FORTINET

Release Notes

FortiPAM 1.0.0

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
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

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

February 21, 2023
FortiPAM 1.0.0 Release Notes
74-100-870769-20230221

TABLE OF CONTENTS

Change log

Date	Change Description
2023-02-06	Initial release.
2023-02-07	Updated Supported features on page 6.
2023-02-08	Added bugs 881955 and 879025 to Known issues on page 13. Updated FortiPAM deployment options on page 8.
2023-02-21	Updated FortiPAM deployment options on page 8.

FortiPAM 1.0.0 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, and known issues for FortiPAM 1.0.0, build 0016.

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/

Supported features

The following list contains features available in FortiPAM 1.0.0:

1. Support for multiple type of secrets:
   a. Linux, Windows and Windows AD, and macOS servers.
   b. Network devices, such as Cisco IOS, Fortinet Products, Juniper etc.
   c. Typical web accounts such as AWS, vSphere, FortiOS etc.
   d. More secrets can be supported by customized launchers and password changers.
2. Customer secret protection:
   a. Automatic blocking of dangerous commands with SSH filtering profiles.
   b. Logging of all shell commands running on SSH secrets.
   c. Auto password delivery for Linux root password or Cisco enabled password to protect sensitive information from end users.
   d. User can use *Associated Secret* option to switch from regular user to root user for Linux or from normal user mode to enable mode for Cisco routers.
   e. Strong SSH encryption algorithm.
   f. Keyboard-interactive authentication for SSH.
   g. AntiVirus scanning for web-based file transfer and SCP-based file transfer.
   h. Data Leak Prevention safeguards digital assets by defining DLP sensors based on file types, size, or watermarks (only available with CLI).
   i. Block RDP clipboard to prevent data leakage.
   j. Advanced RDP authentication protocols, including CredSSP, TLS.
   k. Access approval and batch scripts approval for sensitive target.
   l. Implements check-out/check-in to avoid simultaneous access to a single secret by multiple users.
   m. ZTNA tag controls for secret launches.
   n. *Tunnel Encryption* option to improve low-security protocol connections (e.g. VNC) and traverse third-party firewall devices.
3. Integration with customer's installed authentication systems using protocols such as RADIUS, LDAP, and SAML.
4. High security protection for FortiPAM login, including:
   a. Two-Factor authentication for local and remote users.
   b. IP-based access control.
   c. Schedule-based access control.
   d. ZTNA device tag-based FortiPAM server access control.
5. Flexible system access control and secret permission control, including:
   a. Role-based access control.
   b. User and group-based secret permission control.
   c. Device tag-based secret permission control.
6. Connect secrets from various OS with flexible solution:
   a. Multiple client OS are supported: Windows 10, Window 11, Linux, and macOS.
   b. Native program launching with FortiClient: Putty, Windows RDP, VNC Viewer, Tight VNC, WinSCP.
   c. Browser based accessing to SSH, RDP, VNC, SFTP, SMBA servers.
   d. Using customized Windows program to connect to the target server.

7. Full surveillance features to monitor all activities on secrets and FortiPAM:
   a. Monitor user login session and terminate suspicious user login session in real-time. Supports disabling users.
   b. Monitor secret connection sessions and disconnect any suspicious connection in real-time.
8. Automated password changing:
   a. Scheduled password (key) changing.
   b. Auto password (key) change after secret check-in.
   c. Password complexity policy.
   d. Secret credential history.
9. Easy system maintenance:
   a. Automatic configuration backups to FTP, SFTP, HTTP, or HTTPS servers.
10. Simpler secret management with Folders:
    a. Folders to organize secrets by region, office, and type.
    b. Folder-based permission control.
    c. Policy-based setting to simplify secret configuration.
11. Administrators can access all the secrets in emergency situations with Glass Breaking mode.
12. Users can access servers by internal IP or internal FQDN with proxy mode.
13. Full audit and reporting features help customer to do log audit and behavior analysis:
    a. Audit user login activities.
    b. Audit user SSH command history.
    c. Audit user activity with recorded video.
    d. Rich user activity statistics report.
14. High Availability ensures the system is highly available to minimize downtime.
15. Geo-redundant Disaster Recovery ensures data availability and protection in the event of a disaster by providing disaster recovery capabilities.
16. TPM or vTPM protects user private keys.
17. RAID support enhances data protection through redundancy and expands storage capacity.

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*.
      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.
         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 1.0.0 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	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

Product integration and support

FortiPAM 1.0.0 supports the following:

Web browser support

FortiPAM version 1.0.0 supports the following web browsers:

- Microsoft Edge version 109
- Mozilla Firefox version 109
- Google Chrome version 109

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

Virtualization software support

FortiPAM version 1.0.0 supports:

- VMware ESXi 6.5 and above
- Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0

FortiPAM-VM

For information about FortiPAM-VM deployments and system requirements, see the FortiPAM virtualization Admin Guides on the Fortinet Docs Library.

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
877321	Improvements to uploading secrets.
877355	Dynamic FQDN sometimes does not work for WEB-RDP.
880618	Firefox does not support extension-only web launching in Linux/MacOS.
874396	Launching Putty ssh secret results in no TLS SNI in connection attempt.
878078	Extension only: If launching a secret with Web SSH and Web FTP, only one session is recorded.
813723	Support 2FA with Web SSH.
872633	LibSSH2 limitation: FortiAnalyzer password verification and Web SSH always fail.
881955	Editing and saving ZTNA rules (firewall policy) causes the AV-scan feature to turn off.
879025	Web launcher fails on auto filling password for the Google cloud platform.

Limitations of FortiPAM

The following list contains features currently unavailable in FortiPAM 1.0.0:

- FortiToken Mobile push not supported for RADIUS user with RADIUS-side 2FA.

www.fortinet.com