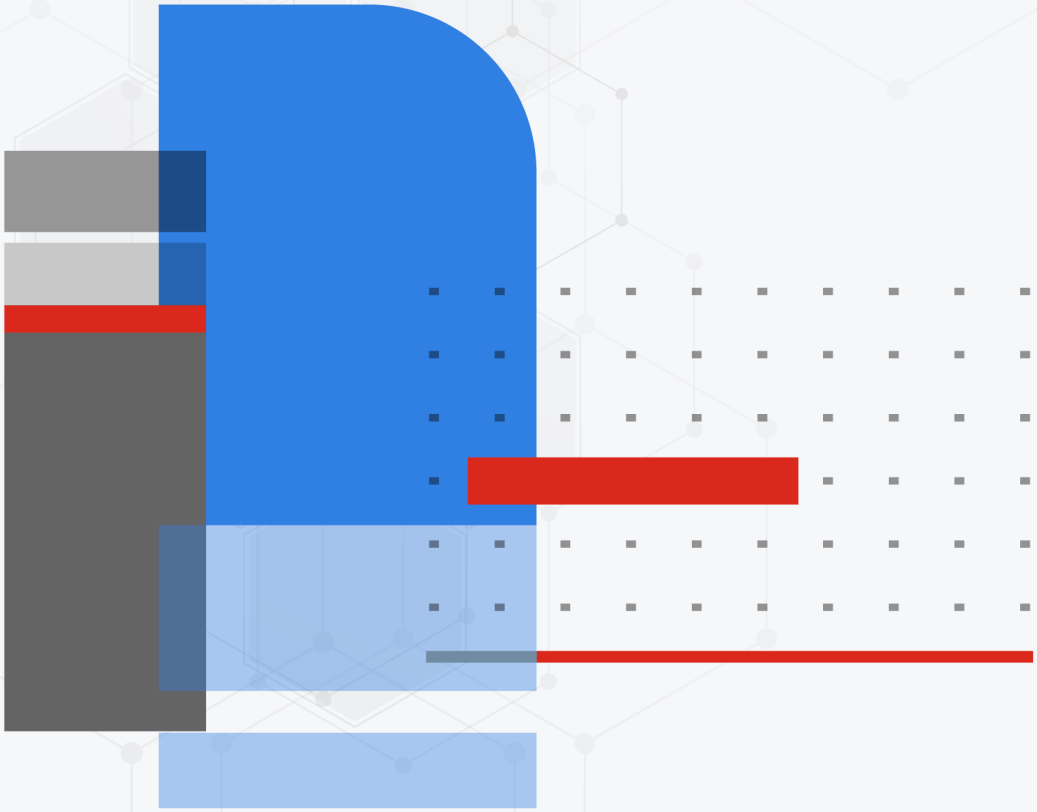
Administration Guide

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

May 8, 2024
FortiPAM 1.1.2 Administration Guide
74-112-899871-20240508

TABLE OF CONTENTS

Change Log

Date	Change Description
2023-08-28	Initial release.
2023-09-20	Updated Creating a secret on page 49.
2023-11-16	Updated FortiAnalyzer logging on page 233.
2023-11-23	Updated Secret list on page 47.
2023-12-08	Renamed *FortiPAM Password Filler* to *Fortinet Privileged Access Agent* across the Admin Guide.
2023-12-20	Updated Personal/public folder on page 73.
2023-12-21	Updated Email alert settings on page 215 and Settings on page 237. Added Testing the email service connection example on page 242.
2024-01-16	Updated Appendix B: Installation on VMware on page 295.
2024-01-23	Updated Launchers on page 103.
2024-05-08	Updated Creating a secret on page 49 and Launching a secret on page 62.

Introduction

FortiPAM is a privileged access management solution. FortiPAM solutions are an important part of an enterprise network, providing role-based access, auditing, and security options for privileged users (users that have system access beyond that of a regular user).

FortiPAM delivers the following functionalities:

- **Credential vaulting:** Users do not need credentials, reducing the risk of credential leaking as no sensitive data is on the user system after a session. Passwords are automatically changed.
- **Privileged account access control:** Users can only access FortiPAM resources based on their roles (standard user or admin user).

  FortiPAM offers secret permission control to access a target server. Admin users can define common policies and a hierarchical approval system for standard users to access sensitive information. FortiPAM also provides options to control risky user activities such as a user attempting to encrypt the disk.

  FortiPAM offers ZTNA tag-based and protocol-based access control (RDP, SSH, VNC, and WEB) and allows access from anywhere, including native web-based access.
- **Privileged activity monitoring and recording:** FortiPAM can monitor, record, and audit privileged user activities.

  FortiPAM provides information on sessions, user keystrokes, and mouse events.

FortiPAM concepts

FortiPAM user

There are two types of FortiPAM user:

- Standard user: Performs management tasks on the target system, e.g., IT staff, IT contractor, Database Administrator (DBA). Standard users are typically IT Managers and IT System Admins.
- Admin user: Performs management tasks on FortiPAM server.

Target

A server/device with a privileged account supporting RDP, SSH, Web, or other admin protocols. Target systems include Windows workstation, Windows domain controller, Web server, Unix server, SQL- server, router, or firewall.

Secrets

The secrets contain information on login, credentials, and the target server IP address. Secrets are core assets in FortiPAM representing methods and credentials to access target systems in your organization.

Launchers

Launchers help users gain remote access to a target without needing to know, view, or copy the password stored in FortiPAM.

Launchers can invoke client-side software on the FortiPAM user's endpoint, which is software to perform management tasks, e.g., Internet Explorer, PuTTY(ssh), RDP client, and SQL-commander.

Folders

Folders help manage a large number of secrets efficiently by organizing them in a hierarchical view. You can organize customers, computers, regions, branch offices, etc., into folders.

You can quickly look for secrets from the folder tree view.

Granting permissions becomes faster as secrets in a folder share the same permission and policy.

Organization of the guide

The FortiPAM Administration Guide contains the following sections:

- FortiPAM installation on page 23 describes basic setup information for getting started with your FortiPAM.
- Licensing on page 29 describes how to register, download, and upload your FortiPAM-VM license.
- Dashboard on page 35 contains widgets providing performance and status information.
- Secrets on page 46 describes features and options related to secrets, folders, secret and job requests, approval lists, and jobs.
- Secret settings on page 92 describes features and options related to templates, launchers, policies, addresses, approval profiles, password changers and policies, character sets, antivirus, DLP, DLP file pattern, SSH filter profiles, and integrity check.
- User management on page 157 describes managing FortiPAM user database.
- Monitoring on page 199 contains information on user logins and active sessions on FortiPAM.
- Log & report on page 201 describes how to view logs and reports on FortiPAM.
- Network on page 221 describes configuring interfaces, static routes, DNS settings, fabric connectors, and packet capture.
- System on page 237 describes managing and configuring basic system settings for FortiPAM. It also contains settings related to ZTNA, HA, certificates, SNMP, automatic backups, firmware, FortiPAM and FortiGuard licenses.

Using the GUI

This section presents an introduction to the graphical user interface (GUI) on your FortiPAM.

The following topics are included in this section:

- Banner on page 10
- Tables on page 15

For information about using the dashboards, see Dashboard on page 35.

Banner

Along the top of each page, the following options are included in the banner:

- Open/close side menu
- *Search icon*: opens GUI based global search. See GUI based global search on page 10.
- Build number

In the build number dropdown, select *Hide Label* to hide the build number.

- *CLI console (**)*: opens the CLI console. See CLI commands on page 11.
- *Help (**)*: opens the online help document.
- *Notifications (**)*: shows latest notifications.
- *Theme*: from the dropdown, select one of the available themes.
- *Admin*: from the dropdown, see FortiPAM version and build, go to system and configuration, change password, or log out. See Admin on page 11.

GUI based global search

The global search option in the GUI allows users to search for keywords appearing in objects and navigation menus to quickly access the object and configuration page. Click the magnifying glass icon in the top-left corner of the banner to access the global search.

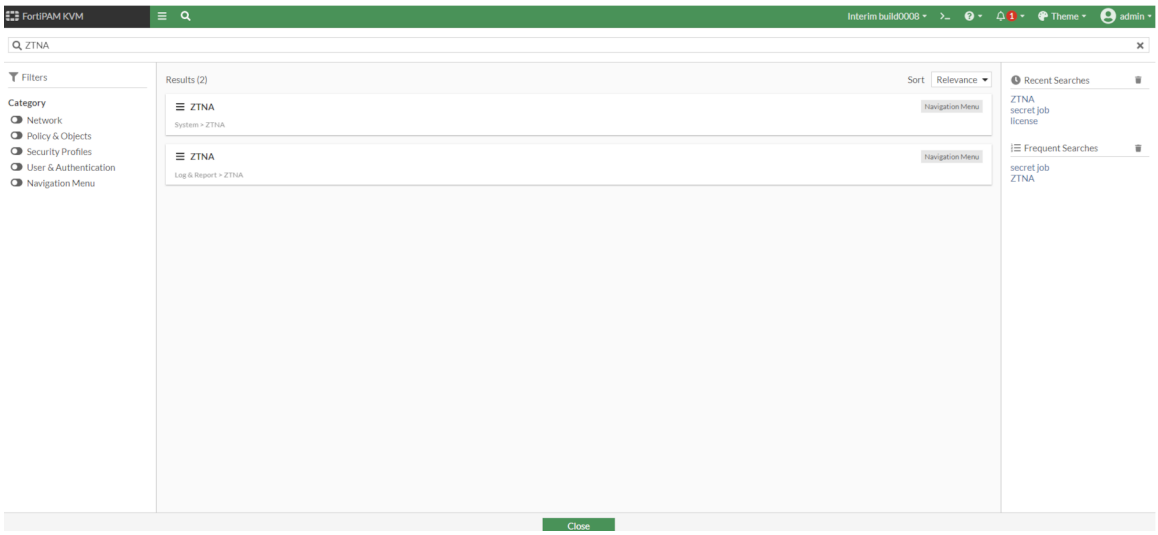
The global search includes the following features:

- Keep a history of frequent and recent searches
- Sort results alphabetically by increasing or decreasing order, and relevance by search weight
- Search by category
- Search in Security Fabric members (accessed by the Security Fabric members dropdown menu in the banner)

Global search example - Example

In this example, searching for the word ZTNA yields the following results:

- *ZTNA* in *System*
- *ZTNA* in *Log & Report*



CLI commands

FortiPAM has CLI commands that are accessed using SSH or Telnet, or through the CLI console if a FortiPAM is installed on a FortiHypervisor.

To open a CLI console, click the >_ icon in the top right corner of the GUI. The console opens on top of the GUI. It can be minimized and multiple consoles can be opened.

CLI commands can be used to initially configure the unit, perform a factory reset, or reset the values if the GUI is not accessible.

The FortiPAM-VM's console allows scrolling up and down through the CLI output by using `Shift+PageUp` and `Shift+PageDown`.

Like FortiOS, the `?` key can be used to display all possible options available to you, depending upon where you are hierarchically-situated.

Admin

The Admin dropdown contains the following information and options:

- FortiPAM build number and version.
- *System*: activate glass breaking mode, maintenance mode, reboot, shutdown, and upload a firmware.

The following actions can only be performed when FortiPAM is in maintenance mode:

- Reboot.
- Shutdown.
- Uploading a firmware. See Uploading a firmware on page 13.
- Uploading a license. See Licensing on page 29.
- Restoring a configuration. See Backup and restore on page 14.

- *Configuration*: backup, restore, see configuration revisions, and run configuration scripts.
- *Change Password*: opens the *Edit Password* window where you can change the administrator password.
- *Logout*: log out of FortiPAM.

Glass Breaking mode

The glass breaking mode gives you access to all secrets in the system.

Glass breaking in FortiPAM means extending the user permission to access data that the user is not authorized to access. Typically, user access is controlled by permission defined in every secret and folder. In a rare situation, such as a network outage or the remote authentication server becoming unreachable, glass breaking allows you to temporarily access important secrets and target servers to resolve issues.

As a best practice, only a few administrators should have access to the glass breaking mode. Further, the glass breaking mode should only be activated under exceptional situations and for disaster recovery. Email notifications can also be configured to send alerts whenever someone enters glass breaking mode. See Email alert when the glass breaking mode is activated example on page 217.

Under glass breaking mode, all administrator activities should be logged for future audits.

Only a user configured with glass breaking permission can activate the glass breaking mode. The permission is defined when configuring a user role in *User Management* > *Role*. See Role on page 174.

When an administrator activates glass breaking mode on FortiPAM, the administrator can bypass normal access control procedures, get access to all folders, secrets, and secret requests, and launch any secret.

To enter glass breaking mode:

1. From the user dropdown on the top-right, select *Activate Glass Breaking Mode* in *System*.
2. Enter a reason for activating the glass breaking mode.
3. Click *OK*.
   The GUI is refreshed, and a red banner is shown on the top: *FortiPAM is in glass breaking mode*.

To deactivate glass breaking mode:

1. From the user dropdown on the top-right, select *Deactivate Glass Breaking Mode* in *System* to deactivate the glass breaking mode.
   The GUI is refreshed, and a message appears on the bottom-right: *Successfully demoted user*.

When you are in the glass breaking mode, FortiPAM enforces video recording on launching a session.

To disable video recordings when in glass breaking mode:

1. Go to *System* > *Settings*.
2. In the *PAM Settings* pane, disable *Enforce recording on glass breaking*.
3. Click *Apply*.

Activate maintenance mode

Suspend all critical processes to allow maintenance related activities.

Uploading a firmware

You can only upload a firmware when in maintenance mode.

To enter maintenance mode:

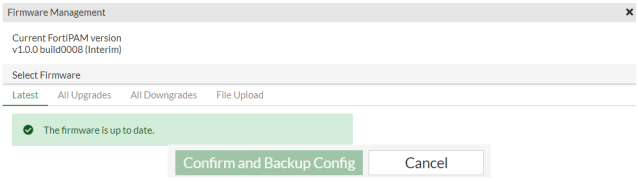
1. From the user dropdrown, select *Activate Maintenance Mode* in *System*.
2. In the *Warning* dialog:
   a. Enter the maximum duration, in minutes.
   b. Enter a reason for activating the maintenance mode.
   c. Click *OK*.

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.

To upload a firmware:

1. In the user dropdown, go to *System* > *Firmware*.
   The *Firmware Management* window opens.



The following options are available:

Latest	Displays the status of the current firmware.

All Upgrades	Displays if new upgrades are available.
All Downgrades	Displays if downgrades are available.
File Upload	Allows you to upload a new firmware image manually.

2. Go to *File Upload*:
   a. Select *Browse*, then locate the firmware image on your local computer.
   b. Click *Open*.
3. 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.

Backup and restore

Fortinet recommends that you back up your FortiPAM configuration to your management computer on a regular basis to ensure that, should the system fail, you can quickly get the system back to its original state with minimal effect to the network. You should also perform a back up after making any changes to the FortiPAM configuration.

You can encrypt the backup file to prevent tampering.

You can perform backups manually. Fortinet recommends backing up all configuration settings from your FortiPAM unit before upgrading the FortiPAM firmware.

Your FortiPAM configuration can also be restored from a backup file on your management computer.

To backup FortiPAM configuration:

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 restore FortiPAM configuration:

1. Enter maintenance mode. See Maintenance mode.
2. In 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*.
5. In *Password*, enter the encryption password.
6. 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.

Revisions

You can manage multiple versions of configuration files on FortiPAM.

Configurations scripts

Configuration scripts are text files that contain CLI command sequences. They can be created using a text editor or copied from a CLI console, either manually or using the Record CLI Script function.

Scripts can be used to run the same task on multiple devices.

A comment line in a script starts with the number sign (#). Comments are not executed.

To run a script using the GUI:

1. In the user dropdown, go to *Configuration* > *Scripts*.
2. Select *Run Script*.
3. In the *Run Script* window:
   a. Select either *Local* or *Remote* as the *Source*.
   b. Select *Browse*, then locate the script on your local computer.
   c. Click *Open*.
4. Click *OK*.
   The script runs immediately, and the table is updated, showing if the script ran successfully.

Tables

Many GUI pages contain tables of information that can be filtered and customized to display specific information in a specific way.

Some tables allow content to be edited directly on that table.

Navigation

Some tables contain information and lists that span multiple pages. Navigation controls will be available at the bottom of the page.

Filters

Filters are used to locate a specific set of information or content in a table. They can be particularly useful for locating specific log entries. The filtering options vary, depending on the type of information in the log.

Depending on the table content, filters can be applied using the filter bar, using a column filter, or based on a cell's content. Some tables allow filtering based on regular expressions.

Administrators with read and write access can define filters. Multiple filters can be applied at one time.

To create a column filter:

1. Select + in the search bar.
2. Select one of the columns as a filter.
3. In the window that opens, you can set combinations of *Contains*, *Exact Match*, and *NOT*.
4. Either enter a term or terms separated by `","` or `|`, or select from the list that appears.
5. Click *Apply*.

You can combine multiple filters by selecting + and repeating steps 2 to 5 for every new filter that you require.

Column settings

Columns can be rearranged, resized, and added or removed from tables.

To add or remove columns:

1. Right-click a column header, or click the gear icon on the left side of the header row that appears when hovering the cursor over the headers.
2. Select columns to add or remove.
3. Click *Apply*.

To rearrange a columns in a table:

1. Click and drag the column header.

To resize a column to fit its contents:

1. Select *Filter/Configure Column* from the column header.
2. In the window that opens, select *Resize to Contents*.
3. Click *Apply*.

To group contents by a column:

1. Select *Filter/Configure Column* from the column header.
2. In the window that appears, select *Group By This Column*.
3. Click *Apply*.

To resize all of the columns in a table to fit their content:

1. Right a column header, or click the gear icon on the left side of the header row that appears when hovering the cursor over the headers.
2. Click *Best Fit All Columns*.

To reset a table to its default view:

1. Right-click a column header, or click the gear icon on the left side of the header row that appears when hovering the cursor over the headers.
2. Click *Reset Table*.

Resetting a table removes applied filters.

To arrange contents in a column by ascending or descending order:

1. Click the up or down arrow to arrange contents in a column by ascending or descending order respectively.

To select multiple entries in a table:

1. Select the first entry.
2. Press and hold `ctrl`, select the second item, and so on.

Modes of operation

FortiPAM can operate in the following two modes:

- **Proxy**: All the launched traffic to the target server is forwarded to FortiPAM first. FortiPAM then connects to the target server. FortiPAM delivers fake credentials to the client machine. FortiPAM manages the credentials and login procedures to the target server.

  All the traffic except web browsing is proxied through FortiPAM.

  The proxy mode is more secure than the non-proxy mode as it does not deliver sensitive information to the client machine.

  In the proxy mode, the administrator can terminate traffic connections if improper user behavior is detected.

  Web SSH, Web RDP, Web VNC, Web SFTP, and Web SMB default launchers always use the proxy mode irrespective of the proxy settings.
- **Non-proxy**: All the launched traffic is directly connected to the target server without FortiPAM. FortiPAM delivers the credential information to the client machine. The native program, PuTTY or the website browser directly connects to the server.

  The direct connection (non-proxy) mode or the web browsing comes with an added risk of credential leakage. To reduce such risks, this mode is strictly controlled by user permissions.

  Users without sufficient permission cannot access direct mode or web browsing launchers.

  The following features do not work when FortiPAM is in non-proxy mode:

- SSH filters
- SSH auto password delivery
- Block RDP clipboard
- RDP security level

PuTTY and WinSCP launchers are not supported when the secret is in non-proxy mode, and the secret uses an SSH key for authentication.

TightVNC launcher is not supported when the secret is in non-proxy mode and requires a username for authentication.

When using launchers with non-proxy mode, launchers may require the environment to be initialized beforehand. You may specify this with init-commands and clean-commands.

Note: Init-commands and clean-commands only run in the non-proxy mode.

To select the mode of operation, see the *Proxy Mode* option when creating or editing a secret. See Creating a secret on page 49. Alternatively, see the *Proxy Mode* option when creating or editing a policy. See Creating a policy on page 113.

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.

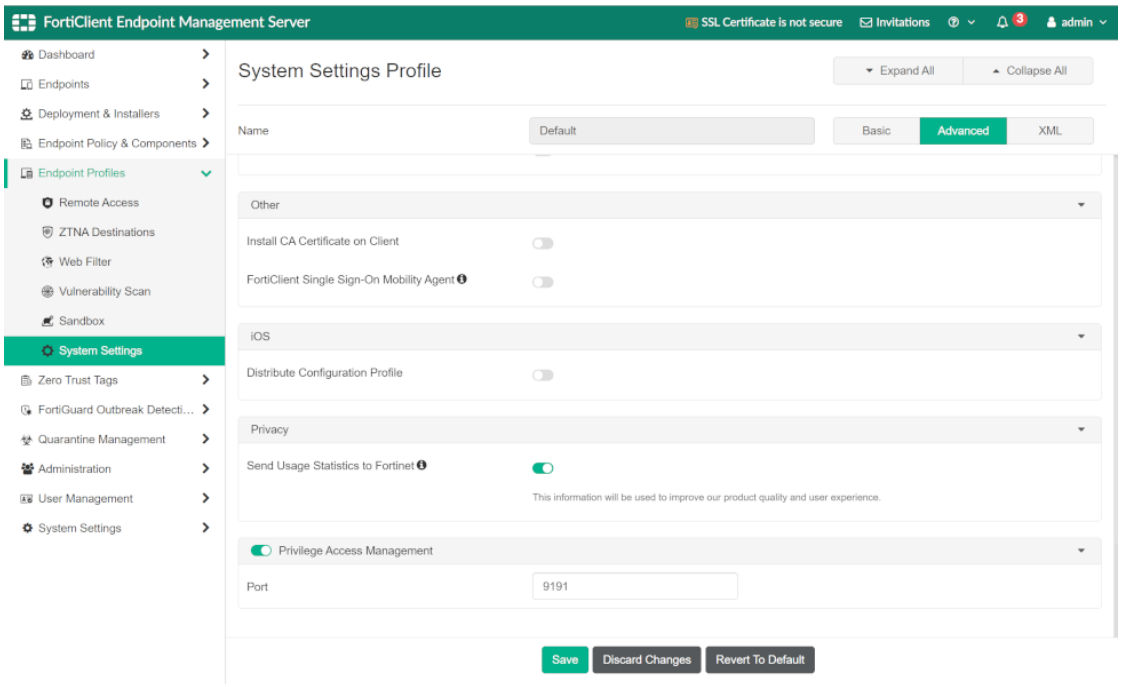
When EMS is not available, standalone FortiClient is recommended. With standalone FortiClient, native launchers such as PuTTY, RDP, VNC Viewer, Tight VNC, and WinSCP can be used to connect to the target server and user can take advantage of functionalities provided by these applications. Also, video 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*.
         iv. In *Port*, enter 9191.

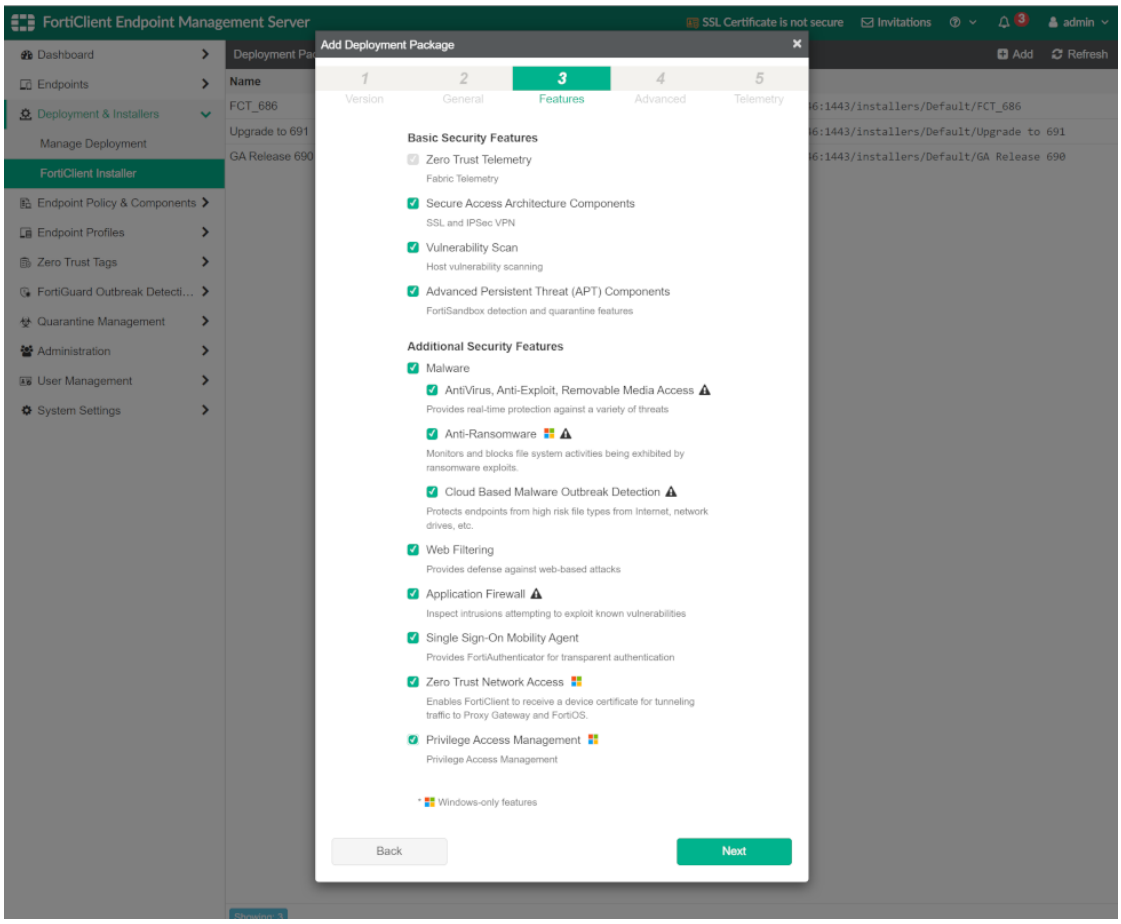
v. Click *Save*.



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.

Feature availability

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

FortiPAM installation

This chapter provides basic setup information for getting started with your FortiPAM.

FortiPAM is a server-side machine. FortiClient is required to be installed on the client side to use the native program on Windows.

The following virtualization environments are supported by FortiPAM 1.1.2:

- VMware ESXi/ ESX 6.5 and above
- KVM
- Microsoft Hyper-V
- Microsoft Azure

FortiPAM supports both Linux and Windows environments.

On Windows, the user may install FortiClient which includes fortivrs as a recording daemon, fortitcs as ZTNA daemon and a chrome extension. With FortiClient installed, the privileged activity recording can be supported. Without it, only web mode can be supported.

See Installing FortiClient with the FortiPAM feature on page 23 and FortiPAM appliance setup on page 24.

Installing FortiClient with the FortiPAM feature

To install FortiClient:

1. Install Google Chrome web browser.
2. Install FortiClient on your endpoint system.
   See the *FortiClient Administration Guide* on the Fortinet Docs Library.

   Ensure that the ZTNA and PAM features are enabled during installation.

   Ensure that no other FortiClient version is installed. If another FortiClient version has already been installed, it should first be uninstalled before installing the FortiPAM version. See Uninstalling FortiClient.
3. Reboot the PC.

Chrome, Firefox, and Edge can automatically install *Fortinet Privileged Access Agent* in addition to fortivrs and fortitcs daemons.

Uninstalling FortiClient

To uninstall FortiClient:

1. Disconnect the FortiClient from EMS.
2. From the *System Tray*, right-click FortiClient, and select shutdown FortiClient.
3. Uninstall FortiClient.
4. Reboot the PC.

FortiPAM appliance setup

Before using FortiPAM-VM, you need to install the KVM or the VMware application to host the FortiPAM-VM device. The installation instructions for FortiPAM-VM assume you are familiar with KVM or the VMware products and terminology.

FortiPAM-VM image installation and initial setup

See Appendix A: Installation on KVM on page 292.

See Appendix B: Installation on VMware on page 295.

See Appendix F: Installation on Hyper-V on page 305.

See Appendix G: Installation on Azure on page 316.

Once FortiPAM-VM is powered on:

1. At the login prompt, enter `admin` and hit *Enter*.
   By default, there is no password, however, a password must be set before you can proceed. Enter and confirm the new administrator password.
2. At the CLI prompt, enter `show system storage` to verify the disk usage type for the two added hard disks. The output looks like the following:

Administrators need to configure a dedicated FortiPAM video disk for video recording.

Two hard disks and two virtual network interface cards need to be added to the VM in VM manager before FortiPAM image installation.

See Appendix A: Installation on KVM on page 292.

```
config system storage
   edit "HD1"
      set status enable
      set media-status enable
      set order 1
      set partition "LOGUSEDXDE8326F6"
      set device "/dev/vda1"
      set size 20023
      set usage log
```

```
    next
    edit "HD2"
       set status enable
       set media-status enable
       set order 2
       set partition "PAMVIDEOB471724F"
       set device "/dev/vdb1"
       set size 20029
       set usage video
    next
end
```

3. Enter the following CLI commands to set up FortiPAM:

```
config system interface
   edit "port1"
      set ip 172.16.x.x/x #Depending on your network setting
      set allowaccess ssh https http
      set type physical
      set snmp-index 1
   next
   edit "port2"
      set ip x.x.x.x/x
      set allowaccess ssh https http
      set type physical
      set snmp-index 2
   next
end
config router static
   edit 1
      set gateway x.x.x.x
      set device "port1"
   next
end
```

4. FortiPAM requires license. To upload a license. See Licensing on page 29.
   If the network layout is unable to resolve the correct external FortiGuard server after an external DNS server is set, enter the following commands:

```
config system fortiguard
   set fortiguard-anycast disable
   unset update-server-location
   unset sdns-server-ip
end
```

   Optionally, enter the following commands to use the external FortiGuard server in case the FortiGuard server cannot be correctly resolved:

```
config system central-management
   config server-list
      edit 1
         set server-type update rating
         set server-address <addr>
      next
   end
   set include-default-servers disable
end
```

5. To improve security, disable HTTP on the physical interface:

```
config system interface
   edit "port1"
      set allowaccess ssh
```

```
    next
    edit "port2"
       set allowaccess ssh
    next
  end
```

6. Enter the following CLI commands to configure the firewall.
   The CLI commands are used to allocate a static IP address as the virtual IP address for FortiPAM. The static IP address is used as FortiPAM GUI server IP address.

```
config firewall vip
   edit "fortipam_vip"
      set type access-proxy
      set extip 172.16.xxx.xxx #use an external visible virtual IP address that can be
           same as the port1 interface
      set extintf "any"
      set server-type https
      set extport 443
      set ssl-certificate "Fortinet_SSL"
   next
end
```

7. On a web browser, go to `https://172.16.xxx.xxx` to access FortiPAM GUI using the virtual IP address.

To update a firmware image:

1. Enter maintenance mode. See Maintenance mode.
2. In the user dropdown on the top-right, go to *System* > *Firmware*.
   The *Firmware Management* window opens.
3. Go to *File Upload*:
   a. Select *Browse*, then locate the `image.out` FortiPAM firmware image on your local computer.
   b. Click *Open*.
4. Click *Confirm and Backup Config*. FortiPAM then reboots and the firmware has been updated.

FortiPAM may take few minutes to reboot.

FortiPAM with TPM

FortiPAM supports TPM (Trusted Platform Module) to improve protection for secret credentials.

TPM should be enabled when you initially install FortiPAM.

If you enable TPM after secrets have been configured on FortiPAM, secret credentials may be corrupted.

To check if the FortiPAM hardware device has TPM capability:

1. Before enabling TPM on FortiPAM, enter the following CLI command:

```
diagnose tpm selftest
```

If the output is `Successfully tested. Works as expected`, then TPM is installed on your FortiPAM hardware device.

To enable TPM on FortiPAM hardware device:

1. In the CLI console, enter the following commands:
```
config system global
   set private-data-encryption enable
end
```

FortiPAM-VM with vTPM enabled

If FortiPAM is a VM instance, the vTPM (virtual TPM) package must be installed, and vTPM enabled then.

See Appendix C: Installing vTPM package on KVM and adding vTPM to FortiPAM-VM on page 300.

On FortiPAM-VM, TPM can only be enabled after enabling vTPM.

To enable vTPM on FortiPAM-VM:

1. In the CLI console, enter the following commands:
```
config system global
   set v-tpm enable
end
```

To enable TPM on FortiPAM-VM:

FortiPAM-VM must be in maintenance mode to change TPM settings.

1. In the CLI console, enter the following commands:
```
config sys maintenance
   set mode enable
end
config system global
   set private-data-encryption enable
end
Be carefull!!!This operation will refresh all ciphered data!
Backup the current configuration file at first!
Do you want to continue? (y/n)y
Please type your private data encryption key (32 hexadecimal numbers):
0123456789abcdef0123456789abcdef
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
0123456789abcdef0123456789abcdef
Your private data encryption key is accepted.
```

The key must be the same for data restoration between source FortiPAM and destination FortiPAM.

To disable TPM:

1. In the CLI console, enter the following commands:

```
config sys maintenance
   set mode enable
end
config system global
   set private-data-encryption disable
end
Be carefull!!!This operation will refresh all ciphered data!
+Backup the current configuration file at first!
+Do you want to continue? (y/n)y
```

For FortiPAM-VM, vTPM should be disabled after disabling TPM.

To disable vTPM for FortiPAM-VM:

1. In the CLI console, enter the following commands:

```
config system global
   set v-tpm disable
end
This operation will stop using vTPM module
Do you want to continue? (y/n)y
```

Connecting to target remote systems

Requirements to connect to a target server or PC:

1. Install PuTTY using default settings. See Download PuTTY.
2. Optionally, install VNC Viewer. See Download VNC Viewer.
3. Optionally, install TightVNC. See Download TightVNC.
4. Optionally, install WinSCP for file transfer. See Download WinSCP.
5. Optionally, you can engage web browser-based SSH, RDP, or VNC remote connections in the absence of FortiClient.

Licensing

FortiPAM platforms work in evaluation mode until licensed.

In the evaluation mode:

1. A maximum of 2 users are allowed; a default *Super Administrator* and an additional user.
2. You can log in to the firewall VIP using `https`.
3. The evaluation license expires after 15 days.
4. All the features are available. You can create secret and launch secrets for a target server.
5. FortiPAM does not have a valid serial number.
6. No FortiCare support is available.

FortiPAM configured with less than 2 CPUs and 2048 MB of RAM works in the evaluation mode until licensed. Otherwise, a valid license is required.

DLP is available for secret launching only when you have a valid Advanced Malware Protection (`AVDB & DLP`) license.

Registering and downloading your license

After placing an order for FortiPAM-VM, a license registration code is sent to the email address used in the order form. Use the license registration code provided to register the FortiPAM-VM with FortiCloud.

Upon registration, download the license file. You will need this file to activate your FortiPAM-VM. You can configure basic network settings from the CLI to complete the deployment. Once the license file is uploaded, the CLI and GUI are fully functional.

1. Go to FortiCloud and create a new account or log in with an existing account.
   The *Asset Management* portal opens.
2. On the *Asset Management* portal, click *Register Now* to register FortiPAM.
3. Provide the registration code:
   a. Enter a registration code.
   b. Choose your end user type as either a government or non-government user.
   c. Click *Next*.
4. The *Fortinet Product Registration Agreement* page displays. Select the check box to indicate that you have read, understood, and accepted the service contract. Click *Next*.
5. The *Verification* page displays. Select the checkbox to indicate that you accept the terms. Click *Confirm*.
   Registration is now complete and your registration summary is displayed.
6. On the *Registration Complete* page, download the license file (`.lic`) to your computer.
   You will upload this license to activate the FortiPAM-VM as shown in Uploading the license file to FortiPAM-VM.

Note: After registering a license, Fortinet servers can take up to 30 minutes to fully recognize the new license. When you upload the license file to activate the FortiPAM-VM, if you get an error that the license is invalid, wait 30 minutes and try again.

When FortiPAM is initially deployed, it is in evaluation mode. Once you have downloaded the license (`.lic`) file from FortiCloud, you must load the `.lic` file to FortiPAM so that FortiPAM has a valid serial number.

Upload the license file to FortiPAM-VM:

You must be in maintenance mode to be able to upload a license. See Maintenance mode in Admin on page 11.

1. Log in to FortiPAM-VM from a browser.
   Access FortiPAM by using the IP address configured on FortiPAM port1.
   The *Upload License File* pane appears immediately after you log in.
   If FortiPAM is in evaluation mode, go to *Dashboard* > *Status*, click the *Virtual Machine* widget, and click *FortiPAM VM License*.

   Use the `https` prefix with the FortiPAM IP address to access the FortiPAM-VM GUI.
2. In the *Upload License File* pane, select *Upload* and browse to the license file on your management computer.
3. Click *OK*.
4. After the boot up, the license status changes to valid.

   Use the CLI command `get system status` to verify the license status.

License expiry and renewal

FortiPAM must have a valid license to provide all the services. Therefore, you must keep track of the license status.

By default, FortiPAM sends license expiration notification 30 days before a license expires.

The license expiry notification timing can be adjusted by using the following CLI command:

```
config alertemail setting
   set FDS-license-expiring-days 30 #adjust the number of days
end
```

To renew a license, contact the FortiPAM sales team. After purchasing FortiPAM services, you receive the service registration document that includes the service name in the title and a contract registration code.

Follow the procedure as detailed in Renewing FortiPAM-VM license on page 33 to renew FortiPAM-VM license.

License status

FortiPAM license status can be found in the *Licenses* widget available in *Dashboard* > *Status*. See Licenses widget on page 40.

Email alert for license expiration

License expiration email notification is one of the critical system notifications.

When a FortiPAM license is about to expire, i.e., the license is expiring within the next 30 days; a warning dialog appears when you log in to FortiPAM.

Also, a red banner appears on the top once you are logged in, alerting you about license expiry.

To set up email alerts for license expiry:

1. Ensure that *Email Service* is set up in *System* > *Settings*. See Settings on page 237.
2. Go to *Log & Report* > *Email Alert Settings*, and select *Enable email notification*.
3. In the *Critical System Notification* tab:
   a. In *From*, enter the email address of the sender.
   b. In *To*, enter the email address of the receiver.
4. Click *Apply*.
   Alternatively, you can add an email address where the notification is sent when creating or editing a user in *User Management* > *User Definition* (*Configure User Details* tab).

For expiring Advanced Malware Protection and FortiCare support, license expiration email notifications and warnings are sent to the administrator.

CLI configuration for setting up email alerts for license expiry - example**:**

```
config system automation-action
   edit "License Expired Notification Email"
      set action-type email
      set email-subject "FortiPAM %%log.devname%% %%log.logdesc%%"
      set email-to "admin1@fortinet.com" "admin2@fortinet.com" # receiver email address
      set message "Your license is expiring soon. Please renew at your earliest
           convenience. If your FortiPAM Subscription license is expired, only super
           admin will be allowed to access FortiPAM until a new license is applied.
           Detail:
           %%log%%"
              set description "Default automation action configuration for sending an
                   email when a license is near expiration."
   next
end
```

Subscription license

FortiPAM-VM is licensed by annual subscription. The FortiPAM-VM subscription license controls the licensed user seats. Once the license expires:

1. Only a user with *Super Administrator* role can log in to the FortiPAM GUI.
2. FortiPAM goes into maintenance mode.
   In the maintenance mode:
   a. All secrets/folders are read-only.
   b. Critical processes are suspended including manual and scheduled password changing.
3. You cannot launch secrets.

A *Super Administrator* can enable the glass breaking mode to see all the secrets.

Although not recommended, a *Super Administrator* can promote normal users to the *Super Administrator* role, allowing users to continue logging in to FortiPAM.

Users with permission, such as the *Default Administrator* role, can still access FortiPAM through `ssh` and the CLI console.

Advanced Malware Protection (formerly AntiVirus and DLP license)

The FortiPAM-VM subscription license includes Advanced Malware Protection and FortiCare support. For FortiPAM hardware models, Advanced Malware Protection and FortiCare support licenses are purchased separately as annual contracts.

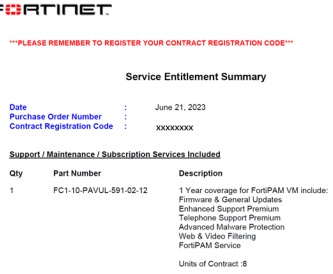
The Advanced Malware Protection (`AVDB & DLP`) licenses are related to the file scanning feature in file launchers. Once the Advanced Malware Protection license expires:

1. The antivirus scanning continues to work, however the antivirus database is not updated and no new signatures are added.
2. DLP feature stops working. The DLP feature requires a valid license.

Renewing FortiPAM-VM license

To renew FortiPAM-VM license:

1. Purchase a new license for the appropriate number of seats.
2. Copy the *Contract Registration Code* and save it for later user.



PLEASE REMEMBER TO REGISTER YOUR CONTRACT REGISTRATION CODE

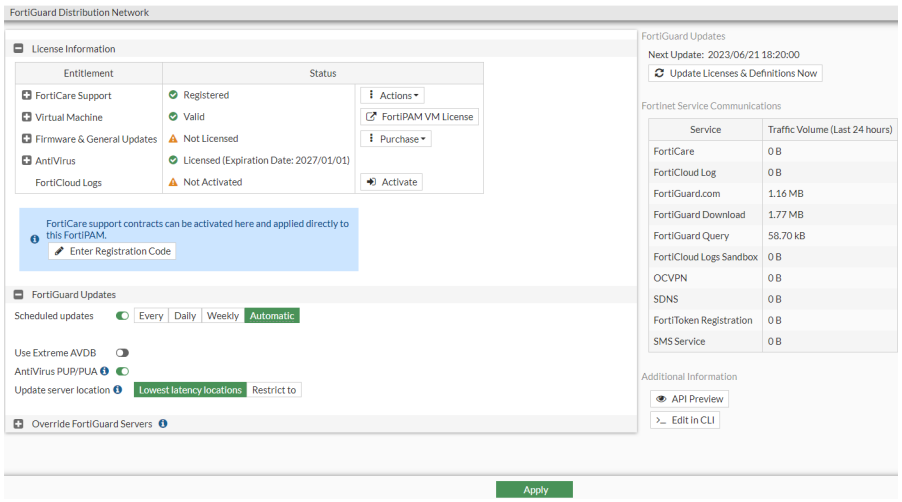
Service Entitlement Summary

Date : June 21, 2023
Purchase Order Number :
Contract Registration Code : xxxxxxxx

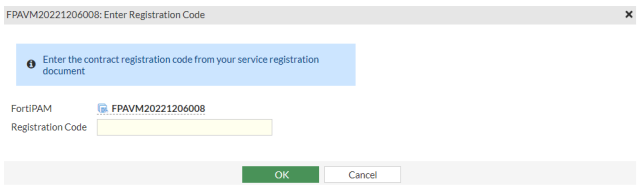
Support / Maintenance / Subscription Services Included

Qty	Part Number	Description
1	FC1-10-PAVUL-591-02-12	1 Year coverage for FortiPAM VM include: Firmware & General Updates Enhanced Support Premium Telephone Support Premium Advanced Malware Protection Web & Video Filtering FortiPAM Service Units of Contract :8

3. You can register the code to FortiCloud by either:
   a. **Registering via the FortiPAM GUI**:
      i. Log in to FortiPAM and go to *System* > *FortiGuard License*.

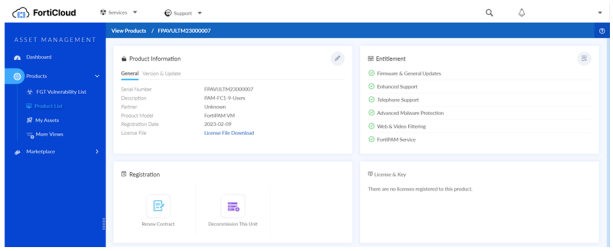


      ii. In *License Information*, click *Enter Registration Code*.
      The *Enter Registration Code* window opens.



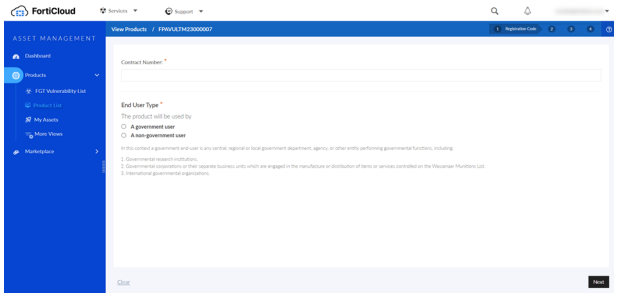
      iii. In *Registration Code*, enter the *Contract Registration Code* that you saved in step 2.
      iv. Click *OK*.
      v. Click *Apply*.
   b. **Registering directly on FortiCloud**:
      i. Go to FortiCloud and create a new account or log in with an existing account.
      The *Asset Management* portal opens.
      ii. Go to *Products* > *Product List*.

iii. Double-click your FortiPAM unit, and in *Registration*, select *Renew Contract*.



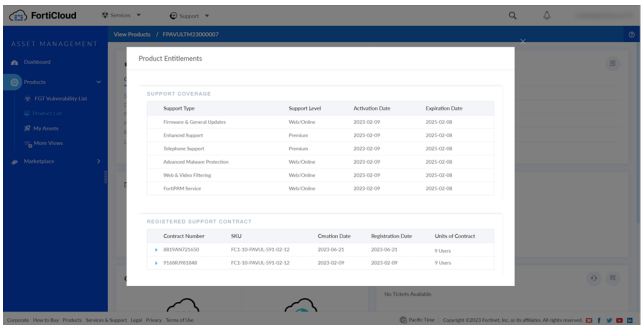
iv. Enter the *Contract Registration Code* that you earlier saved in step 2 in the *Contract Number* field.

v. In *Choose End User Type*, select your end user type as either government or a non-government user.



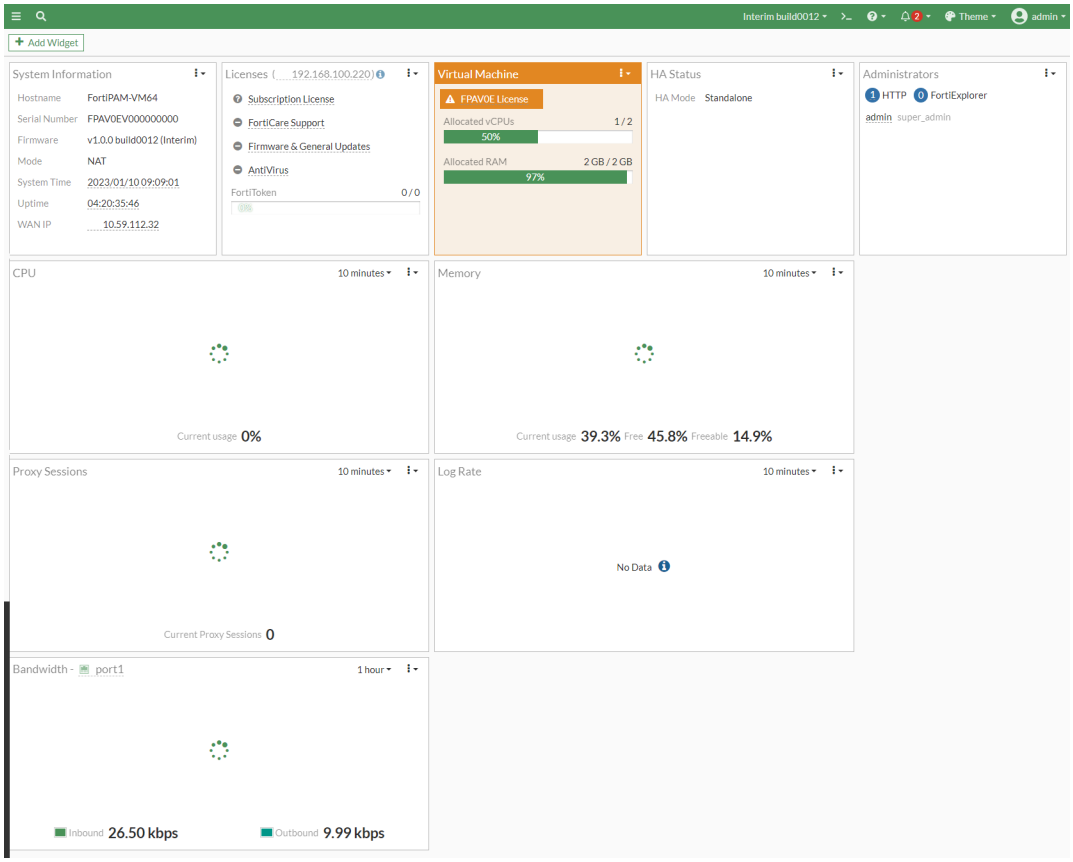
vi. Click *Next* and follow the prompts to complete renewing the license.

In *Entitlement*, click *Show Contracts* to see the contracts with their expiration dates.



Dashboard

The *Dashboard* page displays widgets that provide performance and status information, allowing you to configure some basic system settings. These widgets appear on a single dashboard.



When you select the vertical ellipses (⋮) option next to a dashboard the following actions are available:

Edit Dashboard	Select to edit the selected dashboard's name.
Delete Dashboard	Select to delete the selected dashboard. The *Status* dashboard cannot be deleted.
Add Menu Shortcut	Select to add the selected dashboard to *Menu Shortcuts*.

The following widgets are displayed in the *Status* dashboard by default:

System Information	Displays basic information about the FortiPAM system including host name, serial number, firmware version, mode, system time, uptime, and WAN IP address.

	From this widget you can manually update the FortiPAM firmware to a different release. See Uploading a firmware on page 13 and System information widget on page 39. You can also configure system settings using this widget. For information on system settings, see Settings on page 237.
Licenses	Displays the status of your license and FortiGuard subscriptions. See Licenses widget on page 40.
Virtual Machine	Displays license information, number of allocated vCPUs, and how much RAM has been allocated. See VM license on page 44.
HA status	Displays HA mode. See High availability on page 253.
CPU	The real-time CPU usage is displayed for different time frames. Select the time frame from the dropdown at the top of the widget. Hovering over any point on the graph displays the average CPU usage along with a time stamp.  To see per core CPU usage, select the CPU widget and click *Show per core CPU usage*.
Memory	Real-time memory usage is displayed for different time frames. Select the time frame from the dropdown at the top of the widget. Hovering over any point on the graph displays the percentage of memory used along with a time stamp.
Proxy Sessions	Displays how many proxy sessions are active. Select the time frame from the dropdown at the top of the widget. Hovering over any point on the graph displays the number of proxy sessions with a time stamp.
Log Rate	Displays the real-time log rate. Select the time frame from the dropdown at the top of the widget. See Log settings on page 212.
Bandwidth	Displays the real-time incoming and outgoing traffic bandwidth for the selected interface. Select the time frame from the dropdown at the top of the widget. Hovering over any point on the graph displays the bandwidth with a time stamp.

You can add the *Interface Bandwidth* widget to monitor the real-time incoming and outgoing traffic bandwidth of the selected interface over the selected time frame.

You can add the following *System* widgets to the *Dashboard*:

Administrators	Information about active administrator sessions.
HA Status	HA status of the device.
License Status	Status of various licenses, such as FortiCare Support and IPS.
System Information	General system information of the FortiPAM including hostname, serial number, and firmware version.
Top System Events	Show system events.
Virtual Machine	Virtual machine license information and resource allocations.

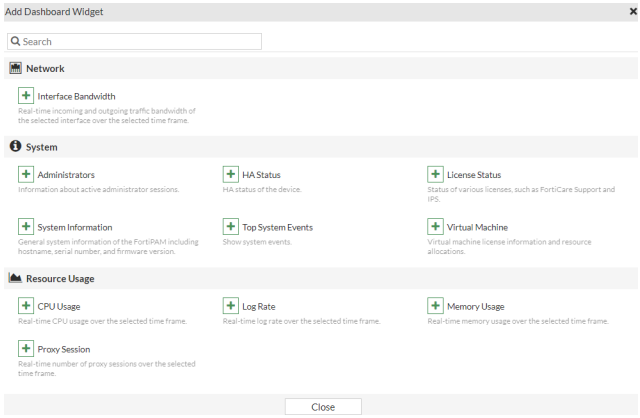
You can add the following *Resource Usage* widgets to the *Dashboard*:

CPU Usage	Real-time CPU usage over the selected time frame.
Log Rate	Real-time log rate over the selected time frame.
Memory Usage	Real-time memory usage over the selected time frame.
Proxy Session	Real-time number of proxy sessions over the selected time frame.

Adding a widget to a dashboard

To add a widget to a dashboard:

1. In a dashboard, select *Add Widget*.
   The *Add Dashboard Widget* window opens.



2. Select the widget you want to add to the dashboard.
   The *Add Dashboard Widget* - `Widget Name` window opens.
3. Enter the following information:

Fabric member	See Fabric Member.
Interface	From the dropdown, select an interface or create a new interface. **Note**: The option is only available when adding the *Interface Bandwidth* widget.
Note: Options in *Time period* and *Sort by* may vary depending on the widget you intend to add.	
Time Period	Select from the following time periods to display: • *5 minutes* • *1 hour* • *24 hours*
Visualization	Select the type of chart to display. **Note**: For the *Top System Events* widget only the *Table View* is available.
Sort by	Sort by: • *Level* • *Events*

4. Click *Add Widget*.

Widget actions

All or some of the following actions are available for a widget when you click the vertical ellipsis (⋮) option for a widget:

Resize	Select and then select the number of squares you want to extend the widget to.
Settings	Select and then in *Edit Dashboard Widget* - `Widget Name`, specify the *Fabric Member*, interface (if available), and click *OK*. Select from the following options: • *Default*: Uses the current fabric member. • *Specify*: Select a fabric member from the FortiPAM dropdown, i.e., a FortiPAM instance. Choosing a specific fabric member for this widget will override the behavior for the entire dashboard. After this is done, the fabric member selection is on each individual widget. • *Interface*: From the dropdown, select an interface or create a new interface.
Remove	Select *x* to remove the widget.

Select the pin (📌) icon on a widget to expand and pin hidden content.

Adding a custom dashboard

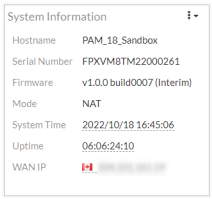
To add a custom dashboard:

1. In the menu, go to *Dashboard* and select +.
   The *Add Dashboard* dialog opens.

2. In *Add Dashboard*, enter a name for the new dashboard.
3. Click *OK*.
   A new dashboard with no widget is set up.
4. Use *Add Widget* to add new widgets to the dashboard.

System information widget

The system dashboard includes a *System Information* widget, which displays the current status of FortiPAM and enables you to configure basic system settings.



The following information is available on this widget:

Host Name	The identifying name assigned to this FortiPAM unit. For more information, see Changing the host name on page 39.
Serial Number	The serial number of FortiPAM. The serial number is unique to FortiPAM and does not change with firmware upgrades. The serial number is used for identification when connecting to the FortiGuard server.
Firmware	The version and build number of the firmware installed on FortiPAM. To update the firmware, you must download the latest version from FortiCloud. See Uploading a firmware on page 13.
Mode	The current operating mode of the FortiPAM unit. A unit can operate in NAT mode or transparent mode.
System Time	The current date and time according to the FortiPAM unit's internal clock. For more information, see Configuring the system date, time, and time zone on page 40.
Uptime	The duration of time FortiPAM has been running since it was last started or restarted.
WAN IP	The WAN IP address and location. Additionally, if the WAN IP is blocked in the FortiGuard server, there is a notification in the notification area, located in the upper right-hand corner of the *Dashboard*. Clicking on the notification opens a window with the relevant blocklist information.

Changing the host name

The *System Information* widget displays the full host name.

To change the host name:

1. Go to *Dashboard* > *Status*.
2. Select the *System Information* widget and then click *Configure settings in System* > *Settings*.
   The *System Settings* window opens.
3. In *System Settings*, update the host name in *Host name*.
4. Click *Apply*.

Configuring the system date, time, and time zone

You can either manually set the FortiPAM system date and time, or configure the FortiPAM unit to automatically keep its system time correct by synchronizing with an NTP server.

To configure the date and time manually:

1. Go to *Dashboard* > *Status*.
2. Select the *System Information* widget and then click *Configure settings in System* > *Settings*.
3. From the *Time Zone* dropdown, select a timezone.
   If you want to change the date and time manually, select *Manual Settings* for *Set Time*:
   a. In *Date*, either enter the date or select the *Calendar* icon and then select a date.
   b. In *Time*, either enter the time or select the *Clock* icon and then select a time.
4. Click *Apply* to save changes.

To automatically synchronize FortiPAM unit's clock with the NTP server:

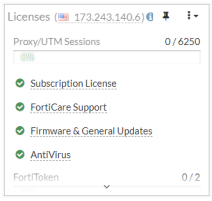
1. Go to *Dashboard* > *Status*.
2. Select the *System Information* widget and then click *Configure settings in System* > *Settings*.
3. From the *Time Zone* dropdown, select a timezone.
4. In *Set Time*, select *NTP*.
5. In *Select Server*, either select *Fortiguard* or *Custom*.
   If you select *Custom*, enter the *Custom Server IP Address*.

Custom server details must be configured in the CLI.

6. In *Sync interval*, enter how often, in minutes, that the device synchronizes time with the NTP server.
7. Click *Apply* to save changes.

Licenses widget

The *Licenses* widget displays the statuses of your licenses and FortiGuard subscriptions. It also allows you to update your device's registration status and FortiGuard definitions.



Hovering over the *Licenses* widget displays status information for *Subscription License*, *FortiCare Support*, *Firmware & General Updates*, *AntiVirus*, and *FortiToken*.

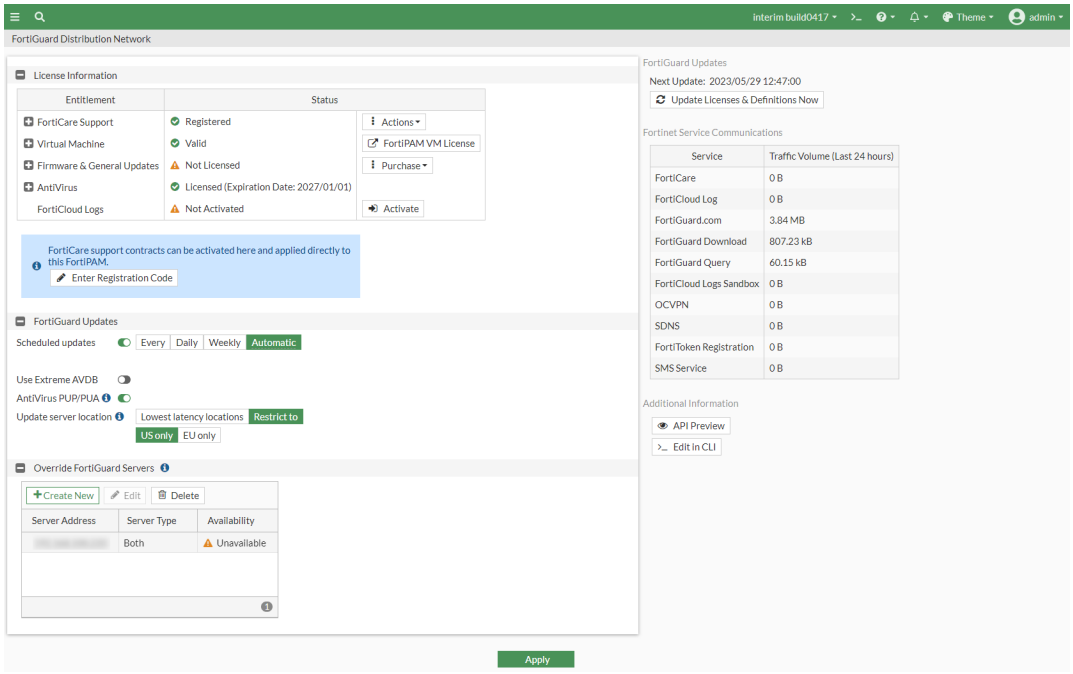
To view details on licenses, see FortiGuard Distribution Network on page 41.

FortiGuard Distribution Network

The FortiGuard Distribution Network page provides information and configuration settings for FortiGuard subscription services. For more information about FortiGuard services, see FortiGuard Labs.

To view and configure FortiGuard connections:

1. Go to *Dashboard* > *Status*.
2. In the *License* widget, click any option except *FortiToken*, and select *View details in System* > *FortiGuard*. The *FortiGuard Distribution Network* window opens.



The following settings are available in the window:

License Information	
FortiCare Support	The availability or status of your unit's support contract. You can update your registration status by selecting *Enter Registration Code* and loading the license file from a location on your computer.

	 From the *Actions* dropdown: • Select *Login to My Account* to log in to FortiCloud. • Select *Transfer FortiPAM to Another Account* to transfer this FortiPAM device to another FortiCloud account. Fill in the verification details and then review and transfer the device.
Virtual Machine	To upload or check your virtual machine license, select *FortiPAM VM License*. See Uploading a license file.
Firmware & General Updates	Displays the status of *Application Control Signatures*, *Device & OS Identification*, and *Internet Service Database Definitions*. **To upgrade the database:** 1. From the *Actions* dropdown, select *Upgrade Database*. 2. Select *Upload* and locate the application control signatures file from your computer. 3. Select *OK*.  From the *Actions* dropdown, select *View List* to see a list of application control signatures.  To purchase upgrades, select *Enter Registration Code* from the *Purchase* dropdown, enter the *Registration Code* in the new window, and click *OK*.
Antivirus	The FortiGuard AntiVirus Service provides fully automated updates to ensure protection against the latest content level threats. It employs advanced virus, spyware, and heuristic detection engines to prevent both new and evolving threats from gaining access to your network and protects against vulnerabilities.  To renew the AntiVirus service, select *Enter Registration Code* from the *Renew* dropdown, enter the *Registration Code* in the new window, and click *OK*.
FortiCloud Logs	To activate FortiCloud logs: 1. Select *Activate*. 2. Confirm the password of your FortiCloud account. 3. Select from the following domains: • *Europe* • *US* • *Global* 4. Ensure that *Send logs to FortiCloud Logs* is enabled.

	5. Click *OK*.
FortiGuard Updates	
Scheduled updates	Enable to receive scheduled updates and then select when the updates occur: Every *1-23* hours, *Daily* at a specific hour, or *Weekly* on a specific day at a specific hour, or automatically within every one hour period. **Note**: The option is enabled by default.
Use Extreme AVDB	 **Note**: The option is disabled by default.
AntiVirus PUP/PUA	Enable antivirus grayware checks for potentially unwanted applications. **Note**: The option is enabled by default.

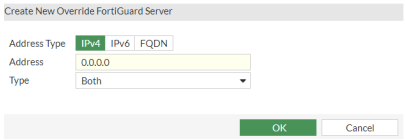
Update server location	Update the FortiGuard server location to:
	• *Lowest latency locations*
	or
	• Restrict to:
	  • *US only*
	  • *EU only*
	Changing the server location overrides all FortiGuard/FortiCloud/FortiCare servers.

Override FortiGuard Servers By default, the FortiPAM unit updates signature packages and queries rating servers using public FortiGuard servers. You can override this list of servers. You can also disable communication with public FortiGuard servers. See Override FortiGuard Servers on page 43.	

Override FortiGuard Servers

To override FortiGuard servers

1. In step 2 when configuring FortiGuard connections, select *Create New* in the *Override FortiGuard Servers* pane. The *Create New Override FortiGuard Server* window opens.



2. Enter the following information:

Address Type	Select from the following three options: • *IPv4* • *IPv6* • *FQDN*
Address	Depending on your selection in *Address Type*, enter an IPv4/IPv6 address, or an FQDN.
Type	Select the type of update to receive: • *Antivirus & IPS updates* • *Filtering* • *Both*

3. Click *OK*.

Select a server in the list and select *Edit* to edit the server.

Select servers in the list and select *Delete* to delete the servers.

To remove multiple servers quickly, select multiple rows in the list by holding down the `Ctrl` or `Shift` keys and then select *Delete*.

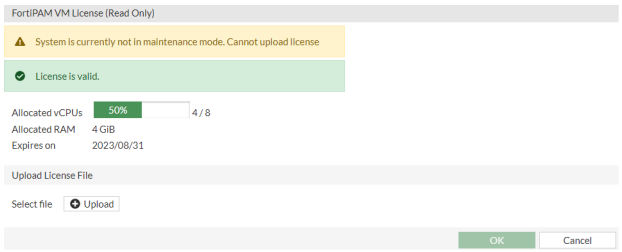
To update the licenses and definition immediately, select *Update Licenses & Definitions Now*.

VM license

Click on the *Virtual Machine* widget and then select *FortiPAM VM License*.

The *FortiPAM VM License* page displays whether the license is valid or not, the allocated vCPUs, RAM, and the license expiry date.

You must be in maintenance mode to be able to upload a license. See Maintenance mode in Admin on page 11.



To upload a license, see Uploading a license.

Secrets

User name and password/key of servers can be securely stored in FortiPAM as secrets. The secrets contain information on login, credentials, and the target server IP address. The end user can use the secret to access servers.

In FortiPAM, actual credentials are protected, and FortiPAM users cannot access the credentials except in some cases as described below. Login credentials can be changed automatically and manually for different use cases.

User names and password of domain controller can be securely stored in FortiPAM secrets.

Website user names and passwords can be securely stored in FortiPAM.

FortiPAM works with FortiClient and the browser extension to automatically fill the user name and password when the user browses a website.

Users with the following permission can view secret passwords on the GUI:

- Owner of the secret
- Editor of the secret

Viewer of the secret cannot see the secret password on the GUI.

Components:

- Servers: the server that the end users require to access.
- FortiClient: supports privileged activity recording and ZTNA tunnel setting up in proxy mode.
- FortiPAM: back to back user agent to access the target website in proxy mode.

FortiPAM supports client and browser to launch a session to servers.

FortiPAM supports the following servers and credentials:

SSH server: Password mode and Key mode
RDP server
macOS VNC server
Linux VNC server
Integrated with Windows AD by Samba or LDAPs
Web account credentials

Besides client mode launch for secrets, FortiPAM also supports browser mode where no client software is required.

The following client and browser modes are supported by FortiPAM:

- Client mode: PuTTY, Windows Remote Desktop, RealVNC, TightVNC, and WinSCP etc
- Browser mode: Web SSH, Web RDP, Web VNC, Web SMB, Web SFTP and Web Account.

In *Secrets*, you can access the following tabs:

- Secret list on page 47
- Personal/public folder on page 73
- My requests list on page 82
- Approval list on page 85
- Job list on page 88

Secret list

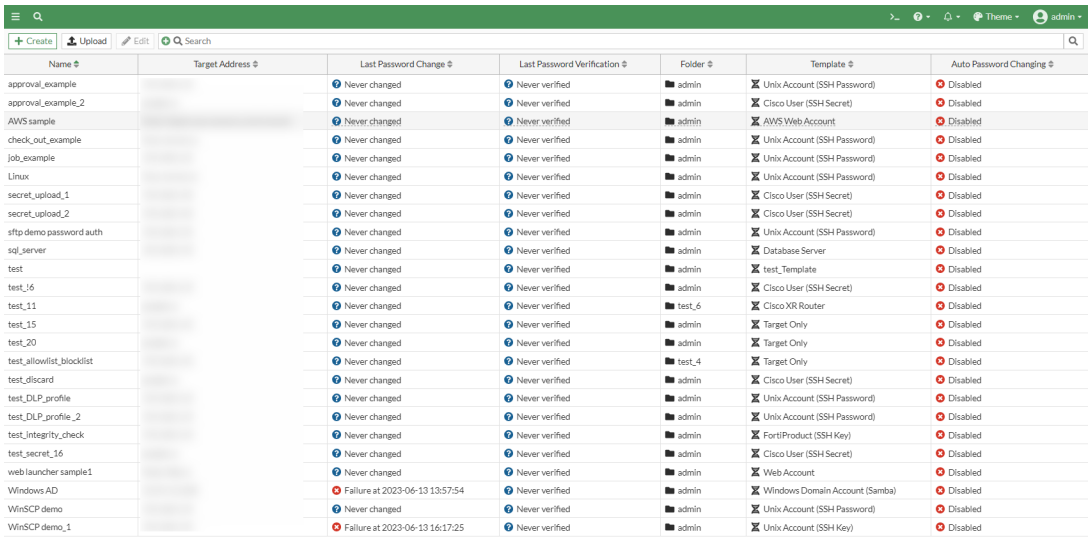
Secret List in *Secrets* displays a list of configured secrets.

To access any of the secrets, you require *Secret List* access.

No matter what permissions the secrets are provided, the secrets are not available anymore if the access control for *Secret List* in the *Role* page is set to *None*. See Role on page 174.

For each secret the following columns are displayed:

- *Name*
- *Target Address*
- *Last Password Change*
- *Last Password Verification*
- *Folder*
- *Template*
- *Auto Password Changing*



The *Last Password Verification* column gives an overview of the secret password status.

Use the sorting arrows next to the column names to sort columns in an ascending or descending order, e.g.:

Name

Clicking the upper arrow in the *Name* column arranges the secret entries in an ascending order.

The *Secrets List* tab contains the following options:

Create	Select to create a new secret. See Creating a secret on page 49.
Upload	Select and then select *Upload Secret* to upload secrets using the secret upload template file, or download the secret upload template by selecting *Download Template*. See Uploading secrets using the secret upload template on page 63.
Edit	Select to edit the selected secret. When a secret request is approved, the *Launcher Status* timer shows the remaining time till you (as a requester) have access to the secret when you double-click to open the secret in *Secrets* > *Secret List*. When editing a secret, click *Discard Changes* to discard all the changes you made.

Move	Select to move the selected secret.
Delete	Select to delete the selected secrets.
Clone	Select to clone the selected secret.
Add favorite	Select to add the selected secret to the favorite folder.
Remove favorite	Select to remove the selected secret from the favorite folder.
Launch Secret	Launch the selected secret. See Launching a secret on page 62.
Make Request	Make request to launch or perform a job on the secret. Make a request on page 83.
Search	Enter a search term in the search field, then hit `Enter` to search the secrets list. To narrow down your search, see Column filter. The following column filters are available: • *Name* • *Target Address* • *Last Password Change* • *Last Password Verification* • *Folder* • *Template* • *Auto Password Changing* • *ID*

Not all options are available for a secret. The options depend on how the secret has been set up, e.g., The *Make Request* option is only available when the secret has *Requires Approval to Launch Secret* enabled.

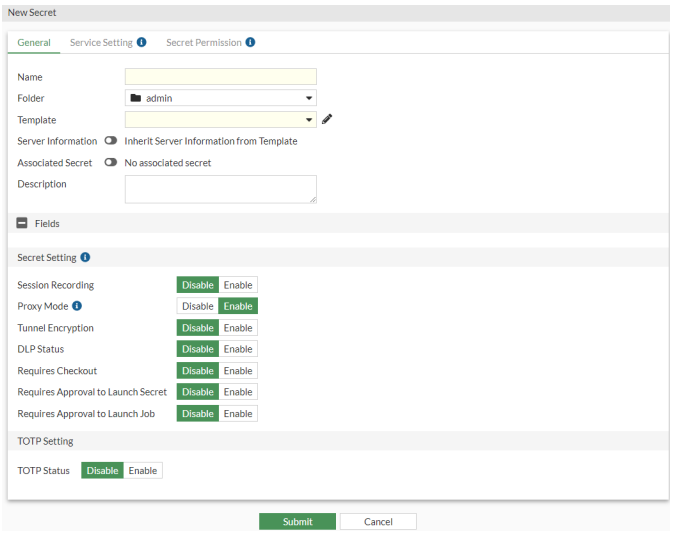
Creating a secret

To create a secret:

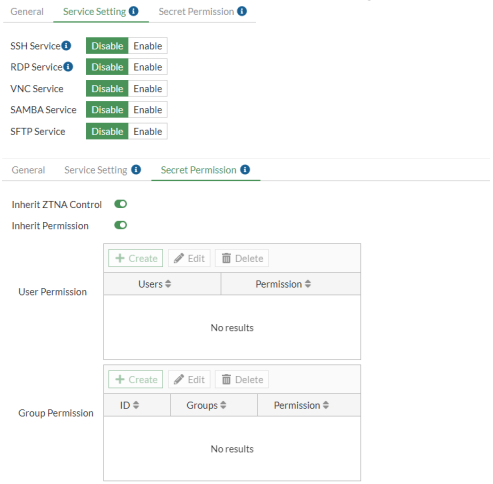
1. Go to *Secrets* > *Secret List*.
   Alternatively, go to *Personal Folder/Public Folder* in *Secrets*, select *Open Tree*, locate the folder where you intend to add the secret, and click *Open Folder*.
   From the *Create* dropdown, select *Secret*, and skip to step 6.
2. In *Secret List*, select *Create*.
   The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.

The folder is already selected if you are creating secret from inside a folder.

4. Select *Create Secret*.
   The *General* tab opens.



5. To switch to either *Service Setting* or *Secret Permission* tab, select the tab.

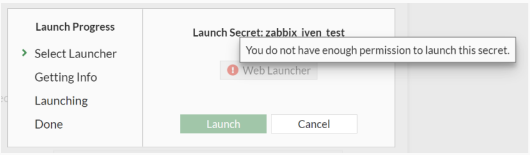


6. Enter the following information:

Name	Name of the secret.
Folder	The folder where the secret is added. See Personal/public folder on page 73. The folder is already selected in step 2. Use the dropdown, if you want to change the folder.
Template	From the dropdown, select a template. Select *Create* to create a new template. See Creating secret templates on page 95.

	 **To change the template after selecting one:** 1. Select the pen icon. 2. In the *Convert Secret Template* pane, select a template to transfer old field values to new fields where applicable. 3. Click *OK*.
Associated Secret	Enable and then from the dropdown, select an associated secret for the new secret being created. When enabled, changing password or verifying password requires credentials from the associated secret. **Note**: The option is disabled by default.
Description	Optionally, enter a description.
Fields	Enter a value in a field.  The options in the fields depend on the selected template.  For fields where a host is required when using the FortiPAM browser extension, enter the URL instead.
Secret Setting	
	Some settings may not be configurable as they are protected by the policy that applies to the folder where the secret is added.
	The owner of the secret must configure password verification and change settings before the secret utilizes the password changer and password verification. However, a user can manually trigger these actions if they have sufficient permissions.
Automatic Password Changing	Enable/disable automatic password changing. When enabled, password changer for secrets is activated to periodically change the password.
Recursive	Displays the password changing schedule based on your selections for the related settings.
Start Time	The date and time when the recurring schedule begins. Enter date (MM/DD/YYYY) and time or select the *Calendar* icon and then select a date and time.
Recurrence	From the dropdown, select from the following three frequencies of recurrence: • *Daily*

	• *Weekly* • *Monthly*
Repeat every	The number of days/weeks/months after which the password is changed (1-400).
Occurs on	Select from the following days of the month when the password is automatically changed: • *First* • *Second* • *Third* • *Last* • *Last Day* • *Day* When you select *Day*, select + to add days of the month when the password is automatically changed. Select days of the week when the password is automatically changed. **Note**: The option is only available when *Recurrence* is set as *Weekly* or *Monthly*.
Automatic Password Verification	Enable/disable automatic password verification. When enabled, password changer for secrets is activated to periodically verify the password, and check if the target server is still available.
Interval (min)	The time interval at which the secret passwords are tested for accuracy, in minutes (default = 60, 5 - 44640).
Start Time	The date and time when the *Interval(min)* begins. Enter date (MM/DD/YYYY) and time or select the *Calendar* icon and then select a date and time.
Session Recording	Enable/disable session recording. When enabled, user action performed on the secret is recorded.  The video file is available in the log for users with appropriate permission.
Proxy Mode	Enable/disable the proxy mode. When enabled, FortiPAM is responsible to proxy the connection from the user to the secret. In the proxy mode: • Web launcher is available to users who have the permission to view the secret password. • Web launcher is disabled for users who do not have the permission to view the secret password. When disabled, the non-proxy (direct) mode is used. See Modes of operation on page 17. In the non-proxy mode:

	• Web launcher is available to users who have the permission to view the secret password. • Web launcher is disabled for users who do not have the permission to view the secret password. When launchers are disabled, the *Launch* option is unavailable and a tooltip is displayed instead: 
Tunnel Encryption	Enable/disable tunnel encryption. When launching a native launcher, FortiClient creates a tunnel between the endpoint and FortiPAM. The protocol stack is HTTP/TLS/TCP. The HTTP request gives information on the target server then FortiPAM connects to the target server. After that, two protocol options exist for the tunnel between FortiClient and FortiPAM. One is to clear the TLS layer for better throughput and performance. The other is to keep the TLS layer. The launcher's protocol traffic is inside the TLS secure tunnel. If the launcher's protocol is not secure, like VNC, it is strongly recommended to enable this option so that the traffic is in a secure tunnel. When there is an HTTPS Man In The Middle device, e.g., FortiGate or FortiWeb between FortiClient and FortiPAM, you must enable the *Tunnel Encryption* option. Otherwise, the connection will be disconnected, and the launching will fail.
DLP Status	Enable/disable DLP. See Data loss prevention (DLP) protection for secrets on page 139.
DLP Profile	From the dropdown, select a DLP profile.
Antivirus Scan	Enable/disable antivirus scan. When enabled, it enforces an antivirus profile on the secret. See AntiVirus on page 136.
Antivirus Profile	From the dropdown, select an antivirus profile.
Requires Checkout	Enable/disable requiring checkout. When enabled, a user has exclusive access to a secret for a limited time. At a given time, only one user can check out a secret. Other approved users must wait for the secret to be checked in or wait for the checkout duration to lapse before accessing the secret. See Check out and check in a secret on page 63.

Checkout Duration	The checkout duration, in minutes (default = 30, 3 - 120).
Checkin Password Change	Enable/disable automatically changing the password when the user checks in.
Renew Checkout	Enable/disable renewing checkouts.
Max Renew Count	When *Renew Checkout* is enabled, enter the maximum number of renewals allowed for the user with exclusive access to the secret (default = 1, 1 - 5).
Requires Approval to Launch Secret	Enable/disable requiring approval to launch a secret. When enabled, users must request permission from the approvers defined in the approval profile before gaining access. From the dropdown, select an approval profile.  Use the search bar to look up an approval profile.  Use the pen icon next to the approval profile to edit it. See Make a request on page 83 and Approval flow on page 120.
Requires Approval to Launch Job	When enabled, users must request permission from the approvers defined in the approval profile before executing a job on a secret. From the dropdown, select an approval profile.  Use the search bar to look up an approval profile.  Use the pen icon next to the approval profile to edit it. See Make a request on page 83 and Approval flow on page 120.
Bypass Approval	Enable/disable secret owners to bypass the secret request/approval process, i.e., secret owners do not require approval to launch secrets they own, given that *Bypass Approval* is enabled. **Note**: The option is disabled by default and only available when *Requires Approval to Launch Job* is enabled.

TOTP Setting

Enable/disable TOTP (Time-based one-time password) for the secret.

TOTP is used when the target server requires TOTP as the 2FA.

To configure TOTP settings via the CLI, see Configuring TOTP settings via the secret CLI commands Example on page 61.

See Limitations of TOTP on FortiPAM on page 103.

Note: The option is disabled by default.

Verification Code with	The verification code issued by: • *3rd Party* (default) • *FortiToken* **Note**: The option is only available when TOTP status is enabled.
Shared Key	The TOTP key from the target server or any other 3rd party authenticator. The TOTP key is usually a binary string and delivered in `base64`/`base32` encoding format.  Use the eye icon to hide/unhide the shared key. **Note**: The option is only available when the *Verification Code with* is set as *3rd Party*.
Activation Code	The FortiToken Mobile activation code. When using FortiToken Mobile as the TOTP mobile application, an activation code from the FortiToken Mobile token issuer is required to activate the token. In that case, you must provide the activation token, and FortiPAM then acts as a surrogate for the FortiToken Mobile application.  FortiToken TOTP can only be configured via the GUI. **Note**: The option is only available when *Verification Code with* is set as *FortiToken*.

Service Setting

Turn on/off the service settings.

You can individually toggle on or off each service, controlling whether or not FortiPAM is allowed to use the specific service to connect to the secret.

The port used by each service specified in the template can also be overridden to use a custom port specific to the secret.

SSH Service	Enable/disable SSH service. The *SSH Service* toggle controls *Web SSH*, *Web SFTP*, *PuTTY*, and the *WinSCP* launchers. **Note**: *SSH Filter*, *RSA Sign Algorithm*, and *Connect over SSH with*, and *SSH Auto-Password* options are only available when *Template* is already selected.
Use Template Default Port	Use the template default port or disable and enter a port number.
SSH Filter	Enable/disable using an SSH filter profile. See SSH filter profiles on page 148.
SSH Filter Profile	From the dropdown, select an SSH filter profile. **Note**: The option is only available when *SSH Filter* is enabled.

	 Use the search bar to look up an SSH filter profile.
RSA Sign Algorithm	To improve compatibility with different SSH servers, select a sign in algorithm for RSA-based public key authentication: • *RSA SHA-256 signing algorithm* • *RSA SHA-512 signing algorithm* • *RSA SHA-1 signing algorithm* (default)
Connect over SSH with	If the setting is set to *Self* (default), the secret launches SSH with its own username and password. If the setting is set to *Associated Secret*, the secret launches SSH with the associated secret's username and password.
SSH Auto-Password	Enable or disable automatically delivering passwords to the server when the user enters privileged commands (e.g., `sudo` in Unix system and `enable` in Cisco devices) in the SSH shell terminal. For secrets using Cisco server info template, an associated secret must be set to enable this feature. **Note**: The option only works when *Proxy Mode* is enabled.
RDP Service	Enable/disable RDP service. The *RDP Service* toggle controls *Web RDP* and the *Remote Desktop-Windows* launchers. **Note**: *Block RDP Clipboard*, *RDP Security Level*, *RDP Restricted Admin Mode*, and *Keyboard Layout* options are available only when *Template* is already selected.
Use Template Default Port	Use the template default port or disable and enter a port number.
Block RDP Clipboard	Enable/disable allowing users to copy/paste from the secret launcher.
RDP Security Level	Select a security level when establishing a RDP connection to the secret: • *Best Effort* (default): If the server supports NLA, FortiPAM uses NLA to authenticate. Otherwise, FortiPAM conducts standard RDP authentication with the server through RDP over TLS. • *NLA*: Network Level Authentication (CredSSP). When an RDP launcher is launched, FortiPAM is forced to use CredSSP (NLA) to authenticate with the target server. • *RDP*: FortiPAM uses the standard RDP encryption provided by the RDP protocol without using TLS (Web-RDP only). • *TLS*: RDP over TLS. FortiPAM uses secured connection with encryption protocol TLS to connect with the target server.
RDP Restricted Admin Mode	Enable/disable RDP restricted admin mode.

	Restricted admin mode prevents the transmission of reusable credentials to the remote system to which you connect using remote desktop. This prevents your credentials from being harvested during the initial connection process if the remote server has been compromised. **Note**: The option is only available when *RDP Security Level* is set as *Best Effort* or *NLA*.
Keyboard Layout	From the dropdown, select a keyboard layout (default = *English, United States*)
VNC Service	Enable/disable VNC service. The *VNC Service* toggle controls the *Web VNC*, *VNC Viewer*, and *TightVNC* launchers.
Use Template Default Port	Use the template default port or disable and enter a port number. **Note**: The port number you enter is used to connect to the VNC launcher.
Display Number	Enter the display number to be added to the VNC port defined in the template (default = 0). **Notes**: • The display number can only be set if the custom port on the template is the VNC default port, i.e., port `5900`, and the secret uses the default template for VNC. Otherwise, the display number option is the custom port option. • The display number cannot be set with a custom port. • The option is only available when *Use Template Default Port* is enabled.
SAMBA Service	Enable/disable SAMBA service. The *SAMBA Service* toggle controls the *Web SMB* launcher.
Use Template Default Port	Use the template default port or disable and enter a port number.
SFTP Service	Enable/disable SFTP service. The *SFTP Service* toggle controls the *Web SFTP* launcher.
Use Template Default Port	Use the template default port or disable and enter a port number.
Secret Permission	
	By default, secret permission is the same as the folder where they are located.
	When customizing secret permission, ensure that you log in with an account with *Owner* or *Edit* permission to the secret or the folder where the secret is located.
Inherit ZTNA Control	Enable to inherit ZTNA control access permission from the parent folder.

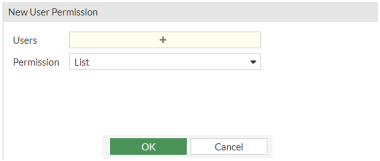
	By default, secrets in a folder follow the ZTNA control set up in the parent folder. However, when creating or editing a secret you can customize the ZTNA control in the *Secret Permission* tab.
ZTNA Control	Enable to limit the permission of launching by `ztna-ems-tag`. You can choose whether to match all the tags or only one of them. The option is only available when *Inherit ZTNA Control* is disabled.
Device Tags	Select + to add ZTNA tags or groups. Use the search bar to look up a ZTNA tag or ZTNA tag group. Only permitted devices with the selected tags are allowed to launch.
Device Match Logic	Define the match logic for the device tags: • *OR*: Devices with any of the selected tags are allowed to launch. • *AND*: Devices must acquire all the selected tags to launch.
Inherit Permission	Enable to inherit permissions that apply to the folder where the secret is located. The option is enabled by default.
User Permission	The level of user access to the secret. See User Permission on page 59. This option is only available when *Inherit Permission* is disabled. For column settings, see Tables on page 15.
Group Permission	The level of user group access to the secrets. See Group Permission on page 60. This option is only available when *Inherit Permission* is disabled. For column settings, see Tables on page 15.

Target Filter	Enable/disable filtering addresses. When enabled, *Allow*/*Deny* addresses, i.e., create a list of allowed or blocked addresses. Creating allowlist/blocklist helps you improve security by allowing/blocking IP addresses. The filter does not apply to the Domain-Controlled address. Select +, from the *Select Entries* list, select addresses, and click *Close*. Use the search bar to look up an address. Click the delete icon to delete all the addresses and reset the list. **Note**: The option is disabled by default and only available when editing a secret that has one of its fields set as *Domain*.

7. Click *Submit*.
   See Launching a secret on page 62 and Example secret configurations example on page 69.

User Permission

1. In step 5 when Creating a secret, select *Create* in *User Permission*.
   The *New User Permission* window opens.



2. Enter the following information:

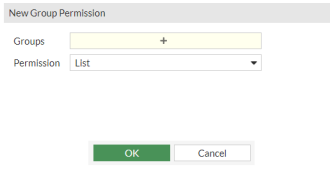
Users	Select + and from the list, select users in the *Select Entries* window. **To add a new user:** 1. From the *Select Entries* window, select *Create* and then select *+User Definition*. The *New User Definition* wizard opens. 2. Follow the steps in Creating a user on page 159, starting step 2 to create a new user.  Use the search bar to look up a user.  Use the pen icon next to a user to edit it.
Permission	From the dropdown, select an option: • *None*: No access. • *List*: Ability to list secrets. You cannot see detailed information on secrets. • *View*: Ability to view secret details and launch a secret. • *Edit*: Ability to create/edit secrets and launch the secrets. • *Owner*: The highest possible permission level with the ability to create, edit, delete, and launch secrets.

3. Click *OK*.

From the list, select a user permission entry and then select *Edit* to edit it.
From the list, select user permission entries and then select *Delete* to delete them.

Group Permission

1. In step 5 when Creating a secret, select *Create* in *Group Permission*.
The *New Group Permission* window opens.



2. Enter the following information:

Groups	Select + and from the list, select user groups in the *Select Entries* window. **To add a new user group:** 1. From the *Select Entries* window, select *Create*. The *Create New User Group* window opens. 2. Follow the steps in Creating user groups, starting step 3.  Use the search bar to look up a user group.  Use the pen icon next to a user group to edit it.
Permission	From the dropdown, select an option: • *None*: No access. • *List*: Ability to list secrets. You cannot see detailed information on secrets. • *View*: Ability to view secret details and launch a secret. • *Edit*: Ability to create/edit secrets and launch the secrets. • *Owner*: The highest possible permission level with the ability to create, edit, delete, and launch secrets.

3. Click *OK*.

From the list, select a user group permission entry and then select *Edit* to edit it.
From the list, select user group permission entries and then select *Delete* to delete them.

Configuring TOTP settings via the secret CLI commands - Example

To configure TOTP settings via the CLI:

1. In the CLI console, enter the following commands to use the secret template TOTP settings for the secret:

```
config secret database
   edit 1
      config totp-setting
         set status enable
         set use-template-setting enable
         set shared-key xxxxxxxxxxxx
      end
   end
```

To configure TOTP settings via the CLI:

1. In the CLI console, enter the following commands to disable the secret template TOTP settings and instead configure a custom TOTP setting for the secret:

```
config secret database
   edit 1
      config totp-setting
         set status enable
         set use-template-setting disable
         set totp-length 6
         set totp-duration 30
         set hash-type hmac-sha1
         set shared-key xxxxxxxxxxxx
      end
   end
```

Launching a secret

To launch a secret:

1. Go to *Secrets* > *Secret List*.
2. In the *Secrets List*, double-click a secret to open.
   Alternatively, in *Secrets* > *Personal Folder/Public Folder*, go to the folder where the secret is located, and double-click the secret to open.

If the secret does not show up, it may be because you do not have the necessary permission to access the secret or the folder where the secret is located.

3. Click *Launch Secret*.
   The *Launch Progress* window opens.
4. From the list, select a launcher, and select *Launch*.

Chrome, Edge and Firefox have extensions to support video recording for browser based launchers.

AWS does not work with *Web SSH*.

When using file launchers, the following two security features can be enabled in a secret:

Note: Examples of a file launcher include WinSCP, Web SMB, and Web SFTP.

   a. By assigning an antivirus profile to a secret, the user can be protected from downloading viruses and the server can be protected from virus being uploaded. See the *Antivirus Scan* option in Creating a policy on page 113 and Creating a secret on page 49. Also, see AntiVirus on page 136.
   b. By assigning a DLP sensor to a secret, the server can be protected from sensitive information being uploaded and downloaded from the server. See Data loss prevention (DLP) protection for secrets on page 139.

5. After the session is finished, close the launcher.

See Check out and check in a secret on page 63.

Blocklist and allowlist for RDP target IP address restriction

When launching a secret with the *Windows Domain Account* template, you can input any IP address as the target secret.

Blocklist and allowlist can help you to improve security by allowing preconfigured IP addresses.

See the *Target Filter* option in the *Permission* pane in Creating a secret on page 49.

Check out and check in a secret

Checking out a secret gives you exclusive access to the secret for a limited time.

Checking in a secret allows other approved users to access the secret.

To check out a secret:

1. Go to *Secrets* > *Secret List*.
2. In *Secrets List*, double-click a secret to open.
   Alternatively, in *Folders*, go to the folder where the secret is located, and double-click the secret to open.

If the secret does not show up, it may be because you do not have the necessary permission to access the secret or the folder where the secret is located.

3. On the top-right, click *Check-out Secret* to check out the secret.

If the *Check-out Secret* button does not show up, it may be because another user has checked out the secret. At a given time, only one user can check out a secret. Other approved users must wait for the secret to be checked in or wait for the checkout duration to lapse before accessing the secret.

See *Requires Checkout* option when Creating a secret on page 49.

To check in a secret:

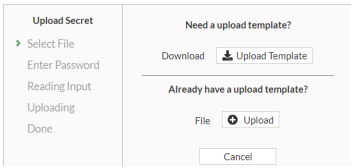
1. Go to *Secrets* > *Secret List*.
2. In *Secrets List*, double-click a secret to open.
   Alternatively, in *Folders*, go to the folder where the secret is located, and double-click the secret to open.
3. On the top-right, click *Check-in Secret* to check in the secret.
   Other approved users can now access the secret.

Uploading secrets using the secret upload template

On the *Secret List* page, the uploading secrets feature provides a convenient and faster way to import multiple secrets to FortiPAM at once. You first download the secret upload file template from FortiPAM, input secret-related information such as *Secret Template*, *Target Address*, *Account Name*, and *Account Password* into the file, and then import the file to FortiPAM. All the secrets in the file are added to FortiPAM automatically.

To upload secrets using the secret upload template:

1. Go to *Secrets* > *Secret List* and select *Upload*.
   The *Upload Secret* dialog opens.



2. Select *Upload Template* to download the secret upload template.
   The *Download Template* dialog opens.

3. In *Password*, enter a password to encrypt the secret upload template excel file.
   The secret upload template is downloaded on your computer. The file is named `fpam_secret`.
4. Open the secret upload template (`fpam_secret.xlsm`), enter the password that was used to encrypt the file in step 3, and click *OK*.
   You can now access the secret upload template.
   The secret upload template currently includes the following features:
   - Checks template completion when you quit; a warning appears if the template is incomplete.
   - Highlights fields that need to be filled in.
   - Checks the target address syntax. Currently supports IPv4 addresses and FQDN only.
5. Upon opening the `fpam_secret` file for the first time, enable editing and content for Macros.
6. From the *Secret Template* column, select a supported template.

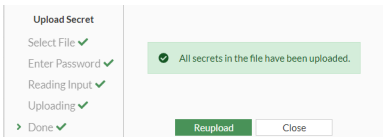
All the default secret templates are supported.

You can create custom secret templates in the secret upload template file by selecting *Customized* from the *Secret Template* column.

7. Fill in the fields highlighted in yellow.

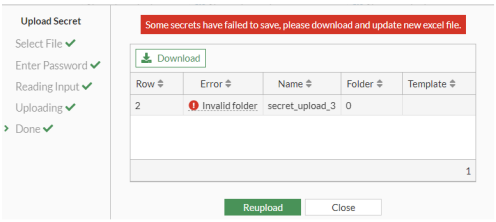
The fields highlighted in red cannot be edited.

8. Save the file as `.xlsm`(Excel workbook) or a `.csv`(Comma delimited) file on your computer.
9. In the *Upload Secret* dialog, select *Upload*, locate the secret upload template file and click *Open*.
10. In *Password*, enter the password set in step 3 to decrypt the secret upload template, and click *Next*.
    Once the secret upload template file is successfully uploaded, *All secrets in the file have been uploaded* message displays.



11. Click *Close*.
12. To refresh the secret list, select *Reload Now* from the message that appears on the bottom-right.

Any failed rows will be displayed in *Upload Secret*, and detailed information can be downloaded by clicking *Download*.



Change password

FortiPAM allows you to manually change the password in a secret.

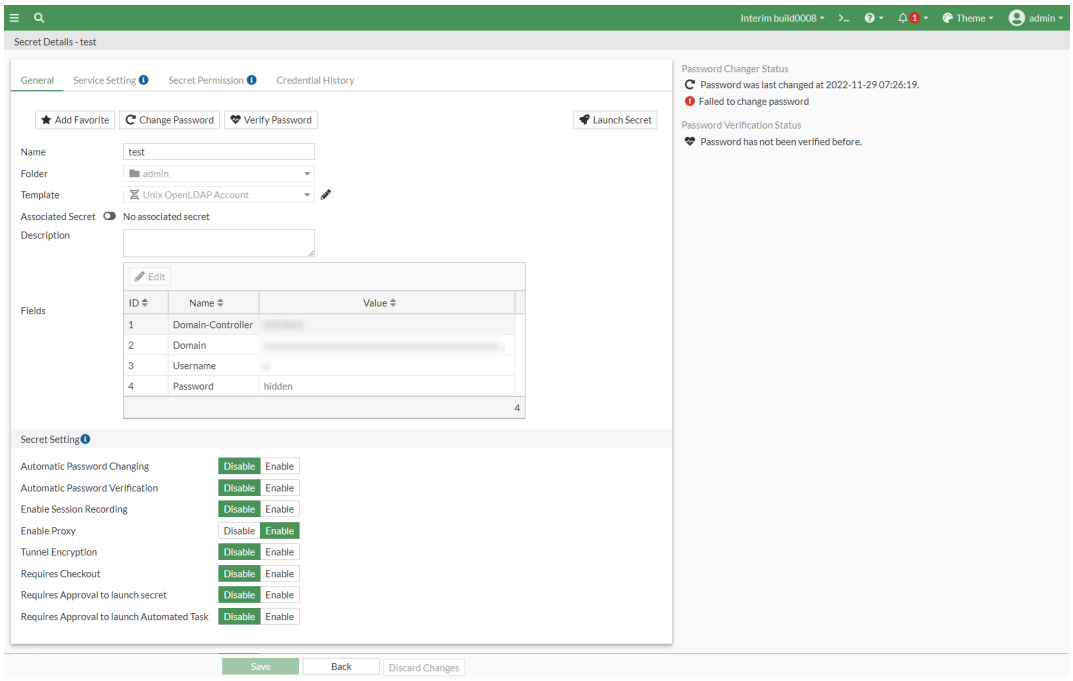
You can only manually change the passwords every 30 seconds.

You can also set up a secret to automatically change the password by enabling *Automatic Password Changing* when creating or editing a secret.

See Automatic password changing on page 131.

To change the password:

1. Go to *Secret* > *Secret List*.
2. In *Secret List*, select a secret, and select *Edit*.
   Alternatively, in *Secrets* > *Personal Folder/Public Folder*, select the folder where the secret is located, and double-click the secret.
   The *Secret Details* window opens.



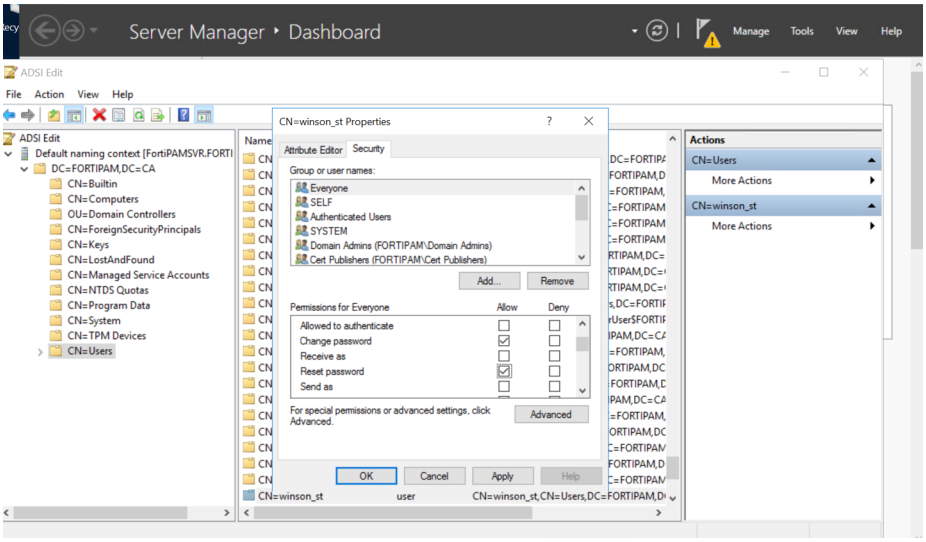
3. From the top, select *Change Password* to change the password.
4. In *Generate next password*, select from the following two options:
   - *Randomly*: automatically change the password.
   - *Customized*: enter a new password manually.

   Note: The *Customized* option may be disabled if the secret template does not use password for authentication.

   To be able to successfully change the password manually, the password must follow password requirements set in Password policies on page 132.

5. If the password changer failed to change the password last time, it reuses the previously attempted password if it has not been reset.
   In *Reuse attempted password*, select *Yes* to reuse the last attempted password that failed or select *No* to generate a new password.
   If you selected *No* in *Reuse attempted password*, select *Randomly* to generate a new password automatically or select *Customized* to enter the password manually.
6. Click *OK*.
   Once the password has changed, *Password Changer Status* shows the date and time when the password was changed and its status.

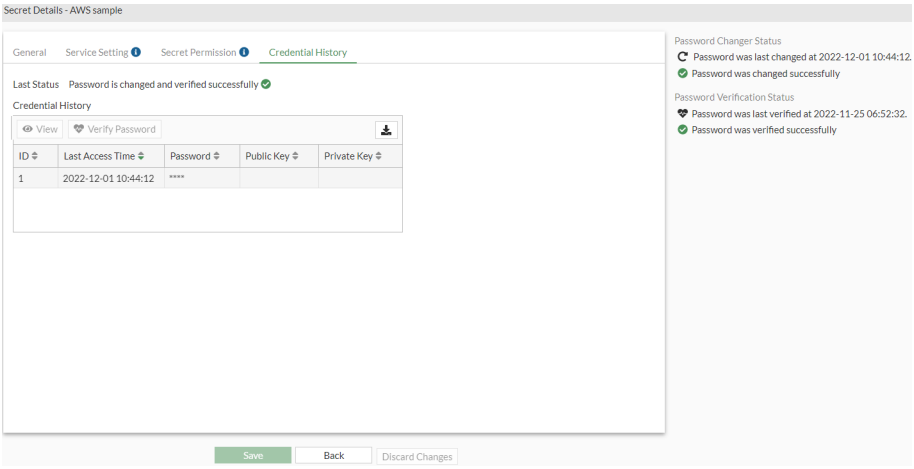
When using a password changer on Windows AD by LDAPs, it is required to enable both *Change password* and *Reset password* for the user on Windows AD.



Credential History

FortiPAM retains any previous credentials that have been used by the secret before. These credentials appear in the *Credential History* tab in the secret page. If the last password change failed, FortiPAM retains the last credential that was tried. You can use the credential history to restore the secret password if the credential on the remote server and FortiPAM are out of sync.

When editing a secret, go to the *Credential History* tab to see a history of changes made to the password.



To view previous credentials:

1. Go to *Secrets* > *Secret List*.
2. In *Secret List*, select a secret, and select *Edit*.
   Alternatively, in *Secrets* > *Personal Folder/Public Folder*, select the folder where the secret is located, and double-click the secret.

The *Secret Details* window opens.

3. Go to the *Credential History* tab.
4. To view the last credential used from a failed password change, click *View Last Credential* to show the password/private key in clear text.
   To view the credentials that have previously been successful, click the entry row to view and then click *View* to show the password/private key in clear text.
   To clear the last credential used in a failed password change, click *Clear Last Credential*. The last credential used is removed from the credential history.

To restore password using credential history:

1. Go to *Secrets* > *Secret List*.
2. In *Secret List*, select a secret, and select *Edit*.
   Alternatively, in *Secrets* > *Personal Folder/Public Folder*, select the folder where the secret is located, and double-click the secret.
   The *Secret Details* window opens.
3. Go to the *Credential History* tab.
4. To use the last credential from a failed password change, click *Verify Last Credential*.
   If the password change is successful, a message shows up asking if you want to restore the credential. Click *Yes* to restore the credential.
   To use a previous entry, click the entry row to use and click *Verify Password*. A message appears if the password change is successful.

To configure Windows to allow FortiPAM to change its local user password by SAMBA:

1. On Windows, open *Local Security Policy*.
2. Go to *Local Policies* > *Security Options* > *Network access: Restrict clients allowed to make remote calls to SAM*.
3. Right-click *Network access: Restrict clients allowed to make remote calls to SAM* and select *Properties*.
4. Select *Edit Security...*.
5. Add users to *Group or user names:* in the *Security Settings for Remote Access to SAM* window.
6. Click *OK*.
7. Click *OK*.

Verify password

On FortiPAM, you can verify the password in a secret manually to check its accuracy, and confirm if the target server is reachable.

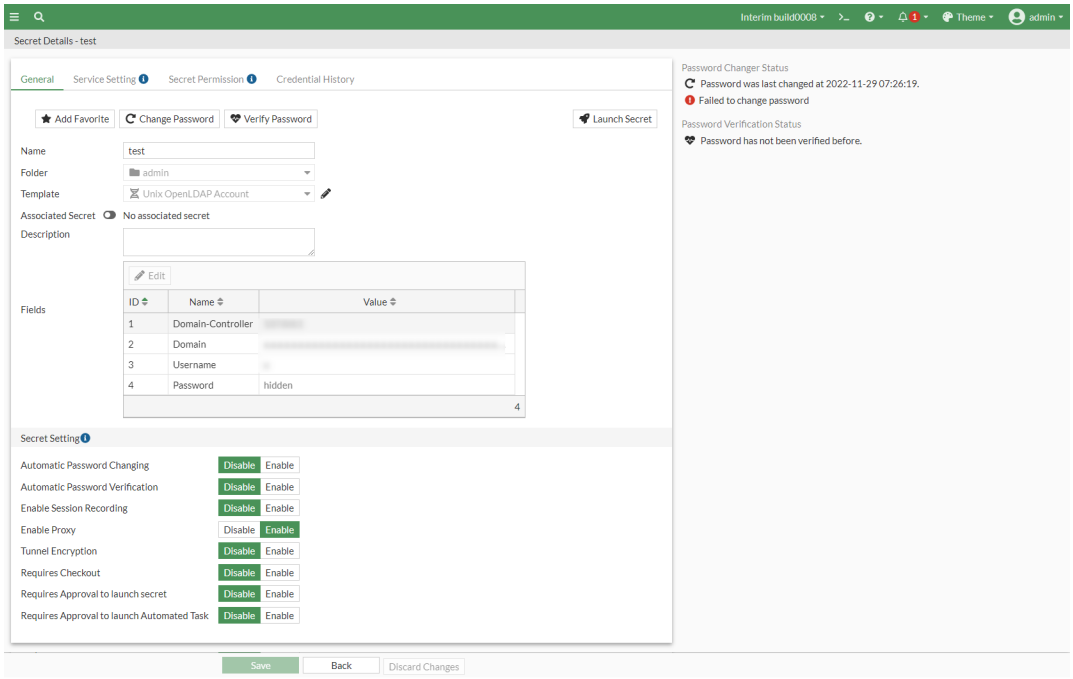
You can only manually verify passwords every 5 seconds.

You can also set up a secret to automatically verify the password by enabling *Automatic Password Verification* when creating or editing a secret.

See Automatic password verification on page 132.

To verify the password:

1. Go to *Secrets* > *Secret List*.
2. In *Secret List*, select a secret, and select *Edit*.
   Alternatively, go to *Folders*, and select the folder where the secret is located, and double-click the secret.
   The *Secret Details* window opens.



3. From the top, select *Verify Password*.
   Once the password has been verified, *Password Verification Status* shows the date and time when the password was verified and its status.

Example secret configurations - example

To configure an SSH password:

1. Go to *Secrets* > *Secret List*.
2. In *Secret List*, select *Create*.
   The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create Secret*.
   The *New Secret window* opens.
5. Enter a secret name.
6. In the *Template* dropdown, select *Unix Account (SSH Password)* default template.
7. In *Fields*, enter information for the following fields:
   a. *Host*
   b. *Username*
   c. *Password*
8. Click *Submit*.

To configure an SSH key:

1. Repeat steps 1 to 4 as shown in Configuring an SSH password.
2. Enter a secret name.
3. In the *Template* dropdown, select *Unix Account (SSH Key)* default template.
4. In *Fields*, enter information for the following fields:
   a. *Host*
   b. *Username*
   c. *Public-key* and *Private-key*:
   Select from the following three options:
   - Upload a key file by selecting *File Upload* and then click *Upload* to locate and upload the key file from your computer.
   - Select *Text* and enter the public key in the space below.
   - Select *Generate* and then select a type of encryption algorithm (*RSA*, *DSA*, *ECDSA*, and *ED25519*) and number of *Bits* to use in the auto-generated key-pair.

   When *ED25519* is selected as the encryption algorithm, *Bits* are not required.

   Using the auto-generated key-pair clears out any existing key-pair.

   d. *Passphrase*, if any.
5. Ensure that proxy is enabled in the *Secret Setting* pane.

   An SSH key can only be launched when the secret has *Enable Proxy* checked.

6. Click *Submit*.
   If using an AWS-VM, ensure that *RSA Sign Algorithm* is set to *RSA SHA-256 signing algorithm* in the *Service Setting* tab.

To configure a Windows AD-LDAP secret:

1. Repeat steps 1 to 4 as shown in Configuring an SSH password.
2. Enter a secret name.
3. In the *Template* dropdown, select *Windows Domain Account* default template.
4. In *Fields*, enter information for the following fields:
   a. *Domain-Controller*
   b. *Domain*
   c. *Username*
   d. *Password*
5. Click *Submit*.

To configure Windows Samba secret:

1. Repeat steps 1 to 4 as shown in Configuring an SSH password.
2. Enter a secret name.
3. In the *Template* dropdown, select *Windows Domain Account(Samba)*.
4. In *Fields*, enter information for the following fields:
   a. *Domain-Controller*
   b. *Domain*
   c. *Username*
   d. *Password*
5. Click *Submit*.

To configure a Cisco secret:

1. Repeat steps 1 to 4 as shown in Configuring an SSH password.
2. Enter a secret name.
3. In the *Template* dropdown, select *Cisco User (SSH Secret)*.
4. In *Fields*, enter information for the following fields:
   a. *Host*
   b. *Username*
   c. *Password*
5. Click *Submit*.
   If the password change feature needs to be used, then one more secret needs to be created for the Cisco enable command:
   a. Repeat steps 1 and 2.
   b. In the *Template* dropdown, select *Cisco Enable Secret*.
   c. In *Fields*, enter information for the following fields:
      i. *Host*
      ii. *Password*
   d. Click *Submit*.
6. Go to the *Service Setting* tab for the Cisco secret that was earlier created (steps 1 - 5).
7. Optionally, enable *SSH Auto-Password*.
8. Go to the *General* tab, and ensure that *Associated Secret* is enabled.
9. In the *Associated Secret* dropdown, select the Cisco enable secret.
10. Click *Save*.

To configure an AWS web account secret:

1. Repeat steps 1 to 4 as shown in Configuring an SSH password.
2. Enter a secret name.
3. In the *Template* dropdown, select *AWS Web Account*.
4. In *Fields*, enter information for the following fields:
   a. *URL*
   b. *Username*
   c. *Password*

d. *AccountID*: Used for IAM accounts.
For AWS root accounts, the field remains empty. Otherwise, the web extension treats the secret as an IAM account secret impacting the login process.

5. Click *Submit*.

Personal/public folder

Folders are the containers of secrets. Folders help you organize customers, computers, regions, and branch offices, etc.

Before you create any secret, you should choose a folder where the secret is added.

You can organize your folders as trees. With folders, granting permissions is simplified as all the secrets in a folder share permissions.

Each folder has different permission to different user or user group. A folder may be set to have one of the following permission:

- *View*: Ability to view secrets and subfolders in a folder.
- *Add*: Ability to create new secrets and subfolders.
- *Edit*: Ability to create/edit secrets, subfolders, and the folder itself.
- *Owner*: The highest possible permission level with the ability to create, edit, delete, and move secrets, subfolders, and the folder itself.

The following shows a folder with secrets in it:

The *Personal Folder/Public Folder* tab in *Secrets* contains the following options:

Go back up one level in the tree	Click to go back up a level in the tree.
Edit Current Folder	Edit the current folder.
Create	From the dropdown, create a secret or a folder. See Creating a secret on page 49 and Creating a folder on page 76.
Delete	Delete selected subfolders or secrets. See Delete a subfolder or a secret.
Open Tree	Select to open the folder tree. You can use this option to go to a folder. See Opening a folder on page 74.
Search	Enter a search term in the search field, then hit `Enter` to search the folders list. To narrow down your search, see Column filter.

Launch Secret, *Make Request*, *Edit* (edit selected folder or secret), *Move*, *Clone* (make a copy of the selected secret), and *Add Favorite* (add secret to the favorite list) options can be found when you right-click a secret or a folder.

Opening a folder

Before opening a folder, ensure that your account has sufficient permission to view folders.

To open a folder:

1. Go to *Secrets* > *Personal Folder/Public Folder*, and select *Open Tree*.
   Alternatively, in the folder list, double-click a folder to open.
2. In the *Open* window, locate the folder you intend to open from the tree.
3. Click *Open Folder*.

Moving a subfolder

Before moving a subfolder, ensure that your account has sufficient permission to move subfolders.

To move a subfolder:

1. Go to *Secrets* > *Personal Folder/Public Folder*, and select *Open Tree*.
2. In the *Open* window, from the tree, locate the parent folder for the subfolder you intend to move and click *Open Folder*.
3. Right-click the subfolder and select *Move*.
   The *Move to* window opens.
4. Select the destination folder from the tree and then select *Move Folder*.

Moving a secret to a different folder

Before moving a secret, ensure that your account has sufficient permission to move secrets.

To move a secret:

1. Go to *Secrets* > *Personal Folder/Public Folder*, and select *Open Tree*.
2. In the *Open* window, from the tree, locate the folder where the secret resides and click *Open Folder*.
3. Right-click the secret and select *Move*.
   The *Move to* window opens.
4. Select the destination folder from the tree and then select *Move Secret*.

Moving multiple secrets to a different folder

To move multiple secrets to a different folder:

1. Go to *Secrets* > *Personal Folder/ Public Folder*, and select *Open Tree*.
2. In the *Open* dialog, from the tree, locate the folder where the secrets reside and click *Open Folder*.
3. Hold the `ctrl` key as you select the secrets from the folder.
4. Right-click and then select *Move*.
5. In the dialog that appears, locate the target folder where the selected secrets will be moved to, and click *Move Secret*.

If you do not have *Write* permission for the first secret you selected, the *Move* option is disabled.

If some secrets fail to move due to insufficient permissions, select *Click here for more details* to view the list of secrets that failed to move.

Editing a subfolder or a secret:

Before editing a folder or a secret, ensure that your account has sufficient permission to edit folders and secrets.

To edit a subfolder or a secret:

1. Go to *Secrets* > *Personal Folder/Public Folder*, and select *Open Tree*.
2. In the *Open* window, from the tree, locate the parent folder where the subfolder or the secret resides and click *Open Folder*.

To edit the current folder you are in, select *Edit Current Folder*.

3. Right-click a subfolder or secret and then select *Edit*.

   The *Edit Secret Folder* or *Secret Details* window opens.
4. Update the options as needed.

The options when editing the folder or a secret are same as when creating a folder or a secret.

See Creating a folder on page 76 and Creating a secret on page 49.

Deleting a subfolder or a secret:

Before deleting a folder or a secret, ensure that your account has sufficient permission to delete folders or secrets.

To delete a subfolder or a secret:

1. Go to *Secrets* > *Personal Folder/Public Folder*, and select *Open Tree*.
2. In the *Open* window, from the tree, locate the parent folder where the subfolder or the secret resides and click *Open Folder*.
3. Right-click a subfolder or secret and then select *Delete*.
   The *Confirm* dialog appears.
4. Select *OK* to delete the selected folder or secret.

You can only delete an empty folder.

Adding a favorite:

To add a favorite:

1. Go to *Secrets* > *Personal Folder/Public Folder*, and select *Open Tree*.
2. In the *Open* window, from the tree, locate the parent folder where the secret resides and click *Open Folder*.
3. Right-click a secret and then select *Add Favorite*.

Removing a secret from favorite

To remove a secret from favorite:

1. From *Favorite Secrets* in the tree menu, select *Actions* next to the secret you intend to remove from favorites and then select *Remove Favorite* to remove the secret from *Favorite Secrets*.

Creating a folder

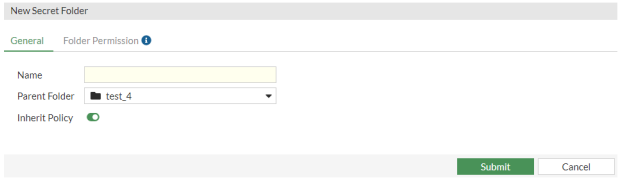
To create a folder:

1. Go to *Secrets* > *Personal/Public Folder* and select *Open Tree*.
2. In the *Open* window, select where you intend to create a folder.

You can create a folder in an existing folder or select *Folder* from the *Create* dropdown in *Root* to create a root folder.

3. Click *Open Folder*.

4. From the *Create* dropdown, select *Folder*.
The *New Secret Folder* window opens.



5. Enter the following information:

General	
Name	Name of the folder.
Parent Folder	From the dropdown, select a parent folder or select *Create* to create a new parent folder. The parent folder is set in step 2. The parent folder cannot be changed for a root folder. Use the search bar to look for a folder. Use the pen icon next to the folder to edit it.
Inherit Policy	Enable to inherit policy that applies to the parent folder. The option is enabled by default when creating a subfolder. You cannot inherit policy for a root folder.
Secret Policy	From the dropdown, select a policy that applies to the folder or select *Create* to create a new policy. See Creating a policy on page 113.

	 Use the search bar to look for a policy.
	 Use the pen icon next to the policy to edit it.
	 This option is only available when *Inherit Policy* is disabled.

Folder Permission

Use the settings in the pane to control access to the folder.

Inherit ZTNA Control	Enable to inherit ZTNA control access permission from the parent folder.
	 By default, secrets in a folder follow the ZTNA control set up in the parent folder. However, when creating or editing a secret you can customize the ZTNA control in the *Secret Permission* tab. See Creating a secret on page 49.
	 The option is enabled by default when creating a subfolder.
	 You cannot inherit ZTNA control access permission for a root folder.
ZTNA Control	Enable to limit access by `ztna-ems-tag`. You can choose whether to match all the tags or only one of them.
	 The option is only available when *Inherit ZTNA Control* is disabled.
Device Tags	Select + to add ZTNA tags or groups.
	 Use the search bar to look up a ZTNA tag or ZTNA tag group.
	Only permitted devices with the selected tags are allowed to launch.
Device Match Logic	Define the match logic for the device tags:

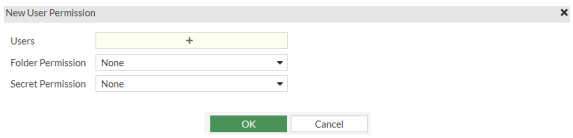
	• *OR*: Devices with any of the selected tags are allowed to launch. • *AND*: Devices must acquire all the selected tags to launch.
Inherit Permission	Enable to inherit permission from the parent folder. The option is enabled by default when creating a subfolder. You cannot inherit permission for a root folder. **Note**: The setting can only be disabled if you have the *Owner* permission. Also, the setting cannot be disabled for any subfolder of the personal folder, i.e., the folder generated for every user.
User Permission	The level of user access to the folder and secrets in the folder. See User Permission on page 79. This option is only available when *Inherit Permission* is disabled. For column settings, see Tables on page 15.
Group Permission	The level of user group access to the folder and secrets in the folder. See Group Permission on page 81. This option is only available when *Inherit Permission* is disabled. For column settings, see Tables on page 15.

6. Click *Submit*.

User Permission

To create a user permission:

1. In step 4 when Creating a folder, select *Create* in *User Permission* when *Inherit Permission* is disabled. The *New User Permission* window opens.



2. Enter the following information:

Users	Select + and from the list, select users in the *Select Entries* window.  Use the search bar to look up a user.  Use the pen icon next to the user to edit it. **To add a new user:** 1. From the *Select Entries* window, select *Create* and then select *+User Definition*. The *New User Definition* wizard opens. 2. Follow the steps in Creating a user on page 159, starting step 2 to create a new user.
Folder Permission	From the dropdown, select an option: • *None*: No access. • *View*: Ability to view secrets and subfolders in the folder. • *Add Secret*: Ability to create new secrets. • *Edit*: Ability to create/edit secrets, subfolders, and the folder itself. • *Owner*: The highest possible permission level with the ability to create, edit, delete, and move secrets, subfolders, and the folder itself.
Secret Permission	From the dropdown, select an option: • *None*: No access. • *List*: Ability to list secrets. You cannot see detailed information on secrets. • *View*: Ability to view secret details and launch a secret. • *Edit*: Ability to create/edit secrets and launch the secrets. • *Owner*: The highest possible permission level with the ability to create, edit, delete, move, and launch secrets.

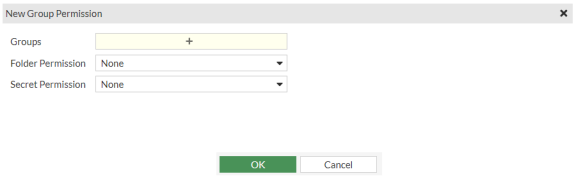
3. Click *OK*.

	From the list, select a user permission and then select *Edit* to edit the user permission. From the list, select user permissions and then select *Delete* to delete the user permissions.

Group Permission

To create group permission:

1. In step 4 when Creating a folder, select *Create* in *Group Permission* when *Inherit Permission* is disabled.
   The *New Group Permission* window opens.



2. Enter the following information:

Groups	Select + and from the list, select user groups in the *Select Entries* window. Use the search bar to look up a user group. Use the pen icon next to the user group to edit it. **To add a new user group:** 1. From the *Select Entries* window, select *Create*. The *Create New User Group* window opens. 2. Follow the steps in Creating user groups, starting step 3.
Folder Permission	From the dropdown, select an option: • *None*: No access. • *View*: Ability to view secrets and subfolders in the folder. • *Add Secret*: Ability to create new secrets. • *Edit*: Ability to create/edit secrets, subfolders, and the folder itself. • *Owner*: The highest possible permission level with the ability to create, edit, delete, and move secrets, subfolders, and the folder itself.
Secret Permission	From the dropdown, select an option: • *None*: No access. • *List*: Ability to list secrets. You cannot see detailed information on secrets. • *View*: Ability to view secret details and launch a secret. • *Edit*: Ability to create/edit secrets and launch the secrets. • *Owner*: The highest possible permission level with the ability to create, edit, delete, move, and launch secrets.

3. Click *OK*.

From the list, select a user group permission and then select *Edit* to edit the user group permission.

From the list, select user group permissions and then select *Delete* to delete the user group permissions.

My requests list

To launch secrets where approval from the members of the approval group(s) is required, you must send out a request.

The request would then be reviewed by the members of the approval group(s), and could be approved or denied by any members of the groups.

Access is granted to the user for only a period of time.

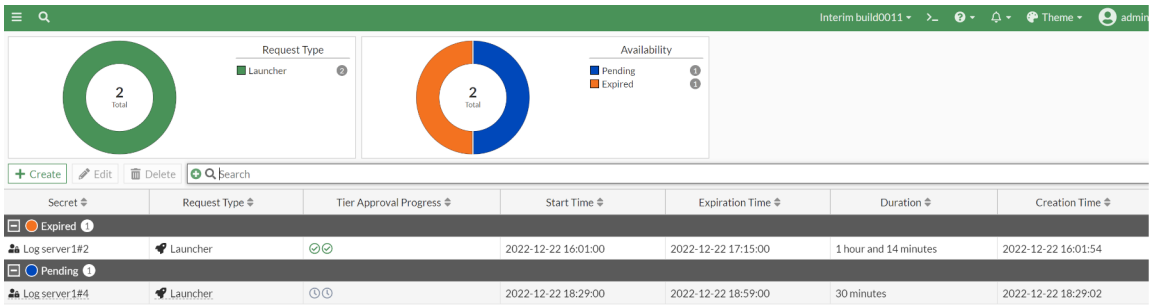
Go to *Secrets* > *My Request List* to see list of secret requests.

The widgets at the top display:

- The request types and their count.
- The status of the requests and their count.

For every request the following fields are listed:

- *Secret*: Secret name with the request ID.
- *Request Type*
- *Tier Approval Progress*
- *Start Time*
- *Expiration Time*
- *Duration*
- *Creation Time*



All requests stay in the list until they are deleted.

Hover over a request in the list to see additional information about the secret.

When an approved request's access time is up, the secret session is terminated even though the secret session is still on.

The *My Request List* tab contains the following options:

Create	Select to create a new request. See Make a request on page 83.
Edit	Select to edit the selected request.  When a secret request is approved, the *Launcher Status* timer shows the remaining time till you (as a requester) have access to the secret when you (as a requester) double-click to open the secret request in *Secrets* > *My Request List*.
Delete	Select to delete the selected requests.
Search	Enter a search term in the search field, then hit `Enter` to search the requests list. To narrow down your search, see Column filter.

Double-click a request to open it and select *Go to Secret* to go to the related secret or select *View Approvers Comments* to view comments from the approvers.

Make a request

To make a request:

1. Go to *Secrets* > *Secret List*.
2. In the *Secrets List*, double-click a secret to open.

   Alternatively, in *Secrets* > *Personal Folder/Public Folder*, go to the folder where the secret is located, and double-click the secret to open.

   You can also go to *Secrets* > *My Requests List*, select *Create*, and skip to step 4.

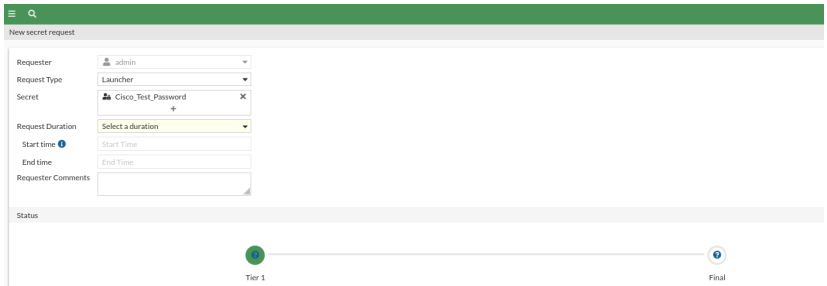
If the secret does not show up, it may be because you do not have the necessary permission to access the secret or the folder where the secret is located.

3. On the top-right, click *Make Request* to send out a request to launch the secret.

If the *Make Request* option does not appear, it is because *Requires Approval to Launch Secret* or *Requires Approval to Launch Job* is disabled in the *Secret Setting* pane when creating or editing a secret.

See Creating a secret on page 49.

The *New secret request* window opens.



4. Enter the following information:

Requester	The requester. **Note**: The option cannot be changed.
Request Type	Select from the following request types: • *Launcher* • *Job*
Secret	When the *Request Type* is *Launcher*, select + and select secrets from the *Select Entries* list. These are secrets with *Requires Approval to Launch Secret* enabled. See Creating a secret on page 49. If available, hover over the secret to see additional information including the folder where the secret is located and the secret template being used for the secret. When the *Request Type* is *Launcher*, use the search bar to look up a secret with *Requires Approval to Launch Secret* enabled.
Job	When the *Request Type* is *Job*, secret associated with the job is automatically selected. The option becomes non-editable. This is the secret with *Requires Approval to Launch Job* enabled. Not all jobs require approval. When editing a secret, the *Requires Approval to Launch Job* option in the *Secret Setting* pane determines which jobs require approval. Select + and select jobs from the *Select Entries* list. **Note**: The option is only available when the *Request Type* is *Job*.

Request Duration	When the *Request Type* is *Launcher*, from the dropdown, select a duration of time or select *Custom* and then enter a date (MM/DD/YYYY) and time range. Alternatively, select the calendar icon and select a start/end date and time. When the *Request Type* is *Job*, the start time is the latest scheduled time among all selected jobs. Enter an end date (MM/DD/YYYY) and time.
Request Comments	Optionally, enter comments for the request.
Status	Current status of the request.

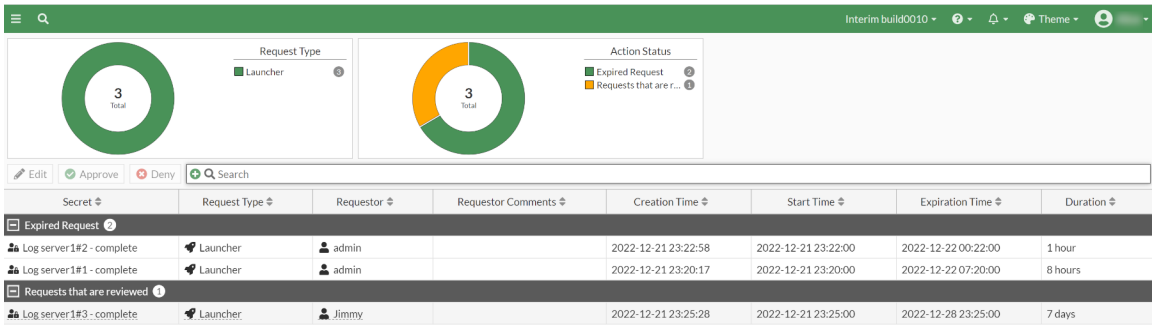
5. Click *Submit*.
   Once the request is submitted, it appears in *My Request List* and *Approval List* tab. See My requests list on page 82 and Approval list on page 85.
   Reviewers specified in Approval profile on page 121 are sent email notifications so that they can log in to FortiPAM from the email link. If the request is approved or denied, the status of the request changes to *Approved* or *Denied* respectively in *My Request List*.

For the approver's email notification, an approver only receives the notification when the request goes to the corresponding tier where the approver is located.

Approval list

Go to *Secrets* > *Approval List* to see a list of secret requests for review.

The *Approval List* tab looks like the following:



The widgets at the top display:

- The request types and their count.
- The status of the requests and their count.

All requests stay in the list until they are deleted.

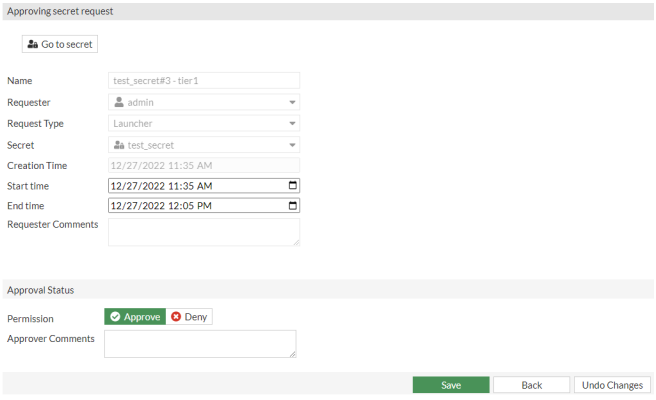
The *Approval List* tab contains the following options:

Edit	Select a request and then select *Edit* to approve or deny the selected request. Alternatively, double-click a request to review the request. See Approve a request on page 86. When a secret request is approved, the *Launcher Status* timer shows the remaining time till the requester has access to the secret when you (as an approver) double-click to open the reviewed request in *Secrets* > *Approval List*.
Approve	Select to approve the selected requests. See Reviewing multiple requests on page 87.
Deny	Select to deny the selected requests. See Reviewing multiple requests on page 87.
Search	Enter a search term in the search field, then hit `Enter` to search the reviews list. To narrow down your search, see Column filter.

Approve a request

To approve or deny a secret request:

1. Go to *Secrets* > *Approval List*, select secret request, and then select *Edit*.
   Alternatively, double-click a request to open it.
   The *Approving secret request* window opens.



In *Start time* and *End time*, select the *Calendar* icon and select a new date and time range to override the requested duration. Alternatively, enter a new date and time range.

2. In the *Approval Status* pane:
   a. In *Permission*, select *Approve* or *Deny*.
   b. In *Approver Comments*, enter comments related to the secret request.

Approver comments are visible to the requester.

3. Click *Save*.

Select *Go to secret* to go to the secret.

Before a request is sent to the next tier or is finalized, the approval action can be revoked by the reviewer who approved it.

If the *Request Type* is *Job*, the output of script can be checked in logs.

Once a secret request is approved or denied, the request status appears in the *Approval List* tab and the status is updated in the My requests list on page 82 tab.

If the request is denied, the user can see the reviewer comments.

To see the reviewer comments:

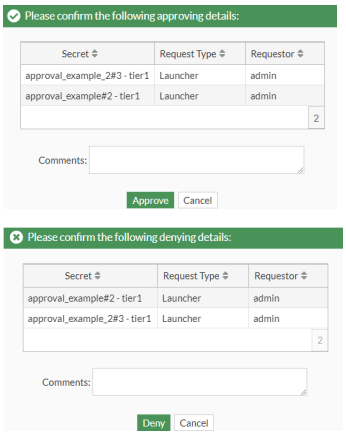
1. Go to *Secrets* > *My Request List*.
2. Double-click the denied request under *Denied/Expired*.
3. Select *View Approvers Comments* to see the reviewer comment.
   Alternatively, go to *Secrets* > *Approval List*, under *Denied/Expired Request*, double-click the request to see the reviewer comments in the *Approval Status* pane.

Reviewing multiple requests

You can approve/deny multiple secret/job requests together in *Secrets* > *Approval List*.

To review multiple requests:

1. Go to *Secrets* > *Approval List*, select multiple secret/job requests from the *Action is required* column, and then select *Approve/Deny*.
   The *Please confirm the following approving/denying details* window opens:



2. From the table, select secret/job requests.
3. Optionally, enter comments about the secret/job request.

Approver comments are visible to the requester.

4. Click *Approve/Deny*.
   Before a request is sent to the next tier or is finalized, the approval action can be revoked by the reviewer who approved it.

If the *Request Type* is *Job*, the output of script can be checked in logs.

Once a secret request is approved or denied, the request status appears in the *Approval List* tab and the status is updated in the My requests list on page 82 tab.

Job list

Go to *Secrets* > *Job List* to create jobs.

A job is an automated task that executes the predefined script at a scheduled time. It could be a one-time or recursive event.

Jobs in FortiPAM allow you to run scripts. Optionally, you can set up a recurring schedule for this script.

For each job; name, secret, status, execution, type, schedule type, and approval status are displayed.

Jobs are not executed when FortiPAM is in maintenance mode.

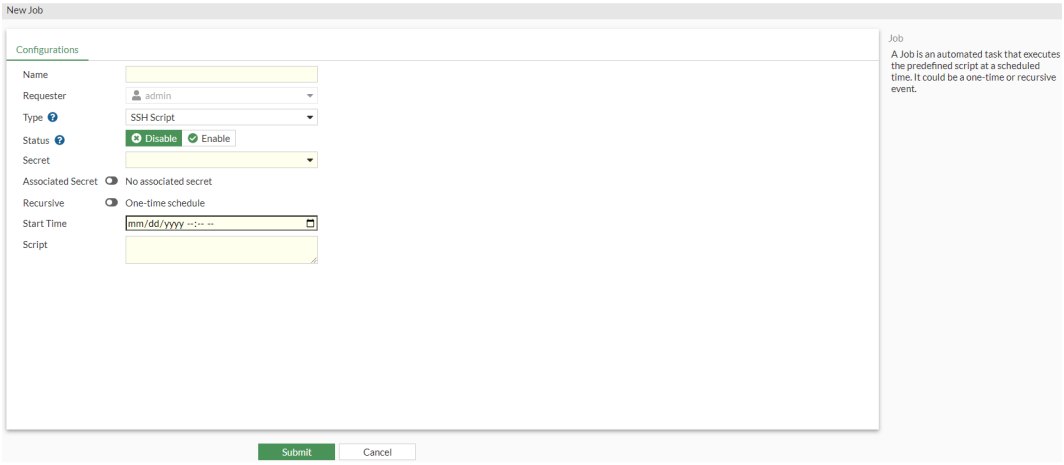
The *Job List* tab contains the following options:

+Create	Select to create a job. See Creating a job on page 89.
Edit	Select to edit the selected job.
Delete	Select to delete the selected jobs.
Search	Enter a search term in the search field, then hit `Enter` to search the jobs list. To narrow down your search, see Column filter.

Creating a job

To create a job:

1. Go to *Secrets* > *Job List*.
2. Select *+Create*.
   The *New Job* window opens.



3. Enter the following information:

Name	Name of the job.
Requester	From the dropdown, select a requester.
Type	From the dropdown, select from the following two options: • *SSH Script*: targeting secrets that work on linux-like machines (default). • *SSH Procedure*: targeting secrets that run on SSH server, e.g., FortiGate, Cisco, or Ubuntu.
Status	Enable/disable the execution of the job (default = disable).
Secret	From the dropdown, select a secret or create a new secret.  Use the search bar to look for a secret.

	 Use the pen icon next to a secret to edit it.
Associated Secret	Enable and then from the dropdown, select an associated secret or create a new secret. When enabled, changing password or verifying password requires credentials from the associated secret. **Note**: The option is disabled by default.  Use the search bar to look for a secret.  Use the pen icon next to a secret to edit it.
Recursive	Enable to set up a recurring schedule. Displays the job execution schedule based on your selections for the related settings. **Note**: The option is disabled by default.
Start Time	The date and time when recurring schedule begins. Enter date (MM/DD/YYYY) and time or select the *Calendar* icon and then select a date and time.
Recurrence	From the dropdown, select from the following three frequencies of recurrence: • *Daily* • *Weekly* • *Monthly* **Note**: The option is only available when *Recursive* is enabled.
Repeat every	The number of days/weeks/months after which the job is executed (1- 400). **Note**: The option is only available when *Recursive* is enabled.
Occurs on	Select from the following days of the month when the job is automatically executed: • *First* • *Second* • *Third* • *Last* • *Last Day* • *Day* Select days of the week when the job is automatically executed.

	When you select *Day*, select + to add days of the month when the job is automatically executed. **Note**: The option is only available when *Recurrence* is set as *Weekly* or *Monthly*.
Script	Enter the script.

4. Click *Submit*.

When editing a job, select the *Make Request* option from the top to make a request to perform a job on the secret associated with the job. See Make a request on page 83.

When editing a job, select the *Log* tabs to see logs related to the job. See Log & report on page 201.

Fort a script job type, you can check the result on the *Edit Job* page after the job is executed.

Secret settings

Secret Settings allows you to configure secret related settings for FortiPAM.

Go to *Secret Settings* to access the following tabs:

Templates

Templates in *Secret Settings* displays a list of customizable and default templates.

The secrets used in FortiPAM are based on templates. The secret templates are customizable so as to meet your requirements.

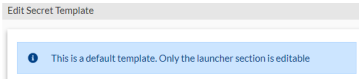
Secret templates allow configuring the fields a secret requires, as well as the types of launchers that are allowed for the secrets. A password changer can also be configured to automatically change a secret's passwords. See Password changers on page 124.

FortiPAM provides the following default templates:

Cisco User (SSH Secret)	Basic template for Cisco SSH account.
Machine	Basic template for a general machine, with all default launchers.
Windows Domain Account	Basic template for a Windows Domain account.
Unix Account (SSH Key)	Basic template for a Unix SSH Key account.
FortiProduct (SSH Password)	Basic template for a FortiProduct SSH Password account
Unix Account (SSH Password)	Basic template for a Unix SSH Password account.
FortiProduct (SSH Key)	Basic template for a FortiProduct SSH Key account.

Cisco Enable Secret	Basic template for Cisco enabled secret account.
Unix OpenLDAP Account	Basic template for an Open LDAP account.
AWS Web Account	Basic template for an AWS account.
Target Only	Basic template for a secret that only manages the target host. When you launch a secret based on the *Target Only* template, you have the following two options: • You can use the current user's general FortiPAM login credentials to finish the authentication to the target server, i.e., SSO mode. Note that the SSO mode only applies to user logins via the general mode, and MFA credentials (if any) are dismissed. • Dynamically enter the credentials for the target server during secret launching. SAML user authentication is not available for secrets based on the *Target Only* template.
Cisco XR Router	A basic template for Cisco server with XR IOS.
Web Account	Basic template for a Web account.
Windows Machine	Basics template for a Windows machine.
Unix Account (Web CIFS)	Basic template for accessing a Unix system with SMB/CIFS service.
Windows Domain Account (Samba)	Basic template for a Samba Windows Domain account.
ESXi Server	A basic template for ESXi server using username and password.
Database Server	A basic template for SQL server using SQL username and password authentication.

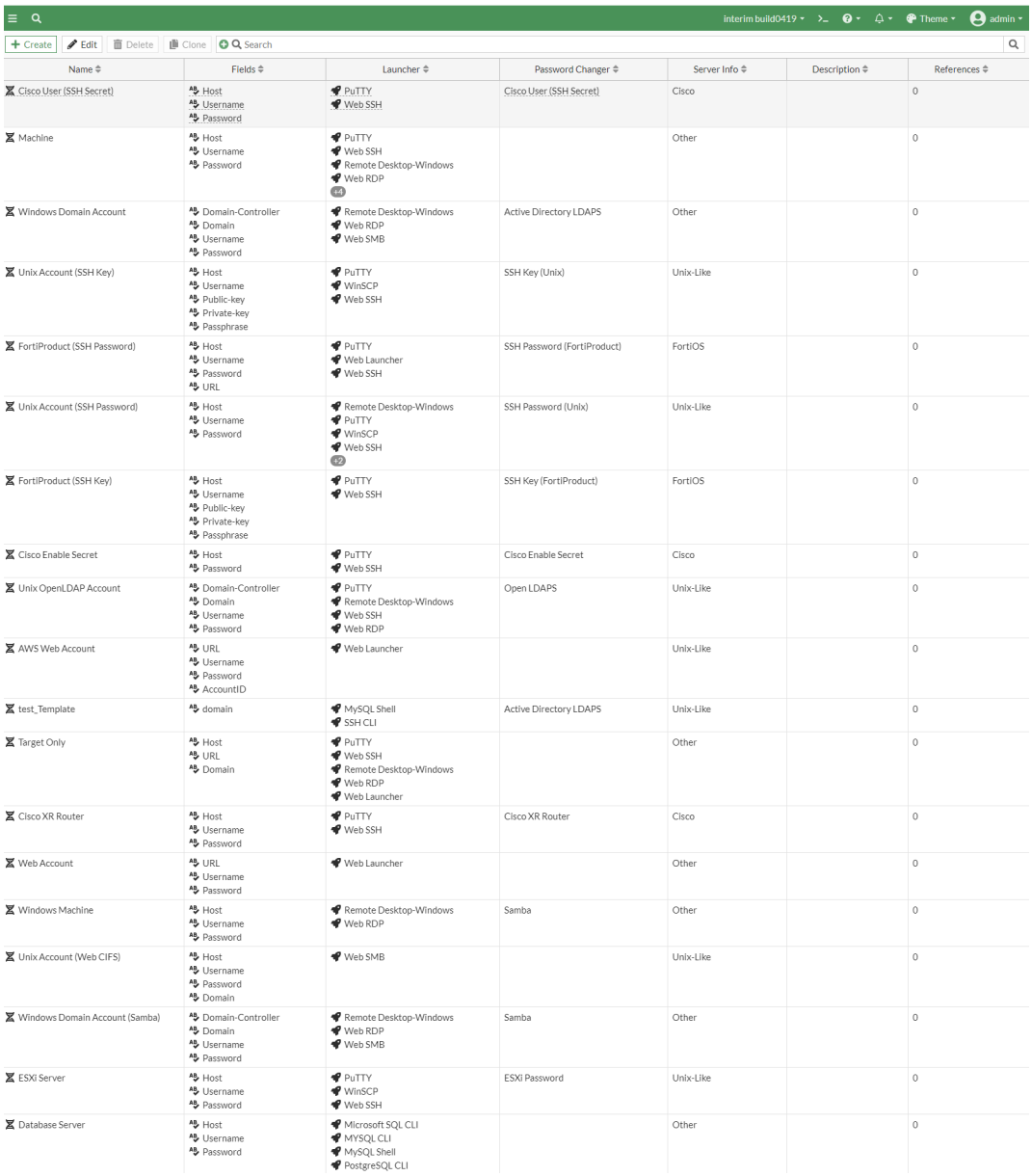
Starting FortiPAM 1.1.0, only the *Launcher* pane of a default secret template can be modified.



The following default templates have *Server Information* set to *Unix-Like*:

- *Unix OpenLDAP Account*
- *Unix Account (SSH Password)*
- *Unix Account (SSH Key)*
- *Unix Account (Web CIFS)*
- *ESXi Server*

For each template; name, fields, launcher, password changer, server info, description, and references are displayed.



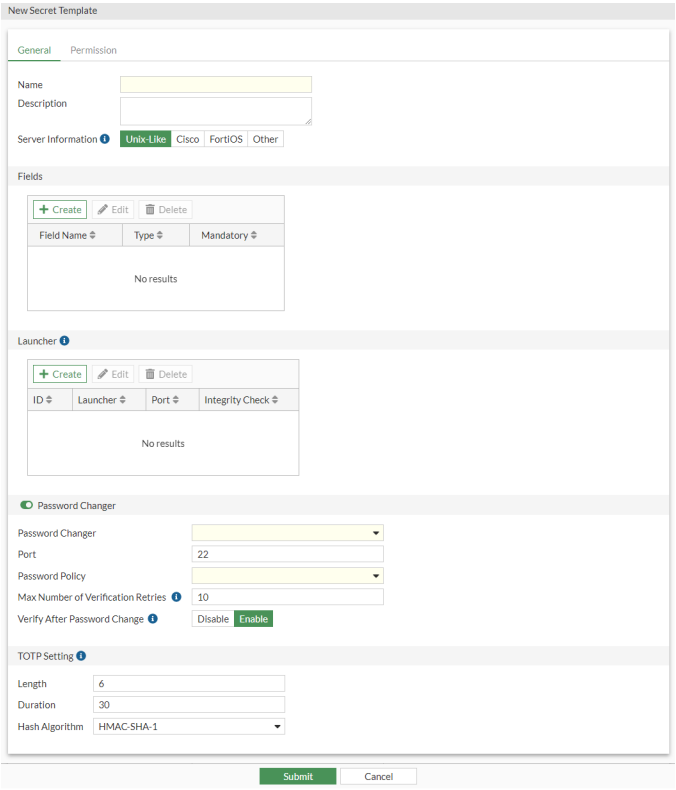
The secret templates list contains the following options:

Create	Select to create a new template. See Creating secret templates on page 95.
Edit	Select to edit the selected template.
Delete	Select to delete the selected templates.
Clone	Select to clone the selected templates.
Search	Enter a search term in the search field, then hit `Enter` to search the secret templates list. To narrow down your search, see Column filter.

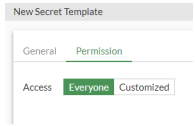
Creating secret templates

To create a secret template:

1. Go to *Secret Settings* > *Templates*.
2. In the secret templates list, select *Create*.
   The *General* tab in the *New Secret Template* window opens.



3. Select *Permission* from the top to switch to the *Permission* tab.



4. Enter the following information:

General	
Name	Name of the template.
Description	Optionally, enter a description.
Server Information	The general type of server to which the template is intended to connect: • *Unix-Like* • *Cisco* • *FortiOS* • *Other*
Fields	Secrets require fields to enter the secret related information.

To add new fields, select *Create* and then enter the following information, and click *OK*:

Field Name	The name of the field.
Type	From the dropdown, select a field type: • *Domain:* A domain field. • *Passphrase:* A passphrase fields. • *Password:* A password field. • *Private-Key:* A private-key field. • *Public-Key:* A public-key field. • *Target-Address:* A target address field. • *Text:* A text field. • *URL:* A URL field. • *Username:* A username field.
Mandatory	Enable to make this field mandatory or disable if this field will be optional.

From the list, select a field and then select *Edit* to edit the field.
From the list, select fields and then select *Delete* to delete the fields.

Launcher

Launcher helps you access a target server. See Launchers on page 103.

A launcher allows you to log in to a website or device without you needing to know the credentials.

To add a new launcher, select *Create* and then enter the following information, and click *OK*:

You can add up to a maximum of 20 launchers.

Launcher Name	From the dropdown, select a launcher.  Use the search bar to look up a launcher.  Use the pen icon to edit a custom launcher. To create a new launcher, in the dropdown, select *Create*. Enter the following information and click *OK*:

Name	The name of the launcher.
Type	From the dropdown, select a launcher type: • *Other client*: Other client launcher type. • *Remote desktop*: RDP client launcher type. • *SSH client*: SSH client launcher type. • *VNC*: VNC client launcher type.

Executable	The program file name, e.g., `putty.exe` for an SSH client.
	 
	Ensure that the program path is already added to the environment variable path in Windows before launching the secret.
	Note:
	An absolute path is also supported, e.g.:
	`C:\Users\user1\Documents\putty.exe`
	`C:\Users\user1\Documents\New folder\putty.exe`

Parameter	The command line parameters: • `$DOMAIN` • `$TARGET` • `$HOST` • `$USER` • `$PASSWORD` • `$VNCPASSWORD` • `$PASSPHRASE` • `$PUB_KEY` • `$PRI_KEY` • `$URL` • `$PORT` • `$TMPFILE` - Example For `putty.exe` as the *Executable*, `-l $USER -pw $PASSWORD $HOST` are the parameters.

	For `putty.exe` as the *Executable* for SSH execution, `-l $USER -pw $PASSWORD $HOST -m C:\Users\user1\Desktop\cmd.txt` or `-l $USER -pw $PASSWORD $HOST -m "C:\Program Files\cmd.txt"` are the parameters.
	Note:
	When there is no space in the path, double quotes are not necessary:
	`-l $USER -pw $PASSWORD $HOST -m C:\Users\user1\Desktop\cmd.txt`
	When there is space in the path, double quotes must be used with backslash:
	`-l $USER -pw $PASSWORD $HOST -m "C:\Program Files\cmd.txt"`

Initial Commands	Configure initializing the environment. See Creating a new launcher command.
Clean Commands	Configure cleaning the environment. See Creating a new launcher command.
Launcher Port	The launcher port number.  The port number will be mapped to the launcher variable `` `$PORT` ``.  The minimum allowed value is `1`.
Integrity Check	Enable/disable integrity check. For information on integrity check, see Integrity check on page 153.  The *Integrity Check* option can only be edited if you choose a launcher in the *Launcher Name* option with a client software entry enabled and selected. **Note**: The option is disabled by default.

 From the list, select a launcher and then select *Edit* to edit the launcher.
From the list, select launchers and then select *Delete* to delete the launchers.

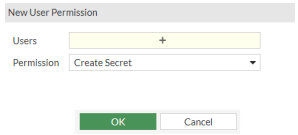
Password Changer A password changer can be configured for a custom secret template to change the password of a secret periodically and to check the health of a secret periodically. **Note**: The option is enabled by default.	
Password Changer	From the dropdown, select the password changer that will be used for this template or create a new password changer. See Creating a password changer on page 125.  Use the search for to look up a password changer.  Use the pen icon next to a password changer to edit it.
Port	The port used for the password changer (default = 22).
Password Policy	The password policy to use in the password changer. From the dropdown, select a password policy or create a new password policy. See Creating a password policy on page 133.  Use the search for to look up a password policy.  Use the pen icon next to a password policy to edit it.
Max Number of Verification Retries	The maximum number of retries allowed after which the connection fails (default = 10).
Verify After Password Change	When enabled, whenever secrets with the template conducts a password change, a verification of the newly changed password is ran. **Note**: The option is enabled by default.
TOTP Setting TOTP (Time-based one-time password) settings. The TOTP configuration from a secret template can be inherited by all the secrets using this template. When configuring the secret, you can override the secret template TOTP configuration. See *TOTP Setting* in Creating a secret on page 49. See Limitations of TOTP on FortiPAM on page 103.	
Length	The length of the TOTP (default = 6, 4 - 9).
Duration	The duration for which the TOTP is valid, in seconds (default = 30, 30 - 90).

Hash Algorithm	Select from the following hash algorithms for TOTP: • *HMAC-SHA-1* (default) • *HMAC-SHA-256* • *HMAC-SHA-512*
Permission	
Template access control settings.	
Access	Template accessible to: • *Everyone*: All users have *Read/Write* permission for templates (default). • *Customized*: A user permission and a group permission table must be configured.
User Permission	The level of user access to the template. See User Permission on page 100. The option is only available when *Access* is set to *Customized*. For column settings, see Tables on page 15.
Group Permission	The level of user group access to the template. See Group Permission on page 101. The option is only available when *Access* is set to *Customized*. For column settings, see Tables on page 15.

5. Click *Submit*.

User Permission

1. In Step 3, when Creating secret templates on page 95, select *Create* in *User Permission*.
   The *New User Permission* window opens.



2. Enter the following information:

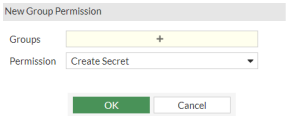
Users	Select + and from the list, select users in the *Select Entries* window. **To add a new user:** 1. From the *Select Entries* window, select *Create* and then select *+User Definition*. The *New User Definition* wizard opens. 2. Follow the steps in Creating a user on page 159, starting step 2 to create a new user.  Use the search bar to look up a user.  Use the pen icon next to a user to edit it.
Permission	From the dropdown, select an option: • *Create Secret*: Ability to see and use the template to create secrets. • *Owner*: The highest possible permission level with the ability to create, edit, and delete templates.  Every template must have at least one owner.

3. Click *OK*.

 From the list, select a user permission entry and then select *Edit* to edit it.
From the list, select user permission entries and then select *Delete* to delete them.

Group Permission

1. In Step 3, when Creating secret templates on page 95, select *Create* in *Group Permission*.
The *New Group Permission* window opens.



2. Enter the following information:

Groups	Select + and from the list, select user groups in the *Select Entries* window. **To add a new user group:** 1. From the *Select Entries* window, select *Create*. The *Create New User Group* window opens. 2. Follow the steps in Creating user groups, starting step 3.  Use the search bar to look up a user group.  Use the pen icon next to a user group to edit it.
Permission	From the dropdown, select an option: • *Create Secret*: Ability to see and use the template to create secrets. • *Owner*: The highest possible permission level with the ability to create, edit, and delete templates.  Every template must have at least one owner.

3. Click *OK*.

 From the list, select a user group permission entry and then select *Edit* to edit it.
From the list, select user group permission entries and then select *Delete* to delete them.

Configuring TOTP settings via the secret template CLI commands - Example

To configure TOTP settings via the CLI:

1. In the CLI console, enter the following commands:

```
config secret template
   edit Unix\ Account\ (SSH\ Password)
      config totp-setting
         set totp-length 8
         set totp-duration 30
         set hash-type hmac-sha1
      end
   end
```

Limitations of TOTP on FortiPAM

1. TOTP auto delivery only supports SSH target authentication.
2. Password changer does not support public key + TOTP authentication.
3. With TOTP, WebSSH only supports the keyboard-interactive authentication method.
4. With a non-proxy or Web launcher, the TOTP code must be copied and entered manually.
5. Do not enable the password changer for an SSH server with password + FortiToken authentication if the username, password, and FortiToken are from another LDAP server.

Launchers

Secret launchers allow users to remotely gain access to a target without the need to know, view, or copy the passwords stored in FortiPAM.

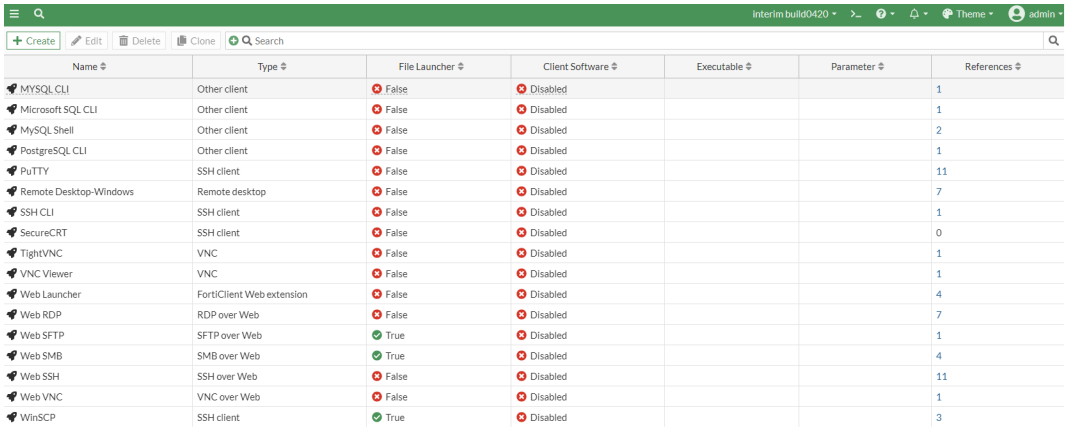
A secret launcher stores an executable and the parameters needed to start a connection to a target.

In proxy mode, browsing triggers ZTNA tunnel between the FortiClient and FortiPAM server.

The FortiPAM chrome extension may have compatibility issues for some specific login pages and cannot fill in the user name and password.

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

For each secret launcher; name, type, file launcher, client software, executable, parameter, and references are displayed.



Name	Type	File Launcher	Client Software	Executable	Parameter	References
MYSQL CLI	Other client	False	Disabled			1
Microsoft SQL CLI	Other client	False	Disabled			1
MySQL Shell	Other client	False	Disabled			2
PostgreSQL CLI	Other client	False	Disabled			1
PuTTY	SSH client	False	Disabled			11
Remote Desktop-Windows	Remote desktop	False	Disabled			7
SSH CLI	SSH client	False	Disabled			1
SecureCRT	SSH client	False	Disabled			0
TightVNC	VNC	False	Disabled			1
VNC Viewer	VNC	False	Disabled			1
Web Launcher	FortiClient Web extension	False	Disabled			4
Web RDP	RDP over Web	False	Disabled			7
Web SFTP	SFTP over Web	True	Disabled			1
Web SMB	SMB over Web	True	Disabled			4
Web SSH	SSH over Web	False	Disabled			11
Web VNC	VNC over Web	False	Disabled			1
WinSCP	SSH client	True	Disabled			3

The following default launchers are available in FortiPAM:

- *MySQL CLI*: A MYSQL CLI launcher for `mysql.exe`.
- *Microsoft SQL CLI*: A MSSQL CLI launcher for `sqlcmd.exe`.
- *MySQL Shell*: A MYSQL CLI launcher for `mysqlsh.exe`.
- *PostgreSQL CLI*: A MYSQL CLI launcher for `mysqlsh.exe`.

PostgreSQL CLI default launcher is connected to postgres by default.

To switch the database:

1. use `\l` to see the full list of all the available database.
2. Use `\c \<dbname\>` to change to the desired database.

Only the non-proxy mode is supported for database related CLI launchers.

- *PuTTY*: A basic SSH client using PuTTY.
- *Remote Desktop- Windows*: A basic RDP client using remote desktop.
- *SSH CLI*: An SSH CLI launcher for `ssh.exe`.
- *SecureCRT*: An SSH Client using SecureCRT.
- *TightVNC*: A basic VNC client using TightVNC.

The TightVNC client does not support connecting to a macOS server in non-proxy mode.

- *VNC Viewer*: A basic VNC client using VNC Viewer.
- *Web Launcher*: A basic web launcher using Fortinet's FortiClient web extension.

Web Launcher is unavailable to users with only *View* permission, as the password can be retrieved using browser dev tools.

Web Launcher is only available to users with *Edit* or *Owner* permission.

For information on setting up folder and secret permissions, see Creating a folder on page 76 or Creating a secret on page 49.

- *Web RDP*: A basic browser based RDP launcher.
- *Web SFTP*: A basic browser based SFTP web launcher.
- *Web SMB*: A basic browser based SMB web launcher.
- *Web SSH*: A basic browser based SSH web launcher.

To copy and paste in the Web SSH console, select the text and then use `Ctrl+ Shift + v`.

- *Web VNC*: A basic browser based VNC web launcher.
- *WinSCP*: A basic WinSCP client using SSH.

- *FortiClient Web extension FortiClient Web Launcher*
- *RDP over Web RDP over Web Launcher*
- *SSH over Web SSH over Web Launcher*
- *VNC over Web VNC over Web Launcher*
- *SMB over Web SMB over Web Launcher*
- *SFTP over Web SFTP over Web Launcher*

The following launchers should not be used for customized launcher:

- *FortiClient Web extension FortiClient Web Launcher*
- *RDP over Web RDP over Web Launcher*
- *SSH over Web SSH over Web Launcher*
- *VNC over Web VNC over Web Launcher*
- *SMB over Web SMB over Web Launcher*
- *SFTP over Web SFTP over Web Launcher*

These launchers will be removed in a future FortiPAM version.

Chrome, Edge, and Firefox are the supported browsers.

Starting FortiPAM 1.1.0, only the *Client Software* toggle/dropdown of a default secret launcher can be modified.

Web SSH, Web RDP, Web VNC, Web SFTP, and Web SMB default launchers always work in proxy mode irrespective of the *Proxy Mode* setting.

PuTTY and WinSCP launchers are not supported when the secret is in non-proxy mode, and the secret uses an SSH key for authentication.

TightVNC launcher is not supported when the secret is in non-proxy mode and requires a username for authentication.

In proxy mode, the following launchers are available to all users:

- Web SSH
- Web RDP
- Web VNC
- Web SFTP
- Web SMB
- Web Launcher
- PuTTY
- WinSCP

- RDP
- VNC Viewer
- TightVNC

In non-proxy mode, the following launchers are available to all users:

- Web SSH (always in proxy mode)
- Web RDP (always in proxy mode)
- Web VNC (always in proxy mode)
- Web SFTP (always in proxy mode)
- Web SMB (always in proxy mode)

In non-proxy mode, the following launchers are only available to users with the permission to view secret password:

- PuTTY
- WinSCP
- RDP
- VNC Viewer
- TightVNC

The *Launchers* tab contains the following options:

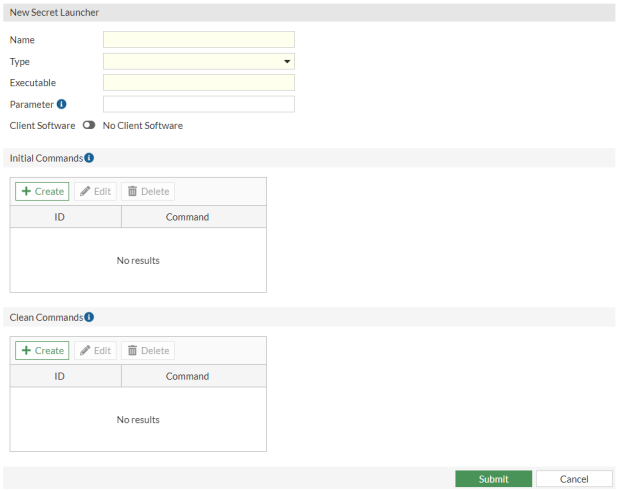
Create	Select to create a new launcher.Creating a launcher on page 106.
Edit	Select to edit the selected launcher.
Delete	Select to delete the selected launchers.
Clone	Select to clone the selected launcher.
Search	Enter a search term in the search field, then hit `Enter` to search the launchers list. To narrow down your search, see Column filter.

Creating a launcher

To create a launcher:

1. Go to *Secret Settings* > *Launchers*.
2. In the secret launchers list, select *Create* to create a new secret launcher.

3. The *New Secret Launcher* window opens.



4. Enter the following information:

Name	The name of the launcher.
Type	From the dropdown, select a type: • *Other client*: Other client launcher type. • *Remote desktop*: RDP client launcher type. • *SSH client*: SSH client launcher type. • *VNC*: VNC client launcher type.

Executable	The program file name, e.g., `putty.exe` for an SSH client.
	
	Ensure that the program path is already added to the environment variable path in Windows before launching the secret.
	
	An absolute path is also supported, e.g.:
	`C:\Users\user1\Documents\putty.exe`
	`C:\Users\user1\Documents\New folder\putty.exe`

Parameter	The command line parameters from the *Available Variables* list. Valid field variables are: • `$DOMAIN` • `$HOST` • `$USER` • `$PASSWORD` • `$VNCPASSWORD`

`$VNCPASSWORD` is filled with the obfuscated password sometimes used by VNC when saving the password to a file.

- `$PASSPHRASE`

`$PASSPHRASE` refers to the passphrase of SSH keys.

- `$PUB_KEY`
- `$PRI_KEY`
- `$URL`
- `$PORT`

`$PORT` is filled in using the port value assigned to the launcher in the template.

- `$TMPFILE`

`$TMPFILE` is filled in with the path to a temporary file, generally for use with launchers that require loading config files (when launching with non-proxy mode).

User input variables are:

- `$TARGET`

The `$TARGET` user input variable can replace the `$HOST` field variable. This allows you to specify the 'target' at the launch time rather than having it hard coded in secret itself.

- Example

For `putty.exe` as the *Executable*, `-l $USER -pw $PASSWORD $HOST` are the parameters.

For `putty.exe` as the *Executable* for SSH execution, `-l $USER -pw $PASSWORD $HOST -m C:\Users\user1\Desktop\cmd.txt`

or

`-l $USER -pw $PASSWORD $HOST -m "C:\Program Files\cmd.txt"` are the parameters.

Note:

When there is no space in the path, double quotes are not necessary:

`-l $USER -pw $PASSWORD $HOST -m C:\Users\user1\Desktop\cmd.txt`

When there is space in the path, double quotes must be used with backslash:

	`-l $USER -pw $PASSWORD $HOST -m "C:\Program Files\cmd.txt"`
Client Software	Enable to select a client software entry from the dropdown. See Integrity check on page 153. Use the search bar to look up a client software entry. **Note**: The option is disabled by default.
Initial Commands Configure initializing the environment. See Creating a new launcher command on page 109.	
Clean Commands Configure cleaning the environment. See Creating a new launcher command on page 109.	

5. Click *Submit*.

Non-proxy environment

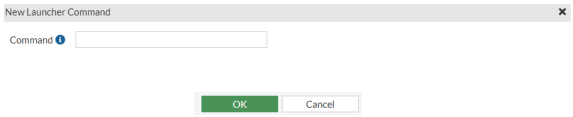
When using launchers with non-proxy mode, launchers may require the environment to be initialized beforehand. You may specify this with init-commands and clean-commands.

Note: Init-commands and clean-commands only run in the non-proxy mode.

Creating a new launcher command

To create a new launcher command:

1. In step 3 when Creating a secret launcher, select *Create* in the *Initial Commands* or *Clean Commands* pane. The *New Launcher Command* window opens.



2. In *Command*, enter the command.

Enter `$` to get the list of valid variables.

3. Click *OK*.

- Select the command from the list and then select *Edit* to edit it.
- Select command(s) from the list and then select *Delete* to delete them.

You can create launchers to be used as file launchers for SSH clients, SMB over the Web, SFTP over the Web, and other types of launchers.

Creating launchers via the CLI - Example

1. In the CLI console, enter the following commands:

```
config secret launcher
   edit "Example Windows RDP"
      set exe "mstsc.exe"
      set para "/V:$TARGET:$PORT /noConsentPrompt"
      set type rdp
      config init-commands
         edit 1
            set cmd "cmdkey /generic:$TARGET /user:$USER /pass:$PASSWORD"
         next
      end
      config clean-commands
         edit 1
            set cmd "cmdkey /del:$TARGET"
         next
      end
   next
end
```

Example secret configurations with launchers - example

To configure a secret with Web SSH launcher:

1. Go to *Secrets* > *Secret List*.
2. In *Secret List*, select *Create*.
   The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create Secret*.
   The *New Secret* window opens.
5. Enter a name for the secret.
6. In the *Template* dropdown, select from the following templates if the templates meet your requirements else see Creating secret templates on page 95 to create a new template:
   Note: Ensure that the template uses *Web SSH* as its launcher.
   a. *Unix Account (SSH Password)*
   b. *Unix Account (SSH Key)*
   c. *FortiProduct (SSH Password)*

   Unix Account (SSH Password), *Unix Account (SSH Key)*, and *FortiProduct(SSH Password)* secret templates are preconfigured with *Web SSH* launcher.
7. In *Fields*, enter the required information.
8. Click *Submit*.

9. In the secret list, select the newly created secret, and select *Launch Secret*.
10. In *Launch Progress*, select *Web SSH*, and then select *Launch*.

To configure a secret with Web RDP launcher:

1. Repeat steps 1 to 5 from Configuring a secret with Web SSH launcher to create a new secret.
2. In the *Template* dropdown, select from the following templates if the templates meet your requirements else see Creating secret templates on page 95 to create a new template:
   a. *Windows Domain Account*
   b. *Windows Domain Account(Samba)*
   Note: Ensure that the template uses *Web RDP* as its launcher.

   Windows Domain Account and *Windows Domain Account(Samba)* secret templates are preconfigured with *Web RDP* launcher.

3. Repeat steps 7 to 9 from Configuring a secret with Web SSH launcher.
4. In *Launch Progress*, select *Web RDP*, and then select *Launch*.

To configure a secret with Web VNC launcher:

1. Repeat steps 1 to 5 from Configuring a secret with Web SSH launcher to create a new secret.
2. In the *Template* dropdown, select the *Machine* template if the template meet your requirements else see Creating secret templates on page 95 to create a new template.
   Note: Ensure that the template uses *Web VNC* as its launcher.

   The *Machine* secret template is preconfigured with *Web VNC* launcher.

   Alternatively, in the CLI console, enter the following commands to create a new template with *Web VNC* launcher:

```
config secret template
   edit <name> #name of the template
      config field
         edit <name> #name of the field
            set type username
            set mandatory enable #the field is mandatory
         next
         edit <name>
            set type password
            set mandatory enable
         next
      end
      config launcher
         edit <id>
            set launcher-name "Web VNC" #Web VNC set as the secret launcher
            set port 5900 #default value
         next
      end
```

   From the *Template* dropdown, select the template you created using the CLI.

3. Repeat steps 7 to 9 from Configuring a secret with Web SSH launcher.
   Ensure that *Automatic Password Changing* is disabled.
4. In *Launch Progress*, select *Web VNC*, and then select *Launch*.

Policies

A secret policy aims to establish guidelines for handling and to protect sensitive information, such as passwords, secret attributes, and personal data. The secret policy helps organizations maintain the confidentiality, integrity, and availability of sensitive information and to minimize the risk of data breaches.

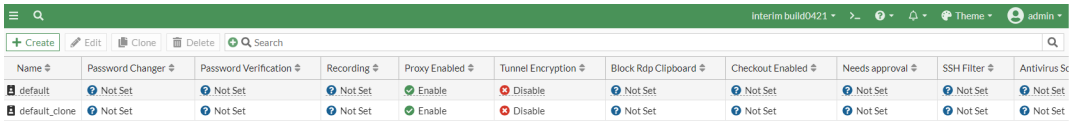
Policies in *Secret Settings* displays a list of secret policies.

Secret policies controls the settings related to a secret. A policy is assigned to a folder when the folder is created. Secrets in a folder follow the rules set in the policy associated with the folder.

A policy allows you to set the following attributes by default for a secret:

- Automatic Password Changing
- Automatic Password Verification
- Enable Session Recording
- Enable Proxy
- Tunnel Encryption
- Requires Checkout
- Requires Approval to Launch Secret
- Requires Approval to Launch Job
- Block RDP Clipboard
- SSH Filter
- Antivirus Scan
- RDP Security Level

The *Policies* tab looks like the following:



The *Policies* list contains the following options:

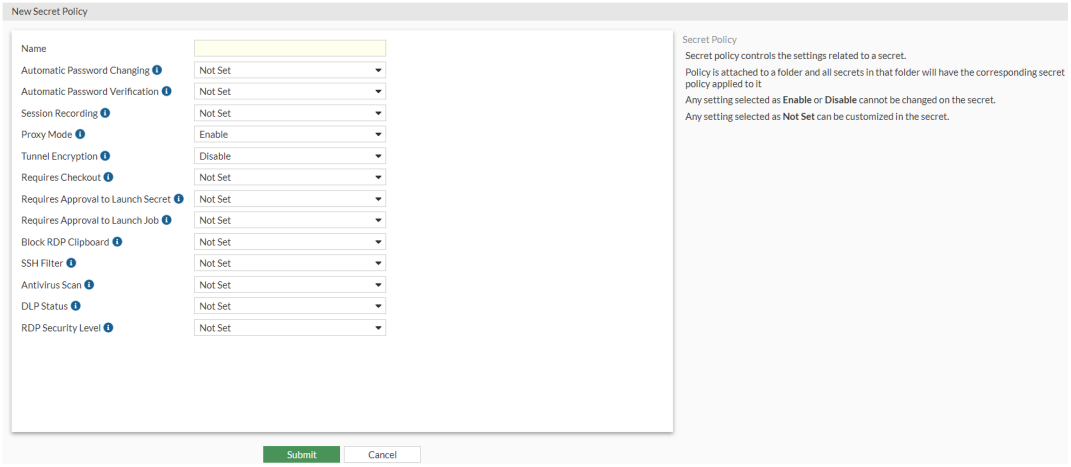
Create	Select to create a policy. See Creating a policy on page 113.
Edit	Select to edit the selected policy.
Clone	Select to clone the selected policy.
Delete	Select to delete the selected policies.

	The default secret policy cannot be deleted.
Search	Enter a search term in the search field, then hit `Enter` to search the policies list. To narrow down your search, see Column filter.

Creating a policy

To create a policy:

1. Go to *Secret Settings* > *Policies*.
2. In *Policies*, select *Create*.
   The *New Secret Policy* window opens.



3. Enter the following information:

Name	Name of the policy.
Automatic Password Changing	Select *Enable*, *Disable*, or *Not Set*. When enabled, password changer for secrets is activated to periodically change the password.
Recursive	Displays the password changing schedule based on your selections for the related settings.
Start Time	The date and time when the *Change Interval (min)* begins. Enter date (MM/DD/YYYY) and time or select the *Calendar* icon and then select a date and time.
Recurrence	From the dropdown, select from the following three frequencies of recurrence: • *Daily* • *Weekly* • *Monthly*

Repeat every	The number of days/weeks/months after which the password is changed (1-400).
Occurs on	Select from the following days of the month when the password is automatically changed: • *First* • *Second* • *Third* • *Last* • *Last Day* • *Day* Select days of the week when the password is automatically changed. When you select *Day*, select + to add days of the month when the password is automatically changed. **Note**: The option is only available when *Recurrence* is set as *Weekly* or *Monthly*.
Editable in Secret	Enable/disable users from customizing the password change schedule in the secret.
Automatic Password Verification	Select *Enable*, *Disable*, or *Not Set*. When enabled, password changer for secrets is activated to periodically verify the password.
Verification Interval (min)	The time interval at which the secrets are tested for accuracy, in minutes (default = 60, 5 - 44640).
Start Time	The date and time when the *Interval(min)* begins. Enter date (MM/DD/YYYY) and time or select the *Calendar* icon and then select a date and time.
Editable in Secret	When enabled, you can customize the password verification schedule in the secret.
Session Recording	Select *Enable*, *Disable*, or *Not Set*. When enabled, user action performed on the secret is recorded.  The video file is available in the log for users with appropriate permission.
Proxy Mode	Select *Enable*, *Disable*, or *Not Set*. When enabled, FortiPAM is responsible to proxy the connection from the user to the secret. When disabled, the non-proxy (direct) mode is used. See Modes of operation on page 17.
Tunnel Encryption	Select *Enable*, *Disable*, or *Not Set*. When launching a native launcher, FortiClient creates a tunnel between the endpoint and FortiPAM. The protocol stack is HTTP/TLS/TCP.

	The HTTP request gives information on the target server then FortiPAM connects to the target server. After that, two protocol options exist for the tunnel between FortiClient and FortiPAM. One is to clear the TLS layer for better throughput and performance. The other is to keep the TLS layer. The launcher's protocol traffic is inside the TLS secure tunnel. If the launcher's protocol is not secure, like VNC, it is strongly recommended to enable this option so that the traffic is in a secure tunnel.  When there is an HTTPS Man In The Middle device, e.g., FortiGate or FortiWeb between FortiClient and FortiPAM, you must enable the *Tunnel Encryption* option. Otherwise, the connection will be disconnected, and the launching will fail. When set to *Not Set*, secrets using the policy can have the option set as either *Enable* or *Disable*. When the option is enabled or disabled, all the secrets using this policy have the same setting for this option as set in the policy.
Requires Checkout	Select *Enable*, *Disable*, or *Not Set*. When enabled, users are forced to check out the secret before gaining access.  At a given time, only one user can check out a secret. Other approved users must wait for the secret to be checked in or wait for the checkout duration to lapse before accessing the secret. See Check out and check in a secret on page 63.
Checkout duration	The checkout duration, in minutes (default = 30, 3 - 120).
Checkin Password Change	Enable/disable automatically changing the password when the user checks in.
Renew Checkout	Enable/disable renewing checkouts.
Max Renew Count	When *Renew Checkout* is enabled, enter the maximum number of renewals allowed for the user with exclusive access to the secret (default = 1, 1 - 5).
Requires Approval to Launch Secret	Select *Enable*, *Disable*, or *Not Set*. When enabled, users are forced to request permission from the approvers defined in the approval profile before gaining access. See Make a request on page 83 and Approval flow on page 120.
Requires Approval to Launch Job	When enabled, users are forced to request permission from the approvers defined in approval profile before being able to perform a job on a secret. See Make a request on page 83 and Approval flow on page 120.
Approval Profile	From the dropdown, select an approval profile, or select *Create* to create a new approval profile. See Approval profile on page 121.

	 Use the search bar to look up an approval profile.  Use the pen icon next to the approval profile to edit it.
Block RDP Clipboard	Select *Enable*, *Disable*, or *Not Set*. When enabled, user is unable to copy/paste from the secret launcher.
SSH Filter	Select *Enable*, *Disable*, or *Not Set*. When enabled, commands defined in the SSH profile to be executed on the secret are blocked.
SSH Filter Profile	From the dropdown, select an SSH filter profile.
Antivirus Scan	Select *Enable*, *Disable*, or *Not Set*. When enabled, it enforces an antivirus profile on the secret. See AntiVirus on page 136.
Antivirus Profile	From the dropdown, select an antivirus profile.
DLP Status	Select *Enable*, *Disable*, or *Not Set*. When enabled, it enforces a particular DLP profile on the secret.
DLP Filter Profile	From the dropdown, select a DLP filter profile.
RDP Security Level	Select a security level when establishing a RDP connection to the secret: • *Best Effort*: If the server supports NLA, FortiPAM uses NLA to authenticate. Otherwise, FortiPAM conducts standard RDP authentication with the server through RDP over TLS. • *NLA*: Network Level Authentication (CredSSP). When an RDP launcher is launched, FortiPAM is forced to use CredSSP (NLA) to authenticate with the target server. • *Not Set* • *RDP*: FortiPAM uses the standard RDP encryption provided by the RDP protocol without using TLS (Web-RDP only). • *TLS*: RDP over TLS. FortiPAM uses secured connection with encryption protocol TLS to connect with the target server.
RDP Restricted Admin Mode	Enable/disable RDP restricted admin mode. Restricted admin mode prevents the transmission of reusable credentials to the remote system to which you connect using remote desktop. This prevents your credentials from being harvested during the initial connection process if the remote server has been compromised. **Note**: The option is only available when *RDP Security Level* is set as *Best Effort* or *NLA*.

Settings set as *Enable* or *Disable* cannot be changed on the secret.

Settings set as *Not Set* can be customized in the secret.

For example - example:

While setting up a policy:

- If *Automatic Password Changing* is enabled, then the secrets in the folder where the policy applies has *Automatic Password Changing* enabled as well.
- If *Automatic Password Changing* is not set, then the secrets in the folder where the policy applies can have *Automatic Password Changing* set as either *Enable* or *Disable*.

4. Click *Submit*.

See Applying a policy to a folder on page 117.

Applying a policy to a folder

To apply a policy to a folder:

1. Go to a folder in *Secrets* > *Personal Folder/Public Folder*.
2. Either select *Edit Current Folder* to edit the folder and skip to step 5, or from the *Create* dropdown, select *Folder*.
3. Enter the name of the folder.
4. From the *Parent Folder* dropdown, select a folder.
5. Enable *Inherit Policy*, so that the folder follows the parent folder policy.

You cannot inherit policy for a root folder.

If *Inherit Policy* is disabled, from the *Secret Policy* dropdown, select a policy profile.

Select *Create* to create a new secret policy. See Creating a policy on page 113.

Use the search bar to look up a policy.

Use the pen icon next to a policy to edit it.

6. Click *Save/Submit*.

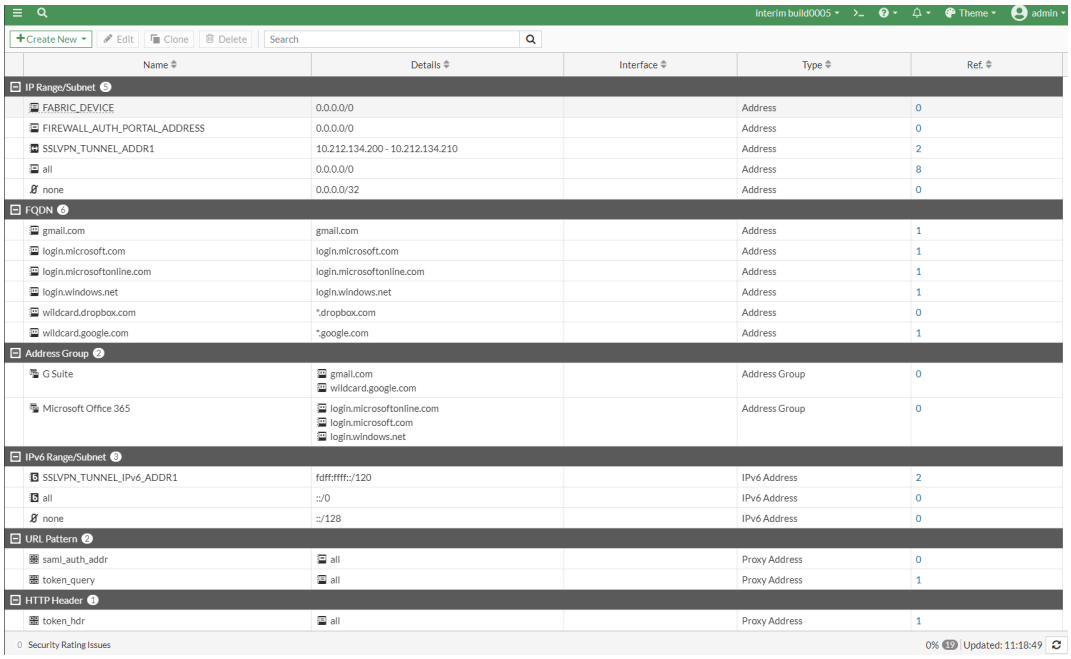
Addresses

The *Addresses* tab in *Secret Settings* displays a list of configured addresses.

An address is a set of one or more IP addresses, represented as a domain name, an IP address and a subnet mask, or an IP address range. You can also specify an address as a country. The address can apply to all interfaces, or you can configure a specific interface.

You can create an address groups, which defines a group of related addresses.

For an address; name, details, interface, type, and references are shown.



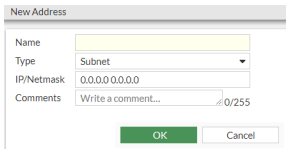
The *Addresses* tab contains the following options:

+Create New	From the dropdown, select *Address* or *Address Group* to create an address or an address group. See Creating an address on page 118 and Creating an address group on page 119
Edit	Select to edit the selected address or address group.
Clone	Select to clone the selected address or address group.
Delete	Select to delete the selected addresses or address groups.
Search	Enter a search term in the search field, then hit `Enter` to search the list. To narrow down your search, see Column filter.
Refresh	To refresh the contents, click the refresh icon on the bottom-right.

Creating an address

To create an address:

1. Go to *Secret Settings* > *Addresses*.
2. From the *+Create New* dropdown ,select *Address*.
   The *New Address* window opens.



3. Enter the following information:

Name	Name of the address.
Type	From the dropdown, select from the following options when the *Category* is *Address*: • *Subnet* (default) • *IP Range* • *FQDN*
IP/Netmask	Enter the IP address and the netmask. **Note**: The option is only available when the *Type* is *Subnet*.
IP Range	Enter the IP address range. **Note**: The option is only available when the *Type* is *IP Range*.
FQDN	Enter the Fully Qualified Domain Name (FQDN). **Note**: The option is only available when the *Type* is *FQDN*.
Comments	Optionally, enter comments about the address.

4. Click *OK*.

Creating an address using the CLI - example

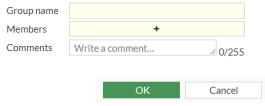
1. Enter the following commands in the CLI console:

```
config firewall address
   edit "SSLVPN_TUNNEL_ADDR1" #The address name.
      set uuid 1e1315b4-fcbf-51ec-d1be-f59b45e347b9
      set type iprange
      set start-ip 10.212.134.200
      set end-ip 10.212.134.210
   next
end
```

Creating an address group

To create an address group:

1. Go to *Secret Settings* > *Addresses*.
2. From the *+Create New* dropdown, select *Address Group*.



3. Enter the following information:

Group name	Name of the group.
Members	Select +, and in *Select Entries*, select a member or create an address or an address group, click *Close*.  Use the search bar to look for a member.  Use the pen icon next to the member to edit it.
Comments	Optionally, enter comments about the address group.

4. Click *OK*.

Creating an address group using the CLI - example

1. Enter the following commands in the CLI console:

```
config firewall addrgrp
   edit "G Suite" #The address group name.
      set uuid 1d22ff2a-fcbf-51ec-442e-9003cab1eecb
         set member "gmail.com" "wildcard.google.com"
   next
end
```

Approval flow

To launch secrets where approval from the members of the approval group(s) is required, an approval profile needs to be set up.

By default, secrets do not require approval to access them. See Enabling approval profiles for a secret on page 121.

The approval profile defines the number of tiers of approvals required for the user to be able to launch the secret. Each tier includes the following information:

- The number of approvals required to pass through the tier.
- The users reviewing the secret request.
- The user groups reviewing the secret request.

FortiPAM supports up to 3 approval tiers.

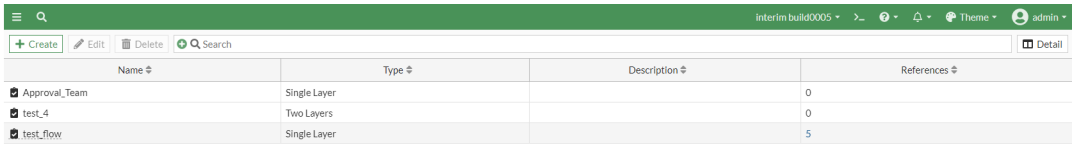
See Approval profile on page 121.

Approval profile

Go to *Approval Profile* in *Secret Settings* to see a list of the configured approval profiles.

For every approval profile, the following fields are shown:

- *Name*
- *Type*
- *Description*
- *Reference*



For secret requests, before the request is finalized, a *Deny* action from any member of the approval profile stops the request from going to the subsequent approval tier. The requester is immediately alerted about the denial of the request.

The *Approval Profile* tab contains the following information:

Create	Select to create a new approval profile. See Create an approval profile on page 122.
Edit	Select to edit the selected approval profile.
Delete	Select to delete the selected profiles.
Search	Enter a search term in the search field, then hit `Enter` to search the approval profiles list. To narrow down your search, see Column filter.
Details	Select to see details of the selected approval profile.

Enabling approval profiles for a secret

To enable approval profile:

1. Go *Secrets* > *Secret List*.
2. In *Secret List*, select a secret and then select *Edit*.
   The *Secret Details* window opens.
3. In the *Secret Setting* pane, enable *Requires Approval to Launch Secret* to require users to request permission from the approvers defined in the approval profile for secret launching.

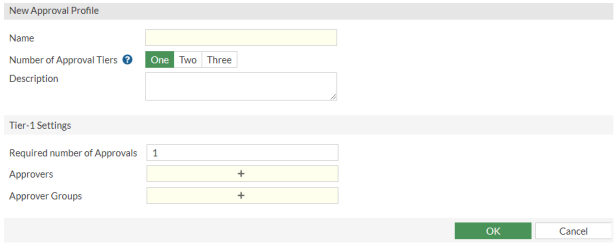
Alternatively, enable *Requires Approval to Launch Job* to require users to request permission from the approvers defined in the approval profile for job execution.

4. In the *Approval Profile* dropdown, select an approval profile, or select *Create* to create a new approval profile. See Create an approval profile on page 122.
5. Click *Save*.

Create an approval profile

To create an approval request:

1. Go to *Secret Settings* > *Approval Profile*.
2. Select *Create* to create a new approval profile.
   The *New Approval Profile* window opens.



3. Enter the following information:

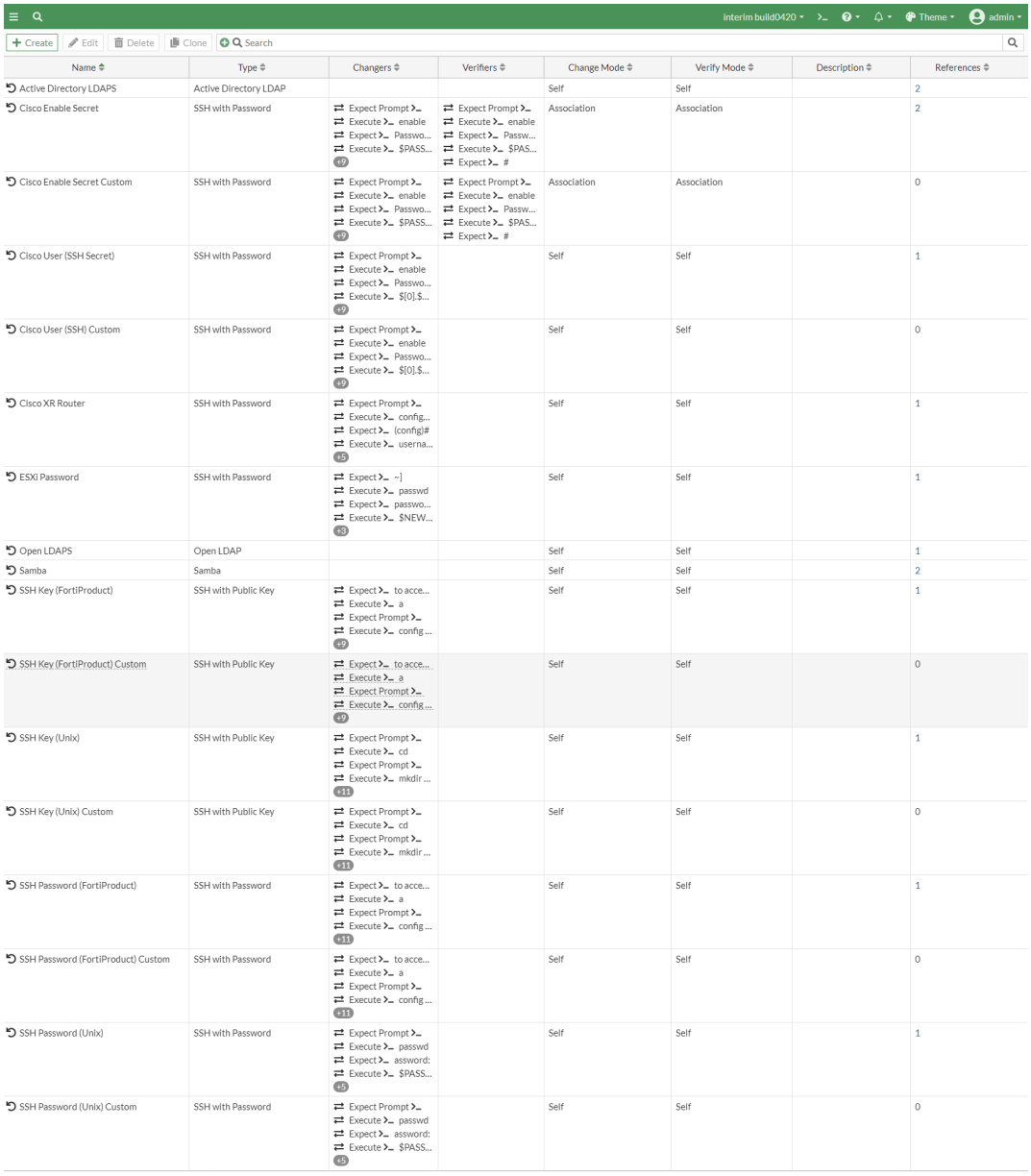
Name	The name of the approval profile.
Number of Approval Tiers	The number of approval tiers a secret request is processed through.
Description	Optionally, enter a description.
Tier-1 Settings	
	 Tier 2 and 3 options are same as tier 1.
Required number of Approvals	The minimum number of approvals required.  The number of user or user groups reviewing a secret request as part of an approval profile must be at least equal to the number of approvals required to pass the request to the next tier or approve it.
Approvers	Select + and from the list, select users in the *Select Entries* window. The selected users will review the secret request. **To add a new user:** 1. From the *Select Entries* window, select *Create*. The *New User Definition* wizard opens. 2. Follow the steps in Creating a user on page 159, starting step 2 to create a new user.  Use the search bar to look up a user.
Approver Groups	Select + and from the list, select user groups in the *Select Entries* window. The selected user groups will review the secret request. **To add a new user group:** 1. From the *Select Entries* window, select *Create*. The *Create New User Group* window opens. 2. Follow the steps in Creating user groups, starting step 3.  Use the search bar to look up a user group.

4. Click *OK*.

Password changers

A password changer can be configured for a custom secret template to periodically change the password of a secret and periodically check the health of a secret.

For each password changer; name, type, changers, verifiers, change mode, verify mode, description, and references are displayed.



Name	Type	Changers	Verifiers	Change Mode	Verify Mode	Description	References
Active Directory LDAPS	Active Directory LDAP			Self	Self		2
Cisco Enable Secret	SSH with Password	Expect Prompt >_ Execute >_ enable Expect >_ Passwo... Execute >_ $PASS... +7	Expect Prompt >_ Execute >_ enable Expect >_ Passw... Execute >_ $PAS... Expect >_ #	Association	Association		2
Cisco Enable Secret Custom	SSH with Password	Expect Prompt >_ Execute >_ enable Expect >_ Passwo... Execute >_ $PASS... +9	Expect Prompt >_ Execute >_ enable Expect >_ Passw... Execute >_ $PAS... Expect >_ #	Association	Association		0
Cisco User (SSH Secret)	SSH with Password	Expect Prompt >_ Execute >_ enable Expect >_ Passwo... Execute >_ ${0}.$... +7		Self	Self		1
Cisco User (SSH) Custom	SSH with Password	Expect Prompt >_ Execute >_ enable Expect >_ Passwo... Execute >_ ${0}.$... +9		Self	Self		0
Cisco XR Router	SSH with Password	Expect Prompt >_ Execute >_ config... Expect >_ (config)# Execute >_ userna... +5		Self	Self		1
ESXi Password	SSH with Password	Expect >_ ~] Execute >_ passwd Expect >_ passwo... Execute >_ $NEW... +3		Self	Self		1
Open LDAPS	Open LDAP			Self	Self		1
Samba	Samba			Self	Self		2
SSH Key (FortiProduct)	SSH with Public Key	Expect >_ to acce... Execute >_ a Expect Prompt >_ Execute >_ config ... +9		Self	Self		1
SSH Key (FortiProduct) Custom	SSH with Public Key	Expect >_ to acce... Execute >_ a Expect Prompt >_ Execute >_ config ... +9		Self	Self		0
SSH Key (Unix)	SSH with Public Key	Expect Prompt >_ Execute >_ cd Expect Prompt >_ Execute >_ mkdir ... +11		Self	Self		1
SSH Key (Unix) Custom	SSH with Public Key	Expect Prompt >_ Execute >_ cd Expect Prompt >_ Execute >_ mkdir ... +11		Self	Self		0
SSH Password (FortiProduct)	SSH with Password	Expect >_ to acce... Execute >_ a Expect Prompt >_ Execute >_ config ... +11		Self	Self		1
SSH Password (FortiProduct) Custom	SSH with Password	Expect >_ to acce... Execute >_ a Expect Prompt >_ Execute >_ config ... +11		Self	Self		0
SSH Password (Unix)	SSH with Password	Expect Prompt >_ Execute >_ passwd Expect >_ assword: Execute >_ $PASS... +5		Self	Self		1
SSH Password (Unix) Custom	SSH with Password	Expect Prompt >_ Execute >_ passwd Expect >_ assword: Execute >_ $PASS... +5		Self	Self		0

FortiPAM offers the following default password changers:

- Active Directory LDAPS
- Cisco Enable Secret
- Cisco User (SSH Secret)

- Cisco XR Router
- ESXi Password
- Open LDAPS
- Samba
- SSH Key (FortiProduct)
- SSH Key (Unix)
- SSH Password (FortiProduct)
- SSH Password (Unix)

Default password changers cannot be edited.

Custom password changers are clones of their default counterparts and are editable.

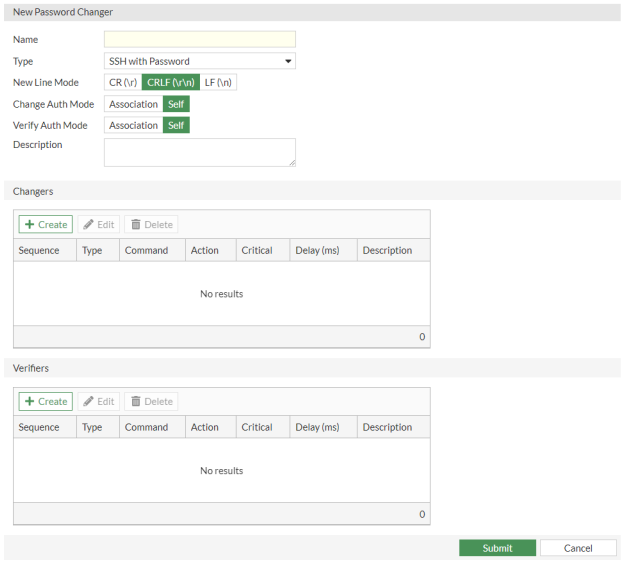
The *Password Changers* tab in *Secret Settings* contains the following options:

Create	Select to create a new password changer. See Creating a password changer on page 125.
Edit	Select to edit the selected password changer.
Delete	Select to delete the selected password changers.
Clone	Select to clone the selected password changer.
Search	Enter a search term in the search field, then hit `Enter` to search the password changers list. To narrow down your search, see Column filter.

Creating a password changer

To create a password changer:

1. Log in to FortiPAM with an account that has sufficient permission to create a password changer.
2. Go to *Secret Settings* > *Password Changers*.
3. Select *Create* to create a new password changer.
   The *New Password Changer* window opens.



4. Enter the following information:

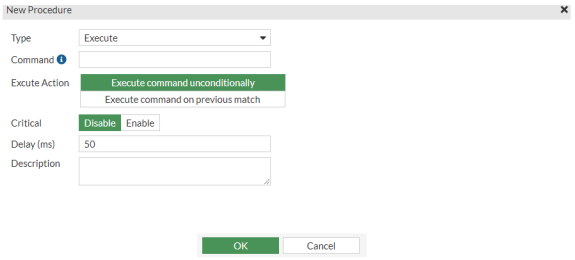
Name	The name of the password changer.
Type	From the dropdown, select a type: • *Active Directory LDAP* • *Open LDAP* • *Samba* • *SSH with Public Key* • *SSH with Password* (default)
New Line Mode	Select from the following options: • *CR (\r)*: Carriage Return (\r) • *CRLF (\r\n)*: Carriage Return and Line Feed (\r\n) (default) • *LF (\n)*: Line Feed (\n)
Change Auth Mode	Select from the following two options: • *Association*: Changing password requires credentials from the associated secret. See *Associated Secret* option when Creating a secret on page 49. • *Self*: Secret can change its password (default).
Verify Auth Mode	Select from the following two options: • *Association*: Verifying password requires credentials from the associated secret. See *Associated Secret* option when Creating a secret on page 49. • *Self*: Secret can verify its password (default).
Description	Optionally, enter a description.
Changers	The password changing procedure. See Changers.

	The option is available only when the *Type* is *SSH with Public Key* or *SSH with Password*.
Verifiers	The password verification procedure. See Verifiers.
	The option is available only when the *Type* is *SSH with Public Key* or *SSH with Password*.

5. Click *Submit*.

Changers

1. In step 4 when Creating a password changer, select *Create* in *Changers*.
   The *New Procedure* window opens.



2. Enter the following information:

Type	From the dropdown, select from the following options: • *Execute* • *Expect* • *Expect Prompt*
Command	Commands to execute on the password changer. Valid variables are: • `$USER` • `$PASSWORD` • `$PASSPHRASE` • `$NEWPASSWD` • `$NEW_PUB_KEY` • `$NEW_PRI_KEY` • `$[0].$` • `$PUB_KEY` **Note**: `$[0].$` could be used when an associated secret is used. In this case, `$[0].$USER` means the username of the associated secret. `$[0].$PASSWORD` means the password of the associated secret.  Enter `$` to get the list of valid variables. **Note**: The option is only available when the *Type* is *Execute*.
Response	The prompted line in target server.  Enter `$` to get the list of valid variables. **Note**: The option is only available when the *Type* is *Expect*.
Execute Action	Either select *Execute command unconditionally* or *Execute command on previous match*. **Note**: The option is only available when the *Type* is *Execute*.
Expect Action	From the dropdown, select from the following three options: • *Abort procedure on string not matched* • *Continue procedure on string not matched* • *Abort procedure on string matched* **Note**: The option is only available when the *Type* is *Expect* or *Expect Prompt*.
Critical	Enable to indicate that the step is critical.

	Password changing is successful when all steps before the critical step are passed. Steps after the critical step are optional, password changer ignores the optional steps if they fail.
Delay (ms)	The maximum waiting time for the current action, in ms (default = 50, 50 - 20000).
Description	Optionally, enter a description.

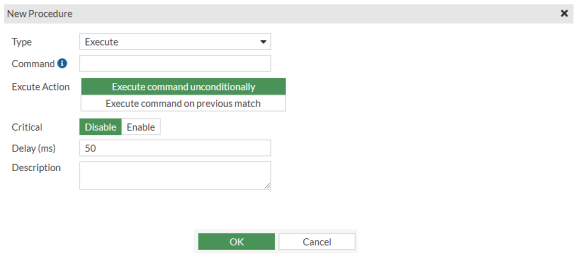
To reorder the changer sequence, drag from the sequence number and then drop.

3. Click *OK*.

From the list, select a changer and then select *Edit* to edit the changer.
From the list, select changer and then select *Delete* to delete the changer.

Verifiers

1. In step 4 when Creating a password changer, select *Create* in *Verifiers*.
The *New Procedure* window opens.



2. Enter the following information:

Type	From the dropdown, select from the following options: • *Execute* • *Expect* • *Expect Prompt*
Command	Commands to execute on the password changer. Valid variables are: • `$USER` • `$PASSWORD` • `$PASSPHRASE` • `$NEWPASSWD` • `$NEW_PUB_KEY`

	• $NEW_PRI_KEY • $[0].$ • $PUB_KEY **Note**: $[0].$ could be used when an associated secret is used. In this case, $[0].$USER means the username of the associated secret. $[0].$PASSWORD means the password of the associated secret.  Enter $ to get the list of valid variables. **Note**: The option is only available when the *Type* is *Execute*.
Response	The prompted line in target server.  Enter $ to get the list of valid variables. **Note**: The option is only available when the *Type* is *Expect*.
Execute Action	Either select *Execute command unconditionally* or *Execute command on previous match*. **Note**: The option is only available when the *Type* is *Execute*.
Expect Action	From the dropdown, select from the following three options: • *Abort procedure on string not matched* • *Continue procedure on string not matched* • *Abort procedure on string matched* **Note**: The option is only available when the *Type* is *Expect* or *Expect Prompt*.
Critical	Enable to indicate that the step is critical.  Password verification is successful when all steps before the critical step are passed. Steps after the critical step are optional, password verifier ignores the optional steps if they fail.
Delay	The maximum waiting time for the current action, in ms (default = 50, 50 - 20000).
Description	Optionally, enter a description.

 To reorder the verifier sequence, drag from the sequence number and then drop.

3. Click *OK*.

From the list, select a verifier and then select *Edit* to edit the verifier.
From the list, select verifier and then select *Delete* to delete the verifier.

See Automatic password changing on page 131 and Automatic password verification on page 132.

Automatic password changing

A password changer linked to a secret template can be activated to periodically change the password in a secret that uses this secret template.

To automatically change the password:

1. Go to *Secrets* > *Secret List*.
   Alternatively, go to *Secrets* > *Personal Folder/Public Folder*, and select the folder where the secret is located.
2. Double-click the secret to edit it.
3. In the *Secret Setting* pane:
   a. Enable *Automatic Password Changing*.
   b. In *Start Time*, enter the date and time when the recurring schedule begins. Alternatively, select the *Calendar* icon and then select a date and time.
   c. In *Recurrence*, select from the following three frequencies of recurrence:
      i. *Daily*
      ii. *Weekly*
      iii. *Monthly*
   d. In *Repeat every*, enter the number of days/weeks/months after which the password is changed.
   e. In *Occurs on*, select from the following days of the month when the password is automatically changed:
      i. *First*
      ii. *Second*
      iii. *Third*
      iv. *Last*
      v. *Last Day*
      vi. *Day*
      When you select *Day*, select + to add days of the month when the password is automatically changed.
      Select days of the week when the password is automatically changed.
      Note: The *Occurs on* option is only available when *Recurrence* is set as *Weekly* or *Monthly*.
      The automatic password changing schedule is displayed in *Recursive*.
4. Click *Save*.

If *Automatic Password Changing* is enabled then the *Password Changer Status* shows the amount of time after which the password is automatically changed.

Automatic password verification

A password changer linked to a secret template can be activated to periodically verify the password, and check if the target server is still available for a secret that uses this secret template.

To automatically verify the password:

1. Go to *Secrets* > *Secret List*.
   Alternatively, go to *Secrets* > *Personal Folder/Public Folder*, and select the folder where the secret is located.
2. Double-click the secret to edit it.
3. In the *Secret Setting* pane:
   a. Enable *Automatic Password Verification*.
   b. In *Interval (min)*, enter the time interval at which the password is verified.
   c. In *Start Time*, enter a date and time.
   Alternatively, select the calendar icon, and select a date and time.
4. Click *Save*.

If *Automatic Password Verification* is enabled then the *Password Verification Status* shows the amount of time after which the password is automatically verified.

Password policies

Using a secure password is vital to prevent unauthorized access. FortiPAM allows you to create password policy for secret passwords generated by the password changer. See Password changers on page 124.

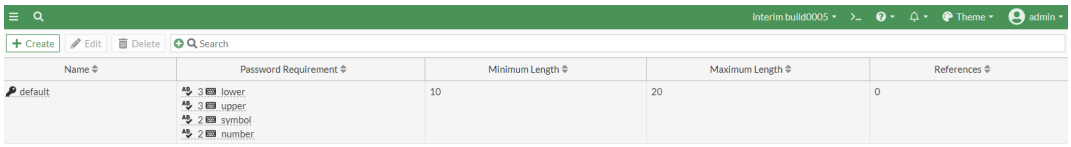
With password policies, you can enforce specific criteria for a new password, including:

- Minimum length between 8 and 64 characters.
- Maximum length up to 64 characters.
- The password must contain uppercase (A, B, C) and/or lowercase (a, b, c) characters.
- The password must contain numbers (1, 2, 3).
- The password must contain special or non-alphanumeric characters `(!, @, #, $, %, ^, &, *, (, and )).`

Password policies can only be applied to a secret template when *Password Changer* is enabled for the template.

Password policies are not applicable to SSH keys (Password changer *Type* is *SSH with Public Key*).

For each password policy; name, password requirement, minimum length, maximum length, and references are displayed.



The default password policy has the following features:

- *Minimum length*: 10
- *Maximum length*: 20
- *Password Requirements*: 3, 3, 2, and 2 minimum number of characters from the *lower*, *upper*, *symbol*, and *number* character sets respectively. See Character sets on page 135.

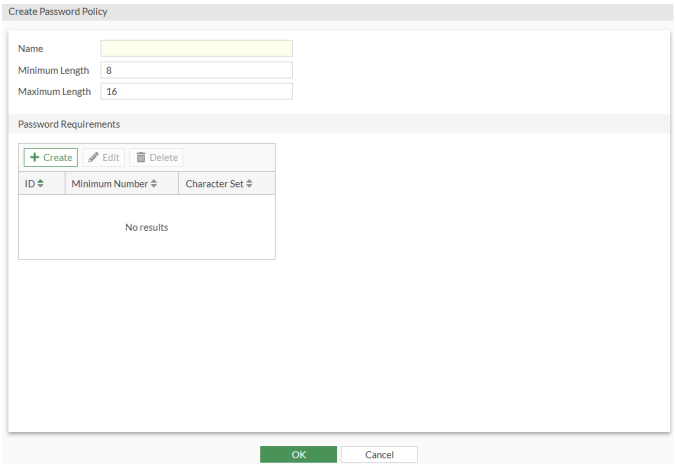
The *Password Policies* tab contains the following options:

Create	Select to create a new password policy. Password policies on page 132.
Edit	Select to edit the selected password policy.
Delete	Select to delete the selected password policies.
Search	Enter a search term in the search field, then hit `Enter` to search the password policies list. To narrow down your search, see Column filter.

Creating a password policy

To create a password policy:

1. Go to *Secret Settings* > *Password Policies*
2. Select *Create* to create a new password policy.
   The *Create Password Policy* window opens.



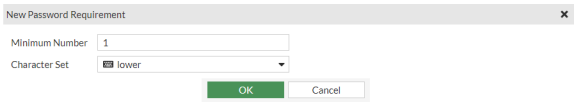
3. Enter the following information:

Name	The name of the password policy.
Minimum Length	The minimum length of the password (default = 8).
Maximum Length	The maximum length of the password (default = 16).
Password Requirements	The requirements for the password to be successfully created. See Password Requirements.

4. Click *OK*.

Password Requirements

1. In step 2 when Creating a password policy, select *Create* in *Password Requirements*.
The *New Password Requirement* window opens.



2. Enter the following information:

Minimum Number	The minimum number of characters from the *Character Set* (default = 1).
Character Set	From the dropdown, select a character set or create a new character set (default = lower). See Creating a character set on page 135.

Use the search bar to look up a character set.

Use the pen icon next to the character set to edit it.

3. Click *OK*.

From the list, select a requirement and then select *Edit* to edit the requirement.
From the list, select requirements and then select *Delete* to delete the requirements.

See Applying a password policy to a secret template on page 134.

Applying a password policy to a secret template

To apply a password policy to a secret template:

1. Go to *Secret Settings* > *Templates*.
2. From the list, double-click a secret template to edit the template.
Alternatively, select a template and then select *Edit* to edit the template.

The *Edit Secret Template* window opens.

Default templates cannot be modified.
Administrators can clone a default template and then select a password policy.

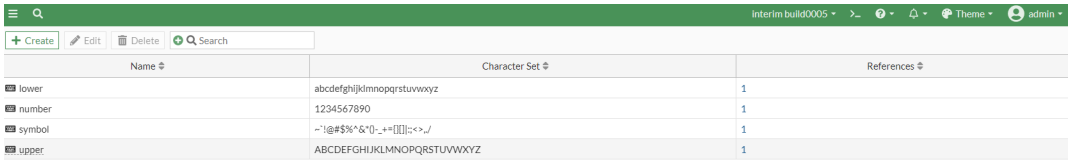
3. In the *Password Changer* pane, from the *Password Policy* dropdown, select a password policy or create a new password policy. See Creating a password policy on page 133 and Creating secret templates on page 95.
4. Click *Save*.

Character sets

A character set is a group of varied characters used in password policies. Character sets provide building blocks for passwords. See Password policies on page 132.

Character Sets in *Secret Settings* displays a list of configured character sets.

For each character set; name, character set, and references are displayed.



The following default character sets are available in FortiPAM:

- *symbol*: contains some special characters.
- *number*: contains all numbers.
- *lower*: contains all lowercase English letters.
- *upper*: contains all uppercase English letters.

The *Character Sets* tab contains the following options:

Create	Select to create a new character set. See Creating a character set on page 135.
Edit	Select to edit the selected character set.
Delete	Select to delete the selected character sets.
Search	Enter a search term in the search field, then hit `Enter` to search the character sets list. To narrow down your search, see Column filter.

Creating a character set

To create a character set:

1. Go to *Secret Settings* > *Character Sets*.
2. Select *Create* to create a new character set.
   The *New Character Set* window opens.

3. Enter the following information:

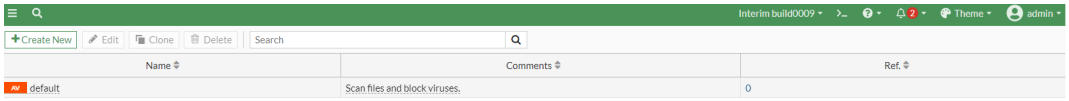
Name	The name of the character set.
Character Set	The character set.

4. Click *OK*.

AntiVirus

FortiPAM offers the unique ability to prevent, detect, and remove malware when you transfer files between local PCs and privileged servers. FortiPAM will detect the potential malware uploaded to or downloaded from the related secret server if a secret is configured with an antivirus profile. Examples of file launchers include WinSCP, Web SMB, and Web SFTP.

For each antivirus profile; name, comments, and references are displayed.



A *default* antivirus profile is available that blocks malware transmission.

Once configured, you can add the antivirus profile to a secret. See Enabling antivirus scan in a secret on page 138.

You can also customize these profiles or create your profile to inspect specific protocols, remove viruses, analyze suspicious files with FortiSandbox, and apply botnet protection to network traffic. Note that for *Web SMB* and *Web SFTP* launchers, you must inspect the HTTP protocol in the AV profile. While for *WinSCP* launcher, SSH protocol needs to be inspected.

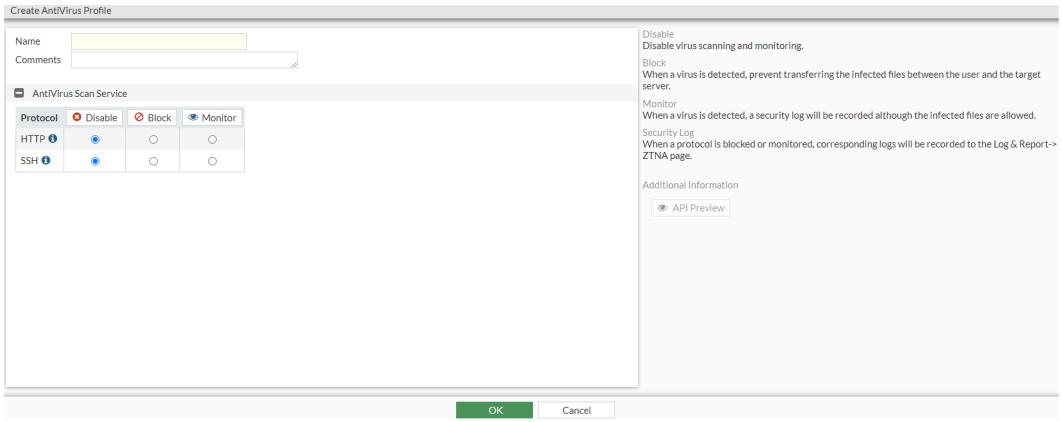
The *AntiVirus* tab contains the following options:

Create New	Select to create a new antivirus profile. See Creating an antivirus profile on page 137.
Edit	Select to edit the selected antivirus profile.
Clone	Select to clone the selected antivirus profile.
Delete	Select to delete the selected antivirus profiles.
Search	Enter a search term in the search field, then hit `Enter` to search the antivirus profile list.

Creating an antivirus profile

To create an antivirus profile:

1. Go to *Secret Settings* > *AntiVirus* and select *Create New* to create a new antivirus profile.
   The *Create AntiVirus Profile* window opens.



2. Enter the following information:

Name	The name of the antivirus profile.
Comments	Optionally, enter comments about the antivirus profile.

AntiVirus Scan Service

For *HTTP* and *SSH* protocols, set the antivirus service as disable, block, or monitor (default = *Disable*):

- *Disable*: Disable antivirus scanning and monitoring.
- *Block*: When a virus is detected, prevent the infected files from uploading to or downloading from the target server. A security log is recorded and available in *Log & Report* > *ZTNA*.
- *Monitor*: When a virus is detected, allow the infected files. A security log is recorded and available *Log & Report* > *ZTNA*.

Notes:

- HTTP protocol applies to *Web SFTP* and *Web SMB* launchers.
- SCP protocol applies to the *WinSCP* launcher.

3. Click *OK*.

AV protection via the CLI - Example

1. In the CLI console, enter the following commands:

```
config antivirus profile
   edit <profile-name>
      config http
         set av-scan block
      end
      config ssh
         set av-scan block
      end
   next
end
```

Enabling antivirus scan in a secret

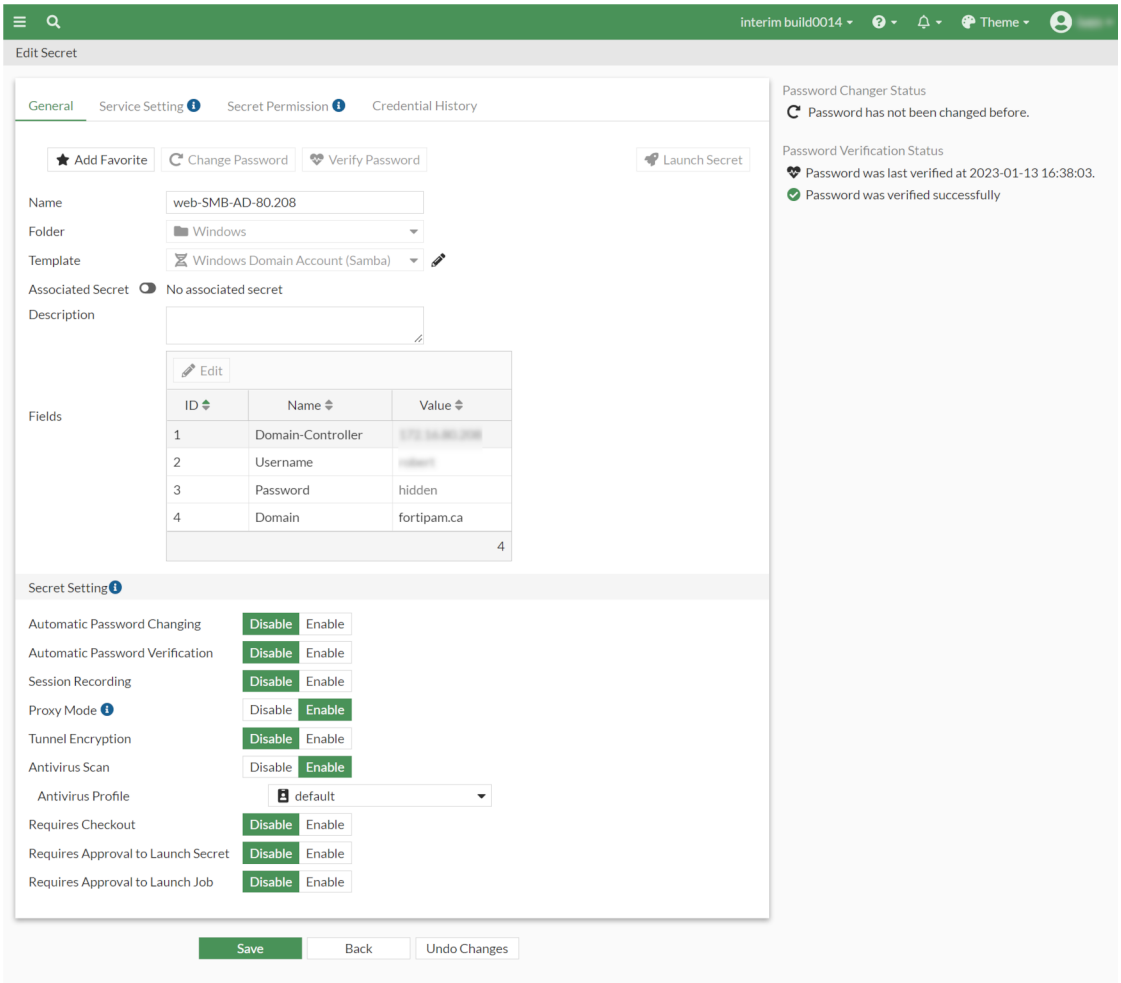
To enable antivirus scan in a secret:

1. Go to *Secrets* > *Secret List*.
2. In the *Secrets List*, double-click a secret to open.
   Alternatively, in *Secrets* > *Personal Folder/Public Folder*, go to the folder where the secret is located, and double-click the secret to open.

If the secret does not show up, it may be because you do not have the necessary permission to access the secret or the folder where the secret is located.

---

3. In the *Secret Setting* pane, enable *Antivirus Scan*.
4. From the *Antivirus Profile* dropdown, select an antivirus profile. See Creating an antivirus profile on page 137.
5. Click *Save*.



Data loss prevention (DLP) protection for secrets

DLP is available for secret launching only when you have a valid Advanced Malware Protection (`AVDB & DLP`) license.

DLP, or Data Loss Prevention, is a cybersecurity solution that detects and prevents data breaches. Since it blocks the extraction of sensitive data, users can use it for internal security and regulatory compliance.

The filters in a DLP sensor can examine traffic for the following:

- Known files using DLP fingerprinting
- Known files using DLP watermarking
- Particular file types
- Particular file names
- Files larger than a specified size
- Data matching a specified regular expression

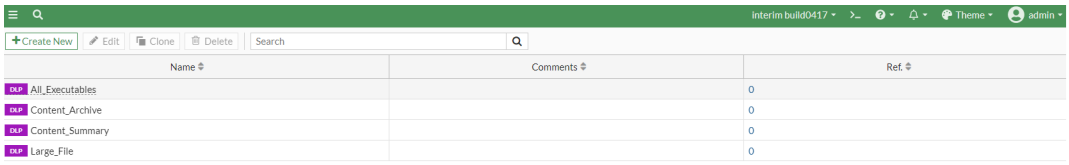
DLP is primarily used to stop sensitive data from leaving your network. DLP can also prevent unwanted data from entering your network and archive some or all of the content that passes through the FortiPAM. DLP archiving is configured per filter, which allows a single sensor to archive only the required data. You can configure the DLP archiving protocol on the GUI and via the CLI.

The following basic filter types can be configured on the GUI and via the CLI:

- **File type and name**: A file type filter allows you to block, allow, log, or quarantine based on the file type specified in the file filter list. See Supported file types on page 144.
- **File size**: A file size filter checks for files that exceed the specific size and performs the DLP sensor's configured action on them.
- **Regular expression**: A regular expression filter filters files or messages based on the configured regular expression pattern.

Data Leak Prevention in *Secret Settings* displays a list of configured DLP sensors.

For each DLP sensor; name, comments, and reference are shown.



FortiPAM offers the following preconfigured DLP sensors:

- `All_Executables`: Includes a DLP filter rule that filters all the available protocols by their file types.
- `Content_Archive`
- `Content_Summary`
- `Large_Files`: Includes a DLP filter rule that filters all the available protocols by their file sizes.

You cannot delete the default DLP sensors.

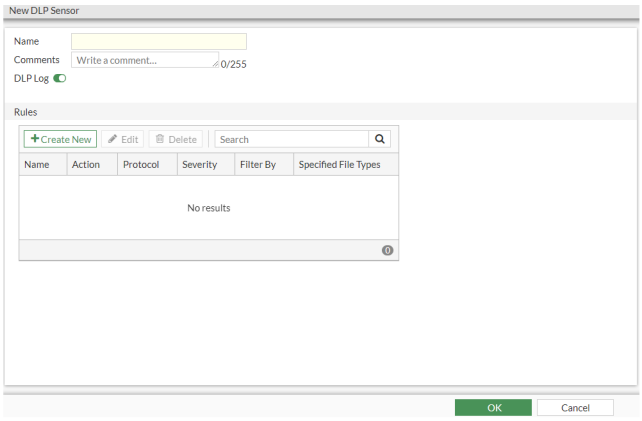
The *Data Leak Prevention* tab contains the following options:

Create New	Select to create a new DLP sensor. See Creating a DLP sensor on page 140.
Edit	Select to edit the selected DLP sensor.
Clone	Select to clone the selected DLP sensor.
Delete	Select to delete the selected DLP sensors.
Search	Search the DLP sensors list.

Creating a DLP sensor

To create a DLP sensor:

1. Go to *Secret Settings* > *Data Leak Prevention*.
2. From the DLP sensors list, select *Create New*.
   The *New DLP Sensor* window opens.



3. Enter the following information:

Name	Name of the DLP sensor.
Comments	Optionally, enter a description for the DLP sensor.
DLP Log	Enable to generate a log entry when data matches the configured patterns. The option is enabled by default.
Rules	Create or edit DLP filter rules. See Creating DLP filter rules on page 141.

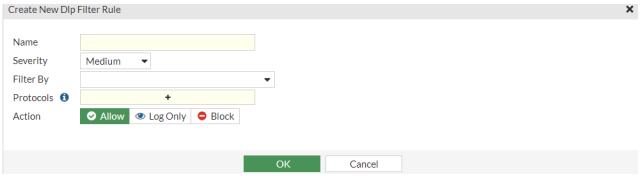
4. Click *OK*.

Creating DLP filter rules

Use the search bar to look up a DLP filter rule.

To create a DLP filet rule:

1. In step 2 when Creating a DLP sensor on page 140, select *Create New* in *Rules*.
   The *Create New Dlp Filter Rule* window opens.



2. Enter the following information:

Name	Name of the DLP filter rule.
Severity	Select a severity for the DLP filter rule: *Information*, *Low*, *Medium*, *High*, or *Critical*.
Filter By	Select the filter from the dropdown list: • *credit-credit (Match Credit Card Numbers)* • *ssn (Match Social Security Numbers)* • *regexp (Match a Regular Expression)* • *file-type (Match a DLP File Pattern)* • *file-size (Match Any File Over Size)* • *file-type-and-size (Match DLP File Pattern and File Size Over)* • *encrypted (Look for Encrypted files)* • *watermark (Look for Defined File Watermarks)* • *fingerprint (Match against fingerprint sensitivity)*
Regular Expression	Enter the pattern that network traffic is examined for. **Note**: The option is only available when *Match a Regular Expression* is set as the filter.
File Size	Enter the maximum file size in kilobytes (default = 10, 0 - 4294967295). **Note**: The option is only available when *Match Any File Over Size* or *Match DLP File Pattern and File Size Over* is set as the filter.
Company Identifier	Enter the company identifier. The company identifier is to make sure that you are only blocking watermarks that your company has placed on the files, not watermarks with the same name by other companies. **Note**: The option is only available when *Look for Defined File Watermarks* is set as the filter.
File Pattern	Select or create a DLP file pattern.  Use the pen icon next to the file pattern to edit it. **Note**: The option is only available when *Match a DLP File Pattern* or *Match DLP File Pattern and File Size Over* is set as the filter.
Protocols	Select one or more protocols that the filter will examine. This allows resources to be optimized by only examining relevant traffic. The available protocols are *HTTP-GET*, *HTTP-POST*, and *SSH*.  Filtering MAPI and SSH protocols only works in the proxy mo de.

	Use the search bar to look up a protocol.
Sensitivity	Select a sensitivity for the DLP filter rule: *Critical*, *Private*, and *Warning*. **Note**: The option is only available when *Look for Defined File Watermarks* or *Match against fingerprint sensitivity* is selected as the filter.
Action	Select an action to take if the filter is triggered. Available actions are *Allow*, *Log Only*, and *Block*.

3. Click *OK*.

From the list, select a rule and then select *Edit* to edit the rule.
From the list, select rules and then select *Delete* to delete the rules.

DLP via the CLI - Example

To configure a file type and name filter:

1. In the CLI console, enter the following commands to create a file pattern to filter files based on the file name pattern or file type. In this example, we intend to filter for GIFs and PDFs:

```
config dlp filepattern
   edit 11
      set name "sample_config"
      config entries
         edit "*.gif"
            set filter-type pattern
         next
         edit "pdf"
            set filter-type type
            set file-type pdf
         next
      end
   next
end
```

2. Create the DLP sensor (**Note**: `http-get` and `http-post` protocols apply to *Web SFTP* and *Web SMB* launchers):

```
config dlp sensor
   edit <name>
      config filter
         edit <id>
            set name <string>
            set proto {http-get http-post ssh}
            set filter-by file-type
            set file-type 11
            set action {allow | log-only | block | quarantine-ip}
         next
      end
   next
end
```

To configure a file size filtering:

1. In the CLI console, use the following commands:

```
config dlp sensor
   edit <name>
      config filter
         edit <id>
            set name <string>
            set proto {http-get http-post ssh}
            set filter-by file-size
            set file-type 11
            set action {allow | log-only | block | quarantine-ip}
         next
      end
   next
end
```

To configure regular expression filtering:

1. In the CLI console, use the following commands:

```
config dlp sensor
   edit <name>
      config filter
         edit <id>
            set name <string>
            set type {file | message}
            set proto {http-get http-post ssh}
            set filter-by regexp
            set regexp <string>
            set action {allow | log-only | block | quarantine-ip}
         next
      end
   next
end
```

Supported file types

The following file types are supported in DLP profiles:

Type	Description
.net	Match .NET files
7z	Match 7-Zip files
activemime	Match ActiveMime files
arj	Match ARJ compressed files
aspack	Match ASPack files
avi	Match AVI files
base64	Match Base64 files

Type	Description
bat	Match Windows batch files
binhex	Match BinHex files
bmp	Match BMP files
bzip	Match Bzip files
bzip2	Match Bzip2 files
cab	Match Windows CAB files
chm	Match Windows compiled HTML help files
class	Match CLASS files
cod	Match COD files
crx	Match Chrome extension files
dmg	Match Apple disk image files
elf	Match ELF files
exe	Match Windows executable files
flac	Match FLAC files
fsg	Match FSG files
gif	Match GIF files
gzip	Match Gzip files
hlp	Match Windows help files
hta	Match HTA files
html	Match HTML files
iso	Match ISO archive files
jad	Match JAD files
javascript	Match JavaScript files
jpeg	Match JPEG files
lzh	Match LZH compressed files
mach-o	Match Mach object files
mime	Match MIME files
mov	Match MOV files
mp3	Match MP3 files
mpeg	Match MPEG files

Type	Description
msi	Match Windows Installer MSI Bzip files
msoffice	Match MS-Office files. For example, DOC, XLS, PPT, and so on.
msofficex	Match MS-Office XML files. For example, DOCX, XLSX, PPTX, and so on.
pdf	Match PDF files
petite	Match Petite files
png	Match PNG files
rar	Match RAR archives
rm	Match RM files
sis	Match SIS files
tar	Match TAR files
tiff	Match TIFF files
torrent	Match torrent files
unknown*	Match unknown files
upx	Match UPX files
uue	Match UUE files
wav	Match WAV files
wma	Match WMA files
xar	Match XAR archive files
xz	Match XZ files
zip	Match ZIP files

*This file type is only available in DLP profiles.

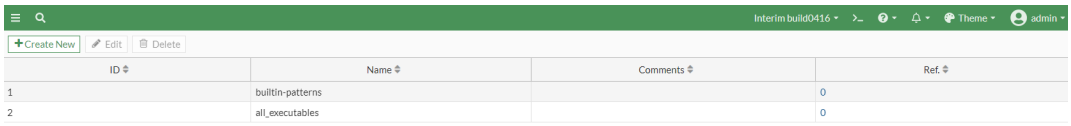
DLP file pattern

DLP file patterns match selected file types and file patterns. They are used as DLP filter rules in DLP sensors.

DLP File Pattern in *Secret Settings* displays a list of configured DLP file patterns.

For each DLP file pattern; ID, name, comments, and reference are shown.

The *Ref.* column displays the number of times the object is referenced to other objects. To view the location of the referenced object, select the number in *Ref.*; the *Object Usage* window opens and displays the various locations of the referenced object.



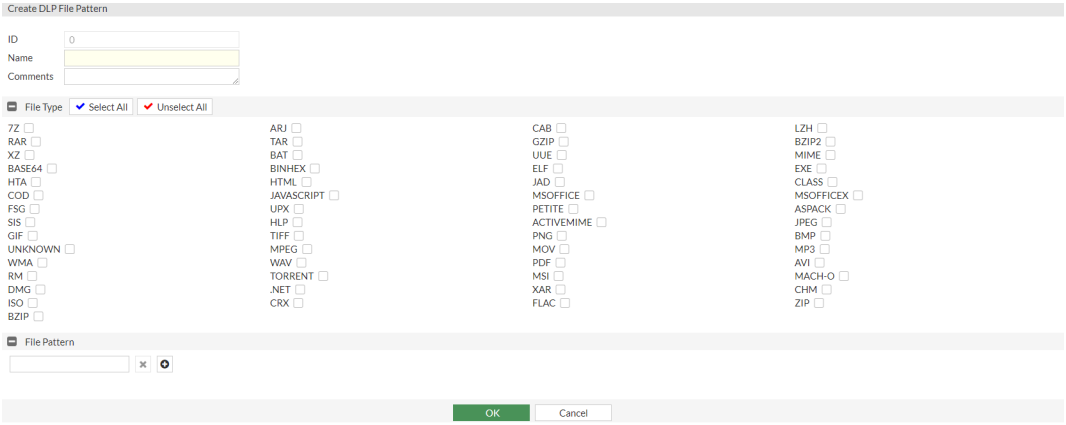
The *DLP File Pattern* tab contains the following options:

Create New	Create a DLP file pattern. See Creating a DLP file pattern on page 147.
Edit	Select to edit the selected DLP file pattern.
Delete	Select to delete the selected DLP file patterns.

Creating a DLP file pattern

To create a DLP file pattern:

1. Go to *Secret Settings* > *DLP File Pattern*.
2. From the DLP file pattern list, select *Create New*.
   The *Create DLP File Pattern* window opens.



3. Enter the following information:

ID	Identifier for the DLP file pattern.
Name	The name of the DLP file pattern.
Comments	Optionally, enter a description for the DLP file pattern.
File Type	Select one or more file types. To select all the file types, click *Select All*. To unselect all the file types, click *Unselect All*.
File Pattern	Enter one or more file patterns.

4. Click *OK*.

SSH filter profiles

SSH Filter Profiles tab in *Secret Settings* displays a list of SSH filter profiles.

A filter can be created to prevent certain commands from running on an SSH terminal.

For each SSH profile; name, block, log, default command log, extra shell commands, and reference are displayed.

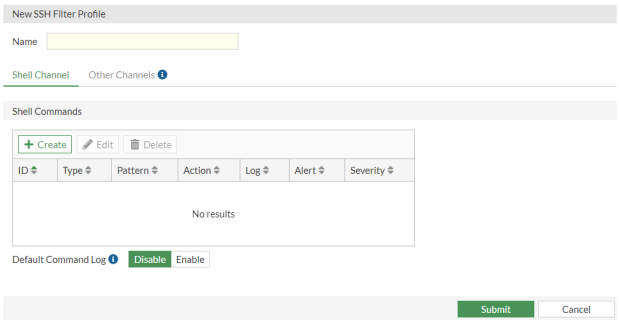
The *SSH Filter Profiles* tab contains the following options:

Create	Select to create a new SSH filter profile. See Creating an SSH filter on page 148.
Edit	Select to edit the selected SSH filter profile.
Delete	Select to delete the selected SSH filter profiles.
Search	Enter a search term in the search field, then hit `Enter` to search the SSH filter profiles list. To narrow down your search, see Column filter.

Creating an SSH filter

To create an SSH filter profile:

1. Go to *Secret Settings* > *SSH Filter Profiles*.
2. In *SSH Filter Profiles*, select *Create*.
   The *New SSH Filter Profile* window opens.



3. Enter the following information:

Name	Name of the SSH filter.

Shell Commands

Shell commands can be created to block a command in the SSH terminal.

See Creating Shell Commands.

	Select a shell command from the list and then select *Edit* to edit the command. When editing a shell command the options are same as when creating one.
	Select shell commands from the list then select *Delete* to delete the commands.

Default Command Log	Enable/disable logging unmatched shell commands. **Note**: The option is disabled by default

Other Channels

Use this tab for advanced settings.

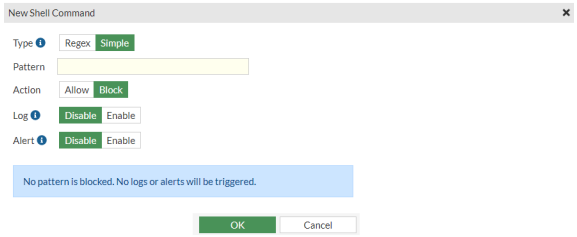
Note: Settings in the tab require setting up a custom launcher.

Block Channel	Select from the SSH blocking options (multiple options may be selected): • *X11*: X server forwarding • *SSH execution* • *Port forwarding* • *Tunnel forwarding* • *SFTP* • *SCP* • *Unknown channel*: Unknown channel (any channel other than the six listed here and the shell channel.)
Log Activity	SSH logging options. These are log activities related to selected channels regardless of the blocking status (multiple options may be selected): • *X11*: X server forwarding • *SSH execution* • *Port forwarding* • *Tunnel forwarding* • *SFTP* • *SCP* • *Unknown channel*

4. Click *Submit*.

To create a shell command:

1. In the *New SSH Filter Profile* window, select *Create* in the *Shell Commands* pane.



2. In the *New Shell Command* window, enter the following information:

Type	Select the matching type: • *Regex*: Match command line using regular expression. Choosing the option blocks any command matching *Regex* in *Pattern*. • *Simple*: Match single command (default). Choosing the option matches any command fitting the one in *Pattern*.
Pattern	SSH shell command pattern. For example: • When the *Type* is *Regex*, pattern `.*` stands for all the commands and pattern `sh.*` stands for all the commands beginning with `sh` including show and shutdown. • When the *Type* is *Simple*, pattern `rm` stands for the rm command on Linux, e.g., `'rm -rf /*','rm test.py'`.
Action	Action to take for URL filter matches: • *Allow*: Allow the SSH shell command on the target server. • *Block*: Block the SSH shell command on the target server (default). For example when the *Type* is *Regex*, the *Pattern* is `conf.*`, and the *Action* is *Block*. This blocks all the configuration actions on the target server.
Log	Enable/disable logging. When enabled, the action logs are available in *Log & Report* > *SSH*.
Alert	Enable/disable alert. When enabled, the alert message is sent based on the configurations in *Log & Report* > *Email Alert Settings*.
Severity	The severity of the actions reported in *Log & Report* > *SSH* and alert messages: • *Critical* • *High* • *Medium* • *Low* (default) **Note**: The option is only available when *Log* is enabled.

3. Click *OK*.

Adding SSH filter to secret

To add SSH filter to a secret:

1. Go to *Secrets* > *Secret List*.
2. In the *Secrets List*, double-click a secret to open.
   Alternatively, in *Secrets* > *Personal Folder/Private Folder*, go to the folder where the secret is located, and double-click the secret to open.

If the secret does not show up, it may be because you do not have the necessary permission to access the secret or the folder where the secret is located.

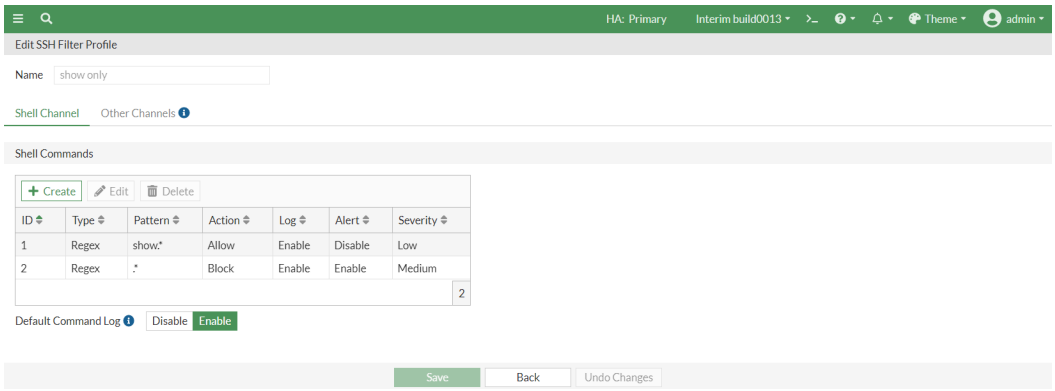
3. In *Service Setting* tab, ensure that *SSH Service* is enabled.
4. Enable *SSH Filter* and then select an SSH filter profile from the *SSH Filter Profile* dropdown.
5. Click *Save*.

Example SSH filter profiles - example

To configure an SSH filter profile that only allows `show` command on the target server (FortiGate or Cisco routers):

1. Go to *Secret Settings* > *SSH Filter Profiles*.
2. In *SSH Filter Profiles*, select *Create*.
   The *New SSH Filter Profile* window opens.
3. Enter a name for the SSH filter profile. In this example, the SSH filter profile is named `show only`.
4. In *Shell Commands*, select *Create*:
   a. In *Type*, select *Regex*.
   b. In *Pattern*, enter `show.*`.
   c. In *Action*, select *Allow*.
   d. In *Log*, select *Enable*.
   e. In *Alert*, select *Disable*.
   f. In *Severity*, select *Low*.
   g. Click *OK*.
5. In *Shell Commands*, select *Create* again:
   a. In *Type*, select *Regex*.
   b. In *Pattern*, enter `.*`.
   c. In *Action*, select *Block*.
   d. In *Log*, select *Enable*.
   e. In *Alert*, select *Enable*.
   f. In *Severity*, select *Medium*.
   g. Click *OK*.
6. Enable *Default Command Log*.

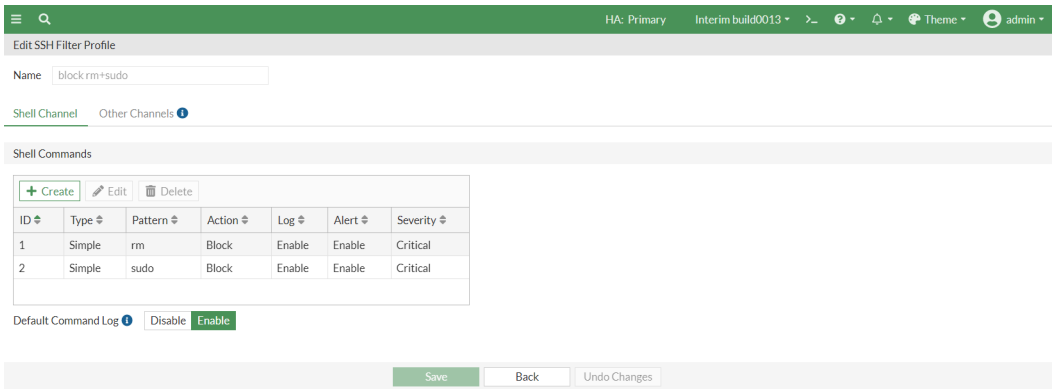
7. Click *Submit*.



To configure an SSH filter profile that blocks `rm` and `sudo` commands on the target Linux server:

1. Go to *Secret Settings* > *SSH Filter Profiles*.
2. In *SSH Filter Profiles*, select *Create*.
   The *New SSH Filter Profile* window opens.
3. Enter a name for the SSH filter profile. In this example, the SSH filter profile is named `block rm+sudo`.
4. In *Shell Commands*, select *Create*:
   a. In *Type*, select *Simple*.
   b. In *Pattern*, enter `rm`.
   c. In *Action*, select *Block*.
   d. In *Log*, select *Enable*.
   e. In *Alert*, select *Enable*.
   f. In *Severity*, select *Critical*.
   g. Click *OK*.
5. In *Shell Commands*, select *Create* again:
   a. In *Type*, select *Simple*.
   b. In *Pattern*, enter `sudo`.
   c. In *Action*, select *Block*.
   d. In *Log*, select *Enable*.
   e. In *Alert*, select *Enable*.
   f. In *Severity*, select *Critical*.
   g. Click *OK*.
6. Enable *Default Command Log*.

7. Click *Submit*.



Integrity check

For every launcher, you can configure a client software entry in the *Integrity Check* tab in *Secret Settings* to enable integrity checks.

Client software integrity check requires FortiPAM 1.1 and FortiClient 7.2.2.

When the integrity check fails, the launching stops and a prompt appears showing where to download a version of the client software based on your FortiPAM configurations.

Using integrity check prevents launching of corrupt executables.

The following two types of integrity checks are available:

- *Executable hash*: Comparing the executable hash with the provided value.
- *Certificate*: Checking the certificate of a file.

An integrity check is considered passed when at least one version of the client software package is matched.

For each integrity check; name, number of pages, and references are displayed.

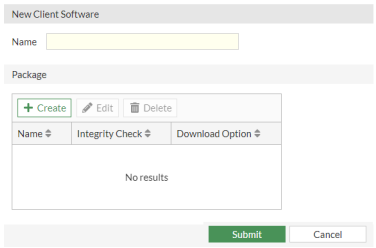
The *Integrity Check* tab contains the following options:

Create	Select to create a client software entry for integrity check. See Creating a client software entry for integrity check on page 154.
Edit	Select to edit the selected client software entry.
Delete	Select to delete the selected client software entries.
Search	Enter a search term in the search field, then hit `Enter` to search the client software entry list. To narrow down your search, see Column filter.

Creating a client software entry for integrity check

To create a client software entry for integrity check:

1. Go to *Secret Settings* > *Integrity Check* and select *Create*.
   The *New Client Software* window opens.



2. Enter the following information:

Name	The name of the client software entry.

Package

Configure client software packages. See Creating client software packages on page 154.

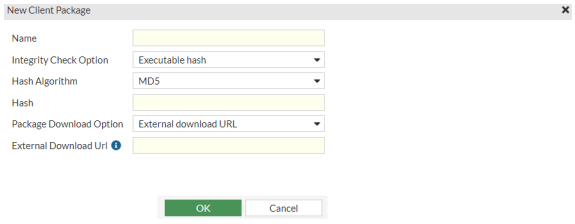
While creating a client software entry for integrity check, you can either store the software package locally, i.e., on the FortiPAM disk or provide an external URL to the package for downloading.

3. Click *Submit*.

Creating client software packages

To create a client software package

1. In Step 1, when Creating a client software entry, select *Create* in the *Package* pane.
   The *New Client Package* window opens.



2. Enter the following information:

Name	The name of the client software package.
Integrity Check Option	Select from the following integrity check options: • *Executable hash*: Comparing the executable hash with the provided value (default). • *Certificate*: Checking the certificate of a file.
Hash Algorithm	Select from the following hash algorithms: • *MD5* (default) • *SHA-1* • *SHA-256* **Note**: The option is only available when the *Integrity Check Option* is *Executable hash*.
Hash	The package/folder hexadecimal hash value. **Note**: The option is only available when the *Integrity Check Option* is *Executable hash*.
CA Certificate	From the dropdown, select a CA certificate.  Use the search bar to look up a CA certificate. **Note**: The option is only available when *Integrity Check Option* is *Certificate*.
Package Download Option	Select from the following two options: • *Internal download URL* • *External download URL* (default)
External Download Url	The external download URL for the client software package.  Only installers are supported. **Note**: The option is only available when the *Package Download Option* is *External download URL*.
Package	Select + *Upload File*, locate the client software package from your management computer, and click *Open*. **Note**: The option is only available when the *Package Download Option* is *Internal download URL*.

3. Click *OK*.

 From the list, select a client software package and then select *Edit* to edit the packages.
From the list, select client software packages and then select *Delete* to delete the packages.

Creating a client software entry for integrity check via the CLI - Example

1. In the CLI console, enter the following commands to configure the client software table. In the example, for the PuTTY launcher, we have two client software packages. `x64` checks the file certificate and downloads the package from an external link. `x86` checks against the MD5 checksum and stores the package locally.

```
config secret client-software
   edit "putty"
      config pkg
         edit "x64"
            set integrity-check cert
            set download-option external
            set external-url
                 "https://the.earth.li/~sgtatham/putty/latest/w64/putty.exe"
            set ca "Fortinet_SSL"
            set client-name "putty"
         next
         edit "x86"
            set hash-algo MD5
            set hash "aeb47b393079d8c92169f1ef88dd5696"
            set package-name "putty.exe"
            set client-name "putty"
         next
      end
   next
end
```

2. Enter the following commands to go to the secret launcher table and bind the client software entry with the launcher.

```
config secret launcher
   edit "PuTTY"
      set type ssh
      set client-software "putty"
   next
end
```

3. Enter the following commands to enable the integrity check option in the launcher settings of the template.

```
config secret template
   edit "Unix Account (SSH Password)"
      config launcher
         edit 2
            set launcher-name "PuTTY"
            set port 22
            set integrity-check enable
         next
      end
   next
end
```

With the configurations set as above, the secret with *Unix Account (SSH Password)* template and *PuTTY* as the launcher includes an integrity check each time it is launched.

User management

In *User Management*, you can access the following tabs:

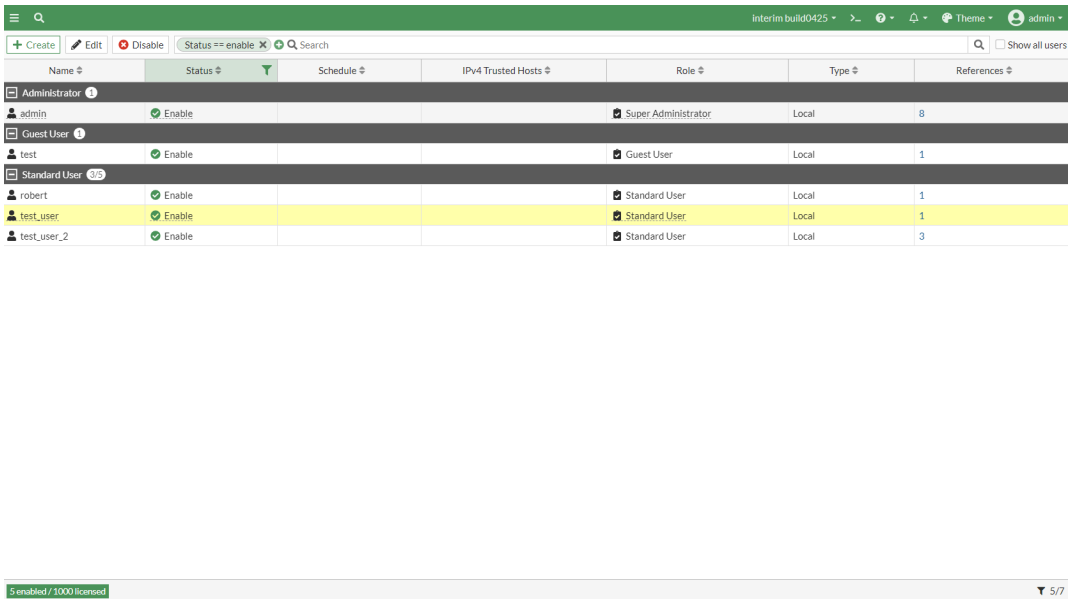
User definition

User Definition in *User Management* displays a list of FortiPAM users listed by their role types.

For each user; name, status, schedule, IPv4 trusted hosts, role, type, and references are shown.

By default, FortiPAM only lists enabled users.

Enable *Show all users* to list all the users.



The user definitions list contains the following options:

Create	Select to create a new user. See Creating a user on page 159.
Edit	Select to edit the selected user account.
Disable	Select to disable the selected user account or accounts.
Search	Enter a search term in the search field, then hit `Enter` to search the user definition list. To narrow down your search, see Column filter.
Show all users	Enable to list all the users, including disabled users.

On the bottom-left, the number of enabled users and the total number of allowed users are displayed as a label. This label is green when seats are available. The label turns red when all the seats have been used up. Once the seats are used up, new users cannot be enabled without disabling enabled users.

To enable/disable a user:

1. Right-click a user from the user definition list and then select *Enable/Disable* from *Set status*.
2. To refresh the user definition list, select *Reload Now* from the message that appears on the bottom-right.

To delete a user:

1. Right-click a user from the user definition list and then select *Delete*.

Before deleting a user, you must remove all the associated items in the *References* column. Otherwise, deletion fails.

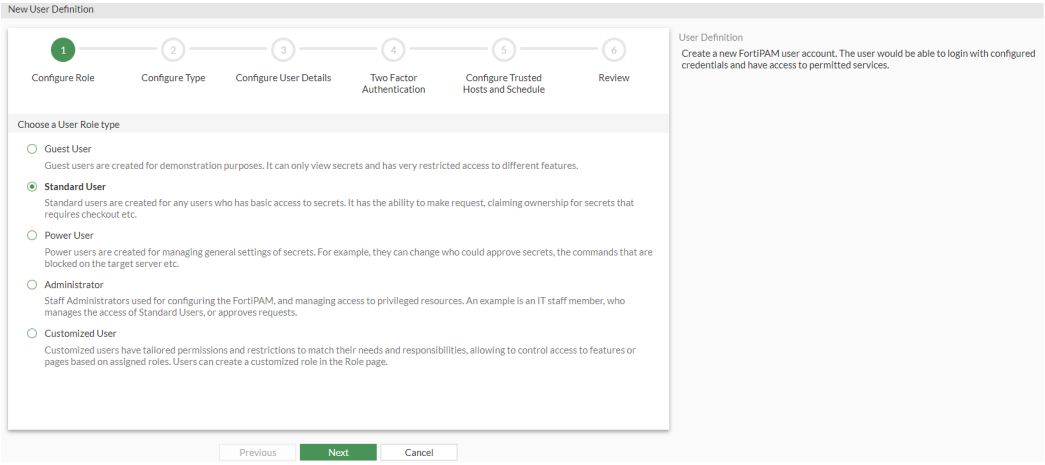
Creating a user

By default, FortiPAM has a default user with the username `admin` and no password.

When you go into the system for the first time, you must set a password for this account. Additional users can be added later.

To create a user:

1. Go to *User Management* > *User Definition*, and select *Create*
   The *New User Definition* wizard is launched.



2. Enter the following information, and click *Next* after each tab:

Configure Role	
Choose a User Role type	Select from the following user role types: • *Guest User* • *Standard User* • *Power User* • *Administrator* • *Customized User* For *Administrator*, select from one of the available administrator roles from the *Choose an Administrator Role* dropdown. For *Customized User*, select from one of the available custom roles from the *Choose a custom defined Role* dropdown.

The administrator/custom role decides what an administrator or a customized user can see. Depending on the nature of the administrator work, access level, or seniority, you can allow them to view and configure as much or as little as required.

	 Use the search bar to look for an administrator/custom role. For information on the user types and their roles, see Users in FortiPAM on page 163 and Role on page 174.
Configure Type	
Choose a User type	Select a user type: • *Local User*  To change the local user password, see Admin on page 11. • *API User* • *Remote User*: Select the option if you want to enable login for one remote user in a remote group, and assign the user the remote user type for the FortiPAM session. For *Remote User*, select a remote group where the user is found. See User groups on page 171.  Use the search bar to look for a remote group. For information on the user types, see Users in FortiPAM on page 163.
Configure User Details	
Username	The username.  Do not use < > ( ) # " ' ` characters in the username.
Password	The password. **Note**: This option is only available when the user type is local.
Confirm Password	Enter the password again to confirm. **Note**: This option is only available when the user type is local.
Status	Enable/disable user login to FortiPAM.

	 When you attempt to create a new user that exceeds the licensed seats, the *Status* option in the *Configure User Details* tab cannot be enabled. As you hover over the *Enable* button, a tooltip appears, alerting you that the user cannot be enabled as you have exceeded your license seat. **Note**: The option is not available when the user type is an API user.
Email address	The email address.
Critical System Email Alert	Enable/disable sending critical system alerts via email. **Note**: The option is disabled by default.
General Email Alert	Enable/disable sending general alerts via email. **Note**: The option is disabled by default.
Comments	Optionally, enter comments about the user.
Two Factor Authentication Enable/disable using two-factor authentication. **Note**: Two factor authentication is disabled by default. **Note**: Two factor authentication is not available for an API user. You can also set up **Two Factor Authentication** using CLI. See Two Factor Authentication using CLI.	
Authentication Type	Specify the type of user authentication used: • *FortiToken* • *FortiToken Cloud*. See 2FA with FortiToken Cloud example on page 164. • *Email based two-factor authentication* (default) • *SMS based two-factor authentication*
Token	From the dropdown, select a token. **Note**: The option is mandatory and only available when the *Authentication Type* is *FortiToken*.
Send Activation Code	Enable/disable sending activation codes, and select either *Email* or *SMS* as the mode to send the activation code.  To select the *SMS* option, enable *SMS* first. **Note**: This option is only available when *FortiToken Cloud* is the *Authentication Type*.
Email address	The email address. **Note**: This option is mandatory when: • *Authentication Type* is *FortiToken*. • *Authentication Type* is *FortiToken Cloud*. • *Authentication Type* is *Email based two-factor authentication.*

	 The email address is synched from the email address added in the *Configure User Details* pane.
SMS	Enable/disable SMS. **Note**: This option is enabled when *SMS based two-factor authentication* is selected.
Country Dial Code	From the dropdown, select a country code. **Note**: The option is mandatory when: • *Authentication Type* is *SMS based two-factor authentication*. • *SMS* is enabled for any other *Authentication Type*.
Phone Number	Enter the phone number. **Note**: The option is mandatory when: • *Authentication Type* is *SMS based two-factor authentication*. • *SMS* is enabled for any other *Authentication Type*.
Configure Trusted Hosts	
IPv4 Trusted Hosts	Trusted IPv4 addresses users use to connect to FortiPAM.  Use + button to add a new IPv4 address and *x* to delete an added IPv4 address.
Configure the schedule for which the user can connect to the FortiPAM	Enable/disable configuring the login schedule for the users. From the dropdown, select a schedule. See Schedule on page 193. **Note**: This option is disabled by default.

3. In the *Review* tab, verify the information you entered and click *Submit* to create the user.

 Use the pen icon to edit tabs.

 Alternatively, use the CLI commands to create users.

To regenerate the API key:

1. Go to *User Management* > *User Definition*.
2. Select the API user whose API key you intend to change and then select *Edit*.
3. In the *Details* pane, select *Re-generate API Key*.

4. In the *Re-generate API Key* window, select *Generate*.

Regenerating the API key will immediately revoke access for any API consumers using the current key.

A new API key for the API user is generated.

5. Click *Close*.

CLI configuration to set up a local user - example**:**

```
config system admin
   edit <user_name>
      set accprofile <role_name>
      set password <password>
   next
end
```

CLI configuration to set up a remote LDAP user - example**:**

```
config system admin
   edit <ldap_username>
      set remote-auth enable
      set accprofile <profname>
      set remote-group <ldap_group_name>
   next
end
```

CLI configuration to set up a remote RADIUS user - example**:**

```
config system admin
   edit <radius_username>
      set remote-auth enable
      set accprofile <profname>
      set remote-group <radius_group_name>
   next
end
```

CLI configuration to enable two-factor authentication - example**:**

```
config system admin
   edit <username>
      set password "myPassword"
      set two-factor <fortitoken | fortitoken-cloud | email>
      set fortitoken <serial_number>
      set email-to "username@example.com"
   next
end
```

Users in FortiPAM

The following user types are available:

- *Local User*: Information configured and stored on the FortiPAM.
- *API User*: Accesses FortiPAM by using a token via REST API instead of the GUI.
- *Remote User*: Information configured and stored on a remote server.

FortiPAM users can have one of the following role types:

- *Guest User*: For demonstration purposes only. Guest users can only view secrets and have restricted access to FortiPAM features.
- *Standard User*: Logs in, makes requests for resources, and connect to the privileged resources.

  The standard user role is for basic use only. A standard user is not allowed to configure or manage access to privileged resources, e.g., a user that connects to the workstation.
- *Power User*: For managing general secret settings, e.g., a power user can change who approves secrets, commands blocked on the target server, etc.
- *Administrator*: Staff administrators used for configuring FortiPAM, and managing access to privileged resources, e.g., an IT staff member managing the access of standard users or approving requests.
- 

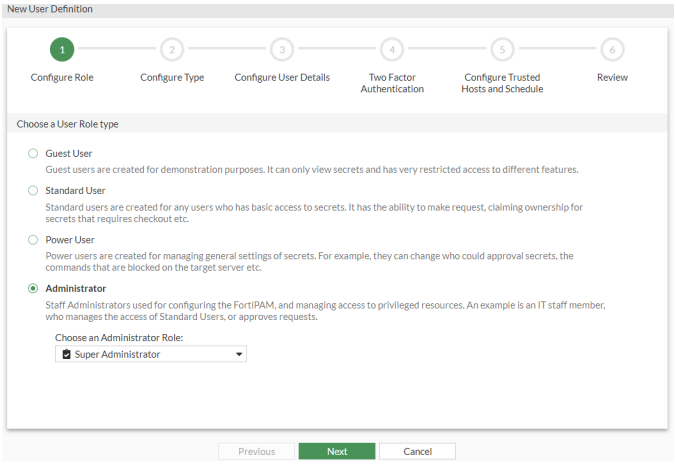
  For *Administrator*, administrator roles are available. See Role on page 174.
- *Customized User*: Customized users have tailored permissions and restrictions to match their needs and responsibilities, allowing them to control access to features or pages based on assigned roles. You can create a customized role in Role.

  See Creating a user on page 159.

2FA with FortiToken Cloud - example

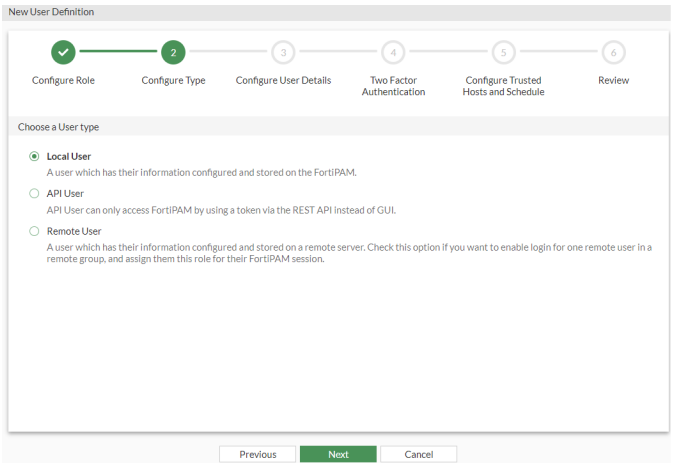
To configure a user with FortiToken Cloud as the authentication type:

1. Go to *User Management* > *User Definition*, and select *Create*.
   The *New User Definition* wizard is launched.
2. In *Choose a User Role type*, select *Administrator*, and from the *Choose an Administrator Role* dropdown, select *Super Administrator*.



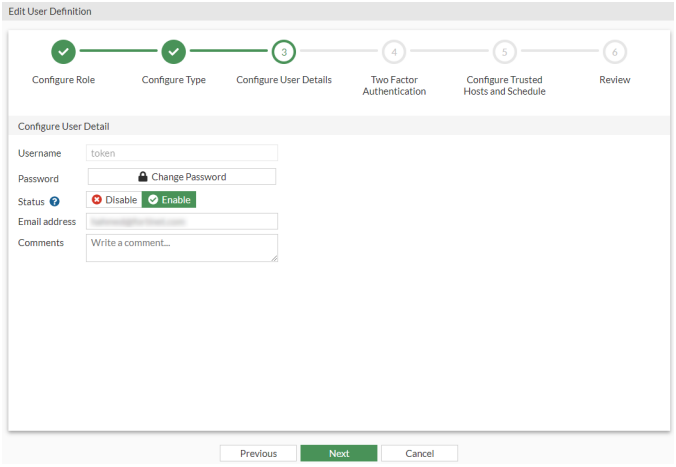
3. Click *Next*.

4. In *Choose a User type*, select either *Local User* or *Remote User*.
   In this example, *Local User* is selected.



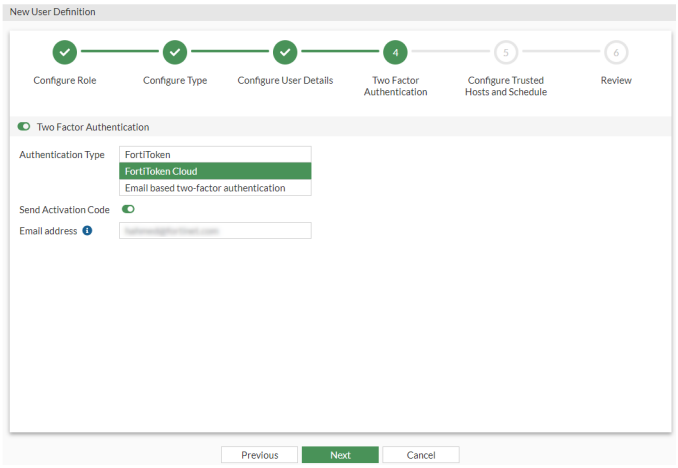
For *Remote User*, select a remote group where the user is found. See User groups on page 171.

5. Click *Next*.
6. In *Configure User Detail*:
   a. In *Username*, enter a name.
   b. In *Password*, enter a password.
   c. In *Confirm Password*, reenter password to confirm.
   d. In *Status*, enable logging in to FortiPAM.
   e. In *Email address*, enter an email address.



7. Click *Next*.
8. Enable *Two Factor Authentication*, and:
   a. In *Authentication Type*, select *FortiToken Cloud*.
   b. Enable *Send Activation Code*.

c. In *Email address*, enter the email address where the activation code for FortiToken Cloud is sent.



d. Click *Next*.

9. Click *Next*.
10. In the *Review* tab, verify the information you entered and click *Submit* to create the user.
11. From the user dropdown on the top-right, select *Logout*.
12. On the login screen, enter the username and password for the user you just created, and select *Continue*.
13. On the token screen, enter the token from your FortiToken Mobile and select *Continue* to log in to FortiPAM, or approve the push login request that appears on your mobile phone to log in to FortiPAM.

CLI configuration to set up a user with FortiToken Cloud as the authentication type - example**:**

```
config system admin
   edit "token"
      set accprofile "super_admin" #administrator role
      set two-factor fortitoken-cloud
      set email-to "username@example.com"
      set password "myPassword"
   next
end
```

CLI configuration to set up an interface for FortiPAM - example**:**

```
config system interface
   edit "port1"
      set ip 192.168.1.99 255.255.255.0
      set allowaccess https ssh http
      set type physical
      set snmp-index 1
   next
end
```

CLI configuration to set up a virtual IP address for FortiPAM - example**:**

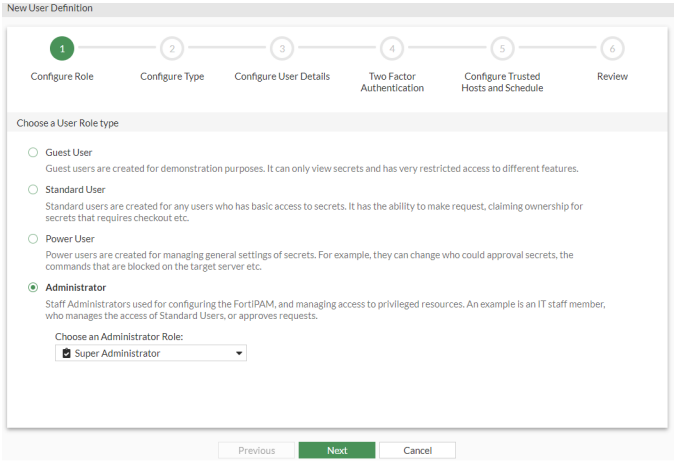
```
config firewall vip
   edit "fortipam_vip"
      set uuid 858a44ac-f359-51ec-e7ec-717ef0afbf4d
      set type access-proxy
      set extip 192.168.1.109 #VIP and the interface IP address are different.
      set extintf "any"
```

```
      set server-type https
      set extport 443
      set ssl-certificate "Fortinet_SSL"
    next
end
```

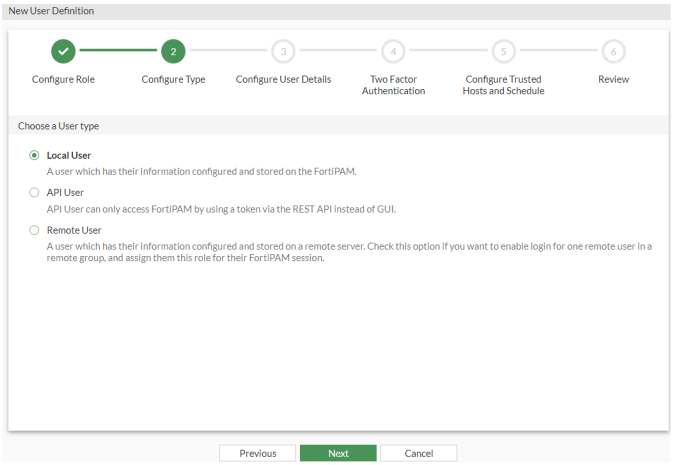
2FA with FortiToken - example

To configure a user with FortiToken as the authentication type:

1. Go to *User Management* > *User Definition*, and select *Create*.
   The *New User Definition* wizard is launched.
2. In *Choose a User Role type*, select *Administrator*, and from the *Choose an Administrator Role* dropdown, select *Super Administrator*.

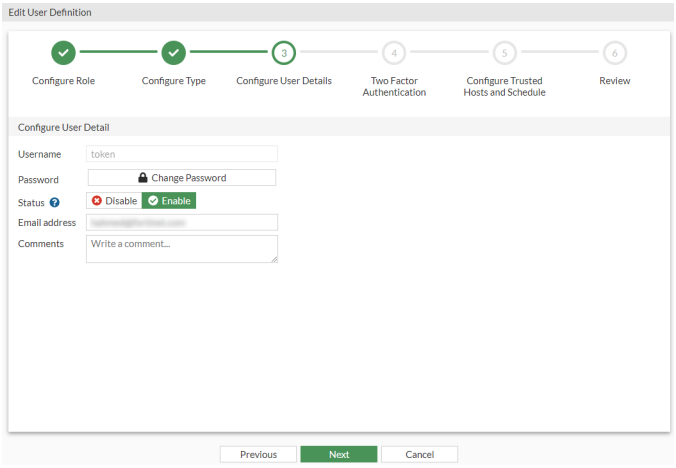


3. Click *Next*.
4. In *Choose a User type*, select either *Local User* or *Remote User*.
   In this example, *Local User* is selected.

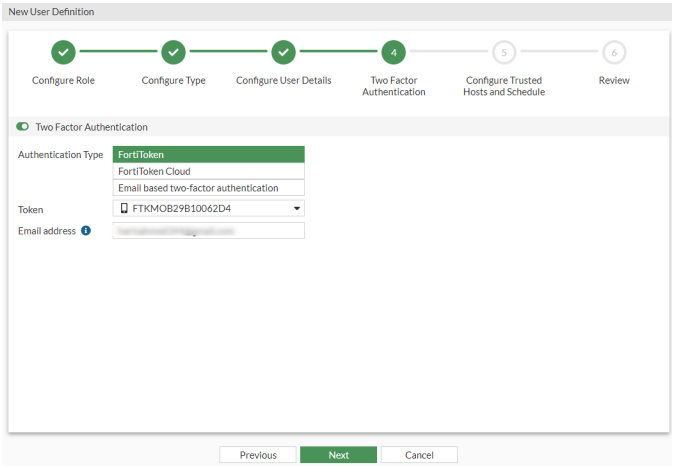


For *Remote User*, select a remote group where the user is found. See User groups on page 171.

5. Click *Next*.
6. In *Configure User Detail*:
   a. In *Username*, enter a name.
   b. In *Password*, enter a password.
   c. In *Confirm Password*, reenter password to confirm.
   d. In *Status*, enable logging in to FortiPAM.
   e. In *Email address*, enter an email address.



7. Click *Next*.
8. Enable *Two Factor Authentication*, and:
   a. In *Authentication Type*, select *FortiToken*.
   b. From the *Token* dropdown, select a FortiToken.
   c. In *Email address*, enter the user email address.



   d. Click *Next*.
9. Click *Next*.
10. In the *Review* tab, verify the information you entered and click *Submit* to create the user.
11. Go to *User Management* > *FortiTokens*, select the token used in step 8 from the list and then click *Provision*. An email notification is sent to the user. This is the email address configured in step 8.
12. To enable FortiToken push notification:
    a. Go to *Network* > *Interfaces* and double-click port1.
    b. In *Administrative Access*, select *FTM*.

c. In the CLI console, enter the following commands:

```
config system ftm-push
   set server-cert "Fortinet_Factory"
   set server x.x.x.x #IP address of the FortiPAM interface
   set status enable
end
```

13. From the user dropdown on the top-right, select *Logout*.
14. On the login screen, enter the username and password for the user you just created, and select *Continue*.
15. On the token screen, enter the token from your FortiToken Mobile and select *Continue* to log in to FortiPAM, or approve the push login request that appears on your mobile phone to log in to FortiPAM. See Setting up FortiToken Mobile on page 169.

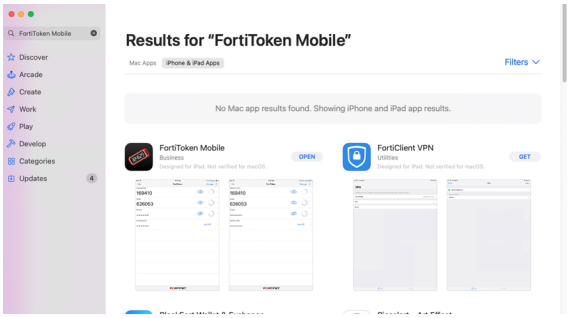
CLI configuration to set up a user with FortiToken as the authentication type - example**:**

```
config system admin
   edit "token"
      set accprofile "super_admin" #administrator role
      set two-factor fortitoken
      set fortitoken "FTKMOB29B10062D4"
      set email-to "username@example.com"
      set password "myPassword"
   next
end
```

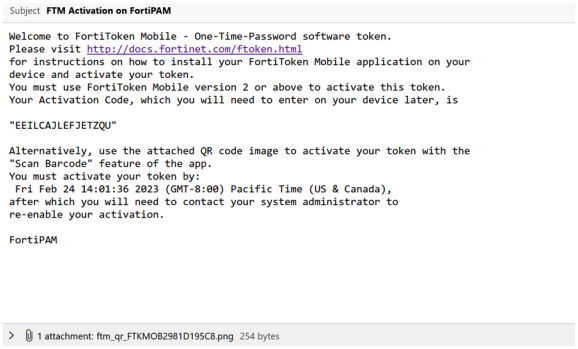
Setting up FortiToken Mobile

To set up FortiToken Mobile:

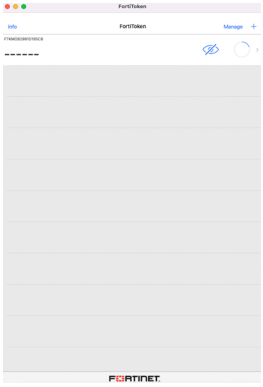
1. In the App Store, look for FortiToken Mobile and install the application.



2. After your system administrator assigns a token to you, you will receive a notification with an activation code and an activation expiration date by which you must activate your token. For more information on *Token Activation*, see *FortiToken Mobile User Guide*.



3. Open the FortiToken Mobile application and click + icon on the top-right to add a token.



4. There are two ways to add a token to the FortiToken Mobile application:
   a. **Scan QR code**: If your device supports QR code recognition, select + in the FortiToken Mobile home screen and point your device camera at the QR code attached to the activation email.

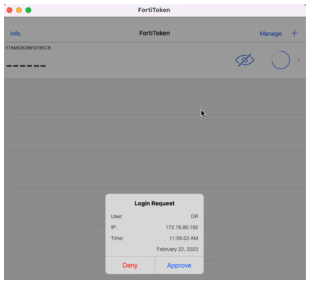
   b. **Enter Manually**:
      i. Select + and then select *Enter Manually* from the bottom.
      ii. Select *Fortinet* and enter *Name* and *Key*.

Key is the activation key from your activation email notification and must be entered exactly as it appears in the activation message, either by typing or copying and pasting.

      iii. Click *Done*.
      FortiToken Mobile communicates with the secure provisioning server to activate your token. The token is now displayed in the token list view.

5. Click the eye icon to retrieve the token to be used in step 15 when configuring 2FA with FortiToken.

Alternatively, if approving the push login request in step 15 when configuring 2FA with FortiToken, click *Approve* in *Login Request*.

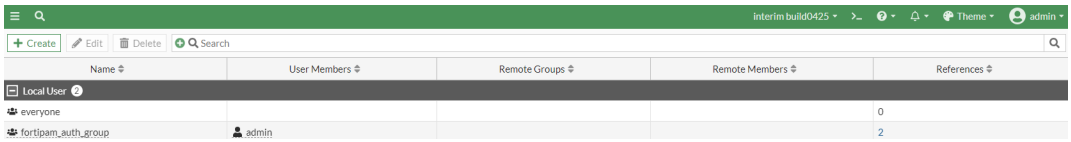


User groups

User Groups in *User Management* displays a list of user groups.

The following two default user groups are available:

- *everyone*: By default, every user belongs to this user group.
- *fortipam_auth_group*: By default, the *Super Administrator* admin user belongs to this user group. Users can be added or removed from this user group.



User groups can contain references to individual users or references to groups defined on an existing LDAP server.

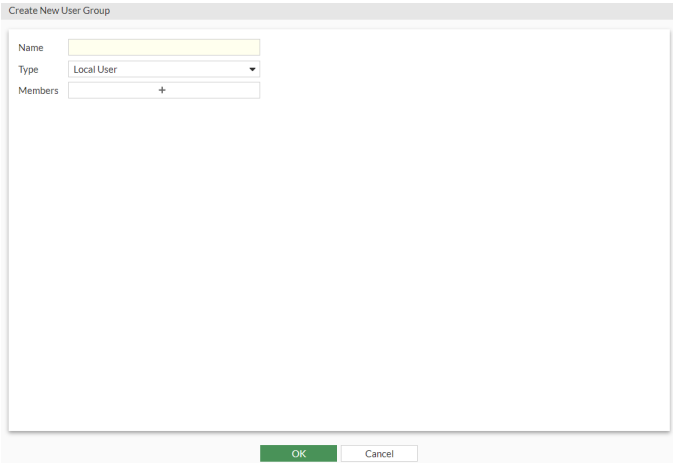
Users can be assigned to groups during user account configuration, or by creating or editing the groups to add users to it.

The *User Groups* tab contains the following options:

Create	Select to create a new user group.
Edit	Select to edit the selected user group.
Delete	Select to delete the selected user groups.
Search	Enter a search term in the search field, then hit `Enter` to search the user groups list. To narrow down your search, see Column filter.

To create a new user group:

1. Go to *User Management* > *User Groups*.
2. Select *Create* to create a new user group.
   The *Create New User Group* window opens.



3. Enter the following information:

Name	Name of the group.
Type	Select the type of the group: • *Remote* • *Local User*
Members	Select + to add existing members to the user group from the list and select *Close*, or select *Create* to create a new user. See Creating a user on page 159.  Use the search bar to look for a user.
Remote Groups	By adding a remote server to the user group, the group will contain all user accounts on that server. Optionally, a specific user group on the remote server can be included to restrict the scope to that group. See Creating Remote Groups. **Note:** This pane is available only when the *Type* is *Remote*.  Select remote groups from the list and select *Delete* to delete the remote groups. Select a remote group from the list and select *Edit* to edit the remote group.

4. Click *OK*.

To create a new remote group:

1. In the *Create New User Group* window, select *Create* in *Remote Groups*.

The *Remote Groups* pane is only available when the *Type* is *Remote*.

The *Add Group Match* window opens.

2. In *Remote Server* dropdown, select LDAP, RADIUS, and SAML servers:
   a. If an LDAP server is selected, from the remote users list, select the remote users to import.

At least one LDAP server must be already configured. See LDAP servers on page 184.

Hold `ctrl` and click to select multiple users.

To narrow down your search, see Column filter.

You can filter your search by *Group*, or enter a custom filter and select *Apply*.

Enable *Show entries in subtree* to list remote users in the subtree.

LDAP filters consist of one or more clauses which can be combined with logical AND/OR operators.

Filter syntax differs depending on the LDAP server software.

See the following examples - examples:

- Users with given name starting with the letter "h":

```
(&(objectClass=person)(givenName=h*))
```

- All groups:

```
(&(objectClass=posixGroup)(cn=*))
```

   b. Optionally, if a RADIUS server is selected, select **+**, and enter group names in *Groups*.

At least one RADIUS server must be already configured. See RADIUS servers on page 191.

   c. Optionally, if a SAML server is selected, select **+**, and enter group names in *Groups*.

At least one SAML server must be already configured.

3. Click *OK* to save changes to group match.

Alternatively, use the CLI commands to create a user group.

CLI configuration to set up an LDAP user group - example**:**

```
config user group
   edit <ldap_group_name>
      set member <ldap_server_name>
      config match
         edit 1
            set server-name <ldap_server_name>
            set group-name "cn=User,dc=XYA, dc=COM"
         next
      end
   next
end
```

CLI configuration to set up a RADIUS user group - example**:**

```
config user group
   edit <radius_group_name>
      set member <radius_server_name>
   next
end
```

Role

Roles or access profiles define what a user can do when logged into FortiPAM.

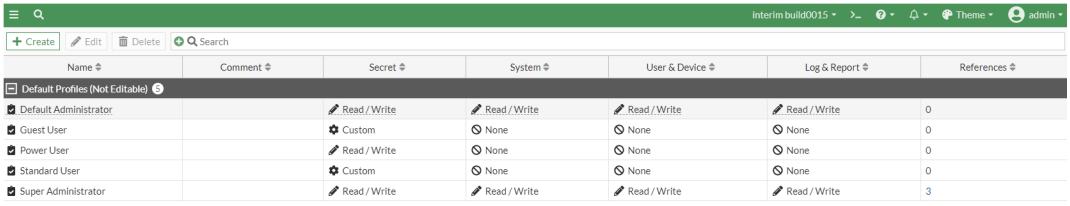
When a new user is created, it must have a specific role. See Creating a user on page 159.

When you create a standard user, a default normal user role is assigned to the new user automatically.

When setting up an administrator, administrator roles can be selected from the *Choose an Adminstrator Role* dropdown. See Creating a user on page 159.

The administrator role decides what the administrator can see.

Go to *Roles* in *User Management* to see a list of configured roles.



There are five default roles:

Default roles cannot be edited.

- *Default Administrator*: Read/write access same as a super administrator, but no access to maintenance mode and glass breaking.
- *Guest User*: For demonstration purposes only. Guest users can only view secrets and have restricted access to FortiPAM features.
- *Power User*: For managing general secret settings, e.g., a power user can change who approves secrets, commands blocked on the target server, etc.
- *Standard User*: Logs in, makes requests for resources, and connect to the privileged resources.

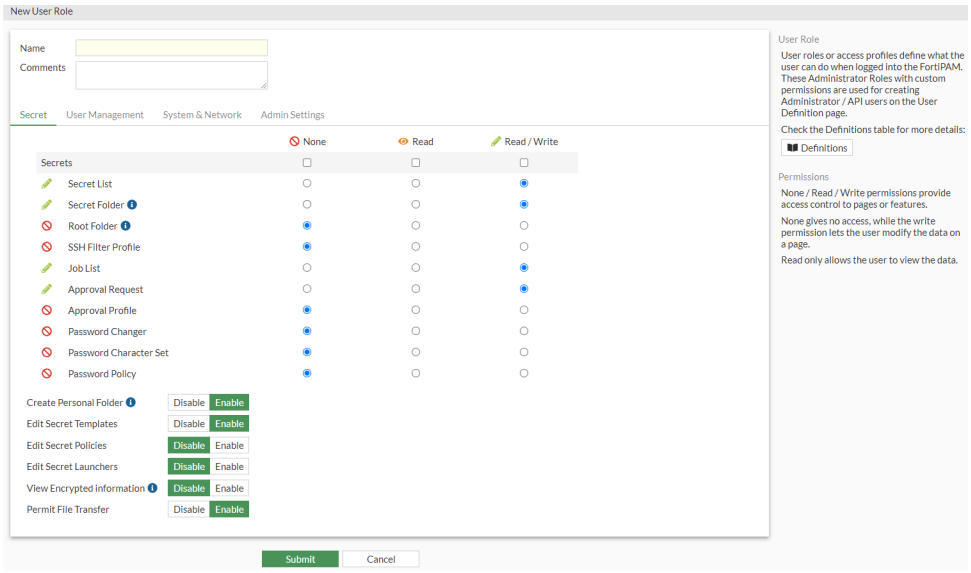
  Users with *Standard User* role do not have the privilege to manage FortiPAM devices.

- *Super Administrator*: Privilege to manage and monitor the FortiPAM device.
  Users with *Super Administrator* role also include privilege of secret server.
- The *Roles* tab contains the following options:

Create	Select to create a new role.
Edit	Select to edit the selected role.
Delete	Select to delete the selected roles.
Search	Enter a search term in the search field, then hit `Enter` to search the roles list. To narrow down your search, see Column filter.

To create a role:

1. Go to *User Management* > *Role*, and select *Create*.
   The *Secret* tab in the *New User Role* window opens.



Pages and features are organized and separated into different access controls.

There are two types of access controls:

- *Radio*: Provides *None*, *Read*, and *Read/Write* access.
- *Switch*: Enable/disable a feature.

For each feature, select from the following access levels:

- *None*
- *Read*: View access.

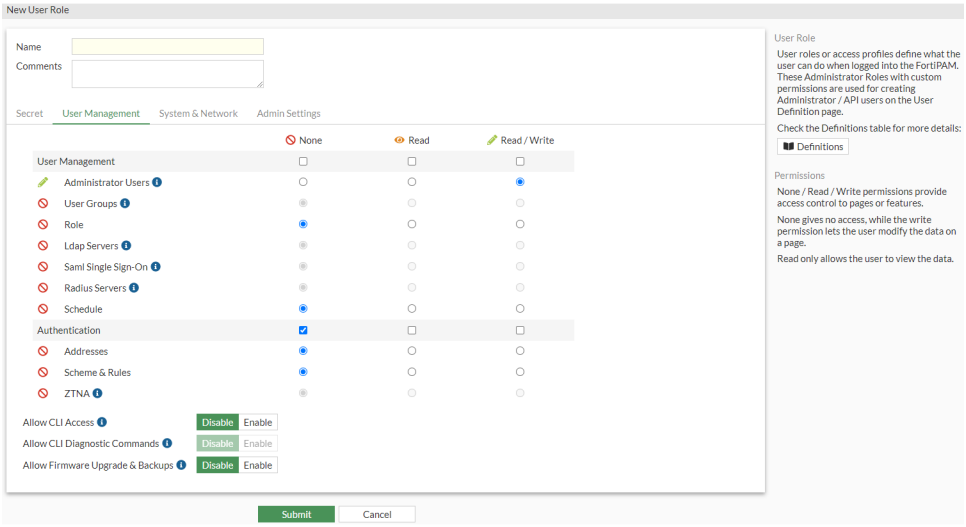
  Note: When an administrator has only read access to a feature, the administrator can access the GUI page and can use the `get` and `show` CLI command for that feature, but cannot make changes to the configuration.
- *Read/Write*: View, change, and execute access.

2. Enter the following information:

Name	The name of the role.
Comment	Optionally, enter comments about the role.
Secret Select *None*, *Read*, or *Read/Write* to set access level globally for all the secret features.	
Secret List	Set the access level for Secret list page. It also controls whether pages: *Secret Templates*, *Policies* and *Launchers* can be viewed.
Secret Folder	Set the access level for *Folders*. **Note**: You can restrict the corresponding folder and secret permissions under a specific secret.
Root Folder	Permission to create folders in *Root*. **Note**: The *Secret Folder* must be set to at least *Read* permission to enable accessing the root folder.
SSH Filter Profile	Set the access level for *SSH Filter Profiles* page.

Job List	Set the access level for *Jobs List* page.
Approval Request	Set the access level for *My Request* and *Request Review* page in *Approval Request*.
Approval Profile	Set the access level for *Approval Profile* page in *Approval Flow*.
Password Changer	Set the access level for *Password Changers* page in *Password Changing*.
Password Character Set	Set the access level for *Character Sets* page in *Password Changing*.
Password Policy	Set the access level for *Password Policies* page in *Password Changing*.
Create Personal Folder	Enable/disable creating a personal folder right after the user is created. **Note**: The *Secret Folder* permission must be *Read/Write*.
Edit Secret Templates	Enable/disable editing the *Secret Templates* page.
Edit Secret Policies	Enable/disable editing the *Policies* page.
Edit Secret Launchers	Enable/disable editing the *Secret Launchers* page.
View Encrypted Secret Information	Enable/disable viewing the secret password, passphrase, and ssh-key. **Note**: *Secret List* must be set to *Read/Write* permission to view the encrypted secret information.
Permit File Transfer	Enable/disable permitting file transfer.

3. Select the *User Management* tab.
The *User Management* tab opens.

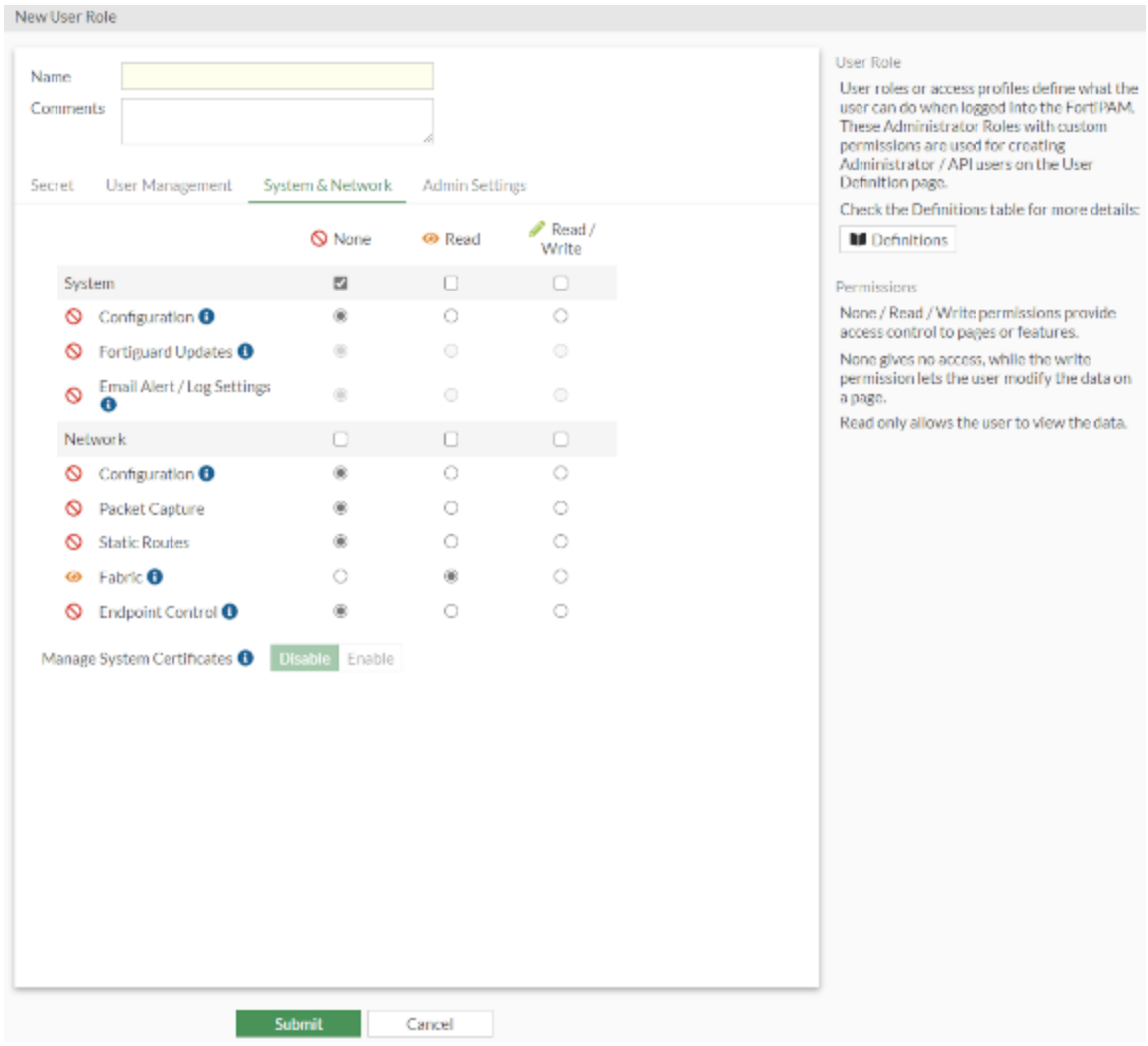


4. Enter the following information:

User Management Select *None*, *Read*, or *Read/Write* to set access level globally for all the user management features.	
Administrator Users	Set the access level for the *User Definition* page in *User Management* and the *Backup* page in *System*.
User Groups	Set the access level for *User Groups* page in *User Management*.

	Note: *Ldap Servers*, *Saml Single Sign-On*, and *Radius Servers* must be set to at least *Read* permission to access *User Groups*.
Role	Set the access level for *Role* page in *User Management*.
Ldap Servers	Set the access level for *Ldap Servers* page in *User Management*. **Note**: *Scheme & Rules* must be set to at least *Read* permission to access LDAP servers.
Saml Single Sign-On	Set the access level for *Saml Single Sign-On* page in *User Management*. **Note**: *Addresses* and *Scheme & Rules* must be set to at least *Read* permission to access SAML servers.
Radius Servers	Set the access level for *Radius Servers* page in *User Management*. **Note**: *Scheme & Rules* must be set to at least *Read* permission to access RADIUS servers.
Schedule	Set the access level for *Schedule* page in *User Management*.
Authentication Select *None*, *Read*, or *Read/Write* to set access level globally for all the authentication features.	
Addresses	Set the access level for *Addresses* page in *Authentication*.
Schemes & Rules	Set the access level for *Scheme & Rules* page in *Authentication*. **Note**: This requires the *Write* permission to *User Groups*, *Ldap Servers*, *Saml Single Sign-On*, and *Radius Servers*.
ZTNA	Set the access level for *ZTNA* page in *System*. **Note**: This requires the same permission as *Schedule* and *Addresses*. - Examples • If all required permissions are *Read/ Write*, the ZTNA can only be either *None* or *Read/Write*. • If *Schedule* is set to *Read* and the rest is set to *Read/Write*, *ZTNA* can only be *None*.
Allow CLI Access	Enable/disable CLI access. **Note**: The *Administrator Users* must be set to *Write* permission to have CLI access.
Allow CLI Diagnostic Commands	Enable/disable access to diagnostic CLI commands. **Note**: *System Configuration* must be set to *Write* permission to manage system certificates.  The role must have *Allow CLI Access* enabled to access the diagnostic commands.
Allow Firmware Upgrade & Backups	Enable/disable permission to use firmware upgrades and configuration backup features.

5. Select the *System & Network* tab.
   The *System & Network* tab opens.

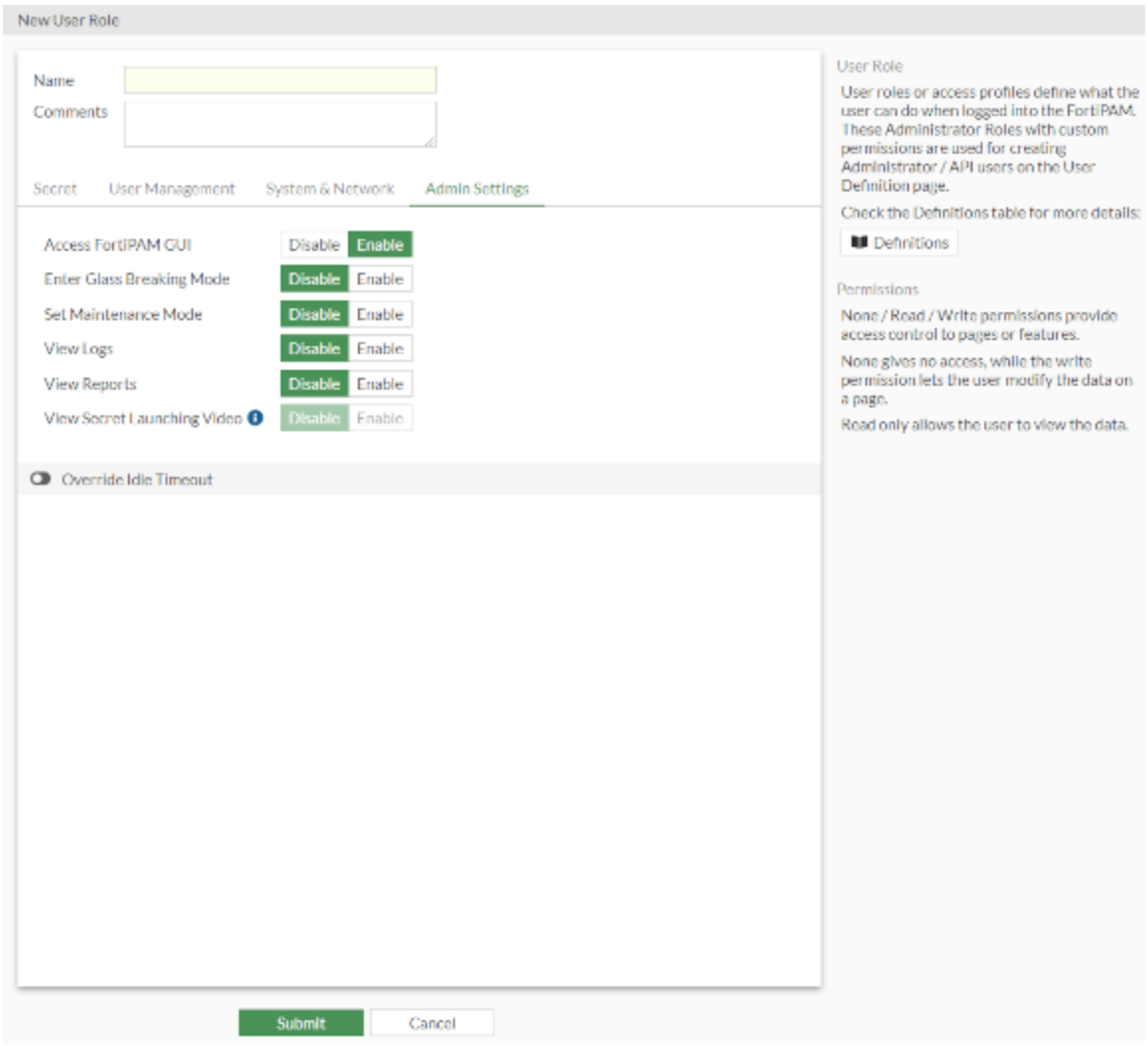


6. Enter the following information:

System Select *None*, *Read*, or *Read/Write* to set access level globally for all the system features.	
Configuration	Set the access level for: • *DNS Settings* in *Network*. • *SNMP*, *Settings*, and *HA* pages in *System*. • VM License uploading; *System Reboot*, and *Shutdown* settings. • *Configuration Revisions* and *Scripts*.
FortiGuard Updates	Set the access level for *FortiGuard* page from *Dashboard*. The *System Configuration* is set to *Write* to have access to the *FortiGuard* page.
Email Alert/Log Settings	Set the access level for *Email Alert Settings* and *Log Settings* in *Log & Report*. **Note**: • The *Fabric* and *System Configuration* is set to *Write* to have full access to

	the *Log Settings* page. • The *View Reports* access needs to be enabled to have settings, *Local Reports* and *Historical FortiView* in the *Log Settings* page.
Network Select *None*, *Read*, or *Read/Write* to set access level globally for all the network features.	
Configuration	Set the access level for *Interfaces* page in *Network*.
Packet Capture	Set the access level for *Packet Capture* page in *Network*.
Static Routes	Set the access level for *Static Routes* page in *Network*.
Fabric	Set the access level for *FortiAnalyzer Logging* card on the *Fabric Connectors* page in *Security Fabric*.
Endpoint Control	Set the access level for *FortiClient EMS* card on the *Fabric Connectors* page in *Security Fabric* and *ZTNA Tags* in *System* > *ZTNA*.
Manage System Certificates	Enable/disable accessing the *Certificates* page in *System*. **Note**: *System Configuration* must have the *Write* permission.

7. Select the *Admin Settings* tab.
   The *Admin Settings* tab opens.



8. Enter the following information:

Access FortiPAM GUI	Enable/disable accessing FortiPAM GUI.
Enter Glass Breaking Mode	Enable/disable glass breaking mode. **Note**: The glass breaking mode gives you access to all secrets in the system.
Set Maintenance Mode	Enable/disable maintenance mode. Note: Suspend all critical processes to allow maintenance related activities.
View Logs	Enable/disable viewing *Events*, *Secrets*, *ZTNA*, and *SSH* logs in *Log & Report*.
View Reports	Enable/disable viewing *Reports* in *Log & Report*.
View Secret Launching Video	Enable/disable viewing playback videos in *Secret Video*. **Note**: *View Logs* must be enabled since the secret videos are available in *Log & Report* > *Secret* page.
Override Idle Timeout Enable to override the idle timeout.	

Never Timeout	Enable to never timeout. **Note**: The option is disabled by default.
Offline	Set the time after which the user with the role goes offline, in minutes (1 - 480, default = 10).

9. Click *OK*.

Alternatively, you can also use the CLI to create roles.

CLI configuration to set up a user role - example**:**

```
config system accprofile
   edit "Default Administrator"
      set secfabgrp read-write
      set ftviewgrp read-write
      set authgrp read-write
      set sysgrp read-write
      set netgrp read-write
      set loggrp read-write
      set fwgrp read-write
      set vpngrp read-write
      set utmgrp read-write
      set wanoptgrp read-write
      set secretgrp read-write
      set cli enable
      set system-diagnostics enable
   next
   edit "pam_standard_user"
      set secfabgrp read
      set ftviewgrp read
      set authgrp read
      set secretgrp custom
      set system-diagnostics disable
      config secretgrp-permission
         set launcher read
         set pwd-changer read
         set template read-write
         set secret-policy read
         set request read-write
         set folder-table read-write
         set secret-table read-write
         set create-personal-folder read-write
      end
   next
```

Access control options

When creating or editing a role, select *Definitions* to see access control definitions.

Access Control	Definition
Secrets	
Secret List	It controls access to the Secret list page. It also controls whether pages: *Secret Templates*, *Policies* and *Launchers* can be viewed.
Secret Folder	Controls the access to *Folders*. **Note**: You can restrict the corresponding folder and secret permissions under a specific folder and secret.
Root Folder	Permission to create folders in *Root*.
SSH Filter Profile	Access to the *SSH Filter Profiles* page.
Job List	Access to the *Job List* page.
Approval Request	Access to the *My Request* and *Request Review* page in *Approval Request*.
Approval Profile	Access to the *Approval Profile* page in *Approval Flow*.
Password Changer	Access to *Password Changers* page in *Password Changing*.
Password Character Set	Access to *Character Sets* page in *Password Changing*.
Password Policy	Access to *Password Policies* page in *Password Changing*.
Create Personal Folder	Enable/disable creating a personal folder right after the user is created.
Edit Secret Templates	Enable/disable editing the *Secret Templates* page.
Edit Secret Policies	Enable/disable editing the *Policies* page.
Edit Secret Launchers	Enable/disable editing the *Secret Launchers* page.
View Encrypted information	Enable/disable viewing the secret password, passphrase and ssh-key. The Secret list must have *Write* permission to view the encrypted secret information.
User Management	
Administrator Users	Access to the *User Definition* page in *User Management* and the *Backup* page in *System*.
User Groups	Access to the *User Groups* page in *User Management*.
Role	Access to the *Role* page in *User Management*.
Ldap Servers	Access to the *Ldap Servers* page in *User Management*.
Saml Single Sign-On	Access to the *Saml Single Sign-On* page in *User Management*.
Radius Servers	Access to the *Radius Servers* page in *User Management*.
Schedule	Access to the *Schedule* page in *User Management*.
Allow CLI Access	Enable/disable CLI access.
Allow CLI Diagnostic Commands	Enable/disable access to diagnostic CLI commands.

Access Control	Definition
Allow Firmware Upgrade & Backups	Enable/disable permission to use firmware and configuration backup features.
Authentication	
Addresses	Access to the *Addresses* page.
Scheme & Rules	Access to the *Scheme & Rules* page.
ZTNA	Access to the *ZTNA* page in *System*.
Network	
Configuration	Access to the *Interfaces* page in *Network*.
Packet Capture	Access to the *Packet Capture* page in *Network*.
Static Routes	Access to the *Static Routes* page in *Network*.
Fabric	Access to the *FortiAnalyzer Logging* card on the *Fabric Connectors* page in *Security Fabric*.
Endpoint Control	Access to the *FortiClient EMS* card on the *Fabric Connectors* page in *Security Fabric*.
Manage System Certificates	Enable/disable accessing the *Certificates* page in *System*.
System	
Configuration	Access to: • *DNS Settings* in *Network*. • *SNMP*, *Settings*, and *HA* pages in *System*. • VM License uploading; *System Reboot*, and *Shutdown* settings. • *Configuration Revisions* and *Scripts*.
FortiGuard Updates	Access to the *FortiGuard* page from *Dashboard*.
Email Alert/Log Settings	Access to *Email Alert Settings* and *Log Settings* in *Log & Report*.
Admin Settings	
Access FortiPAM GUI	Enable/disable accessing FortiPAM GUI.
Enter Glass Breaking Mode	Enable/disable glass breaking mode.
Set Maintenance Mode	Enable/disable maintenance mode.
View Logs	Enable/disable viewing *Events*, *Secrets*, *ZTNA*, and *SSH* logs in *Log & Report*.
View Reports	Enable/disable viewing *Reports* in *Log & Report*.
View Secret Launching Video	Enable/disable viewing playback videos in *Secret Video*.

LDAP servers

Users can use remote authentication servers, such as an LDAP server, to connect to FortiPAM.

LDAP servers store users' information including credentials and group membership. This information can authenticate FortiPAM remote users and provide groups for authorization.

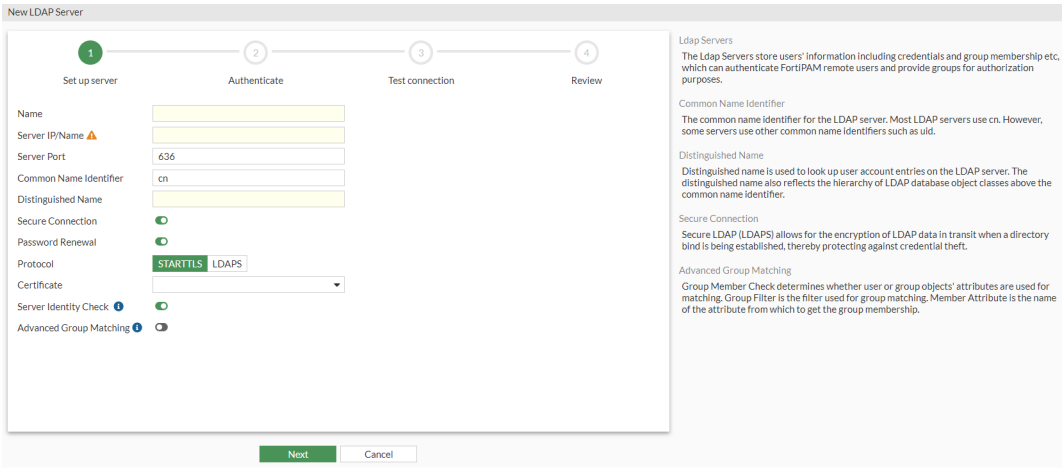
Go to *LDAP servers* in *User Management* to see a list of LDAP servers.

The *LDAP server* tab contains the following options:

Create	Select to create an LDAP server.
Edit	Select to edit the selected LDAP server.
Delete	Select to delete the selected LDAP roles.
Search	Enter a search term in the search field, then hit `Enter` to search the LDAP servers list. To narrow down your search, see Column filter.

To create an LDAP server:

1. Go to *User Management* > *LDAP servers*, and select *Create*.
   The *New LDAP Server* wizard opens.



2. Enter the following information, and click *Next* after each tab:

Set up server	
Name	Name of the server.
Server IP/name	The IP address or FQDN for this remote server.
Server Port	The port number for LDAP traffic (default = 636).
Common Name Identifier	The common name identifier for the LDAP server. Most LDAP servers use `cn`. However, some servers use other common name identifiers such as `UID`. (default = `cn`).
Distinguished Name	The distinguished name is used to look up entries on the LDAP server.

	The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier.
Secure Connection	Enable to use a secure LDAP server connection for authentication. Secure LDAP (LDAPS) allows for the encryption of LDAP data in transit when a directory bind is being established, thereby protecting against credential theft. **Note**: This option is enabled by default.
Password Renewal	Enable to allow LDAP users to renew passwords. **Note**: This option is only available when *Secure Connection* is enabled. **Note**: This option is enabled by default.
Protocol	When *Secure Connection* is enabled, select either *LDAPS* or *STARTTLS* (default).
Certificate	When *Secure Connection* is enabled, select the certificate from the dropdown.  Use the search bar to look up a certificate.
Server Identity Check	Enable to verify server domain name/IP address against the server certificate. **Note**: This option is only available when *Secure Connection* is enabled. **Note**: This option is enabled by default.
Advanced Group Matching	Group member check determines whether user or group objects' attributes are used for matching. Group Filter is the filter used for group matching. Member attribute is the name of the attribute from which to get the group membership.  Depending on the LDAP server, you may need to configure additional properties to ensure LDAP groups are correctly matched. **Note**: The option is disabled by default.
Group Member Check	From the dropdown, select a group member check option (default = `Ldap::grp::member::check:user-attr`).
Group Filter	Enter the group filter for group matching.
Group Search Base	Enter the search base used for searching a group.
Member Attribute	Specify the value for this attribute. This value must match the attribute of the group in LDAP server. All users part of the LDAP group with the attribute matching the attribute will inherit the administrative permissions specified for this group (default = `memberof`).
Authenticate	
Username	The username.
Password	The password.

3. Click *Test connection* to test the connection to the LDAP server.

Test connection is only available to users who have *Write* permission for *Ldap Servers*. See Role on page 174.

If the credentials to the server are valid, it shows *Successful*.

4. In the *Review* tab, verify the information you entered and click *Submit* to create the LDAP server.

Use the pen icon to edit tabs.

Alternatively, use the CLI commands to create LDAP servers.

CLI configuration to set up an LDAP server - example**:**

```
config user ldap
   edit <name>
      set server <server_ip>
      set cnid "cn"
      set dn "dc=XYZ,dc=fortinet,dc=COM"
      set type regular
      set username <ldap_username>
      set password <password>
   next
end
config authentication scheme
   edit "fortipam_auth_scheme"
      set method form
      set user-database "local-admin-db" <ldap_server_name>
   next
end
```

Setting up remote LDAP authentication includes the following steps:

1. Configuring the LDAP server. See Configuring an LDAP server.
2. Adding the LDAP server to a user group. See User groups on page 171.
3. Configuring the administrator account. See Creating a user on page 159.

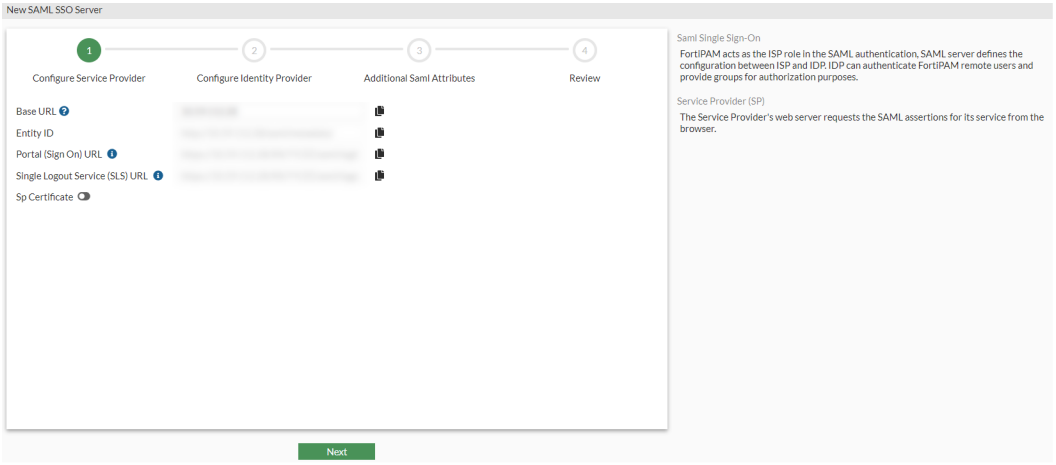
SAML Single Sign-On (SSO)

SAML SSO can be configured in *User Management*.

FortiPAM acts as the SP in SAML authentication. The SAML server defines the configuration between SP and IdP. An IdP can authenticate FortiPAM remote users and provide groups for authorization.

To create a SAML SSO server:

1. Go to *User Management* > *Saml Single Sign-On*.



2. Enter the following information, and click *Next* after each tab:

Configure Service Provider	
Base URL	The URL where the Identity Provider (IdP) sends SAML authentication requests. **Note**: The address should be WAN-accessible and can be an IP address or an FQDN. **Note**: To include a port, append it after a colon. For example: `200.1.1.1.:443`.
Entity ID	Enter the SP entity ID.
Portal (Sign On) URL	The SAML service provider login URL. The URL is used to initiate a single sign-on. **Note**: Not all IdPs require a *Portal (Sign On) URL*. **Note**: The *Portal (Sign On) URL* is alternatively referred to as the Portal URL or the Sign On URL.
Single Logout Service (SLS) URL	The SP Single Logout Service (SLS) logout URL. The IdP sends the logout response to this URL. **Note**: The *Single Logout Service (SLS) URL* is alternatively referred to as the SLS URL, Single Logout Service URL, or the Logout URL.
Sp Certificate	Enable this option and import the SP certificate for authentication request signing by the SP. **Note**: This option is disabled by default.
Configure Identity Provider An IdP provides SAML assertions for the service provider and redirects the user's browser back to the service provider web server.	

Log in to the IdP to find the following information.

Type	Select either *Fortinet Product* or a *Custom* IdP.
IdP Address	The IdP address. **Note**: This option is only available when the *Type* is *Fortinet Product*.
Prefix	Enter the IdP prefix. **Note**: The prefix is appended to the end of the IdP URLs. **Note**: This option is only available when the *Type* is *Fortinet Product*.
IdP Certificate	Select a server certificate to use for the SP. Whenever the configuration changes on the IdP, you need to upload the new certificate reflecting the changes.
IdP entity ID	The IdP's entity ID, for example: `http://www.example.com/saml-idp/xxx/metadata/` **Note**: This option is only available when the *Type* is *Custom*.
IdP single sign-on URL	The IdP's login URL, for example: `http://www.example.com/saml-idp/xxx/login/` **Note**: This option is only available when the *Type* is *Custom*.
IdP single logout URL	The IdP's logout URL, for example: `http://www.example.com/saml-idp/xxx/logout/` **Note**: This option is only available when the *Type* is *Custom*.
Additional Saml Attributes FortiPAM looks for the attributes to verify authentication attempts. Configure your IdP to include the attributes in the SAML attribute statement.	
Attribute used to identify users	Enter the SAML attribute used to identify the users.
Attribute used to identify groups	Enter the SAML attribute used to identify the groups.
AD FS claim	Enable AD FS claim. **Note**: This option is disabled by default.
User claim type	From the dropdown, select a user claim type (default = `User Principal Name`).
Group claim type	From the dropdown, select a group claim type (default = `User Group`).

3. In the *Review* tab, verify the information you entered and click *Submit* to create the SAML SSO server.

Use the pen icon to edit tabs.

Alternatively, use the CLI commands to configure an IdP.

CLI configuration to set up a SAML IdP - example**:**

```
config user saml
   edit <SAML Name>
      set entity-id "http://<PAM_VIP>/saml/metadata/"
      set single-sign-on-url "https://<PAM_VIP>/XX/YY/ZZ/saml/login/"
      set single-logout-url "https://<PAM_VIP>/remote/saml/logout/"
      set idp-entity-id "http://<iDP URL>/<idp_entity_id>"
      set idp-single-sign-on-url "https://<iDP_URL>/<sign_on_url>"
      set idp-single-logout-url "https://<iDP_URL>/<sign_out_url>"
      set idp-cert <iDP Certificate>
      set user-name "username"
      set group-name "group"
      set digest-method sha256
   next
end
config firewall access-proxy
   edit "fortipam_access_proxy"
      set vip "fortipam_vip"
      config api-gateway
         edit 4
            set service samlsp
            set saml-server "fortipam-saml-sso-server"
         next
      end
   next
end
config authentication scheme
   edit "fortipam_saml_auth_scheme"
      set method saml
      set saml-server "fortipam-saml-sso-server"
   next
end
config authentication rule
   edit "fortipam_saml_auth_rule" #Create a new rule and move it above the default
        "fortipam_auth" rule.
      set srcaddr "all"
      set dstaddr "saml_auth_addr"
      set ip-based disable
      set active-auth-method "fortipam_saml_auth_scheme"
      set web-auth-cookie enable
   next
   edit "fortipam_auth"
      set srcaddr "all"
```

```
      set ip-based disable
      set active-auth-method "fortipam_auth_scheme"
      set web-auth-cookie enable
   next
end
```

CLI configuration to enable SAML authentication on the login page - example

```
config system global
   set saml-authentication enable
end
```

To log in to FortiPAM as a SAML user:

1. On the login page, from the *Local* dropdown, select *SAML*.
2. Select *Continue* to open the SAML login page.
3. Enter the username and password to log in to FortiPAM.

RADIUS servers

RADIUS servers can be configured in *User Management*.

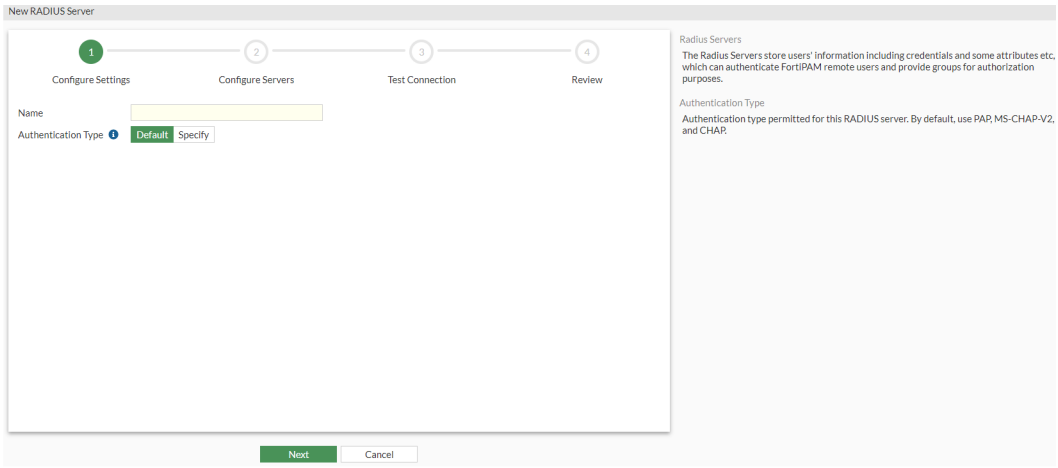
The RADIUS servers store users' information including credentials and some attributes. This information can authenticate FortiPAM remote users and provide groups for authorization.

The *Radius servers* tab contains the following options:

Create	Select to create a new RADIUS server.
Edit	Select to edit the selected RADIUS server.
Clone	Select to clone the selected RADIUS server.
Delete	Select to delete the selected RADIUS servers.
Search	Enter a search term in the search field, then hit `Enter` to search the RADIUS server list. To narrow down your search, see Column filter.

To create a RADIUS server:

1. Go to *User Management* > *Radius Servers*, and select *Create*.
   The *New RADIUS Server* wizard opens.



2. Enter the following information, and click *Next* after each tab:

Configure Settings	
Name	The name of the RADIUS server.
Authentication Type	Select either *Default* or *Specify*. If *Specify* is selected, from the dropdown, select from the following authentication types: • *CHAP*: Challenge Handshake Authentication Protocol. • *MS-CHAP*: Microsoft Challenge Handshake Authentication Protocol. • *MS-CHAP-V2*: Microsoft Challenge Handshake Authentication Protocol version 2. • *PAP*: Password Authentication Protocol.
Configure Servers	
Primary Server	The access request is always be sent to the primary server first. If the request is denied with an `Access-Reject`, then the user authentication fails.
IP/Name	The IP address or the FQDN.
Secret	The pre-shared passphrase used to access the RADIUS server.
Secondary Server	If there is no response from the primary server, the access request is sent to the secondary server.
IP/Name	The IP address or the FQDN.
Secret	The pre-shared passphrase used to access the RADIUS server.

3. Click *Test connection* to test the connection to the RADIUS server.
   If the credentials to the server are valid, it shows *Successful*.
4. In the *Review* tab, verify the information you entered and click *Submit* to create the RADIUS server.

Use the pen icon to edit tabs.

Alternatively, use the CLI commands to create RADIUS servers.

CLI configuration to set up a RADIUS server - example**:**

```
config user radius
   edit <radius_server_name>
      set server <server_ip>
      set secret <secret>
   next
end
config authentication scheme
   edit "fortipam_auth_scheme"
      set method form
      set user-database "local-admin-db" <radius_server_name>
   next
end
```

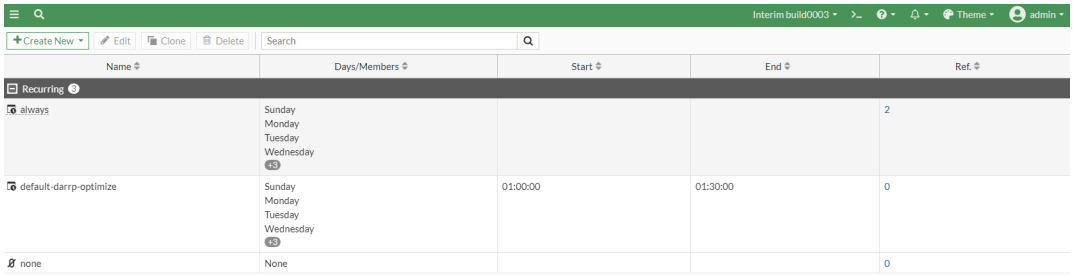
Setting up RADIUS authentication includes the following steps:

1. Configure the RADIUS server. Configuring a RADIUS server.
2. Adding the RADIUS server to a user group. User groups on page 171.
3. Configuring a RADIUS user. Creating a user on page 159.

Schedule

Schedule can be configured in *User Management*.

Set up a schedule to configure when the users can connect to FortiPAM.

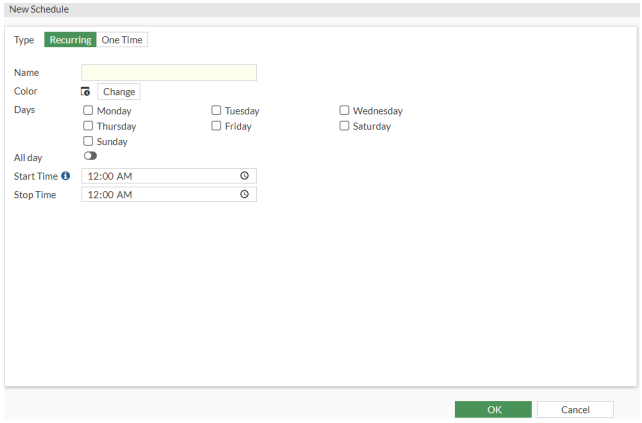


The *Schedule* tab contains the following options:

Create	Select to create a new schedule.
Edit	Select to edit the selected schedule.
Clone	Select to clone the selected schedule.
Delete	Select to delete the selected schedules.
Search	Enter a search term in the search field, then hit `Enter` to search the schedule list.

To create a schedule:

1. Go to *User Management* > *Schedule*.
2. From the *Create* dropdown, select *Schedule*.
   The *New Schedule* window opens.



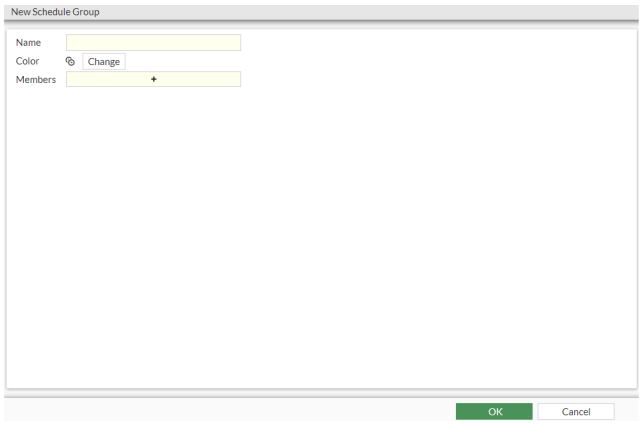
3. In the *New Schedule* window, enter the following information:

Type	Select either *Recurring* or *One Time*.
Name	The name of the schedule.
Color	Select *Change* and then select a color.
Days	Select the days of the week when the schedule applies. **Note**: This option is only available when the *Type* is *Recurring*.
All day	Enable to apply the schedule all day. **Note**: This option is only available when the *Type* is *Recurring*.
Start Date	Enter the start date and time. Alternatively, select the calendar icon and then select a date. Similarly, select the clock icon and then select a time. **Note**: This option is only available when the *Type* is *One Time*.
Start Time	Enter the start time. Alternatively, select the clock icon and then select a start time. **Note**: This option is only available when the *Type* is *Recurring* and *All day* is disabled.
End Date	Enter the end date and time. Alternatively, select the calendar icon and then select a date. Similarly, select the clock icon and then select a time. **Note**: This option is only available when the *Type* is *One Time*.
Stop Time	Enter the stop time. Alternatively, select the clock icon and then select a stop time.  If the stop time is set earlier than the start time, the stop time is the same time the next day. **Note**: This option is only available when *Type* is *Recurring* and *All day* is disabled.
Pre-expiration event log	Select to create an event log *Number of days* before the *End Date*. **Note**: This option is only available when the *Type* is *One Time*.
Number of days before	Enter the number of days (1 - 100, default = 3). **Note**: This option is only available when the *Type* is *One Time* and *Pre-expiration event log* is enabled.

4. Click *OK*.

To create a schedule group:

1. Go to *User Management* > *Schedule*.
2. From the *Create* dropdown, select *Schedule Group*.
   The *New Schedule Group* window opens.



3. In the *New Schedule* window, enter the following information:

Name	The name of the schedule group.
Color	Select *Change* and then select a color.
Members	From the dropdown, select +, and in *Select Entries*, select members. If a new schedule is required, select *Create* then select the type of schedule to create a new schedule. Use the search bar to look for members. Use the pen icon next to a schedule to edit the scheudle.

4. Click *Close*
5. Click *OK*.

FortiTokens

Go to *User Management* > *FortiTokens* to view a list of configured FortiTokens.

To access the *FortiTokens* page, you require *Read* or higher permission to *User Groups*, *Ldap Servers*, *Saml Single Sign-On*, and *Radius Servers*. See Role on page 174.

For each FortiToken; type, serial number, status, user, drift, and comments are displayed by default.

To add the *License* column, click *Configure Table* when hovering over table headers, select *License*, and click *Apply*.

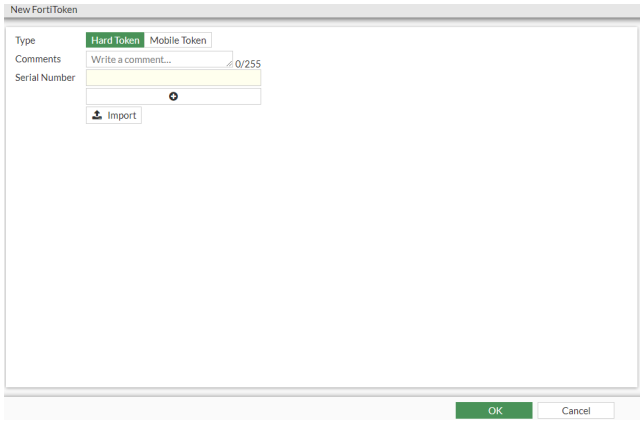
By default, two FortiTokens are available.

The following information is shown on the *FortiTokens* tab:

Create New	Create a new FortiToken.
Edit	Edit the selected FortiToken.
Delete	Delete the selected FortiToken(s).
Activate	Activate the selected FortiToken(s).
Provision	Provision the selected FortiToken(s).
Refresh	Refresh FortiToken(s).
Search	Search the FortiToken list.

To add FortiTokens:

1. Go to *User Management* > *FortiTokens*, and select *Create*.
   The *New FortiToken* window opens.



2. Enter the following information:

Type	The token type: • *Hard Token* • *Mobile Token*
Comments	Optionally, enter comments about the token. **Note**: This option is only available when the *Type* is *Hard Token*.
Serial Number	The FortiToken serial number.  To add multiple FortiTokens, select + and enter a new serial number. **Note**: This option is only available when the *Type* is *Hard Token*.
Activation Code	The activation code. **Note**: This option is only available when the *Type* is *Mobile Token*.
Import	Select the option to import multiple tokens by selecting one of the following and clicking *OK*: • *Serial Number File*: Select *Upload* to load a CSV file that contains token serial numbers.  FortiToken devices have a serial number barcode on the m used to create the import file. • *Seed File*: Select *Upload* to load a CSV file that contains token serial numbers, encrypted seeds, and IV values. **Note**: This option is only available when the *Type* is *Hard Token*.

3. Click *OK*.

Monitoring FortiTokens

You can also view the list of FortiTokens, their status, token clock drift, and which user they are assigned to from the FortiToken list found at *User Management* > *FortiTokens*.

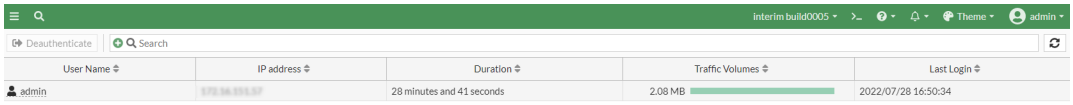
Monitoring

Go to *Monitoring* to access the following tabs:

User monitor

The *User Monitor* tab in *Monitoring* displays all the logged-in users along with information such as their role, logged-in IP address, the duration they have logged in for, traffic volume, and the timestamp of when they logged in. It is a helpful tool for monitoring the overall activities of the users on FortiPAM. For example, if the administrator sees an unusual amount of traffic from a specific user. It could indicate that a risky operation is being performed, and the administrator may deauthenticate the user if the administrator deems the user is a malicious actor.

For every login; username, IP address, duration, traffic volume, and the last login date and time are displayed.



The *User Monitor* tab contains the following options:

Deauthenticate	Select to deauthenticate the selected users.
Search	Enter a search term in the search field, then hit `Enter` to search the user monitor list. To narrow down your search, see Column filter.
Refresh	To refresh the contents, click the refresh icon.

Active sessions

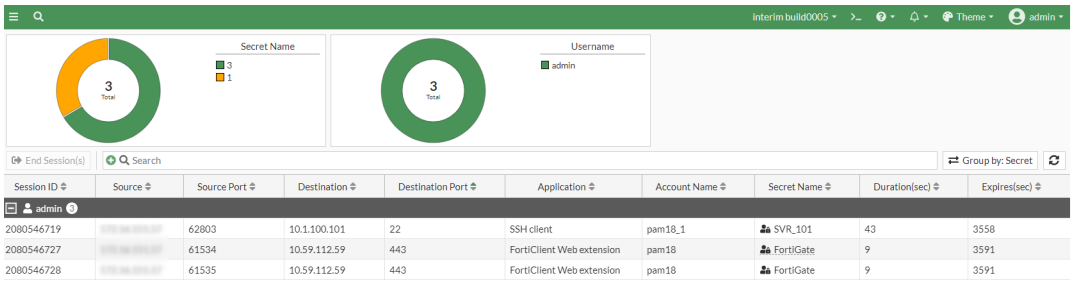
The *Active Sessions* tab in *Monitoring* provides a way to oversee activities of launched secrets from FortiPAM. The page lists out all the launched secrets with information such as source IP: Port, destination IP: Port, the application that is launched and username, etc. Additionally, an *End Session(s)* button is available if the administrator wishes to terminate any of the launched secrets. This monitor is especially powerful in situations where there is malicious activity being conducted by a user because the administrator will be able to terminate the session right away with the *End Session(s)* button to protect the integrity of the secret.

On the top, the following widgets are displayed:

- *Secret Name*: displays the total count of the secrets being used.
- *Username*: displays the total count of the users using secrets.

For every session, the following columns are displayed:

- Session ID
- Source
- Source Port
- Destination
- Destination Port
- Application
- Account Name
- Secret Name
- Duration (sec)
- Expires (sec)



The *Active Sessions* tab contains the following options:

End Session(s)	Select to terminate the selected sessions.
Search	Enter a search term in the search field, then hit `Enter` to search the active sessions list. To narrow down your search, see Column filter.
Group by	Select to group the active sessions by either username or secret.
Refresh	To refresh the contents, click the refresh icon.

Log & report

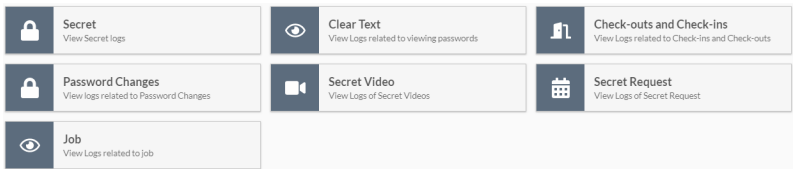
Logging and reporting are valuable components to help you understand what is happening on your network and to inform you about network activities, such as system and user events.

Reports show the recorded activity in a more readable format. A report gathers all the log information that it needs, then presents it in a graphical format with a customizable design and automatically generated charts showing what is happening on the network.

Go to *Log & Report* to access the following tabs:

Secret

Go to *Secret* in *Log & Report* to see logs related to the following:



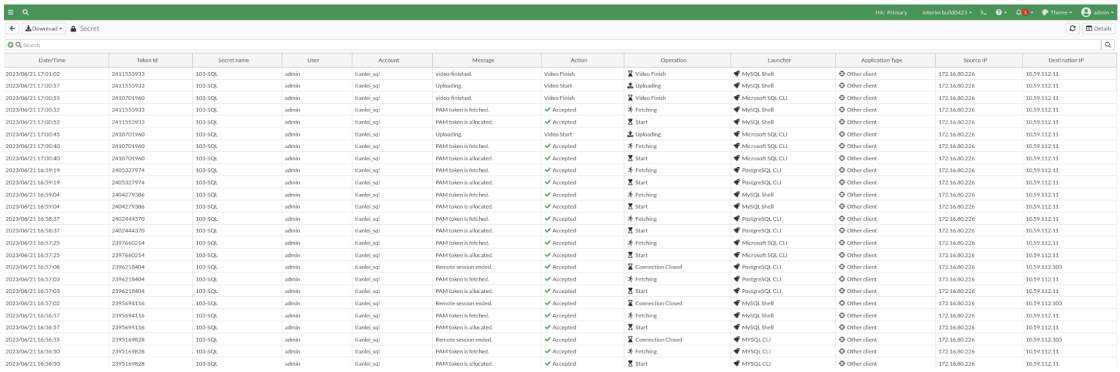
The following options are available in the tabs:

Back (←)	Go back to *Secret*.

Download	From the dropdown in *Secret* and *Secret Video*: • Select *Log* to export the selected secret session log to your computer as a text file named as *secret-xyz-YYYY_MM_DD.txt*. • Having selected a video log labelled as *Video Finish*, from the dropdown, select *Video* to download the secret video in `WebM` format. In tabs except *Secret* and *Secret Video*, select to export the selected secret session log to your computer as a text file named as `secret-xyz-YYYY_MM_DD.txt`.
Refresh	To refresh the contents, click the refresh icon.
Details	Select to see details for the selected log entry.
Search	Enter a search term in the search field, then hit `Enter` to search the secret video list. To narrow down your search, see Column filter.

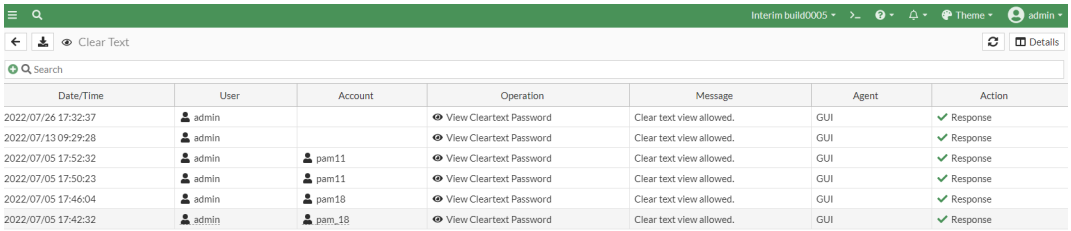
Secret

Selecting *Secret* opens all the secret logs. Different subcategories of secret logs are displayed when you click on a secret log.



Clear Text

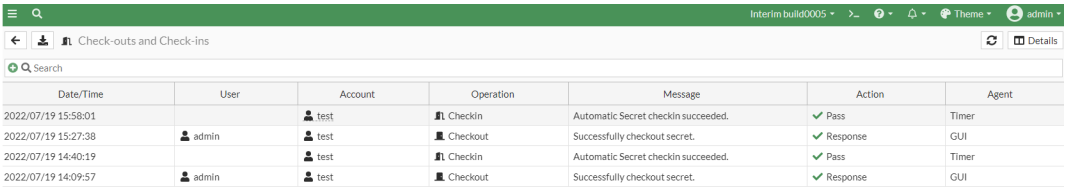
Selecting *Clear Text* shows logs related to viewing passwords. This category of the secret log shows all the information related to the launching of a secret, uploading of a video, termination of a launched session, and status of a FortiPAM token.



Date/Time	User	Account	Operation	Message	Agent	Action
2022/07/26 17:32:37	admin		View Cleartext Password	Clear text view allowed.	GUI	Response
2022/07/13 09:29:28	admin		View Cleartext Password	Clear text view allowed.	GUI	Response
2022/07/05 17:52:32	admin	pam11	View Cleartext Password	Clear text view allowed.	GUI	Response
2022/07/05 17:50:23	admin	pam11	View Cleartext Password	Clear text view allowed.	GUI	Response
2022/07/05 17:46:04	admin	pam18	View Cleartext Password	Clear text view allowed.	GUI	Response
2022/07/05 17:42:32	admin	pam_18	View Cleartext Password	Clear text view allowed.	GUI	Response

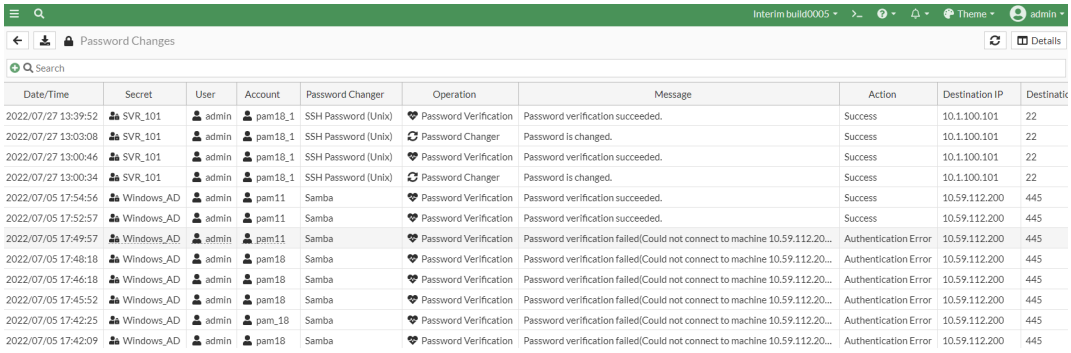
Check-outs and Check-ins

Selecting *Check-outs and Check-ins* shows logs related to password check-ins and check-outs. It displays all the information related to secret check-out and check-in.



Password Changes

Selecting *Password Changers* shows logs related to password changers. It displays all the information about when a password changer is triggered on a secret. It indicates whether the operation is successful and who initiated the operation. Operations such as password verification or change of password are recorded here.

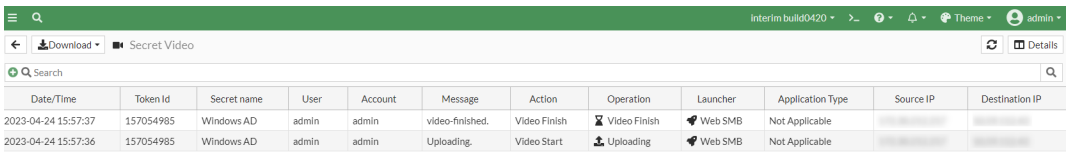


Secret Video

Selecting *Secret Video* shows logs related to secret videos. This category of the secret log shows all the videos of launched secrets from FortiPAM. It is helpful to assist in auditing a user's behavior on the secret, ensuring that no malicious activity is performed.

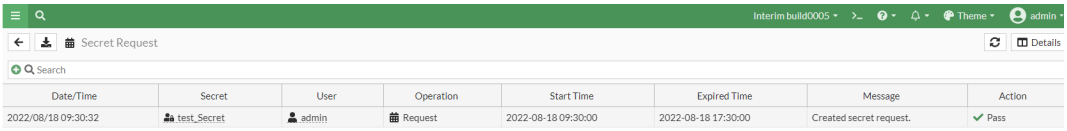
To view a recorded video of a launched secret, select the log with the operation labelled as *Video Finish*, then click the *Details* button located at the right of the menu button. Once the slider opens up, the administrator can see the video player.

To download a recorded video of a launched secret, select the log with the operation labelled as *Video Finish*, then from the *Download* dropdown at the top, select *Video*. The video is downloaded in `WebM` format.



Secret Request

Selecting *Secret Request* shows logs related to secret requests. This category of the secret log shows all the information related to a secret that requires secret approval. It indicates when a request is submitted for a secret or when a request is approved or denied.



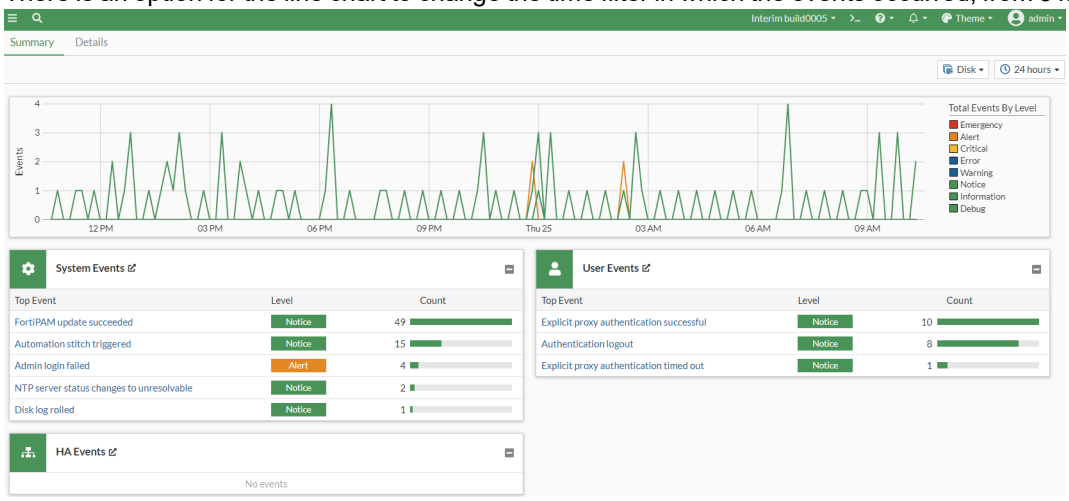
Job

Selecting *Job* shows all logs related to jobs. This category of secret log keeps track of all the events related to an execution of a job on a secret. This includes the job name, the user who initiated the job, the type of the job, and whether the job is executed successfully.

Events

The following two tabs are available in *Events*:

- *Summary*
  The *Summary* tab displays the top five most frequent events in each type of event log and a line chart to show aggregated events by each severity level. Clicking on a peak in the line chart will display the specific event count for the selected severity level.
  There is an option for the line chart to change the time filter in which the events occurred, from 5 minutes to 7 days.



  The *System Events* log contains events such as:
  - Upgrade and downgrade of the system
  - Change of system configuration, such as timezone and FortiPAM recording settings
  - Deletion of outdated video files
  - Report generation

- Reload of AntiVirus database

  And more.

The *User Events* log contains events such as:

- IP address and time when the user logs in or logs out
- Login failure reason
- User login as a normal user or API user

  And more.

The *HA Events* log contains events such as:

- Change in HA clusters
- Synchronization status with the HA peers

  And more.

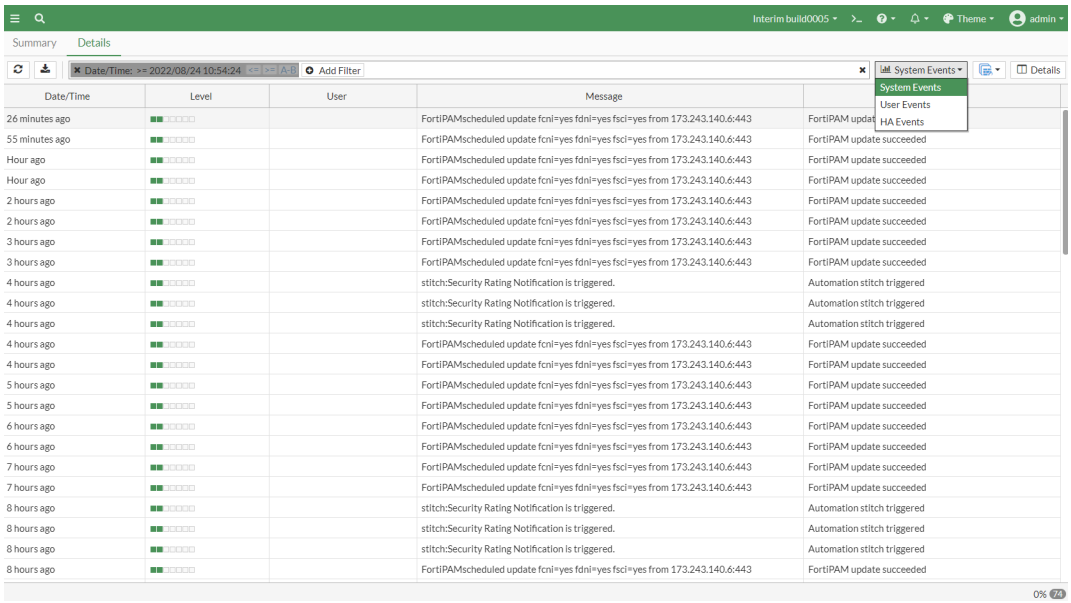
The following options and widgets are available in the *Summary* tab:

Disk	Logs sourced from the disk.
Time frame	From the dropdown, select from the following time filters: • *5 minutes* • *1 hour* • *24 hours* • *7 days*
System Events	Top system events by count.
User Events	Top user events by count.
HA Events	Top HA events by count.

In *System Events*, *User Events*, or *HA Events* widgets, select an event to open the corresponding details tab with all the logs for the event listed in a table.

- *Details*

  The tab displays the related information of each log for a specific event type. The event type can be toggled with the event type dropdown located right of the search bar. Different filters can be added, such as date/time to filter logs in a time range.



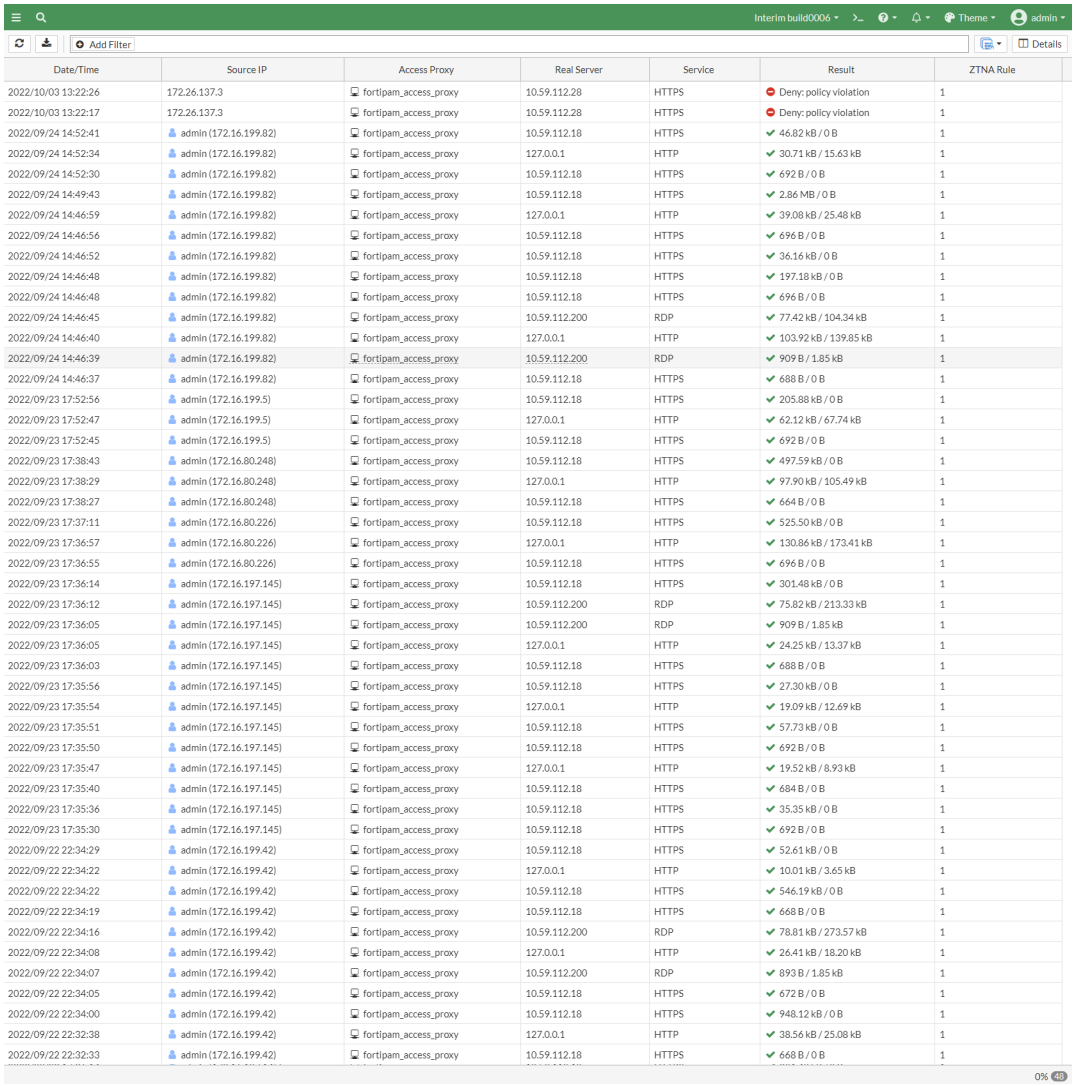
The following options are available in the *Details* tab:

Refresh	To refresh the contents, click the refresh icon.
Download log	Select to export the selected log entry to your computer as a text file.
+Add Filter	From the dropdown, select a filter, select or add additional details about the filter to be used and hit `Enter`. **Note**: Logs can be filtered by date and time. The log viewer can be filtered with a custom range or with specific time frames.  Time frame settings for each *Log & Report* page are independent. For example, changing the time frame on the *System Events* page does not automatically change the time frame on the *User Events* and *HA Events* pages.
System Events	From the dropdown, select from the following event types to display: • *System Events* • *User Events* • *HA Events*
Log location	Logs sourced from the FortiPAM disk.
Details	Select a log entry and then select *Details* to see more information about the log.

ZTNA

Go to ZTNA in *Log & Report* to see ZTNA related logs.

The ZTNA log keeps track of ZTNA related traffics. This can include when a ZTNA rule cannot be matched, an API gateway cannot be matched, or when a secret configured with device permission fails to connect.



The following options are available in the *ZTNA* tab:

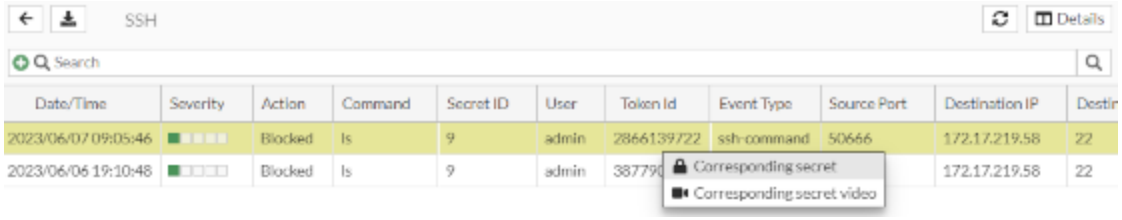
Refresh	To refresh the contents, click the refresh icon.
Download Log	Select to export the selected ZTNA log to your computer as a text file.
+Add Filter	From the dropdown, select a filter, select or add additional details about the filter to be used and hit `Enter`. **Note**: Logs can be filtered by date and time. The log viewer can be filtered with a custom range or with specific time frames.
Log location	The FortiPAM disk.
Details	Select to see details for the selected log entry.

SSH

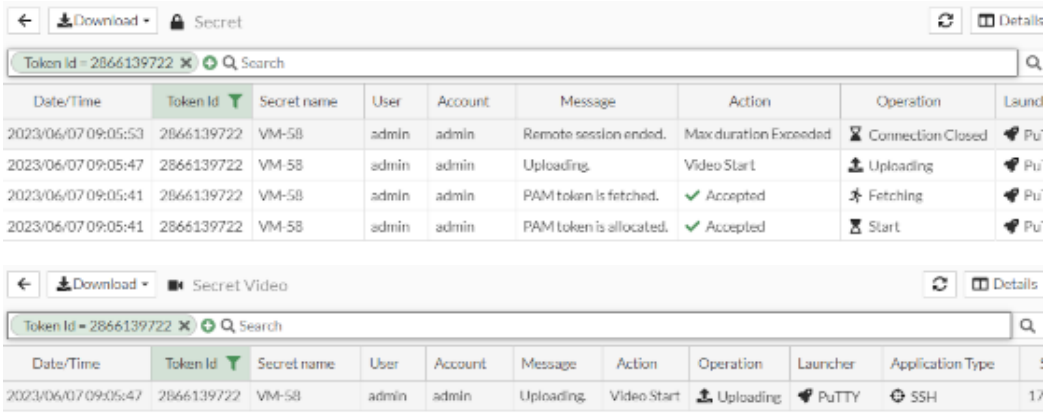
Go to *SSH* in *Log & Report* to see SSH related logs.

For each SSH log, the following columns are displayed:

- Date/time
- Severity
- Action
- Command
- Secret ID
- User
- Token Id
- Event Type
- Group
- Source Port
- Destination IP
- Destination Port
- Protocol



Selecting the *Corresponding secret* or the *Corresponding secret video* buttons when you right-click an SSH log takes you to the corresponding secret log or the secret video log, respectively.



The SSH log keeps track of all the events related to the SSH filter profile. It contains information such as the severity of a command, the destination IP and port used to execute the command, and the action associated with the log. The action

may be *Blocked*, indicating the command has been blocked from executing on the secret or *Passthrough*, representing it is allowed to execute on the secret.

The following options are available in the *SSH* tab:

Back ()	Go back to *SSH*.
Download log	Select to export the selected SSH log to your computer as a text file.
Refresh	To refresh the contents, click the refresh icon.
Details	Select to see details for the selected log entry.
Search	Enter a search term in the search field, then hit `Enter` to search the secret video list. To narrow down your search, see Column filter.

Antivirus

Go to *Log & Report* > *Antivirus* to see logs related to antivirus.

The antivirus log records when, during the antivirus scanning process, the FortiPAM unit finds a match within the antivirus profile, which includes the presence of a virus or grayware signature.

The following options are available in the *Antivirus* tab:

Refresh	To refresh the contents, click the refresh icon.
Download Log	Select to export the selected antivirus logs to your computer as a text file.
+Add Filter	From the dropdown, select a filter, select or add additional details about the filter to be used and hit `Enter`. **Note**: Logs can be filtered by date and time. The log viewer can be filtered with a custom range or with specific time frames.
Log location	The FortiPAM disk.
Details	Select to see details for the selected log entry.

Date leak prevention

Go to *Log & Report* > *Data Leak Prevention* to see logs related to DLP.

The data leak prevention (DLP) log provides valuable information about the sensitive data trying to get through to your network as well as any unwanted data trying to get into your network.

The following options are available in the *Data Leak Prevention* tab:

Refresh	To refresh the contents, click the refresh icon.

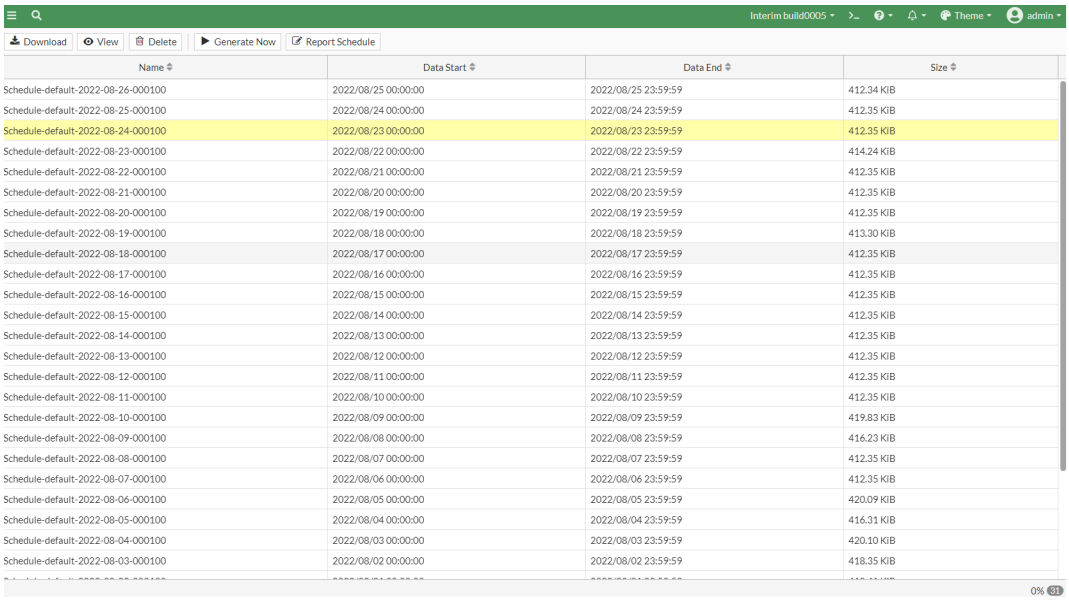
Download Log	Select to export the selected DLP logs to your computer as a text file.
+Add Filter	From the dropdown, select a filter, select or add additional details about the filter to be used and hit `Enter`. **Note**: Logs can be filtered by date and time. The log viewer can be filtered with a custom range or with specific time frames.
Log location	The FortiPAM disk.
Details	Select to see details for the selected log entry.

Reports

Reports in *Log & Reports* show a list of audit reports generated to comply with audit requirements. The reports include:

- User Login: Top successful logins, top failed logins, and top failed logins by reason.
- System: Maintenance mode, top maintenance mode activation by user, glass breaking mode, top glass breaking mode activation by user, and HA mode.
- Secret (includes the following):
  - Secret launch success
  - Top secret launch success by secret name
  - Top secret launch success by secret name and user
  - Password change
  - Top successful password change by secret name
  - Top successful password change by secret name and user
  - Top failed password change by secret name
  - Top failed password change by secret name and reason
  - Top failed password change by secret name, user and reason
  - Password verification
  - Top successful password verification by secret name
  - Top successful password verification by secret name and user
  - Top failed password verification by secret name
  - Top failed password verification by secret name and reason
  - Top failed password verification by secret name, user and reason
  - Clear text view
  - Top clear text view by secret name
  - Top clear text view by secret name and user

For each report; name, data start, data end, and the size are displayed.



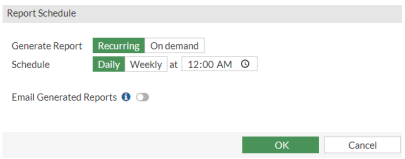
The *Reports* tab contains the following options:

Download	Select to export the selected report to your computer as a pdf file.
View	Select to view the selected report.
Delete	Select to delete the selected reports.
Generate Now	Select to regenerate a report and click OK in the *Confirm* window. Regenerating a report may take several minutes.
Report Schedule	Select to schedule a generating a report. See Schedule generating reports on page 211.

Schedule generating reports

To schedule generating a report:

1. Go to *Log & Report* > *Reports* and select *Report Schedule*.
   The *Report Schedule* dialog opens.



2. In *Generate Report*, select from the following two options:
   a. *Recurring*: Select to generate reports periodically.
   b. *On demand*: Select to generate reports on demand.

3. In *Schedule*, select either *Daily* or *Weekly*:
   a. *Daily*: Enter the time or select the clock icon and then select the time from the dropdown.
   b. *Weekly*: Enter the time or select the clock icon and then select the time from the dropdown. In the *Day* dropdown, select a day of the week.

   Note: *Schedule* is only available when *Generate Report* is set as *Recurring*.
4. Enable *Email Generated Reports* and enter the recipient email addresses where the reports are sent.

Before enabling the option, you must configure an email messaging server in *System* > *Settings* and configure a username in *Email Alert Settings*.

See Email alert settings on page 215.

Note: The option is disabled by default.

5. Click *OK*.

Customizing reports

FortiPAM allows you to customize reports to display attributes according to your preference.

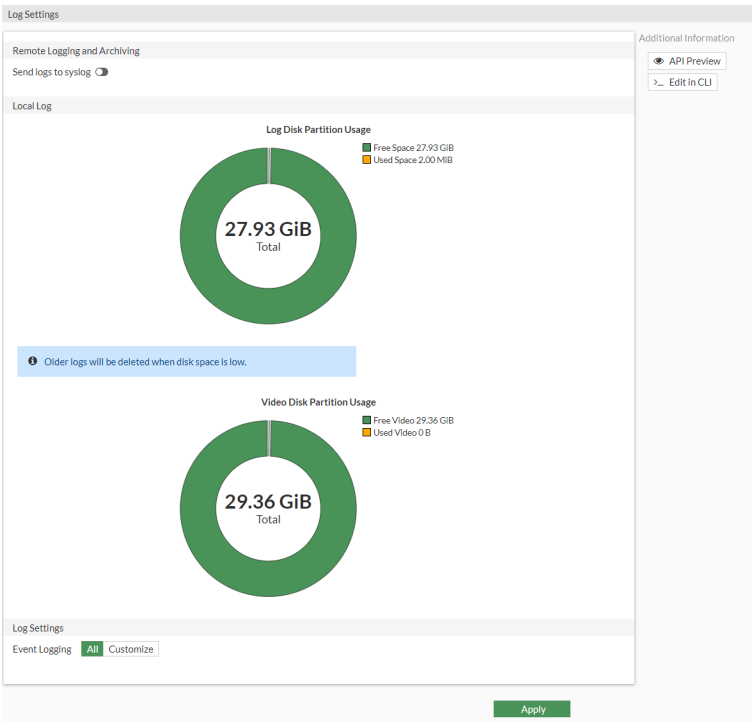
You can change the report attributes from the CLI console only.

CLI configuration to customize report attributes - example

```
config report layout
   edit default
      config body-item #Configure report body items.
         show #By default, a report displays all the available charts.
         delete 301 #Deletes Bandwidth and Application related charts.
      end
end
execute report-config reset
   y #Enter "y" to update the report layout based on the new configuration.
```

Log settings

Log settings determine what information is recorded in logs, where the logs are stored, and how often storage occurs.



Remote Logging and Archiving	
Send logs to syslog	Enable/disable sending logs to syslog. See Configuring parameters to send logs to syslog server on page 214. **Note**: The option is disabled by default.
Local Log	
Log Disk Partition Usage	The disk usage (free and used space).
Video Disk Partition Usage	The video disk partition usage (free and used video disk partition).
Log Settings	
Event Logging	By default, the system logs all the events: system activity, user activity, and HA. You can customize event logging by selecting *Customize* and then unselecting options under *Customize*. **Note**: No event logs are recorded and displayed on the *Log & Report* > *Events* page for unselected events.

Older logs are deleted when disk space is low.

Disabling disk storage

Although it is not suggested that you disable the disk storage, FortiPAM allows you to disable the disk storage via the CLI.

To disable disk storage:

If you intend to disable the disk storage, ensure that the memory storage is enabled to make the log pages work correctly:

```
config log memory setting
   set status enable
end
```

1. In the CLI console, enter the following commands:

```
config log disk setting
   set status disable
end
```

Configuring parameters to send logs to syslog server

To configure parameters to send logs to syslog server:

1. Go to *Log & Report > Log Settings*.
2. In *Additional Information*, select *Edit in CLI*.
   The CLI console opens.
3. Use the following parameters:

status {enable | disable}	Enable/disable remote syslog logging (default = disable).
The following parameters are only available when the `status` is set as `enable`.	
server <string>	Address of the remote syslog server.
mode {legacy-reliable | reliable | udp}	The remote syslog logging mode: • `legacy-reliable`: Legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog). • `reliable`: Reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP). • `udp`: syslogging over UDP (default).
port <integer>	The server listening port number (default = 514, 0 - 65535).
facility {kernel | user | mail | daemon | auth | syslog | lpr | news | uucp | cron | authpriv | ftp | ntp | audit | alert | clock | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7}	The remote syslog facility (default = `local7`): • `kernel`: Kernel messages. • `user`: Random user-level messages. • `mail`: Mail system. • `daemon`: System daemons. • `auth`: Security/authorization messages. • `syslog`: Messages generated internally by syslog. • `lpr`: Line printer subsystem. • `news`: Network news subsystem. • `uucp`: Network news subsystem. • `cron`: Clock daemon.

	• `authpriv`: Security/authorization messages (private). • `ftp`: FTP daemon. • `ntp`: NTP daemon. • `audit`: Log audit. • `alert`: Log alert. • `clock`: Clock daemon. • `local0 ... local7`: Reserved for local use.
source-ip <string>	The source IP address of syslog.
format {cef | csv | default | rfc5424}	The log format: • `cef`: CEF (Common Event Format) format. • `csv`: CSV (Comma Separated Values) format. • `default`: Syslog format (default). • `rfc5424`: Syslog RFC5424 format.
priority {default | low}	The log transmission priority: • `default`: Set Syslog transmission priority to default (default). • `low`: Set Syslog transmission priority to low.
max-log-rate <integer>	The syslog maximum log rate in MBps (default = 0, 0 - 100000 where 0 = unlimited).
interface-select-method {auto | sdwan | specify}	Specify how to select outgoing interface to reach the server: • `auto`: Set outgoing interface automatically (default). • `sdwan`: Set outgoing interface by SD-WAN or policy routing rules. • `specify`: Set outgoing interface manually.

4. After adjusting the parameters, click *x* to close the CLI console.

Email alert settings

Enabling *Email Alert Settings* allows FortiPAM to send alert emails to administrators.

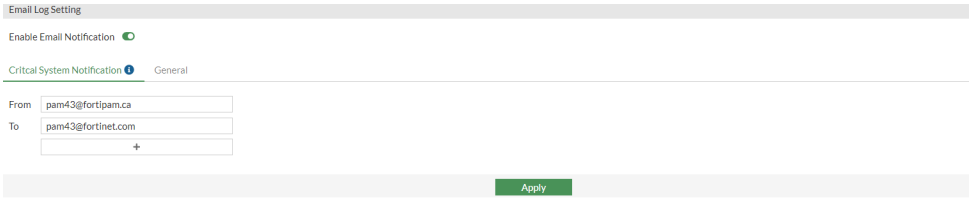
To configure a mail service:

1. Go to *System* > *Settings*.
2. You can set up the email service from the *Email Service* pane in the *Advanced* tab. See Settings on page 237.
   By default, the Fortinet mail server is used. You can set up a custom email server by enabling *Use custom settings* in the *Email Service* pane in the *Advanced* tab and configuring the related settings.

To enable Email alert setting:

1. Go to *Log & Report* > *Email Alert Settings*, and select *Enable email notification*.
   The following two tabs are available:

- *Critical System Notification*: Includes setting up glass breaking and license expiring notifications.
- *General*



2. In the *Critical System Notification* tab, enter the following information:

From	The email address of the sender.
To	The email address of the receiver. Select + to add additional email addresses.

3. In the *General* tab, enter the following information:

From	The email address of the sender. fortipam@example.com
To	The email address of the receiver. admin1@example.com admin2@example.com Select + to add additional email addresses.
Alert parameter	Select from the following two options: • *Events*: Alerts are sent when an event occurs, e.g., system or user events. See Events on page 204. • *Severity*: From the dropdown, select the minimum level of severity at which the alerts are sent.
Interval	The time interval at which the alerts are sent, in minutes (default = 5, 1-99999). **Note**: The option is only available when the *Alert parameter* is set as *Events*.
Security **Note**: The pane is only available when the *Alert parameter* is set as *Events*.	
Virus detected	Enable/disable sending alerts when virus detected.
Administrative **Note**: The pane is only available when the *Alert parameter* is set as *Events*.	
Configuration change	Enable/disable sending alerts when a configuration is changed.

	Note: The option is disabled by default.
HA status change	Enable/disable sending alerts when the HA status changes. **Note**: The option is disabled by default.

4. Click *Apply*.

Email alert when the glass breaking mode is activated - example

To set up email alerts when the glass breaking mode is activated:

1. Ensure that *Email Service* is set up in *System* > *Settings*. See Settings on page 237.
2. Go to *Log & Report* > *Email Alert Settings*, and select *Enable email notification*.
3. In the *Critical System Notification* tab:
   a. In *From*, enter the email address of the sender.
   b. In *To*, enter the email address of the receiver.
4. Click *Apply*.

Setting up an email alert for glass breaking excludes other important notifications, e.g., administrative change (configuration and HA status) and security (virus detection).

Debug settings

Customer Support may request a copy of your debug logs for troubleshooting.

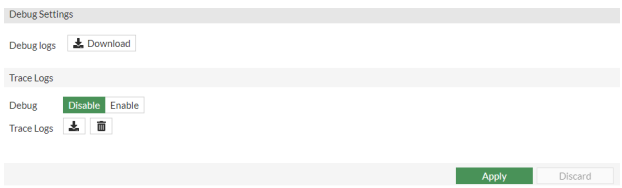
Go to *Log & Report* > *Debug Settings* and click *Download* in the *Debug Settings* pane to download the debug logs for troubleshooting.

Trace logs

FortiPAM trace GUI tool is available in the *Trace Logs* pane in *Log & Report* > *Debug Settings*.

To set up and download trace logs:

1. Go to *Log & Report* > *Debug Settings*.
   The *Debug Settings* window opens.

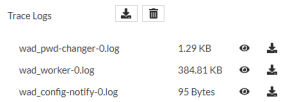


2. In the *Trace Logs* pane, enter the following information:

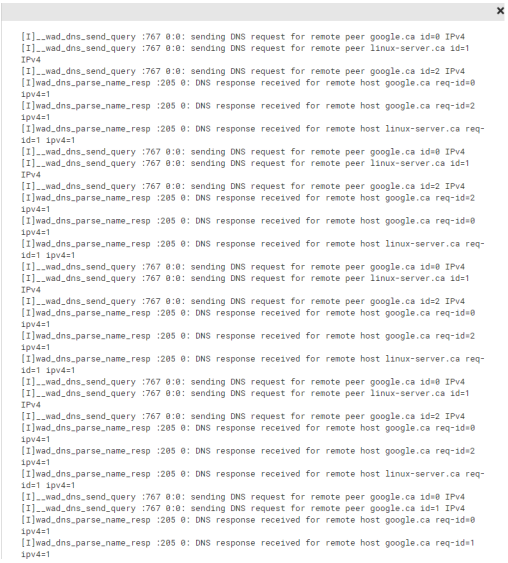
Debug	Enable/disable trace logs. **Note**: The option is disabled by default.
Category	Select + and then select categories to trace from the *Select Entries* window. Click *Close* once you have selected all the required trace categories.  Use the search bar to look up a trace category. **Note**: The option is only available when *Debug* is enabled.
Debug Level	From the dropdown, select a debug level for the trace: • *Verbose* • *Info* (default) • *Warning* • *Error* **Note**: The option is only available when *Debug* is enabled.
Filter	From the dropdown, select a filter: • *None* (default) • *Internal* • *TCP Forwarding* • *Both* See FortiPAM HTTP filter on page 290. **Note**: The option is only available when *Debug* is enabled.
Overwrite	Enable/disable overwriting when the file reaches maximum size. **Note**: • The option is disabled by default. • The option is only available when *Debug* is enabled.
Drop Unknown Session	Enable to drop unknown sessions. See FortiPAM HTTP filter on page 290. **Note**: • The option is disabled by default. • The option is only available when *Debug* is enabled.
Maximum File Size	The maximum size for each trace log file, in MB (default = 1, 1 - 10). **Note**: The option is only available when *Debug* is enabled.
Trace Logs	Select from the following two options: • : Download all the trace logs. • : Clear all the log traces.

3. Click *Apply*.
When FortiPAM is recording trace logs, a list of the logs appears in *Trace Logs*. You can download or view a trace log by clicking the eye or the download icon next to the trace log.

Viewing does not stop the trace recording, but downloading turns off the trace recording.



When you click the eye icon next to a trace log, you can view it.



4. When the diagnostic is finished, disable *Debug* to stop recording.

Automation trigger settings

FortiPAM can be configured to perform actions when an event log is triggered. This is in the system automation table.

Automation trigger settings can only be configured via the CLI.

Automation trigger settings via the CLI - Example

To configure automation trigger settings:

1. In the CLI console, enter the following commands:

```
config system automation-trigger
   edit "fold_chg"
      set event-type event-log
      set logid 44547 #from the log id (logid="0100044547) remove the category prefix
      set logic and
      config fields
```

```
        edit 1
           set match regex
           set name "msg"
           set value "E*t"
        next
        edit 2
           set name "user"
           set value "u1"
        next
     end
  next
end
```

If the field is set to match regex, it uses the regular expression to match the field with the `value _name_`. Otherwise, it uses the default match, using `_*_` character as a wildcard.

If the logic is set to `_and_`, all fields must match to trigger the action. Otherwise, if it is set to `_or_`, any field matching triggers the action.

Network

Go to *Network* to configure network related settings for FortiPAM.

The menu provides features for configuring and viewing basic network settings, such as the unit interfaces, static routes, Domain Name System (DNS) options, fabric connectors, and packet capture.

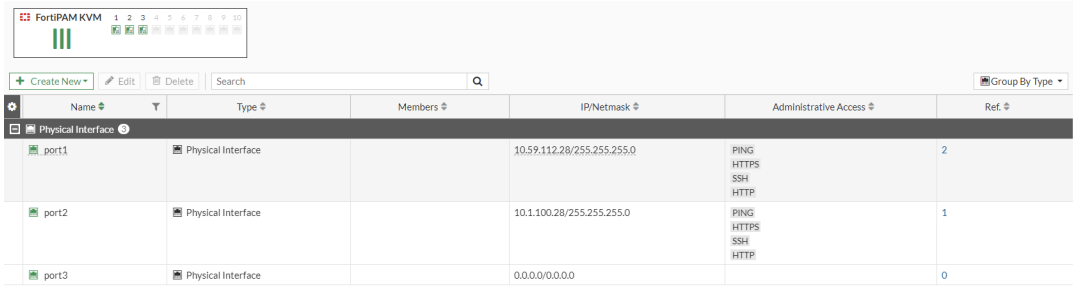
The *Network* tab contains the following tabs:

- Interfaces on page 221
- Static routes on page 225
- DNS settings on page 228
- Fabric Connectors on page 230
- Packet capture on page 234

Interfaces

In *Network* > *Interfaces*, you can configure the interfaces that handle incoming and outgoing traffic.

For each interface/zone; name, type, members, IP/Netmask, administrative access, and references are displayed.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available in the *Interface* tab:

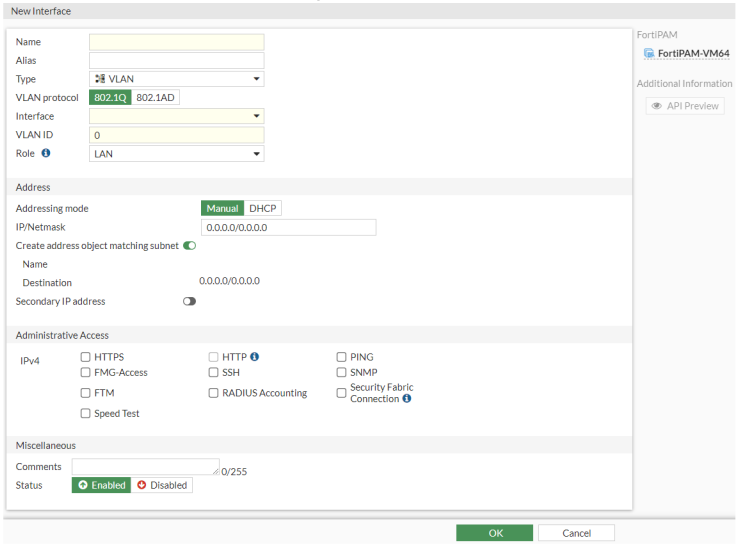
+Create New	Select to create an interface or a zone. See Creating an interface on page 222 and Creating a zone on page 225.
Edit	Select to edit the selected interface or zone.
Delete	Select to delete the selected interfaces or zones.
Search	Use the search bar to look for an interface or a zone.

Group By Type	From the dropdown, group the list of interfaces or zones by type, role, status, or zone. You may also choose to set no grouping.
Refresh	To refresh the contents, click the refresh icon on the bottom-right.

Creating an interface

To create an interface:

1. Go to *Network* > *Interfaces*.
2. From *+Create New*, select *Interface*.
   The *New Interface* window opens.



3. Enter the following information:

Name	Name of the interface.
Alias	Enter an alternate name for a physical interface on the FortiPAM device. This field appears when you edit an existing interface. The alias does not appear in logs. The maximum length of the alias is 25 characters.
Type	From the dropdown, select a configuration type: • *802.3ad Aggregate* • *Redundant Interface* • *VLAN* (default)
VLAN protocol	Select either *802.1Q* or *802.1AD*. **Note**: The field is available when *Type* is set to *VLAN*.
Interface	Select the name of the physical interface that you want to add a VLAN interface to. Once created, the VLAN interface is listed below its physical interface in the Interface list.

	 You cannot change the physical interface of a VLAN interface.  Use the search bar to look for an interface.  Use the pen icon next to an interface to edit the interface. **Note**: The field is available when *Type* is set to *VLAN*.
VLAN ID	Enter the VLAN ID. The VLAN ID can be any number between 1 and 4094 and must match the VLAN ID added by the IEEE 802.1Q-compliant router or switch that is connected to the VLAN subinterface. The VLAN ID can be edited after the interface is added. **Note**: The field is available when *Type* is set to *VLAN*.
Interface members	Select members for some interface types. **Note**: The field is available when *Type* is set to *802.3ad Aggregate* or *Redundant Interface*.
Role	Set the role setting for the interface. Different settings will be shown or hidden when editing an interface depending on the role: • *LAN*: Used to connected to a local network of endpoints. It is default role for new interfaces. • *WAN*: Used to connected to the internet. When WAN is selected, the *Estimated bandwidth* setting is available, and *Create address object matching subnet* is not available. • *DMZ*: Used to connected to the DMZ. • *Undefined*: The interface has no specific role. When selected, *Create address object matching subnet* is not available.
Estimated bandwidth	The estimated WAN bandwidth, in kbps (upstream and downstream). The values can be entered manually, or saved from a speed test executed on the interface. These values are used to estimate WAN usage. **Note**: The option is only available when the *Role* is set as *WAN*.
Address	
Addressing mode	Select the addressing mode for the interface. • *Manual*: Add an IP address and netmask for the interface. • *DHCP*: Get the interface IP address and other network settings from a DHCP server.
IP/Netmask	If *Addressing mode* is set to *Manual*, enter an IPv4 address and subnet mask for the interface.

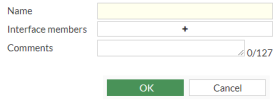
	 FortiPAM interfaces cannot have IP addresses on the same subnet. **Note**: The option is only available when the *Addressing mode* is *Manual*.
Retrieve default gateway from server	Enable to retrieve the default gateway from the server. The default gateway is added to the static routing table. **Note**: The option is enabled by default. **Note**: The option is only available when the *Addressing mode* is *DHCP*.
Distance	Enter the administrative distance for the default gateway retrieved from the DHCP server (default = 5, 1 - 255). *Distance* specifies the relative priority of a route when there are multiple routes to the same destination. A lower administrative distance indicates a more preferred route. **Note**: The option is only available when *Retrieve default gateway from server* is enabled.
Override internal DNS	Enable to use the DNS addresses retrieved from the DHCP server instead of the DNS server IP addresses on the DNS page. **Note**: The option is enabled by default. **Note**: The option is only available when the *Addressing mode* is *DHCP*.
Create address object matching subnet	Enable to automatically create an address object that matches the interface subnet. **Note**: The option is enabled by default. **Note**: The option is available when *Role* is set to *LAN* or *DMZ*.
Secondary IP address	Add additional IPv4 addresses to this interface. **Note**: The option is disabled by default. **Note**: The option is only available when the *Addressing mode* is *Manual*.
Administrative Access	
IPv4	Select the types of administrative access permitted for IPv4 connections to this interface.
Miscellaneous	
Comments	Optionally, enter comments about the source interface.
Status	Enable/disable the source interface.

4. Click *OK*.

Creating a zone

To create a zone:

1. Go to Network > Interface.
2. From *+Create New*, select *Zone*.
   The *New Zone* window opens.



3. Enter the following information:

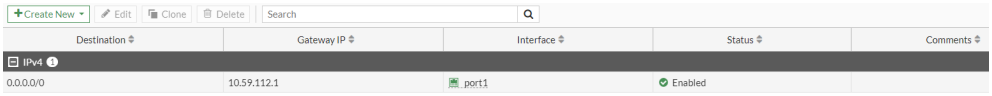
Name	Name of the zone. You can change the name of the zone after creating it.
Interface members	Select the ports to be included in the zone or create new ports. Use the search bar to look for an interface. Use the pen icon next to an interface to edit the interface.
Comments	Optionally, enter a description about the zone.

4. Click *OK*.

Static routes

Go to *Network* > *Static Routing* to see a list of static routes that control the flow of traffic through the FortiPAM device.

For each static route; destination, gateway IP address, interface, status, and comments are displayed.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

The following options are available in the *Static Routes* tab:

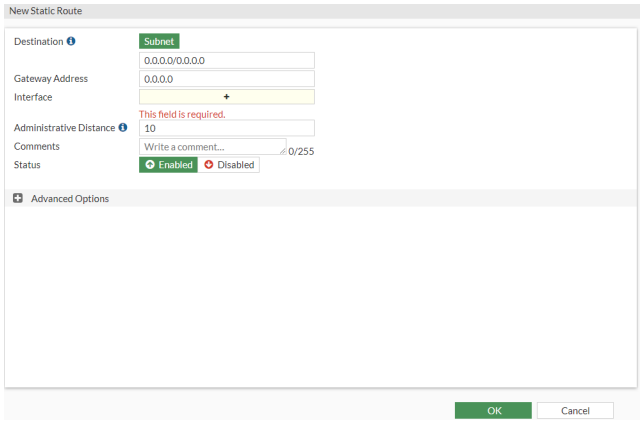
+Create New	From the dropdown, select to create an IPv4 static route. See Creating an IPv4 static route on page 226.

Edit	Select to edit the selected static route.
Clone	Select to clone the selected static route.
Delete	Select to delete the selected static route.
Search	Use the search bar to look for a static route.

Creating an IPv4 static route

To create an IPv4 static route:

1. Go to *Network* > *Static Routes*.
2. Select *Create New* to create a new IPv4 static route.
   The *New Static Route* window opens.



3. Enter the following information:

Destination	The destination IP addresses and network masks of packets that the FortiPAM unit intercepts. Enter the IPv4 address and netmask of the new static route.
Gateway Address	The IP addresses of the next-hop routers to which intercepted packets are forwarded. Enter the gateway IP address for those packets that you intend to intercept. **Note**: *Gateway Address* is unavailable when the *Interface* is *Blackhole*.
Interface	The interface the static route is configured to. Select + and in *Select Entries*, select the interface or create a new interface. A blackhole route is a route that drops all traffic sent to it. Blackhole routes are used to dispose of packets instead of responding to suspicious inquiries. This provides added security since the originator will not discover any information from the target network. Blackhole routes can also limit traffic on a subnet. If some subnet addresses are not in use, traffic to those addresses, which may be valid or malicious, can be directed to a blackhole for added security and to reduce traffic on the subnet.  Use the search bar to look for an interface.  Use the pen icon next to an interface to edit the interface.
Administrative Distance	The number of hops the static route has to the configured gateway. The administrative distance is used to determine the cost of the route. Smaller distances are considered "better" route that should be used when multiple paths exist to the same destination (default = 10, 1 - 255). The route with same distance are considered as equal-cost multi-path (ECMP).
Comments	Optionally, enter a description about the static route.
Status	Enable/disable the static route.
Advanced Options	
Priority	A number for the priority of the static route. Routes with a larger number will have a lower priority. Routes with the same priority are considered as ECMP (default = 1 when creating an IPv4 static route, 1 - 65535).  Priority can only be customized for statically configured route s. The priority of routes dynamically learned from the routing protocols is always 1.

API Preview	The *API Preview* allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. The feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

4. Click *OK*.

To use API preview:

1. Click *API Preview*.
   The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* (enabled by default) to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

DNS settings

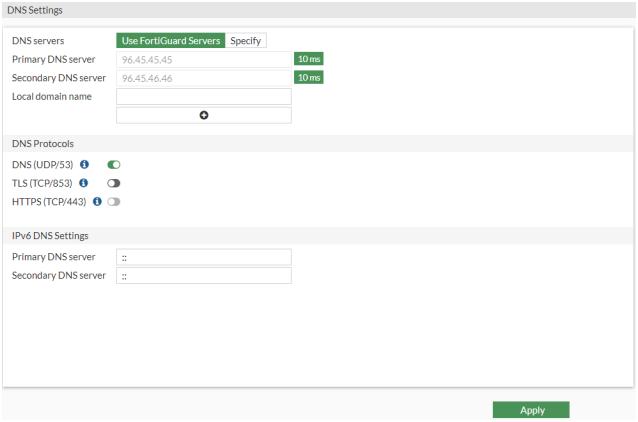
Domain name system (DNS) is used by devices to locate websites by mapping a domain name to a website's IP address.

You can specify the IP addresses of the DNS servers to which your FortiPAM unit connects.

To configure DNS settings, go to *Network* > *DNS Settings*.

To configure DNS settings:

1. Go to *Network* > *DNS Settings*.



2. In the *DNS Settings* window, enter the following information:

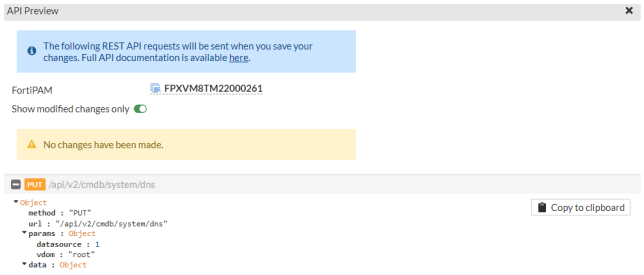
DNS servers	Select *Use FortiGuard Severs* or *Specify*. If you select *Specify*, enter the IP addresses for the primary and secondary DNS servers.
Primary DNS server	Enter the IPv4 or IPv6 address for the primary DNS server. **Note**: For an IPv4 address, the option is only available to edit when *DNS servers* is *Specify*.
Secondary DNS server	Enter the IPv4 or IPv6 address for the secondary DNS server. **Note**: For an IPv4 address, the option is only available to edit when *DNS servers* is *Specify*.
Local domain name	The domain name to append to addresses with no domain portion when performing DNS lookups.  Select + to add additional local domain names.  You can add up to 8 local domain names.
DNS Protocols	
DNS (UDP/53)	Enable or disable the use of clear-text DNS over port 53. **Note**: The option is disabled by default and only available to edit when *DNS servers* is *Specify*.
TLS (TCP/853)	Enable or disable the use of DNS over TLS (DoT). **Note**: The option is enabled by default and only available to edit when *DNS servers* is *Specify*.
HTTPS (TCP/443)	Enable or disable the use of DNS over HTTPS (DoH). **Note**: The option is disabled by default and only available to edit when *DNS servers* is *Specify*.
SSL certificate	From the dropdown, select an SSL certificate or click *Create* to import a certificate (default = `Fortinet_Factory`). SSL certificate is used by the DNS proxy as a DNS server so that the DNS proxy can provide service over TLS as well as normal UDP/TCP.  Use the search bar to look for an SSL certificate.
Server hostname	The host name of the DNS server (default = `globalsdns.fortinet.net`).

You can add up to 4 server hostnames.

3. Click *Apply*.

To use API preview:

1. Click *API Preview*.
   The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.



2. Enable *Show modified changes only* (enabled by default) to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Security fabric

The Security Fabric allows your network to automatically see and dynamically isolate affected devices, partition network segments, update rules, push out new policies, and remove malware.

The Security Fabric is designed to cover the entire attack surface and provide you with complete visibility into your network. It allows you to collect, share, and correlate threat intelligence between security and network devices, centrally manage and orchestrate policies, automatically synchronize resources to enforce policies, and coordinate a response to threats detected anywhere across the extended network. The unified management interface provides you with cooperative security alerts, recommendations, audit reports, and full policy control across the Security Fabric that will give you confidence that your network is secure.

See Fabric Connectors on page 230.

Fabric Connectors

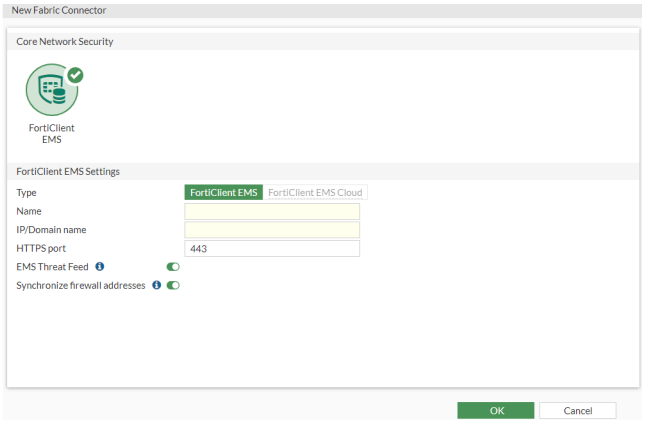
Fabric connectors provide integration with Fortinet products to automate the process of managing dynamic security updates without manual intervention.

In HA and DR setup, the EMS configuration, such as server name and IP, can be synced to secondary and DR nodes. However, secondary and DR nodes need to be authorized by EMS individually. It is recommended that after configuring

HA, admin test failover, log in to the new primary, and follow the same procedure to authorize secondary and DR nodes on the EMS server.

To create a FortiClient EMS fabric connector:

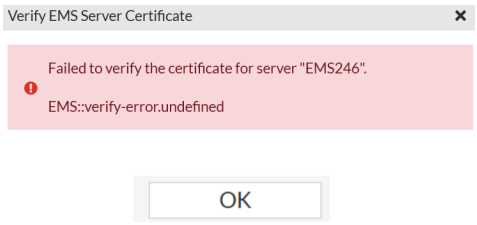
1. Go to *Network* > *Fabric Connectors*.
2. In the *Core Network Security* pane, select *FortiClient EMS* and then select *Edit*.
   The *New Fabric Connector* pane opens.



3. Enter the following information:

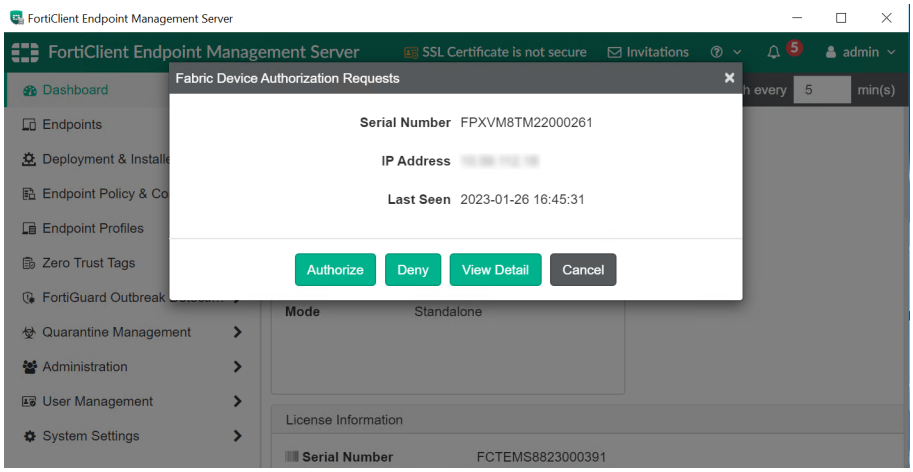
Type	Select from the following two options: • *FortiClient EMS* • *FortiClient EMS Cloud* The *FortiClient EMS Cloud* option requires FortiClient EMS Cloud entitlement.
Name	The name of the FortiClient EMS connector.
IP/Domain name	The IP address or the domain name of the FortiClient EMS.
HTTPS port	The HTTPS port number for the FortiClient EMS (default = 443, 1 - 65535).
EMS Threat Feed	Enable to allow FortiPAM to pull FortiClient malware hash from FortiClient EMS. **Note**: The option is enabled by default.
Synchronize firewall addresses	Enable to automatically create and synchronize firewall addresses for all EMS tags. **Note**: The option is enabled by default.

4. Click *OK*.
   FortiPAM attempts to verify the EMS server certificate.

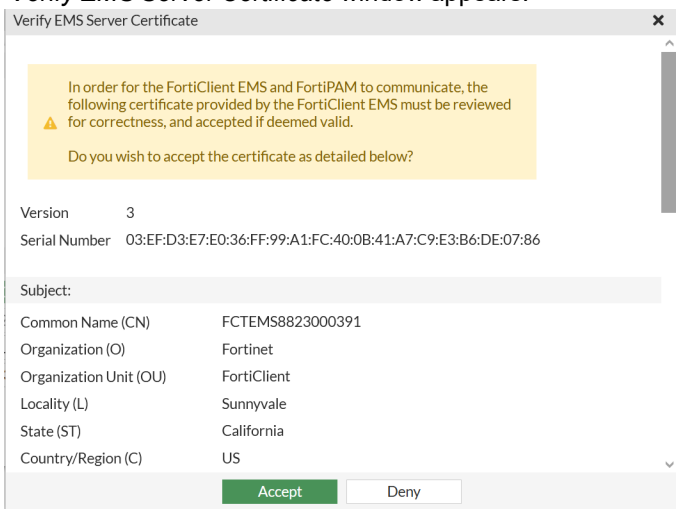


To delete a fabric connector, select *Delete* to delete the selected fabric connector.

5. Relogin to the EMS server.
   Fabric Device Authorization Requests prompt appears.



6. In *Fabric Device Authorization Requests*, click *Authorize* to authorize FortiPAM connection.
7. In the *Edit Fabric Connector* pane on FortiPAM (for the newly configured connector), click *Authorize* in *FortiClient EMS Status*.
   Verify EMS Server Certificate window appears.



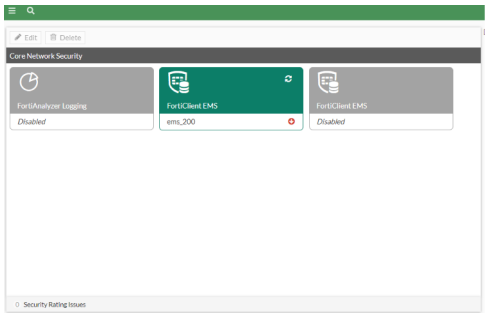
8. In the *Verify EMS Server Certificate* window, select *Accept* to accept the certificate from the EMS-side.
   FortiPAM is now successfully connected to the EMS server.

FortiAnalyzer logging

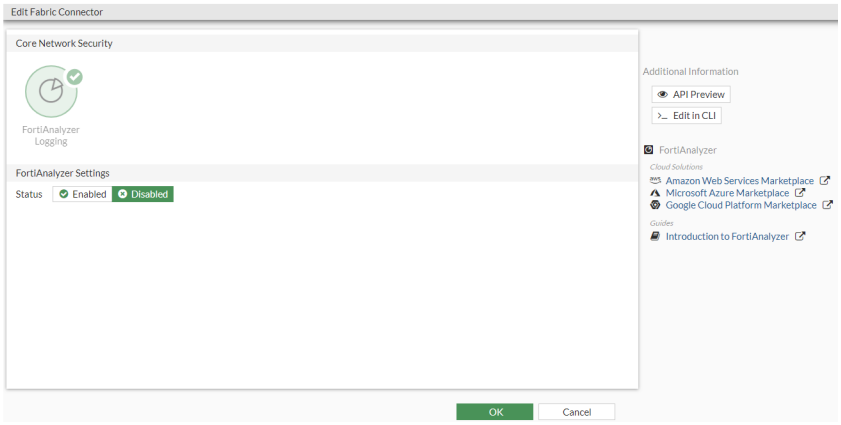
FortiAnalyzer is a remote logging server that helps keep an extra copy of logs from FortiPAM.

To configure FortiAnalyzer logging:

1. Go to *Network* > *Fabric Connectors*.
   Core Network Security opens.



2. Select *FortiAnalyzer Logging* and select *Edit*.
   The *Edit Fabric Connector* window opens.



3. In the *FortiAnalyzer Settings* pane, set the *Status* as *Enabled*.
4. Enter the following information:

Server	Enter the server IP address or the FQDN. Select *Test Connectivity* to test the connection to the server.
Upload option	The option is set to *Store & Upload Logs*. **Note**: The option is non-editable.
Upload interval	Select an upload interval: • *Daily* (default) • *Weekly* • *Monthly*
Day	From the dropdown, select a day. **Note**: The option is only available when the *Upload interval* is *Weekly*.

Date	From the dropdown, select a date. **Note**: The option is only available when the *Upload interval* is *Monthly*.
Time	Enter a time or select the clock icon to select a time.
Allow access to FortiPAM REST API	Enable/disable FortiPAM REST API access (default = enable).
Verify FortiAnalyzer certificate	Enable/disable verifying the FortiAnalyzer certificate (default = enable). **Note**: The option is only available when *Allow access to FortiPAM REST API* is enabled.

5. Click *OK*.
6. In the window that opens, verify the FortiAnalyzer serial number and click *Accept*.
7. Check the *FortiAnalyzer Status*. If the connection is unauthorized, click Authorize to log in to FortiAnalyzer and authorize FortiPAM.

To configure FortiAnalyzer logging via the CLI - Example

```
config log fortianalyzer setting
   set status enable
   set server faz.fortipam.ca
end
```

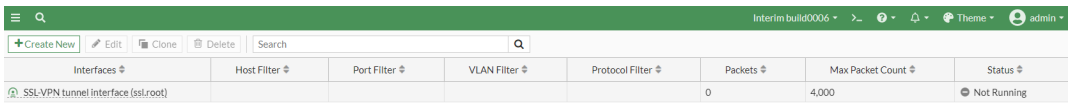
Packet capture

You can create a filter on an interface to capture a specified number of packets to examine.

Go to *Network* > *Packet Capture* to see existing packet capture filters.

For each packet capture filter the following are displayed:

- Interfaces
- Host filter
- Post filter
- VLAN filter
- Protocol filter
- Packets
- Maximum packet count
- Status



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

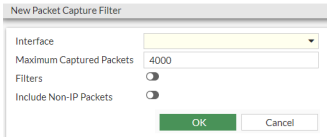
The following options are available in the *Packet Capture* tab:

+Create New	Select to create a new packet capture filter. See Creating a packet capture filter on page 235.
Edit	Select to edit the selected packet capture filter.
Clone	Select to clone the selected packet capture filter.
Delete	Select to delete the selected packet capture filter.
Search	Use the search bar to look for a packet capture filter.

Creating a packet capture filter

To create a packet capture filter:

1. Go to *Network* > *Packet Capture*.
2. Select *+Create New*.
   The *New Packet Capture Filter* window opens.



3. Enter the following information:

Interface	Select or create a new interface.  Use the search bar to look for an interface.  Use the pen icon next to an interface to edit the interface.
Maximum Captured Packets	Enter how many packets to collect (default = 4000, 1 - 1000000).
Filters	Enable *Filters*, you can create filters for host names, ports, VLAN identifiers, and protocols.  Use commas to separate items. Use a hyphen to specify a ra nge. **Note**: The option is disabled by default.
Include Non-IP Packets	Select this option if you want to include packets from non-IP protocols. **Note**: The option is disabled by default.
API Preview	The *API Preview* allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview.  This feature is not available if the user is logged in as an adm inistrator that has read-only GUI permissions.

4. Click *OK*.

To use API preview:

1. Click *API Preview*.
   The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* (enabled by default) to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

System

Go to *System* to manage and configure the basic system options for FortiPAM.

You can also manage certificates, set up HA cluster and SNMP, and configure ZTNA related settings, automated backup, firmware upgrades, FortiPAM and FortiGuard licenses.

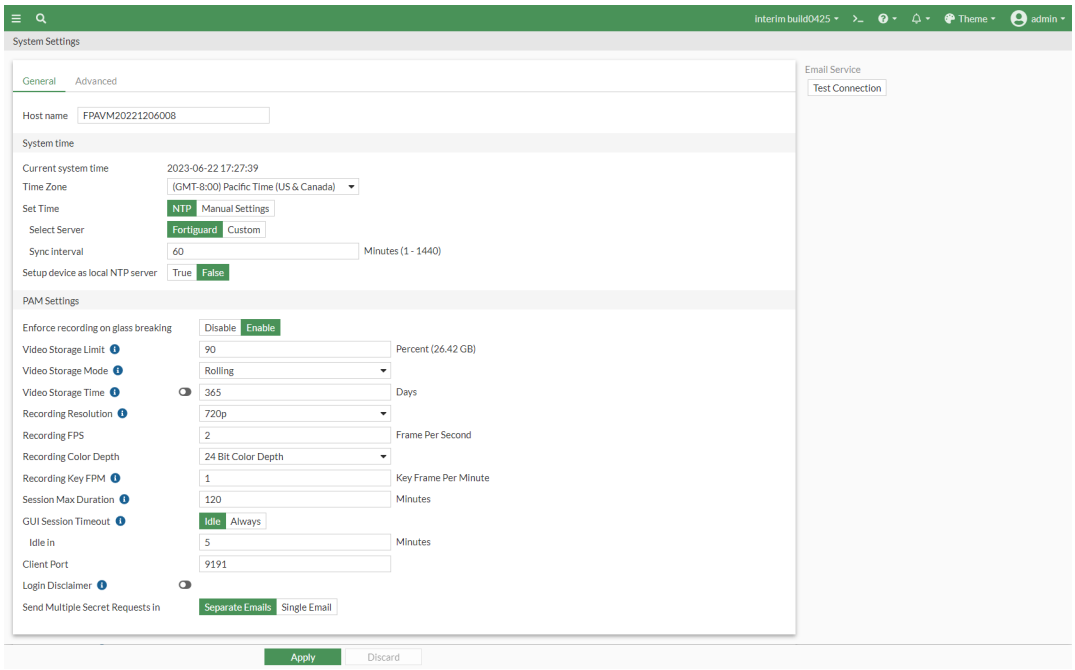
System contains the following tabs:

Settings

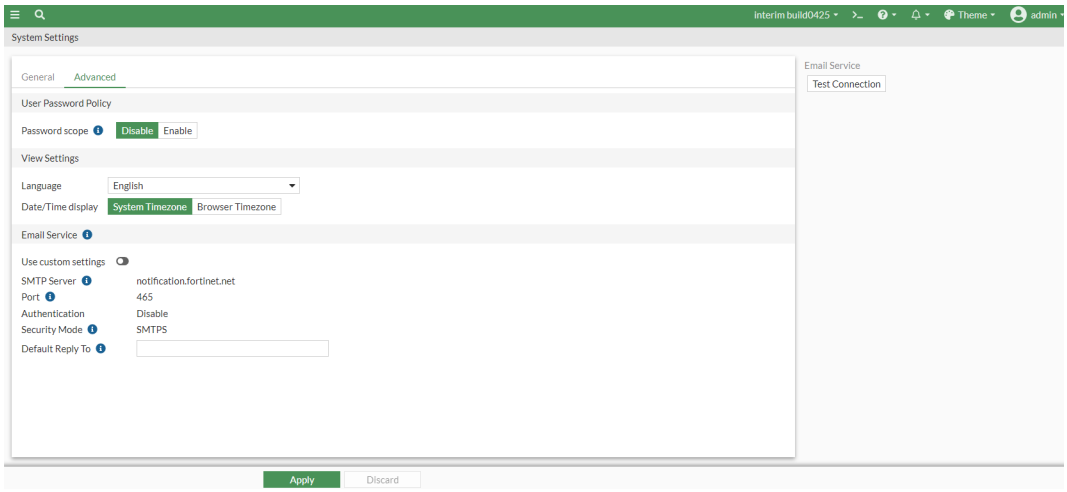
Go to *System* > *Settings* to access system configuration that you can update after installing FortiPAM.

To update System Settings:

1. Go to *System* > *Settings*.
   The *General* tab in the *System Settings* window opens.



2. To switch to the *Advanced* tab, select *Advanced*.



3. In *System Settings*, enter the following information:

General tab

Host name	The identifying name assigned to this FortiPAM unit.

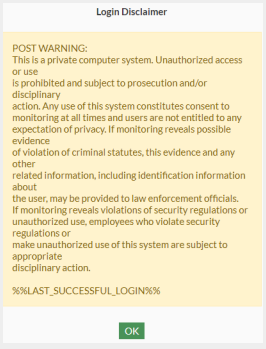
System time pane

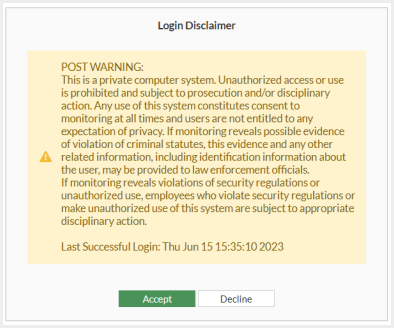
System time	
Current system time	The current date and time on the FortiPAM internal clock or NTP servers.
Time Zone	From the dropdown, select a timezone.

Set Time	Select from the following options: • *NTP*: The NTP (Network Time Protocol) server (default). • *Manual Settings*
Select Server	Select a server from the following two options: • *FortiGuard* (default) • *Custom* **Note**: The option is only available when *Set Time* is *NTP*.
Custom Server IP Address	The custom server IP address.  Custom NTP server details must be configured via the CLI. **Note**: The option is only available when *Set Time* is *NTP* and the *Select Server* is *Custom*.
Sync internal	Enter how often, in minutes, that the device synchronizes its time with the NTP server (default = 60, 1 - 1440). **Note**: The option is only available when *Set Time* is *NTP*.
Date	Enter the date or select the calendar icon, and from the dropdown, select a date. **Note**: The option is only available when *Set Time* is *Manual Settings*.
Time	Enter the time or select the clock icon, and from the dropdown, select a time. **Note**: The option is only available when *Set Time* is *Manual Settings*.
Setup device as local NTP server	Select *True* to configure the FortiPAM as a local NTP server (default = *False*).
Listen on Interfaces	Set the interface or interfaces that the FortiPAM will listen for NTP requests on. **Note**: The option is only available when *Setup device on local NTP server* is set as *True*.

PAM Settings pane

PAM Settings	
Enforce recording on glass breaking	In glass breaking mode, the administrator has permission to launch all secrets. This setting is to enforce video recording on all launching sessions. (default = enable).
Video Storage Limit	The maximum percentage of the video disk partition size that can be used for storing FortiPAM session video recordings (default = 90, 10 - 90).
Video Storage Mode	From the dropdown, select a PAM session video recording storage mode (default = *Rolling*): • *Rolling*: Evict the oldest PAM video recording within the *Video Storage Time* when the video storage limit is reached. • *Stop*: Stop storing new PAM video recordings when the disk quota is full.

Video Storage Time	The number of days for which a video is stored. Video files are removed from FortiPAM once the time has elapsed (default = 365, 0 - 36500).  Enable the toggle or enter `0` for no time limit. **Note**: The option is only available when the *Video Storage Mode* is *Rolling*.
Recording Resolution	From the dropdown, select a resolution for the PAM video recordings: • *480p* • *720p* (default) • *1080p*
Recording FPS	Enter the PAM video recording frame rate (default = 2, 1- 15).
Recording Color Depth	From the dropdown, select a color depth: • *24 Bit Color Depth* (default) • *32 Bit Color Depth*
Recording Key FPM	Enter the PAM video recording key frame rate per minute (default = 1, 1 - 60).
Session Max Duration	Enter the maximum duration for a PAM session, in minutes (default = 120, 1 - 10000).
User Session Timeout	Enter the duration elapsed after which an idle user is logged out, in minutes (default = 5, 1 - 480).  A shorter duration for *User Session Timeout* is more secure.
Client Port	Enter the port number that FortiPAM uses to connect to FortiClient (default = 9191, 1 - 65536).
Login Disclaimer	Enable/disable displaying a disclaimer message once a user successfully logs in. Once enabled, enter a disclaimer in the text box. Alternatively, you can use the default login disclaimer. 

	%%LAST_SUCCESSFUL_LOGIN%% displays when the last successful login occurred.  Click the eye icon to preview the login disclaimer. **Note**: The option is disabled by default.
Send Multiple Secret Requests in	When sending multiple secret request notifications to a reviewer: • *Separate Emails*: Send the secret request notifications as separate emails (default). • *Single Email*: Send the secret request notifications as a single email.
Period	Enter the time interval at which multiple secret request notifications are sent, in seconds (default = 60, 60 - 600). **Note**: The option is only available when *Send Multiple Secret Requests in* is set to *Single Email*.

Advanced tab

User Password Policy pane

User Password Policy	
Password scope	Enable/disable password scope (default = disable). **Note**: This applies to local user passwords.
Minimum length	The minimum length of the password (default = 8, 1 - 128).
Minimum number of new characters	Enter the minimum number of new characters required in the password (default = 0, maximum = 200).
Character requirements	Enable/disable character requirements (default = disable). When enabled, enter the number of upper case, lower case, numbers, and special (non-alphanumeric) characters required in the password. **Note**: Special characters are non-alphanumeric.
Allow password reuse	Enable/disable password reuse (default = enable).

Password expiration	Enable and enter the number of days after which the password expires (default = 90, 0 - 999).

View Settings pane

View Settings	
Language	From the dropdown, select a language.
Date/Time display	Select from the following two options: • *System Timezone*: Use the FortiPAM unit's configured timezone. • *Browser Timezone*: Use the web browser timezone.

Email Service pane

Email Service See Testing the email service connection example on page 242.	
Use custom settings	Enable to edit options in the *Email Service* pane.
SMTP Server	The SMTP server IP address or the hostname, e.g., `smtp.example.com` and `notification.fortinet.net`.
Port	The recipient port number.  The default port value depends on the chosen *Security Mode*. For *None* and *STARTTLS*, the default value is 25. For *SMTPS*, the default value is 465.
Authentication	If required by the email server, enable authentication. If enabled, enter the *Username* and *Password*.
Security Mode	Set the connection security mode used by the email server: • *None* • *SMTPS* (default) • *STARTTLS*
Default Reply To	Optionally, enter the reply to email address, such as `noreply@example.com`. This address will override the *Email from* email address that is configured for an alert email. See Email alert settings on page 215.

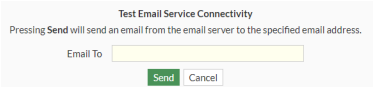
4. Click *Apply*.

Testing the email service connection - example

To test the email service connection:

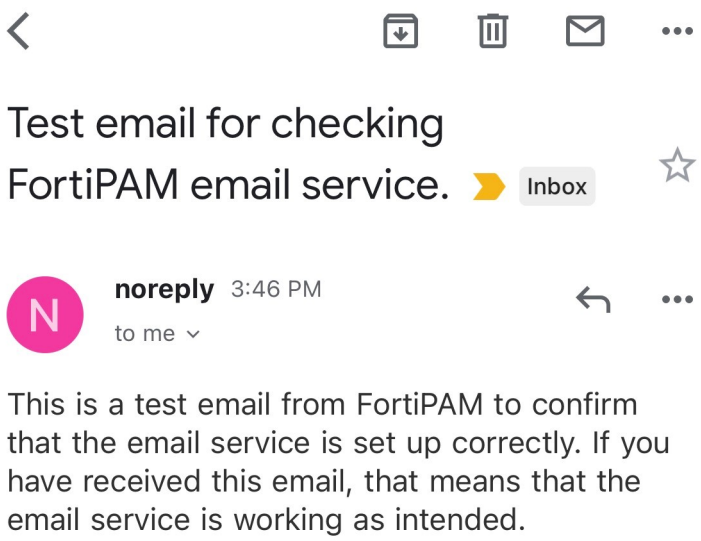
1. Go to *System* > *Settings*.
   In this example, we use the default Fortinet mail server (`notification.fortinet.net`).

2. In the *Email Service* pane in the *Advanced* tab:
   a. In *Default Reply To*, enter the email address that is used to send emails.
3. Click *Apply*.
   To configure alert emails, see Email alert settings on page 215.
4. Once the email service settings have been set up, click *Test Connection* from the top-right.
   The *Test Email Service Connectivity* dialog opens.



5. In *Email To*, enter an email address where the test email is sent to.
6. Click *Send*.
   Once the email is successfully sent, you see the following message on the bottom-right:

   The test email looks like the following:

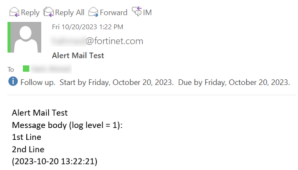


To test the email service connection via the CLI:

1. In the CLI console, enter the following command:

```
diagnose log alertmail test
```

   If the email service is correctly setup, you should receive a test email that looks like the following:



2. If you do not receive the test email:
   a. In the CLI console, enter the following CLI commands to collect the debug logs:

```
diagnose debug reset
diagnose debug enable
diagnose debug console timestamp enable
diagnose debug application alertmail -1
```

   b. In the CLI console, enter the following CLI command to send a test email:

```
diagnose log alertmail test
```

   c. In the CLI console, enter the following CLI commands to disable debugging:

```
diagnose debug disable
diagnose debug reset
```

3. To save the output, select *Download* from the top-right of the CLI window or use PuTTY to log the output.

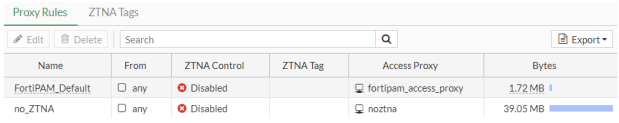
ZTNA

For an introduction to Zero Trust Network Access (ZTNA), see Zero Trust Network Access introduction in the FortiOS Admin Guide.

In *System* > *ZTNA*, you can set up proxy rules and ZTNA tags.

ZTNA servers can only be set via the CLI (`config firewall access-proxy`).

The *ZTNA* tab looks like the following:



The following options are available in all the *ZTNA* tabs:

+Create New Group	Select to create a ZTNA tag group. See Creating a ZTNA tag group on page 247
Edit	Select to edit the selected proxy rule or a tag group. See Editing a proxy rule on page 245.
Delete	Select to delete the selected proxy rules and tag groups.
Search	Use the search bar to look for a proxy rule or a tag. To narrow down your search in the *ZTNA Tags* tabs, see Column filter.

Export	From the dropdown, select to export the list of proxy rules to your computer as a CSV file or a JSON file.
Refresh	To refresh the contents, click the refresh icon on the bottom-right. **Note**: The option may not be available in all the tabs.

Editing a proxy rule

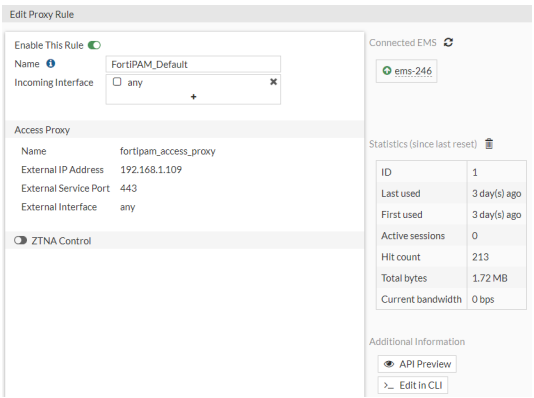
A proxy rule is used to enforce access control. ZTNA tags or tag groups can be added into a rule to enforce zero trust role based access.

On the FortiPAM GUI, you can only edit an existing proxy rule. Use the CLI to create new proxy rules (`config firewall policy`).

A default *FortiPAM_Default* proxy rule is available in the proxy rules list.

To configure a proxy rule:

1. Go to *System* > *ZTNA*.
2. In the proxy rules list, select a proxy rule and then select *Edit*.
   Alternatively, in the proxy rules list, double-click a proxy rule to edit it.
   The *Edit Proxy Rule* window opens.



3. Enter the following information:

Enable this rule	Toggle on to enable the proxy rule.
Name	The name of the proxy rule.  Names are not fixed and can be changed later.
Incoming Interface	Select incoming interfaces or create new interfaces.  Use the search bar to look for an interface.  Use the pen icon next to the interface to edit it.
Access Proxy The corresponding access proxy and VIP.  The *Access Proxy* pane is read-only.	
ZTNA Control Enable/disable ZTNA control for the proxy rule.  ZTNA control is equivalent to `client-cert` in the access proxy.	
ZTNA Tag	Add the ZTNA tags or tag groups that are allowed access. ZTNA tags are synchronized from the EMS side.  Use the search bar to look for a ZTNA tag. Creating a ZTNA tag group on page 247
Match ZTNA tags	If multiple tags are included, select *Any* or *All* (default = *Any*).

Under *Connected EMS* on the right, you can see connected EMS(s).
Hovering over one of the EMS displays a tooltip with additional details about that EMS.

4. Click *OK*.

Creating a ZTNA tag group

After FortiPAM connects to the FortiClient EMS, it automatically synchronizes ZTNA tags.

ZTNA tags related information is listed in the ZTNA tags list. You can customize ZTNA tag groups to categorize user access based on multiple tags.

Hover over a tag name to see more information about the tag, such as its resolved address.

To create a ZTNA group:

1. Go to *System* > *ZTNA* and select the *ZTNA Tags* tab.
2. Select *+Create New Group*.
   The *New ZTNA Tag Group* window opens.

3. In *Name*, enter a name for the group.
4. In *Members*, select +, and from the *Select Entries* window, select members or create new members.

   Use the search bar to look for a member.

5. Optionally, enter comments about the ZTNA tag group.
6. Click *OK*.

ZTNA user control

When ZTNA control is set up on FortiPAM, you can only connect to FortiPAM and launch a secret from the endpoint PC with allowed ZTNA tags. The endpoint PC must install FortiClient and connect to the same EMS server.

To use the FortiPAM ZTNA control feature:

- You must connect to the same EMS server for the client where the FortiClient runs.
- You must enable the *ZTNA Control* option when editing a proxy rule. See Editing a proxy rule on page 245.
- You must configure another access proxy with a different VIP and client certificate disabled to launch secrets without ZTNA control successfully for clients not connected to the same EMS as FortiPAM.

To set up EMS in the GUI:

1. Go to *Network* > *Fabric Connectors*.
2. Select *FortiClient EMS* and click *Edit*.

3. In *Name*, enter the EMS name.
4. In *IP/Domain name*, enter the IP address or the domain name of the EMS.
5. In *HTTPS port*, enter the HTTPS port for the EMS.
6. Click *OK*.

Refer to *FortiClient EMS Status* to check the status of the FortiClient EMS.

If there is an error connecting to the EMS server, log in to the EMS server, authorize FortiPAM in *Administration* > *Fabric Device*, and click *Accept* in *Verify EMS Server Certificate*.

For more information, see Fabric Connectors on page 230.

To set EMS using the CLI:

1. In the CLI console, enter the following commands to configure an EMS:

```
config endpoint-control fctems
   edit "ems_200"
      set server "10.59.112.200"
   next
end
```

2. After adding an EMS server, the CLI asks you to verify using `execute fctems verify ems_200`.

- example

```
execute fctems verify ems_200
   Subject: C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiClient, CN
        = FCTEMS8822002925, emailAddress = support@fortinet.com
   Issuer: C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate
        Authority, CN = support, emailAddress = support@fortinet.com
   Valid from: 2022-04-25 18:17:42 GMT
   Valid to: 2038-01-19 03:14:07 GMT
   Fingerprint: 35:12:95:DA:A5:2E:20:F9:8F:99:88:75:25:BC:D8:A3
   Root CA: No
   Version: 3
   Serial Num:
   a4:35:c8
   Extensions:
   Name: X509v3 Basic Constraints
   Critical: no
   Content:
   CA:FALSE
EMS configuration needs user to confirm server certificate.
Do you wish to add the above certificate to trusted remote certificates? (y/n)y
Certificate successfully configured and verified.
```

If authentication is denied, log in to the EMS server and authorize FortiPAM in *Administration* > *Fabric Device*.

Using EMS tag for endpoint control

You can create Zero Trust tagging rules for endpoints on an EMS server based on operating system versions, logged-in domains, running processes, and other criteria. EMS uses the rules to dynamically group endpoints with different tags. FortiPAM can use these ZTNA tags in proxy rules (firewall policy) to control which endpoint has access to FortiPAM. For

this, at least one FortiClient EMS must be added in *Network* > *Fabric Connectors*, and FortiPAM must be successfully connected to this EMS server.

FortiClient EMS is a security management solution that enables scalable and centralized management of endpoints. See ZTNA tag control example on page 249.

ZTNA tag control - example

To add ZTNA tag control using the CLI:

In the access proxy, `client-cert` must be enabled. You can use `ztna-ems-tag` to give FortiPAM access to endpoints with this tag.

1. In the CLI console enter the following commands:

```
config firewall access-proxy
   edit "fortipam_access_proxy"
      set vip "fortipam_vip"
      set client-cert enable #Must be enabled
      config api-gateway
         edit 1
            set url-map "/pam"
            set service pam-service
         next
         edit 2
            set url-map "/tcp"
            set service tcp-forwarding
            config realservers
               edit 1
                  set address "all"
               next
            end
         next
         edit 3
            set service gui
            config realservers
               edit 1
                  set ip 127.0.0.1
                  set port 80
               next
            end
         next
      end
   next
end
config firewall policy
   edit 1
      set type access-proxy
      set name "FortiPAM_Default"
      set srcintf "any"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set access-proxy "fortipam_access_proxy"
```

```
        set ztna-ems-tag "FCTEMS8822002925_pam-ems-tag-office" #Only endpoints with this
             tag can access FortiPAM
        set utm-status enable
        set groups "SSO_Guest_Users"
        set ssl-ssh-profile "deep-inspection"
    next
end
```

ZTNA-based FortiPAM access control

When ZTNA control is enforced on FortiPAM, devices without FortiClient installed cannot access FortiPAM.

If you want to grant access to the user using the browser extension-only solution, you can create multiple proxy rules to achieve this. See CLI configuration for a user with browser extension-only solution example on page 251.

Enable ZTNA control to only allow endpoints with selected tags to access FortiPAM

To enable ZTNA control:

1. Go to *System* > *ZTNA*.
2. In the proxy rules list, select the *FortiPAM_Default* proxy rule and then select *Edit*.
3. Enable *ZTNA Control*.
4. In *ZTNA Tag*, add the ZTNA tags or tag groups that are allowed access.

When selecting ZTNA tags, you can view all the ZTNA tags from the EMS server.

5. Click *OK*.
6. From the user dropdown on the top-right, select *Logout*.
7. When attempting to log in, a certificate check appears on the browser.
   Click *OK* to proceed with logging in to FortiPAM.

CLI configuration for a user from endpoint installed with FortiClient (multiple proxy rules) - example

In this example, a user from an endpoint installed with FortiClient can access FortiPAM via VIP `192.168.1.109` provided that the endpoint contains `FCTEMS8822008307_Office_Windows_PC` or `FCTEMS8822008307_MIS_Team` ZTNA tag.

1. In the CLI console, enter the following commands:

```
config firewall vip
   edit "fortipam_vip"
      set type access-proxy
      set extip 192.168.1.109
      set extintf "any"
      set server-type https
```

```
      set extport 443
      set ssl-certificate "Fortinet_SSL"
   next
end
config firewall access-proxy
   edit "fortipam_access_proxy"
      set vip "fortipam_vip"
      set client-cert enable
      config api-gateway
         edit 1
            set url-map "/pam"
            set service pam-service
         next
         edit 2
            set url-map "/tcp"
            set service tcp-forwarding
            config realservers
               edit 1
                  set address "all"
               next
            end
         next
         edit 3
            set service gui
            config realservers
               edit 1
                  set ip 127.0.0.1
                  set port 80
               next
            end
         next
      end
   next
end
config firewall policy
   edit 1
      set type access-proxy
      set name "FortiPAM_Default"
      set srcintf "any"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set access-proxy "fortipam_access_proxy"
      set ztna-ems-tag "FCTEMS8822008307_Office_Windows_PC" "FCTEMS8822008307_MIS_
          Team"
      set groups "SSO_Guest_Users"
      set ssl-ssh-profile "deep-inspection"
   next
end
```

CLI configuration for a user with browser extension-only solution - example

In this example, users with IP address `192.168.1.2` access FortiPAM via the VIP `192.168.1.108` from an endpoint with no FortiClient installed or no match with the ZTNA policy in the previous example.

The firewall policy is more restrictive than the previous example and allows fewer source addresses. Two VIPs are required for this setup. Also, you can set it up to allow access within a certain schedule only.

The `access-proxy` setting links to the name of the corresponding firewall access-proxy. The VIP setting links to the name of the corresponding firewall VIP. The VIP represents the FortiPAM ZTNA gateway to which clients make HTTPS connections. The service/server mappings define the virtual host matching rules and the actual server mappings of the HTTPS requests. When creating an access proxy, it is recommended to copy the default access proxy and modify only the VIP and `client-cert` settings to ensure proper configuration.

1. In the CLI console, enter the following commands:

```
config firewall vip
   edit "fortipam_vip-no-ztna"
      set type access-proxy
      set extip 192.168.1.108
      set extintf "any"
      set server-type https
      set extport 443
      set ssl-certificate "Fortinet_SSL"
   next
end
config firewall access-proxy
   edit "fortipam_access_proxy-no-ztna"
      set vip "fortipam_vip-no-ztna"
      config api-gateway
         edit 1
            set url-map "/pam"
            set service pam-service
         next
         edit 2
            set url-map "/tcp"
            set service tcp-forwarding
            config realservers
               edit 1
                  set address "all"
               next
            end
         next
         edit 3
            set service gui
            config realservers
               edit 1
                  set ip 127.0.0.1
                  set port 80
               next
            end
         next
      end
   next
end
config firewall address
   edit "192.168.1.2"
      set subnet 192.168.1.2 255.255.255.255
   next
end
config firewall policy
   edit 2
      set type access-proxy
```

```
        set name "no ZTNA"
        set srcintf "any"
        set srcaddr "192.168.1.2"
        set dstaddr "all"
        set action accept
        set schedule "always"
        set access-proxy "fortipam_access_proxy-no-ztna"
        set groups "SSO_Guest_Users"
        set ssl-ssh-profile "deep-inspection"
    next
end
```

High availability

Multiple FortiPAM units can operate as an high availability (HA) cluster to provide even higher reliability.

FortiPAM can operate in Active-Passive HA mode.

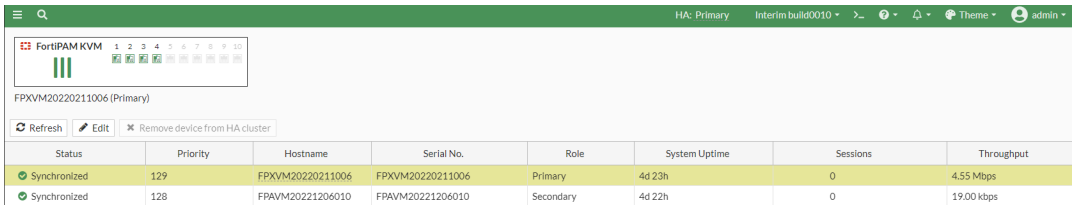
Active-Passive: Clustered fail-over mode where all of the configuration is synchronized between the devices.

PAM configurations, such as users and secrets, are automatically synced to secondary devices to ensure PAM services can be operated or recovered when the primary device is down. All tasks are handled by the primary device as long as system events and logs are only recorded on the primary device.

Your FortiPAM device can be configured as a standalone unit, or you can configure up to three FortiPAM devices in HA, one Active and up to two Passive mode devices, for failover protection and/or disaster recovery.

HA requires an additional license for each cluster unit with the same number of seats as you have for the primary FortiPAM. Each FortiPAM device in HA must be the same device model and version number.

The following shows FortiPAM devices in Active-Passive mode:



Status, priority, hostname, serial number, role, system uptime, sessions, and throughput are displayed for each unit in the HA cluster.

- Click *Refresh* to fetch the latest information on the HA topology in use.
- Select a FortiPAM unit and select *Remove device from HA cluster* to remove the FortiPAM unit from the HA cluster.
- To edit a FortiPAM unit in an HA cluster, select the FortiPAM unit and then select *Edit*.

The primary unit in an Active-Passive cluster cannot be removed from the cluster.

Before configuring an HA cluster, ensure that interfaces are not using the DHCP mode to get IP addresses.

Configuring HA and cluster settings

To configure HA and cluster settings:

1. Go to *System* > *HA*.
2. Configure the following settings:

Mode	From the dropdown, select *Standalone* or *Active-Passive*. If you select *Standalone*, no other options are displayed.
Device priority	You can set a different device priority for each cluster member to control the order in which cluster units become the primary unit (HA primary) when the primary unit fails. The device with the highest device priority becomes the primary unit (default = 128, 0 - 255). Since all videos and logs are only stored on the primary device, one FortiPAM should be configured with higher priority. And with override enabled, the primary unit with the highest device priority will always become the primary unit. The override setting and device priority value are not synchronized to all cluster units. You must enable override and adjust device priority manually and separately for each cluster unit.
Cluster Settings	
Group name	Enter a name to identify the cluster.
Password	Select *Change* to enter a password to identify the HA cluster. The maximum password length is 15 characters. The password must be the same for all cluster FortiPAM units before the FortiPAM units can form the HA cluster. It is suggested that you add a password to protect the HA cluster.

	 Each HA cluster device on the same network must have different passwords.
Monitor interfaces	Select the specific ports to monitor or create new interfaces.  Use the search bar to look for an interface.  Use the pen icon next to the interface to edit it. If a monitored interface fails or is disconnected from its network, the interface leaves the cluster and a link failover occurs. The link failover causes the cluster to reroute the traffic being processed by that interface to the same interface of another cluster that still has a connection to the network. This other cluster becomes the new primary unit.
Heartbeat interfaces	Select to enable or disable the HA heartbeat communication for each interface in the cluster and then set the heartbeat interface priority. You can also create new interfaces.  Use the search bar to look for an interface.  Use the pen icon next to the interface to edit it. The heartbeat interface with the highest priority processes all heartbeat traffic. You must select at least one heartbeat interface. If the interface functioning as the heartbeat fails, the heartbeat is transferred to another interface configured as a heartbeat interface. If heartbeat communication is interrupted, the cluster stops processing traffic. Priority ranges from 0 to 512.  Heartbeat interfaces should use dedicated interfaces and not share the VIP interface.

Management Interface Reservation

Enable or disable the management interface reservation.

Note: The option is disabled by default.

You can provide direct management access to individual cluster units by reserving a management interface as part of the HA configuration. After this management interface is reserved, you can configure a different IP address, administrative access, and other interface settings for this interface for each cluster unit. You can also specify static routing settings for this interface. Then by connecting this interface of each cluster unit to your network, you can manage each cluster unit separately from a different IP address.

Interface	Select the management interface or create a new interface.  Use the search bar to look for an interface.  Use the pen icon next to the interface to edit it.  Management interfaces should use dedicated interfaces.
Gateway	Enter the IPv4 address for the remote gateway.
IPv6 gateway	Enter the IPv6 address for the remote gateway.
Destination subnet	Enter the destination subnet.

Unicast Status

Enable the unicast HA heartbeat in virtual machine (VM) environments that do not support broadcast communication.

Note: The option is disabled by default.

Note: The pane is only available when the *Mode* is *Active-Passive*.

 When disabling this option to change from HA unicast to multicast, you must reboot all units in the cluster for the change to take effect.

Peer IP	Enter the IP address of the HA heartbeat interface of the other FortiPAM-VM in the HA cluster. **Note**: The option is only available when *Unicast Heartbeat* is enabled.
Override	Enable to use the primary server by default whenever it is available. **Note**: The option is enabled by default.

3. Click *OK*.

HA failover

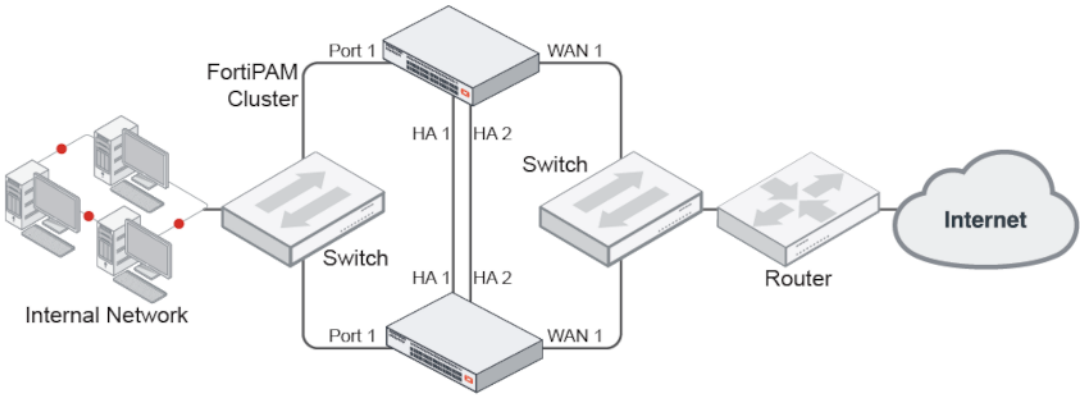
When primary FortiPAM is down, secondary will take the primary role and permanently enter maintenance mode. Under maintenance mode, all critical processes will be temporarily suspended. Admin can bring up the original primary device

or disable maintenance mode on the new primary device to resume all FortiPAM features.

HA active-passive cluster setup

An HA Active-Passive (A-P) cluster can be set up using the GUI or CLI.

This example uses the following network topology:

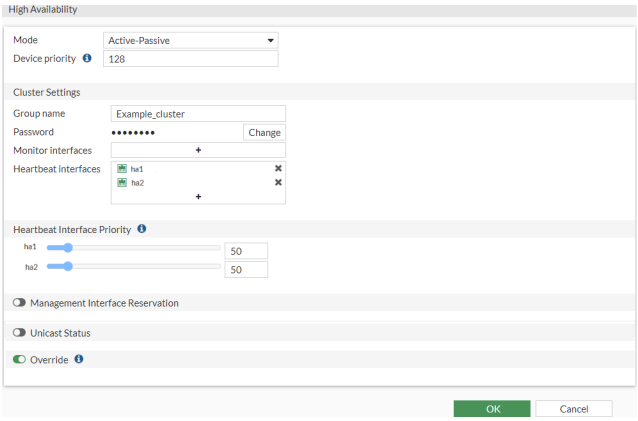


To set up an HA A-P cluster using the GUI:

1. Make all the necessary connections as shown in the topology diagram.
2. Log into one of the FortiPAM devices.
3. Go to *System* > *HA* and set the following options:

Mode	*Active-Passive*.
Device priority	128 or higher.
Group name	Example_cluster.
Heartbeat interfaces	ha1 and ha2.

Except for the device priority, these settings must be the same on all FortiPAM devices in the cluster.



4. Leave the remaining settings on default. They can be changed after the cluster is in operation.
5. Click *OK*.

The FortiPAM negotiates to establish an HA cluster. Connectivity with the FortiPAM may be temporarily lost.

6. Factory reset the other FortiPAM that will be in the cluster, configure GUI access, then repeat steps 1 to 5, omitting setting the device priority, to join the cluster.

To set up an HA A-P cluster using the CLI:

1. Make all the necessary connections as shown in the topology diagram.
2. Log into one of the FortiPAM devices.
3. Change the host name of the FortiPAM:

```
config system global
   set hostname Example1_host
end
```

Changing the host name makes it easier to identify individual cluster units in the cluster operations.

4. Enable HA

```
config system ha
   set mode active-passive
   set group-name Example_cluster
   set hbdev ha1 10 ha2 20
end
```

5. Leave the remaining settings as their default values. They can be changed after the cluster is in operation.
6. Repeat steps 1 to 5 on the other FortiPAM devices to join the cluster, giving each device a unique hostname.

Upgrading FortiPAM devices in an HA cluster

You can upgrade the firmware on an HA cluster in the same way as on a standalone FortiPAM. During a firmware upgrade, the cluster upgrades the primary unit and all of the secondary units to the new firmware image.

Before upgrading a cluster, back up your configuration. See Backup and restore on page 14.

Uninterrupted upgrade

An uninterrupted upgrade occurs without interrupting communication in the cluster.

To upgrade the cluster firmware without interrupting communication, the following steps are followed. These steps are transparent to the user and the network, and might result in the cluster selecting a new primary unit.

1. The administrator uploads a new firmware image using the GUI or CLI. See Uploading a firmware on page 13.
2. The firmware is upgraded on all of the secondary units.
3. A new primary unit is selected from the upgraded secondary units.
4. The firmware is upgraded on the former primary unit.
5. Primary unit selection occurs, according to the standard primary unit selection process.
   If all of the secondary units crash or otherwise stop responding during the upgrade process, the primary unit will continue to operate normally, and will not be upgraded until at least one secondary rejoins the cluster.

Interrupted upgrade

An interrupted upgrade upgrades all cluster members at the same time. This takes less time than an uninterrupted upgrade, but it interrupts communication in the cluster.

Interrupted upgrade is disabled by default.

To enable interrupted upgrade:

```
config system ha
   set uninterruptible-upgrade disable
end
```

Disaster recovery

FortiPAM supports adding a disaster recovery node in a remote site. It uses HA to implement this feature.

Disaster recovery can only be set up using the CLI commands.

The HA primary and secondary nodes are set up in a location while HA disaster recovery node is set up in a remote location. The 3 nodes form an HA cluster.

On the disaster recovery node, use the following CLI command to enable it:

```
config system ha
```

```
   set disaster-recovery-node enable
end
```

HA primary node - CLI example

```
config system ha
   set override enable
   set priority 200
   set unicast-status enable
   set unicast-gateway 10.1.2.33
   config unicast-peers
      edit 35
         set peer-ip 10.1.3.35
      next
      edit 37
         set peer-ip 10.1.2.37
      next
   end
```

HA secondary node - CLI example

```
config system ha
   set override enable
   set priority 100
   set unicast-status enable
   set unicast-gateway 10.1.2.33
   config unicast-peers
      edit 35
         set peer-ip 10.1.3.35
      next
      edit 36
         set peer-ip 10.1.2.36
      next
   end
```

Disaster recovery node - CLI example

```
config system ha
   set override enable
   set disaster-recovery-node enable
   set unicast-status enable
   set unicast-gateway 10.1.3.33
   config unicast-peers
      edit 36
         set peer-ip 10.1.2.36
      next
      edit 37
         set peer-ip 10.1.2.37
      next
   end
```

The disaster recovery node has a lower heartbeat interval, in ms (default = 600).

Use the following CLI command to change the interval:

```
config system ha
   set disaster-recovery-hb-interval <integer>
end
```

A disaster recovery node on a remote site is most likely under a different network segment from the primary. You must configure different interface IP, VIP, and gateway for the disaster recovery node based on the network design. In this case, the below setting should be configured. So that the VIP, system interface, static route, SAML server, and FortiToken Mobile push configuration among the primary, secondary, and disaster recovery nodes do not sync. When HA fails over to the disaster recovery node, FortiPAM can operate on the disaster recovery node's VIP as long as other services.

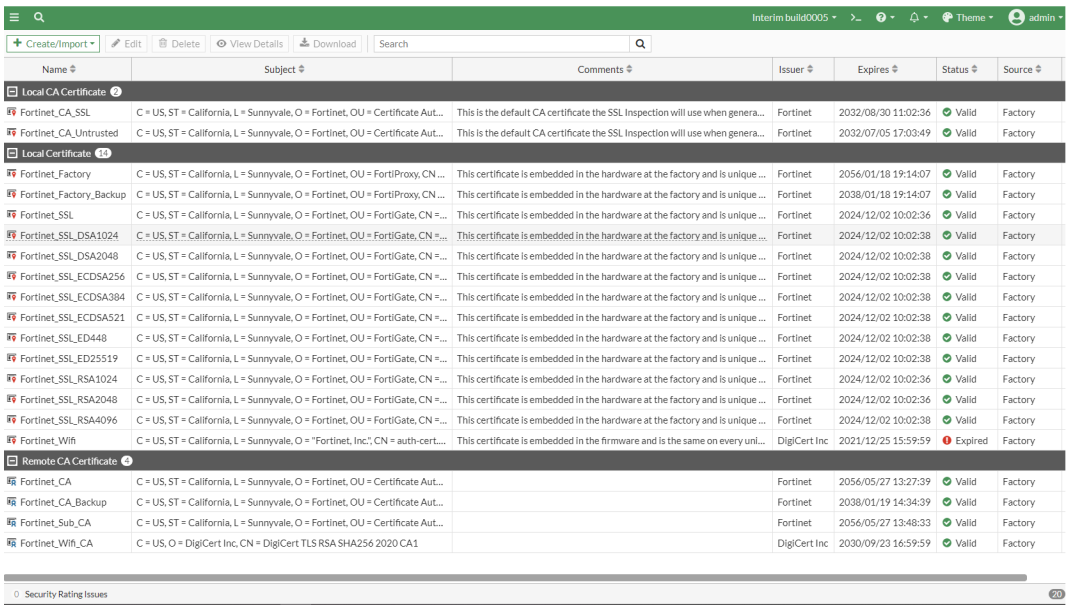
```
config system vdom-exception
   edit 1
      set object firewall.vip
   next
   edit 2
      set object system.interface
   next
   edit 3
      set object router.static
   next
   edit 4
      set object user.saml
   next
   edit 5
      set object system.ftm-push
   next
end
```

If you do wish to sync the above settings from the primary to the secondary, you need to edit them on the secondary manually.

When HA primary, secondary, and disaster recovery nodes use different VIPs, they must be added individually as service providers on a SAML server. And the SAML server configurations on FortiPAM HA members are also different.

Certificates

Go to *System* > *Certificates* to manage certificates.



There are three types of certificates that FortiPAM uses:

- **Local certificates**: Local certificates are issued for a specific server or web site. Generally they are very specific and often for an internal enterprise network.
- **CA certificates**: External CA certificates are similar to local certificates, except they apply to a broader range of addresses or to whole company. A CA certificate would be issued for an entire web domain, instead of just a single web page. External CA certificates can be deleted, downloaded, and their details can be viewed, in the same way as local certificates.
- **Remote certificates**: These remote certificates are public certificates without private keys. They can be deleted, imported, and downloaded, and their details can be viewed in the same way as local certificates.

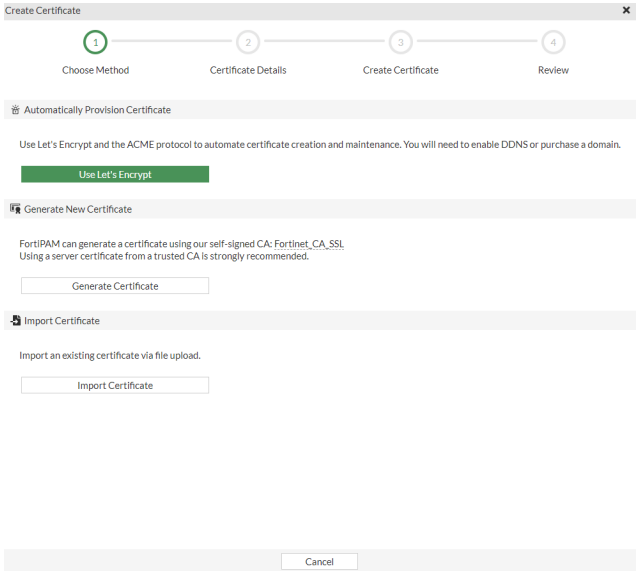
The *Certificates* tab contains the following options:

+Create/Import	From the dropdown, select *Certificate*, *Generate CSR*, *CA Certificate*, *Remote Certificate*, and *CRL*. See: • Creating a certificate on page 263 • Generating a CSR (Certificate Signing Request) on page 266 • Importing CA certificate on page 268 • Uploading a remote certificate on page 269 • Importing a CRL (Certificate revocation list) on page 269
Edit	Select to edit the selected certificate.
Delete	Select to delete the selected certificates.
View Details	Select to see details about the selected certificate.
Download	Select to download the selected certificate.
Search	Use the search bar to look for a certificate.

Creating a certificate

To create a certificate

1. Go to *System* > *Certificates*.
2. From *+Create/Import*, select *Certificate*.
   The *Create Certificate* wizard opens.



3. Enter the following information:

Choose Method	
Automatically Provision Certificate	Select *Use Let's Encrypt* to automatically create a certificate using the ACME protocol with Let's Encrypt service. You will need to enable DDNS or purchase a domain.
Generate New Certificate	Select *Generate Certificate* to generate a certificate using the self-signed `Fortinet_CA_SSL` CA. Using a server certificate from a trusted CA is strongly recommended.
Import Certificate	Select *Import Certificate* to import an existing certificate by uploading the file.
Certificate Details Enter the certificate details and click *Create* to create a certificate.	
Automatically Provision Certificate	The certificate will be automatically provisioned using the ACME protocol with the Let's Encrypt service. It is the easiest way to install a trusted certificate.

Certificate name	The name of the certificate.
Domain	The public FQDN of FortiPAM. **Note**: The option is only available when the *Chosen Method* is *Automatically Provision Certificate*.
Email	The email address. **Note**: The option is only available when the *Chosen Method* is *Automatically Provision Certificate*.
Set ACME Interface	If this is the first time enrolling a server certificate with Let's Encrypt on this FortiPAM unit, the *Set ACME Interface* pane opens. **Note**: The options in the pane are only available when the *Chosen Method* is *Automatically Provision Certificate*.
ACME Interface	Select + and from *Select Entries*, select ports, or create new interfaces on which the ACME client will listen for challenges to provision and renew certificates. Click *OK* when you have selected interfaces.  Use the search bar to look for an interface.  Use the pen icon next to the interface to edit it.
Generate New Certificate	
Certificate authority	The certificate authority. **Note**: The option is only available when the *Chosen Method* is *Generate New Certificate*.
Common name	The common name of the certificate. Enter an FQDN or an IPv4 address.  The common name should match the FQDN or the IP address of the primary SSL-VPN interface. **Note**: The option is only available when the *Chosen Method* is *Generate New Certificate*.
Subject alternative name	An IP address or FQDN. Subject alternative names (SAN) allow you to protect multiple host names with a single SSL certificate. SAN is part of the X.509 certificate standard. **Note**: The option is only available when the *Chosen Method* is *Generate New Certificate*.

Update Your List of Trusted Certificate Authorities	Select *Download CA Certificate* to download `Fortinet_CA_SSL` CA to your computer.  `Fortinet_CA_SSL` is a local CA certificate. To avoid certificate warnings, you must download it and install it on each client machine. **Note**: The option is only available when the *Chosen Method* is *Generate New Certificate*.
Import Certificate	
Type	Select from the following three options: • *Local Certificate* • *PKCS #12 Certificate* • *Certificate* **Note**: The option is only available when the *Chosen Method* is *Import Certificate*.
Certificate file	Select *+Upload* and locate the certificate file on your local computer. **Note**: The option is only available when the *Chosen Method* is *Import Certificate* and the *Type* is either *Local Certificate* or *Certificate*.
Certificate with key file	Select *+Upload* and locate the certificate with key file on your local computer. **Note**: The option is only available when the *Chosen Method* is *Import Certificate* and the *Type* is *PKCS #12 Certificate*.
Password	Enter the password. **Note**: The option is only available when the *Chosen Method* is *Import Certificate* and the *Type* is either *PKCS #12 Certificate* or *Certificate*.
Confirm Password	Reenter the password to confirm. **Note**: The option is only available when the *Chosen Method* is *Import Certificate* and the *Type* is *PKCS #12 Certificate* or *Certificate*.
Key file	Select *+Upload* and locate the key file on your local computer. **Note**: The option is only available when the *Chosen Method* is *Import Certificate* and the *Type* is *Certificate*.
Review	
Enable *ACME log* to see logs related to the certificate created using the ACME protocol. **Note**: The option is only available when *Chosen Method* is *Automatically Provision Certificate*.	
Update Your List of Trusted Certificate Authorities	If you have not already downloaded the `Fortinet_CA_SSL` CA to your computer, select *Download CA Certificate* to download it. **Note**: The option is only available when the *Chosen Method* is *Generate New Certificate*.

4. Click *OK*.

Generating a CSR (Certificate Signing Request)

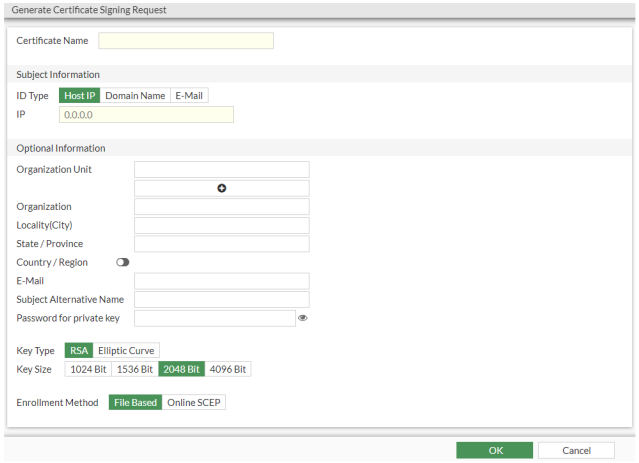
Whether you create certificates locally or obtain them from an external certificate service, you need to generate a Certificate Signing Request (CSR).

When a CSR is generated, a private and public key pair is created for FortiPAM. The generated request includes the public key of the device, and information such as the unit's public static IP address, domain name, or email address. The device private key remains confidential on the unit.

After the request is submitted to a CA, the CA verifies the information and register the contact information on a digital certificate that contains a serial number, an expiration date, and the public key of the CA. The CA then signs the certificate, after which you can install the certificate on FortiPAM.

To generate a CSR:

1. Go to *System* > *Certificates*.
2. From *+Create/Import*, select *Generate CSR*.
   The *Generate Certificate Signing Request* window opens.



3. Enter the following information:

Certificate Name	Enter a unique name for the certificate request, such as the host name or the serial number of the device.  Do not include spaces in the certificate to ensure compatibility as a PKCS12 file.
Subject Information	
ID Type	Select the ID type: • *Host IP*: Select if the unit has a static IP address. Enter the device IP address in the *IP* field (default). • *Domain Name*: Enter the device domain name or FQDN in the *Domain Name* field. • *E-mail*: Enter the email address of the device administrator in the *E-mail* field.
Optional Information Optional information to further identify the device.	
Organizational Unit	The name of the department.  Up to 5 OUs can be added.
Organization	The legal name of the company or organization.
Locality (City)	The name of the city where the unit is located.
State/Province	The name of the state or province where the unit is located.
Country/Region	Enable and then enter the country where the unit is located. Select from the dropdown.  The option is disabled by default.
E-mail	The contact email address.
Subject Alternative Name	One or more alternative names, separated by commas, for which the certificate is also valid. An alternative name can be: email address, IP address, URI, DNS name, or a directory name. Each name must be preceded by its type, for example: IP:`1.2.3.4`, or URL: `http://your.url.here/`.
Password for private key	The password for the private key.

Key Type	Select *RSA* or *Elliptic Curve*. **Note**: The default is RSA.
Key Size	If you selected *RSA* for the *Key Type*, select the *Key size*: *1024 Bit*, *1536 Bit*, *2048 Bit* (default), or *4096 Bit*. Larger key sizes are more secure but slower to generate. If you selected *Elliptic Curve* for the *Key Type*, select the *Curve Name*: *secp256r1* (default), *secp384r1*, or *secp521r1*.
Enrollment Method	Select the enrollment method. • *File Based*: Generate the certificate request (default). • *Online SCEP*: Obtain a signed, Simple Certificate Enrollment Protocol (SCEP) based certificate automatically over the network. Enter the CA server URL and challenge password in their respective fields.

4. Click *OK*.

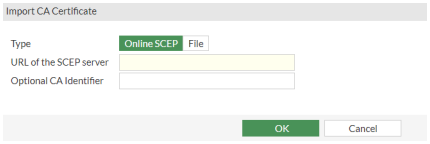
Importing CA certificate

CA root certificates are similar to local certificates, however they apply to a broader range of addresses or to whole company; they are one step higher up in the organizational chain. Using the local certificate example, a CA root certificate would be issued for all of `www.example.com` instead of just the smaller single web page.

You can import a CA certificate to FortiPAM.

To import a CA certificate:

1. Go to *System* > *Certificates*.
2. From *+Create/Import*, select *CA Certificate*.
   The *Import CA Certificate* window opens.



3. Enter the following information:

Type	Select either *Online SCEP* or *File*.
URL of the SCEP server	The URL of the SCEP server. **Note**: The option is only available when the *Type* is *Online SCEP*.
Optional CA Identifier	Optionally, enter the CA identifier. **Note**: The option is only available when the *Type* is *Online SCEP*.
+Upload	Select and locate the certificate file on your computer. **Note**: The option is only available when the *Type* is *File*.

4. Click *OK*.

Uploading a remote certificate

Remote certificates are public certificates without a private key. Remote certificates can be uploaded to the FortiPAM unit.

To upload a remote certificate:

1. Go to *System* > *Certificates*.
2. From *+Create/Import*, select *Remote Certificate*.
   The *Upload Remote Certificate* window opens.

3. Select *+Upload* and locate the certificate file on your computer.
4. Click *OK*.

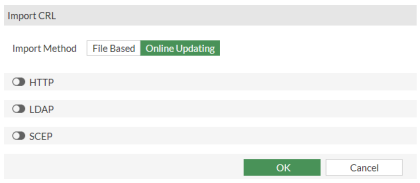
Importing a CRL (Certificate revocation list)

Certificate revocation list (CRL) is a list of certificates that have been revoked and are no longer usable. This list includes certificates that have expired, been stolen, or otherwise compromised. If your certificate is on this list, it will not be accepted. CRLs are maintained by the CA that issues the certificates and includes the date and time when the next CRL will be issued as well as a sequence number to help ensure you have the most current version of the CRL.

CRLs can be imported to FortiPAM.

To import a CRL:

1. Go *System* > *Certificates*.
2. From *+Create/Import*, select *CRL*.
   The *Import CRL* window opens.



3. Enter the following information:

Imported Method	Select either *File Based* or *Online Updating*.
+Upload	Select and locate the certificate file on your computer. **Note**: The option is only available when the *Imported Method* is *File Based*.

HTTP

Enable HTTP updating and enter the *URL of the HTTP server*.

Note: The option disabled by default.

Note: The pane is only available when the *Imported Method* is *Online Updating*.

LDAP

Enable LDAP updating and select an LDAP server from the dropdown or create a new one.

	Use the search bar to look for an LDAP server.

	Use the pen icon next to an LDAP server to edit the server.

Enter the *Username* and the *Password*.

Note: The option disabled by default.

Note: The pane is only available when the *Imported Method* is *Online Updating*.

SCEP

Enable SCEP updating and select a local certificate or create a new certificate for SCEP communication for the online CRL.

	Use the search bar to look for a certificate.

Enter the *URL of the SCEP server*.

Note: The option disabled by default.

Note: The pane is only available when the *Imported Method* is *Online Updating*.

4. Click *OK*.

SNMP

The Simple Network Management Protocol (SNMP) allows you to monitor hardware on your network. You can configure the hardware, such as the FortiPAM SNMP agent, to report system information and traps.

SNMP traps alert you to events that happen, such as a log disk becoming full, or a virus being detected. These traps are sent to the SNMP managers. An SNMP manager (or host) is typically a computer running an application that can read the incoming traps and event messages from the agent and can send out SNMP queries to the SNMP agents.

By using an SNMP manager, you can access SNMP traps and data from any FortiPAM interface configured for SNMP management access. Part of configuring an SNMP manager is to list it as a host in a community on the FortiPAM unit it will be monitoring. Otherwise, the SNMP manager will not receive any traps from, and be unable to query, that FortiPAM unit.

When using SNMP, you must also ensure you have added the correct Management Information Base (MIB) files to the unit, regardless of whether or not your SNMP manager already includes standard and private MIBs in a ready-to-use, compiled database. A MIB is a text file that describes a list of SNMP data objects used by the SNMP manager. See Fortinet MIBs on page 273 for more information.

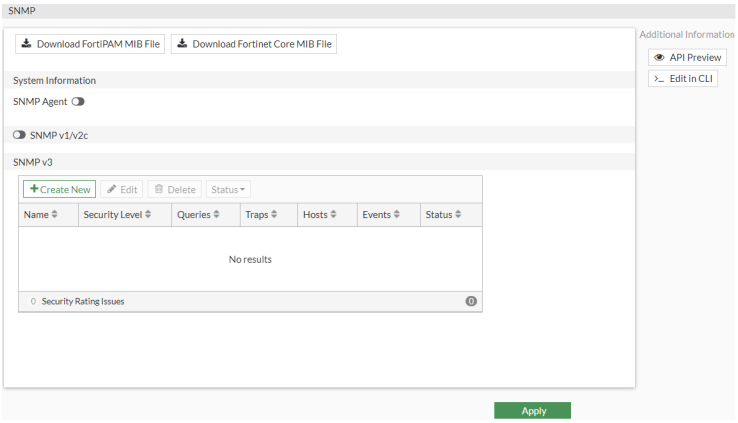
The FortiPAM SNMP implementation is read-only. SNMP v1, v2c, and v3 compliant SNMP managers have read-only access to FortiPAM system information through queries and can receive trap messages from the unit.

The FortiPAM SNMP v3 implementation includes support for queries, traps, authentication, and privacy. Authentication and privacy can be configured in the CLI or the GUI.

For security reasons, Fortinet recommends that neither “public” nor “private” be used for SNMP community names.

If you want to allow SNMP access on an interface, you must go to *Network* > *Interfaces* and select *SNMP* in *Administrative Access* in the settings for the interface that you want the SNMP manager to connect to.

For SNMP configuration, go to *System* > *SNMP*.



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

Configure the following settings and click *Apply*.

Download FortiPAM MIB File	Download the FortiPAM MIB file.
Download Fortinet Core MIB File	Download the Fortinet MIB file. See Fortinet MIBs on page 273.
System Information	
SNMP Agent	Enable the FortiPAM SNMP agent. See SNMP agent on page 274.
SNMP v1/v2c Enable to see the list of the communities for SNMP v1/v2c (disabled by default). From within this section, you can create, edit or remove SNMP communities.	
Create New	Creates a new SNMP community. When you select *Create New*, the *New SNMP Community* page opens. See Creating or editing an SNMP community on page 275.
Edit	Modifies settings within an SNMP community. When you click *Edit*, the *Edit SNMP Community* page opens.
Delete	Removes an SNMP community from the list. To remove multiple SNMP communities, select multiple rows in the list by holding down the `Ctrl` or `Shift` keys and then select *Delete*.
Status	Enable or disable the SNMP community.
Name	The name of the community.
Queries	Indicates whether queries protocols (v1 and v2c) are enabled or disabled. A green check mark indicates that queries are enabled; a red x indicates that queries are disabled.
Traps	Indicates whether trap protocols (v1 and v2c) are enabled or disabled. A green check mark indicates that traps are enabled; a red x indicates that traps are disabled.
Hosts	List of hosts that are part of the SNMP community.
Events	Number of events that have occurred.
Status	Indicates whether the SNMP community is enabled or disabled.
SNMP v3 Lists the SNMP v3 users. From within this section, you can edit, create or remove an SNMP v3 user.	
Create New	Creates a new SNMP v3 user. When you select *Create New*, the *Create New SNMP User* page opens. See Creating or editing an SNMP user on page 277.
Edit	Modifies settings within the SNMP v3 user. When you click *Edit*, the *Edit SNMP User* page opens.

Delete	Removes an SNMP v3 user from the page. To remove multiple SNMP v3 users, select multiple rows in the list by holding down the `Ctrl` or `Shift` keys and then select *Delete*.
Status	Enable or disable the SNMP v3 user.
Name	The name of the SNMP v3 user.
Security Level	The security level of the user.
Queries	Indicates whether queries are enabled or disabled. A green check mark indicates that queries are enabled; a red x indicates that queries are disabled.
Traps	Indicates whether trap protocols (v1 and v2c) are enabled or disabled. A green check mark indicates that traps are enabled; a red x indicates that traps are disabled.
Hosts	List of hosts.
Events	Number of SNMP events associated with the SNMPv3 user.
Status	Indicates whether the SNMPv3 user is enabled or disabled.

Fortinet MIBs

The FortiPAM SNMP agent supports Fortinet proprietary MIBs, as well as standard RFC 1213 and RFC 2665 MIBs. RFC support includes support for the parts of RFC 2665 (Ethernet-like MIB) and the parts of RFC 1213 (MIB II) that apply to FortiPAM unit configuration.

There are two MIB files for FortiPAM units; both files are required for proper SNMP data collection:

- **Fortinet MIB**: contains traps, fields, and information that is common to all Fortinet products.
- **FortiPAM MIB**: contains traps, fields, and information that is specific to FortiPAM units.

The Fortinet MIB and FortiPAM MIB, along with the two RFC MIBs, are listed in the table in this section.

To download the MIB files, go to *System* > *SNMP* and select a MIB link in the SNMP section. See SNMP on page 271.

Your SNMP manager may already include standard and private MIBs in a compiled database that is ready to use. You must add the Fortinet proprietary MIB to this database to have access to the Fortinet-specific information.

MIB files are updated for each version of FortiPAM. When upgrading the firmware, ensure that you update the Fortinet FortiPAM MIB file compiled in your SNMP manager as well.

MIB file name	Description
FORTINET-CORE-MIB.mib	The Fortinet MIB includes all system configuration information and trap information that is common to all Fortinet products. Your SNMP manager requires this information to monitor FortiPAM unit configuration settings and receive traps from the FortiPAM SNMP agent.

MIB file name	Description
FORTINET-FORTIPAM-MIB.mib	The FortiPAM MIB includes all system configuration information and trap information that is specific to FortiPAM units. Your SNMP manager requires this information to monitor FortiPAM configuration settings and receive traps from the FortiPAM SNMP agent. FortiManager systems require this MIB to monitor FortiPAM units.

SNMP get command syntax

Normally, to get configuration and status information for a FortiPAM unit, an SNMP manager would use an SNMP get command to get the information in a MIB field. The SNMP get command syntax would be similar to:

```
snmpget -v2c -c <community_name> <address_ipv4> {<OID> | <MIB_field>}
```

where:

- `<community_name>` refers to the SNMP community name added to the FortiPAM configuration. You can add more than one community name to a FortiPAM SNMP configuration. The most commonly used community name is public. For security reasons, Fortinet recommends that neither public nor private be used for SNMP community names.
- `<address_ipv4>` is the IP address of the FortiPAM interface that the SNMP manager connects to
- `{<OID> | <MIB_field>}` is the object identifier for the MIB field or the MIB field name itself.

For example, to retrieve the serial number of the FortiPAM device, the following command could be issued:

```
snmpget -v2c -c fortinet 192.168.1.110 1.3.6.1.4.1.12356.100.1.1.1.0
```

```
iso.3.6.1.4.1.12356.100.1.1.1.0 = STRING: "FPXVM2TM22000445"
```

In this example, the community name is fortinet, the IP address of the interface configured for SNMP management access is `192.168.1.110`. The serial number of the FortiPAM device is queried using the OID:

`1.3.6.1.4.1.12356.100.1.1.1.0`.

SNMP agent

The FortiPAM SNMP agent must be enabled before configuring other SNMP options. Enter information about the FortiPAM unit to identify it so that when your SNMP manager receives traps from the FortiPAM unit, you will know which unit sent the information.

To configure the SNMP agent in the GUI:

1. Go to *System* > *SNMP*.
2. Enable *SNMP Agent*.
3. Enter a description for the agent. The description can be up to 255 characters long.
4. Enter the physical location of the unit. The system location description can be up to 255 characters long.
5. Enter the contact information for the person responsible for this FortiPAM unit. The contact information can be up to 255 characters.
6. Click *Apply* to save your changes.

To configure the SNMP agent with the CLI:

Enter the following CLI commands:

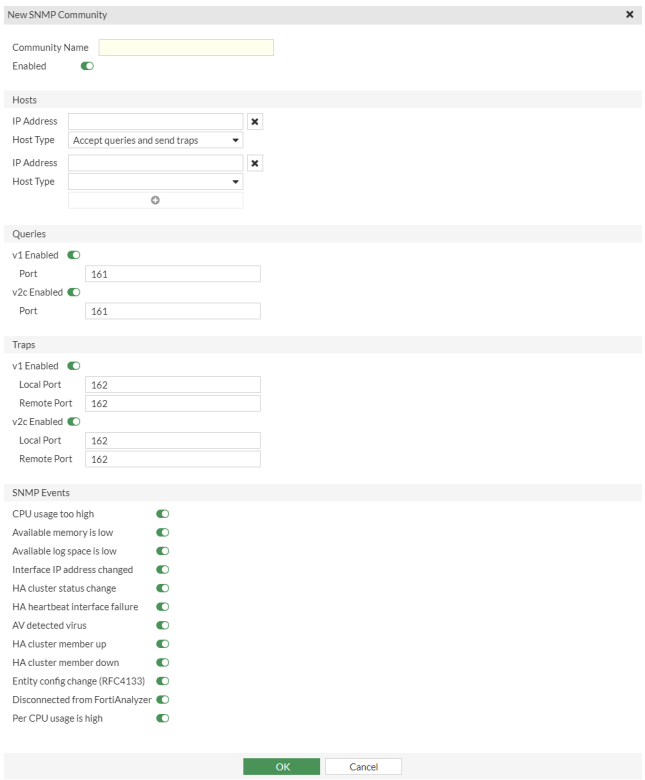
```
config system snmp sysinfo
   set status enable
   set contact-info <contact_information>
   set description <description_of_FortiPAM>
   set location <FortiPAM_location>
end
```

Creating or editing an SNMP community

An SNMP community is a grouping of devices for network administration purposes. Within that SNMP community, devices can communicate by sending and receiving traps and other information. One device can belong to multiple communities, such as one administrator terminal monitoring both a firewall SNMP and a printer SNMP community.

Add SNMP communities to your FortiPAM unit so that SNMP managers can view system information and receive SNMP traps. You can add up to three SNMP communities. Each community can have a different configuration for SNMP queries and traps and can be configured to monitor the FortiPAM unit for a different set of events. You can also add the IP addresses of up to sixteen SNMP managers to each community.

Enabling *SNMP v1/v2c* and selecting *Create New* in the *SNMP v1/v2c* pane opens the *New SNMP Community* page, which provides settings for configuring a new SNMP community. Double-clicking a community from the SNMP v1/v2c table opens the *Edit SNMP Community* page. Alternatively, select a community from the list and then select *Edit* to edit the SNMP community.

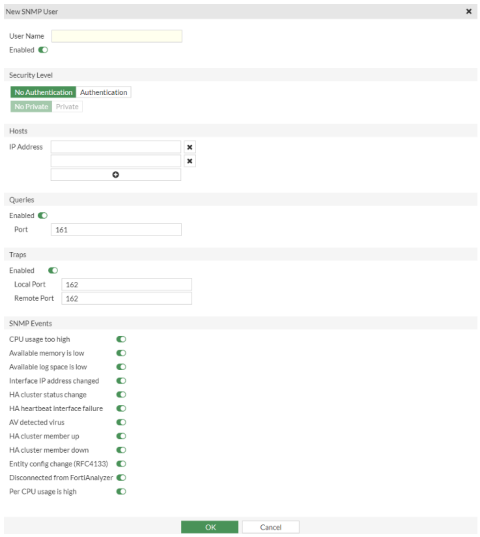


Configure the following settings in the *New SNMP Community* page or *Edit SNMP Community page* and click *OK*:

Community Name	Enter a name to identify the SNMP community. After you create the SNMP community, you cannot edit the name.
Enabled	Enable or disable the SNMP community.
Hosts Settings for configuring the hosts of an SNMP community.	
IP Address	Enter the IP address/netmask of the SNMP managers that can use the settings in this SNMP community to monitor the unit. You can also set the IP address to 0.0.0.0 to so that any SNMP manager can use this SNMP community.
Host Type	Select one of the following: *Accept queries and send traps*, *Accept queries only*, or *Send traps only*.
X	Removes an SNMP manager from the list within the *Hosts* section.
+	Select to add a blank line to the Hosts list. You can add up to 16 SNMP managers to a single community.
Queries Settings for configuring queries for both SNMP v1 and v2c.	
v1 Enabled	Enable or disable SNMP v1 queries.
Port	Enter the port number (161 by default) that the SNMP managers in this community use for SNMP v1 and SNMP v2c queries to receive configuration information from the unit. The SNMP client software and the unit must use the same port for queries.
v2c Enabled	Enable or disable SNMP v2c queries.
Traps Settings for configuring local and remote ports for both v1 and v2c.	
v1 Enabled	Enable or disable SNMP v1 traps.
Local Port	Enter the local port numbers (162 by default) that the unit uses to send SNMP v1 or SNMP v2c traps to the SNMP managers in this community. The SNMP client software and the unit must use the same port for traps.
Remote Port	Enter the remote port number (162 by default) that the unit uses to send SNMP traps to the SNMP managers in this community. The SNMP client software and the unit must use the same port for traps.
v2C Enabled	Enable or disable SNMP v2c traps.
SNMP Events Enable each SNMP event for which the unit should send traps to the SNMP managers in this community. **Note**: The **CPU usage too high** trap's sensitivity is slightly reduced by spreading values out over 8 polling cycles. This reduction prevents sharp spikes due to CPU intensive short-term events such as changing a policy.	

Creating or editing an SNMP user

Selecting *Create New* in the *SNMP v3* pane opens the *New SNMP User* page, which provides settings for configuring a new SNMP v3 user. Double-clicking a user from the SNMP v3 table opens the *Edit SNMP User* page. Alternatively, select an SNMP user and then select *Edit* to edit the SNMP user.



Configure the following settings in the *New SNMP User* page or *Edit SNMP User* page and click *OK*:

User Name	Enter the name of the user. After you create an SNMP user, you cannot change the user name.
Enabled	Enable or disable this SNMP user.
Security Level Select the type of security level the user will have: • *No Authentication* • *Authentication* and *No Private*—Select the authentication algorithm and enter password to use. • *Authentication* and *Private*—Select the authentication and encryption algorithm and enter the passwords to use.	
Authentication/Encryption Algorithm	If the security level is set to *Authentication* and *No Private*, you can select from the following authentication algorithms: • *MD5* • *SHA1* (default) • *SHA224* • *SHA256* • *SHA384* • *SHA512* If the security level is set to *Authentication* and *Private*, you can also select from the following encryption algorithms in addition to authentication algorithms: • *AES* (default) • *DES* • *AES256*

	• *AES256 Cisco*
Password	If the security level is set to *Authentication*, select *Change* and enter a password in the *Password* field.
Hosts Settings for configuring the hosts of an SNMP community.	
IP Address	Enter the IP address of the notification host. If you want to add more than one host, select + to add another host. Up to 16 hosts can be added. Select *X* to delete any hosts.
Queries Settings for configuring queries for both SNMP v1 and v2c.	
Enabled	Enable or disable the query. By default, the query is enabled.
Port	Enter the port number in the *Port* field (161 by default).
Traps Settings for configuring local and remote ports for both v1 and v2c.	
Enabled	Enable or disable the trap.
Local Port	Enter the local port number (162 by default).
Remote Port	Enter the remote port numbers (162 by default).
SNMP Events Select the SNMP events that will be associated with the user.	

Backup

FortiPAM configuration contains not only the system settings but also all user information and secret data. It is crucial to have a backup to avoid data loss. Whenever a hardware failure or system relocation is needed, a new FortiPAM can be easily set up by restoring the previous backup configuration. In the case of accidentally deleting data, you can retrieve the original configuration from the backup and paste the data back.

FortiPAM has two ways to back up its configuration:

- Manually trigger from the user menu. See *Backup and restore* in Admin on page 11.
- Configure automatically and periodically backup to an FTP, SFTP, HTTP or HTTPS server in *System* > *Backup* as discussed here.

System Events, secret logs, and videos are not contained in backup configuration file.

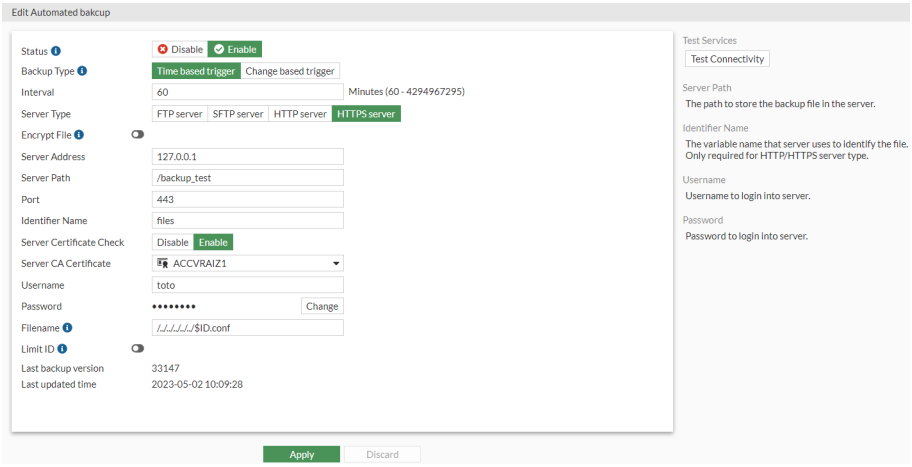
Whenever restoring a backup configuration, keep in mind that the secret password or key may not be the most recent one.

To ensure that all credentials are correct in a configuration file, you can enable maintenance mode first so that no password changer is executed. And then manually trigger the configuration backup. See *Activate maintenance mode* in Admin on page 11.

Generally speaking, the configuration should be backed up consistently and regularly to minimize the amount of data loss between backup copies. The lesser the frequency of backup configurations, the more the risk for data loss when recovering from a backup.

To update automated backup settings:

1. Go to *System* > *Backup*.
   The *Edit Automated backup* window opens.



2. Enter the following information:

Status	Enable or disable automatic backup. **Note**: The option is enabled by default.
Backup Type	Select from the following two options: • *Time based trigger*: FortiPAM sends the backup configuration to the server every *Interval* minutes. • *Change based trigger*: FortiPAM checks the configuration every *Interval* minutes and if the configuration has changed, FortiPAM sends it to the server (default).
Interval	The time interval required in backup, in minutes (default = 60, 60 - 4294967295).
Server Type	Select from the following server types: • *FTP server* (default) • *SFTP server* • *HTTP server* • *HTTPS server*

	 To successfully configure an HTTP/HTTPS server to backup with user authentication, ensure that you have filled in the username and password fields. The backup process will not function correctly if you leave either field empty. Alternatively, you can leave both fields empty if you want to avoid user authentication.
Encrypt File	Enable and enter cipher key to encrypt the backup file.  The administrator must enter the same cipher key when restoring the configuration to FortiPAM. **Note**: The option is disabled by default.
Server Address	The IP address of the server.
Server Path	The path to store the backup file in the server.
Port	The port of the file server. Default values: • 21 (FTP server) (default) • 22 (SFTP server) • 80 (HTTP server) • 443 (HTTPS server)  When upgrading, the port number is set according to the server type (ftp = 21, sftp = 22, http = 80, and https = 443).
Identifier Name	The variable name that server uses to identify the file. **Note**: Only required for *HTTP/HTTPS server* type.
Server Certificate Check	Enable/disable server identity check. This verifies the server domain name/IP address against the server certificate. **Note**: The option is disabled by default. **Note**: The option is only available for *HTTPS server*.
Server CA Certificate	From the dropdown, select a server CA certificate for server certificate check. **Note**: The option is only available when *Server Certificate Check* is enabled.
Username	Username to log in to the server.
Password	Password to log in to the server.
Filename	Filename pattern of the backup configuration. Valid variables are: `$SN $YYYY $MM $DD $hh $mm $ss $ID`. **Note**: The `$ID` variable is mandatory in the filename pattern

	 Enter `$` to get the list of variables.
Limit ID	Enable to limit the value of `$ID` in the file name. The option allows administrators to set a maximum number of backup files (default = 1, 1 - 4294967295) to be stored on a backup server using specific filename patterns. For example, if the backup filename follows the format `PAM-$SN-$ID.conf`, where `$ID` represents the backup ID, when `$ID` reaches the maximum limit, it is reset to 0. The new backup file overwrites the old backup file using the same name.
Last backup version	The last backup version (noneditable).
Last updated time	The date and time when automatic backup was last done (noneditable).

3. Click *Apply*.
4. Click *Test Connectivity* to test the connection to the backup server.

Configuring automated backup settings on the CLI

```
config system backup
   set status {enable | disable}
   set cipher <passwd>
   set type {time-based | change-based}
   set server-type {ftp | sftp | http | https}
   set server-address <string>
   set server-path <path>
   set port <integer>
   set file-field-name <string>
   set server-user <string>
   set server-pass <passwd>
   set filename-pattern {$SN $YYYY $MM $DD $hh $mm $ss $ID}
   set ca-cert <string>
   set server-identity-check {enable | disable}
   set interval <integer>
   set max-id <integer>
   set backup-id <integer>
   set last-version <integer>
   set updated-time <integer>
end
```

Variables	Description
status {enable | disable}	Enable/disable automatic backup (default = enable).
cipher <passwd>	Enter the cipher key.
type {time-based | change-based}	Set the backup type: • `time-based`: Time based trigger. • `change-based`: Change based trigger (default).

Variables	Description
server-type {ftp | sftp | http | https}	Set the server type: • `ftp` (default) • `sftp` • `http` • `https`
server-address <string>	Enter the address of file server.
server-path <path>	Enter the path of file server (default = `/`).
port <integer>	Enter the port number of the file server (default = 21, 1 - 65535).
file-field-name <string>	Enter the field name for file upload (default = `files`).
server-user <string>	Enter the username of the server account.
server-pass <passwd>	Enter the password of the server account.
filename-pattern {$SN $YYYY $MM $DD $hh $mm $ss $ID}	Enter the file name pattern of the backup configuration (default = `$ID.conf`). **Note**: The `$ID` variable is mandatory in the filename pattern.
ca-cert <string>	Enter the CA certificate name.
server-identity-check {enable | disable}	Enable/disable server identity check (verify server domain name/IP address against the server certificate) (default = disable).
interval<integer>	Enter an interval for the backup, in minutes (60 - 4294967295, default = 60).
max-id <integer>	Enter the limit for `backup-id` (default = 0). **Note**: Use 0 to set no limit.
backup-id <integer>	The current backup id number. **Note**: The variable cannot be modified.
last-version <integer>	The last backup version. **Note**: The variable cannot be modified.
updated-time <integer>	The time when the last update was done. **Note**: The variable cannot be modified.

Example CLI configuration - Example

Backup to SFTP/FTP server

```
config system backup
   set status enable
   set server-type sftp
   set server-address "10.59.112.254"
   set server-path "backup/"
   set port 22
   set server-user "sftp_user"
   set server-pass <sftp_user_password>
   set filename-pattern "$SN-$YYYY-$MM-$DD-$hh-$mm-$ss-$ID.conf"
end
```

Backup to HTTPS/HTTP server

```
config system backup
   set status enable
   set server-type https
   set server-address "10.59.112.254"
   set server-path "/http_user/upload.php"
   set port 443
   set file-field-name "file"
   set server-user "http_user"
   set server-pass QA@fortinet
   set filename-pattern "$SN-$ID.conf"
   set ca-cert "ACCVRAIZ1"
   set server-identity-check enable
end
```

If user authentication is not required for HTTP and HTTPS servers, `server-user` and `server-pass` variables are not required.

Following is an example of php file to accept the submitted backup file.

```
fwd-svr@fwdsvr-virtual-machine:/var/www/html/http_user$ cat upload.php
<?php
   $name = $_FILES['file']['name'];
   $temp = $_FILES['file']['tmp_name'];
   if(move_uploaded_file($temp,"backup/".$name)){
   echo "Your file was uploaded";
   }
   else
   {
   echo "Your file couldn't upload";
   }
?>
```

Sending backup file to a server - Example

The example shows how an administrator can verify system backup configuration and the connection to the backup server.

To send a backup file to a server:

1. In the CLI console, enter the following commands:
   ```
   diagnose debug enable
   diagnose test application wad 1000
   ....
   ....
Process [13]: type=secret-approval(14) index=0 pid=1080 state=running
 diagnosis=yes debug=enable valgrind=supported/disabled
   ```
2. Find the process with the `type secret-approval` and the index.
   In the example above, the process `type` is `14` and `index` is `0`.
3. Generate the diagnosis process using `2<process type><index>`.
   In the example above, the diagnosis process is `21400`.
4. Enter the following command:
   ```
   diagnose test application wad 21400
   ```

```
Set diagnosis process: type=secret-approval index=0 pid=1080
```

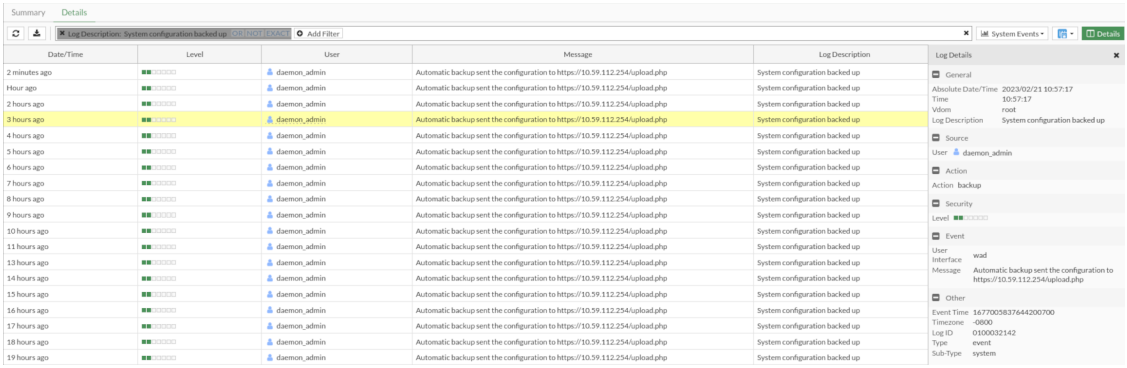
5. Enter the following command:

```
diagnose test application wad
WAD process 1080 test usage:
....
701: Test sending file using backup config
```

6. Enter the following command:

```
diagnose test application wad 701
Sending backup to server using system.backup settings manually.
Finished sending backup to server. Check to see if backup file was successfully
uploaded.
```

Additionally, you can check *System Events* in *Log & Report* > *Events* to determine whether the system configuration backup process was successful.



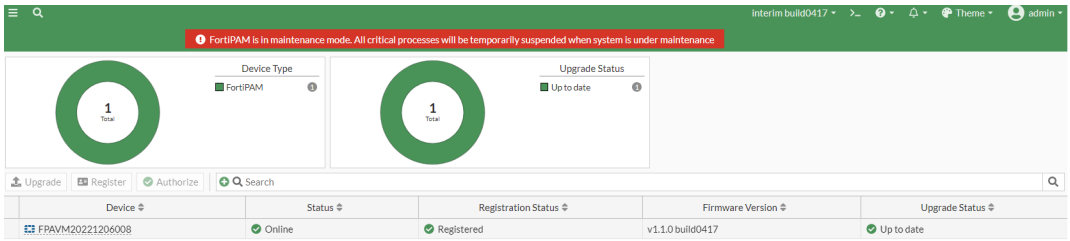
Firmware

The FortiPAM firmware can be upgraded from *System* > *Firmware*.

The widgets at the top display:

- The total number of FortiPAM devices.
- The upgrade status of the FortiPAM devices.

The *Firmware* tab displays the device name, device status, registration status, firmware version, and the upgrade status.



The following options are available in the *Firmware* tab:

Upgrade	Upgrade the FortiPAM firmware. See Uploading a firmware on page 13.

Register	
Authorize	
Search	Enter a search term in the search field, then hit `Enter` to search. To narrow down your search, see Column filter.

Upgrading the firmware

Periodically, Fortinet issues firmware upgrades that fix known issues, add new features and functionality, and generally improve your FortiPAM experience.

Before proceeding to upgrade the system, Fortinet recommends that you back up the configuration. See Backup and restore on page 14.

To be able to upgrade the firmware, you must first register your FortiPAM with Fortinet. See Licensing on page 29.

To upgrade the firmware from FortiPAM GUI, see Uploading a firmware on page 13.

Always review all sections in *FortiPAM Release Notes* prior to upgrading your device.

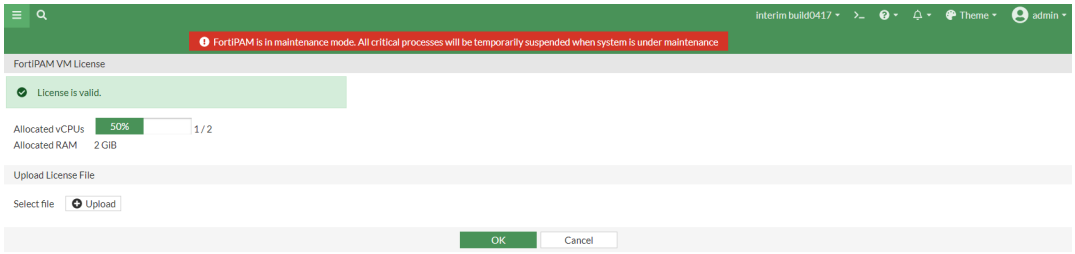
FortiPAM license

The FortiPAM-VM license can be uploaded from *System* > *FortiPAM License*.

You must be in maintenance mode to be able to upload a license. See Maintenance mode in Admin on page 11.

To upload a new license:

1. Go to *System* > *FortiPAM License*.
   The *FortiPAM VM License* window opens.



2. In the *Upload License File* pane, select *Upload* and browse to the license file on your management computer.

3. Click *OK*.
4. After the boot up, the license status changes to valid.

Use the CLI command `get system status` to verify the license status.

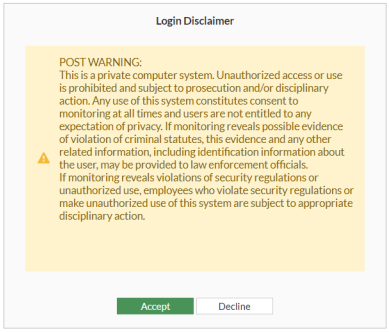
FortiGuard license

Go to *System* > *FortiGuard License* to configure FortiGuard subscription services. See FortiGuard Distribution Network on page 41.

Disclaimers via the CLI

FortiPAM allows you to set up login disclaimers.

Once you are successfully authenticated, a login disclaimer banner appears. You must click *Accept* to access FortiPAM. If you click *Decline*, you are logged out immediately.



Starting FortiPAM 1.1.0, you can set up login disclaimers in the GUI using the *Login Disclaimer* toggle and the text box available in the *PAM Settings* pane in *System* > *Settings*.

Disclaimers via the CLI - Example

To configure a login disclaimer:

1. In the CLI console, enter the following command to enable the login disclaimer:

```
config system global
   set post-login-banner enable #display the administrator access disclaimer message
        after an administrator successfully logs in
end
```

2. In the CLI console, enter the following commands to set up the login disclaimer:

```
config system replacemsg admin post_admin-disclaimer-text
   set buffer "POST WARNING:
      This is a private computer system. Unauthorized access or use is prohibited and
           subject to prosecution and/or disciplinary action. Any use of this system
           constitutes consent to monitoring at all times and users are not entitled
           to any expectation of privacy. If monitoring reveals possible evidence of
           violation of criminal statutes, this evidence and any other related
           information, including identification information about the user, may be
           provided to law enforcement officials. If monitoring reveals violations of
           security regulations or unauthorized use, employees who violate security
           regulations or make unauthorized use of this system are subject to
           appropriate disciplinary action."
   set header none
   set format text
end
```

The disclaimer must begin and end with quotation marks.

Troubleshooting

FortiPAM operation requires multiple components to work together. Generally, a browser and FortiClient are necessary on the client side to connect to the FortiPAM GUI. Secrets on FortiPAM can then be used to connect to the target host.

If the FortiPAM system runs abnormally, pinpointing the failed component can be challenging. This chapter presents the usage of built-in debug tools to speed up finding errors.

You must have system administrator and CLI permissions to use the debug features including debug trace files. See Role on page 174.

To use FortiPAM debug feature, debug category and level must be set.

In the CLI console, enter the following commands to set debug category and level:

```
diagnose wad debug enable category <category>
diagnose wad debug enable level <level>
```

For example:

```
diagnose wad debug enable category session #The category is session
diagnose wad debug enable level info #The level is set to info
```

For debug level settings, all the higher level traces are included, e.g., when the debug level is set to `info`, `error` and `warn` levels are displayed too, but `verbose` is hidden.

Once the `category` and `level` variables are set up in the CLI, traces are displayed in the CLI.

For more troubleshooting information and a Q&A section, check out the FortiPAM Community page: https://community.fortinet.com/t5/FortiPAM/tkb-p/TKB52.

Troubleshoot using trace files

To successfully capture each daemon's trace as separate log files, use FortiPAM debug trace files. You can then view each file and locate the source of an issue.

To use FortiPAM trace file debug feature, debug category and level must be set. See Troubleshooting on page 288.

Related CLI commands:

Command	Description
diagnose wad debug file {enable | disable}	Enable/disable dump trace to files.
diagnose wad debug file max_ size <size>	Set the maximum size for trace files.
diagnose wad debug file overwrite {enable | disable}	Allow overwriting when the file reaches maximum size.
diagnose wad debug file clear	Clear all the trace files.
diagnose wad debug file list	Show all trace related file stats.
diagnose wad debug file show {trace_file_name | all}	Show a specific or all trace file content.
diagnose wad debug file send tftp <addr> <save_zip_name.tar.gz>	Send trace files to TFTP server.
diagnose wad debug file send ftp <save_zip_name.tar.gz> <addr>: [port] [username] [password]	Send trace files to FTP server.

Example troubleshooting - example

1. In the CLI console, enter the following commands to set debug category and level:
   ```
   diagnose wad debug enable category secret
   diagnose wad debug enable level info
   ```
2. Enter the following command to set the maximum size for trace files:
   ```
   diagnose wad debug file max-size 2
   ```
3. Enter the following command to enable dump trace to files:
   ```
   diagnose wad debug file enable
   ```
   Trace file is displayed now.
4. Enter the following command to disable dump trace to files:
   ```
   diagnose wad debug file disable
   ```
5. Enter the following command to show all trace related file stats:
   ```
   diagnose wad debug file list
   size:0000000000, wad_worker-1.log
   size:0000000000, wad_cert-inspection-0.log
   size:0000000000, wad_debug-0.log
   size:0000000000, wad_algo-0.log
   size:0000000000, wad_user-info-0.log
   size:0000000000, wad_dispatcher-0.log
   ```

```
size:0000000000, wad_secret-approval-0.log
size:0000000000, wad_config-notify-0.log
size:0000000000, wad_informer-0.log
size:0000000000, wad_YouTube-filter-cache-service-0.log
size:0000006869, wad_worker-0.log
size:0000000000, wad_pwd-changer-0.log
size:0000000000, wad_manager-0.log
```

6. Enter the following command to clear all the trace files:
   ```
   diagnose wad debug clear
   ```
7. Enter the following command to show a specific file content:
   ```
   diagnose wad debug file show wad_worker-0.log
   ```

```
[I][p:1066][s:369910368][r:2588] wad_gui_secret_handler :4123 Successfully fetched
     database list for admin
[I][p:1066][s:369910368][r:2588] wad_gui_secret_handler :4510 attach response body to
     response
[I][p:1066][s:369910368][r:2590] wad_gui_secret_handler :4060 METHOD OVERRIDE to GET,
     fetching list
[I][p:1066][s:369910368][r:2590] wad_gui_secret_folder_post_select :1669 Dev is NULL
[I][p:1066][s:369910368][r:2590] wad_gui_secret_folder_post_select :1715 filter gets
     all personal secret folders
[I][p:1066][s:369910368][r:2590] wad_gui_secret_handler :4088 Successfully fetched
     folder list for admin
[I][p:1066][s:369910368][r:2590] wad_gui_secret_handler :4510 attach response body to
     response
[I][p:1066][s:369910370][r:2592] wad_gui_secret_handler :4060 METHOD OVERRIDE to GET,
     fetching list
[I][p:1066][s:369910370][r:2592] wad_gui_secret_folder_post_select :1669 Dev is NULL
[I][p:1066][s:369910370][r:2592] wad_gui_secret_handler :4088 Successfully fetched
     folder list for admin
.
.
```

FortiPAM HTTP filter

When turning on the HTTP category debug, it can generate a lot of traces from the GUI. In the case where GUI traffic is not needed, using the FortiPAM HTTP filter helps clean out traffic that is not required.

You must have system administrator and CLI permissions to use the FortiPAM HTTP filter.

To use the FortiPAM trace filter feature:

1. In the CLI console, enter the following command to set the debug category to http:
   ```
   diagnose wad debug enable category http
   ```
2. Optionally, enter the following command to set the debug level:
   ```
   diagnose wad debug enable level <level>
   ```
3. Use the following CLI command to set up a filter for the FortiPAM traffic:
   ```
   diagnose wad filter pam
   ```

Variable	Description
none	Reset FortiPAM filter setting. All the HTTP traffic traces are displayed.
internal	Internal FortiPAM trace. HTTP traffic with `/pam api-gateway` is displayed, e.g., FortiClient and secret launcher traffic.
tcp-forward	TCP-forward trace. Traffic trace with `/tcp api-gateway` is displayed, e.g., TCP tunneling information when starting a launcher.
both	Internal FortiPAM and TCP-forward trace. HTTP traffic with `/tcp` and `/pam api-gateway` is displayed.

For most cases, the `both` option is recommended for the filter.

The FortiPAM filter can be used with `diagnose wad filter drop-unknown-session 1` to ignore more information during session initialization.

- Examples

1. Turning on `drop-unknown-session` with the `internal` option (`diagnose wad filter pam internal`) and launching a secret shows the following trace:

```
PAM # [I][p:1070][s:930509823][r:2694] wad_http_req_proc_policy: 10453 ses_
     ctx:ct|Pvx|M|H|C|A1 fwd_srv=<nil>[I][p:1070][s:930509823][r:2694] wad_dump_fwd_
     http_resp: 2663 hreq=0x7f34b46a2e58 Forward response from Internal:
HTTP/1.1 200 OK
Content-Type: application/json
Content-Length: 309
[I][p:1070][s:930509826][r:2701] wad_dump_fwd_http_resp: 2663 hreq=0x7f34b46a2e58
     Forward response from Internal:
HTTP/1.1 200 OK
Proxy-Agent: FortiPAM/1.0
X-Range: bytes=773458-
Content-Length: 0
```

2. Turning on `drop-unknown-session` with the `tcp-forward` option (`diagnose wad filter pam tcp-forward`) and launching a secret shows the following trace:

```
[I][p:1070][s:930509852][r:2799] wad_http_req_check_vs_tunnel_type :5182 Check redir
     PROXY port=22((null))
[I][p:1070][s:930509852][r:2799] wad_http_req_check_vs_tunnel_type :5190 TCP tunnel
     detected without type.
[I][p:1070][s:930509852][r:2799] wad_dump_fwd_http_resp :2663 hreq=0x7f34b46a41f8
     Forward response from Internal:
HTTP/1.1 101 Switching Protocols
Upgrade: tcp-forwarding/1.0
Connection: Upgrade
```

Appendix A: Installation on KVM

Once you have downloaded the `fortipam.qcow2` you can create the virtual machine in your KVM account.

To deploy FortiPAM virtual machine:

1. Launch *Virtual Machine Manager* on your KVM host server.
2. From the Virtual Machine Manager (VMM) home page, select *Create a new virtual machine*.
3. Select *Import existing disk image* and select *Forward*.
4. Select *Browse*.
   If you saved the `fortipam.qcow2` file to */var/lib/libvirt/images*, it will be visible on the right. If you saved it somewhere else on your server, select *Browse Local*, find it, and select *Open*.
5. Select the *OS type* as *Generic default* and select *Forward*.
6. Specify the amount of memory and the number of CPUs to allocate to this virtual machine.
   You can set the memory as 4GB and the CPUs to 4.
   Select *Forward*.
7. Enter the name for the VM.
   A new VM includes one network adapter by default.
8. Check *Customize configuration* before installation, and select *Finish*.

To add additional hard disks:

Before opening your virtual machine for the first time you will need to configure two additional hard disks.

1. Click *Add Hardware* in the Virt-manager application, and select the option to add an additional storage disk.
2. For the *Storage size*, select a size according to the disk sizing guidelines. See *System requirements* in the *KVM Admin Guide*.
3. For *Bus type* select *VirtIO*.
4. Click *Finish*.

To add ethernet interfaces:

Before opening your virtual machine for the first time you will need to configure two ethernet interfaces.

1. In the Virtual Machine Manager, locate the VM name, then select *Open* from the toolbar.
2. Select `NIC:xxxx`; the default network adapter.
3. In *Network source* dropdown, select `Host device enxxxx: macvtap`.
4. In the *Device model* dropdown, select *virtio*.
5. Click *Apply*.
6. Click *Add Hardware*, and select the option to add an additional interface.
7. In the *Device model* dropdown, select *virtio*.
8. Select *Finish*.
9. Click *Begin Installation* to start installing the new VM.

To add log/video disks or modify disk sizes after first powering up FortiPAM-VM:

1. In the CLI console, enter `sh sys storage` to verify that the disk size change was successful:

```
config system storage
   edit "HD1"
      set status enable
      set media-status enable
      set order 1
      set partition "LOGUSEDX83555B0F"
      set device "/dev/vda1"
      set size 20029
      set usage log
   next
   edit "HD2"
      set status enable
      set media-status enable
      set order 2
      set partition "PAMVIDEOBAED79CD"
      set device "/dev/vdb1"
      set size 301354
      set usage video
   next
   edit "HD3"
      set status enable
      set media-status disable
      set order 3
      set partition ''
      set device ''
```

If the displayed disk size is not what you had configured, enter the following command to format the log and the video disk:

```
execute disk format <disk_ref>
```

Note: `<disk_ref>` can be checked using the command execute disk list.

HD1 is used for the log disk and the `disk_ref` is 256.

HD2 is used for the video disk and the `disk_ref` is 16.

In the above example, disks can be formatted by entering the following commands:

```
execute disk format 256 #HD1
execute disk format 16 #HD2
```

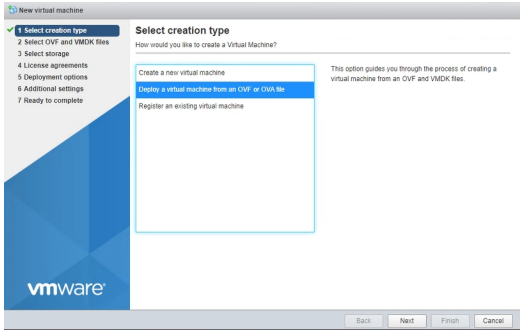
Disk formatting results in the loss of all existing logs and videos.

Appendix B: Installation on VMware

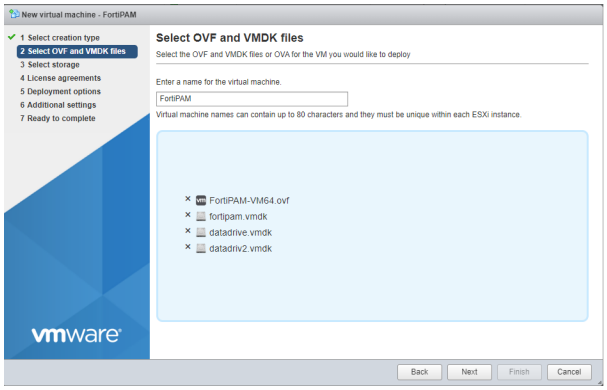
Once you have downloaded the `out.ovf.zip` file and extracted the package contents to a folder on your management computer, you can deploy it into your VMware environment.

To deploy the FortiPAM-VM OVF template:

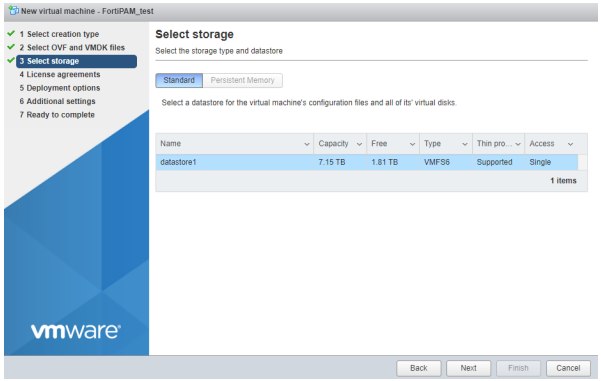
1. Connect to your VMware ESXi server by visiting its URL in your browser. Enter your username and password, and click *Log in*.
2. Select *Create/Register VM*.
   The VM creation wizard opens.
3. Select *Deploy a virtual machine from an OVF or OVA file*, and click *Next*.



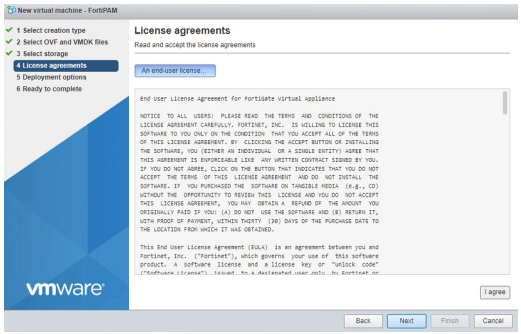
4. Enter a name for your VM and select the files (FortiPAM-VM64.ovf, fortipam.vmdk, datadrive.vmdk, and datadriv2.vmdk) previously extracted to your management computer, and click *Next*.



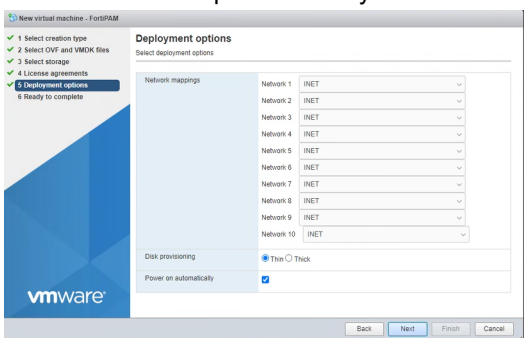
5. Select which ESXi server's datastore to use for the deployment of FortiPAM-VM, and click *Next*.



6. Read the licensing terms and click *I agree* and *Next*.

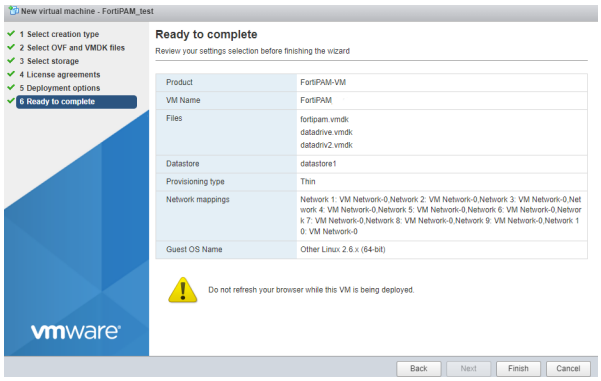


7. Select the appropriate network mappings, disk provisioning, and power on options for your deployment, and click *Next*.
   - **Thin Provision**: This option optimizes storage use at the cost of sub-optimal disk I/O rates. It allocates disk space only when a write occurs to a block, but the total volume size is reported by VMFS to the OS. Other volumes can take the remaining space. This allows you to float between your servers and expand storage when your size monitoring indicates there is a problem. Once a Thin Provisioned block is allocated, it remains in the volume regardless of whether you have deleted data, etc.
   - **Thick Provision**: This option has higher storage requirements, but benefits from optimal disk I/O rates. It allocates the disk space statically. No other volumes can take the allocated space.

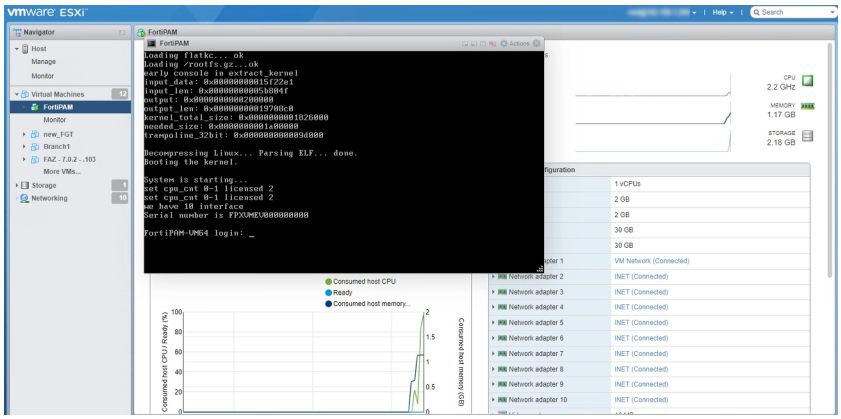


   By default, the log disk and video disk size are 30 GB. If you want to change the size, unselect *Power on automatically* to ensure that any disk size change is made before first powering on the VM.

8. Review the summary of your VM settings, and click *Finish*.



9. Select your newly created VM and launch it.
The VM console will be displayed where you can monitor the booting progress of your FortiPAM-VM.



See FortiPAM appliance setup on page 24 for CLI related settings to verify the disk usage type and set up FortiPAM.

10. The default size for the log and the video disk is 30 GB. If the size does not meet your requirement, see *Log and video disk size guidelines* in *System requirements* in the *VMware ESXi Admin Guide*.

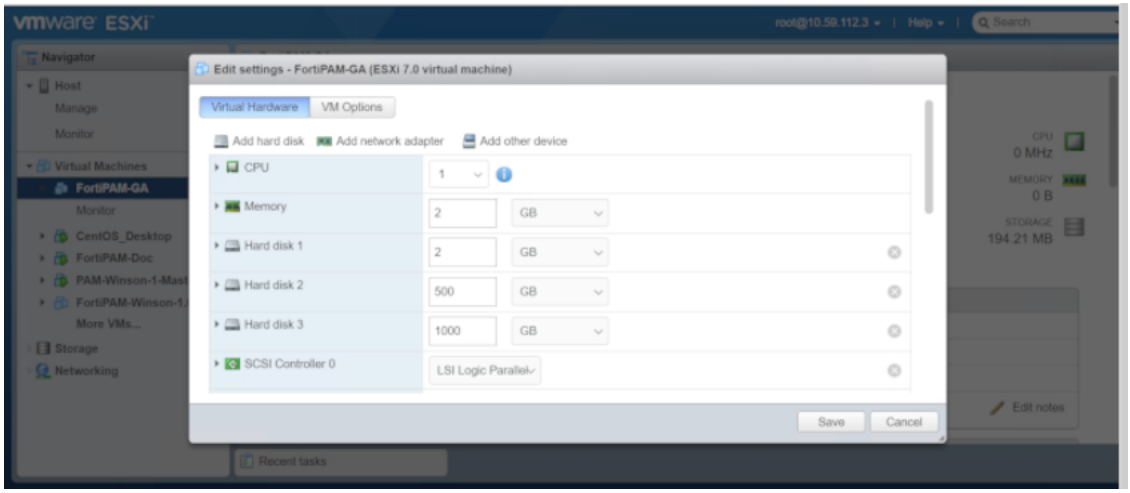
To adjust the log or video disk size:

Disk size tuning results in the loss of existing logs and videos.

---

a. Shutdown your VM.
b. In the VMware vSphere Client, right-click the name of the virtual appliance, and select *Edit settings*.
The *Edit settings* page is displayed.
c. Ensure that you are in the *Virtual Hardware* tab.
d. Keep *Hard disk 1* as 2 GB. *Hard disk 1* is used for FortiPAM bootup.

e. Adjust *Hard disk 2* for log disk size and adjust *Hard disk 3* for video disk size.



f. Click *Save* to save the changes.
You can now power on the VM.

11. If *Power on automatically* is unselected in step 7 and the VM has never been powered on, any disk size change automatically takes effect after the VM is powered on the first time.
If the disk sizes are tuned after powering on the VM for the first time, enter `sh sys storage` CLI command to verify that the disk size change was successful:

```
config system storage
   edit "HD1"
      set status enable
      set media-status enable
      set order 1
      set partition "LOGUSEDX83555B0F"
      set device "/dev/vda1"
      set size 20029
      set usage log
   next
   edit "HD2"
      set status enable
      set media-status enable
      set order 2
      set partition "PAMVIDEOBAED79CD"
      set device "/dev/vdb1"
      set size 301354
      set usage video
   next
   edit "HD3"
      set status enable
      set media-status disable
      set order 3
      set partition ''
      set device ''
```

If the displayed disk size is not what you had configured, enter the following command to format the log and the video disk:

```
execute disk format <disk_ref>
```

Note: `<disk_ref>` can be checked using the command execute disk list.

HD1 is used for the log disk and the `disk_ref` is 256.

HD2 is used for the video disk and the `disk_ref` is 16.

In the above example, disks can be formatted by entering the following commands:

```
execute disk format 256 #HD1
execute disk format 16 #HD2
```

Disk formatting results in the loss of all existing logs and videos.

Appendix C: Installing vTPM package on KVM and adding vTPM to FortiPAM-VM

For added security when installing FortiPAM on KVM, vTPM package must be installed, and vTPM added to the FortiPAM-VM.

To install vTPM package on KVM (Ubuntu):

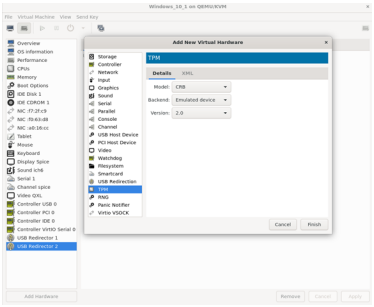
1. In the command line, enter the following commands:

```
mkdir TPM_WorkSpace
cd TPM_WorkSpace/
git clone https://git.seabios.org/seabios.git
git clone https://github.com/stefanberger/libtpms.git
ls
cd libtpms
sudo apt-get -y install automake autoconf libtool gcc build-essential libssl-dev dh-
     exec pkg-config gawk
./autogen.sh --with-openssl --with-tpm2
make dist
dpkg-buildpackage -us -uc -j$(nproc)
cd ..
ls
sudo dpkg -i libtpms0_0.10.0~dev1_amd64.deb libtpms-dev_0.10.0~dev1_amd64.deb
git clone https://github.com/stefanberger/swtpm.git
cd swtpm
sudo su
ln -s /dev/null /etc/systemd/system/trousers.service
exit
sudo apt-get -y install libfuse-dev libglib2.0-dev libgmp-dev expect libtasn1-dev
     socat tpm-tools python3-twisted gnutls-dev gnutls-bin softhsm2 libseccomp-dev
     dh-apparmor libjson-glib-dev
dpkg-buildpackage -us -uc -j$(nproc)
dpkg -i swtpm_0.8.0~dev1_amd64.deb swtpm-dev_0.8.0~dev1_amd64.deb swtpm-libs_
     0.8.0~dev1_amd64.deb swtpm-tools_0.8.0~dev1_amd64.deb
```

To add vTPM when creating a FortiPAM-VM:

1. Deploy FortiPAM, see Appendix A: Installation on KVM on page 292.
2. Before opening the virtual machine for the first time, in the Virt-manager application, click *Add Hardware*.
3. From the menu, select *TPM*.
4. In the *Details* tab:
   a. In *Model*, select *CRB*.
   b. In *Backend*, select *Emulated device*.
   c. In *Version*, select *2.0*.

d. Click *Finish*.



This adds *TPM v2.0* to the list of hardware devices on the left.

Appendix D: vTPM for FortiPAM on VMware

To successfully enable vTPM, you must configure a key provider on the VMware vSphere client.

Ensure that TPM is set up as part of the initial configuration, i.e., before powering on the FortiPAM-VM for the first time.

To configure a key provider:

1. Select the virtual appliance in the VMware vSphere client and go to *Configure* > *Security* > *Key Providers*.
2. In *Key Providers*, from the *Add* dropdown, select *Add Native Key Provider*.
3. In the *Add Native Key Provider* window:
   a. Enter a name for the native key provider.
   b. Deselect *Use key provider only with TPM protected ESXi hosts*.
   c. Select *ADD KEY PROVIDER*.
4. Select the new key provider from the key providers list and then select *BACK UP*.
   The *Back up Native Key Provider* window opens.
5. Select *BACK UP KEY PROVIDER*.
   The key provider is saved on your computer.

To enable vTPM for FortiPAM:

1. Right-click the virtual appliance in the VMware vSphere client and select *Edit Settings*.

Ensure that the *Guest OS Version* in *VM Options* tab is set to *Other 4.x or later Linux (64-bit)* or higher.

2. In *Edit Settings*, click *Add New Device* and select *Trusted Platform Module*.
3. Click *OK*.

Appendix E: Enabling soft RAID on KVM or VMware

To expand hard disk capacity, you can enable RAID on the FortiPAM-VM. After RAID is enabled, hard disk capacity can be expanded from 2 TB to 16 TB.

Individual disks of sizes up to 2 TB are supported.

Starting FortiPAM 1.1.0, the disk size is limited by the GPT partition size.

Soft RAID is supported on KVM and VMware platforms. Hyper-V and other platforms are not supported yet.

Note: Soft RAID for VMware requires disks of the same size.

RAID can only be configured using the CLI commands.

Enabling, disabling, and changing the RAID level, erases all the data on the log and video disk. Also, the FortiPAM device reboots every time RAID is enabled, disabled, or the RAID level is changed.

To configure RAID via CLI:

1. Before enabling RAID, enter the following command in the CLI console to verify that the FortiPAM has multiple disks:
   ```
   execute disk list
   ```
   or
   ```
   diagnose hardware deviceinfo disk
   ```

   Use `diagnose system disk info` to check the disk-related information.

2. In the CLI console, enter the following command to enable RAID:
   ```
   execute disk raid enable <RAID level> #The default value is Raid-0
   ```
   Two partitions will be created after RAID is enabled. One partition for log and one for video.

   To disable RAID, enter `execute disk raid disable`.

When there are two disks, RAID `level 0` and `1` are available. Only when there are four disks, RAID `level 5` and `10` are available.

3. From the *Admin* dropdown in the banner, go to *System* > *Reboot* to reboot FortiPAM.

Reboot is only available when FortiPAM is in maintenance mode.
To enable the maintenance mode, see Enabling maintenance mode.

4. In the *Reboot* window, click *OK* to confirm.
Optionally, enter an event log message.
5. For the FortiPAM-VM, in the CLI console, check the RAID status by entering the following command:

```
execute disk raid status #Raid is now available
```

If the above steps do not enable RAID on FortiPAM-VM, use the following workaround:
1. Factory reset your FortiPAM-VM.
2. Remove disk from your FortiPAM-VM, then add the disk again.
3. Now follow the steps in Configuring RAID via CLI.

Rebuilding a RAID with a different RAID level

Admin can only rebuild RAID at the same RAID level if a RAID error has been detected. Also, changing the RAID level takes a while and deletes all data on the disk.

Use the following CLI command to rebuild RAID:

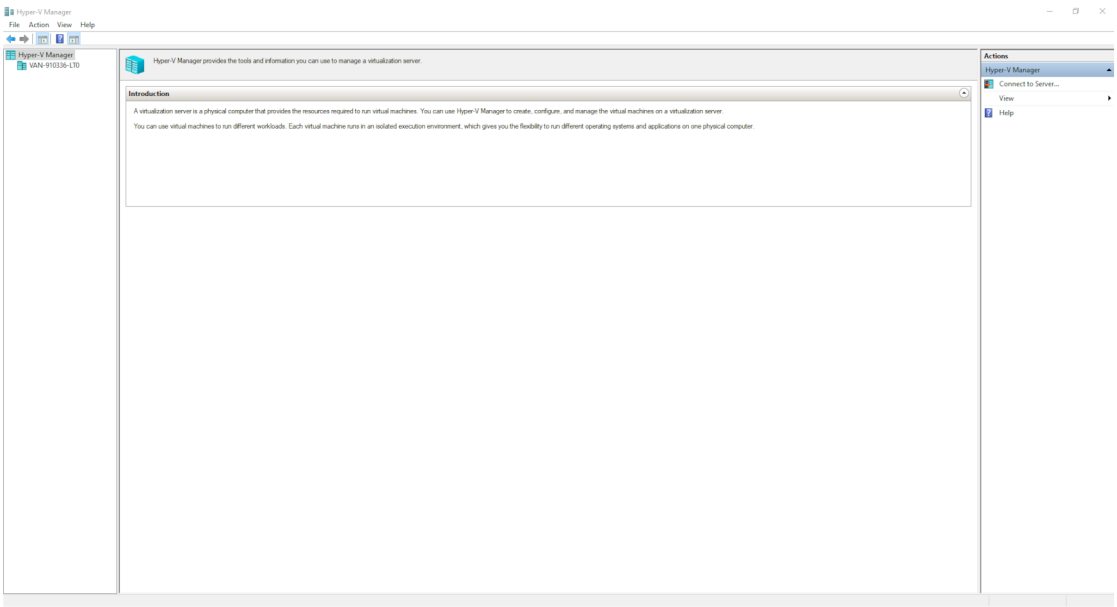
```
execute disk raid rebuild-level <RAID level>
```

Appendix F: Installation on Hyper-V

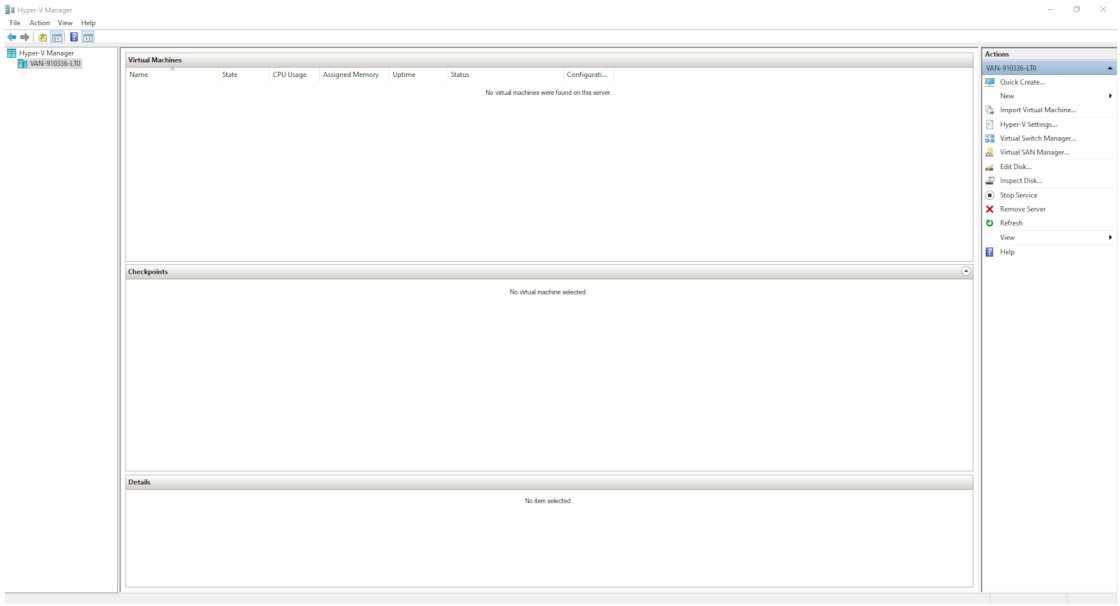
Once you have downloaded the `out.hyperv.zip` file and extracted the package contents to a folder on your management computer/Microsoft server, you can deploy the VHD package to your MS Hyper-V environment.

To deploy FortiPAM-VM on MS Hyper-V without TPM support:

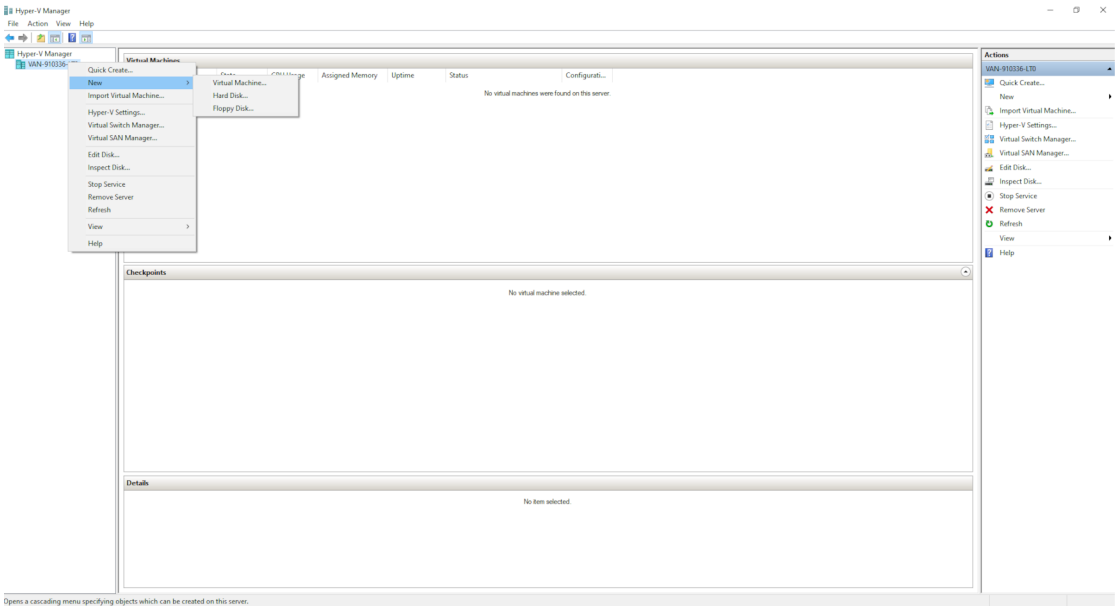
1. Launch the Hyper-V Manager on your management computer.
   The *Hyper-V Manager* homepage opens.



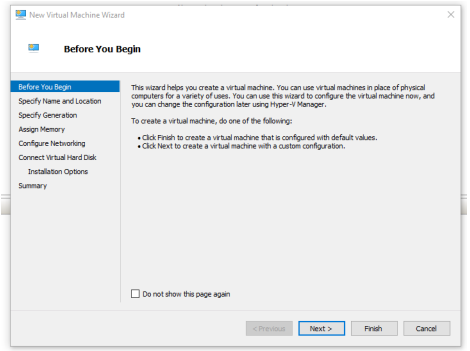
2. In the left tree menu, select your management computer.
   The server details page is displayed.



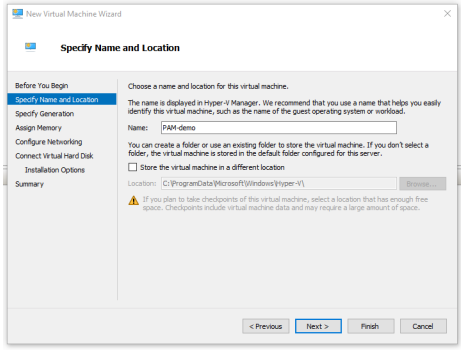
3. Right-click the server/management computer and select *New* > *Virtual Machine*. Optionally, in the *Action* menu, select *New* and select *Virtual Machine*.



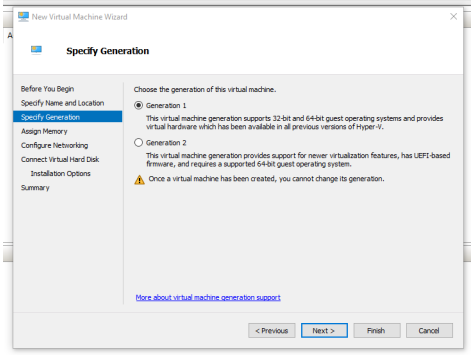
The *New Virtual Machine Wizard* opens.



4. In *New Virtual Machine Wizard*, click *Next* to create a VM with a custom configuration.
   The *Specify Name and Location* tab is displayed.
5. In *Specify Name and Location*, enter a name for this VM, and click *Next*.
   The *Hyper-V Manager* displays the name you enter for the VM.

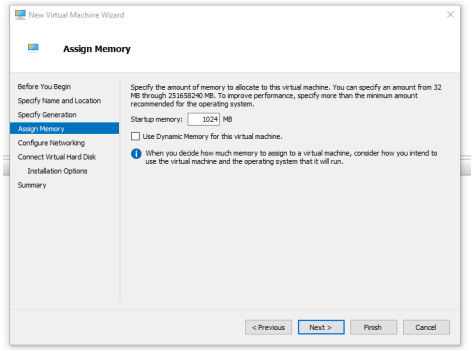


6. In *Specify Generation*, select *Generation 1*, and click *Next*.



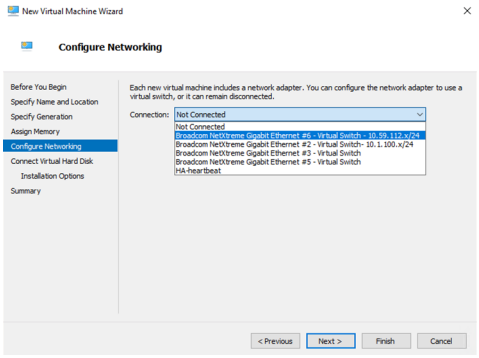
Generation 1 does not support TPM. To install FortiPAM-VM on Hyper-V with TPM, see Deploying FortiPAM on Hyper-V with TPM.

7. In *Assign Memory*, specify the amount of memory to allocate to this VM in *Startup memory*, and click *Next*.
   Ensure that *Use Dynamic Memory for this virtual machine* is unchecked.

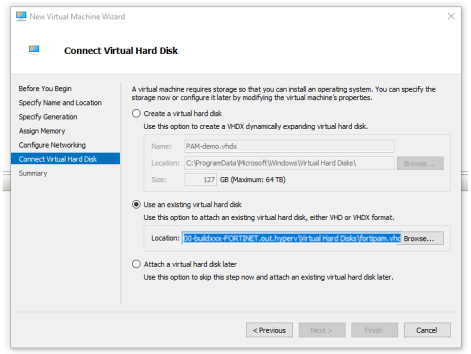


FortiPAM configured with less than 2 CPUs and 2048 MB of RAM works in the evaluation mode until licensed. Otherwise, a valid license is required.

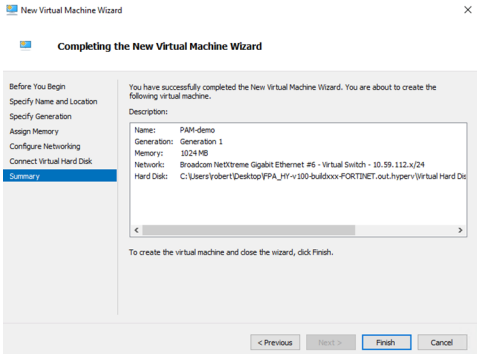
8. In *Configure Networking*, from the *Connection* dropdown, select a network adapter, and click *Next*.
   Each new VM includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected. You can configure more network adapters in the *Settings* window later.



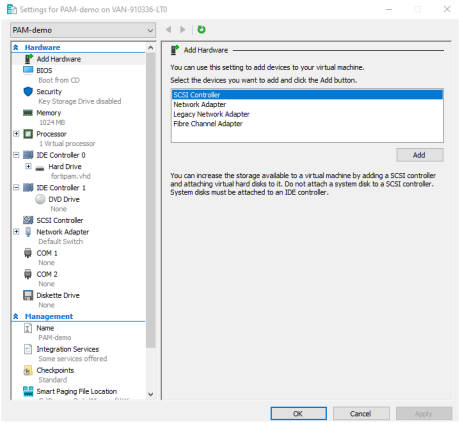
9. In *Connect Virtual Hard Disk*, select *Use an existing virtual hard disk*, click *Browse* and locate the `fortipam.vhd` file that you downloaded from FortiCloud, and click *Next*.



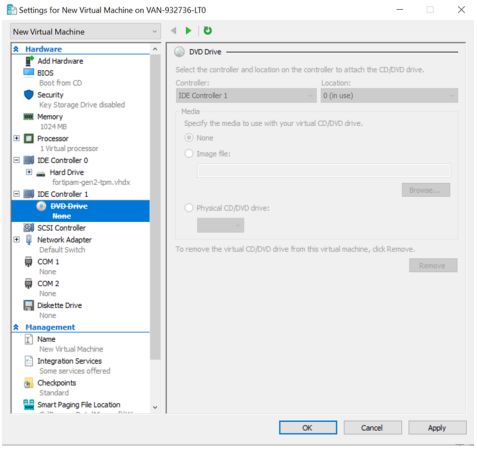
10. In *Completing the New Virtual Machine Wizard*, the installation summary is displayed.



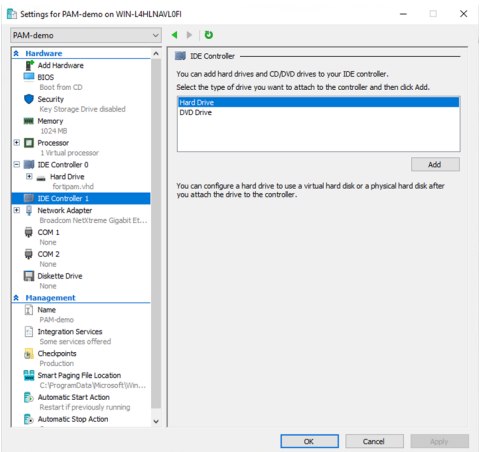
11. To create the VM and close the wizard, click *Finish*.
12. Right-click the VM and select *Settings* from the menu. Optionally, having selected the VM, in the *Action* menu, click *Settings*.



13. In *Hardware*, to remove a DVD drive:
    a. Select a DVD drive in *IDE Controller 1*.
    b. Click *Remove*.
    c. Click *Apply*.



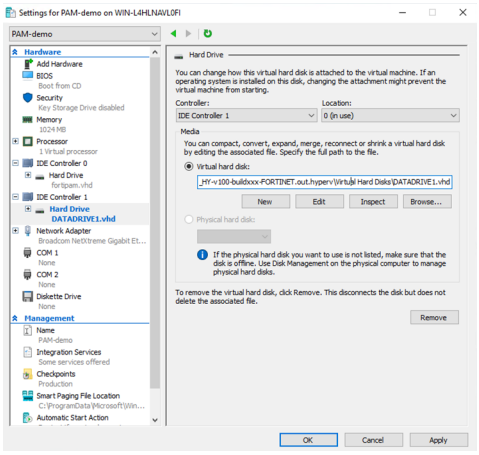
14. In *Hardware*, to add a hard drive:
    a. Click *IDE Controller 1*.
    b. Select *Hard Drive*.



    c. Click *Add*.

d. In *Hard Drive*, click *Browse* and locate the `DATADRIVE1.vhd` file that is in the same folder as `fortipam.vhd` file.

e. Click *Apply*.



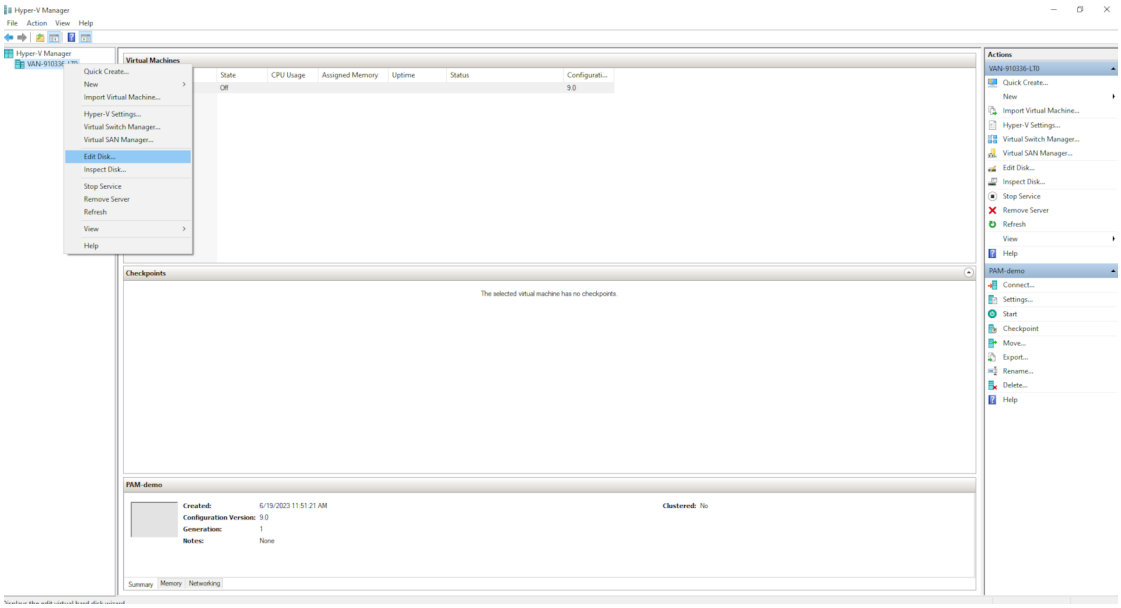
f. Click *OK*.

15. Repeat step 14 to add a second disk, `DATADRIVE2.vhd`.
16. From the virtual machines list, right-click the FortiPAM-VM and select *Start* to power on the VM.
17. Select your newly created VM and launch it.
    See FortiPAM appliance setup on page 24 for CLI related settings to verify the disk usage type and set up FortiPAM.

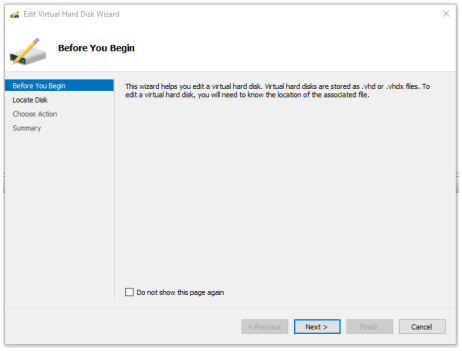
To deploy FortiPAM-VM on MS Hyper-V with TPM support:

To use FortiPAM with TPM on a Hyper-V platform, first, you must convert the virtual hard disk from `*.vhd` to `*.vhdx` format (step 1) and then specify *Generation 2* when creating a new VM (step 2). Finally, you must enable TPM on Hyper-V before powering on the VM (step 3).

1. **Converting hard disk to `*.vhdx`**:
   a. In the left tree menu, right-click the server/management computer and select *Edit Disk*. Optionally, having selected the server, select *Action* and then select *Edit Disk*.

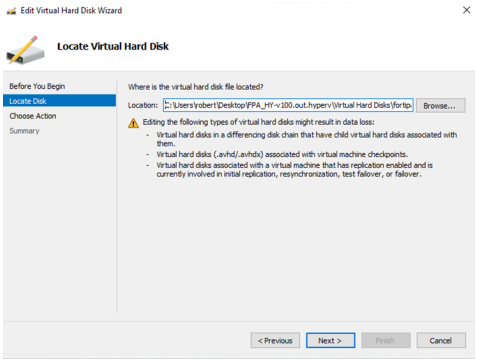


The *Edit Virtual Hard Disk Wizard* opens.

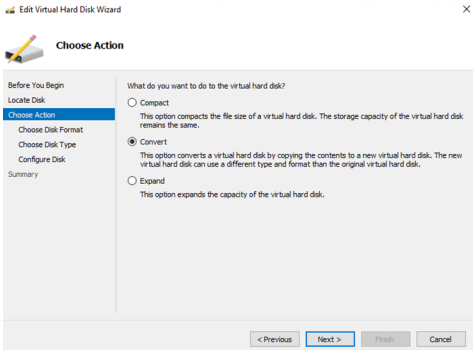


b. In the *Edit Virtual Hard Disk Wizard*, click *Next*.

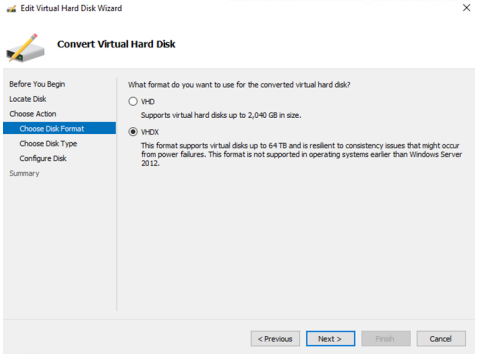
c. In *Locate Virtual Hard Disk*, click *Browse* and locate the `fortipam.vhd` file that you downloaded from FortiCloud, and click *Next*.



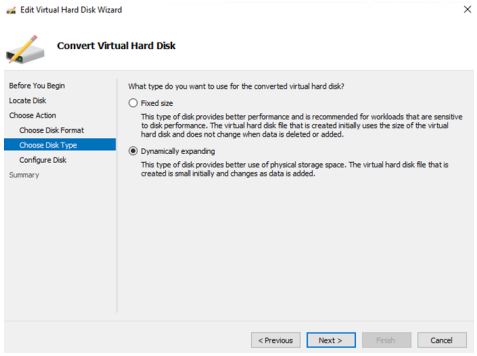
d. In *Choose Action*, select *Convert*, and click *Next*.



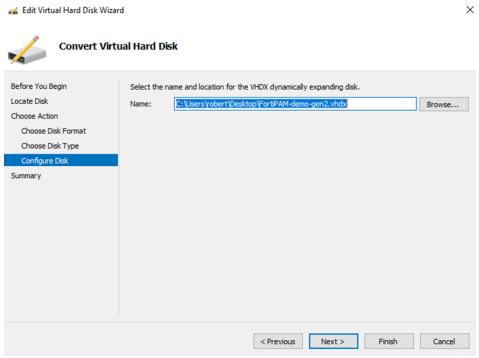
e. In *Choose Action* > *Choose Disk Format*, select *VHDX*, and click *Next*.



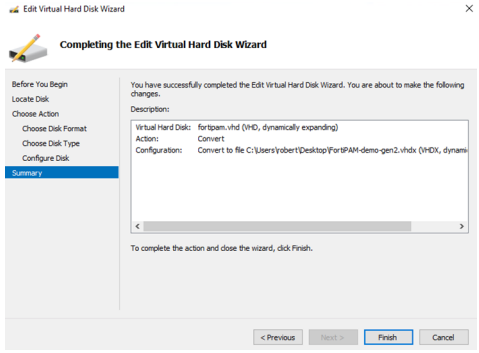
f. In *Choose Action* > *Choose Disk Type*, select *Dynamically expanding*, and click *Next*.



g. In *Choose Action* > *Configure Disk*, enter a name for the VHDX disk, click *Browse* to configure a location for this disk, and click *Next*.



h. In *Completing the Edit Virtual Hard Disk Wizard*, the summary is displayed.

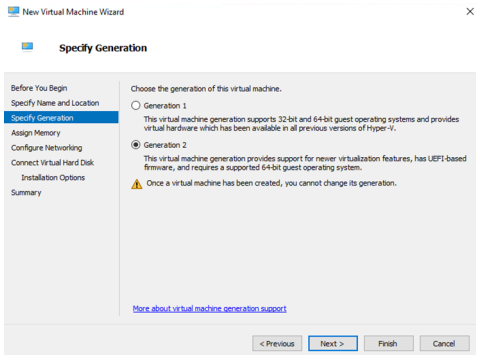


i. Click *Finish*.

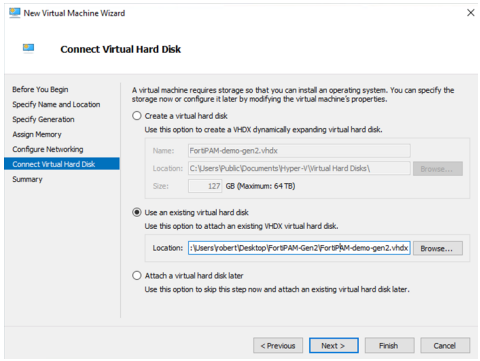
j. Repeat steps *a* to *i* to convert `DATADRIVE1.vhd` and `DATADRIVE2.vhd`.

2. **Creating a 2nd generation Hyper-V VM**:
   Follow the same procedure as detailed in Deploying FortiPAM-VM on Hyper-V without TPM, except:

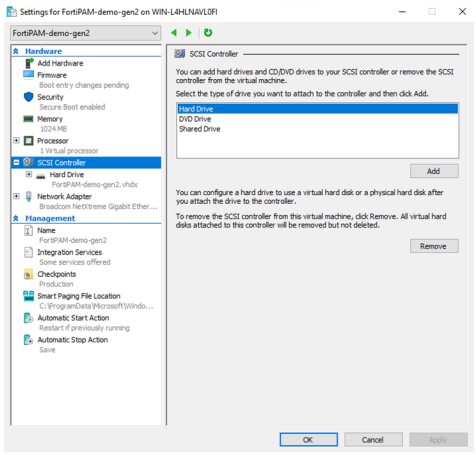
a. In Step 6, select *Generation 2*.



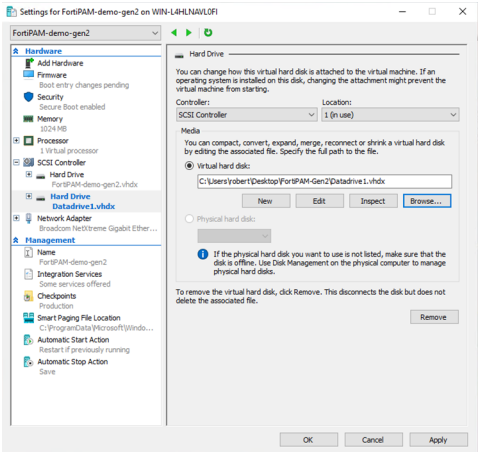
b. In Step 9, click *Browse* and locate the `*.vhdx` file that you converted from `fortipam.vhd`.



c. In step 14 (a, b, and c), click *SCSI Controller*, select *Hard Drive*, and click *Add*.



d. In step 14 d, in *Hard Drive*, click *Browse* and locate the `*.vhdx` file for `DATADRIVE1.vhd` that you earlier converted in Converting hard disk to *.vhdx.

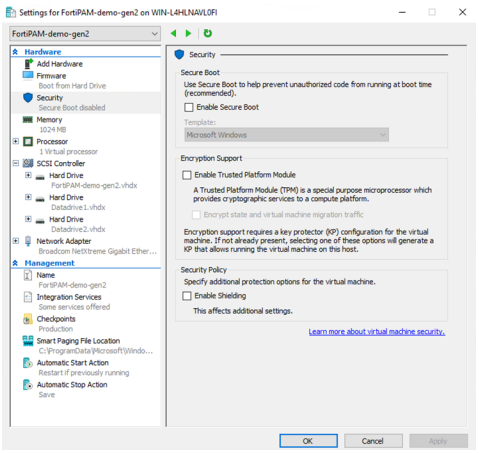


e. Repeat steps *c* and *d* to add `*.vhdx` file for `DATADRIVE2.vhd`.

Secure boot must be disabled before starting the VM.

To disable secure boot:

1. From the virtual machines list, right-click the VM and select *Settings*. Optionally, having select the VM, select *Action* and then select *Settings*.
2. Go to *Security* and uncheck *Enable Secure Boot*.
3. Click *Apply*.



4. Click *OK*.

---

3. **Enabling TPM on Hyper-V**:

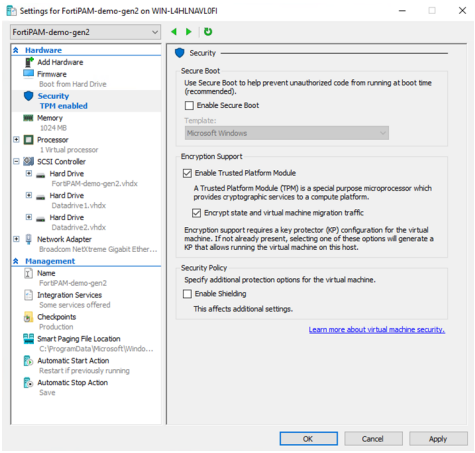
Ensure that TPM is set up as part of the initial configuration, i.e., before powering on the FortiPAM-VM for the first time.

---

a. From the virtual machines list, right-click the VM and select *Settings*. Optionally, having select the VM, select *Action* and then select *Settings*.

b. Go to Security and check *Enable Trusted Platform Module*. Optionally, enable *Encrypt state and virtual machine migration traffic*.

c. Click *Apply*.



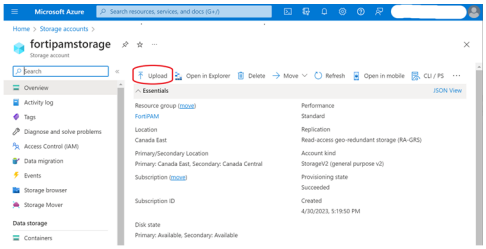
d. Click *OK*.
You can now power on your VM.

Appendix G: Installation on Azure

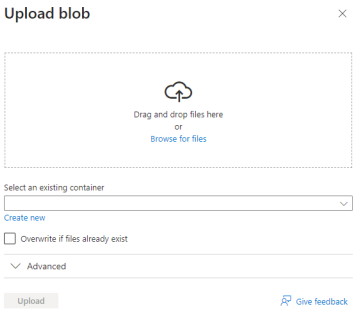
Uploading the VHD file to an Azure storage account

To upload the VHD file to an Azure storage account:

1. Unzip the `FPA_AZURE-v100-buildXXXX-FORTINET.out.hyperv.zip` file and store the `fortipam.vhd` file on your management computer.
2. Go to your storage account on the Microsoft Azure Portal and click *Upload*.



The *Upload blob* window opens.

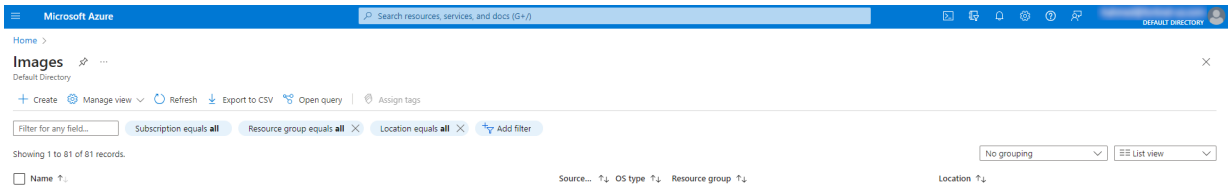


3. Select *Browse for files* and locate the `fortipam.vhd` file that you downloaded and unzipped in step 1.
4. Click *Upload*.

Creating an image on Azure Images

To create an image:

1. Go to *Images* on the Azure Portal and select *Create*.

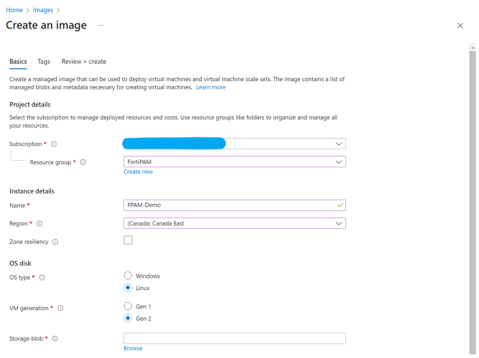


The *Create an image* wizard opens.

2. From the *Resource group* dropdown, select a resource group.

3. In *Name*, enter the name for the image.
4. In the *Region* dropdown, select a region.
5. In *OS type*, select *Linux*.
6. In *VM generation*, you can select *Gen 1* or *Gen 2*.

Gen 1 VMs use BIOS-based architecture, whereas *Gen 2* VMs use the new UEFI-based boot architecture.

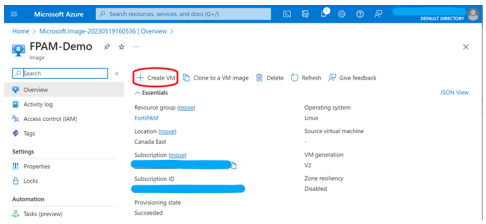


7. In the *Storage blob*, click *Browse*, locate the `fortipam.vhd` file that you uploaded to your storage account in Uploading the VHD file to an Azure storage account on page 316, and click *Next : Tags*.
8. Optionally, in *Tags*, enter tags, and click *Next : Review + Create*.
9. Review your settings and then click *Create*.
   Note: The deployment may take several minutes to finish.

Creating the FortiPAM-VM

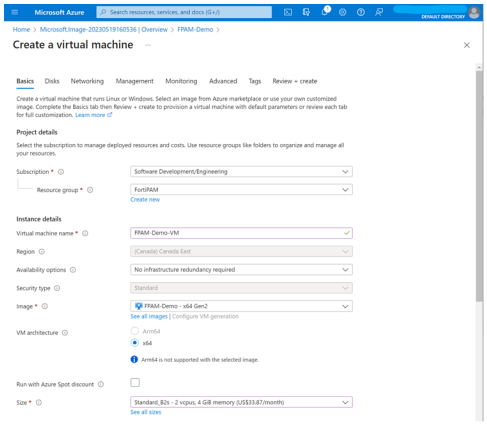
To create the FortiPAM-VM:

1. On the Azure Portal, open the image you created in Creating an image on Azure Images on page 316, and click *Create VM*.



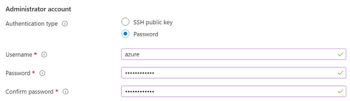
   The *Create a virtual machine* wizard opens.
2. In *Virtual machine name*, enter a name for the VM being created.
3. In the *Region* dropdown, select a region if the region is not automatically selected.
4. In the *Image* dropdown, select the image created in Creating an image on Azure Images on page 316 if the image is not automatically selected.

5. In the *Size* dropdown, select a size that supports the workload you intend to perform.

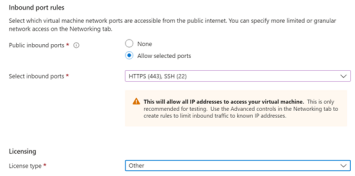


6. In the *Administrator account* pane:
   a. In *Authentication type*, select *Password*.
   b. In *Username*, enter a username.
   c. In *Password*, enter the password.
   d. In *Confirm password*, enter the password again to confirm.

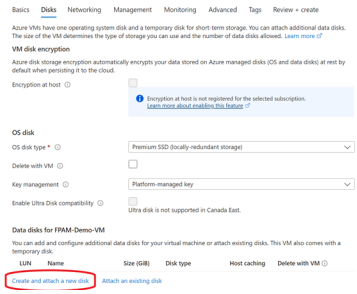
The account is created with the *Super Administrator* role on FortiPAM.



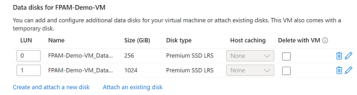
7. In the *Inbound port rules* pane:
   a. In *Public inbound ports*, select *Allow selected ports*.
   b. In the *Select inbound ports* dropdown, select *HTTPS (443), SSH (22)*.
8. In the *License Type* dropdown, select *Other*, and click *Next*.



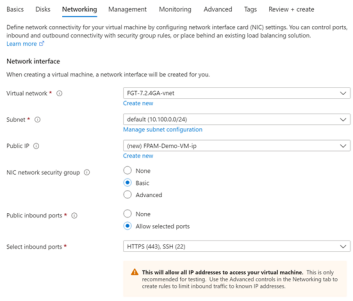
9. In *Data disks for FPAM-demo-VM*, select *Create and attach a new disk*.



10. Create a disk for the log and another for the video, and click *Next*.



11. In the *Networking* tab:
    a. In the *Virtual network* dropdown, select a virtual network.
    b. In the *Subnet* dropdown, select a subnet.
    c. In the *Public IP* dropdown, select a public IP address or create a new public IP address.
    d. In *NIC network security group*, select *Basic*.
    e. In *Public inbound ports*, select *Allow selected ports*.
    f. In the *Select inbound ports* dropdown, select *HTTPS (443), SSH (22)*, and click *Next*.

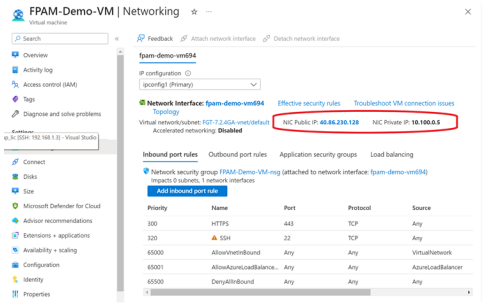


12. Click *Next* and navigate through the remaining tabs.
13. Finally, review your settings and then click *Create*.

    Note: The VM deployment may take several minutes to finish.

Initial configuration

1. On the FortiPAM-VM *Networking* page, copy and save the network interface's private and public IP addresses.



2. In the VM serial console, log in as the default super admin set up in step 6 of Creating the FortiPAM-VM on page 317.
3. Using the following CLI commands, configure `port1`:

```
config system interface
   edit port1
      set mode static #by default, set as dhcp
      set ip 10.100.0.5/24 #set to the private IP address assigned by Azure in step 1
      set allowaccess ssh https #by default, only ssh
   next
end
```

4. Using the following CLI commands, configure a static route:

```
config router static
```

```
    edit 1
       set gateway 10.100.0.1
       set device port1
    next
end
```

5. On a web browser, go to `https://<Public IP>` to access the FortiPAM-VM GUI.
   Note: The public IP address was saved in step 1.
6. Log in with the super admin username and password as set up in step 6 of Creating the FortiPAM-VM on page 317.
   The *FortiPAM VM license* window appears immediately after you log in.
7. In the *Upload License File* pane, select *Upload* and browse to the license file on your management computer.
8. Click *OK*.
   After the boot up, the license status changes to valid.
   You can now use your FortiPAM-VM deployed on Azure.

Evaluation license is not available on Azure.

Appendix H: FortiPAM hardware RAID CLI commands

The FortiPAM hardware devices 1000G and 3000G are equipped with a hardware RAID card. All the hard disks are configured in the RAID-10 group.

For the FortiPAM hardware devices, in the CLI console, check the RAID status by entering the following command:

```
diagnose system raid status
   Storcli RAID:
   RAID Level: Raid-10
   RAID Status: OK
   RAID Size: 5587GB
   Groups: 3
   Disk 0: OK 1862GB Group-1
   Disk 1: OK 1862GB Group-1
   Disk 2: OK 1862GB Group-2
   Disk 3: OK 1862GB Group-2
   Disk 4: OK 1862GB Group-3
   Disk 5: OK 1862GB Group-3
   Disk 6: Unavailable 0GB
   Disk 7: Unavailable 0GB
   Disk 8: Unavailable 0GB
   Disk 9: Unavailable 0GB
   Disk 10: Unavailable 0GB
   Disk 11: Unavailable 0GB
   Disk 12: Unavailable 0GB
   Disk 13: Unavailable 0GB
   Disk 14: Unavailable 0GB
   Disk 15: Unavailable 0GB
   .
   .
   .
```

For the FortiPAM hardware devices, in the CLI console, check the disk status by entering the following command:

```
diagnose system disk health
   Disk 0: SMART Health Status: OK
   Disk 1: SMART Health Status: OK
   Disk 2: SMART Health Status: OK
   Disk 3: SMART Health Status: OK
   Disk 4: SMART Health Status: OK
   Disk 5: SMART Health Status: OK
   Disk 6: Unavailable
   Disk 7: Unavailable
   Disk 8: Unavailable
   Disk 9: Unavailable
   Disk 10: Unavailable
   Disk 11: Unavailable
   Disk 12: Unavailable
   Disk 13: Unavailable
   Disk 14: Unavailable
   Disk 15: Unavailable
   .
   .
```

.

For the FortiPAM hardware devices, in the CLI console, check the disk information by entering the following command:

```
diagnose system disk info
   Disk 0:
   Vendor: SEAGATE
   Product: ST2000NM001B
   Revision: N001
   Compliance: SPC-5
   User Capacity: 2,000,398,934,016 bytes [2.00 TB]
   Logical block size: 512 bytes
   LU is fully provisioned
   Rotation Rate: 7200 rpm
   Form Factor: 3.5 inches
   Logical Unit id: 0x5000c500d9c75b8b
   Serial number: WRE06YSQ0000C246A3JM
   Device type: disk
   Transport protocol: SAS (SPL-3)
   Local Time is: Thu Apr 13 12:12:44 2023 GMT
   SMART support is: Available - device has SMART capability.
   SMART support is: Enabled
   Temperature Warning: Enabled
   .
   .
   .
```

Creating a RAID-10 disk group on hardware FortiPAM

By default, FortiPAM 1000G and 3000G are configured in RAID-10.

You can recreate RAID-10 using the CLI.

Since all the data on the disks are wiped off. You must perform a backup before using this CLI command.

Use the following CLI command to create a RAID-10 disk group:

```
execute raid create-and-format
   This operation will create RAID disk and format it to ext4 file system.
   All existing data will be lost!
   Do you want to continue? (y/n)
```

Hot swapping failed disks on FortiPAM 1000G/3000G

The following procedure was drawn from a simulated case of a failed disk. The procedure that applies to your use case may be different.

1. Unplug the disk.
2. Run the `diagnose system raid status` CLI command.
   The disk status turns *Unavailable*.
3. Plug the disk back.
   The disk status turns *Failed*.
4. Run the `execute raid delete \[disk-index\]` CLI command.
   After a while, the disk status turns *Unused*.
5. Unplug the disk.
6. After a while, plug the disk again.
7. The disk status turns *Rebuilding*.
8. Keep FortiPAM 1000G/3000G running.
   After 10 hours, the disk status turns *OK*.
   RAID is recovered.

www.fortinet.com