FORTINET

Release Notes

FortiPAM 1.0.2

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

April 20, 2023
FortiPAM 1.0.2 Release Notes
74-102-897781-20230420

TABLE OF CONTENTS

Change log

Date	Change Description
2023-03-28	Initial release.
2023-04-20	Updated FortiPAM deployment options on page 7.

FortiPAM 1.0.2 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, resolved issues, and known issues for FortiPAM 1.0.2, build 0020.

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 1.0.2 is a patch release. There are no new features. See Resolved issues on page 16 and Known issues on page 17 for more information.

FortiPAM deployment options

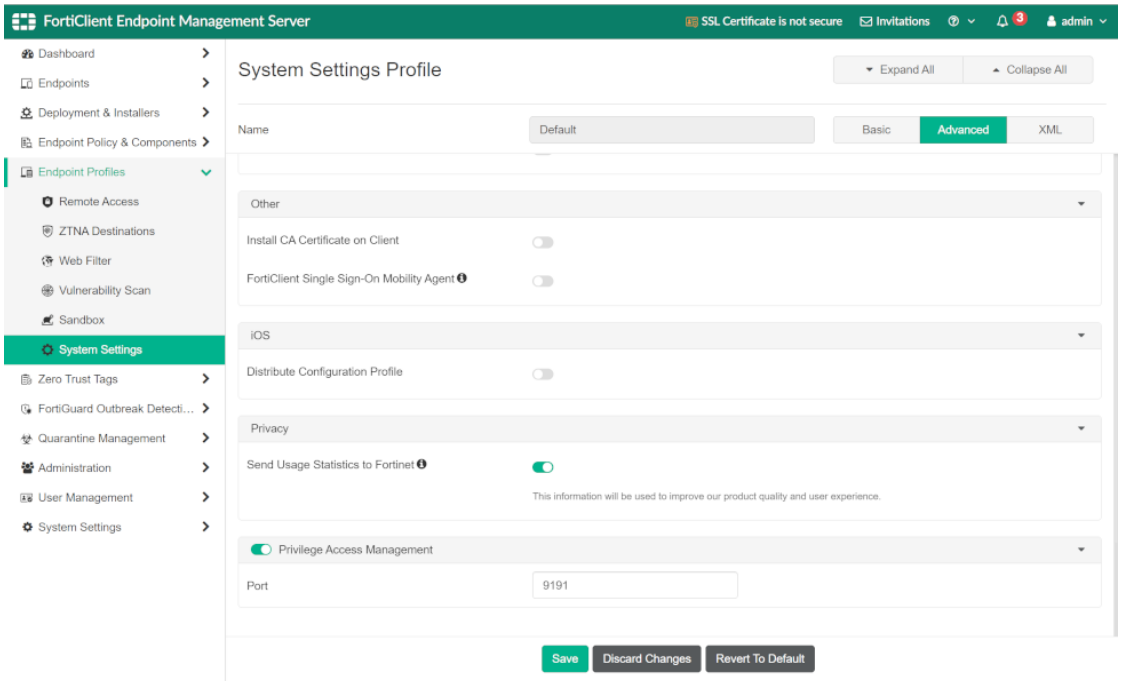
A full FortiPAM solution involves FortiPAM, EMS, and standard FortiClient. When both FortiPAM and FortiClient register to EMS, ZTNA endpoint control is available for secret launching and FortiPAM server access control. Both FortiPAM and the target server is protected by the highest security level.

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.

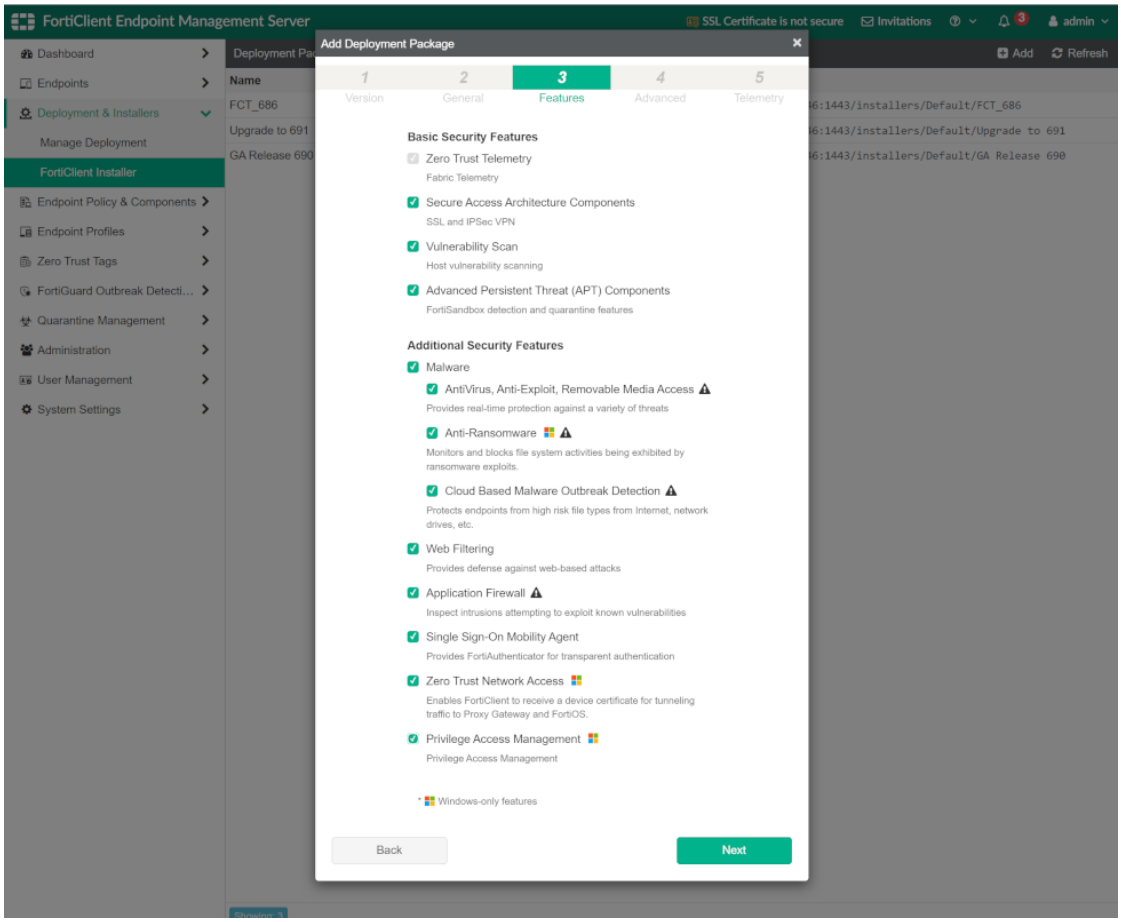
If FortiClient is not available, e.g., a user with Linux or MacOS system, Chrome and Edge extension called *FortiPAM Password Filler* is available on Chrome Web Store and Microsoft Edge Add-ons. On this extension-only setup, web-based launchers and web browsing are supported. The extension can record 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 1.0.2 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

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

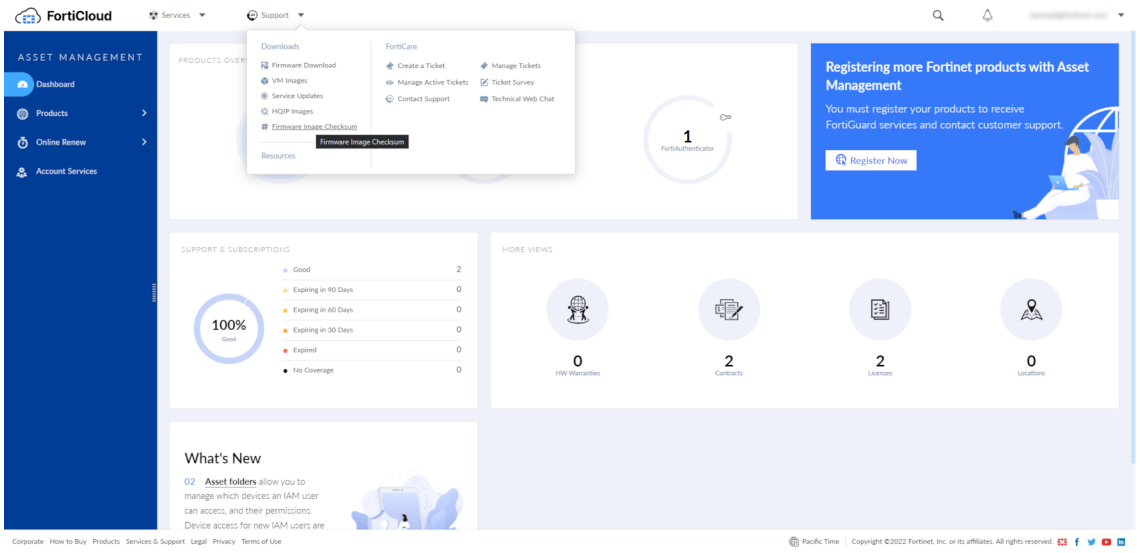
To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

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.



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.

Hardware support

FortiPAM 1.0.2 supports:

- FortiPAM 1000G
- FortiPAM 3000G

Product integration and support

FortiPAM 1.0.2 supports the following:

Web browser support

FortiPAM version 1.0.2 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 1.0.2 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.

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
894298	Folder and secrets are lost after reboot.

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
894625	After the downgrade from build 0017(1.0.1) to 0016 (1.0.0), FortiPAM cannot be accessed by GUI and SSH due to interface configuration becoming unavailable.

Limitations of FortiPAM

The following list contains features currently unavailable in FortiPAM 1.0.2:

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

www.fortinet.com