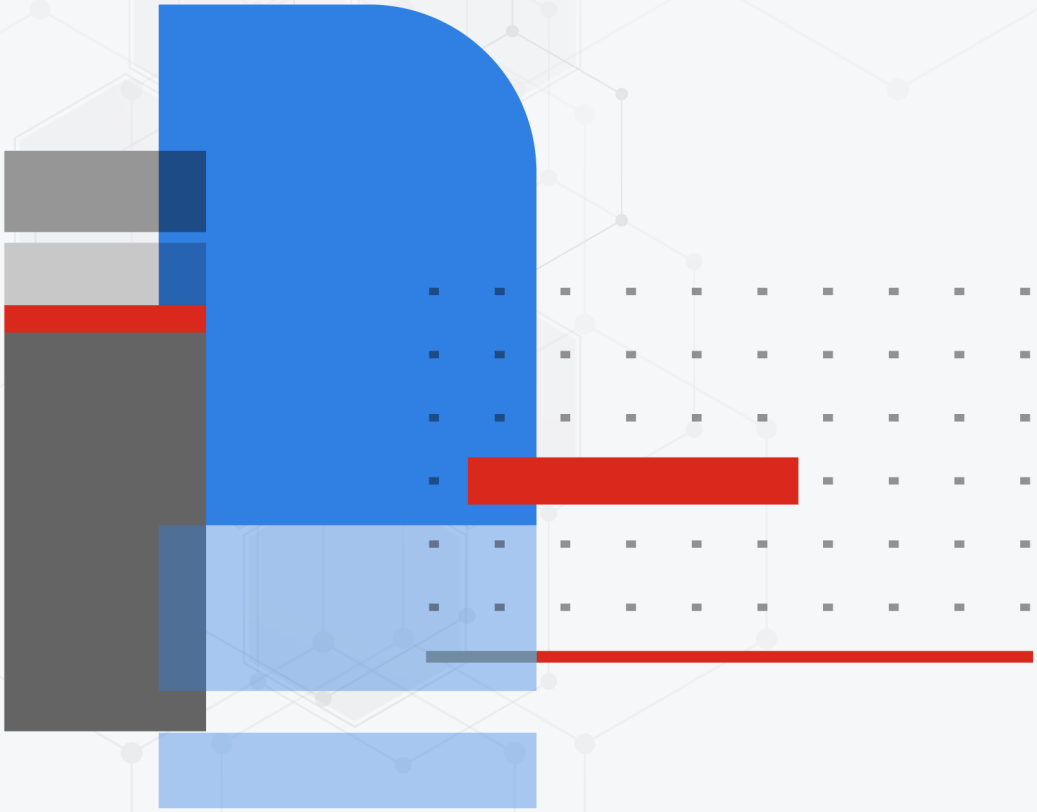
Release Notes

FortiPAM 1.1.2



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

FORTINET VIDEO LIBRARY
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

FORTINET TRAINING INSTITUTE
https://training.fortinet.com

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

December 8, 2023
FortiPAM 1.1.2 Release Notes
74-112-947423-20231208

TABLE OF CONTENTS

Change log

Date	Change Description
2023-08-28	Initial release.
2023-12-08	Renamed *FortiPAM Password Filler* to *Fortinet Privileged Access Agent* across the Release Notes.

FortiPAM 1.1.2 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, resolved issues, and known issues for FortiPAM 1.1.2, build 0432.

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 1.1.2 includes the following enhancements:

912019- Secret launching rate control to avoid DoS attacks

To avoid DoS attacks, multiple secret launching from the same user within 1 second is blocked.

926257- DLP filter rule: Displays filter type

When creating or editing a DLP filter rule in *Secret Settings* > *Data Leak Prevention*, the *Filter By* dropdown now lists the filters.

When editing a DLP sensor in *Secret Settings* > *Data Leak Prevention*:

- The *Specified File Types* column in the *Rules* pane now displays both; the file type ID and the file type name.
- The *filter-by* column in the *Rules* pane has been renamed to *Filter By*.

FortiPAM deployment options

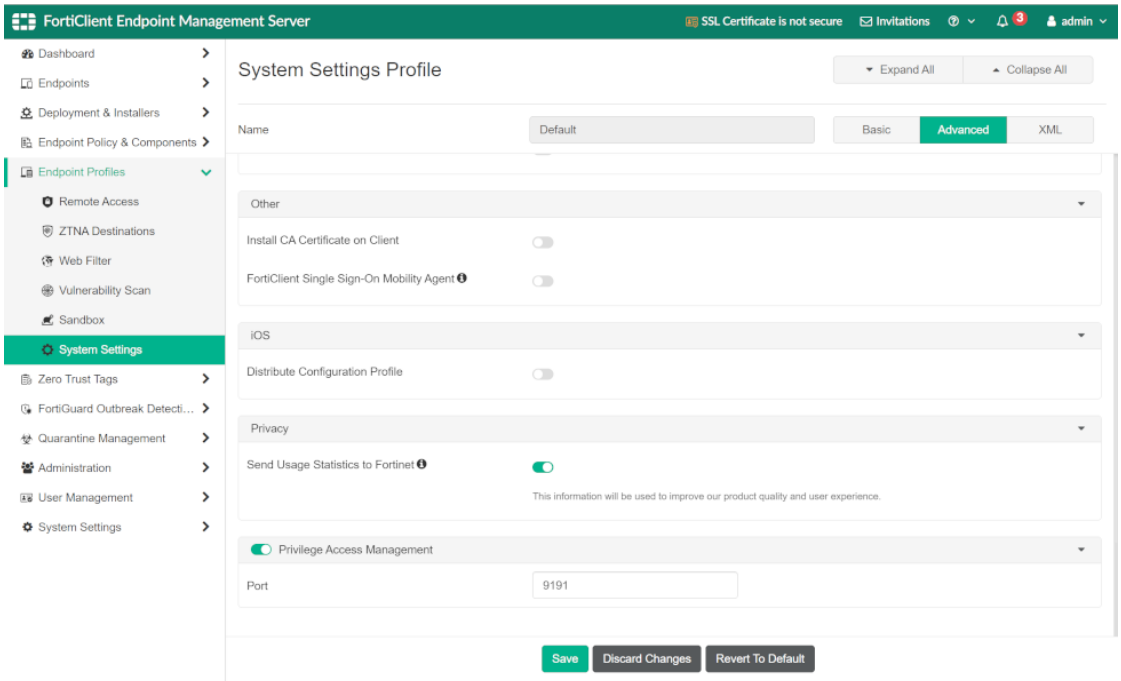
A full FortiPAM solution involves FortiPAM, EMS, and standard FortiClient. When both FortiPAM and FortiClient register to EMS, ZTNA endpoint control is available for secret launching and FortiPAM server access control. Both FortiPAM and the target server is protected by the highest security level.

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 *Fortinet Privileged Access Agent* 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.

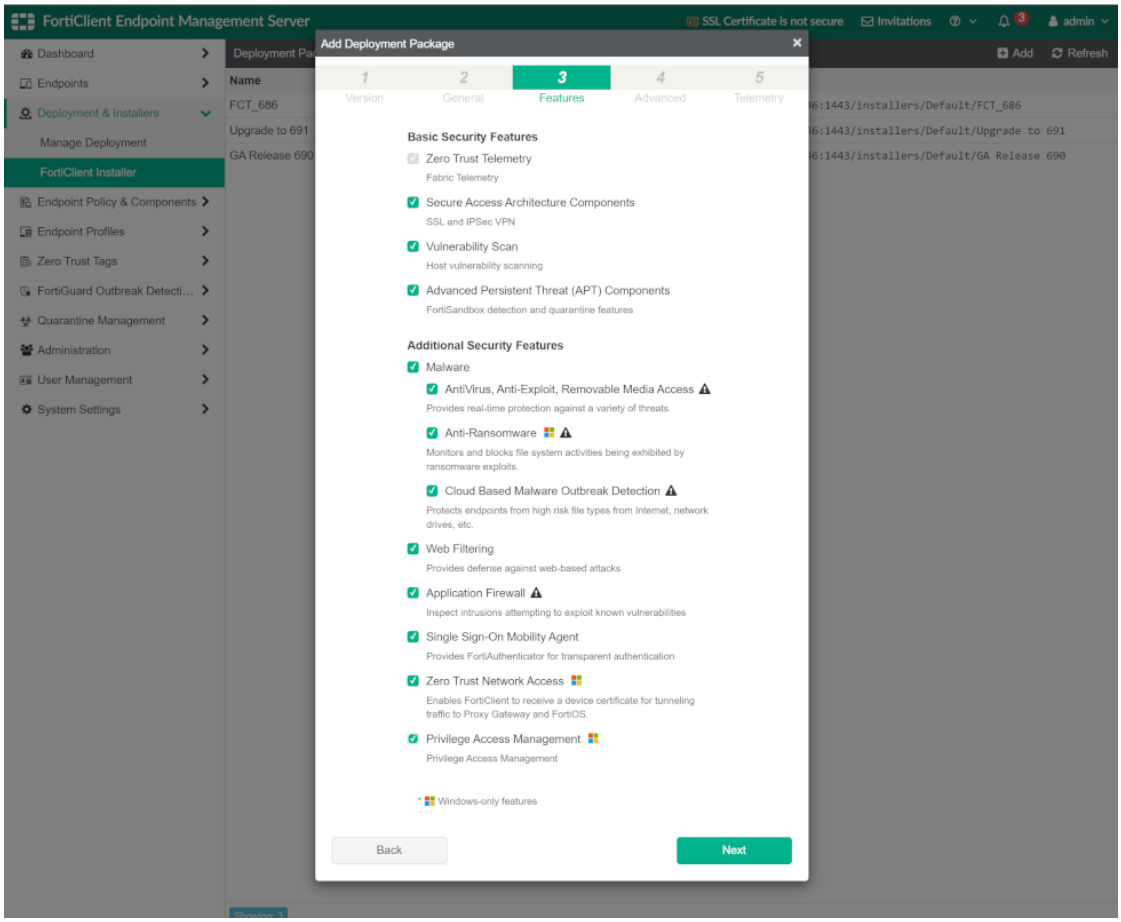
1. If EMS (7.2.0 or later) is available:
   a. **EMS Server**:
      i. Enable *Privilege Access Management*-
         i. Navigate to *Endpoint Profiles* > *System Settings*.
         ii. Edit the *Default System Setting Profiles*.
         iii. Select *Advanced* and enable *Privilege Access Management*.



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 *Fortinet Privileged Access Agent* 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 *Fortinet Privileged Access Agent* 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 *Fortinet Privileged Access Agent* 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 *Fortinet Privileged Access Agent* 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 1.1.2 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

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

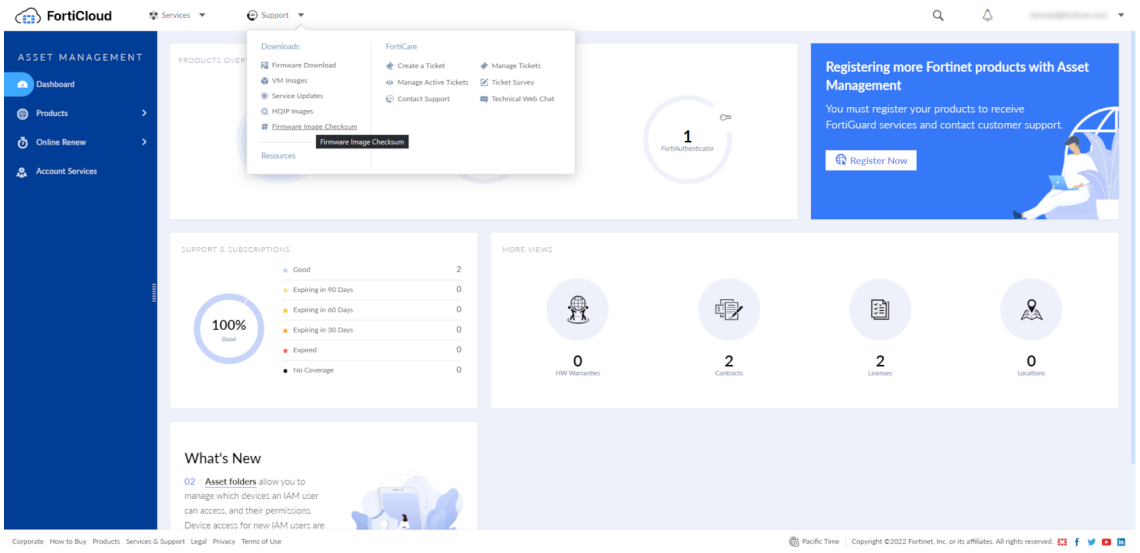
To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

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 dropdown, select *Activate Maintenance Mode* in *System*.
   a. Enter the maximum duration, in minutes.
   b. Enter a reason for activating the maintenance mode.
   c. Click *OK*.

   When in maintenance mode, select *Renew Maintenance Mode* in *System*, enter the new duration and reason and then click *OK* to renew the maintenance mode.

   When in maintenance mode, select *Deactivate Maintenance Mode* in *System* to deactivate the maintenance mode.

2. In the user dropdown, go to *System* > *Firmware*.
   The *Firmware Management* window opens.
3. Go to the *File Upload* tab:
   a. Select *Browse*, then locate the firmware image on your local computer.
   b. Click *Open*.

c. Click *Confirm and Backup Config*.
The firmware image uploads from your local computer to the FortiPAM device, which will then reboot. For a short period of time during this reboot, the FortiPAM device is offline and unavailable.

To restore the configuration manually:

1. You can only restore a configuration when in maintenance mode.
Repeat step 1 from Upgrading the firmware.
2. In the the user dropdown, go to *Configuration* > *Restore*.
The *Restore System Configuration window* opens.
3. Select *Local PC* as the option to restore from.
4. Select *Upload*:
   a. Locate the backup file on your local computer.
   b. Click *Open*.
   c. In *Password*, enter the encryption password for the backup file.
   d. Click *OK*.

When you restore the configuration from a backup file, any information changed since the backup will be lost. Any active sessions will be ended and must be restarted. You will have to log back in when the system reboots.

Product integration and support

FortiPAM 1.1.2 supports the following:

Web browser support

FortiPAM version 1.1.2 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 1.1.2 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 1.1.2 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.

Bug ID	Description
941426	FortiPAM issues related to RDP, 2FA RADIUS authentication, and logging.
943242	OpenSSH key upload fails when uploading secrets using the secret upload template feature.
926257	Improve the DLP sensor profile GUI display.
937021	Remove the hard coded LDAPS port and TLS version setting for the password changer.
931825	After GUI idle timeout, the FortiPAM web interface is blank or shows `0/` error.
935765	Memory leak when logging in using VIP or launching secrets with ZTNA control.
935081	Double free in cache management.

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.

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.
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.
875146	When the license status is pending, the GUI keeps refreshing.

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.

www.fortinet.com