FORTINET

Release Notes

FortiPAM 1.8.0

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

January 8, 2026
FortiPAM 1.8.0 Release Notes
74-180-1208533-20260108

TABLE OF CONTENTS

Change log

Date	Change Description
2025-12-01	Initial release.
2025-12-10	Updated Virtualization software support on page 22.
2025-12-12	Added What's new on page 8.
2026-01-08	Updated Special notices on page 7.

FortiPAM 1.8.0 release

This document provides a summary of new features, enhancements, support information, installation instructions, caveats, resolved issues, and known issues for FortiPAM 1.8.0, build 1689.

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.

FortiPAM 1.8.0 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 1.8.0, 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 1.8.0, adjust the storage limit in the *Advanced* tab in *System > Settings*.

FortiPAM not compatible with FortiClient EMS 7.4.5

FortiPAM 1.8.0 is not compatible with FortiClient EMS version 7.4.5 GA.

What's new

The following list contains new and expanded features added in FortiPAM 1.8.0.

Secret/Launch

1128508- Customized resolution on Web RDP

Starting FortiPAM 1.8.0, a new *Resolution* option is available in the *Launch Progress* dialog when a secret is launched with the *Web RDP* launcher.

The new *Resolution* option allows you to customize the *Web RDP* session resolution.

1134577- RDP connection failure diagnosis tools to end users

Starting FortiPAM 1.8.0, a new *Native RDP Diagnostics* option is available when you open a secret.

Clicking the new *Native RDP Diagnostics* option displays diagnostic information for various scenarios:

1. **Successful launch**
   `Our diagnosis shows that your last native RDP connection started successfully at time 2025-08-14 11:06:09. If you're using rdp-security-leve \"TLS\" and you got blocked at the login screen of the remote server, likely that you didn't have the correct RDP credential filled in the secret.`
2. **Failed launch due to incorrect Security Level of RDP**
   `Native RDP currently does not support rdp-security-level \"RDP\". Use \"TLS\" or \"Best-effort\" instead! Error code: 0x0068.\nAdditional information: N/A. \nLast launched at 2025-08-14 11:09:22\n`
3. **Failed launch due to incorrect password with NLA**
   `NLA failed because server's response indicates there's an error in the challenge response. Did you have the correct credentials in the secret? Error code: 0x0140.\nAdditional information: N/A. \nLast launched at 2025-08-14 11:15:20\n`
4. **Failed launch due to incorrect password with TLS**
   `Our diagnosis shows that your last native RDP connection started successfully at time 2025-08-14 11:06:09. If you're using rdp-security-leve \"TLS\" and you got blocked at the login screen of the remote server, likely that you didn't have the correct RDP credential filled in the secret.`
5. **Failed launch due to incorrect domain with TLS**
   `Our diagnosis shows that your last native RDP connection started successfully at time 2025-08-14 11:06:09. If you're using rdp-security-leve \"TLS\" and you got blocked at the login screen of the remote server, likely that you didn't have the correct RDP credential filled in the secret.`

6. **Failed launch due to network unreachable**
   `The RDP diagnosis information are empty (currently have info of secret 0, requested for 2). Please launch your native RDP again!"`
7. **Failed launch due to target without RDP service**
   No new diag created. Displays the last time of the diagnostics message.

1189926- Folder edit refactor

When editing a folder:

- Secret policy is displayed when inherited.
- Selecting a parent folder opens tree view similar to when editing a secret.
- Previously available separate tab have been combined into a single page.
- *Permission* removed from personal folders.

1171919, 1191816, 1164981- Secret edit page enhancements

In FortiPAM 1.8.0, when editing a secret from the secrets list in *Secrets > Secrets*:

- New *DLP Log* and *Antivirus Log* tabs available in the *Audit tab*.
- *New Requests & Jobs* tab available displaying references for requests/jobs.
- Simplified services in the *Settings* page that displays only related services, e.g, for a secret that uses *Web Account* secret template, only the corresponding *Web Service* pane is displayed.

963330- Password expiry notification

Starting FortiPAM 1.8.0, you can manually set up the password expiry notification:

1. When creating/editing a secret, a new *Password Expiration Setting* option is available in the *Password Management* pane in the *Settings* tab.
   When *Password Expiration Setting* is enabled, in *Password Expires After x Days*, enter the number of days after which the password expires.
   Once set up, the remaining password expiry time is displayed under *Password Expiration Status* on the left.
2. In the *Email Settings* tab in *System > Settings*, a new *Secret Password Expiration Notification* field available.
   In *Secret Password Expiration Notification*, set how many days in advance to notify the user before their password expires.
   Note: This only works when *Password Expiration Setting* is enabled for a secret.
3. A new password expiration secret event.
   Subscribers configured with a valid email address receive notification email when *Password Expiration* is selected in the *Event Subscription* tab when configuring a secret.
   Secret owners configured with a valid email address receive the password expiration notification.
4. In the *Password Event* pane in *Log & Report > Secret Event & Video*, password expiring and expired logs are generated.
   A related email notification is sent out.
   Notes:

a. For the password expiry notification to work, you must configure at least one or more direct secret owners with a valid email address.
b. The notifications email does not apply to the configured direct owners in the secret owner group.
c. Go to *Log & Report > Email Alert Settings*, and select *Enable email notification*.
This is required to receive email notifications.
d. This password expiration notification is mutually exclusive with *Automatic Password Changing*.

1178099- Support credential replacement for Siemens TIA Portal Cloud

Starting FortiPAM 1.8.0, FortiPAM now supports replacing credential for the Siemens TIA Portal Cloud.

When creating/editing a target in *Secrets > Targets*, a new *Siemens-Tia* option available in the *Website Vendor* dropdown.

1178353- Web API password changer enhancements

New enhancements for the customized Web API password changer:

1. Supports CSRF token extraction from cookie using the following new configurations:
   a. `extract-csrftoken`: Enable/disable.
   b. `csrf-key`: Indicate the key to extract CSRF token in cookie.
   c. `$CSRFTOKEN`: Store the extracted CSRF token value.
2. Supports multi-layer `http` JSON body parsing:
   - The `http` body may have multi-layer and contains the value that needs to be used in the post password change process.

   Example configuration EXAMPLE

```
edit x
 set type expect
 set expect-code 200
 set expect-str-in-body "\"retval\": 1"
 set token-location body #set location to body
 set extract-token enable #must be enabled
 set token-key "data.users.0.id"
next
```

   Notes:
   - The token key string helps locate the user ID that may be used later.
   - The token value is stored into the variable `$TOKEN`.

Variable	Description
`data`	JSON object key value.
`users`	JSON object value array name.

Variable	Description
0	Array object index.
id	Object key.

http body response:

```
{
 "result": {
   "retval": 1,
   "message": null
 },
 "data": {
   "users": [
     {
       "id": 55,
       "name":"gavin",
       "is_auth_blocked": false,
       "last_seen": null,
       "comments": null,
       "password_Created_at": "2025-10-09T23:29:33.797"
    },
    {
       "id": 2,
       "name": "robert",
       "is_auth_blocked": false,
       "last_seen": null,
       "comments": "",
       "password_created_at": "2024-09-20T19:54:55.599"
   },
   {
      "id": 54,
      "name": "xiaojun",
      "is_auth_blocked": false,
      "last_seen": null,
      "comments": "",
      "password_created_at": "2025-10-09T23:29:33.797"
   }
  ],
  "total": 3
 }
}
```

1180781- New password changer for FortiOS 7.6.3 or higher

Starting FortiPAM 1.8.0, a new *SSH Password (FortiOS 7.6.3 and higher)* password changer available to support a new change for FortiOS 7.6.3 and above.

1185540- SSH script new line mode setting

In FortiPAM 1.8.0, a new *New Line Mode* setting available when creating/editing a job entry in *Secrets > Jobs*.

Additionally, the *New Job* window has been refactored for improved user experience.

1186608- *Powershell* job support

Starting FortiPAM 1.8.0, FortiPAM supports the *Powershell* job type.

A new *Powershell* option is available in the *Type* dropdown when creating or editing a job in *Secrets > Jobs*.

1180921- Support multiple ZTNA tunnels: New *Service Address* field type

Starting FortiPAM 1.8.0, FortiPAM now supports a new field type called *Service Address*, which allows administrators to define one or more service access points (such as IP address ranges, FQDNs, or CIDR blocks) associated with a secret.

Each *Service Address* represents a network endpoint with an optional port or port range.

This is useful for secrets that connect to multiple network services or systems sharing similar credentials.

Each *Service Address* entry supports the following formats:

Format	Description	Example
`<ip>[-<ip>]:<port>[<port>]`	Single IP address or an IP address range with a specific port or port range.	`192.168.10.1 - 192.168.10.5:22-25`
`<CIDR>:<port>[<port>]`	Subnet with optional port range.	`192.168.10.0/24:443`
`<FQDN>:<port>[<port>]`	Fully Qualified Domain Name (FQDN) with optional port range.	`example.com:8080 - 8085`
`<ip>[-<ip>]`	IP address or IP address range only.	`192.168.10.10 - 192.168.10.15`

When defining a launcher supporting *Service Address* field, ensure that *Start FortiClient Session in Multiprocess Mode* is enabled.

Benefits:

- The *Service Address* field type provides administrators with flexible, structured control over how network endpoints are defined within secrets.
- It is ideal for environments where multiple service IP addresses or subnets share the same authentication credentials, while maintaining compatibility with OT-type launchers and manual target selection.

Restrictions and notes:

- **Mutual exclusivity**-
  Templates containing *Service Address* cannot include other address-type fields such as *Target Address*, *Domain*, or *URL*.
- **Launcher compatibility**-
  Templates with a *Service Address* field supports OT-Client launchers only.
- **Password verification/change**-
  Secrets with *Service Address* fields do not support password verification or password changer features.
- **Target selection**-
  When a template contains a *Service Address* field, auto-match creation for targets is disabled.
  Targets must be manually selected from those with *Service Address* settings.
- **Hidden settings**-
  When using a *Service Address* field, unrelated settings such as *Web Proxy* or *Domain/URL* fields are hidden.

User/Group

1168964- Support Regular Expression match for a JWT user

Starting FortiPAM 1.8.0, FortiPAM now supports the following two match methods to authenticate a JWT user:

- *Exact Match*
- *Regex Match*

1179107- Concurrent secret launch limitation

The maximum number of secrets a user can launch simultaneously is restricted.

A new global setting *Max Launched Sessions* available in the *Advanced* pane in *System > Settings*.

Note: By default, applies to all users.

A new *Max Launched Sessions* setting in *User Details* when creating/editing a user.

Note: This setting is configured per user.

1192528- Auto provision email address and display name for SAML users

Starting FortiPAM 1.8.0, FortiPAM supports getting user display name and email address for auto provision SAML user when the two fields are configured in the remote SAML IdP and are included in the SAML response.

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

- *Display Name*
- *Email address*

When configuring a SAML server, the following two new fields are available:

- *Attribute used to identify display name*
- *Attribute used to identify email address*

The following CLI command has been introduced:

```
config user saml
 edit "fortipam-saml-sso-server"
  set email-attr "email" #email
  set display-name-attr "disname" #display name
 next
end
```

For every user, there is a new configuration supported to store the user display name for both local and remote users.

Once the user display name is configured, it shows on the top-right beside the username.

```
config system admin
 edit "pam_saml"
  set remote-auth enable
  set accprofile "Default Administrator"
  set display-name "fortinet" #display name
  set force-saml-login enable
  set email-to "pam_saml@fortinet.com"
 next
end
```

In the FortiPAM 1.8.0 GUI, *Display Name* and *Email address* are configured so as to match the attribute value in the SAML IdP.

FortiPAM auto provisions the SAML users from the remote IdP server with best effort.

Notes:

1. When no display name or email address information synchronizes from the remote server, the administrator can edit those fields.
2. After auto provisioned 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.

1172128, 1228968- User SSO cache

Starting FortiPAM 1.8.0, FortiPAM now caches each user's last-selected SSO provider.

On subsequent logins, the system automatically uses the previously chosen provider.

When launching a secret, the previously available *SSO User* option has been renamed to *Authenticate using PAM login credentials*.

1192051- New flag for SAML authentication: SAML assertion and response must be signed

Starting FortiPAM 1.8.0, a new `require-signed-resp-and-asrt` flag has been introduced for SAML authentication.

When the flag is enabled, FortiPAM expects both SAML assertion and response to be signed.

```
config user saml
 edit x
  set require-signed-resp-and-asrt {enable | disable} #default = disable
 next
end
```

System/Log

930125- FQDN setting for request email notification

Starting FortiPAM 1.8.0, a new *Proxy FQDN* field is available in the *Advanced* tab in *System > Settings*.

The new *Proxy FQDN* setting allows you to set up the FortiPAM FQDN used for email notifications.

1139972- New invitee list page

A new *Invited Users* tab in *Monitoring*.

You can now revoke invitation from an invitee.

A new *Invitation* tab in the *Secret Events & Videos* dropdown in the *Logs* tab in *Log & Report > Secret Event & Video* informing you about the status of an invitation.

1184826, 1191610- Concurrent logon licensing (VM only)

Starting FortiPAM 1.8.0, FortiPAM introduces a new type of FortiPAM Concurrent Logon License (FCLL, `SKU-1303`) to support concurrent logon sessions based on the purchased license seats.

1. With FCLL, seats mean maximum concurrent logon sessions instead of the enabled user count.
2. The number of enabled users can be up to 3000 (maximum user capacity in the system).
3. Floating license in HA is applicable to FCLL.
4. HA nodes must have the same FCLL license type, i.e., `SKU-1303`.
5. When the active logon sessions hit the licensed concurrent logons, i.e., maximum concurrent logons allowed, any new login attempt is rejected with the following error message:

   ```
   Concurrent Logon Limit Reaced
   The concurrent logon limit has reached the limit allowed by license.
   ```

```
Please try again later.
```

6. In *Dashboard*, on the *Virtual Machine* widget, a new *Concurrent License* entry displays FCLL is being used.
7. In *Dashboard*, on the *Licenses* widget, when you hover over *Subscription License*, the maximum licensed concurrent logons and the active concurrent logons are displayed.

988761- Auto-disabling for auto-provisioned remote users

Starting FortiPAM 1.8.0, auto-provisioned remote users can be automatically disabled due to prolonged inactivity.

This frees up user license seats by automatically disabling inactive accounts.

A new *User Max Inactivity Days* field available in the *Other* pane in *Advanced* tab in *System > Settings*.

When a user is disabled, a system log entry is generated.

You can view it in the *Logs* tab in *Log & Report > System Event* under *User Events*.

Setting the *User Max Inactivity Days* field to `0` disables the feature. Inactive users are not automatically disabled and remain in the system indefinitely.

1138886, 1180154- Limit users to log in to some interfaces

Starting FortiPAM 1.8.0, a new *Allowed Access Portal Roles* setting available when editing a network interface in *Network > Interfaces*.

From *Allowed Access Portal Roles*, you can select a role.

Only users whose role is selected are allowed to log in.

Alternatively, use the following new CLI command to only allow users with selected role to log in:

```
config system interface
 edit "port1"
  set gui-access-role <roles>
 next
end
```

1133468- Support key-based SFTP authentication for remote video storage

Starting FortiPAM 1.8.0, a new *Authentication Method* dropdown is available in the *Remote Video Storage* tab in *System > Backup*.

From *Authentication Method* dropdown, choose the authentication method for the remote storage server:

- *Password*: Password of the remote storage server as the login credential.
- *Keypair*: Drag and drop/upload/paste the public/private key.

1195011- Support key- based SFTP authentication for auto-backup

Starting FortiPAM 1.8.0, a new *Authentication Method* dropdown is available in the *Configuration Backup* tab in *System > Backup*.

From *Authentication Method* dropdown, choose the authentication method for auto-backup:

- *Password*: Password of the remote storage server as the login credential.
- *Keypair*: Drag and drop/upload/paste the public/private key.

Note: The new *Authentication Method* setting is only available when *Server Type* is *SFTP server*.

1192909- Secret log enhancements

Starting FortiPAM 1.8.0, the following new secret log related enhancements have been introduced:

1. For *SSMS* and OT type launchers (*TIA Portal*, *TIA Portal V16 Logon*, *TIA Portal V19 Logon*), a new *Session Close Log* setting is available when you open the launcher (*Secret Settings > Launchers*):
   a. *Single*: Only a single session close log is saved.
      Note: This is the legacy secret log behavior.
   b. *Multiple*: All the session close logs are saved.
      Note: All the connections during a session are recorded and available in the secret log table.

   Note: For all the other launchers, *Session Close Log* is *Multiple*.
2. New *Secret connection started* secret log message.
   This new log message indicates when FortiPAM establishes connection to the target (*Operation*: *Target connected*, *Message*: *Secret connection started*).
3. Corresponding to the *Target connected* operation, there is now a new *Target disconnected* operation.
   The *Secret session ended* log message has been renamed to *Secret connection stopped*.
4. For *Web Browsing*, *Web SFTP*, *Web SMB* launchers, the log message is updated similar to 2 and 3 while keeping the legacy log.

1189656- System/secret logs pushed to Syslog server

After enabling/setting up *Send logs to syslog* in *Log & Report > Log Settings*, FortiPAM pushes the system and secret logs to the Syslog server, e.g., a FortiSIEM device.

Others

1203822- New FortiPAM 1100G hardware model

Starting FortiPAM 1.8.0, FortiPAM now supports a new FortiPAM 1100G hardware model.

For information on configuration capacity for the FortiPAM 1100G hardware model, Configuration capacity for FortiPAM hardware appliances and VM on page 29.

Note:

1. When connecting with a FortiAnalyzer device, FortiAnalyzer 7.6.5 or higher is required.
2. When connecting with EMS, EMS 7.4.1 or higher is required.

1189833- New FortiPAM 3100G hardware model

Starting FortiPAM 1.8.0, FortiPAM now supports a new FortiPAM 3100G hardware model.

For information on configuration capacity for the FortiPAM 3100G hardware model, see Configuration capacity for FortiPAM hardware appliances and VM on page 29.

Note:

1. When connecting with a FortiAnalyzer device, FortiAnalyzer 7.6.5 or higher is required.
2. When connecting with EMS, EMS 7.4.1 or higher is required.

1227940- FortiSRA consolidated into FortiPAM

In 1.8.0, FortiSRA has been consolidated into FortiPAM.

For information on migrating from FortiSRA to FortiPAM, see Migration from FortiSRA to FortiPAM on page 27.

Note:

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.

1236701- FortiPAM on OCI

Starting 1.8.0, FortiPAM is compatible with Oracle Cloud Infrastructure (OCI), including:

- Oracle Public Cloud (OPC)
- Dedicated Region Cloud@Customer (DRCC)

Note:

1. Log and video disk encryption is not supported.
2. Virtual Trusted Platform Module (vTPM) is not supported.

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

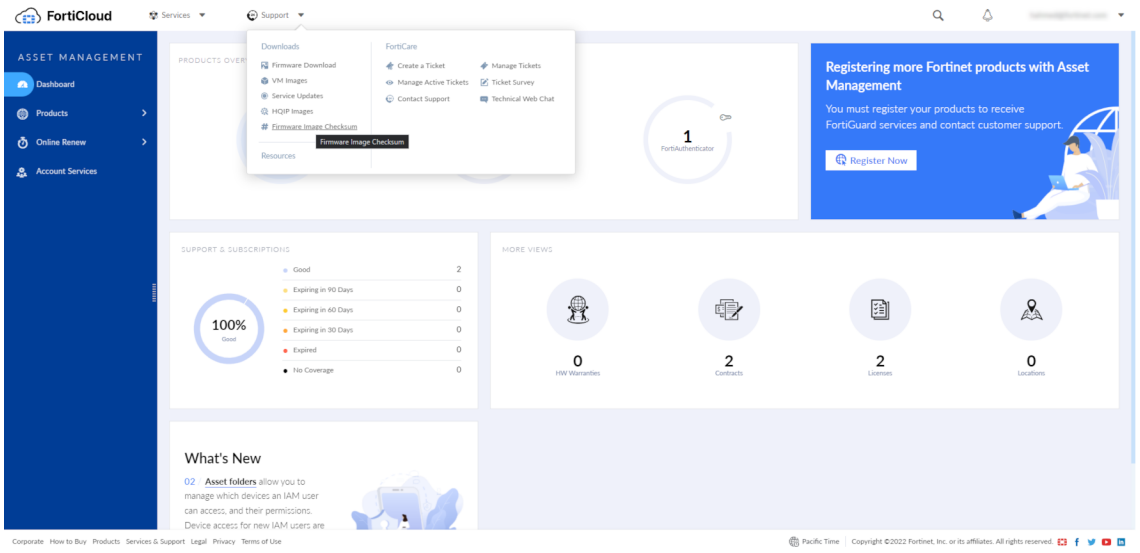
To verify the integrity of the firmware file, use a checksum tool to compute the firmware file's MD5 checksum. Compare it with the checksum indicated by Fortinet. If the checksums match, the file is intact.

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:

From	To
1.6.x	1.8.0
1.7.x	1.8.0

Product integration and support

FortiPAM 1.8.0 supports the following:

Web browser support

FortiPAM version 1.8.0 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 1.8.0 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 1.8.0 supports the following FortiPAM hardware models:

FortiPAM 1000G
FortiPAM 1100G
FortiPAM 3000G
FortiPAM 3100G

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
1211000	Secret approvals do not send emails when using approval groups rather than users.
1221265	Scheduled LDAPs password change failure (reconcile mode).
1210740	Unable to change the password changer in a new template under *Secret Settings*.
1212330	*List* secret permission causes the secret page to not load.

User/Group

Bug ID	Description
1216736	IPv4 *Trusted Hosts* does not work for API users.

System/Log

Bug ID	Description
1172633	Backup malfunction.
1210728	Remove "DR" terminology from the HA configuration.

Others

Bug ID	Description
1219623	(GMT+2:00) Cairo DST not taking effect.
1208346	Lost connectivity to the FortiPAM GUI WAD crashes.

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.

User/Group

Bug ID	Description
1218938	FortiIdentity Cloud active code 64 not supported on TOTP.

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 1000G	FortiPAM 1100G	FortiPAM 3000G	FortiPAM 3100G	FortiPAM-VM
Secret	50000	50000	100000	100000	100000
Target	5000	5000	10000	10000	10000
Folder	2000	2000	6000	6000	6000
User	3000	3000	3000	3000	3000
User group	2000	2000	5000	5000	5000
Request	5000	5000	10000	10000	10000
Gateway	256	256	256	256	256

www.fortinet.com