982-20240813

TABLE OF CONTENTS

Change log

Date	Change Description
2024-07-30	Initial release.
2024-07-31	Updated What' s new on page 7.
2024-08-01	Added bug 1061739 to Known issues on page 29.
2024-08-09	Updated Upgrade instructions on page 21.
2024-08-13	Added bug 940442 to Common Vulnerabilities and Exposures on page 28 in Resolved issues on page 26.

FortiPAM 1.4.0 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, resolved issues, and known issues for FortiPAM 1.4.0, build 1135.

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 1.4.0 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.

What' s new

FortiPAM version 1.4.0 includes the following enhancements:

Secret/Launch

1001227- Distributed network gateway architecture Reverse mode

The reverse gateway feature extends the distributed architecture functionality.

The introduction of Gateway allows accessibility from a FortiPAM located in a public network to a private enterprise network.

Gateway introduced forward type network gateway, i.e., the connection is from FortiPAM to the network gateway and then to the target. This type of in-bound connection can be blocked by an edge or internal firewall and FortiPAM cannot reach the target via the gateway.

To resolve this deployment restriction, FortiPAM supports reverse gateway feature.

The FortiPAM can be reached from a reverse gateway and the reverse gateway makes the first connection to FortiPAM as the control plane connection. This is a persistent connection that uses health checks to detect connection issues and supports reconnection.

New *Type* option when creating a gateway that allows you to configure the gateway as forward or reverse type.

When the *Type* is reverse:

- New *Health Check* options allows you to periodically check if the gateway is still alive.
- Using the new *Gateway ID* option, you can specify the gateway client certificate common name to create a mapping between FortiPAM and the gateway.

A new *Type* column in *Secrets* > *Gateway* that tells you the type of the gateways available, i.e., forward or reverse.

For a reverse gateway, the status is shown on the top-right.

994084- Access Target with associated secret credentials

Starting FortiPAM 1.4.0, you can now launch secrets using associated secret credentials not only on Linux and Cisco, but also Windows.

All launchers support launching one secret using another associated secret's credentials. This can be used to store common credential in one secret which can be used by multiple other secrets. This makes the information stored in a secret compact and flexible.

The credential information includes:

- User name
- Password
- Domain
- Public key

- Private key
- Passphrase

The following new options were added when creating or editing a secret in *Secrets* > *Secrets*:

- A new *Launch with Associated Secret Credentials* toggle when *Associated Secret* is enabled in the *General* pane. When the option is enabled, associated secret credential information is used for launching a secret. The credential information stored in the primary secret is not used.

  You must ensure that all the required information is stored in the associated secret.

- A new *Auto-Switch Account* option in the *Service Setting* pane when *SSH Service* is enabled and a *Template* is already selected. The option is only available when:
  - *SSH Service* is enabled, i.e., it will only work with SSH launchers.
  - *Launch with Associated Secret Credentials* is enabled in the *General* pane.

  When the *Auto-Switch Account* option is enabled, upon launching the current secret, the secret uses the associated secret (if applicable) and automatically switches to the current account.

  When the *Auto-Switch Account* option is disabled, secret launching finishes in the account stored in the associated secret since the credential information was received from the associated secret.

Additionally, *Connect over SSH with* option has been removed.

Note that when both *Launch with Associated Secret Credentials* and *Auto-Switch Account* options are enabled, the same functionality is offered as with the *Connect over SSH with* an associated secret. Launching a secret uses the associated secret credential information to log in and switch to the account stored in the primary secret.

If both *Launch with Associated Secret Credentials* and *Auto-Switch Account* are disabled, the same functionality is offered as with the *Connect over SSH with* itself option. Launching a secret only uses the primary secret for launching. Here, the associated secret provides password for the primary secret without a password, e.g., an SSH secret with keys or a secret with *SSH Auto-Password* enabled and using password changing.

1004629- Customize maximum credential history in a template

A new *Max Record of Credential History* field when configuring a template in *Secret Settings* > *Templates*.

In the new *Max Record of Credential History* field, you can set up the maximum number of credential history to be kept in the database.

1000861- Session Monitor refactor based on launch

Starting FortiPAM 1.4.0, the active session monitor is replaced with active launch monitor. One entry represents one launch instead of one session.

Multiple sessions may be made during a single launch. Some launch may still appear in the list even though the launch session is closed.

When the source port is `port 0`, no active TCP connection is attached to the launch.

The *Disconnect* button allows the administrator to terminate a secret launch session. The session attached to the launch is broken.

Two new CLI commands have been added for launch monitor and management.

You can now use the following CLI command to list all the active launches:

```
diagnose wad token list
```

You can use the following CLI command to delete already added launches:

```
diagnose wad token clear <token_id>
```

The `token_id` variable is optional.

If no `token_id` is given, all the active launches are deleted.

By deleting active launches, sessions associated with all the launches are broken.

The video connection remains intact until the window is closed.

1020348- Warnings for duplicating credentials

Starting FortiPAM 1.4.0, you now receive a secret duplication warning when you create or edit a secret with target address and user name of an existing secret.

This helps avoid password conflicts. If there are duplicate secrets (the same target address and user name) and one secret password is changed, the other secret may not launch as the target password has already been updated.

968129, 1006370- Secret service permission

The introduction of launcher permission in secret allows you to customize user with access to only certain types of launchers. This protects some launchers that are more sensetive.

When creating a secret in *Secrets* > *Secrets*:

- The previously available *Secret Setting* pane in *General* is now available as a separate *Secret Setting* tab.
- The ZTNA settings in the *Permission* tab are now available as a separate *ZTNA* pane.
- The *User Permission/Group Permission* table in the *Permission* tab is now available with a new look as a separate pane in the *Permission* tab.

When creating a folder in *Secrets* > *Personal Folder/Public Folder*:

- The ZTNA settings in the *Permission* tab are now available as a separate *ZTNA* pane.
- The *User Permission/Group Permission* table in the *Permission* tab is now available with a new look as a separate pane in the *Permission* tab.

When creating a secret template in *Secret Settings* > *Templates*:

- The table listing fields is available with a new look.
- The table listing launchers is available with a new look.
- The *Access* option in the *Permission* tab has been renamed to *Accessibility*.
- *User Permission/Group Permission* in the *Permission* tab have been replaced with *Create Secret* and *Owner* options.

  From the dropdown, you can assign the *Create Secret* and *Owner* permissions to user and user groups.

When creating a target in *Secrets* > *Targets*:

- The *Access* option in the *Permission* tab has been renamed to *Accessibility*.
- *User Permission/Group Permission* in the *Permission* tab have been replaced with *Create Secret* and *Owner* options.

  From the dropdown, you can assign the *Create Secret* and *Owner* permissions to user and user groups.

1018981- Three new default SQL templates: Microsoft SQL, MySQL, PostgreSQL

FortiPAM now includes the following three new SQL secret templates:

- *Microsoft SQL*
- *MySQL*
- *PostgreSQL*

This solves the issue of having only one database template entry by creating three new SQL secret database template types from the *Database Server* default template. You can now create more precise database secrets for each specific type.

971240- Display full folder path

FortiPAM now displays the path to the folder at the top.

You can see the full path of the current folder and jump to a parent folder by clicking the parent folder from the folder path.

Click the predecessor folder from the path breadcrumb to go to the predecessor folder.

Also, the following new GUI changes were introduced:

- The *Go back up one level in the tree* option has been removed.
- The *Open Tree* option is renamed to *Tree*.

1021461- Support website login with 2FA(TOTP) and more exact auto filling for web extension

When you launch a secret with web launcher, the extension automatically inputs user name and password to log in to the target website.

However, the web launching feature has the following three limitations:

- When launching to some special website, the extension cannot find the user name or the password field correctly using its predefined key.
- After logging in to a website, the extension tries to fill user name or password into an unrelated field.
- The extension can only fill in user name, password, but 2FA Token is not supported.

In FortiPAM 1.4.0, the web launching feature has been improved with the introduction of auto web filler.

When using a secret template that uses *Web Launcher* as the secret launcher, a new *Web Filler tab* allows you to configure advanced web filler settings, so that extension can locate the correct web elements to patch credential information into.

The following options are available:

- *Authentication path*: The extension checks the URL it visits against the authentication path and applies the configured setting if it is a match. The authentication path can only be part of the desired URL.

  For example, `/#login` can be added instead of `https://fortipam.ca/#login` to allow matching on various sites.
- *Field*: Represents the field from the secret to be patched to the element located by the selector.
  - *Web Element Selector*: Represents the selector for the element in HTML. This can be located with the inspect mode.
  - *Override Path*: Represents if the path should be searched for the selector instead of the authentication path.
  - *Mask*: Represents if there is a mask for the value to be filled in.
- *Token*: The token from the secret is patched to the element located by the selector.
  - *Attribute*: The token value.
  - *Web Element Selector*: Represents the selector for the element in HTML. This can be located with the inspect mode.
  - *Override Path*: Represents if the path should be searched for the selector instead of the authentication path.
  - *Mask*: Represents if there is a mask for the value to be filled in.

Also, more secret fields can be sent to the extension and auto filled during the login process as long as the token is used for 2FA.

The feature needs Microsoft Edge and Google Chrome extension V3.

963791- FortiGate web password change

A new *FortiProduct (Web)* default template available in *Secret Settings* > *Templates* for web based products, e.g., FortiGate and FortiProxy.

The *FortiProduct (Web)* default template includes a new *Web API (Product)* password changer.

959751- Block copy for web based launching

A new *Block Clipboard* option in the *Secret Setting* tab when creating/editing a secret in *Secrets* > *Secrets* and when creating/editing a secret policy in *Secret Settings* > *Policies*.

When enabled, for the following launchers, you cannot copy content from the launched secret web page:

- *Web Launcher*
- *Web SSH*
- *Web Telnet*
- *Web SMB*
- *Web SFTP*

When enabled, copying content from the remote computer to the local computer is blocked for the following launchers, but does not affect copy/paste on the remote computer itself:

- *Web RDP*
- Native *RDP*

Note that the previously available *Block RDP Clipboard* option in the *Service Setting* tab when creating/editing a secret and in the *New Secret Policy*/*Edit Secret Policy* window when creating/editing a secret policy in *Secret Settings* > *Policies* has been removed.

The feature needs Microsoft Edge and Google Chrome extension V3.

959751- Support `Ctrl+C/V` for Web RDP session

Starting FortiPAM 1.4.0, you can use copy/paste keyboard shortcuts (`Ctrl + c`/ `Ctrl + v`) without the need to first press `F8`.

The `Ctrl + c`/ `Ctrl + v` shortcut and right-click to copy/paste functionality are not yet supported on the Mozilla Firefox web browser.

Right-click to copy/paste is not yet supported on Google Chrome and Microsoft Edge web browsers.

The feature needs Microsoft Edge and Google Chrome extension V3.

1002904- Secure certificates as secrets

A new default *Certificate Vault* template is introduced in FortiPAM 1.4.0.

With the new default template *Certificate Vault*, you can store certificate with or without corresponding private key and passphrase in FortiPAM. The validity of this certificate will be monitored by FortiPAM.

Using the new *Certificate Vault* template, you can create secrets to store certificates in *Secrets* > *Secrets*.

The following new options are available when creating a secret using the *Certificate Vault* template:

- *Certificate* field.
- *Log Expiring Certificate* option in the *Secret Setting* tab: Enabling the option generates a log for an expiring certificate.

Disabling *Log Expiring Certificate* stops the generation of log entries for an expiring certificate.

In addition, email alerts for expiring certificates are stopped if you disable this option.

A new *Certificate* tab in *Log & Report* > *Email Alert Settings*.

Using the new *Certificate* tab, you can now set email alerts for expiring certificates.

890941- SSH filter Allow mode

In addition to the legacy (Deny) mode, an Allow mode has been added to accept certain commands and deny the rest.

The new Allow mode permits you to configure SSH profiles that will only allow certain SSH pattern commands to be executed while blocking other commands.

The *SSH Filter Profiles* in *Secret Settings* now include the following enhancements:

- Two new modes: *Deny*/*Allow*
  In *Deny* mode, the SSH command patterns configured in the SSH filter profile cannot be used. This means that these commands cannot be executed.

  In *Allow* mode, the SSH command patterns configured in the SSH filter profile can be used. This means that these commands can be executed while other commands will be blocked by FortiPAM.
- New *Log All Unlisted Commands* option.
- When in *Allow* mode, the following commands are available:
  - *Show Allowed List Command*: Customize command that will list all the commands under allowlist anytime.
  - *Shortcut To Run Listed Commands*: Shortcut to quickly run commands within the allowlist, the shortcut is the number within the list shown by *Show Allowed List Command* option.
- New `Exact-match` pattern type applicable to both *Deny* and *Allow* mode.
  This type of pattern will be exact matched on the SSH filter profile.

1022441- Ansible lookup plugin integration

For API users with an authentication token, the user gets an exact result with secret ID. Additionally, with the `credential_only` option, you can retrieve credential information for the secret without returning the complete secret information.

The Ansible integration enables user to retrieve secret with ansible playbook, and the secret information obtained through Ansible lookup helps the user to locate the desired secret information.

See *FPAM Ansible Lookup Plugin* to install and use FortiPAM Ansible plugin.

964436- Microsoft SQL Server Management Studio (SSMS) monitoring and logging

When editing a secret target that uses *Microsoft SQL* as the default template, you can enable logging on the SQL server, set the maximum log entry size, and monitor all or a specific database using the new *SQL Log* tab.

1044016- Launcher button refactor

When you open a secret, launchers are now available on the top, listed as icons.

Additionally:

- When you open a secret that requires check out, the *Check-out Secret* option is now replaced with the *Check-out* ( ) icon.
- When you open a secret to check it in, the *Check-in Secret* option is now replaced with the *Check-in* ( ) icon.
- When you open a secret, the *Change Password* option is now available under More options.
- When you open a secret, the *Verify Password* option has been replaced with the *Verify* ( ) icon.
- When you open a secret, the *Add/Remove Favorite* option is available under More options.
- When you open a secret that requires you to make a secret access request, the *Make Request* option is now replaced with the *Request* ( ) icon.

1027089, 971921, 1023868- Display privileged account for a target

When setting up a secret as a privileged account for a target, a new tooltip tells you if the target already has a secret set as privileged account. In that case, you cannot set the secret as a privileged account for the target.

When editing a secret target:

- You can see if the target already has a privileged account set up in the *Privileged Account* field.
- A new *Secret List* tab lists all the secrets associated with this target.

The *Host* column in *Secrets* > *Targets* has been renamed to *Target Address*.

990047- Print the system time on videos

A new *Video Time Watermark* option in the *Advanced* pane in *System* > *Settings*. The option allows you to add a watermark to the secret videos with time and timezone information.

A new `video-time-burn` global variable in `secret setting` allows you to include time and timezone information in secret videos.

Limitations:

1. The feature is unavailable when you use the *Fortinet Privileged Access Agent* extension only.
2. The feature is unavailable when you set up secrets using the *Web Account* template.

901040- Approve secret request from email

A new approval link added to the secret approval request email. The approver can use the link to approve or deny the secret access request from the email directly.

To support this, when creating/editing an approval profile in *Secret Settings* > *Approval Profile*, a new *Approval Link Expiry Time* option allows you to set the expiry time for the approve/deny link in the secret approval request email.

Note that the expiry time count starts when the email is sent.

1006338- Support ticket number in secret request

You can now create custom fields for an approval profile in *Secret Settings > Approval Profile*.

A new *Approval Email Customization* pane when creating or editing an approval profile.

The custom fields capture additional information necessary for the approval process tailored to the specific needs of your organization.

The custom fields are of two types, text/number.

The *Customized Email Template* option has been renamed to *Email Template*.

When a user makes a request to launch a secret where an approval profile with custom fields is used, they must specify the required custom fields in the *Fields* pane in the *New secret request* window.

See *Configuring and accessing a secret that uses an approval profile with custom fields* example in the latest *FortiPAM Administration Guide*.

1051104- WebTelnet in Secret Service Setting

FortiPAM now supports setting up web *Telnet Service* in the *Service Setting* tab when creating or editing a secret.

1042899- Windows application filter

Windows application filter is used in Windows server and provides the ability to deny users from installing applications, running certain applications and/or running certain scripts.

Denial is based on directories and usually all executables, scripts, or installers from those directories cannot run.

Exceptions can be added to provide flexibility.

Filters are based on secrets, and different secrets usually have independent filters.

You can add a Windows application filter profile and apply a certain profile to a secret to enable this feature on that secret. FortiPAM generates and maintains a set of application deny rules/filters for that secret.

When a Windows application filter is applied to a secret under a target, a new *Windows Application Filter* tab appears while editing the secret target.

In the new tab, you can see accounts in the secret target, filters applied to accounts, and settings to deactivate/delete all filters.

Prerequisites:

- The host server operates on Windows.
- WinRM is enabled on the host server.
- In FortiPAM, the host server is referred to as "target."
  The target has a privileged account for WinRM access on the host server.
- All secrets whose server information is “Windows” under this target, except for the privileged account, can be used to enable the Windows application filter.

1025126- User schedule based secret launch

A user configured with a schedule, i.e., the user can log in to FortiPAM depending on its schedule only, will have its launching session terminated when the user session exceeds the time set up in the schedule associated with the user.

A new *Terminate Launching Session* option available when configuring a schedule in *User Management* > *Schedule*.

970315- Secret import enhancement

To encourage managing secrets through targets, we now help find existing targets by matching fields— address, domain, or URL.

If non-matching fields are present, the import is considered a duplicate and will not proceed. Otherwise, a new target will be created.

If the secret upload template includes any of the following mandatory fields: *Host*, *Domain*, or *URL*, the corresponding target is modified or created (if applicable).

The new target is created with the naming convention: `import_(Host/Domain/URL).`

The failure to create a target results in the failure to create the corresponding secret.

When importing a secret, FortiPAM first scans if a corresponding target exists by matching *Host*, *URL*, and *Domain*.

If there is a match, FortiPAM chooses the matched target for the secret and creates the secret.

If there is no match, FortiPAM creates a new target automatically first and the target name is `import_[Host/Domain/URL]`. The secret is then created based on the newly created target.

User/Group

936798- Group creation time

A new *Creation Time* column in the following tabs in *User Management*:

- *User Groups*
- *Sponsored Groups*

The *Creation Time* column displays the date and time when a user group or a sponsored group was created.

802577- Support single login anytime anywhere

By default, a user account may be used to log in concurrently from multiple locations. For enhanced security, this setting can be disabled by disabling *Concurrent Log-on* in the *Other General Setting* pane in *System* > *Settings*. When you disable the setting, only one session is allowed per user.

Alternatively, in the CLI console, enter the following commands to disable concurrent login.

```
config system global
 set admin-concurrent disable
end
```

When an admin concurrent session is disabled:

- Additional concurrent admin sessions are blocked while an admin session is active (default)

OR

- FortiPAM automatically terminates any previous sessions when the admin opens a new session.

This behavior can be be changed when the `admin-concurrent` variable is disabled, allowing you to either block additional sessions or terminate (kick out) previous sessions when a new session is opened:

```
config system global
 set admin-concurrent disable
 set admin-new-login-action {block | kick-out} # default = block
end
```

Alternatively, use the *New Log-in Action* option when *Concurrent Log-on* is disabled in *System* > *Settings* to:

- Block additional concurrent admin sessions while an admin session is active (default).
- Terminate any previous sessions when the admin opens a new session.

System/Log

987628- Automatically backup in-use configuration before restoring a new configuration

FortiPAM automatically backs up the in-use configuration file before restoring a new one to avoid any data loss, e.g., when a wrong password is stored and the encrypted disk fails to open.

985502- Protect sensitive data with AES256

Starting FortiPAM 1.4.0, AES 256 cryptographic algorithm is used to protect passwords and keys.

902084- FTP support for video/log backup/restore

FortiPAM now supports backing up and restoring video and log files from a remote FTP server.

This displays videos and logs correctly when you want to replace the disks for video and log files.

923465- Add filters to the report layout

By using filters, you can now only keep relevant information in the report. The *Add Filter* dropdown shows available filter types for a table.

This helps you filter reports to only keep information that are relevant to you, e.g., secret name, folder, user, etc.

You can add the same or different filters multiple times.

Note that using the same filter generates union (or) results while different filters generate intersection (and) results.

When customizing a report layout in *Log & Report* > *Reports* > *General*, you can add filters for the following tables:

- *User Login*
  - *Top Failure By Reason*
- *Secret Launch*:

    - *Top Success By Secret*
    - *Top Success By Secret and User*
- *Password Change*
    - *Top Success By Secret*
    - *Top Success By Secret and User*
    - *Top Failure By Secret*
    - *Top Failure By Secret and Reason*
    - *Top Failure By Secret, User and Reason*
- *Password Verification*
    - *Top Success By Secret*
    - *Top Success by Secret and User*
    - *Top Failure By Secret*
    - *Top Failure By Secret and Reason*
    - *Top Failure By Secret, User and Reason*
- *Clear Text View*
    - *Top View By Secret*
    - *Top View By Secret and User*

949150, 989148, 842754, 901038, 935932- Network Interface GUI refactor

In *Network* > *Interfaces*:

- A new *Explicit Web Proxy* column is available.
- The *Administrative Access* column has been renamed to *Access*.

Editing an interface has now been simplified.

A new *Service Access Setting* pane is available when editing an interface.

The *ZTNA* tab options previously available in *Settings* are now available when editing an interface.

You can configure ZTNA (firewall policy, access proxy, and VIP) when editing and interface.

Due to the complexity of the ZTNA concept, related settings are available when to *GUI Portal* is enabled while editing an interface.

You can enable the *GUI Portal* toggle to provide external access to FortiPAM. The external access IP can be set in *External IP*. There are two modes for the external IP:

- *Sync with Interface IP*: Under this mode, the external IP address reflects the interface IP address after saving.
  Note: To use *Sync with Interface IP*, `extintf` must be configured to a specific interface in the CLI (not `any`).
- *Customize*: Under this mode, you can set a customized external IP address.
  The default setting is *Sync with Interface IP*.

The service port for external access is on the external IP, with the default port being `443`. The SSL certificate ensures secure authentication access to FortiPAM, with `Fortinet_SSL` as the default certificate.

ZTNA Control restricts access to endpoints with matching ZTNA tags. You can select the validation methods and tags from *ZTNA Tag Validation* and *ZTNA Tags*.

Each interface can have more than one matched external access *GUI Portal* configuration, but the FortiPAM GUI displays the best matched configuration on GUI including its VIP.

If the current interface does not have a matched access portal, you can also create a new access portal on the interface page.

Additionally, you cannot edit a proxy rule in the GUI anymore.

1019879- Show error on the GUI when there is log/video disk failure

The following two types of warning messages are available in the notifications dropdown in the FortiPAM banner on the top-right:

1. When one of the log/video disks or both log and video disks are not mounted properly, the disk is not available, and a warning appears.
2. When the log/video disk encryption status does not match the global disk encryption configuration, then the disk encryption format not matching warning appears.

When you click the warning message, you are sent to the *Log & Report* > *Disk Usage* page for more details on the warnings.

You can click the suggested CLI commands to see more disk status information and suggested solutions.

You must resolve these warnings before performing any task on FortiPAM.

The following lists all the possible warning messages:

Disk not available:

1. `Both the log disk and the video disk are not available.`
2. `The log disk is not available.`
3. `The video disk is not available.`

Disk encryption is not matching:

1. `Disk encryption is enabled but none is in encryption format.`
2. `Disk encryption is enabled but the log disk is not in encryption format.`
3. `Disk encryption is enabled but the video disk is not in encryption format.`
4. `Disk encryption is disabled but both are in encryption format.`
5. `Disk encryption is disabled but the log disk is in encryption format.`
6. `Disk encryption is disabled but the video disk is in encryption format.`

1004932- ACME/LE certificate support

You can now use Let's Encrypt and the ACME protocol to automate certificate creation and maintenance.

1014580- Automation stitch for email notifications

Using the new *Automation* tab in *Log & Report*, you can monitor secret activities and system events.

Nine default stitches can be used by enabling and adding your email to action.

You can customize stitches by specifying events and email receivers.

You can add triggers and actions to automation stitches.

885473- FortiToken Cloud trial support

A one-time 30-day trial FortiToken Cloud license is provided for users to try out the *FortiToken Cloud* 2FA method.

When creating a user in *User Management* > *User List* with *FortiToken Cloud* selected in *Two-Factor Authentication*, you can see the *FortiToken Cloud license* status.

Use the *Activate free trial* option to activate free trial licenses from FortiGuard.

When you go to *System* > *FortiGuard License*, a new entitlement *FortiToken Cloud* is available.

Select *Activate free trial* to activate the free trial with 5 FortiToken Cloud tokens.

The trial license is available for 30 days only. This information is displayed in *System* > *FortiGuard License* and when editing the user.

When in trial or when the license has expired, select *Upgrade* to see instructions on how to add a valid license. The option is available in *System* > *FortiGuard License* and when editing the user.

When the license has expired, you cannot use FortiToken Cloud. *FortiToken Cloud License* then displays *No active license* status when creating/editing the user.

FortiToken Cloud entitlement is marked *Expired* in *System* > *FortiGuard License*.

1037451, 1052825- Security status on GUI

FortiPAM now displays private data, vTPM, and log/video disk encryption status in the banner and in *System* > *Settings*.

868067- Log/video disk stats

A new *Disk Usage* tab in *Log & Report* that displays log and video disk usage as charts.

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.

Before upgrading from FortiPAM 1.3.0 to 1.4.0, check *Policies* in *Secret Settings*.

If the *SSH Filter* is enabled, disable and reenable with the SSH filter profile.

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

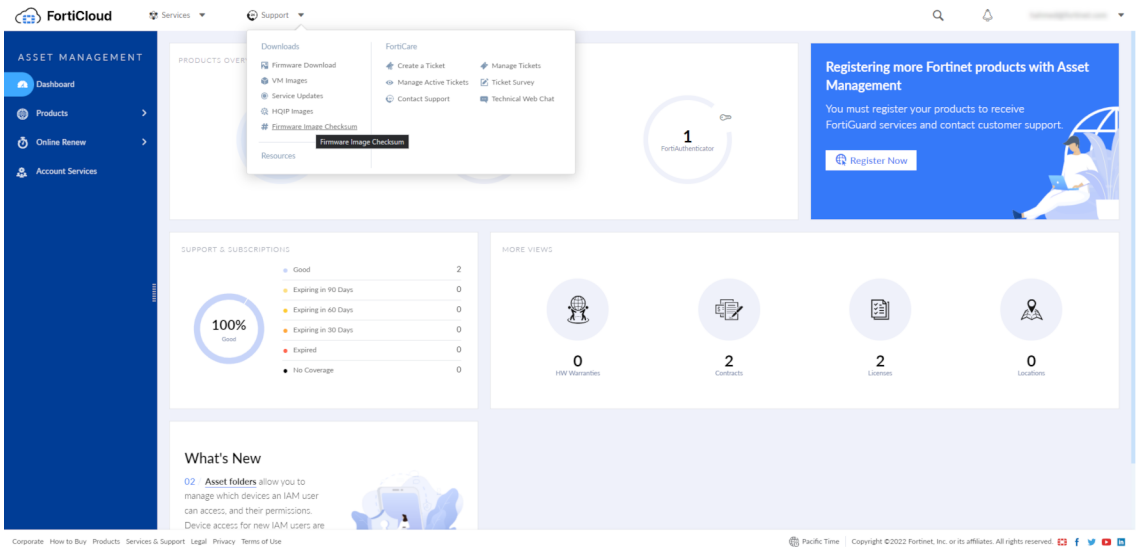
To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

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.x, upgrade to FortiPAM 1.2.0, and then upgrade to FortiPAM 1.4.0.
- From FortiPAM 1.1.x, upgrade to FortiPAM 1.2.0 and then upgrade to FortiPAM 1.4.0.
- From FortiPAM 1.2.0 upgrade to FortiPAM 1.4.0.
- From FortiPAM 1.3.0 upgrade to FortiPAM 1.4.0.

Product integration and support

FortiPAM 1.4.0 supports the following:

Web browser support

FortiPAM version 1.4.0 supports the following web browsers:

- Microsoft Edge version 126
- Mozilla Firefox version 114

  Note: Mozilla Firefox is supported with some limitations.

  See Known issues on page 29 for more information.
- Google Chrome version 126

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

Virtualization software support

FortiPAM version 1.4.0 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 1.4.0 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.

Secret/Launch

Bug ID	Description
1014549	WebSSH TOTP for FortiProduct.
1013311	If a template has been used by secret/target, fields in the template cannot be edited.
1027348	Web launcher auth token times out despite activity within the session.
1032313	Import secrets enhancements.
1042469	Fix for secret launch failed when gateway connected to EMS.
1030944, 1042010	Fix for missing approval profile.
1044907	Unable to access Cisco switches through Web SSH.
993129	SAML login remote user can use an SSO user in the web launcher without typing username/password again.
1037973	WinSCP file uploaded with an SSH filter crashes the WAD process.
1024441	Associated secret switching account is not working on Ubuntu server version.
1047340	Customize password prompt for switching account in the SSH session.
957802	Super Administrator Role should be able to override the standard user secret checkout without glass breaking.
1050100	Launcher SQL Server Management Studio (SSMS) v20.1.10.0 not supported.
1007307	Web proxy password replacement not working for vCenter.
993068	Secret launching does not record the screen for newly opened tabs except the first one (FortiClient 7.4.0).
1023562	Web user account stays signed in even after the PAM session is closed (FortiClient 7.4.0).

User/Group

Bug ID	Description
1041760, 1044544	Fix for LDAP token authentication error.
966330	Trusted Hosts are ineffective for API users.

System/Log

Bug ID	Description
990764	Flex licensing on EMS and EMS Cloud causes FortiPAM ZTNA tag lookup to fail.
1039791	Log level of daily operation should not be higher than the FortiPAM alert.
1018362	Out-of-bounds Write in sndproxy.
1011777	nghttp2 to 1.57.0.

Common Vulnerabilities and Exposures

Bug ID	CVE references
1056207	FortiPAM is no longer vulnerable to the following CVE-Reference(s): • CVE-2024-6387
940442	FortiPAM is no longer vulnerable to the following CVE-Reference(s): • CVE-2022-45862

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
930438	SSH CLI cannot be launched in non-proxy mode.
1043875	Credentials auto-fill not working for Azure web secrets (Firefox only).
1053383	Flexible web filler new feature not supported by Firefox (Firefox only).
1032684	Limitation in implementing Ctrl+C/V in a Web RDP session on the Firefox browser (Firefox only).
1052176	In a Windows secret with associated mode, sometimes, winrm event does not show up with video recording after terminating the launch.
1053436	After disabling Windows App Filter Profile on a secret, those applications are still blocked when launching a secret.
1056863	Web Account launching is not terminated after the schedule expires.

1054389	Reverse Gateway - FortiGate 7.6.0 cannot work in multiple wad workers (FortiGate 7.6.0).
	
	Workaround
	
	For ForitGate 7.6.0 with more than 1 CPU working as the reverse gateway, in the CLI console, set the wad worker count to 1:
	`config system global`
	`  set wad-worker-count 1`
	`end`

1015585	FortiClient completely closes MobaXterm application when a launched secret session reaches maximum duration (FortiClient 7.4.0).
1038568	Blank screen when live streaming or replaying recording for Web VNC on Mac OS (FortiClient 7.4.0).

User/Group

Bug ID	Description
1061739	A role with *NONE* permission for *Approval Profile* cannot see the fields when making a request.

Bug ID	Description
	Workaround: Escalate the standard user to higher role. OR Create a new customized role with higher permission for *Approval Profile* than *NONE*. This issue will be fixed in FortiPAM 1.5.0.

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