Release Notes

FortiPAM 1.1.0

May 15, 2024
FortiPAM 1.1.0 Release Notes
74-110-924351-20240515

TABLE OF CONTENTS

Change log

Date	Change Description
2023-06-28	Initial release.
2023-07-27	Removed bug 850496 from Resolved issues on page 25.
2023-11-23	Updated What' s new on page 7.
2024-01-09	Updated Resolved issues on page 25.
2024-05-15	Updated Resolved issues on page 25.

FortiPAM 1.1.0 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, resolved issues, and known issues for FortiPAM 1.1.0, build 0427.

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.

For additional documentation, please visit:

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

What' s new

FortiPAM version 1.1.0 includes the following enhancements:

842754, 899220- Simplified ZTNA GUI

ZTNA servers and new proxy rules can only be set via the CLI. You can use the GUI to edit existing proxy rules.

When editing a proxy rule, the *Edit Proxy Rule* window has been simplified:

- A new *Enable this rule* toggle added.
- A new *Access Proxy* pane added. The pane display the corresponding access proxy and the VIP.
- A new *ZTNA Control* pane added. *ZTNA Control* allows you to enable/disable ZTNA control for the rule being edited.

  The pane contains *ZTNA Tag* and *Match ZTNA tags* options.
- *ZTNA Server*, *Destination*, *Action*, *Protocol Options*, and *SSL/SSH Inspection* options have been removed.
- The *Logging Options* pane has been removed.

865722, 863356- New backup GUI options

FortiPAM now includes the following new GUI changes in *System* > *Backup*:

- A new *Port* field to enter the port number for the backup server.
- A new *Server Certificate Check* toggle to enable/disable server identity check.
- A new *Server CA Certificate* dropdown to select a server CA certificate for server certificate check.
- A new *Test Connectivity* button to test the connection to the backup server.

863268- DLP related settings can be set up using GUI

New *Data Leak Prevention* and *DLP File Pattern* tabs in *Secret Settings*.

FortiPAM now allows you to set up DLP sensors, DLP filter rules, and DLP file pattern using the GUI.

When creating or editing a secret in *Secrets* > *Secret List*, you can now enable/disable DLP using the new *DLP Status* toggle. If *DLP Status* is enabled, you can enforce a DLP sensor on the secret using the new *DLP Profile* dropdown.

879947, 884995, 883168, 876986, 877093- Secret related GUI updates

While creating a secret in *Secrets* > *Secret List*, you can now:

- Enter values in the *Field* pane for a secret template directly.
- In the *Service Setting* tab:

  - The *LDAPS Service* toggle has been removed.
  - A new *SFTP Service* toggle added.
  - The *SSH Service* toggle controls *Web SSH*, *Web SFTP*, *PuTTY*, and the *WinSCP* launchers.
  - The *RDP Service* toggle controls *Web RDP* and the *Remote Desktop-Windows* launchers.
  - The *VNC Service* toggle controls the *Web VNC*, *VNC Viewer*, and *TightVNC* launchers.
  - The *SAMBA Service* toggle controls the *Web SMB* launcher.
  - The *SFTP Service* toggle controls the *Web SFTP* launcher.
- The *Port* option has been renamed to *Use Template Default Port* in *SSH Service*, *RDP Service*, *VNC Service*, *SAMBA Service*, and *SFTP Service*.
- A new *Inherit ZTNA Control* toggle added to the *Secret Permission* tab.
- *Launch Device Control* toggle renamed to *ZTNA Control*.

When editing a secret:

- The *Edit Secret* window has been renamed to *Secret Details*.
- The *Undo Changes* button has been renamed to *Discard Changes*.

In *Secrets* > *Secret List*:

- The following additional column filters have been introduced:
  - *Target Address*
  - *Last Password Change*
  - *Last Password Verification*
  - *Auto Password Changing*
  - *ID*
- You can now reorder columns.
- The following new columns have been added:
  - *Target Address*
  - *Last Password Change*
  - *Auto Password Changing*

883808, 868242- Configuring RAID via CLI on FortiPAM 1000G/3000G

The FortiPAM hardware devices 1000G and 3000G are equipped with a hardware RAID card. Therefore, you can now check the RAID status for the FortiPAM hardware devices by entering `diagnose system raid status` command in the CLI console.

Use the `diagnose system disk health` CLI command to check the disk status for the FortiPAM hardware devices.

Use the `diagnose system disk info` CLI command to check the disk information.

You can now create a RAID-10 disk group on FortiPAM hardware device using the `execute raid create-and-format` CLI command.

Further, you can also hot swap failed disks on FortiPAM hardware devices.

883594, 898709- FortiPAM on Microsoft Hyper-V

FortiPAM now supports Microsoft Hyper-V virtualization software.

860158- New pages in Log & report: Antivirus and DLP

FortiPAM now offers antivirus and DLP related log information in *Log & Report*.

884593, 896564, 890817, 908686- General GUI reorganization

FortiPAM 1.1.0 includes the following general GUI updates:

- *Folders* has been renamed to *Personal Folder/Public Folder* and moved to *Secrets*.
- *My Requests* has been renamed to *My Request List* and moved to *Secrets*.
- *Request Review* has been renamed to *Approval List* and moved to *Secrets*.
- A new *Secret Settings* menu with:
  - *Templates*- renamed form *Secret Templates*. Previously available in *Secrets*.
  - *Launchers*- renamed from *Secret Launchers*. Previously available in *Secrets*.
  - *Policies*- Previously available in *Secrets*.
  - *Addresses*- Previously available in *Authentication*.
  - *Approval Profile*- Previously available in *Approval Request*.
  - *Password Changers*- Previously available in *Password Changing*.
  - *Password Policies*- Previously available in *Password Changing*.
  - *Character Sets*- Previously available in *Password Changing*.
  - *AntiVirus*- Previously available in *Security Profiles*.
  - *Data Leak Prevention*
  - *DLP File Pattern*
  - *SSH Filter Profiles*- Previously available in *Secrets*.
  - *Integrity Check*
- New *AntiVirus*, *Data Leak Prevention*, and *Debug Settings* pages in *Log & Report*.
- *Fabric Connectors* moved from *Security Fabric* to *Network*.
- New *FortiPAM License* and *FortiGuard License* tabs in *System*.
- *Approval Request* has been removed.
- *Password Changing* has been removed.
- *Authentication* has been removed.
- *Security Profiles* has been removed.
- *Security Fabric* has been removed.

902469, 887801- Send/approve/deny multiple secret/job requests

When sending a secret/job request from *Secrets* > *My Request List*, you can now send access requests for multiple secrets/jobs using the *Secret/Job* option in the *New secret request* window.

FortiPAM now also allows you to approve/deny multiple secret/job requests together in *Secrets* > *Approval List*.

Also, FortiPAM now gives you the option to either combine multiple secret request notifications as one email when sending the notification to a reviewer or send them as separate emails.

For this, a new *Send Multiple Secret Requests in* option is available in the *PAM Settings* pane in *System* > *Settings*.

854712- Client software integrity check

For every launcher in FortiPAM, you can now configure a client software entry in the new *Integrity Check* tab in *Secret Settings* to enable integrity checks.

When the integrity check fails, the launching stops and a prompt appears showing where to download a version of the client software based on your FortiPAM configurations.

New *Client Software* option when creating or editing a secret launcher in *Secret Settings* > *Launchers*.

New *Integrity Check* option when creating a secret launcher in the *Launcher* pane as you create a new template in *Secret Settings* > *Templates*.

Client software integrity check requires FortiPAM 1.1 and FortiClient 7.2.2.

914149- Secret name displayed when editing a secret

When editing a secret, the *Secret Details* window displays the name of the secret being edited in the title across all the tabs.

840512- Tooltip when the number of users exceeds the licensed seats

When you attempt to create a new user that exceeds the licensed seats, the *Status* option in the *Configure User Details* tab cannot be enabled.

As you hover over the *Enable* button, a tooltip appears, alerting you that the user cannot be enabled as you have exceeded your license seat.

On the bottom-left of the user definitions list, the number of enabled users and the total number of allowed users are displayed as a label. This label is green when seats are available. The label turns red when all the seats have been used up. Once the seats are used up, new users cannot be enabled without disabling enabled users.

865654, 885138, 810687- Allowed and blocked addresses

FortiPAM now allows you to set up a list of allowed and blocked addresses in the *Secret Permission* tab using the new *Address Filter* option when editing a secret in *Secrets* > *Secret List*.

Allowlist and blocklist can only be configured when the secret has one of its fields as *Domain* type.

904160- FortiPAM on Microsoft Azure

FortiPAM now supports the Microsoft Azure virtualization software.

804808- Time-based One-Time Password (TOTP) settings for secrets

FortiPAM now supports enabling/disabling TOTP settings from the *TOTP Setting* pane when creating a secret in *Secrets > Secret List*.

TOTP is used when the target server requires TOTP as the 2FA.

The TOTP settings can also be configured from the *TOTP Setting* pane when creating a secret template in *Secret Settings* > *Templates*. The TOTP configuration from a secret template can be then inherited by all the secrets using the template. It is also possible to override the secret template TOTP settings from within a secret configuration.

845099- New target only secret template

FortiPAM now offers a new *Target Only* default secret template. *Target Only* is a basic template for a secret that only manages the target host.

Instead of using a shared common account, the *Target Only* secret template allows users to use user specific login name and password to access a credential-less target only secret.

The template includes only target server related fields, i.e., *Host*, *URL*, and *Domain*.

When you launch a secret based on the *Target Only* template, you have the following two options:

- You can use the current user's general FortiPAM login credentials to finish the authentication to the target server, i.e., SSO mode.
  Note that the SSO mode only applies to user logins via the general mode, and MFA credentials (if any) are dismissed.
- Dynamically enter the credentials for the target server during secret launching.

⚠ SAML user authentication is not available for secrets based on the *Target Only* template.

903079- Launcher pane editable for default secret templates

FortiPAM now allows you to edit the *Launcher* pane for default secret templates in *Secret Settings* > *Templates*.

849255- Secret template access control

FortiPAM now allows you to control access to templates by setting up user and user group permissions when creating a secret template in *Secret Settings* > *Templates*.

891443, 893734- New default templates

In addition to the new *Target Only* default secret template, the following new default secret templates have been introduced:

- *Cisco XR Router*: A basic template for Cisco server with XR IOS.
- *ESXi Server*: A basic template for ESXi server using username and password.
- *Database Server*: A basic template for SQL server using SQL username and password authentication.

Note that only the *Launcher* pane of a default secret template can be modified.

893198, 897591, 853452- New default launchers

FortiPAM now includes the following new default secret launcers:

- *MYSQL CLI*: A MYSQL CLI launcher for `mysql.exe`.
- *Microsoft SQL CLI*: A MSSQL CLI launcher for `sqlcmd.exe`.
- *MySQL Shell*: A MYSQL CLI launcher for `mysqlsh.exe`.
- *PostgreSQL CLI*: A MYSQL CLI launcher for `mysqlsh.exe`.
- *SSH CLI*: An SSH CLI launcher for `ssh.exe`.
- *SecureCRT*: An SSH Client using SecureCRT.

Only the non-proxy mode is supported for database related CLI launchers.

Note that only the *Client Software* toggle/dropdown of a default secret launcher can be modified.

860209- Downloading debug logs and the new trace logs tool

FortiPAM now allows you to download the debug logs for troubleshooting from *Log & Report* > *Debug Settings*.

The trace log debug tool is available in the GUI in the *Trace Logs* pane in *Log & Report* > *Debug Settings*.

814300- Only enabled users listed

By default, FortiPAM now only lists enabled users in *User Management* > *User Definition*.

To see all the users in the user definition list, enable *Show all users*.

Note that you can disable a selected user by clicking *Disable*.

822815- Secret video download

From the new *Download* dropdown, FortiPAM now allows you to download secret videos in *Log & Report* > *Secret* > *Secret/Secret Video*.

848805- Timer when a secret request is granted access

When a secret request is approved, FortiPAM now displays a *Launcher Status* timer that shows the remaining time till you (as a requester) have access to the secret in:

- The *Secret Details* window when you double-click to open the secret from *Secrets* > *Secret List*.
- The *Editing secret request (Read Only)* window when you (as a requester) double-click to open the secret request from *Secrets* > *My Request List*.
- The *Approving secret request (Read Only)* window when you (as an approver) double-click to open the reviewed request in *Requests that are reviewed* column in *Secrets* > *Approval List*.

829558- Token Id for SSH logs

FortiPAM now displays the token ID for an SSH log in the new *Token Id* column in *Log & Report* > *SSH*.

New *Corresponding secret* and *Corresponding secret video* buttons available when you right-click an SSH log in *Log & Report* > *SSH*. The buttons take you to the corresponding secret log or the secret video log, respectively.

894252- Display status of a job

FortiPAM now displays the status of a job in the new *Status* column in *Secrets* > *Job List*.

891443, 893734- New default password changers

FortiPAM offers the following new default password changers:

- *Cisco XR Router*
- *ESXi Password*

881157- New customized user role type

FortiPAM now offers a new customized user role type.

A customized user has tailored permissions and restrictions to match their needs and responsibilities, allowing them to control access to features or pages based on assigned roles.

When creating a new user in *User Management* > *User Definition*:

- A new *Customized User* role type option when you create a new user.
- When the *Customized User* role type is selected, a new *Choose a custom defined Role* dropdown appears, allowing you to select a role from one of the available custom roles.

897541- Send critical system and general alerts to users

FortiPAM now allows sending critical system and general alerts to users via email.

When creating a new user in *User Management* > *User Definition* the following two new options are available in the *Configure User Details* tab:

- *Critical System Email Alert*: Enable/disable sending critical system alerts via email.
- *General Email Alert*: Enable/disable sending general alerts via email.

Note that the *Glassbreaking Notification* tab in *Log & Report* > *Email Alert Settings* has been renamed to *Critical System Notification*, and it now supports glass breaking and license expiry notifications.

886975- ZTNA based access control for folders

FortiPAM now allows you to set up ZTNA based access control for folders, i.e., access to the folder is controlled by ZTNA tags.

The following new options are available when creating a new folder in *Secrets*:

- *Inherit ZTNA Control*: Enable to inherit ZTNA control access permission from the parent folder.
- *ZTNA Control*: Enable to limit access by `ztna-ems-tag`.
- *Device Tags*: Add ZTNA tags or groups by which access to the folder is limited.
- *Device Match Logic*: Define the match logic for the device tags.

896115- New default user group

A new default user group named *everyone* is available.

By default, every user belongs to the new *everyone* default user group.

891441-Cloning secret policies

FortiPAM now allows you to clone existing secret policies (including the default secret policy) using the new *Clone* button in *Secret Settings* > *Policies*.

923636- Simplified system settings

System > *Settings* is now divided into two tabs:

- *General*: *Host name*, *System time*, and *PAM Settings* panes.
- *Advanced*: *User Password Policy*, *View Settings*, and *Email Service* pane.

Admin Session Timeout has been renamed to *User Session Timeout* in the *PAM Settings* pane.

The *Debug Logs* pane has been removed.

867443-Test email service

In *System* > *Settings*, you can now check if the email service was set up correctly by sending a test email using the new *Test Connection* button.

897542- Setting up login disclaimers in GUI

In *System* > *Settings*, you can now set up login disclaimers using the *Login Disclaimer* toggle and text box available in the *PAM Settings* pane.

The login disclaimer now also tells you when the last successful login occurred.

790421- Display number for the VNC service

FortiPAM now supports adding a display number as well as custom port for the VNC service.

When *VNC Service* is enabled in the *Service Setting* tab as you create or edit a secret in *Secrets* > *Secret List*, a new *Display Number* option is available when *Use Template Default Port* is enabled. The option allows you to enter the display number to be added to the VNC port defined in the template.

920458, 864749- Bypass secret request/approval process

FortiPAM now allows secret owners to bypass secret request/approval process.

When creating or editing a secret in *Secrets* > *Secret List*, a new *Bypass Approval* option is available when *Requires Approval to Launch Job* is enabled.

The option allows secret owners to bypass the secret request/approval process, i.e., secret owners do not require approval to launch secrets they own, given that *Bypass Approval* is enabled.

899609- Automation trigger settings

FortiPAM can now be configured to perform actions when an event log is triggered.

You can use `config system automation-trigger` CLI command to configure automation trigger settings.

904137- Alerts for license expiry

FortiPAM now allows you to set up email alerts for license expiry. You can set up the email alert in the *Critical System Notification* tab in *Log & Report* > *Email Alert Settings*.

When a FortiPAM license is about to expire, i.e., the license is expiring within the next 30 days; a warning dialog appears when you log in to FortiPAM.

Also, a red banner appears on the top once you are logged in, alerting you about license expiry.

For expiring Advanced Malware Protection and FortiCare support, license expiration email notifications and warnings are sent.

877321- Secure import of secrets

FortiPAM now allows you to securely import multiple secrets at once using the `fpam_secret.xlsm` secret upload template.

Before downloading, you can encrypt the secret upload template file for added security. When uploading the filled in secret upload template, you are asked the password to decrypt the template file.

Note that all the default secret templates are now supported. Also, you can now create a custom secret template in the secret upload template file.

FortiPAM deployment options

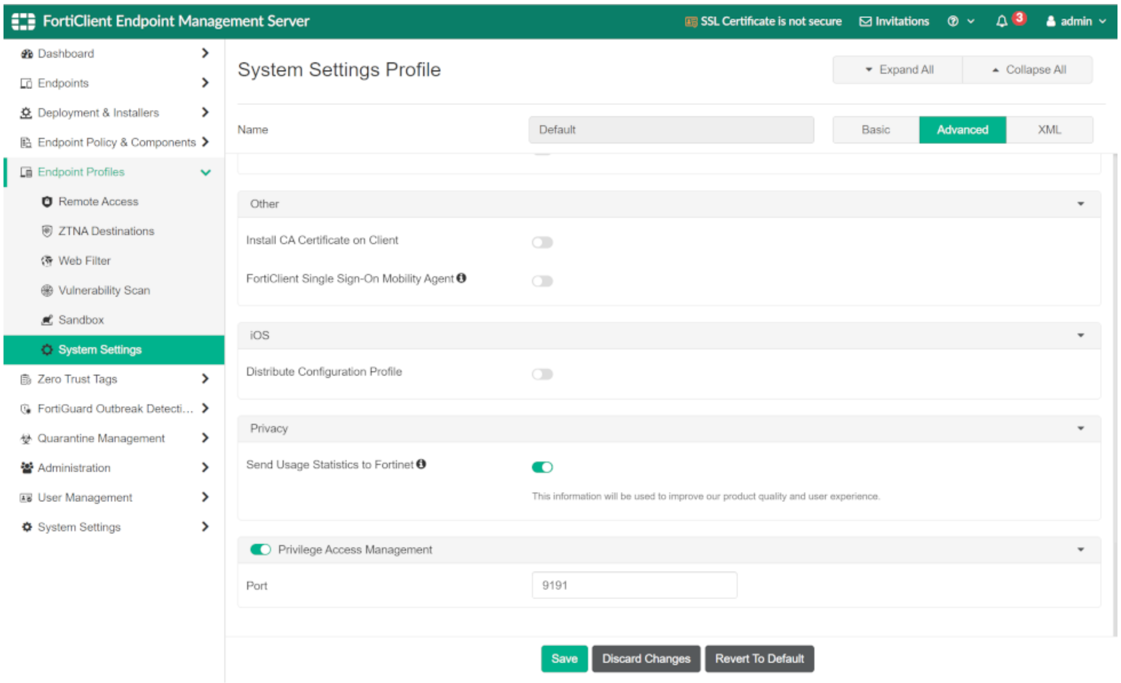
A full FortiPAM solution involves FortiPAM, EMS, and standard FortiClient. When both FortiPAM and FortiClient register to EMS, ZTNA endpoint control is available for secret launching and FortiPAM server access control. Both FortiPAM and the target server is protected by the highest security level.

When EMS is not available, standalone FortiClient is recommended. With standalone FortiClient, native launchers such as PuTTY, RDP, VNC Viewer, Tight VNC, and WinSCP can be used to connect to the target server and user can take advantage of functionalities provided by these applications. Also, video recording for user activity on the target server is sent to FortiPAM in real-time.

If FortiClient is not available, e.g., a user with Linux or MacOS system, Chrome and Edge extension called *FortiPAM Password Filler* is available on Chrome Web Store and Microsoft Edge Add-ons. On this extension-only setup, web-based launchers and web browsing are supported. The extension can record user activities on the target server.

On a system without FortiClient and browser extension, the user can still log in to FortiPAM and use the web-based launchers. However, all other features mentioned above are not available.

1. If EMS (7.2.0 or later) is available:
    a. **EMS Server**:
        i. Enable *Privilege Access Management*-
            i. Navigate to *Endpoint Profiles* > *System Settings*.
            ii. Edit the *Default System Setting Profiles*.
            iii. Select *Advanced* and enable *Privilege Access Management*.



System Settings Profile

Name: Default

Other
- Install CA Certificate on Client: off
- FortiClient Single Sign-On Mobility Agent: off

iOS
- Distribute Configuration Profile: off

Privacy
- Send Usage Statistics to Fortinet: on

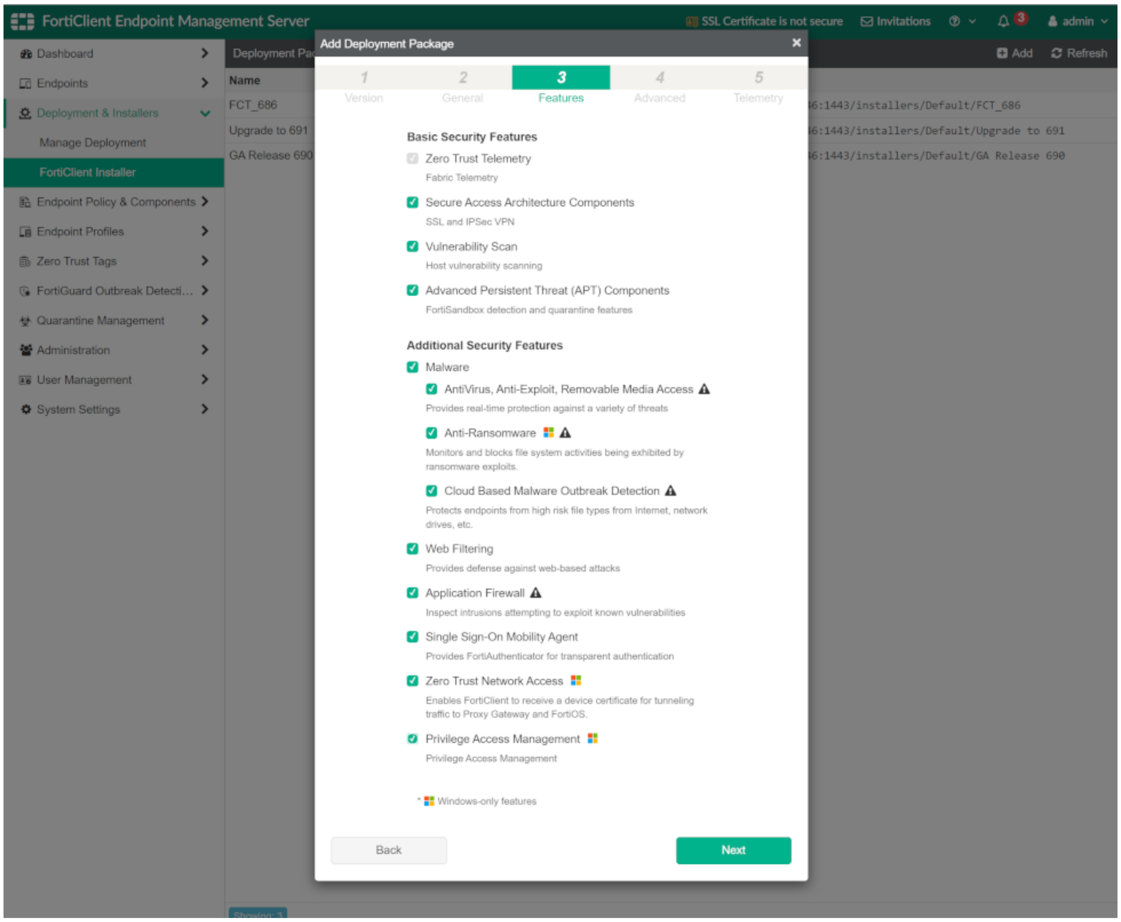
This information will be used to improve our product quality and user experience.

Privilege Access Management: on
- Port: 9191

ii. Push FortiClient (7.2.0 or later) to registered PC-

i. Navigate to *Deployment & Installers* > *FortiClient Installer*.

ii. Add a package with both *Zero Trust Network Access* and *Privilege Access Management* enabled on the third tab of the wizard.



Basic Security Features

☑ Zero Trust Telemetry
Fabric Telemetry

☑ Secure Access Architecture Components
SSL and IPSec VPN

☑ Vulnerability Scan
Host vulnerability scanning

☑ Advanced Persistent Threat (APT) Components
FortiSandbox detection and quarantine features

Additional Security Features

☑ Malware

☑ AntiVirus, Anti-Exploit, Removable Media Access ⚠
Provides real-time protection against a variety of threats

☑ Anti-Ransomware ⊞ ⚠
Monitors and blocks file system activities being exhibited by ransomware exploits.

☑ Cloud Based Malware Outbreak Detection ⚠
Protects endpoints from high risk file types from Internet, network drives, etc.

☑ Web Filtering
Provides defense against web-based attacks

☑ Application Firewall ⚠
Inspect intrusions attempting to exploit known vulnerabilities

☑ Single Sign-On Mobility Agent
Provides FortiAuthenticator for transparent authentication

☑ Zero Trust Network Access ⊞
Enables FortiClient to receive a device certificate for tunneling traffic to Proxy Gateway and FortiOS.

☑ Privilege Access Management ⊞
Privilege Access Management

* ⊞ Windows-only features

iii. Navigate to *Deployment & Installers* > *Manage Deployment* and apply the FortiClient installer package to select endpoint groups.

b. **Windows**: Download standard FortiClient (7.2.0 or later), and enable "ZTNA" and "PAM" functions during the installation. Full FortiPAM features are then supported.
After FortiClient registers to EMS, EMS can automatically deploy the configured FortiClient version to Windows PC.

c. **Linux and MacOS**: Install *FortiPAM Password Filler* extension from the Chrome Web Store or follow the FortiPAM GUI prompt. Then use web-based launchers or web launcher to access the target server.
Note: ZTNA and Native launchers are not supported on extension-only systems.

2. If EMS (7.2.0 or later) is not available:

a. **Windows**: After downloading and installing standalone FortiClient (7.2.0 or later) manually, most PAM features are supported.
Note: A standalone installer contains PAM in its filename such as `FortiClientPAMSetup_7.2.0.0xxx_x64.exe`.
Note: ZTNA is not supported.

b. **Linux and MacOS**: Install *FortiPAM Password Filler* extension from the Chrome Web Store or follow the FortiPAM GUI prompt. Then use web-based launchers or web launcher to access the target server.
Note: ZTNA and Native launchers are not supported on extension-only systems.

3. If FortiClient is not available (extension-only):
   a. **Windows**: Install *FortiPAM Password Filler* extension from the Chrome Web Store or Microsoft Edge Add-ons. Then use web-based launchers or web launcher to access the target server.
      Note: ZTNA and Native launchers are not supported on extension-only systems.
   b. **Linux and MacOS**: Install *FortiPAM Password Filler* extension from the Chrome Web Store or follow the FortiPAM GUI prompt. Then use web-based launchers or web launcher to access the target server.
      Note: ZTNA and Native launchers are not supported on extension-only systems.

   Note: Chrome or Edge web browsers are suggested for use as there is some limitation on Firefox extension-only deployment.

The following table lists FortiPAM 1.1.0 feature availability based on the type of deployment being used:

Feature	FortiPAM with standard FortiClient	FortiPAM with standalone FortiClient	FortiPAM with browser extension	FortiPAM only
Windows OS	✓	✓	✓	✓
Linux OS	X	X	✓	✓
MacOS	X	X	✓	✓
ZTNA	✓	X	X	X
Web-based launchers, i.e, Web-SSH, Web-RDP, Web-VNC, Web-SFTP, and Web-SMB (only supports proxy mode; credential protected in FortiPAM)	✓	✓	✓	✓
Proxy mode web browsing (credential sent to the extension with permission protection)	✓	✓	✓	X
Direct mode web browsing (credential sent to the extension with permission protection)	✓	✓	✓	X
Video recording	✓	✓	✓	X
Instant video uploading	✓	✓	✓	X

Feature	FortiPAM with standard FortiClient	FortiPAM with standalone FortiClient	FortiPAM with browser extension	FortiPAM only
Proxy mode native launchers, i.e, PuTTY, RDP, VNC Viewer, Tight VNC, and WinSCP (credential protected in FortiPAM)	✓	✓	X	X
Direct mode native launchers, i.e, PuTTY, RDP, VNC Viewer, Tight VNC, and WinSCP (credential delivered to FortiClient with permission protection)	✓	✓	X	X

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, upgrade the firmware, and then 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

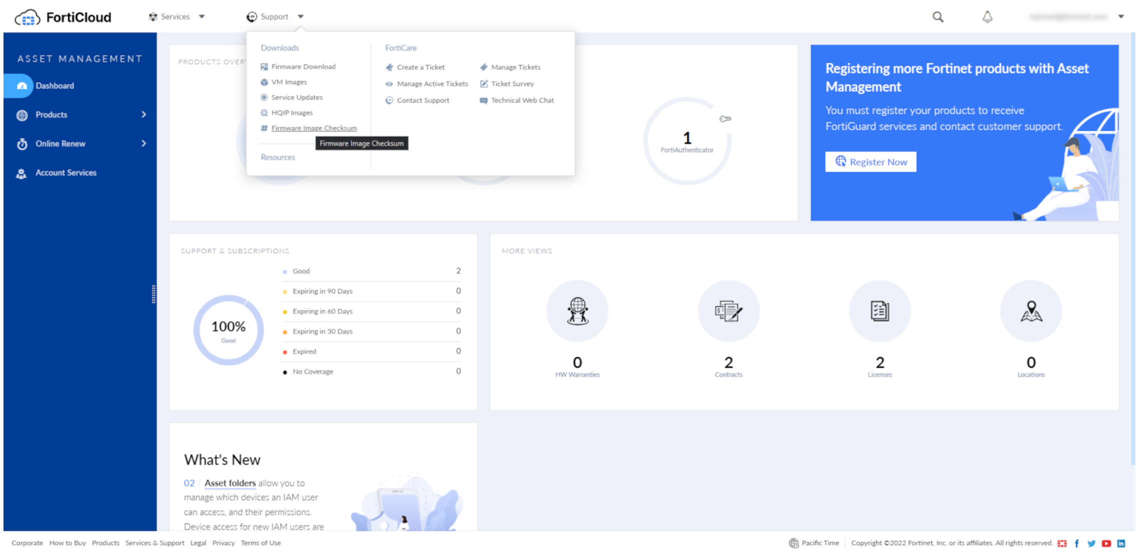
To verify the integrity of the firmware file, use a checksum tool to compute the firmware file’s MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

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

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.

Product integration and support

FortiPAM 1.1.0 supports the following:

- Web browser support on page 23
- Virtualization software support on page 23
- Hardware support on page 23

Web browser support

FortiPAM version 1.1.0 supports the following web browsers:

- Microsoft Edge version 114
- Mozilla Firefox version 114

  Note: Mozilla Firefox is supported with some limitations.

- Google Chrome version 114

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

Virtualization software support

FortiPAM version 1.1.0 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

Hardware support

FortiPAM 1.1.0 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 visit FortiCloud.

Bug ID	Description
927122	Client cert memory leak fix from FortiProxy.
926668	Wad crash when trying to allocate a zero length object.
925922	MySQL typo.
925112	Port from FPX: EMS Cloud Fabric Connector not working.
925675	Display create secret button in personal folder.
924904	WinSCP video file deleted if user clicks reconnect when current connection closed.
924771, 877090	Password changer crash.
924185	`FortiProduct (SSH Key) ` passphrase field is password type.
924967	wad crash when server side is disconnected
921159	Format string bug in httpsd and cli - automation test.
923591	Secret cannot be edited.
877321	Secret upload improvement.
922825	FortiPAM crashes when launching an associated secret to a Cisco server.
918137	Improved user authentication log and replacement message page.
923250	Refactor launch prompt error.
923237	Remove none option in template permission.
922963, 923131, 923599	Hide AV scan if no file launcher.
924403	wad crash when SFTP/SMB authentication request is expired or manually modified.
923988	Add upgrade function for alertemail mail to.
924050	Change the default value of inherit-folder-ztna to disable to avoid configuration lost in upgrade.
919761	Null pointer check to access permission table.
920067, 917965 919085, 920170 918877, 921268, 922752	The user does not have permission to use email service and other GUI issues.
922344	Folder permission validation.

Bug ID	Description
921938	Fix HA sync issue when user password policy is enabled.
921071	SSH auto password delivery fails with server Cisco_7200.
922584	Hide SSL_ERROR_SSL error messages from console.
920106	LDAP/RADIUS 2FA authentication failure.
921742	Format address array.
920257	Use the original client IP for trusted host checking.
920458	Bypass approval feature.
920610, 0920637, 0919554	folder list clone update count.
920506	WAD crash was observed.
920208	Launching web account (FortiGate+DNS+FQDN) logs out the current user
919596	In a folder with \`Add Secret\` and Secret \`List\` permission; clone a secret shows empty fields.
897253	Automatically identify the correct remote server to authenticate a remote user.
919179	Hide unnecessary service.
919670	User info daemon crash.
918890	In target-only, target-address field cannot be empty.
918865	Request enforced for all secrets
863569	Non-proxy PuTTy should be disabled when using an SSH key.
920035	Invalid 'Approved Access' in secret.
919135	WAD crash observed on CM build 0418.
919133	miglogd crash observed on CM build 0418.
896180	FortiPAM hardware license.
918116, 919678	Provide an extra customized http header for extension to indicate video has finished.
804808, 904559	Support totp in SSH authentication.
884593, 0896564, 0890817, 0908686, 0884633	Optimize the navbar menu structure.
915230	Add PAM disk conserve mode.
918418	When installing FortiPAM for the first time, incorrect prompt when enabling email notification.
918485	Allow % in secret url field.
918346	Edit totp html.

Bug ID	Description
913663	Occasionally, server list is stuck unless refreshed.
910784	Enable WebSMB service by default when creating a secret with template ' Unix Account (Web CIFS)'.
917965	api-user cannot add a secret job.
897541, 904137	Include email notification setting in the user wizard.
881157	Add new radio for user defined role in the user wizard.
882407	Job execution time display format issue.
0899609	Add regex and logic options to automation-trigger.
917750	Web app launching failure.
887801, 896115	Secret request refactor for multiple requests in one email.
914149	Add secret name on the title of edit page.
877321	Update template in upload xlsm.
887801, 908824	Add settings related to combine multiple requests into one email; support custom port for baseurl.
913639	Add authentication failure prompt to Web SSH.
886577, 0887801	Add user guide information for secret request email and vnc display number.
914744	HA heartbeat port mimics admin access configuration of port1.
887801	Combine multiple secret request notifications in one email to the approver.
915069	Mask password on release build.
899189	Display sudo disclaimer to user with SSH AUTO password.
914654	Update secret wad cache when template gets updated.
912655	PAM launching failure when NAT is in between.
798866, 913635	Job list execution status.
913523	Image restore from CLI failed when GUI pages are opened.
911223	Provide download blocking replacement message page to users for file blocked by av/dlp.
865654, 0885138, 0810687	Support AD restriction.
911262	Hide DLP settings in secret when AVDB license expires.
840512	Notify user when user number exceed licensed seats.
904137	License expiration notification and restriction.
903079	Enable editing the launcher for default secret templates.

Bug ID	Description
827628	Secret edits fail after cloning.
908671, 912019	FortiPAM HTTP video storage backend refactor.
908444	Allow creation of api-user with schedule.
904438	Check secret duplication before clone.
897591, 853452	Add CLI launchers.
854712	Client software integrity check CLI support.
902469	Support multiple requests
899189	SSH auto password does not support sudo with disclaimer.
860158	Support Logs of AV and DLP on GUI.
905335	Support AntiVirus and DLP license validation check in the scan procedure of file transfer launchers.
912775	Grey out non-editable DLP default sensors.
914061	Missing DLP uploading file logs for `Content_Archive` and `Content_Summary` when launching WebSFTP and WebSMB.
845099	Add target only secret template.
868233, 866748	Multiple file transfer launchers cannot be launched within a single browser at the same time.
906492	Remove disclaimer failed login information.
893740	Modify table size for a different platform.
913687	User unable see secret when they do not have access to the template.
864749	Allow owner to bypass secret approval process.
814300	Improvements on user delete.
822815	Provide a way to explicitly download a secret video from the log page.
847167	Prohibit deleting a root personal folder from the GUI.
874509	Add validators for checking ssh private and public key format.
896096	Hide address types not needed when creating a new address or an address group.
897188	Web Launcher restriction not working.
906942	AWS account creation requires more validation.
911230	Add file size unit for DLP large-file.
910813	Multiple launchings with customized templates.
910780	Unnecessary 'Launch' button.

Bug ID	Description
910297	Adding field type check for sensitive information field when switching templates.
905935	wad crash is observed; wad_aio_module_close closes during stress.
897304	Inherited folder permission should show up in details.
849255	Template and database user filter.
909683	Change all the FortiGate names in VMware ovf files.
909693	If the first firewall policy is disabled, FortiPAM GUI becomes unavailable.
848805	Display remaining time for approved requests.
893730	SSH launching fails after password change for the SSH key using template with password and passphrase.
910367	Optimize secret approval flag in the GUI API.
829558	Add two buttons that could go to the secret /secret video log page with targeted Token ID.
867911	Check RAID disk status every 5 minutes.
909198	PuTTY SSH connecting failure with the FortiTester server.
907267	Add a new parameter for the WinSCP launcher: `/newinstance`.
894252	Add status column for the job listing page.
851587	After running the `execute shutdown` CLI command on FortiPAM 3000G, it does not powered off and its console still echoes the received characters even after being halted.
909718	Format tje string bug in Fclicense daemon.
910007	DLP profile is invisible to standard users.
908190	Grey out the default password changers from the GUI.
879947	WebSFTP and WebSMB cannot be controlled from Service Setting.
909860	Failed to create a customized launcher.
898516	Add the Hyper-V faceplate layout.
872884	Application type in the log for WebSFTP and WebSMB is missing.
865722, 863356	Add the certificate related attribute and test connection to server button.
893484	After the factory reset, the GUI is not available from the default IP address.
802577	Single concurrent session to logout from all wad workers.
902540	The SSH logs page is showing previously displayed secret logs.
907427	Upgrade liburing to latest release version 2.3.
872589	Current system time is not correct when manually setting the time.

Bug ID	Description
907485	The FortiPAM HTTP module is unable to receive complete HTTP POST body from FortiClient's uploaded video.
789786	Fatal error: unable to find "node_mod_common.h" during parallel build.
900435	Unable to delete the last entry of IPv4 trusted hosts for the user.
907101	Correct the typo in New user Definition(1.1).
904443	Able to create identical folder in FortiPAM.
906449	GUI stuck while opening a file with auto-password enabled.
897542	Option to enable/disable the admin login disclaimer and modify the corresponding text.
878078	Extesion Only: If launching a secret with Web SSH or Web FTP; only one session is recorded.
877879	Update the secret name on the favorite menu after changing the secret name in the edit page.
865931	LibGD to 2.3.3.
906156	Failed to create a new user.
905640	Enhance to forbid empty cluster password.
905233	RDP connection failure on the hardware box when recording.
865931	tcpdump vulnerabilities - precaution upgrade to 4.99.1.
886975	Add ZTNA secret launch control on folder.
894302	Separate settings for RADIUS/FAZ when using DR.
879947	Add SFTP service control.
897541	Include email notification setting in the user wizard.
882636, 902400, 865931	Upgrade OpenSSL to 3.0.8.
848549	Add a hint message for `Cisco Enable Secret` when no user secret is associated.
848549	New everyone default user group.
896750	Extend the shell prompt.
878581	When the admin is under the glass breaking mode, request status is not correct after the admin approves the request.
903204	Return the correct port media for FortiPAM3000G/1000G.
874662	SSH procedure needs at least one 'expect' field to work.
901345	When disabling the proxy mode on an SSH key secret, all the default launchers should be disabled.

Bug ID	Description
872781	New access control option for disabling the non-proxy mode.
790421	VNC display variable support.
879582	When the FortiPAM feature is disabled in the EMS, the GUI should display an error message.
862589	Invalid alarm for a secret launching from a non-certificate client.
865453	When failed to connect to FortiClient; no prompt on Chrome.
861389	When there is no ForitClient and the user tries to launch the native launcher; should report an error.
860158	Support logs for AV and DLP on the GUI.
863268	Support DLP configuration on the GUI.
886975	Add "device control by ZTNA Tag" for folders.
902676	WAD SSH proxy could not connect to the Cisco router with KEX "diffie-hellman-group-exchange-sha1" + cipher "aes192-cbc".
893026	Timestamp of log when it is in DST.
865931	Use the correct package signatures.
817957	Update log summary time frame to 7 days.
892493	Change the faceplate port type to fiber to fit the appearance.
867443	Send test emails.
899908	Show "warning" or "disclaimer" when the admin logins to the interface IP address.
901484	Edge case for secret editing.
897253	Remove auto add LDAP/RADIUS server into the default authentication scheme database.
896177	Add FortiPAM upgrade code (template srv-info).
865931	Upgrade the KRB5 version to 1.19.4.
868811	Remove the downgrade configuration migration function.
865931	Upgrade sqlite version to 3.39.2.
849255	Template permission control.
810799	RDP restricted admin mode cannot auto log in to Windows 10/11.
865931	Upgrade curl to 7.86.
865722, 863851	Add certificate validation to automatic backup.
901632	Accept FortiPAM 1.0.x HA member if HA group passwd is empty.
842754, 899220	ZTNA layout enhancement.

Bug ID	Description
865931	Upgrade OpenLDAP version to 2.6.3.
893198	New SecureCRT launcher.
858229, 832286	Only display the entry of public folder list and personal folder; routing enhancement.
865313, 882312	Delete 'SSH Auto-Password' tooltips and delete the job page web API text.
882077	Change FortiGate to FortiPAM on VMware ovf files.
884542	Adding the network diagnose tools support.
893123	FortiPAM 1000G/ 3000G: No disk information, disk health, disk attributes, and disk errors commands on FortiPAM OS.
863354	Add port option to the backup server.
880074	When creating a new role, present the standard user's setting.
883168	Enhancement for Secret List view.
891436	Secret search under associated secret does not work.
890272	Enhancement on managing auto password changing.
893913	View button disappears for credential history.
845705	Allow launching secrets when admin is in the glass breaking mode.
879947	Add SFTP service setting.
863198	Update secret verification status after verification.
845087	Edit View tabs: Place actions above tabs.
891441	Add secret policy clone functionality.
805806	Syntax limitation: The format of [Variable] or Variable# is not allowed.
865012	Remove web launchers from the launcher type drowdown.
896180	Hardcode initial seats to 1000G/3000G.
889961	Support GPT partitions and EXT4 file systems for KVM and VMware platforms.
893356	Update API version to match the firmware version.
849255	Support template clone and add permission flag for template response.
892493	Rearrange port to fit machine appearance.
884631	Rename 'Launch Device Control' to 'ZTNA Control'.
883808, 868242	FortiPAM 1000G/3000G hardware RAID CLI `execute raid create-and-format` and `diagnose system raid status` commands.
896615	Fix FortiToken cloud issue on manually inputting a wrong token.

Bug ID	Description
876725, 840559	Escape special characters in navigation URL.
883477	Use reply-to email as sender address.
871639	Support FortiToken mobile push configured on the FortiAuthenticator side.
893897	Change password visibility process.
893696	SSH auto password does not work when both key and password exist for a secret without an associated secret.
883565	Command log shows the wrong Login user for Web SSH.
877090	Moving multiple secrets and give the option of displaying failed secrets.
849255	Template permission support.
877321	Improve upload procedure to support other templates.
876120	Add commands for web launcher proxy (web-authentication).
891441	Add clone flag to secret policy.
841234	Limit the number of characters in name and email fields to 64.
874658	Prevent job new-line from reverting to the default password changer.
889961	Support GPT partitions and EXT4 file systems for KVM and VMware platforms.
894051	Adjust the secret list API handler so the GUI does not fail.
865731	Set maximum body size for the internal API.
891001	Authentication configuration mandatory field need to be highlighted.
877131	Secret creation/cloning attribute not maintained.
817710	GUI should show the full log message and would be better if the log messages only show changed configurations.
890376	Web SSH crashes when using associated secret authentication.
889900	SSH secret with PuTTY launcher in the proxy mode fails when authenticated with an associate secret.
872781	New access control option for disabling the non-proxy mode.
888479	Fix the secret UUID in the log.
891206	Remove the domain field in the login page when SAML is not configured.
884995	Rename 'Edit Secret' and 'Undo Changes'.
890568	Delete the 16-bit option recording color depth.
827547	When launching on the Cisco OS with Web SSH, the behavior of 'space' and '?' in keyboard are different with normal PuTTY or console.
818585	Web SSH cursor issues.

Bug ID	Description
891437	Web SSH cursor is not at the correct position.
865237	The Launch Secret button and the `pwd-chg-sch-start-date` field are not acting correctly for the secrets created from CLI with automatic password changing set up.
875742	Information error for Web SSH/RDP/VNC.
883168, 876986, 877093	Secret list improvements.
860209	Wad trace GUI API support.
863356	Send test backup function to apache.
872633	Upgrade libssh2 to project trunk build.
876120, 869866	Web proxy keywords table.
885478	Revise layout in secret field so it is easier to edit.
873888	User with view permission to a secret with the 'View Encrypted information' role should be able to view secret password and key.
813008	New Secret > Allow for template switching without field conversion slide.
876629	SSH filter issues.
845705	Allow glass breaking user to launch any secret.
859888, 876121	Restrict the user from upgrading the account profile to a permission higher than they have.
864930	Prevent cmdb from adding a concurrent request.
875356	Allow check-out after check-in.
878496	Support right click to disable/enable a user.
879947	WebSFTP and WebSMB cannot be controlled from Service Setting.
882360	Password policy should not be available when the password changer type is 'SSH with Public Key'.
867177	Hide the Expires column by default in Monitor > Active Sessions.
867443	Add test email function to FortiPAM.
885138	Prevent blocklist and allowlist from being set at the same time.
865931	Port FortiOS ECO 218884: Openssl 3.0.
868521	When creating or cloning a launcher, 'File Launcher' setting is not available on the GUI.
877002	Add FQDN information in email notifications.
790421	VNC dsplay variable support.

Bug ID	Description
810687	Add blocklist/allowlist to GUI API.
865012	Prevent user from setting up a web-app launcher to non-default launcher.
877355	Dynamic FQDN sometimes does not work for Web RDP.
877460	Enable SMS option in the user wizard.
870808	AV Profile not loading value.
879074	Wad crash when no passphrase field in the template.
874851	CLI does not show the FortiClient EMS endpoint in the available options to configure. Also, the CLI is missing 'autocomplete' for the feature.
862156	Change permission for the RADIUS test connection.

Common Vulnerabilities and Exposures

Bug ID	CVE references
912019	FortiPAM 1.1.0 is no longer vulnerable to the following CVE-Reference(s): • CVE-2023-37934
919845	FortiPAM 1.1.0 is no longer vulnerable to the following CVE-Reference(s): • CVE-2023-36640

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 inquires about a particular bug, please visit FortiCloud.

Bug ID	Description
918409	Unable to create a new FortiToken Mobile on FortiPAM.
925112	FortiPAM does not fetch Account Contracts making EMS Cloud connector unavailable (GUI not available).
920865	FortiAnalyzer blocking GUI from loading.
921268	Login idle duration exceeds the limit.
911759	Firefox: TOTP with FortiToken Cloud fails with Web SSH due to repeat authentication request.
873459	Native RDP does not support the RDP authentication method.
916914	Possible secret inconsistency if heartbeat between primary and DR is broken.
918897	Failed to create and edit new files in the proxy mode WinSCP launcher.
920513	ZTNA error from FortiClient when launching a DNS unresolvable URL.
889750	Web SSH errors out on heavy terminal output.
814127	FortiPAM is unable to launch native applications when VIP port is not 443.
905232	`config system storage` CLI command does not work after creating software raid-10.

Maximum values 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 Table-instance limit [1] (VDOM limit) [2] [Global limit][3]	FortiPAM 1000G	FortiPAM 3000G	FortiPAM-VM
Secret			
Folder	2000 (2000) [2000]	6000 (6000) [6000]	6000 (6000) [6000]
Database	5000 (5000) [5000]	10000 (10000) [10000]	10000 (10000) [10000]
Request	5000 (5000) [5000]	10000 (10000) [10000]	10000 (10000) [10000]
Secret launcher			
Initial commands	64 (0) [0]	64 (0) [0]	64 (0) [0]
Clean commands	64 (0) [0]	64 (0) [0]	64 (0) [0]
System			
Zone	0 (200) [0]	0 (500) [0]	0 (500) [0]
Zone interface	0 (0) [0]	0 (0) [0]	0 (0) [0]

Features Table-instance limit [1] (VDOM limit) [2] [Global limit][3]	FortiPAM 1000G	FortiPAM 3000G	FortiPAM-VM
Interface	0 (0) [8192]	0 (0) [8192]	0 (0) [8192]
Interface secondary IP address	32 (0) [0]	32 (0) [0]	32 (0) [0]
Interface IPv6 prefix list	32 (0) [0]	32 (0) [0]	32 (0) [0]
Interface DHCP snooping server list	255 (0) [2048]	255 (0) [2048]	255 (0) [2048]
Account profile	0 (0) [64]	0 (0) [64]	0 (0) [64]
Admin	0 (0) [1000]	0 (0) [3000]	0 (0) [3000]
SNMP community	0 (0) [3]	0 (0) [3]	0 (0) [3]
SNMP community hosts	16 (0) [0]	16 (0) [0]	16 (0) [0]
SNMP community hosts6	16 (0) [0]	16 (0) [0]	16 (0) [0]
SNMP user	0 (0) [32]	0 (0) [32]	0 (0) [32]
Session TTL port	0	0	0

Features Table-instance limit [1] (VDOM limit) [2] [Global limit][3]	FortiPAM 1000G	FortiPAM 3000G	FortiPAM-VM
	(512) [0]	(512) [0]	(512) [0]
DHCP server	0 (1024) [0]	0 (4192) [0]	0 (4192) [0]
DHCP server options	30 (0) [0]	30 (0) [0]	30 (0) [0]
DHCP server reserved address	0 (5000) [0]	0 (5000) [0]	0 (5000) [0]
DHCP server IP range	3 (0) [0]	3 (0) [0]	3 (0) [0]
DHCP server exclude range	16 (0) [0]	16 (0) [0]	16 (0) [0]
MAC address table	0 (2000) [0]	0 (2000) [0]	0 (2000) [0]
ARP table	0 (16834) [16834]	0 (16834) [16834]	0 (16834) [16834]
Proxy ARP	0 (256) [0]	0 (256) [0]	0 (256) [0]
TOS based priority	0 (16) [0]	0 (16) [0]	0 (16) [0]
DSCP based priority	0 (64)	0 (64)	0 (64)

Features Table-instance limit [1] (VDOM limit) [2] [Global limit][3]	FortiPAM 1000G	FortiPAM 3000G	FortiPAM-VM
	[0]	[0]	[0]
Replacement message group	0 (200) [0]	0 (200) [0]	0 (200) [0]
Central management server list	100 (0) [0]	100 (0) [0]	100 (0) [0]
Replacement message images	0 (0) [21]	0 (0) [21]	0 (0) [21]
SAML service-providers assertion-attributes	4 (0) [0]	4 (0) [0]	4 (0) [0]
DNS server hostname	4 (0) [0]	4 (0) [0]	4 (0) [0]
DDNS server IP	4 (0) [0]	4 (0) [0]	4 (0) [0]
VDOM DNS server-hostname	4 (0) [0]	4 (0) [0]	4 (0) [0]
DNS database	0 (4096) [0]	0 (4096) [0]	0 (4096) [0]
DNS IPS URL filter	0 (0) [20]	0 (0) [20]	0 (0) [20]
DNS6 IPS URL filter	0 (0) [20]	0 (0) [20]	0 (0) [20]

Features Table-instance limit [1] (VDOM limit) [2] [Global limit][3]	FortiPAM 1000G	FortiPAM 3000G	FortiPAM-VM
GRE tunnel	0 (0) [0]	0 (0) [0]	0 (0) [0]
VXLAN	0 (0) [0]	0 (0) [0]	0 (0) [0]
User			
RADIUS server	0 (10) [0]	0 (10) [0]	0 (10) [0]
pop3	0 (10) [0]	0 (10) [0]	0 (10) [0]
RADIUS accounting server	4 (0) [0]	4 (0) [0]	4 (0) [0]
TACACS+ server	0 (10) [0]	0 (10) [0]	0 (10) [0]
LDAP server	0 (64) [0]	0 (64) [0]	0 (64) [0]
SAML server	0 (10) [0]	0 (10) [0]	0 (10) [0]
FortiTokens	0 (0) [1000]	0 (0) [5000]	0 (0) [5000]
Local	0 (5000) [0]	0 (0) [0]	0 (0) [0]

Features **Table-instance limit** [1] **(VDOM limit)** [2] **[Global limit]**[3]	**FortiPAM 1000G**	**FortiPAM 3000G**	**FortiPAM-VM**
Peer	0 (5000) [0]	0 (0) [0]	0 (0) [0]
Peer user group	0 (5000) [0]	0 (5000) [0]	0 (5000) [0]
Peer user group members	50000 (0) [0]	50000 (0) [0]	50000 (0) [0]
Address groups	0 (1024) [1024]	0 (8192) [8192]	0 (8192) [8192]
User FSSO polling address groups	0 (1024) [0]	0 (8192) [0]	0 (8192) [0]
User group	0 (2000) [0]	0 (5000) [0]	0 (5000) [0]
User group members	3000 (0) [0]	3000 (0) [0]	3000 (0) [0]
User group guests	1024 (0) [0]	1024 (0) [0]	1024 (0) [0]
FSSO	0 (5) [0]	0 (5) [0]	0 (5) [0]
FSSO polling	0 (100) [100]	0 (100) [100]	0 (100) [100]
Web filter FortiGuard local	0	0	0

Features Table-instance limit [1] (VDOM limit) [2] [Global limit][3]	FortiPAM 1000G	FortiPAM 3000G	FortiPAM-VM
	(52) [0]	(52) [0]	(52) [0]
Firewall			
Address	0 (40000) [40000]	0 (100000) [100000]	0 (100000) [100000]
IPv6 Address	0 (40000) [40000]	0 (100000) [100000]	0 (100000) [100000]
Custom wildcard FQDN	0 (512) [512]	0 (512) [512]	0 (512) [512]
Wildcard FQDN group	0 (512) [512]	0 (512) [512]	0 (512) [512]
Proxy address	0 (24576) [24576]	0 (24576) [24576]	0 (24576) [24576]
Service custom	0 (1024) [0]	0 (4096) [0]	0 (4096) [0]
Service group	0 (4000) [0]	0 (10000) [0]	0 (10000) [0]
Service group member	300 (0) [0]	300 (0) [0]	300 (0) [0]
Onetime schedule	0 (5000) [0]	0 (5000) [0]	0 (5000) [0]

Features Table-instance limit [1] (VDOM limit) [2] [Global limit][3]	FortiPAM 1000G	FortiPAM 3000G	FortiPAM-VM
Recurring schedule	0 (1024) [0]	0 (1024) [0]	0 (1024) [0]
IP pool	0 (512) [0]	0 (512) [0]	0 (512) [0]
Profile group	0 (1000) [1000]	0 (20000) [20000]	0 (20000) [20000]
Profile protocol options	0 (500) [500]	0 (500) [500]	0 (500) [500]
SSH profile	0 (500) [500]	0 (500) [500]	0 (500) [500]
SSH profile SSL exempt	255 (0) [0]	255 (0) [0]	255 (0) [0]
Firewall VIP	0 (32768) [32768]	0 (32768) [32768]	0 (32768) [32768]
VIP monitor	5 (0) [0]	5 (0) [0]	5 (0) [0]
VIP real servers	64 (0) [0]	256 (0) [0]	256 (0) [0]
VIP real servers monitor	5 (0) [0]	5 (0) [0]	5 (0) [0]
VIP group	0	0	0

Features Table-instance limit [1] (VDOM limit) [2] [Global limit][3]	FortiPAM 1000G	FortiPAM 3000G	FortiPAM-VM
	(500) [0]	(500) [0]	(500) [0]
VIP group member	500 (0) [0]	500 (0) [0]	500 (0) [0]
IP MAC binding table	0 (2048) [0]	0 (2048) [0]	0 (2048) [0]
Address group	0 (20000) [20000]	0 (20000) [20000]	0 (20000) [20000]
Address group IPv6	0 (20000) [20000]	0 (20000) [20000]	0 (20000) [20000]
Address group member	1500 (0) [0]	0 (0) [0]	0 (0) [0]
Proxy address group	0 (4096) [4096]	0 (4096) [4096]	0 (4096) [4096]
Proxy address group member	24000 (0) [0]	24000 (0) [0]	24000 (0) [0]
SSH host key	2000 (0) [0]	2000 (0) [0]	2000 (0) [0]
SSH local key	0 (100) [0]	0 (100) [0]	0 (100) [0]
SSH local CA	0 (100)	0 (100)	0 (100)

Features Table-instance limit [1] (VDOM limit) [2] [Global limit][3]	FortiPAM 1000G	FortiPAM 3000G	FortiPAM-VM
	[0]	[0]	[0]
Policy	0 (100000) [100000]	0 (200000) [200000]	0 (200000) [200000]
Custom log fields	5 (0) [0]	5 (0) [0]	5 (0) [0]
Poolname	64 (0) [0]	64 (0) [0]	64 (0) [0]
VIP6	0 (32768) [32768]	0 (32768) [32768]	0 (32768) [32768]
VIP6 monitor	5 (0) [0]	5 (0) [0]	5 (0) [0]
VIP6 real servers	32 (0) [0]	32 (0) [0]	32 (0) [0]
VIP6 real servers monitor	5 (0) [0]	5 (0) [0]	5 (0) [0]
VIP6 group	0 (500) [0]	0 (500) [0]	0 (500) [0]
VIP6 group member	500 (0) [0]	500 (0) [0]	500 (0) [0]
Central SNAT map	0 (30000) [30000]	0 (30000) [30000]	0 (30000) [30000]

Features Table-instance limit [1] (VDOM limit) [2] [Global limit][3]	FortiPAM 1000G	FortiPAM 3000G	FortiPAM-VM
Internet service entry port-range	0 (0) [64]	0 (0) [64]	0 (0) [64]
Service category	0 (5000) [5000]	0 (10000) [10000	0 (10000) [10000
WAN OPT profile	0 (128) [0]	0 (256) [0]	0 (256) [0]
WAN OPT peer	0 (1024) [0]	0 (2048) [0]	0 (2048) [0]
WAN OPT authentication group	0 (128) [0]	0 (256) [0]	0 (256) [0]
WAN OPT SSL server	0 (128) [0]	0 (256) [0]	0 (256) [0]
LDP monitor	0 (256) [0]	0 (512) [0]	0 (512) [0]
Traffic shaper	0 (500) [0]	0 (500) [0]	0 (500) [0]
VPN SSL web portal	0 (2600) [2600]	0 (2600) [2600]	0 (2600) [2600]
VPN SSL web portal: bookmark-group: bookmarks	256 (0) [0]	256 (0) [0]	256 (0) [0]

Features Table-instance limit [1] (VDOM limit) [2] [Global limit][3]	FortiPAM 1000G	FortiPAM 3000G	FortiPAM-VM
VPN SSL web user group: bookmark	0 (2000) [2600]	0 (2000) [2600]	0 (2000) [2600]
VPN SSL web user group bookmark: bookmarks	128 (0) [0]	128 (0) [0]	128 (0) [0]
VPN SSL web user bookmark: bookmarks	128 (0) [0]	128 (0) [0]	128 (0) [0]
IPS: custom	0 (256) [256]	0 (1000) [1000]	0 (1000) [1000]
Router			
Static	0 (10000) [0]	0 (10000) [0]	0 (10000) [0]
Policy	0 (2048) [2048]	0 (2048) [2048]	0 (2048) [2048]
Static6	0 (10000) [0]	0 (10000) [0]	0 (10000) [0]
VPN			
Local certificate	0 (500) [0]	0 (1000) [0]	0 (1000) [0]
CA certificate	0 (500) [0]	0 (500) [0]	0 (500) [0]
CRL certificate	0	0	0

Features Table-instance limit [1] (VDOM limit) [2] [Global limit][3]	FortiPAM 1000G	FortiPAM 3000G	FortiPAM-VM
	(200) [0]	(200) [0]	(200) [0]
IPSec phase1 interface	0 (0) [0]	0 (0) [0]	0 (0) [0]
IPSec phase2 interface	0 (0) [0]	0 (0) [0]	0 (0) [0]
Web filter FortiGuard: local rating	0 (12000) [0]	0 (12000) [0]	0 (12000) [0]
Application			
List	0 (256) [256]	0 (1000) [1000]	0 (1000) [1000]
Custom	0 (1000) [0]	0 (9000) [0]	0 (9000) [0]
CASI profile	0 (256) [256]	0 (1000) [1000	0 (1000) [1000
IPS			
Sensor	0 (256) [256]	0 (1000) [1000]	0 (1000) [1000]
Sensor override exempt IP address	8 (0) [0]	8 (0) [0]	8 (0) [0]
Web filter			
Profile	0	0	0

Features **Table-instance limit** [1] **(VDOM limit)** [2] **[Global limit]**[3]	**FortiPAM 1000G**	**FortiPAM 3000G**	**FortiPAM-VM**
	(1000) [1000]	(20000) [20000]	(20000) [20000]
Web keyword-match	0 (64) [0]	0 (64) [0]	0 (64) [0]
Content	0 (1000) [0]	0 (2000) [0]	0 (2000) [0]
Content entries	0 (32000) [0]	0 (250000) [0]	0 (250000) [0]
Exmword	0 (1000) [0]	0 (2000) [0]	0 (2000) [0]
Exmword entries	0 (32000) [0]	0 (250000) [0]	0 (250000) [0]
URL filter	0 (256) [256]	0 (1000) [1000]	0 (1000) [1000]
URL filter entries	0 (32000) [32000]	0 (250000) [250000]	0 (250000) [250000]
Override	0 (200) [0]	0 (500) [0]	0 (500) [0]
DNS filter			
Profile	0 (32) [32]	0 (500) [500]	0 (500) [500]

Features Table-instance limit [1] (VDOM limit) [2] [Global limit][3]	FortiPAM 1000G	FortiPAM 3000G	FortiPAM-VM
Domain filter	0 (32) [32]	0 (256) [256]	0 (256) [256]
Profile: domain-filter: external-blocklist	10 (0) [0]	10 (0) [0]	10 (0) [0]
Domain filter entries	0 (32000) [32000]	0 (250000) [250000]	0 (250000) [250000]
Email filter			
Profile	0 (32) [0]	0 (500) [0]	0 (500) [0]
Bword	0 (1000) [0]	0 (2000) [0]	0 (2000) [0]
Block allowlist	0 (1000) [0]	0 (2000) [0]	0 (2000) [0]
DNSBL	0 (1000) [0]	0 (2000) [0]	0 (2000) [0]
IP trust	0 (1000) [0]	0 (2000) [0]	0 (2000) [0]
Mheader	0 (1000) [0]	0 (2000) [0]	0 (2000) [0]
Bword entries	0 (32000) [0]	0 (250000) [0]	0 (250000) [0]

Features Table-instance limit [1] (VDOM limit) [2] [Global limit][3]	FortiPAM 1000G	FortiPAM 3000G	FortiPAM-VM
Block allow list entries	0 (100000) [0]	0 (500000) [0]	0 (500000) [0]
DNSBL entries	0 (32000) [0]	0 (250000) [0]	0 (250000) [0]
IP trust entries	0 (32000) [0]	0 (250000) [0]	0 (250000) [0]
Mheader entries	0 (32000) [0]	0 (250000) [0]	0 (250000) [0]
Antivirus			
Profile	0 (32) [0]	0 (500) [0]	0 (500) [0]
Content type	0 (1000) [0]	0 (2000) [0]	0 (2000) [0]
DLP			
File pattern entries	32000 (0) [0]	250000 (0) [0]	250000 (0) [0]
File pattern	0 (5000) [5000]	0 (12500) [12500]	0 (12500) [12500]
Sensor	0 (1000) [1000]	0 (1500) [1500]	0 (1500) [1500]
Sensor filter	3000	4000	4000

Features Table-instance limit [1] (VDOM limit) [2] [Global limit][3]	FortiPAM 1000G	FortiPAM 3000G	FortiPAM-VM
	(0) [0]	(0) [0]	(0) [0]
Sensitivity	0 (128) [0]	0 (128) [0]	0 (128) [0]
File filter			
Profile	0 (1000) [1000]	0 (1500) [1500]	0 (1500) [1500]
Profile rules	3000 (0) [0	4000 (0) [0]	4000 (0) [0]
Report layout			
Report layout	0 (32) [0]	0 (32) [0]	0 (32) [0]
Body item	256 (0) [0]	256 (0) [0]	256 (0) [0]
Page header item	2 (0) [0]	2 (0) [0]	2 (0) [0]
Page footer item	2 (0) [0]	2 (0) [0]	2 (0) [0]
Log threat			
Weight geolocation	0 (10) [0]	0 (10) [0]	0 (10) [0]
Weight web	0	0	0

Features Table-instance limit [1] (VDOM limit) [2] [Global limit][3]	FortiPAM 1000G	FortiPAM 3000G	FortiPAM-VM
	(96) [0]	(96) [0]	(96) [0]
Weight application	0 (32) [0]	0 (32) [0]	0 (32) [0]
Log setting: custom-log-fields	5 (0) [0]	5 (0) [0]	5 (0) [0]
Log tap-device	0 (0) [3]	0 (0) [3]	0 (0) [3]
System automation-trigger: fields	5 (0) [0]	5 (0) [0]	5 (0) [0]
SSH-filter.profile: shell-commands	256 (0) [0]	256 (0) [0]	256 (0) [0]
Endpoint-control fctems	0 (0) [5]	0 (0) [5]	0 (0) [5]
System object-tagging	0 (4096) [4096]	0 (4096) [4096]	0 (4096) [4096]
System HA: HA-mgmt-interfaces	0 (0) [1]	0 (0) [1]	0 (0) [1]
System HA:unicast-peers	0 (0) [7]	0 (0) [7]	0 (0) [7]
System SDN-connector	0 (0)	0 (0)	0 (0)

Features Table-instance limit [1] (VDOM limit) [2] [Global limit][3]	FortiPAM 1000G	FortiPAM 3000G	FortiPAM-VM
	[16]	[16]	[16]
Log FortiAnalyzer setting: serial	8 (0) [0	8 (0) [0	8 (0) [0
Log ForitAnalyzer2 setting: serial	8 (0) [0]	8 (0) [0]	8 (0) [0]
Log ForitAnalyzer3 setting: serial	8 (0) [0]	8 (0) [0]	8 (0) [0]
Log FortiAnalyzer override setting: serial	8 (0) [0]	8 (0) [0]	8 (0) [0]
Log FortiAnalyzer2 override setting: serial	8 (0) [0]	8 (0) [0]	8 (0) [0]
Log FortiAnalyzer3 override setting: serial	8 (0) [0]	8 (0) [0]	8 (0) [0]
System SSO Admin	0 (0) [300]	0 (0) [550]	0 (0) [550]
Firewall internet-service-name	0 (0) [8192]	0 (0) [8192]	0 (0) [8192]
System SSO-FortiCloud-admin	0 (0) [300]	0 (0) [550]	0 (0) [550]
System NETHSM: servers	0 (0) [2]	0 (0) [2]	0 (0) [2]

Features Table-instance limit [1] (VDOM limit) [2] [Global limit][3]	FortiPAM 1000G	FortiPAM 3000G	FortiPAM-VM
System NETHSM: slots	0 (0) [10]	0 (0) [10]	0 (0) [10]
System NETHSM: HA group	0 (0) [2]	0 (0) [2]	0 (0) [2]
System interface MAC	0 (0) [600]	0 (0) [600]	0 (0) [600]

[1] The maximum number of entries in each table instance.

[2] The maximum number of entries over all tables of the same type within each VDOM.

[3] The maximum number of entries over all tables of the same type within the system.

Note: `0` indicates no limit.

FORTINET®

www.fortinet.com