FORTINET

Release Notes

FortiPAM 1.9.0

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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

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

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

May 4, 2026
FortiPAM 1.9.0 Release Notes
74-190-1262498-20260504

TABLE OF CONTENTS

Change log

Date	Change Description
2026-05-04	Initial release.

FortiPAM 1.9.0 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, resolved issues, and known issues for FortiPAM 1.9.0, build 1751.

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.

FortiPAM1.9.0 requires FortiClient 7.4.3 or above to offer the full set of functionalities.

For additional documentation, please visit:

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

Special notices

Do not enable server certificate validation

On the EMS, do not enable the server certificate validation for ZTNA.

Check *Endpoint Profiles > ZTNA Destinations* on the EMS to ensure that the certificate validation is disabled as shown below:

```
<disallow_invalid_server_certificate>0</disallow_invalid_server_certificate>
```

Allow pop up windows on Firefox

When launching web applications on the Firefox browser, allow pop up windows.

Web proxy CA certificate

When launching public websites, FortiPAM uses the selected CA certificate to re-sign the public websites.

When launching private websites, FortiPAM will use untrusted CA to re-sign the private websites.

Client software

Before upgrading to FortiPAM 1.9.0, check if there is a software in *Secret Settings > Client Software*. If yes, reduce the *Video Storage Limit* / *File Storage Limit* (in the *Advanced* tab in *System > Settings*) to allow uploading software from a USB disk (`/data2/pkg`) to the video disk.

After upgrading to FortiPAM 1.9.0, adjust the storage limit in the *Advanced* tab in *System > Settings*.

FortiPAM login page

Starting 1.9.0, FortiPAM offers a new login page that supports viewing clear passwords during entry.

If you have previously customized the login page or login token page, back up your existing modifications before upgrading.

After the upgrade:

1. Load the new default page template.
2. Reapply your backed-up customizations.

What's new

The following list contains new and expanded features added in FortiPAM 1.9.0.

Secret/Launch

1239092- TCP forwarding for native RDP launch

When creating a secret with *RDP Service* enabled, a new *TCP Forwarding* option is available.

Enabling *TCP Forwarding* routes the RDP traffic through TCP forwarding consistent with an *Other clientType* launcher.

As a result, *RDP Security Level*, *RDP Restricted Admin Mode*, *RDP Auto TOTP*, and *Block Clipboard* are not supported for native RDP launchers.

You can enable *TCP Forwarding* for the following reasons:

1. Bypass the certificate revocation check failure warning during the native RDP launch.
2. When connecting to a legacy or 3rd party RDP server that only supports plain text RDP.
3. When the native RDP launch fails due to recent RDP protocol change.

1230813- Secret launcher elevation

Some processes can only be started by the System level, e.g., SSMS, while others require a user.

In FortiPAM 1.9.0, a new *Privilege* option available when configuring a secret launcher in *Secret Settings > Launchers*.

The following options are available under *Privilege*:

- *Launch secret and run init/clean command under USER* (default)
- *Launch secret under SYSTEM*
- *Run init/clean command under SYSTEM*
- *Launch secret and run init/clean command under SYSTEM*

The *Privilege* flag instructs FortiClient whether a process should be launched under System or under a user account.

The *Privilege* flag is supported only in FortiClient 8.0 and later.

When FortiClient 7.x works with FortiPAM 1.9.0 or later, it uses the legacy hardcoded configuration to launch a process on the client PC, i.e., only `SSMS.exe` is started by the System, others require a user.

To confirm whether a launcher is running under the System account or a Windows user, open *Task Manager > Details* and check the *User name* column for the process.

1229992- Kerberos authentication for RDP sessions

Starting FortiPAM 1.9.0, FortiPAM introduces support for Kerberos authentication when launching native RDP sessions using Network Level Authentication (NLA).

Kerberos provides a stronger and more secure authentication mechanism compared to NTLM, and is the preferred method in modern Active Directory environments.

In Active Directory environments, the Kerberos realm typically aligns with the DNS name of the Windows domain, by convention.

FortiPAM automatically uses the configured domain associated with the secret or its target to construct the Kerberos Realm for authentication.

When Kerberos authentication is enabled, FortiPAM uses the domain information configured in the secret target to request a Kerberos ticket from the appropriate Key Distribution Center (KDC).

Best Practices

1. Create a secret using the *Target Only* secret template with target computer FQDN as the host information. Associate the secret with the corresponding *Windows Domain Account* secret, and launch the RDP session using the associated secret credentials.
2. Create a secret using *Windows Domain Account* secret template.
   When launching an RDP session, enter the target FQDN in the *Enter Target* field.

Limitations

- Kerberos authentication is supported only for the native RDP launcher.

1186793- Secret gateway permission support

FortiPAM 1.9.0 introduces the following two new permissions for *Secret Gateways*:

- *Viewer*: Viewer permission provides visibility and usage rights but does not allow modifying or deleting the gateway. A user with *Viewer* permission can use the gateway when configuring a target.
- *Owner*: A user with *Owner* permission receives all capabilities of the *Viewer* role plus the ability to update/delete the secret gateway.

This enhancement provides more granular administrative control and is primarily designed to support the Secret Gateway Proxy Chain feature.

1227053- Approval email using Microsoft Graph

FortiPAM 1.9.0 introduces support for configuring the Approval Email Server using Microsoft Graph, enabling customers to integrate approval workflows with Microsoft 365 mailboxes using modern OAuth based authentication.

This feature provides a secure alternative to traditional SMTP configurations.

1241246- Just-In-Time (JIT) privilege via Secret checkout/check-in (PowerShell)

Starting 1.9.0, FortiPAM introduces Just-In-Time (JIT) privilege elevation for Windows targets during a secret checkout/check-in.

Administrators can attach PowerShell scripts to a secret so that, when a user checks out the secret, FortiPAM will remotely connect to the target via WinRM and add the user to an elevated group, e.g., administrators.

On check-in, FortiPAM removes the user from that group, returning the machine to a least-privilege state.

1272600- Support additional authentication on secret access/launch

Starting 1.9.0, FortiPAM supports setting up additional authentication for accessing and launching secrets:

1. A new *Access Authentication* setting available when configuring a new secret policy in *Secret Settings* > *Policies*.

   When enabled, all secrets in the folder where the policy applies require authentication to access/launch them (default) unless the authentication setting is disabled per secret.

2. A new *Access Authentication* setting available in the *Session Security* pane when configuring a secret in *Secrets* > *Secrets*.
   Access Authentication Status displays the remaining duration of time you have access to the secret.
3. When you open to edit a secret that requires authentication, a new *Access Authentication* dialog opens requiring you to authenticate before accessing the secret.
   The following warning is displayed when you open a secret without authenticating:

   ```
   Editing of the secret is disabled because
   You don't have permission to access this secret.
   Please click here or re-access this page to complete the authentication.
   ```

   Most settings related to a secret that requires authentication for access are not available unless successfully authenticated.

4. When launching a secret with *Access Authentication* enabled, authentication is mandatory for successful launch of the secret.
5. When you attempt to access/launch a secret while being logged in to FortiPAM as a remote RADIUS/LDAP user, select *Authenticate using PAM login credentials* to authenticate using FortiPAM login credentials.

1218001- Secret gateway chaining

FortiPAM now supports Secret Gateway Chaining, which enables multiple secret gateways to be dynamically chained together to securely access targets across segmented networks.

This enhancement simplifies deployment and improves scalability for hybrid and multi-cloud architectures.

In environments where FortiPAM or service gateways are deployed in public cloud or DMZ networks and targets reside in isolated internal networks, Secret Gateway Chaining allows downstream gateways to establish secure reverse connections to upstream gateways.

Gateway information is automatically advertised to the central (root) FortiPAM, eliminating the need for manual configuration of intermediate gateways.

The following new settings are available when configuring the reverse gateway in the *Reverse Service* tab in *Network > Secret Gateway*:

- *Root FortiPAM SN*: Identifies the current device as the root (central) FortiPAM. This serial number is copied to downstream gateway configurations so they can advertise their gateway information to the correct root FortiPAM.
- *Gateway ID Whitelist*: Restricts which downstream gateways are allowed to establish reverse connections based on the CN of their gateway certificate

The following new settings are available when configuring a server in *Network > FortiPAM Server*:

- *Launch via Service Gateway*
- A new *Gateway Setting* pane

An updated *Gateway* pane in *Secrets > Targets* that allows you to select either a dynamic or a static gateway.

Note:

- Only the terminal gateway in the chain requires direct network connectivity to the target.
- All communication between gateways and FortiPAM uses mutual TLS (mTLS) with certificate-based authentication.

1241743- Launcher Process matcher

FortiPAM 1.9.0 introduces three new ways to identify the main process: *Default*, *Window Title*, and *Command Line*.

Window Title matches a Regex against the GUI window title, and *Command Line* matches a Regex against the process execution string.

When `proc-matcher-type` is not default, Multiprocess Mode and Full-screen Recording are forced to `Enable` so FortiClient can watch the whole tree to find the match and guarantee the audit trail is captured.

1231937- Single secret to multiple target hosts

FortiPAM 1.9.0 adds support for using a single secret with multiple approved target hosts.

A new *Multiple Target Address Field Type* when configuring a secret template in *Secret Settings > Templates*.

The *Multiple Target Address* replaces the standard *Service Address Field Type*.

You can configure a *Multiple Target Address* allowlist that supports IP ranges, CIDR, FQDNs, and wildcard FQDNs, and users can select a destination from the approved list when launching a session.

Support for single secret to multiple target hosts requires FortiPAM 1.9.0 or above.
Older versions support multiple addresses only for OT launchers.

1218004- Support for revoking approved secret access requests

Starting FortiPAM 1.9.0, FortiPAM allows approvers to revoke their approvals.

A new *Revoke Approval* option available in a secret approval request that has already been approved (*Secrets > Approvals*).

An approver can revoke their approval at any time regardless of the approval tier or even when the requester has already launched the secret.

Once the approval is revoked:

- If the requester had already launched the secret, the secret session is immediately terminated.
- The secret approval request resets and must be approved/denied.

1231609- Support for Loading Balancing Information for Web RDP targets

Starting FortiPAM 1.9.0, FortiPAM introduces a new *Loading Balancing Information* attribute for targets that use templates with Web RDP default launcher.

This value provides the load balancing information or cookie that should be sent to the connection broker and is configured in the target setting.

User/Group

1221052- Auto provision email address and display name for LDAP users

Starting FortiPAM 1.9.0, FortiPAM supports getting user display name and email address for auto provisioned remote LDAP users.

The following two new fields are available when editing an auto provisioned remote LDAP user:

- *Display Name*
- *Email address*

1. A new auto-provision rule for LDAP user group is configured.
2. When an LDAP user attempts to log in to FortiPAM, it attempts to fetch user display name and email address fields.

FortiPAM auto provisions the user email address and display name from the remote LDAP server with best effort.

Notes:

- When no display name or email address information synchronizes from the remote server, the administrator can edit those fields.
- After auto-provision users are imported into FortiPAM and managed as local users, the display name and the email address field values stop synchronizing with the remote server.

1251884- Non-TOTP 2FA support in WebSSH

Starting FortiPAM 1.9.0, the WebSSH launcher now supports non-TOTP-based 2FA for SSH targets that require an additional authentication challenge during login.

This enhancement allows users to manually enter real-time 2FA codes directly in the WebSSH console.

During login, if the SSH server issues a 2FA challenge, FortiPAM displays the following prompt:

```
Enter token code or no code to send a notification to your FortiToken Mobile
```

You can then manually enter the correct verification code to complete authentication.

Supported 2FA methods

1. FortiAuthenticator-based 2FA
   a. FortiToken Mobile/FortiToken Cloud
   b. SMS
   c. Email
2. 3rd party authentication applications
   a. Google Authenticator and other compatible token tools

   This update ensures that WebSSH can handle a wider range of real-time authentication methods without requiring built-in TOTP configuration on the FortiPAM side.

Configuration requirements

For most deployments, no additional configuration is needed.

However, when using FortiAuthenticator with SMS or Email delivery, FortiPAM requires that at least one of the following SSH-related settings be enabled within the secret:

When configuring a secret in *Secrets > Secrets*, go to the *SSH Service* pane in the *Settings* tab, and configure any of the following:

1. Select *Enable SSH service* and select an SSH filter from the *SSH Filter* dropdown.

   A placeholder (empty) profile is acceptable if no filtering is required.

2. Enable *SSH Auto-Password*.
3. Use a *Target Only* secret template.
   Users manually enter the username and password during login.

These settings ensure that the WebSSH workflow can accept and relay the external 2FA challenge correctly.

Limitation

If a user enters an incorrect 2FA token, the SSH session cannot retry the challenge within the same connection.

- The WebSSH session must be closed.
- The user must relaunch the secret and authenticate again with the correct real-time token.

Recommendation

In some environments, FortiAuthenticator automatic push notifications (FortiToken Mobile auto-push) may behave inconsistently.

For best reliability, manual entry of the 2FA token is recommended.

1186793- Wildcard user support

FortiPAM 1.9.0 introduces support for wildcard users when using the Concurrent Logon license model.

To configure a wildcard remote user, select the new *Match all users in a remote server or group* option available when configuring a new remote user in *User Management > User List*.

This capability allows administrators to permit login for any remote user who matches a remote server group without creating individual static user entries in FortiPAM.

This feature is beneficial for environments with large number of temporary users.

Wildcard user entries must not be assigned to features that generate notifications, e.g., approval roles.

The auto provision rule takes high priority when wildcard matching is enabled.

Only functional under the Concurrent Logon license model.

1192951- SCIM service support

This feature delivers comprehensive SCIM-driven identity lifecycle management combined with administrative visibility and control through the GUI.

It supports automatic provisioning and enforcement, as well as manual import and review of SCIM users and groups.

The system tightly integrates SCIM, SAML, and Auto Provision Rules (APL) to deliver instant identity synchronization, dynamic role and policy assignment, and immediate session enforcement when user or group membership changes.

Go to *User Management > SCIM Service* to create a SCIM client.

A new *SCIM profile* dropdown available when configuring a SAML SSO server in *User Management > Saml Single Sign-On.*

The new *SCIM profile* dropdown allows you to select a configured SCIM client.

This allows the system to link SAML-authenticated users with SCIM-synchronized user and group data, enabling automatic provisioning, dynamic role updates, and real-time authorization enforcement based on SCIM lifecycle events.

1055670- `Message-Authenticator` support for RADIUS

FortiPAM 1.9.0 adds the `Message-Authenticator` attribute to RADIUS requests and introduces the `require-message-authenticator` option under RADIUS server configuration.

This option is enabled by default, which makes validation of the `Message-Authenticator` in the RADIUS response mandatory.

Administrators can set it to disable as a workaround if the RADIUS server does not provide the attribute in the response.

System/Log

1237561- Auto purging auto-provisioned users

Automatic disabling of auto-provisioned users due to prolonged inactivity was introduced in FortiPAM 1.8.0.

Starting FortiPAM 1.9.0, FortiPAM supports automatically purging disabled auto-provisioned users.

A new *Provisioned User Auto-purging* pane available in the *Advanced* tab in *System > Settings*.

The following settings are available in *Provisioned User Auto-purging*:

- *User Max Disabled Days* (new): The number of days after which a disabled auto-provisioned user is deleted.
- *User Max Inactivity Days*: The number of days after which an inactive auto-provisioned user is disabled.

Others

1235062- FortiPAM-VM active-passive HA on OCI

You can now deploy FortiPAM-VM active-passive HA on the OCI platform within an AD.

1208446- New FortiPAM 400G hardware model

Starting FortiPAM 1.9.0, FortiPAM now supports a new FortiPAM 400G hardware model.

For information on configuration capacity for the FortiPAM 400G hardware model, see Configuration capacity for FortiPAM hardware appliances and VM in the latest *FortiPAM Release Notes*.

1051767- New FortiPAM 100G hardware model

Starting FortiPAM 1.9.0, FortiPAM now supports a new FortiPAM 100G hardware model.

> The FortiPAM 100G hardware serves as a gateway-only device.

For information on configuration capacity for the FortiPAM 100G hardware model, see Configuration capacity for FortiPAM hardware appliances and VM in the latest *FortiPAM Release Notes*.

1261155- New FortiPAM login page

Starting 1.9.0, FortiPAM offers a new login page that supports viewing clear passwords during entry.

If you have previously customized the login page or login token page, back up your existing modifications before upgrading.

After the upgrade:

1. Load the new default page template.
2. Reapply your backed-up customizations.

1221902- TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO)

Starting 1.9.0, FortiPAM supports TCP Segmentation Offload (TSO) and Generic Segmentation Offload (GSO) at the system interface level.

These two new settings are enabled by default and are designed to improve overall network performance by reducing CPU overhead during packet transmission.

Both settings are configurable per interface and can be enabled or disabled as needed.

TSO and GSO allow the operating system to transmit large data packets and delegate the task of segmenting them into smaller, network-compliant packets to the NIC or kernel. This offloading significantly reduces CPU processing required for packet segmentation, resulting in improved throughput and lower system load.

In FortiPAM 1.9.0:

- TSO is enabled by default on all system interfaces
- GSO is enabled by default on all system interfaces

Configuration

TSO and GSO settings are only available as CLI commands.

```
config system interface
 edit "port1"
  set tso {enable | disable}
  set gso {enable | disable}
 next
end
```

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 and then upgrade the firmware. Optionally, you can restore your configuration.

Before you can install FortiPAM firmware, you must download the firmware image from FortiCloud, then upload it from your computer to the FortiPAM device. See Upgrading the firmware.

To download the firmware image from FortiCloud:

1. Log into FortiCloud.
2. Go to *Support* > *Downloads*, and select *VM Images* from the dropdown list.
   The *VM Images* page opens.
3. In *Select Product*, select *Other*.
4. Click on the hyperlink that appears.
5. In *Select Product*, select *FortiPAM*.
6. Switch to the *Download* tab and go inside the correct image folder.
7. Click on *HTTPS* for the zip file you intend to download.
   The zip file is downloaded to your management computer.

Image checksums

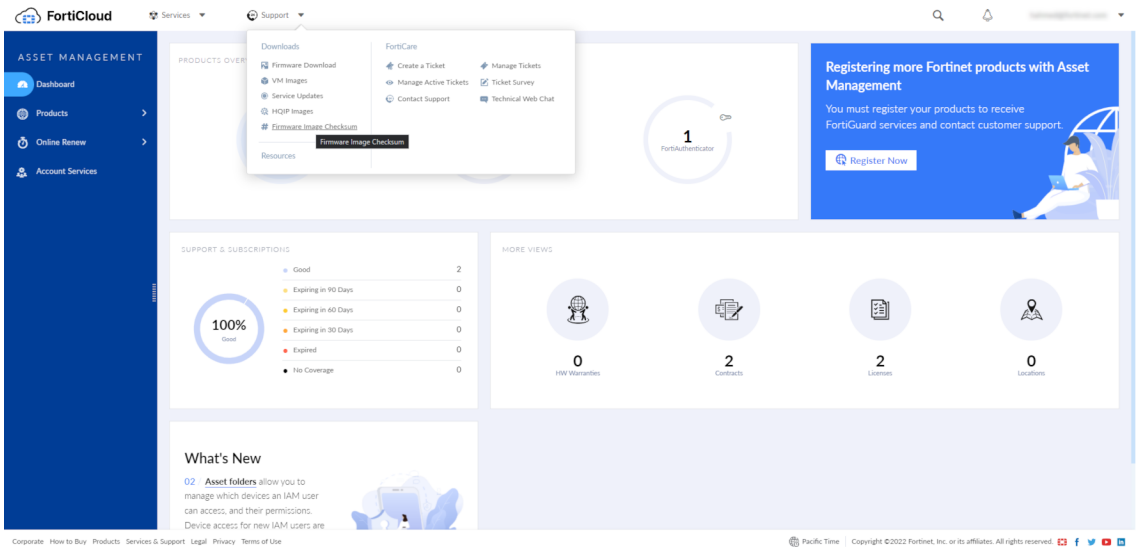
To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

MD5 checksums for software releases are available on FortiCloud.

FortiCloud image checksum tool

After logging in to FortiCloud, in the menus at the top, click *Support*, then click *Firmware Image Checksum*.

In the *Image File Name* field, enter the firmware image file name, including its extension, then click *Get Checksum Code* to get the checksum code.



To backup your configuration manually:

1. In the user dropdown, go to *Configuration* > *Backup*.
   The *Backup System Configuration* window opens.
2. Select *Local PC* as the backup option.
3. Enable *Encryption*, enter and confirm password.
4. Click *OK*.
   The backup file is downloaded to your local computer.

To upgrade the firmware:

1. You can only upload a firmware when in maintenance mode.
   From the user 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.

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.

Once the configuration is restored, select *Deactivate Maintenance Mode* in *System* to deactivate the maintenance mode.

Upgrade paths

Use the following table to verify the list of compatible upgrade paths:

FortiPAM

From	To
1.7.x	1.9.0
1.8.x	1.9.0

FortiSRA

1.4.x > 1.5.x/1.6.x > 1.7.2 > FortiPAM 1.8.x > 1.9.0

Product integration and support

FortiPAM 1.9.0 supports the following:

Web browser support

FortiPAM version 1.9.0 supports the following web browsers:

Google Chrome version 135
Microsoft Edge version 135
Mozilla Firefox version 137 ⚠ Mozilla Firefox is supported with some limitations.

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

Virtualization software support

FortiPAM version 1.9.0 supports:

Alibaba Cloud
AWS (Amazon Web Services)
GCP (Google Cloud Platform)
Linux Kernel-based Virtual Machine (KVM) on Virtual Machine Manager and QEMU 2.5.0
Microsoft Azure
Microsoft Hyper-V
Nutanix

OCI (Oracle Cloud Infrastructure)
Proxmox
VMware ESXi 6.5 and above

Hardware support

FortiPAM 1.9.0 supports the following FortiPAM hardware models:

FortiPAM 100G*
FortiPAM 400G
FortiPAM 1000G
FortiPAM 1100G
FortiPAM 3000G

* The FortiPAM 100G hardware serves as a gateway-only device.

Language support

The FortiPAM GUI can be displayed in the following languages:

Arabic
Chinese (Simplified)
Chinese (Traditional)
English
French
German
Italian
Japanese
Korean
Portuguese
Spanish

For more information on changing the language in the GUI, see the FortiPAM Administration Guide.

FortiPAM-VM

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

Resolved issues

The resolved issues listed below may not list every bug that has been corrected with this release. For inquiries about a particular bug, please contact Technical Support within the FortiCare portal.

Secret/Launch

Bug ID	Description
1243034	Change "Username" and "Password" in default template of "Windows Machine" from Required to Optional.
1200794	Network mapping using secret probing on FortiPAM.
1268756	Explicit Web Proxy Certificate Import GUI vs CLI bevhaviour.
1198058	Web launcher is disabled after importing secret.
1256560	AV-profile is removed when attempting to save changes.
1239711	Customized resolution on Web RDP not available when accessing secrets from the secrets details page.
1237851	Replace Web Credential on Proxy does not work with Associated Secret enabled.
1238033	Error message "Unable to launch secret, request too frequently" when using a native launcher.
1193572	FortiPAM gateway access control.
1228329	Slow web SMB/SFTP file upload speed (1Mbps).
1237849	Add URL decode in the gateway info handler.
1050328	Approver unable to revoke the secret.
1273260	Secret Password Changer Fails for Azure AD web-api password changer.
1276453	Domain field does not accept domains starting with a number.

System/Log

Bug ID	Description
1257731	SFTP Config Backup to a remote server does not work.
1263941	No secret logs are send through syslog in version 1.8.0 nor 1.8.1.
1253814	Unable to view the logs on the FortiPAM when secretgrp set to custom.
1263843	FortiPAM HA synchronization issue caused by some fields missing in the EMS tag.

Bug ID	Description
1260462	HA out of sync because secret target cannot be added into the secondary due to duplicate.
1235477	Changing to concurrent license causes FortiPAM to deny all logins via GUI.
1279383	Stack Buffer Overflow in Log Report.

Others

Bug ID	Description
1243837	FortiPAM 1100G/3100G chassis UID button does not function.
1246179	SSL-VPN Reflected XSS.
1201838	Stack buffer overflow in CLI.
1217886	port FortiOS bug fix for potential html injection.
1242213	Arbitrary file write via /api/usrbwl and /api/usrbwlqry endpoints.
1241847	Fabric connector with EMS 7.4.5 no longer works.
1256882	Agentless only not working on Edge/Chrome.
1242162	Evaluate path in "exec usb-disk delete" command.
1274827	API return code when querying target might be incorrect.
1275950	Wrong API return code for /api/v2/utility/id.

Common Vulnerabilities and Exposures

Bug ID	CVE references
1055670	FortiPAM is no longer vulnerable to the following CVE-Reference(s): • CVE-2024-3596

Visit https://fortiguard.com/psirt for more information.

Known issues

This section lists the known issues of this release, but is not a complete list. For inquiries about a particular bug, please contact Technical Support within the FortiCare portal.

Secret/Launch

Bug ID	Description
1270426	FortiPAM does not support custom certificates and private keys for FortiClient EMS ZTNA.

Migration from FortiSRA to FortiPAM

In version 1.8.0, FortiSRA is merged into FortiPAM.

Starting FortiPAM 1.8.0:

1. The previous FortiSRA default administrator will have the full Super Administrator role, including the ability to launch secrets.
2. With `SKU-591`, an extra seat is added for free.
   For example, when the purchased license seat quantity is 20, then 21 users can be enabled.
   For HA, if a node has 10 licensed seats and the other has 5 users, the primary node can have 16 users enabled.

Upgrade path for FortiSRA:

1. Upgrade FortiSRA from 1.6.x to 1.7.2 using the FortiSRA image.
2. Upgrade FortiSRA from 1.7.2 to FortiPAM 1.8.0 using the FortiPAM 1.8.0 image.

After migration from FortiSRA to FortiPAM, the original FortiSRA administrator becomes a regular administrator on FortiPAM with the ability to create/edit/launch secrets.

This is a free administrator account.

After migration from FortiSRA to FortiPAM, native launchers are automatically created and added to the default templates.

If you do not want to display the native launchers, remove them from the following default templates:

- *Unix Account (SSH Password)*, *VNC Server*, *FortiGate/FortiOS (SSH Key)*,*FortiGate/FortiOS (Web)*, *Machine*, *Windows Domain Account*, etc.

After migration from FortiSRA to FortiPAM, the GUI can report the `Configuration can contain errors` warning.

Run:

```
diag debug config-error-log read
```

Output:

```
"end" @ global.system.replacemsg.auth.auth-sra-login-page:failed command (error -56)
 "end" @ global.system.replacemsg.auth.auth-sra-token-page:failed command (error -56)
 "end" @ global.system.replacemsg.auth.auth-sra-passchg-page:failed command (error -56)
```

The above output is harmless to your system.

Run the following command to clear the output:

```
diag debug config-error-log clear
```

After you migrate from FortiSRA to FortiPAM, you can no longer downgrade back to FortiSRA.
Ensure that you create a snapshot of your FortiSRA before the migration to FortiPAM.

If the FortiSRA license is expired, FortiSRA license may not be available.
If using a new FortiPAM license to replace an expired FortiSRA license, the following must be performed:

Fabric connectors (EMS, FortiAnalyzer)	Reconfigure EMS and FortiAnalyzer to accept FortiPAM connection request
Users with local mobile 2FA	Disable/re-enable 2FA
Users with FortiToken Cloud 2FA	Disable/re-enable 2FA

Configuration capacity for FortiPAM hardware appliances and VM

The following table lists the maximum number of configuration objects per FortiPAM appliance that can be added to the configuration database for different FortiPAM hardware or VM models.

Features	FortiPAM 100G*	FortiPAM 400G	FortiPAM 1000G	FortiPAM 1100G	FortiPAM 3000G	FortiPAM-VM
Secret	-	25000	50000	50000	100000	100000
Target	-	2500	5000	5000	10000	10000
Folder	-	1000	2000	2000	6000	6000
User	100	500	1000	1000	3000	3000
User group	500	500	2000	2000	5000	5000
Request	-	2500	5000	5000	10000	10000
Gateway	256	256	256	256	256	256

***** The FortiPAM 100G hardware serves as a gateway-only device.

www.fortinet.com