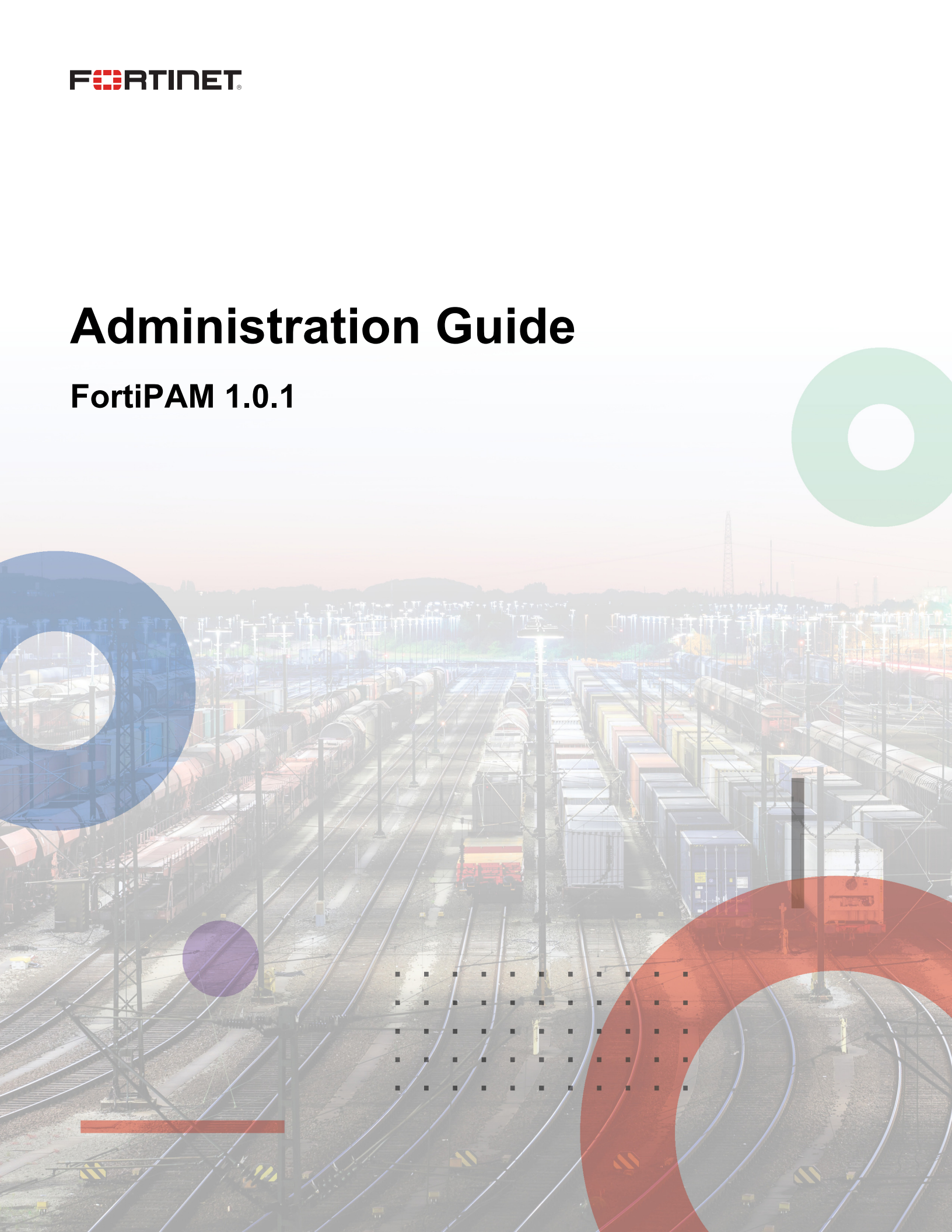


Administration Guide

FortiPAM 1.0.1



FORTINET DOCUMENT LIBRARY

<https://docs.fortinet.com>

FORTINET VIDEO GUIDE

<https://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

FORTINET TRAINING & CERTIFICATION PROGRAM

<https://www.fortinet.com/training-certification>

FORTINET TRAINING INSTITUTE

<https://training.fortinet.com>

FORTIGUARD CENTER

<https://www.fortiguard.com>

END USER LICENSE AGREEMENT

<https://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdoc@fortinet.com



August 10, 2023

FortiPAM 1.0.1 Administration Guide

74-101-869629-20230810

TABLE OF CONTENTS

Change Log	7
Introduction	8
FortiPAM concepts	8
Organization of the guide	9
Using the GUI	9
Banner	10
GUI based global search	10
CLI commands	11
Admin	11
Tables	15
Modes of operation	17
FortiPAM deployment options	18
Feature availability	21
FortiPAM installation	23
Installing FortiClient with the FortiPAM feature	23
FortiPAM appliance setup	24
FortiPAM with TPM	26
Connecting to target remote systems	28
Licensing	29
Dashboard	31
Adding a custom dashboard	34
System information widget	35
Licenses widget	36
VM license	37
Folders	38
Creating a folder	41
Secrets	48
Secret list	49
Creating a secret	50
Launching a secret	60
Check out and check in a secret	61
Uploading secrets using the secret upload template	62
Change password	63
Verify password	66
Example secret configurations example	67
Secret launchers	70
Creating a launcher	72
Secret templates	78
Creating secret templates	79
Policies	84
Creating a policy	85
SSH filter profiles	90

Creating an SSH filter	90
Job list	95
Creating a job	95
Monitoring	98
User monitor	98
Active sessions	98
User management	100
User definition	100
Creating a user	101
User groups	112
Role	116
Access control options	124
LDAP servers	126
SAML Single Sign-On (SSO)	129
RADIUS servers	133
Schedule	135
FortiTokens	138
Approval request	141
My requests	141
Make a request	142
Request review	144
Approve a request	145
Approval flow	146
Approval profile	146
Password changing	150
Character sets	150
Creating a character set	151
Password policies	151
Creating a password policy	152
Password changers	154
Creating a password changer	155
Authentication	163
Addresses	163
Creating an address	164
Creating an address group	169
Scheme & Rules	171
Creating an authentication scheme	172
Creating an authentication rule	179
System	181
Firmware	181
Settings	181
SNMP	185
Fortinet MIBs	188
SNMP agent	189
Creating or editing an SNMP community	189

Creating or editing an SNMP user	191
High availability	193
HA active-passive cluster setup	196
Upgrading FortiPAM devices in an HA cluster	198
Disaster recovery	199
Certificates	201
Creating a certificate	202
Generating a CSR (Certificate Signing Request)	205
Importing CA certificate	207
Uploading a remote certificate	208
Importing a CRL (Certificate revocation list)	208
ZTNA	210
Creating a ZTNA rule	210
Creating a ZTNA server	214
Creating a ZTNA tag group	219
ZTNA user control	219
ZTNA tag control example	221
ZTNA-based FortiPAM access control	222
Backup	225
Sending backup file to a server Example	229
Network	231
Interfaces	231
Creating an interface	232
Creating a zone	235
DNS settings	235
Packet capture	238
Creating a packet capture filter	239
Static routes	241
Creating an IPv4 static route	241
Security profile	244
AntiVirus	244
Creating an antivirus profile	245
Data loss prevention (DLP) protection for secrets	247
Supported file types	249
Security fabric	252
Fabric Connectors	252
FortiAnalyzer logging	254
Log & report	257
Events	257
Secret	259
ZTNA	262
SSH	264
Reports	264
Log settings	266
Email alert settings	269
Email alert when the glass breaking mode is activated example	270

Troubleshooting	272
Troubleshoot using trace files	272
Example troubleshooting example	273
FortiPAM HTTP filter	274
Appendix A: Installation on KVM	276
Appendix B: Installation on VMware	279
Appendix C: Installing vTPM package on KVM and adding vTPM to FortiPAM-VM	284
Appendix D: vTPM for FortiPAM on VMware	286
Appendix E: Enabling soft RAID on KVM or VMware	287

Change Log

Date	Change Description
2023-03-24	Initial release.
2023-03-31	Updated FortiPAM appliance setup on page 24.
2023-04-14	Updated FortiPAM deployment options on page 18.
2023-08-10	Updated High availability on page 193.

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 31](#) contains widgets providing performance and status information.
- [Folders on page 38](#) describes features and options related to folders where secrets reside.
- [Secrets on page 48](#) describes features and options related to secrets, secret launchers, secret templates, policies, SSH filter profiles, and jobs.
- [Monitoring on page 98](#) contains information on user logins and active sessions on FortiPAM.
- [User management on page 100](#) describes managing FortiPAM user database.
- [Approval request on page 141](#) describes how to send a secret approval request, review a request, and create approval profiles when approval from the members of an approval profile is required to launch a secret or perform a job on a secret.
- [Password changing on page 150](#) describes creating password policies, character sets used in password policies, and password changers used to periodically change the password of a secret.
- [Authentication on page 163](#) describes creating addresses, address groups, IPv6 address template, authentication rules, and schemes.
- [System on page 181](#) describes managing and configuring basic system settings for FortiPAM. It also contains settings related to firmware, SNMP, HA, certificates, ZTNA, and automatic backup.
- [Network on page 231](#) describes configuring interfaces, DNS settings, packet capture, and static routes.
- [Security profile on page 244](#) describes configuring FortiPAM security features.
- [Security fabric on page 252](#) describes creating fabric connectors to provide integration with Fortinet products.
- [Log & report on page 257](#) describes how to view logs and reports on FortiPAM.

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 31](#).

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.

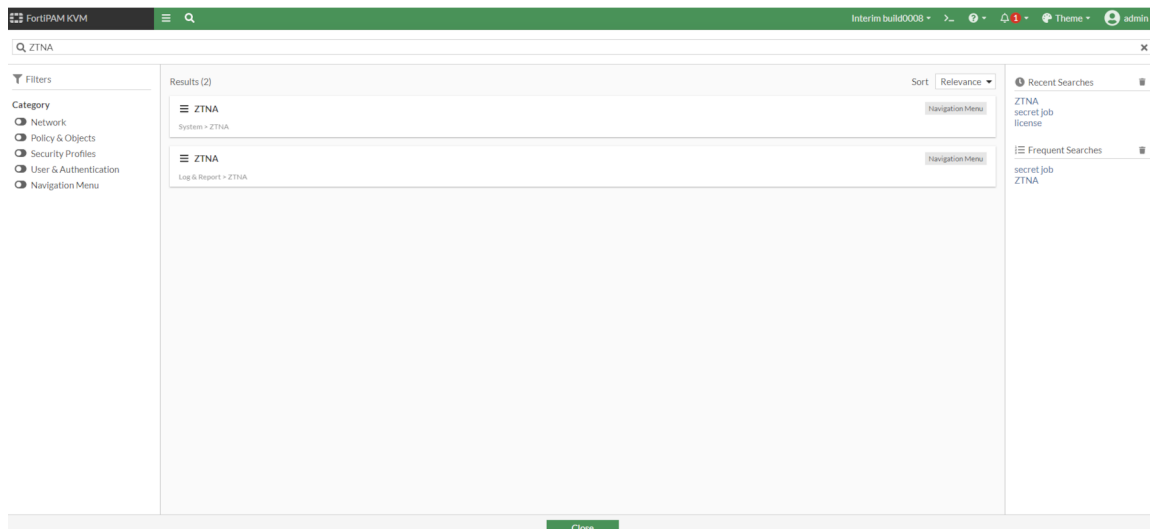
The global search includes the following features:

- 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 270](#).

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 116](#).



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 dropdown, 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*.



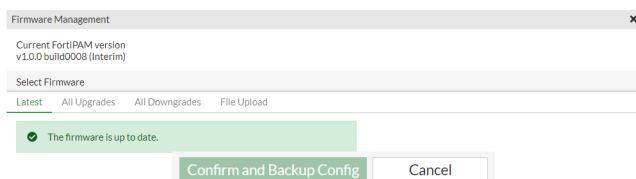
When in maintenance mode, select *Renew Maintenance Mode* in *System*, enter the new duration and reason and then click *OK* to renew the maintenance mode.



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 tabs 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 50](#). Alternatively, see the *Proxy Mode* option when creating or editing a policy. See [Creating a policy on page 85](#).

FortiPAM deployment options

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

When EMS is not available, standalone FortiClient is recommended. With standalone FortiClient, native launchers such as PuTTY, RDP, VNC Viewer, Tight VNC, and WinSCP can be used to connect to the target server and user can take advantage of functionalities provided by these applications. Also, video recording for user activity on the target server is sent to FortiPAM in real-time.

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

On a system without FortiClient and browser extension, the user can still log in to FortiPAM and use the web-based launchers. However, all other features mentioned above are not available.

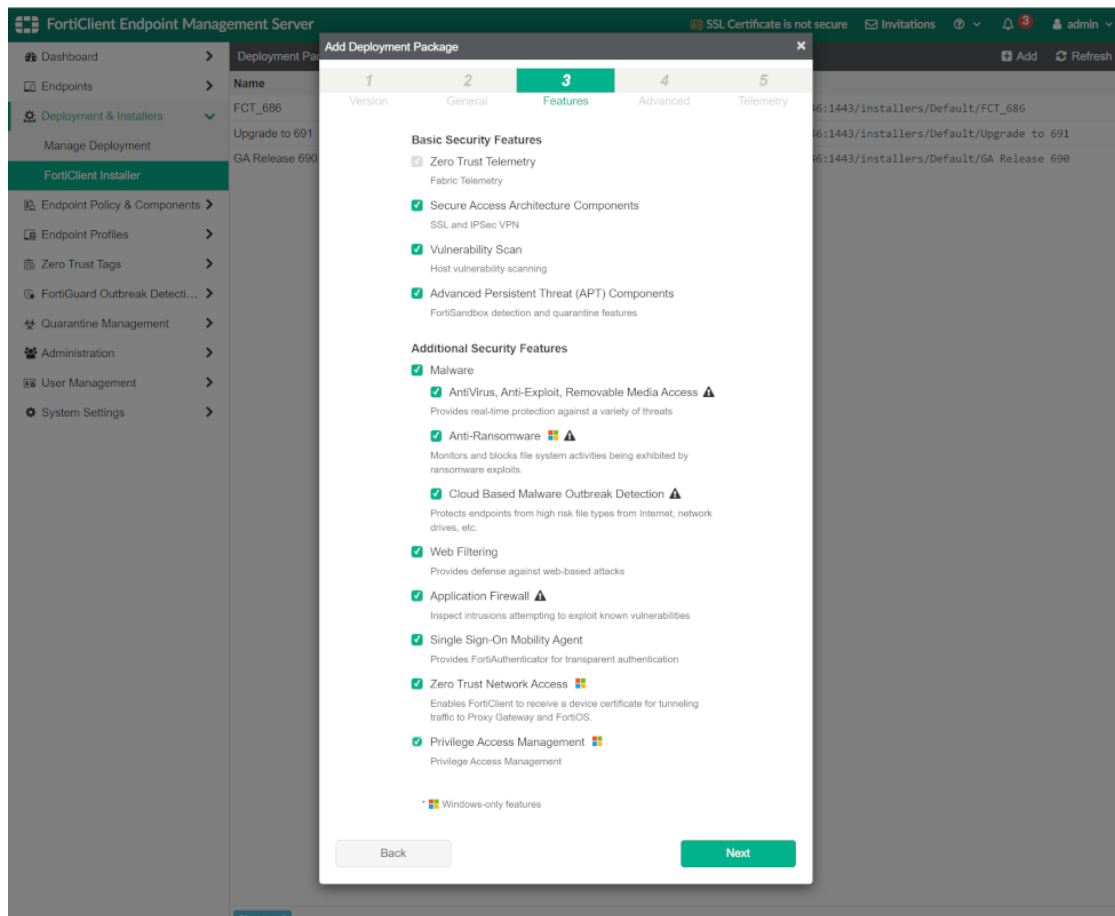
1. If EMS (7.2.0 or later) is available:
 - a. **EMS Server:**
 - i. Enable *Privilege Access Management*.
 - i. Navigate to *Endpoint Profiles > System Settings*.
 - ii. Edit the *Default System Setting Profiles*.

iii. Select *Advanced* and enable *Privilege Access Management*.

The screenshot displays the FortiClient Endpoint Management Server interface. The left sidebar shows the navigation menu with 'System Settings' selected. The main content area is titled 'System Settings Profile' and has three tabs: 'Basic', 'Advanced', and 'XML'. The 'Advanced' tab is active. Under the 'Other' section, there are two toggle switches: 'Install CA Certificate on Client' and 'FortiClient Single Sign-On Mobility Agent', both of which are currently turned off. The 'iOS' section has a toggle for 'Distribute Configuration Profile', which is also turned off. The 'Privacy' section has a toggle for 'Send Usage Statistics to Fortinet', which is turned on. Below this, there is a note: 'This information will be used to improve our product quality and user experience.' The 'Privilege Access Management' section is expanded, showing a toggle that is turned on and a 'Port' field with the value '9191'. At the bottom of the page, there are three buttons: 'Save', 'Discard Changes', and 'Revert To Default'.

ii. Push FortiClient (7.2.0 or later) to registered PC-

- i. Navigate to *Deployment & Installers > FortiClient Installer*.
- ii. Add a package with both *Zero Trust Network Access* and *Privilege Access Management* enabled on the third tab of the wizard.



iii. Navigate to *Deployment & Installers > Manage Deployment* and apply the FortiClient installer package to select endpoint groups.

b. **Windows:** Download standard FortiClient (7.2.0 or later), and enable "ZTNA" and "PAM" functions during the installation. Full FortiPAM features are then supported.
After FortiClient registers to EMS, EMS can automatically deploy the configured FortiClient version to Windows PC.

c. **Linux and MacOS:** Install *FortiPAM Password Filler* extension from the Chrome Web Store or follow the FortiPAM GUI prompt. Then use web-based launchers or web launcher to access the target server.

Note: ZTNA and Native launchers are not supported on extension-only systems.

2. If EMS (7.2.0 or later) is not available:

a. **Windows:** After downloading and installing standalone FortiClient (7.2.0 or later) manually, most PAM features are supported.

Note: A standalone installer contains PAM in its filename such as `FortiClientPAMSetup_7.2.0.0xxx_x64.exe`.

Note: ZTNA is not supported.

b. **Linux and MacOS:** Install *FortiPAM Password Filler* extension from the Chrome Web Store or follow the FortiPAM GUI prompt. Then use web-based launchers or web launcher to access the target server.

Note: ZTNA and Native launchers are not supported on extension-only systems.

3. If FortiClient is not available (extension-only):

a. **Windows:** Install *FortiPAM Password Filler* extension from the Chrome Web Store or Microsoft Edge Add-ons. Then use web-based launchers or web launcher to access the target server.

Note: ZTNA and Native launchers are not supported on extension-only systems.

- b. Linux and MacOS:** Install *FortiPAM Password Filler* extension from the Chrome Web Store or follow the FortiPAM GUI prompt. Then use web-based launchers or web launcher to access the target server.

Note: ZTNA and Native launchers are not supported on extension-only systems.

Note: Chrome or Edge web browsers are suggested for use as there is some limitation on Firefox extension-only deployment.

Feature availability

The following table lists FortiPAM 1.0.1 feature availability based on the type of deployment being used:

Feature	FortiPAM with standard FortiClient	FortiPAM with standalone FortiClient	FortiPAM with browser extension	FortiPAM only
Windows OS	✓	✓	✓	✓
Linux OS	X	X	✓	✓
MacOS	X	X	✓	✓
ZTNA	✓	X	X	X
Web-based launchers, i.e, Web-SSH, Web-RDP, Web-VNC, Web-SFTP, and Web-SMB (only supports proxy mode; credential protected in FortiPAM)	✓	✓	✓	✓
Proxy mode web browsing (credential sent to the extension with permission protection)	✓	✓	✓	X
Direct mode web browsing (credential sent to the extension with permission protection)	✓	✓	✓	X
Video recording	✓	✓	✓	X
Instant video uploading	✓	✓	X	X

Feature	FortiPAM with standard FortiClient	FortiPAM with standalone FortiClient	FortiPAM with browser extension	FortiPAM only
Proxy mode native launchers, i.e., PuTTY, RDP, VNC Viewer, Tight VNC, and WinSCP (credential protected in FortiPAM)	✓	✓	X	X
Direct mode native launchers, i.e., PuTTY, RDP, VNC Viewer, Tight VNC, and WinSCP (credential delivered to FortiClient with permission protection)	✓	✓	X	X

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 1.0.1:

- VMware ESXi/ ESX 6.5 and above
- KVM

FortiPAM supports both Linux and Windows environments.



On Windows, the user may install FortiClient which includes fortivr 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 *FortiPAM Password Filler* in addition to fortivr 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 276](#).

See [Appendix B: Installation on VMware on page 279](#).

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 276](#).

```
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 284](#).



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. One is default super admin and another user can be created.
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.



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.

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.

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.

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.

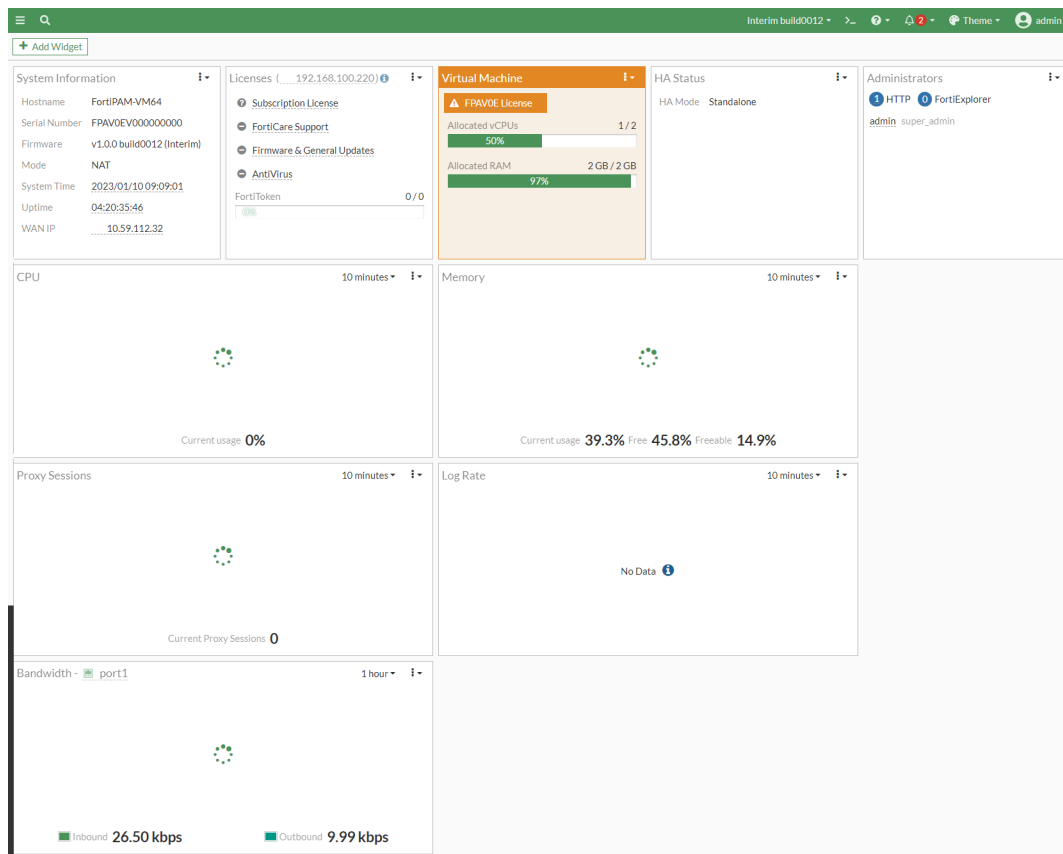
2. In the *Upload License File* pane, select *Upload* and browse to the license file on your management computer.
 3. Click *OK*.
 4. After the boot up, the license status changes to valid.
-



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

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.

	<p>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 35.</p> <p>You can also configure system settings using this widget. For information on system settings, see Settings on page 181.</p>
Licenses	Displays the status of your license and FortiGuard subscriptions. See Licenses widget on page 36 .
Virtual Machine	Displays license information, number of allocated vCPUs, and how much RAM has been allocated. See VM license on page 37 .
HA status	Displays HA mode. See High availability on page 193 .
CPU	<p>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.</p> <hr/> <div style="display: flex; align-items: center;">  <p>To see per core CPU usage, select the CPU widget and click <i>Show per core CPU usage</i>.</p> </div> <hr/>
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 266 .
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.

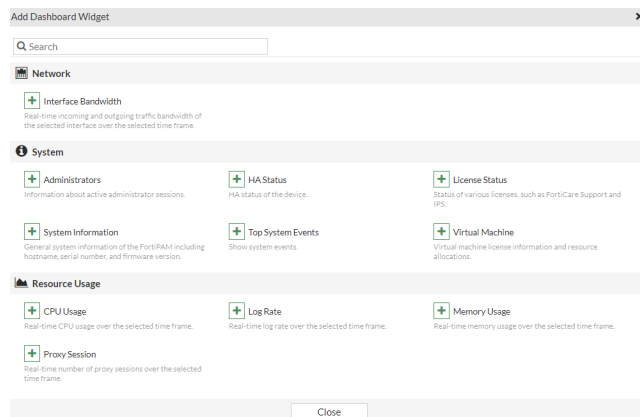
You can add the following *Resource Usage* widgets to the *Dashboard*:

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:

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




- Select the widget you want to add to the dashboard.
The *Add Dashboard Widget - Widget Name* window opens.
- 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 <i>Interface Bandwidth</i> widget.
Note: Options in <i>Time period</i> and <i>Sort by</i> may vary depending on the widget you intend to add.	
Time Period	Select from the following time periods to display: <ul style="list-style-type: none"> 5 minutes 1 hour 24 hours
Visualization	Select the type of chart to display. Note: For the <i>Top System Events</i> widget only the <i>Table View</i> is available.
Sort by	Sort by: <ul style="list-style-type: none"> Level Events

- 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	<p>Select and then in <i>Edit Dashboard Widget</i> - <code>Widget Name</code>, specify the <i>Fabric Member</i>, interface (if available), and click <i>OK</i>.</p> <p>Select from the following options:</p> <ul style="list-style-type: none"> • <i>Default</i>: Uses the current fabric member. • <i>Specify</i>: Select a fabric member from the FortiPAM dropdown, i.e., a FortiPAM instance. <hr/> <div style="display: flex; align-items: center;">  <p>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.</p> </div> <hr/> <ul style="list-style-type: none"> • <i>Interface</i>: 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.


Add Dashboard

Name



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.

System Information	
Hostname	PAM_18_Sandbox
Serial Number	FPXVM8TM22000261
Firmware	v1.0.0 build0007 (Interim)
Mode	NAT
System Time	2022/10/18 16:45:06
Uptime	06:06:24:10
WAN IP	 [Redacted]

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 35 .
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 36 .
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 <i>Dashboard</i> . 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*.

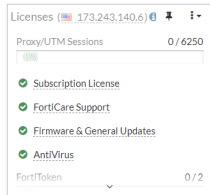


Custom server details must be configured in the CLI.

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*.

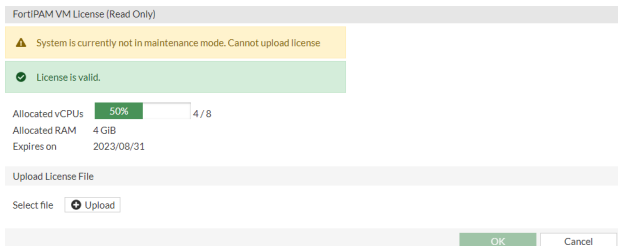
VM license

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](#).

Folders

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 the list of available secrets:

Name	Template	Policy	References
FortiGate	FortiGate (SSH Password)		0
SVR_101	Unix Account (SSH Password)		0
SVR_102	Unix Account (SSH Key)		0
Windows_AD	Windows Domain Account (Samba)		0
test_Secret	AWS Web Account		0

The *Folders* tab contains the following options:

Current Folder	Edit the current folder.
Back up	Return to the parent folder.
Create	From the dropdown, create a secret or a folder. See Creating a secret on page 50 and Creating a folder on page 41 .
Open	Open a folder. See Opening a folder on page 39 .
Move	Move a subfolder or a secret to a different folder. See Moving a subfolder on page 39 and Moving a secret to a different folder on page 39 .
Delete	Delete selected subfolders or secrets. See Delete a subfolder or a secret .
Launch Secret	Launch the selected secret. See Launching a secret on page 60 .

Make Request	Make a request to launch the selected secret. See Make a request on page 142 .
Search	Enter a search term in the search field, then hit <code>Enter</code> to search the folders list. To narrow down your search, see Column filter .
Actions ▾	Select from the following options: <ul style="list-style-type: none"> • Edit Folder • Remove Folder • Add Favorite • Remove Favorite

Opening a folder



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

To open a folder:

1. Go to *Folders*, and from the tree menu select a folder to open.
Alternatively, in a folder window, select *Open*, and then select the destination folder.
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 *Folders*, and from the tree menu select a folder to open.
2. Select the subfolder, and select *Move*.
The *Move to* dialog opens.
3. Select the destination folder from the list 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 *Folders*, and from the tree menu select a folder to open.
2. From the secret list, select a secret, and then select *Move*.
The *Move to* dialog opens.
3. Select the destination folder from the list and then select *Move Secret*.

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 *Folders*, and select a folder from the tree menu.



To edit the folder:

1. Select the folder from the tree menu.
2. Select *Actions*.
3. Select *Edit Folder*.
The *Edit Secret Folder* window opens.
4. Update the options as needed.

2. Select a subfolder or a secret, right-click and then select *Edit*.

The *Edit Secret Folder* or *Edit Secret* window opens.

3. 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 41](#) and [Creating a secret on page 50](#).

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 *Folders*, and select a folder from the tree menu.



To delete the folder:

1. Select the folder from the tree menu.
2. Select *Actions*.
3. Select *Remove Folder*.
4. In the *Confirm* dialog, click *OK* to delete the folder.

2. Select a subfolder or a secret, right-click and then select *Delete*. The *Confirm* dialog appears.
3. Select *OK* to delete the selected folder.

Adding a favorite:

To add a favorite:

1. Go to *Folders*, select a folder, and then select the *Actions* icon.
2. In *Actions*, select *Add Favorite* to add the folder to the *Menu Shortcuts* on top of the tree menu.

Removing a folder from favorite

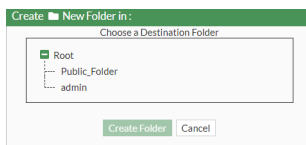
To remove a folder from favorite:

1. From *Menu Shortcuts*, select a folder. Alternatively, select a folder in *Folders*.
2. Select *Actions*, select *Remove Favorite* to remove the folder from *Menu Shortcuts* on top of the tree menu.

Creating a folder

To create a folder:

1. Go to *Folders*, and select + to add a new folder. The *Create New Folder in:* dialog opens.



2. Select the location for the new folder.















You can create a folder in an existing folder or select *Root* to create a root folder.

3. Click *Create Folder*.

A new *Secret Folder* window opens.

4. Enter the following information:

Name	Name of the folder.
Parent Folder	From the dropdown, select a parent folder or select <i>Create</i> 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.

	 <p>You cannot inherit policy for a root folder.</p>
<p>Secret Policy</p>	<p>From the dropdown, select a policy that applies to the folder or select <i>Create</i> to create a new policy. See Creating a policy on page 85.</p> <hr/>  <p>Use the search bar to look for a policy.</p> <hr/>  <p>Use the pen icon next to the policy to edit it.</p> <hr/>  <p>This option is only available when <i>Inherit Policy</i> is disabled.</p>
<p>Folder Permission</p>	
<p>Inherit Permission</p>	<p>Enable to inherit permission from the parent folder.</p> <hr/>  <p>The option is enabled by default when creating a subfolder.</p> <hr/>  <p>You cannot inherit permission for a root folder.</p> <hr/> <p>Note: The setting can only be disabled if you have the <i>Owner</i> permission. Also, the setting cannot be disabled for any subfolder of the personal folder, i.e., the folder generated for every user.</p>
<p>User Permission</p>	<p>The level of user access to the folder and secrets in the folder. See User Permission on page 44.</p> <hr/>  <p>This option is only available when <i>Inherit Permission</i> is disabled.</p> <hr/> <p>For column settings, see Tables on page 15.</p>
<p>Group Permission</p>	<p>The level of user group access to the folder and secrets in the folder. See Group Permission on page 46.</p>



This option is only available when *Inherit Permission* is disabled.

For column settings, see [Tables on page 15](#).

5. 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.



New User Permission x

Users


Folder Permission

Secret Permission

2. Enter the following information:

<p>Users</p>	<p>Select + and from the list, select users in the <i>Select Entries</i> window.</p> <hr/> <div style="display: flex; align-items: center;">  <p>Use the search bar to look up a user.</p> </div> <hr/> <div style="display: flex; align-items: center;">  <p>Use the pen icon next to the user to edit it.</p> </div> <hr/> <p>To add a new user:</p> <ol style="list-style-type: none"> 1. From the <i>Select Entries</i> window, select <i>Create</i> and then select <i>+User Definition</i>. The <i>New User Definition</i> wizard opens. 2. Follow the steps in Creating a user on page 101, starting step 2 to create a new user.
<p>Folder Permission</p>	<p>From the dropdown, select an option:</p> <ul style="list-style-type: none"> • <i>None</i>: No access. • <i>View</i>: Ability to view secrets and subfolders in the folder. • <i>Add Secret</i>: Ability to create new secrets. • <i>Edit</i>: Ability to create/edit secrets, subfolders, and the folder itself. • <i>Owner</i>: The highest possible permission level with the ability to create, edit, delete, and move secrets, subfolders, and the folder itself.
<p>Secret Permission</p>	<p>From the dropdown, select an option:</p> <ul style="list-style-type: none"> • <i>None</i>: No access. • <i>List</i>: Ability to list secrets. You cannot see detailed information on secrets. • <i>View</i>: Ability to view secret details and launch a secret. • <i>Edit</i>: Ability to create/edit secrets and launch the secrets. • <i>Owner</i>: The highest possible permission level with the ability to create, edit, delete, move, and launch secrets.

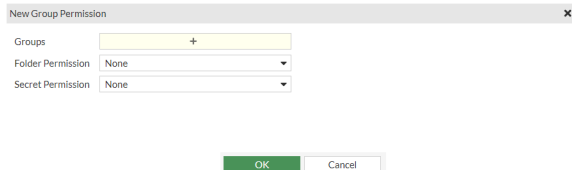
3. Click *OK*.

	<p>From the list, select a user permission and then select <i>Edit</i> to edit the user permission.</p> <p>From the list, select user permissions and then select <i>Delete</i> to delete the user permissions.</p>
---	---



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:

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

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 49](#)
- [Secret launchers on page 70](#)
- [Secret templates on page 78](#)
- [Policies on page 84](#)
- [SSH filter profiles on page 90](#)
- [Job list on page 95](#)

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 116](#).

For each secret; name, last password verification, folder, template, description, and reference are shown.

Name	Last Password Verification	Folder	Template	Description	References
test_secret	Not checked	admin	✗ Cisco User (SSH Secret)		0
test_secret_2	Not checked	admin	✗ Cisco User (SSH Secret)		0
test_secret_3	Not checked	admin	✗ FortiGate (SSH Key)		0



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

The *Secrets List* tab contains the following options:

Create	Select to create a new secret. See Creating a secret on page 50 .
Upload	Select and then select <i>Upload Secret</i> to upload secrets using the secret upload template file, or download the secret upload template by selecting <i>Download Template</i> . See Uploading secrets using the secret upload template on page 62 .

Edit	Select to edit the selected secret.
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 60 .
Make Request	Make request to launch or perform a job on the secret. Make a request on page 142 .
Search	Enter a search term in the search field, then hit <code>Enter</code> to search the secrets list. To narrow down your search, see Column filter .



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 *Folders*, and select a folder where you intend to add a secret. From the *Create* dropdown, select *Secret*, and skip to step 3.
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* pane 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 Folders on page 38 .
	
	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 79](#).



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

Select a field in the table and then select edit to add a value.



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 Settings



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.

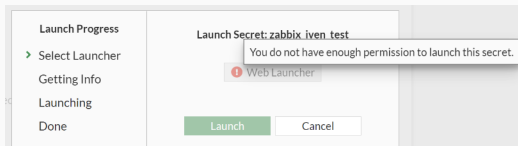
Recurrence	<p>From the dropdown, select from the following three frequencies of recurrence:</p> <ul style="list-style-type: none"> • <i>Daily</i> • <i>Weekly</i> • <i>Monthly</i>
Repeat every	<p>The number of days/weeks/months after which the password is changed (1-400).</p>
Occurs on	<p>Select from the following days of the month when the password is automatically changed:</p> <ul style="list-style-type: none"> • <i>First</i> • <i>Second</i> • <i>Third</i> • <i>Last</i> • <i>Last Day</i> • <i>Day</i> <p>When you select <i>Day</i>, select + to add days of the month when the password is automatically changed.</p> <p>Select days of the week when the password is automatically changed.</p> <p>Note: The option is only available when <i>Recurrence</i> is set as <i>Weekly</i> or <i>Monthly</i>.</p>
Automatic Password Verification	<p>Enable/disable automatic password verification.</p> <p>When enabled, password changer for secrets is activated to periodically verify the password, and check if the target server is still available.</p>
Interval (min)	<p>The time interval at which the secret passwords are tested for accuracy, in minutes (default = 60, 5 - 44640).</p>
Start Time	<p>The date and time when the <i>Interval(min)</i> begins.</p> <p>Enter date (MM/DD/YYYY) and time or select the <i>Calendar</i> icon and then select a date and time.</p>
Session Recording	<p>Enable/disable session recording.</p> <p>When enabled, user action performed on the secret is recorded.</p> <hr/> <div style="display: flex; align-items: center;">  <p>The video file is available in the log for users with appropriate permission.</p> </div> <hr/>
Proxy Mode	<p>Enable/disable the proxy mode.</p> <p>When enabled, FortiPAM is responsible to proxy the connection from the user to the secret.</p> <p>In the proxy mode:</p> <ul style="list-style-type: none"> • 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.

Antivirus Scan

Enable/disable antivirus scan.

When enabled, it enforces an antivirus profile on the secret. See [AntiVirus on page 244](#).

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 61](#).

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 <i>Renew Checkout</i> 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	<p>Enable/disable requiring approval to launch a secret.</p> <p>When enabled, users are forced to request permission from the approvers defined in the approval profile before gaining access. From the dropdown, select an approval profile.</p> <hr/> <div style="display: flex; align-items: center;">  <p>Use the search bar to look up an approval profile.</p> </div> <hr/> <div style="display: flex; align-items: center;">  <p>Use the pen icon next to the approval profile to edit it.</p> </div> <hr/> <p>See Make a request on page 142 and Approval flow on page 146.</p>
Requires Approval to Launch Job	<p>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. From the dropdown, select an approval profile.</p> <hr/> <div style="display: flex; align-items: center;">  <p>Use the search bar to look up an approval profile.</p> </div> <hr/> <div style="display: flex; align-items: center;">  <p>Use the pen icon next to the approval profile to edit it.</p> </div> <hr/> <p>See Make a request on page 142 and Approval flow on page 146.</p>
Service Settings	
Turn on/off the service settings.	
	<p>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.</p> <p>The port used by each service specified in the template can also be overridden to use a custom port specific to the secret.</p>
SSH Service	<p>Enable/disable SSH service.</p> <p>Note: <i>SSH Filter</i>, <i>RSA Sign Algorithm</i>, and <i>Connect over SSH with</i>, and <i>SSH Auto-Password</i> options are only available when <i>Template</i> is already selected.</p>

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 90 .
SSH Filter Profile	From the dropdown, select an SSH filter profile. Note: The option is only available when <i>SSH Filter</i> is enabled.
	 <p>Use the search bar to look up an SSH filter profile.</p>
RSA Sign Algorithm	To improve compatibility with different SSH servers, select a sign in algorithm for RSA-based public key authentication: <ul style="list-style-type: none"> • <i>RSA SHA-256 signing algorithm</i> • <i>RSA SHA-512 signing algorithm</i> • <i>RSA SHA-1 signing algorithm</i> (default)
Connect over SSH with	If the setting is set to <i>Self</i> (default), the secret launches SSH with its own username and password. If the setting is set to <i>Associated Secret</i> , 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., <code>sudo</code> in Unix system and <code>enable</code> 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 <i>Proxy Mode</i> is enabled.
RDP Service	Enable/disable RDP service. Note: <i>Block RDP Clipboard</i> , <i>RDP Security Level</i> , <i>RDP Restricted Admin Mode</i> , and <i>Keyboard Layout</i> options are available only when <i>Template</i> is already selected.
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: <ul style="list-style-type: none"> • <i>Best Effort</i> (default): If the server supports NLA, FortiPAM uses NLA to authenticate. Otherwise, FortiPAM conducts standard RDP authentication with the server through RDP over TLS. • <i>NLA</i>: Network Level Authentication (CredSSP). When an RDP launcher is launched, FortiPAM is forced to use CredSSP (NLA) to authenticate with the target server. • <i>RDP</i>: FortiPAM uses the standard RDP encryption provided by the RDP protocol without using TLS (Web-RDP only). • <i>TLS</i>: RDP over TLS. FortiPAM uses secured connection with encryption protocol TLS to connect with the target server.

RDP Restricted Admin Mode	<p>Enable/disable RDP restricted admin mode.</p> <p>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.</p> <p>Note: The option is only available when <i>RDP Security Level</i> is set as <i>Best Effort</i> or <i>NLA</i>.</p>
Keyboard Layout	From the dropdown, select a keyboard layout (default = <i>English, United States</i>)
VNC Service	Enable/disable VNC service.
Port	Use the template default port or disable and enter a port number.
LDAPS Service	Enable/disable LDAPS service.
Port	Use the template default port or disable and enter a port number.
SAMBA Service	Enable/disable SAMBA service.
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 <i>Owner</i> or <i>Edit</i> permission to the secret or the folder where the secret is located.
Launch Device Control	<p>Enable to limit the permission of launching by <code>ztna-ems-tag</code>.</p> <p>You can choose whether to match all the tags or only one of them.</p>
Device Tags	<p>Select + to add ZTNA tags or groups.</p> <hr/> <p> Use the search bar to look up a ZTNA tag or ZTNA tag group.</p> <hr/> <p>Only permitted devices with the selected tags are allowed to launch.</p>
Device Match Logic	<p>Define the match logic for the device tags:</p> <ul style="list-style-type: none"> • <i>OR</i>: Devices with any of the selected tags are allowed to launch. • <i>AND</i>: 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.

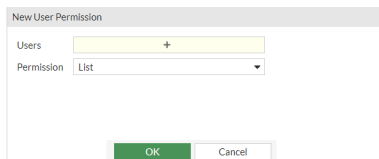
	 <p>The option is enabled by default.</p>
User Permission	<p>The level of user access to the secret. See User Permission on page 58.</p>
	 <p>This option is only available when <i>Inherit Permission</i> is disabled.</p>
	<p>For column settings, see Tables on page 15.</p>
Group Permission	<p>The level of user group access to the secrets. See Group Permission on page 59.</p>
	 <p>This option is only available when <i>Inherit Permission</i> is disabled.</p>
	<p>For column settings, see Tables on page 15.</p>

7. Click *Submit*.



See [Launching a secret on page 60](#) and [Example secret configurations example on page 67](#).

User Permission

- In step 5 when [Creating a secret](#), select *Create* in *User Permission*. The *New User Permission* window opens.



2. Enter the following information:

Users	<p>Select + and from the list, select users in the <i>Select Entries</i> window.</p> <p>To add a new user:</p> <ol style="list-style-type: none"> From the <i>Select Entries</i> window, select <i>Create</i> and then select <i>+User Definition</i>. The <i>New User Definition</i> wizard opens. Follow the steps in Creating a user on page 101, starting step 2 to create a new user. <hr/> <div style="display: flex; align-items: center;">  <div style="margin-left: 10px;">Use the search bar to look up a user.</div> </div> <hr/> <div style="display: flex; align-items: center;">  <div style="margin-left: 10px;">Use the pen icon next to a user to edit it.</div> </div>
--------------	---

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.

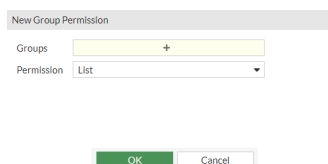
3. Click *OK*.



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

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 and then select *Edit* to edit the user group.
From the list, select user groups and then select *Delete* to delete the user groups.

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 *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. 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 85](#) and [Creating a secret on page 50](#). Also, see [AntiVirus on page 244](#).
- 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 247](#).

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

See [Check out and check in a secret on page 61](#).

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.



This feature is only available on the CLI.

```
config secret database
  edit <Secret ID>
    set address-blacklist <address>
  ...
config secret database
  edit <Secret ID>
    set address-whitelist <address>
  ...
```

Notes:

- If `address-blacklist` is set, all IP addresses except those in `<address>` are blocked. All other IP addresses are allowed.
- If `address-whitelist` is set, IP addresses in `<address>` are allowed. All other IP addresses are blocked.

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 50](#).

To check in a secret:

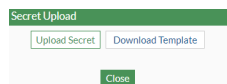
1. Go to *Secrets > Secret List*.
2. In *Secrets List*, double-click a secret to open.
Alternatively, in *Folders*, go to the folder where the secret is located, and double-click the secret to open.
3. On the top-right, click *Check-in Secret* to check in the secret.
Other approved users can now access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



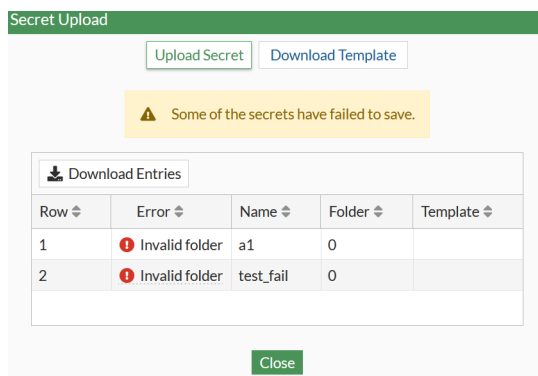
2. Select *Download Template* to download the secret upload template.
The secret upload template is downloaded on your computer. The file is named `FPAM_secret_upload`.
The secret upload template currently includes the following features:
 - Checks template completion when you quit; a warning appears 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.
3. Upon opening the `FPAM_secret_upload` file for the first time, enable editing and content for Macros.

- From the *Secret Template* column, select a supported template.



Windows Domain Account, Unix Account (SSH Password), and Windows Machine secret templates are supported.

- Fill in the fields highlighted in yellow.
- Save the file as `.xlsx`(Excel workbook) or a `.csv`(Comma delimited) file on your computer.
- In the *Secret Upload* dialog, select *Upload Secret*, locate the secret upload template file you created and click *Open*. Once the secret upload template file is successfully uploaded, *All secrets in the file have been uploaded* message displays.
- Click *Close*.
Any failed rows will be displayed in *Secret Upload*, and detailed information can be downloaded by clicking *Download Entries*.



Change password

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



You can only manually change the passwords every 30 seconds.

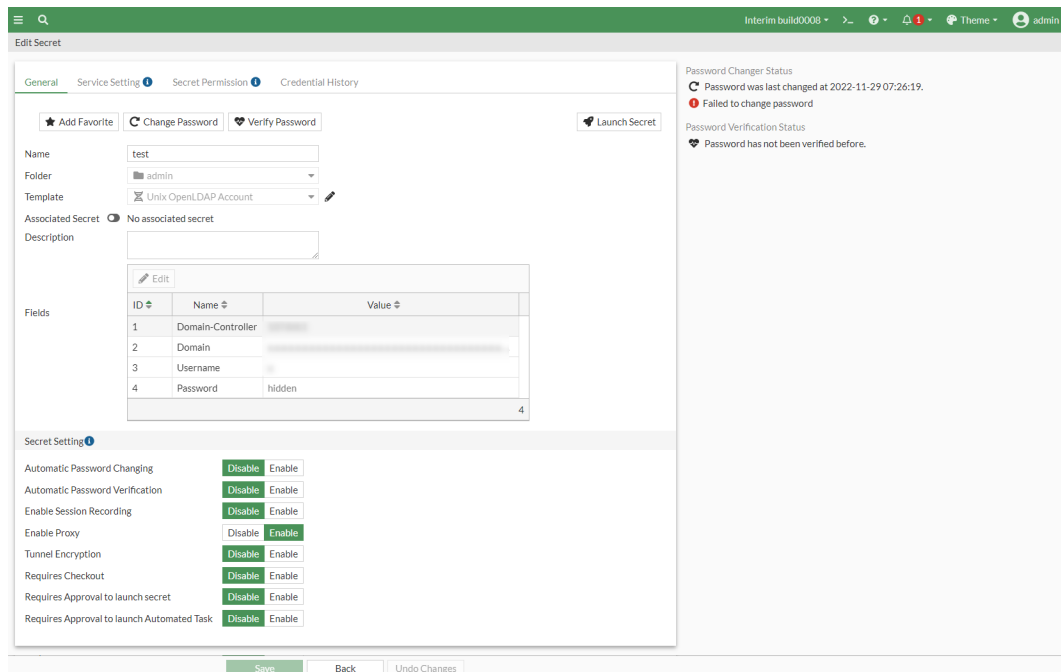


You can also set up a secret to automatically change the password by enabling *Automatic Password Changing* when creating or editing a secret.

See [Automatic password changing on page 161](#).

To change the password:

- Go to *Secret > Secret List*.
- 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 *Edit Secret* 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.

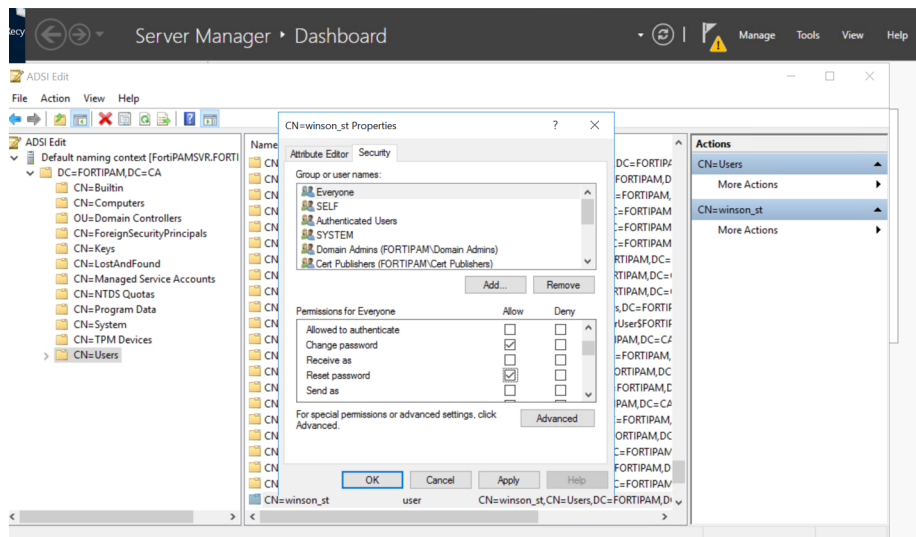
Note: The *Customized* option may be disabled if the secret template does not use password for authentication.



To be able to successfully change the password manually, the password must follow password requirements set in [Password policies on page 151](#).

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.

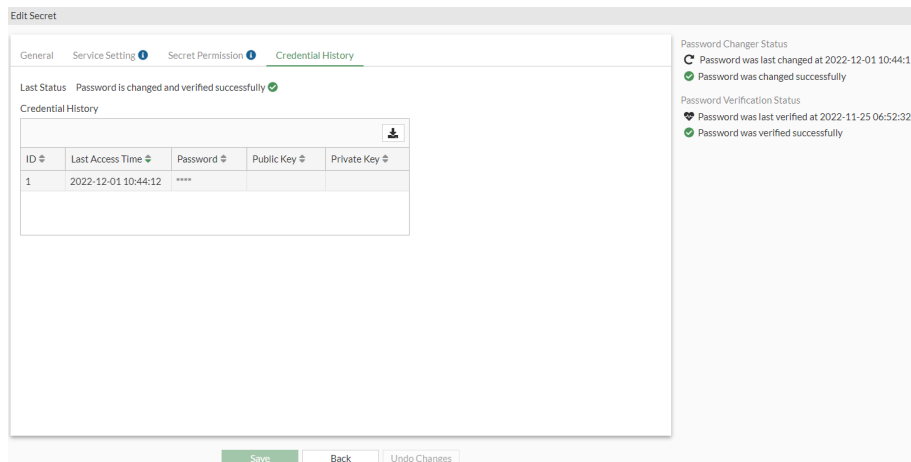
When using a password changer on Windows AD by LDAPs, it is required to enable both *Change password* and *Reset password* for the user on Windows AD.



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, go to *Folders*, and select the folder where the secret is located, and double-click the secret.
The *Edit Secret* 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, go to *Folders*, and select the folder where the secret is located, and double-click the secret.
The *Edit Secret* window opens.
3. Go to the *Credential History* tab.
4. To use the last credential from a failed password change, click *Verify Password*.
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.



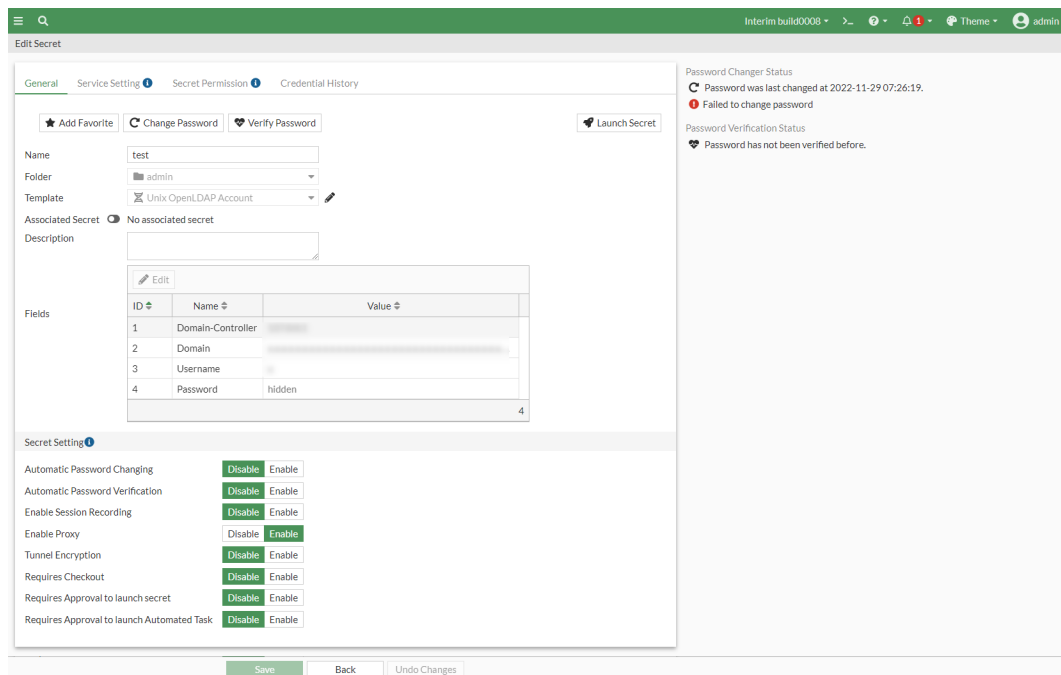
You can only manually verify passwords every 5 seconds.



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 162](#).

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 *Edit Secret* 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 by double-clicking 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 by double-clicking 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 clicking *Upload* to locate and upload the key file from your computer.
 - Select *Text Upload* and enter the public key in the space below.
 - Select *Auto Generated* 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 by double-clicking 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 by double-clicking 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 by double-clicking 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 by double-clicking 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 by double-clicking 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*.

Secret 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.

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

Name	Type	Executable	Parameter	References
PuTTY	SSH client			9
Remote Desktop-Windows	Remote desktop			6
TightVNC	VNC			1
VNC Viewer	VNC			1
Web Launcher	FortiClient Web extension			3
Web RDP	RDP over Web			6
Web SFTP	SFTP over Web			0
Web SMB	SMB over Web			1
Web SSH	SSH over Web			9
Web VNC	VNC over Web			1
WinSCP	SSH client			2

The following default launchers are available in FortiPAM:

- *PuTTY*: A basic SSH client using PuTTY.
- *Remote Desktop- Windows*: A basic RDP client using remote desktop.
- *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 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.

- *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.



The default launchers cannot be edited.



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



In proxy and non-proxy mode:

- Web launcher is available to users who have the permission to view the secret.
- Web launcher is disabled for users who do not have the permission to view the secret.

The *Secret Launchers* tab contains the following options:

Create	Select to create a new launcher. Creating a launcher on page 72.
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 <code>Enter</code> to search the launchers list. To narrow down your search, see Column filter .



Creating a launcher

To create a launcher:

1. Go to *Secrets > Secret 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: <ul style="list-style-type: none"> • <i>Other client</i>: Other client launcher type. • <i>Remote desktop</i>: RDP client launcher type. • <i>SSH client</i>: SSH client launcher type. • <i>VNC</i>: VNC client launcher type.
Executable	<p>The program file name, e.g., <code>putty.exe</code> for an SSH client.</p> <hr/> <p> Ensure that the program path is already added to the environment variable path in Windows before launching the secret.</p> <hr/> <p> An absolute path is also supported. Use the escape character (\) when using an absolute path, e.g.:</p> <pre>C:\\Users\\user1\\Documents\\putty.exe</pre> <pre>C:\\Users\\user1\\Documents\\New folder\\putty.exe</pre>
Parameter	<p>The command line parameters from the <i>Available Variables</i> list.</p> <p>Valid field variables are:</p> <ul style="list-style-type: none"> • \$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.



For the full path of a file, use the escape character double backslash (`\\`) for the `-m` parameter.

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 on page 75](#).

Clean Commands

Configure cleaning the environment. See [Creating a new launcher command on page 75](#).

5. Click *Submit*.

Non-proxy environment

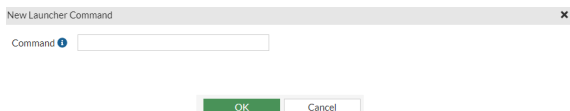
When using launchers with non-proxy mode, launchers may require the environment to be initialized beforehand. You may specify this with `init-commands` and `clean-commands`.

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 79](#) 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 information by double-clicking individual fields, entering the required information, and clicking *OK*.
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 79](#) 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 79](#) 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*.

Secret templates

Secret Templates in *Secrets* 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 154](#).

FortiPAM provides the following default templates:

AWS Web Account	Basic template for an AWS account.
Cisco Enable Secret	Basic template for Cisco enabled secret account.
Cisco User (SSH Secret)	Basic template for Cisco SSH account.
FortiProduct (SSH Password)	Basic template for a FortiProduct SSH Password account.
FortiProduct (SSH Key)	Basic template for a FortiProduct SSH Key account.
Machine	Basic template for a general machine, with all default launchers.
Unix Account (SSH Key)	Basic template for a Unix SSH Key account.
Unix Account (SSH Password)	Basic template for a Unix SSH Password account.
Unix Account (Web CIFS)	Basic template for a Unix Web Samba account.
Unix OpenLDAP Account	Basic template for an Open LDAP account.
Web Account	Basic template for a Web account.
Windows Domain Account	Basic template for a Windows Domain account.
Windows Domain Account (Samba)	Basic template for a Samba Windows Domain account.
Windows Machine	Basics template for a Windows machine.



Default templates cannot be modified.

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

Name #	Fields #	Launcher #	Password Changer #	Server Info #	Description #	References #
X AWS Web Account	Host, Username, Password, AccountID	Web Launcher		Other		0
X Cisco Enable Secret	Host, Username, Password	PuTTY, Web SSH	Cisco Enable Secret	Cisco		0
X Cisco User (SSH Secret)	Host, Username, Password, Public key, Private key, PuTTYGen	PuTTY, Web SSH	Cisco User (SSH Secret)	Cisco		0
X FortiProduct (SSH Key)	Host, Username, Password, Public key, Private key	PuTTY, Web SSH	SSH Key (FortiProduct)	Other		0
X FortiProduct (SSH Password)	Host, Username, Password	PuTTY, Web Launcher, Web SSH	SSH Password (FortiProduct)	Other		0
X Machine	Host, Username, Password	PuTTY, Web SSH, Remote Desktop Windows, Web RDP		Other		0
X Unix Account (SSH Key)	Host, Username, Password, Public key, Private key, PuTTYGen	PuTTY, Web SSH	SSH Key (Unix)	Unix/Linux		0
X Unix Account (SSH Password)	Host, Username, Password	Remote Desktop Windows, PuTTY, Web RDP, Web SSH	SSH Password (Unix)	Unix/Linux		0
X Unix Account (Web-CPS)	Host, Username, Password	Web SMB		Unix/Linux		0
X Unix OpenLDAP Account	Host, Username, Password, Domain Controller, Domain, Username, Password	PuTTY, Remote Desktop Windows, Web RDP, Web SFTP	Open LDAPS	Unix/Linux		0
X Web Account	Host, Username, Password	Web Launcher		Other		0
X Windows Domain Account	Host, Username, Password, Domain Controller, Domain, Username, Password	Remote Desktop Windows, PuTTY, Web RDP, Web SFTP	Active Directory LDAPS	Other		0
X Windows Domain Account (Smb)	Host, Username, Password, Domain Controller, Domain, Username, Password	Remote Desktop Windows, PuTTY, Web RDP, Web SFTP	Samba	Other		0
X Windows Machine	Host, Username, Password	Remote Desktop Windows, Web RDP		Other		0

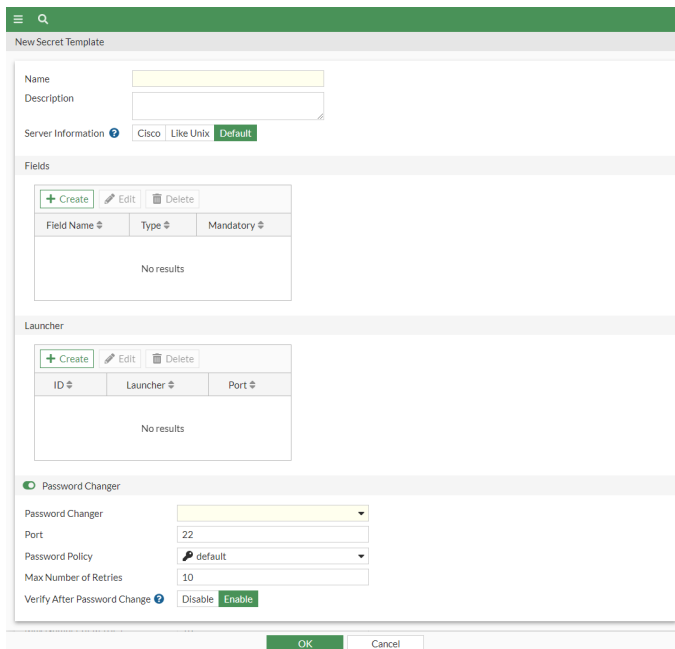
The secret templates list contains the following options:

Create	Select to create a new template. See Creating secret templates on page 79 .
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 *Secrets > Secret Templates*.
2. In the secret templates list, select *Create*.
The *New Secret Template* window opens.



3. Enter the following information:

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: <ul style="list-style-type: none"> • <i>Cisco</i> • <i>Like Unix</i> • <i>Default</i> 						
Fields	Secrets require fields to enter the secret related information. To add new fields, select <i>Create</i> and then enter the following information, and click <i>OK</i> : <table border="1" data-bbox="397 1270 1453 1812"> <tr> <td>Field Name</td> <td>The name of the field.</td> </tr> <tr> <td>Type</td> <td>From the dropdown, select a field type: <ul style="list-style-type: none"> • <i>Domain</i>: A domain field. • <i>Passphrase</i>: A passphrase fields. • <i>Password</i>: A password field. • <i>Private-Key</i>: A private-key field. • <i>Public-Key</i>: A public-key field. • <i>Target-Address</i>: A target address field. • <i>Text</i>: A text field. • <i>URL</i>: A URL field. • <i>Username</i>: A username field. </td> </tr> <tr> <td>Mandatory</td> <td>Enable to make this field mandatory or disable if this field will be optional.</td> </tr> </table>	Field Name	The name of the field.	Type	From the dropdown, select a field type: <ul style="list-style-type: none"> • <i>Domain</i>: A domain field. • <i>Passphrase</i>: A passphrase fields. • <i>Password</i>: A password field. • <i>Private-Key</i>: A private-key field. • <i>Public-Key</i>: A public-key field. • <i>Target-Address</i>: A target address field. • <i>Text</i>: A text field. • <i>URL</i>: A URL field. • <i>Username</i>: A username field. 	Mandatory	Enable to make this field mandatory or disable if this field will be optional.
Field Name	The name of the field.						
Type	From the dropdown, select a field type: <ul style="list-style-type: none"> • <i>Domain</i>: A domain field. • <i>Passphrase</i>: A passphrase fields. • <i>Password</i>: A password field. • <i>Private-Key</i>: A private-key field. • <i>Public-Key</i>: A public-key field. • <i>Target-Address</i>: A target address field. • <i>Text</i>: A text field. • <i>URL</i>: A URL field. • <i>Username</i>: 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 [Secret launchers on page 70](#).

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*:

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. Use the escape character (\) when using an absolute path, 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.



For the full path of a file, use the escape character double backslash (`\\`) for the `-m` parameter.

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.



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 155.](#)



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 152.](#)



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 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.

4. Click *OK*.

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 *Secrets* 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:

Name	Password Changer	Password Verification	Recording	Proxy Enabled	Tunnel Encryption	Block Rdp Clipboard	Checkout Enabled	Needs approval	SSH Filter	Antivirus Scan
default	Not Set	Not Set	Not Set	Enable	Disable	Not Set	Not Set	Not Set	Not Set	Not Set

The *Policies* list contains the following options:

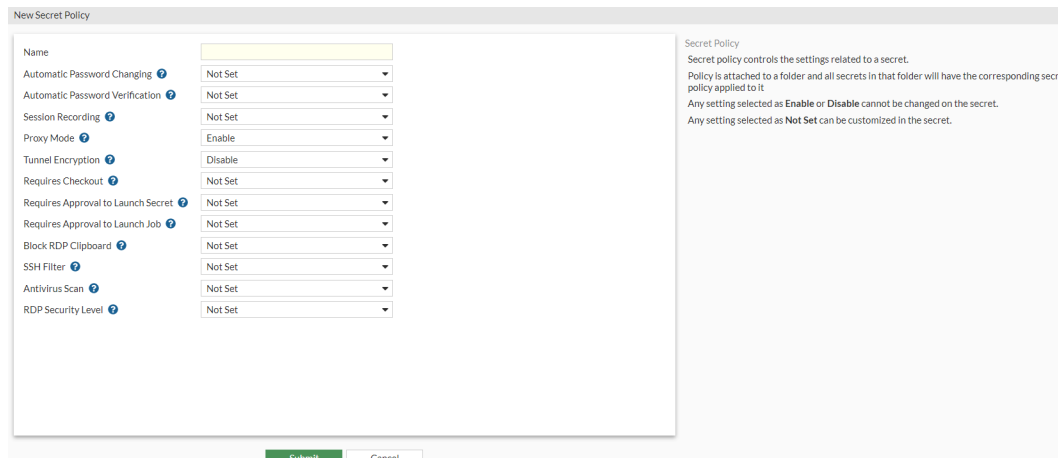
Create	Select to create a policy. See Creating a policy on page 85 .
Edit	Select to edit the selected policies.
Delete	Select to delete the selected policies.
Search	Enter a search term in the search field, then hit Enter to search the policies list. To narrow down your search, see Column filter .

Creating a policy

To create a policy:


1. Go to *Secrets > 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 <i>Enable</i> , <i>Disable</i> , or <i>Not Set</i> . 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 <i>Change Interval (min)</i> begins. Enter date (MM/DD/YYYY) and time or select the <i>Calendar</i> icon and then select a date and time.
Recurrence	From the dropdown, select from the following three frequencies of recurrence: <ul style="list-style-type: none"> • <i>Daily</i> • <i>Weekly</i> • <i>Monthly</i>

Repeat every	The number of days/weeks/months after which the password is changed (1-400).
Occurs on	<p>Select from the following days of the month when the password is automatically changed:</p> <ul style="list-style-type: none"> • <i>First</i> • <i>Second</i> • <i>Third</i> • <i>Last</i> • <i>Last Day</i> • <i>Day</i> <p>Select days of the week when the password is automatically changed. When you select <i>Day</i>, select + to add days of the month when the password is automatically changed.</p> <p>Note: The option is only available when <i>Recurrence</i> is set as <i>Weekly</i> or <i>Monthly</i>.</p>
Editable in Secret	Enable/disable users from customizing the password change schedule in the secret.
Automatic Password Verification	<p>Select <i>Enable</i>, <i>Disable</i>, or <i>Not Set</i>.</p> <p>When enabled, password changer for secrets is activated to periodically verify the password.</p>
Verification Interval (min)	The time interval at which the secrets are tested for accuracy, in minutes (default = 60, 5 - 44640).
Start Time	<p>The date and time when the <i>Interval(min)</i> begins.</p> <p>Enter date (MM/DD/YYYY) and time or select the <i>Calendar</i> icon and then select a date and time.</p>
Editable in Secret	When enabled, you can customize the password verification schedule in the secret.
Session Recording	<p>Select <i>Enable</i>, <i>Disable</i>, or <i>Not Set</i>.</p> <p>When enabled, user action performed on the secret is recorded.</p> <hr/> <div style="display: flex; align-items: center;">  <p>The video file is available in the log for users with appropriate permission.</p> </div> <hr/>
Proxy Mode	<p>Select <i>Enable</i>, <i>Disable</i>, or <i>Not Set</i>.</p> <p>When enabled, FortiPAM is responsible to proxy the connection from the user to the secret.</p> <p>When disabled, the non-proxy (direct) mode is used. See Modes of operation on page 17.</p>
Tunnel Encryption	<p>Select <i>Enable</i>, <i>Disable</i>, or <i>Not Set</i>.</p> <p>When launching a native launcher, FortiClient creates a tunnel between the endpoint and FortiPAM. The protocol stack is HTTP/TLS/TCP.</p>

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 61](#).

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 142](#) and [Approval flow on page 146](#).



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 142](#) and [Approval flow on page 146](#).

Approval Profile

From the dropdown, select an approval profile, or select *Create* to create a new approval profile. See [Approval profile on page 146](#).

	 <p>Use the search bar to look up an approval profile.</p>
	 <p>Use the pen icon next to the approval profile to edit it.</p>
<p>Block RDP Clipboard</p>	<p>Select <i>Enable</i>, <i>Disable</i>, or <i>Not Set</i>. When enabled, user is unable to copy/paste from the secret launcher.</p>
<p>SSH Filter</p>	<p>Select <i>Enable</i>, <i>Disable</i>, or <i>Not Set</i>. When enabled, commands defined in the SSH profile to be executed on the secret are blocked.</p>
<p>SSH Filter Profile</p>	<p>From the dropdown, select an SSH filter profile.</p>
<p>Antivirus Scan</p>	<p>Select <i>Enable</i>, <i>Disable</i>, or <i>Not Set</i>. When enabled, it enforces an antivirus profile on the secret. See AntiVirus on page 244.</p>
<p>Antivirus Profile</p>	<p>From the dropdown, select an antivirus profile.</p>
<p>RDP Security Level</p>	<p>Select a security level when establishing a RDP connection to the secret:</p> <ul style="list-style-type: none"> • <i>Best Effort</i>: If the server supports NLA, FortiPAM uses NLA to authenticate. Otherwise, FortiPAM conducts standard RDP authentication with the server through RDP over TLS. • <i>NLA</i>: Network Level Authentication (CredSSP). When an RDP launcher is launched, FortiPAM is forced to use CredSSP (NLA) to authenticate with the target server. • <i>Not Set</i> • <i>RDP</i>: FortiPAM uses the standard RDP encryption provided by the RDP protocol without using TLS (Web-RDP only). • <i>TLS</i>: RDP over TLS. FortiPAM uses secured connection with encryption protocol TLS to connect with the target server.
<p>RDP Restricted Admin Mode</p>	<p>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 <i>RDP Security Level</i> is set as <i>Best Effort</i> or <i>NLA</i>.</p>



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 89](#).

Applying a policy to a folder

To apply a policy to a folder:

1. Go to the folder in *Folder*.
2. Either select *Current Folder* to edit the folder and skip to step 6, or from the *Create* dropdown, select *Folder*.
When creating a new folder, the *Create New Folder in: dialog* appears.
3. Select a location for the folder and then select *Create Folder*.
4. Enter the name of the folder.
5. From the *Parent Folder* dropdown, select a folder.
6. 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 85](#).



Use the search bar to look up a policy.



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

7. Click *Submit*.

SSH filter profiles

SSH Filter Profiles tab in Secrets 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 90 .
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 <code>Enter</code> 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 *Secrets > SSH Filter Profiles*.
2. In *SSH Filter Profiles*, select *Create*.

The *New SSH Filter Profile* window opens.

The screenshot shows the 'New SSH Filter Profile' window. At the top, there is a 'Name' input field. Below it are two tabs: 'Shell Channel' (selected) and 'Other Channels'. Under the 'Shell Channel' tab, there is a 'Shell Commands' section containing a table with columns: ID, Type, Pattern, Action, Log, Alert, and Severity. The table currently displays 'No results'. Below the table is a 'Default Command Log' section with a 'Disable' button (highlighted in green) and an 'Enable' button. At the bottom right of the window are 'Submit' and 'Cancel' buttons.

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.

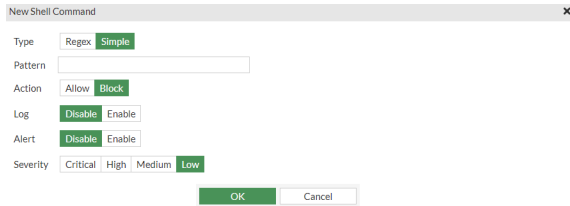
Block Channel	Select from the SSH blocking options (multiple options may be selected): <ul style="list-style-type: none"> • <i>X11</i>: X server forwarding • <i>SSH execution</i> • <i>Port forwarding</i> • <i>Tunnel forwarding</i> • <i>SFTP</i> • <i>SCP</i> • <i>Unknown channel</i>: Unknown channel (any 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): <ul style="list-style-type: none"> • <i>X11</i>: X server forwarding • <i>SSH execution</i> • <i>Port forwarding</i> • <i>Tunnel forwarding</i> • <i>SFTP</i> • <i>SCP</i> • <i>Unknown channel</i>
---------------------	--

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	<p>Select the matching type:</p> <ul style="list-style-type: none"> • <i>Regex</i>: Match command line using regular expression. Choosing the option blocks any command matching <i>Regex</i> in <i>Pattern</i>. • <i>Simple</i>: Match single command (default). Choosing the option matches any command fitting the one in <i>Pattern</i>.
Pattern	<p>SSH shell command pattern.</p> <p>For example:</p> <ul style="list-style-type: none"> • When the <i>Type</i> is <i>Regex</i>, pattern <code>. *</code> stands for all the commands and pattern <code>sh. *</code> stands for all the commands beginning with <code>sh</code> including <code>show</code> and <code>shutdown</code>. • When the <i>Type</i> is <i>Simple</i>, pattern <code>rm</code> stands for the <code>rm</code> command on Linux, e.g., <code>'rm -rf /*'</code>, <code>'rm test.py'</code>.
Action	<p>Action to take for URL filter matches:</p> <ul style="list-style-type: none"> • <i>Allow</i>: Allow the SSH shell command on the target server. • <i>Block</i>: Block the SSH shell command on the target server (default). <p>For example when the <i>Type</i> is <i>Regex</i>, the <i>Pattern</i> is <code>conf. *</code>, and the <i>Action</i> is <i>Block</i>. This blocks all the configuration actions on the target server.</p>
Log	<p>Enable/disable logging.</p> <p>When enabled, the action logs are available in <i>Log & Report > SSH</i>.</p>
Alert	<p>Enable/disable alert.</p> <p>When enabled, the alert message is sent based on the configurations in <i>Log & Report > Email Alert Settings</i>.</p>
Severity	<p>The severity of the actions reported in <i>Log & Report > SSH</i> and alert messages:</p> <ul style="list-style-type: none"> • <i>Critical</i> • <i>High</i> • <i>Medium</i> • <i>Low</i> (default)

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 *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.

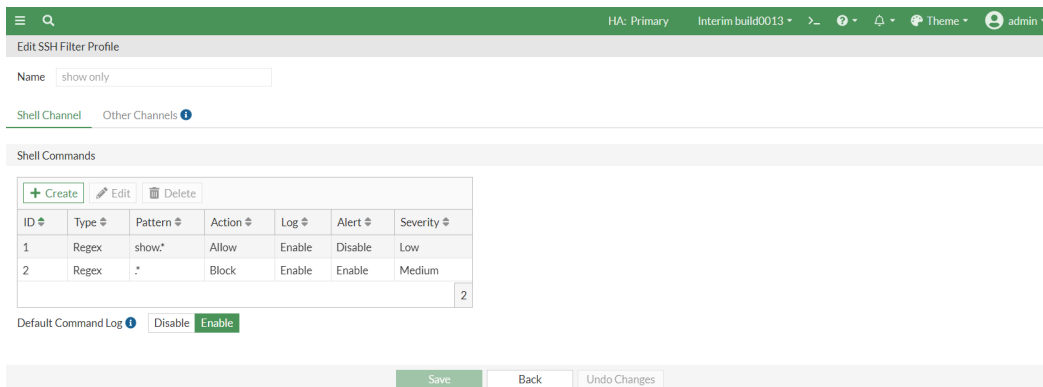
3. In *Service Setting* tab, ensure that *SSH Service* is enabled.
4. Enable *SSH Filter* and then select an SSH filter profile from the *SSH Filter Profile* dropdown.
5. Click *Save*.

Example SSH filter profiles - example

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

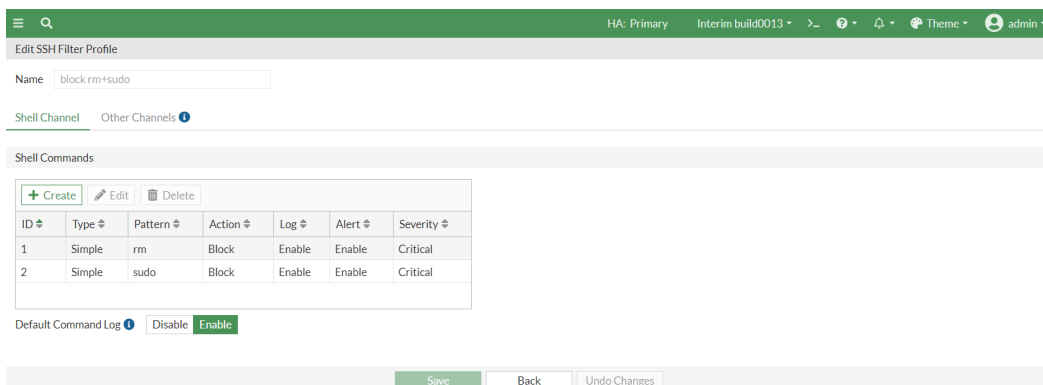
1. Go to *Secrets > SSH Filter Profiles*.
2. In *SSH Filter Profiles*, select *Create*.
The *New SSH Filter Profile* window opens.
3. Enter a name for the SSH filter profile. In this example, the SSH filter profile is named `show only`.
4. In *Shell Commands*, select *Create*:
 - a. In *Type*, select *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. Click *Submit*.



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

1. Go to *Secrets > 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. Click *Submit*.



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, 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 95 .
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: <ul style="list-style-type: none"> • <i>SSH Script</i>: targeting secrets that work on linux-like machines (default). • <i>SSH Procedure</i>: 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. <hr/> <div style="display: flex; align-items: center;">  <p>Use the search bar to look for a secret.</p> </div> <hr/> <div style="display: flex; align-items: center;">  <p>Use the pen icon next to a secret to edit it.</p> </div>
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. <hr/> <div style="display: flex; align-items: center;">  <p>Use the search bar to look for a secret.</p> </div> <hr/> <div style="display: flex; align-items: center;">  <p>Use the pen icon next to a secret to edit it.</p> </div>
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 <i>Calendar</i> icon and then select a date and time.
Recurrence	From the dropdown, select from the following three frequencies of recurrence: <ul style="list-style-type: none"> • <i>Daily</i> • <i>Weekly</i> • <i>Monthly</i> Note: The option is only available when <i>Recursive</i> 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 <i>Recursive</i> is enabled.
Occurs on	Select from the following days of the month when the job is automatically executed: <ul style="list-style-type: none"> • <i>First</i> • <i>Second</i> • <i>Third</i> • <i>Last</i> • <i>Last Day</i> • <i>Day</i> Select days of the week when the job is automatically executed. When you select <i>Day</i> , select + to add days of the month when the job is automatically executed. Note: The option is only available when <i>Recurrence</i> is set as <i>Weekly</i> or <i>Monthly</i> .
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 142](#).



When editing a job, select the *Log* tabs to see logs related to the job. See [Log & report on page 257](#).



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

Monitoring

Go to *Monitoring* to access the following tabs:

- [User monitor on page 98](#)
- [Active sessions on page 98](#)

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.

User Name	IP address	Duration	Traffic Volumes	Last Login
admin	172.16.51.17	28 minutes and 41 seconds	2.08 MB	2022/07/28 16:50:34

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 <code>Enter</code> 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

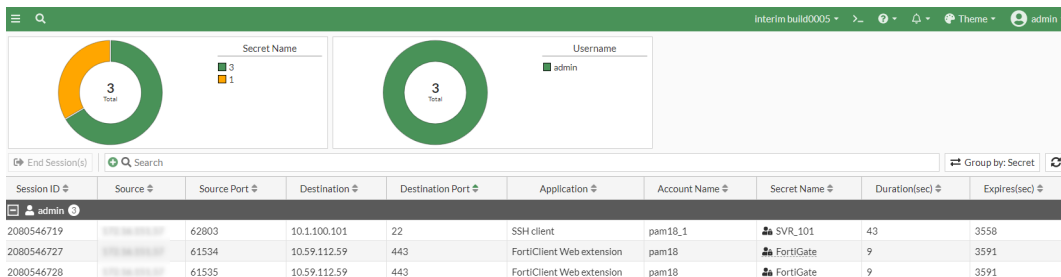
The *Active Sessions* tab in *Monitoring* provides a way to oversee activities of launched secrets from FortiPAM. The page lists out all the launched secrets with information such as source IP: Port, destination IP: Port, the application that is launched and username, etc. Additionally, an *End Session(s)* 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.

User management

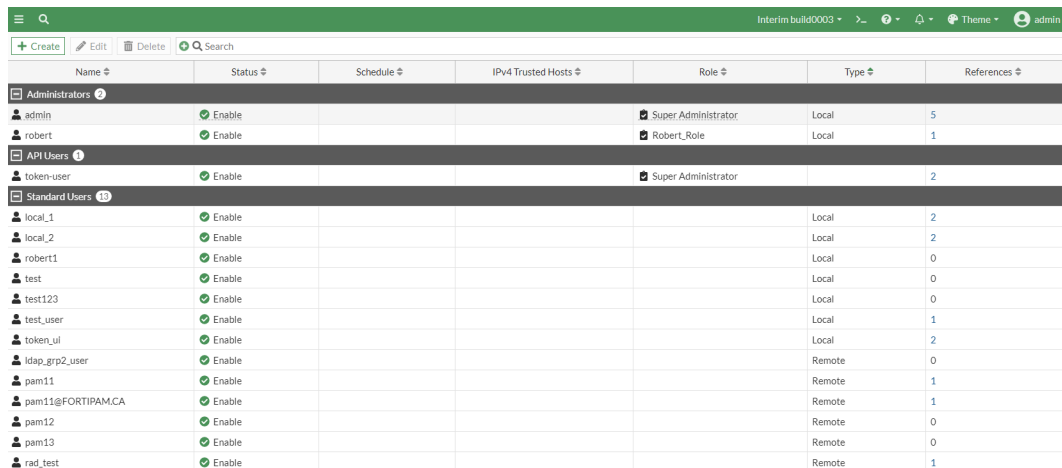
In *User Management*, you can access the following tabs:

- [User definition on page 100](#)
- [User groups on page 112](#)
- [Role on page 116](#)
- [LDAP servers on page 126](#)
- [SAML Single Sign-On \(SSO\) on page 129](#)
- [RADIUS servers on page 133](#)
- [Schedule on page 135](#)
- [FortiTokens on page 138](#)

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.



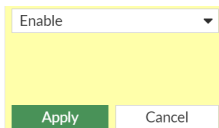
Name	Status	Schedule	IPv4 Trusted Hosts	Role	Type	References
Administrators						
admin	Enable			Super Administrator	Local	5
robert	Enable			Robert_Role	Local	1
API Users						
token-user	Enable			Super Administrator		2
Standard Users						
local_1	Enable				Local	2
local_2	Enable				Local	2
robert1	Enable				Local	0
test	Enable				Local	0
test123	Enable				Local	0
test_user	Enable				Local	1
token_ui	Enable				Local	2
ldap_grp2_user	Enable				Remote	0
pam11	Enable				Remote	1
pam11@FORTIPAM.CA	Enable				Remote	1
pam12	Enable				Remote	0
pam13	Enable				Remote	0
rad_test	Enable				Remote	1

The user definitions list contains the following options:

Create	Select to create a new user. See Creating a user on page 101 .
Edit	Select to edit the selected user account.
Delete	Select to delete the selected user account or accounts.
Search	Enter a search term in the search field, then hit <code>Enter</code> to search the user definition list. To narrow down your search, see Column filter .

To enable/disable a user:

1. Hover over the *Status* column for a user and select the pen icon.



2. From the dropdown, select either *Enable* or *Disable*.
3. Click *Apply*.

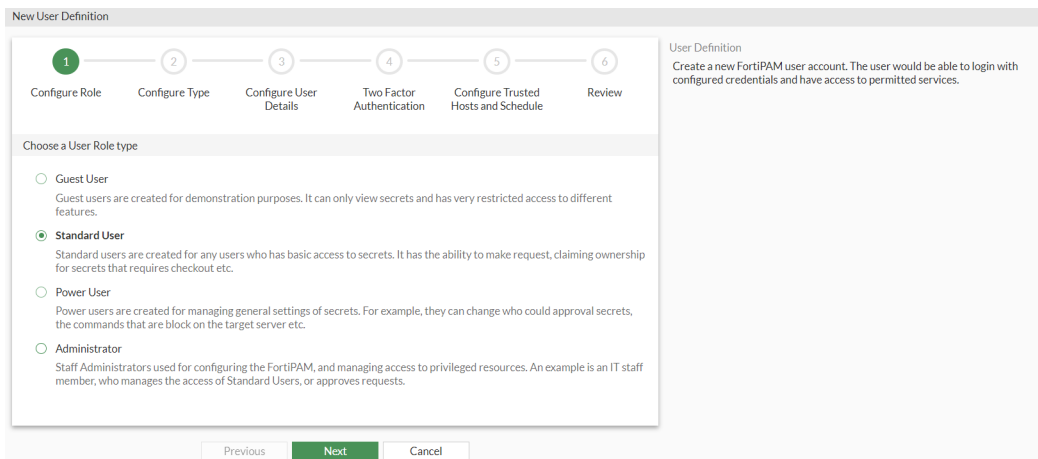
Creating a user



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*

For *Administrator*, select from one of the available administrator roles from the *Choose an Administrator Role* dropdown.



The administrator role decides what the administrator 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 role.

For information on the user types and their roles, see [Users in FortiPAM on page 105](#) and [Role on page 116](#).

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 112](#).



Use the search bar to look for a remote group.

For information on the user types, see [Users in FortiPAM on page 105](#).

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.

	Note: The option is not available when the user type is an API user.
Email address	The email address.
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: <ul style="list-style-type: none"> • <i>FortiToken</i> • <i>FortiToken Cloud</i>. See 2FA with FortiToken Cloud example on page 105. • <i>Email based two-factor authentication</i> (default)
Token	From the dropdown, select a token. This option is mandatory. Note: This option is only available when <i>FortiToken</i> is the <i>Authentication Type</i> .
Send Activation Code	Enable/disable sending activation codes. Note: This option is only available when <i>FortiToken Cloud</i> is the <i>Authentication Type</i> .
Email address	The email address. Note: This option is mandatory.
	 <p>The email address is synched from the email address added in the <i>Configure User Details</i> pane.</p>
Configure Trusted Hosts	
IPv4 Trusted Hosts	Trusted IPv4 addresses users use to connect to FortiPAM.
	 <p>Use + button to add a new IPv4 address and x to delete an added IPv4 address.</p>
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 135 . 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 116.

See [Creating a user](#) on page 101.

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*.

The screenshot shows the 'New User Definition' wizard with six steps: 1. Configure Role, 2. Configure Type, 3. Configure User Details, 4. Two Factor Authentication, 5. Configure Trusted Hosts and Schedule, and 6. Review. Step 2 is active. Under 'Choose a User Role type', the following options are listed:

- Guest User
Guest users are created for demonstration purposes. It can only view secrets and has very restricted access to different features.
- Standard User
Standard users are created for any users who has basic access to secrets. It has the ability to make request, claiming ownership for secrets that requires checkout etc.
- Power User
Power users are created for managing general settings of secrets. For example, they can change who could approval secrets, the commands that are blocked on the target server etc.
- Administrator
Staff Administrators used for configuring the FortiPAM, and managing access to privileged resources. An example is an IT staff member, who manages the access of Standard Users, or approves requests.
Choose an Administrator Role:

Buttons at the bottom: Previous, Next, Cancel.

3. Click *Next*.

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

The screenshot shows the 'New User Definition' wizard with step 2 completed and step 3 active. Under 'Choose a User type', the following options are listed:

- Local User
A user which has their information configured and stored on the FortiPAM.
- API User
API User can only access FortiPAM by using a token via the REST API instead of GUI.
- Remote User
A user which has their information configured and stored on a remote server. Check this option if you want to enable login for one remote user in a remote group, and assign them this role for their FortiPAM session.

Buttons at the bottom: Previous, Next, Cancel.



For *Remote User*, select a remote group where the user is found. See [User groups](#) on page 112.

5. Click *Next*.

6. In *Configure User Detail*:

- In *Username*, enter a name.
- In *Password*, enter a password.
- In *Confirm Password*, reenter password to confirm.
- In *Status*, enable logging in to FortiPAM.

- e. In *Email address*, enter an email address.

Progress bar: 1. Configure Role (checked), 2. Configure Type (checked), 3. Configure User Details (active), 4. Two Factor Authentication, 5. Configure Trusted Hosts and Schedule, 6. Review

Configure User Detail

Username: token

Password: [Change Password](#)

Status: Disable Enable

Email address:

Comments:

Buttons: Previous, Next, Cancel

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.

Progress bar: 1. Configure Role (checked), 2. Configure Type (checked), 3. Configure User Details (checked), 4. Two Factor Authentication (active), 5. Configure Trusted Hosts and Schedule, 6. Review

Two Factor Authentication

Authentication Type: FortiToken
 FortiToken Cloud
 Email based two-factor authentication

Send Activation Code:

Email address:

Buttons: Previous, Next, Cancel

- 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*.

New User Definition

1 2 3 4 5 6
Configure Role Configure Type Configure User Details Two Factor Authentication Configure Trusted Hosts and Schedule Review

Choose a User Role type

Guest User
Guest users are created for demonstration purposes. It can only view secrets and has very restricted access to different features.

Standard User
Standard users are created for any users who has basic access to secrets. It has the ability to make request, claiming ownership for secrets that requires checkout etc.

Power User
Power users are created for managing general settings of secrets. For example, they can change who could approval secrets, the commands that are blocked on the target server etc.

Administrator
Staff Administrators used for configuring the FortiPAM, and managing access to privileged resources. An example is an IT staff member, who manages the access of Standard Users, or approves requests.

Choose an Administrator Role:

Previous Next Cancel

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 112](#).

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 111](#).

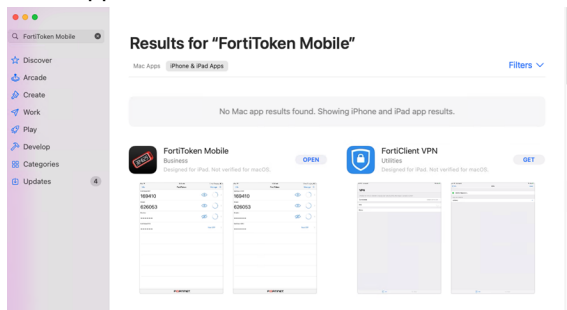
CLI configuration to set up a user with FortiToken as the authentication type - example:

```
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
```

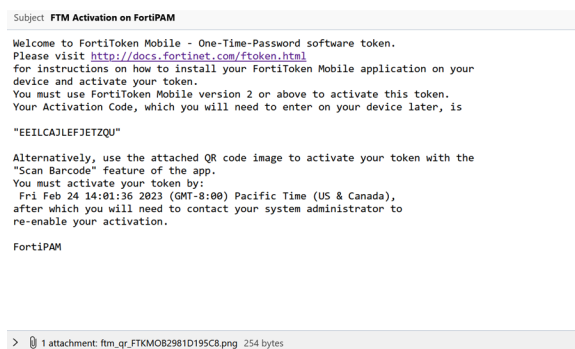
Setting up FortiToken Mobile

To set up FortiToken Mobile:

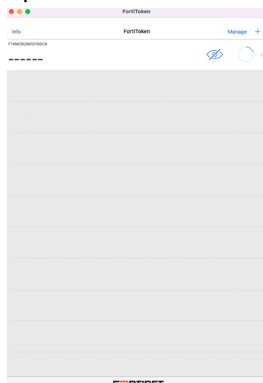
1. In the App Store, look for FortiToken Mobile and install the application.



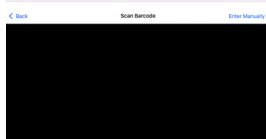
2. After your system administrator assigns a token to you, you will receive a notification with an activation code and an activation expiration date by which you must activate your token. For more information on *Token Activation*, see [FortiToken Mobile User Guide](#).



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*.



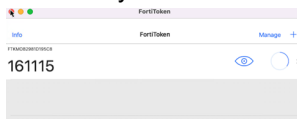
Key is the activation key from your activation email notification and must be entered exactly as it appears in the activation message, either by typing or copying and pasting.

iii. Click *Done*.

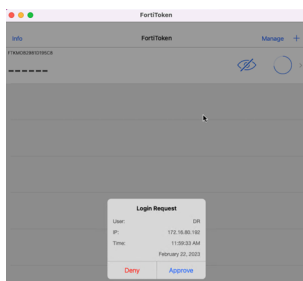
FortiToken Mobile communicates with the secure provisioning server to activate your token. The token is now displayed in the token list view.



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.

Name	User Members	Remote Groups	Remote Members	References
Local User				
fortipam_auth_group	admin			0
test	admin			0

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 <code>Enter</code> 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.

The screenshot shows a dialog box titled "Create New User Group". It has three input fields: "Name" (a text box), "Type" (a dropdown menu currently showing "Local User"), and "Members" (a text box with a "+" sign). At the bottom of the dialog, there are two buttons: "OK" (highlighted in green) and "Cancel".

3. Enter the following information:

Name	Name of the group.
Type	Select the type of the group: <ul style="list-style-type: none"> • <i>Remote</i> • <i>Local User</i>
Members	Select + to add existing members to the user group from the list and select <i>Close</i> , or select <i>Create</i> to create a new user. See Creating a user on page 101 .
	 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 <i>Type</i> is <i>Remote</i> .
	 Select remote groups from the list and select <i>Delete</i> to delete the remote groups. Select a remote group from the list and select <i>Edit</i> 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 126](#).



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 133](#).

- 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 101](#).



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 Administrator Role* dropdown. See [Creating a user on page 101](#).
The administrator role decides what the administrator can see.

Go to *Roles* in *User Management* to see a list of configured roles.

Name	Comment	Secret	System	User & Device	Log & Report	References
Default Profiles (Not Editable)						
Default Administrator		Read / Write	Read / Write	Read / Write	Read / Write	0
Guest User		Custom	None	None	None	0
Power User		Read / Write	None	None	None	0
Standard User		Custom	None	None	None	0
Super Administrator		Read / Write	Read / Write	Read / Write	Read / Write	3

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 <i>None</i> , <i>Read</i> , or <i>Read/Write</i> 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: <i>Secret Templates</i> , <i>Policies</i> and <i>Launchers</i> can be viewed.
Secret Folder	Set the access level for <i>Folders</i> . Note: You can restrict the corresponding folder and secret permissions under a specific secret.
Root Folder	Permission to create folders in <i>Root</i> . Note: The <i>Secret Folder</i> must be set to at least <i>Read</i> permission to enable accessing the root folder.
SSH Filter Profile	Set the access level for <i>SSH Filter Profiles</i> page.
Job List	Set the access level for <i>Jobs List</i> page.
Approval Request	Set the access level for <i>My Request</i> and <i>Request Review</i> page in <i>Approval Request</i> .
Approval Profile	Set the access level for <i>Approval Profile</i> page in <i>Approval Flow</i> .
Password Changer	Set the access level for <i>Password Changers</i> page in <i>Password Changing</i> .
Password Character Set	Set the access level for <i>Character Sets</i> page in <i>Password Changing</i> .
Password Policy	Set the access level for <i>Password Policies</i> page in <i>Password Changing</i> .
Create Personal Folder	Enable/disable creating a personal folder right after the user is created. Note: The <i>Secret Folder</i> permission must be <i>Read/Write</i> .
Edit Secret Templates	Enable/disable editing the <i>Secret Templates</i> page.
Edit Secret Policies	Enable/disable editing the <i>Policies</i> page.
Edit Secret Launchers	Enable/disable editing the <i>Secret Launchers</i> 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 <i>Addresses</i> page in <i>Authentication</i> .
Schemes & Rules	Set the access level for <i>Scheme & Rules</i> page in <i>Authentication</i> . Note: This requires the <i>Write</i> permission to <i>User Groups</i> , <i>Ldap Servers</i> , <i>Saml Single Sign-On</i> , and <i>Radius Servers</i> .
ZTNA	Set the access level for <i>ZTNA</i> page in <i>System</i> . Note: This requires the same permission as <i>Schedule</i> and <i>Addresses</i> . - Examples <ul style="list-style-type: none"> • If all required permissions are <i>Read/Write</i>, the ZTNA can only be either <i>None</i> or <i>Read/Write</i>. • If <i>Schedule</i> is set to <i>Read</i> and the rest is set to <i>Read/Write</i>, ZTNA can only be <i>None</i>.
Allow CLI Access	Enable/disable CLI access. Note: The <i>Administrator Users</i> must be set to <i>Write</i> permission to have CLI access.
Allow CLI Diagnostic Commands	Enable/disable access to diagnostic CLI commands. Note: <i>System Configuration</i> must be set to <i>Write</i> permission to manage system certificates.
	<hr/>  <p>The role must have <i>Allow CLI Access</i> enabled to access the diagnostic commands.</p> <hr/>
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.

New User Role

Name:

Comments:

Secret | User Management | **System & Network** | Admin Settings

	None	Read	Read / Write
System	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Configuration	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
FortiGuard Updates	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Email Alert / Log Settings	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Network	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Configuration	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Packet Capture	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Static Routes	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Fabric	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Endpoint Control	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Manage System Certificates

User Role

User roles or access profiles define what the user can do when logged into the FortiPAM. These Administrator Roles with custom permissions are used for creating Administrator / API users on the User Definition page.

Check the Definitions table for more details:

Permissions

None / Read / Write permissions provide access control to pages or features.

None gives no access, while the write permission lets the user modify the data on a page.

Read only allows the user to view the data.

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 <i>Events</i> , <i>Secrets</i> , <i>ZTNA</i> , and <i>SSH</i> logs in <i>Log & Report</i> .
View Reports	Enable/disable viewing <i>Reports</i> in <i>Log & Report</i> .
View Secret Launching Video	Enable/disable viewing playback videos in <i>Secret Video</i> . Note: <i>View Logs</i> must be enabled since the secret videos are available in <i>Log & Report > Secret</i> 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: <i>Secret Templates</i> , <i>Policies</i> and <i>Launchers</i> can be viewed.
Secret Folder	Controls the access to <i>Folders</i> . Note: You can restrict the corresponding folder and secret permissions under a specific folder and secret.
Root Folder	Permission to create folders in <i>Root</i> .
SSH Filter Profile	Access to the <i>SSH Filter Profiles</i> page.
Job List	Access to the <i>Job List</i> page.
Approval Request	Access to the <i>My Request</i> and <i>Request Review</i> page in <i>Approval Request</i> .
Approval Profile	Access to the <i>Approval Profile</i> page in <i>Approval Flow</i> .
Password Changer	Access to <i>Password Changers</i> page in <i>Password Changing</i> .
Password Character Set	Access to <i>Character Sets</i> page in <i>Password Changing</i> .
Password Policy	Access to <i>Password Policies</i> page in <i>Password Changing</i> .
Create Personal Folder	Enable/disable creating a personal folder right after the user is created.
Edit Secret Templates	Enable/disable editing the <i>Secret Templates</i> page.
Edit Secret Policies	Enable/disable editing the <i>Policies</i> page.
Edit Secret Launchers	Enable/disable editing the <i>Secret Launchers</i> page.
View Encrypted information	Enable/disable viewing the secret password, passphrase and ssh-key. The Secret list must have <i>Write</i> permission to view the encrypted secret information.
User Management	
Administrator Users	Access to the <i>User Definition</i> page in <i>User Management</i> and the <i>Backup</i> page in <i>System</i> .
User Groups	Access to the <i>User Groups</i> page in <i>User Management</i> .
Role	Access to the <i>Role</i> page in <i>User Management</i> .
Ldap Servers	Access to the <i>Ldap Servers</i> page in <i>User Management</i> .
Saml Single Sign-On	Access to the <i>Saml Single Sign-On</i> page in <i>User Management</i> .
Radius Servers	Access to the <i>Radius Servers</i> page in <i>User Management</i> .
Schedule	Access to the <i>Schedule</i> page in <i>User Management</i> .
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 <i>Addresses</i> page.
Scheme & Rules	Access to the <i>Scheme & Rules</i> page.
ZTNA	Access to the <i>ZTNA</i> page in <i>System</i> .
Network	
Configuration	Access to the <i>Interfaces</i> page in <i>Network</i> .
Packet Capture	Access to the <i>Packet Capture</i> page in <i>Network</i> .
Static Routes	Access to the <i>Static Routes</i> page in <i>Network</i> .
Fabric	Access to the <i>FortiAnalyzer Logging</i> card on the <i>Fabric Connectors</i> page in <i>Security Fabric</i> .
Endpoint Control	Access to the <i>FortiClient EMS</i> card on the <i>Fabric Connectors</i> page in <i>Security Fabric</i> .
Manage System Certificates	Enable/disable accessing the <i>Certificates</i> page in <i>System</i> .
System	
Configuration	Access to: <ul style="list-style-type: none"> • <i>DNS Settings</i> in <i>Network</i>. • <i>SNMP, Settings, and HA</i> pages in <i>System</i>. • VM License uploading; <i>System Reboot</i>, and <i>Shutdown</i> settings. • <i>Configuration Revisions</i> and <i>Scripts</i>.
FortiGuard Updates	Access to the <i>FortiGuard</i> page from <i>Dashboard</i> .
Email Alert/Log Settings	Access to <i>Email Alert Settings</i> and <i>Log Settings</i> in <i>Log & Report</i> .
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 <i>Events, Secrets, ZTNA, and SSH</i> logs in <i>Log & Report</i> .
View Reports	Enable/disable viewing <i>Reports</i> in <i>Log & Report</i> .
View Secret Launching Video	Enable/disable viewing playback videos in <i>Secret Video</i> .

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.

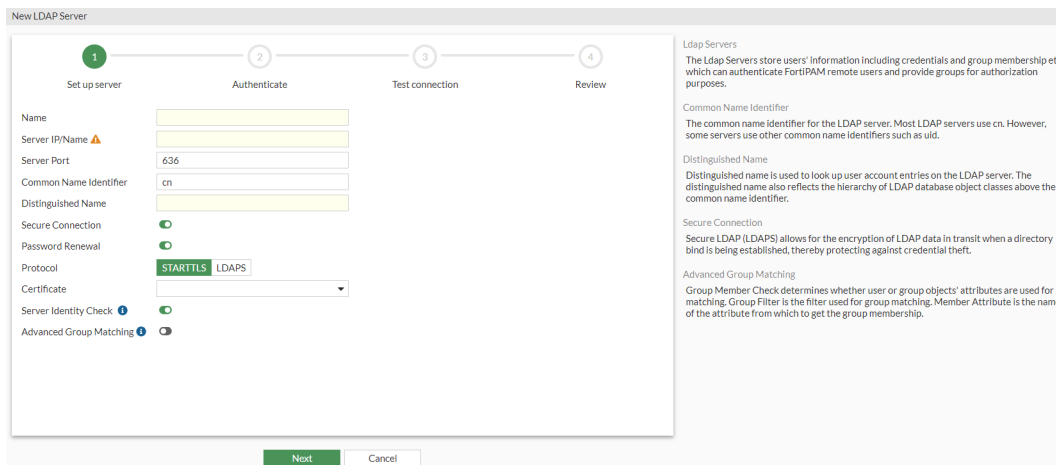
Name	Server	Port	Common Name Identifier	Distinguished Name	References
windows-ad	10.1.100.200	389	cn	dc=fortipam,dc=ca	5

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 <code>cn</code> . However, some servers use other common name identifiers such as <code>UID</code> . (default = <code>cn</code>).
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	<p>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.</p> <p>Note: This option is enabled by default.</p>
Password Renewal	<p>Enable to allow LDAP users to renew passwords.</p> <p>Note: This option is only available when <i>Secure Connection</i> is enabled.</p> <p>Note: This option is enabled by default.</p>
Protocol	When <i>Secure Connection</i> is enabled, select either <i>LDAPS</i> or <i>STARTTLS</i> (default).
Certificate	<p>When <i>Secure Connection</i> is enabled, select the certificate from the dropdown.</p> <hr/> <div style="display: flex; align-items: center;">  <p>Use the search bar to look up a certificate.</p> </div> <hr/>
Server Identity Check	<p>Enable to verify server domain name/IP address against the server certificate.</p> <p>Note: This option is only available when <i>Secure Connection</i> is enabled.</p> <p>Note: This option is enabled by default.</p>
Advanced Group Matching	<p>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.</p> <hr/> <div style="display: flex; align-items: center;">  <p>Depending on the LDAP server, you may need to configure additional properties to ensure LDAP groups are correctly matched.</p> </div> <hr/> <p>Note: The option is disabled by default.</p>
Group Member Check	From the dropdown, select a group member check option (default = <code>Ldap::grp::member::check:user-attr</code>).
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 = <code>memberof</code>).
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 116](#).

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 112](#).
3. Configuring the administrator account. See [Creating a user on page 101](#).

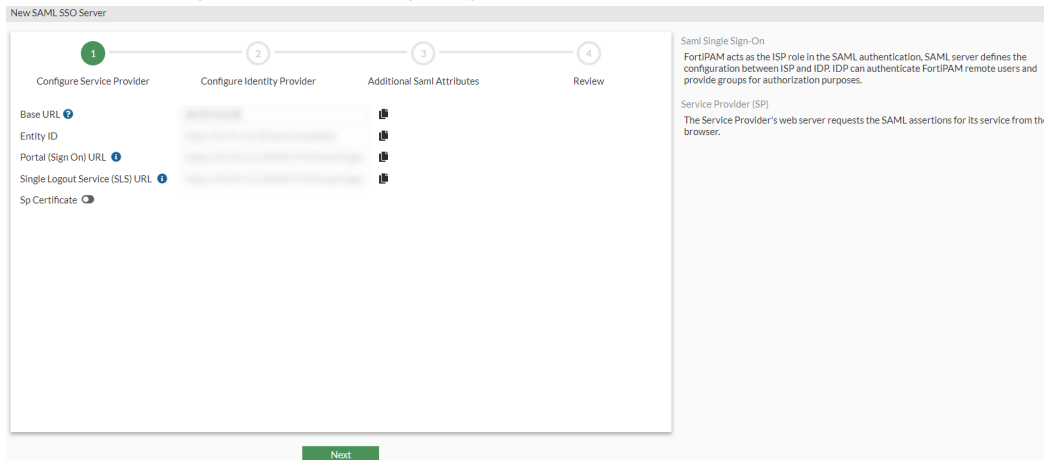
SAML Single Sign-On (SSO)

SAML SSO can be configured in *User Management*.

FortiPAM acts as the ISP in SAML authentication. The SAML server defines the configuration between ISP 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 <i>Fortinet Product</i> or a <i>Custom</i> IdP.
IdP Address	The IdP address. Note: This option is only available when the <i>Type</i> is <i>Fortinet Product</i> .
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 <i>Type</i> is <i>Fortinet Product</i> .
IdP Certificate	Select a server certificate to use for the SP. <div style="text-align: center;">  <p>Whenever the configuration changes on the IdP, you need to upload the new certificate reflecting the changes.</p> </div>
IdP entity ID	The IdP's entity ID, for example: <code>http://www.example.com/saml-idp/xxx/metadata/</code> Note: This option is only available when the <i>Type</i> is <i>Custom</i> .
IdP single sign-on URL	The IdP's login URL, for example: <code>http://www.example.com/saml-idp/xxx/login/</code> Note: This option is only available when the <i>Type</i> is <i>Custom</i> .
IdP single logout URL	The IdP's logout URL, for example: <code>http://www.example.com/saml-idp/xxx/logout/</code> Note: This option is only available when the <i>Type</i> is <i>Custom</i> .
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 = <code>User Principal Name</code>).
Group claim type	From the dropdown, select a group claim type (default = <code>User Group</code>).

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-ss0-server"
      next
    end
  next
end
config authentication scheme
  edit "fortipam_saml_auth_scheme"
    set method saml
    set saml-server "fortipam-saml-ss0-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.

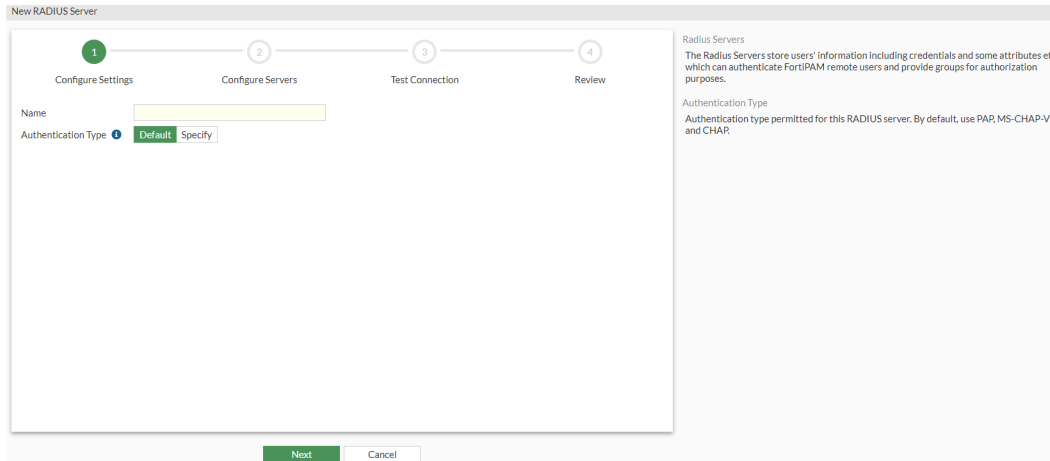
Name	Primary Server IP/Name	References
Authenticator_Radius	10.59.112.55	2

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 112](#).
3. Configuring a RADIUS user. [Creating a user on page 101](#).

Schedule

Schedule can be configured in *User Management*.

Set up a schedule to configure when the users can connect to FortiPAM.

Name	Days/Members	Start	End	Ref
always	Sunday Monday Tuesday Wednesday			2
default-darpp-optimize	Sunday Monday Tuesday Wednesday	01:00:00	01:30:00	0
none	None			0

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.

The screenshot shows the 'New Schedule' dialog box. It has a title bar 'New Schedule' and two tabs: 'Recurring' (selected) and 'One Time'. The dialog contains the following fields and options:

- Name:** A text input field.
- Color:** A color selection button labeled 'Change'.
- Days:** A grid of checkboxes for each day of the week: Monday, Tuesday, Wednesday, Thursday, Friday, Saturday, and Sunday.
- All day:** A checkbox.
- Start Time:** A time selection field set to 12:00 AM.
- Stop Time:** A time selection field set to 12:00 AM.

At the bottom of the dialog are two buttons: 'OK' and 'Cancel'.

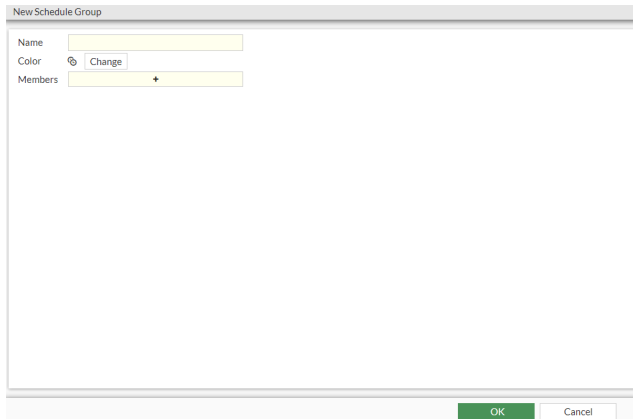
3. In the *New Schedule* window, enter the following information:

Type	Select either <i>Recurring</i> or <i>One Time</i> .
Name	The name of the schedule.
Color	Select <i>Change</i> and then select a color.
Days	Select the days of the week when the schedule applies. Note: This option is only available when the <i>Type</i> is <i>Recurring</i> .
All day	Enable to apply the schedule all day. Note: This option is only available when the <i>Type</i> is <i>Recurring</i> .
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 <i>Type</i> is <i>One Time</i> .
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 <i>Type</i> is <i>Recurring</i> and <i>All day</i> 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 <i>Type</i> is <i>One Time</i> .
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 <i>Type</i> is <i>Recurring</i> and <i>All day</i> is disabled.
Pre-expiration event log	Select to create an event log <i>Number of days</i> before the <i>End Date</i> . Note: This option is only available when the <i>Type</i> is <i>One Time</i> .
Number of days before	Enter the number of days (1 - 100, default = 3). Note: This option is only available when the <i>Type</i> is <i>One Time</i> and <i>Pre-expiration event log</i> 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 <i>Change</i> and then select a color.
Members	From the dropdown, select +, and in <i>Select Entries</i> , select members. If a new schedule is required, select <i>Create</i> 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 schedule.

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 116](#).

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.

Type	Serial Number	Status	User	Drift	Comments
Mobile Token	FTKMOB23F364DDEE	Available		0	
Mobile Token	FTKMOB239B685F9	Available		0	

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.



New FortiToken

Type: Hard Token Mobile Token

Comments: 0/255

Serial Number:

2. Enter the following information:

Type	The token type: <ul style="list-style-type: none"> • <i>Hard Token</i> • <i>Mobile Token</i>
Comments	Optionally, enter comments about the token. Note: This option is only available when the <i>Type</i> is <i>Hard Token</i> .
Serial Number	The FortiToken serial number. <hr/>  To add multiple FortiTokens, select + and enter a new serial number. <hr/> Note: This option is only available when the <i>Type</i> is <i>Hard Token</i> .
Activation Code	The activation code. Note: This option is only available when the <i>Type</i> is <i>Mobile Token</i> .
Import	Select the option to import multiple tokens by selecting one of the following and clicking <i>OK</i> : <ul style="list-style-type: none"> • <i>Serial Number File</i>: Select <i>Upload</i> to load a CSV file that contains token serial numbers. <hr/>  FortiToken devices have a serial number barcode on the m used to create the import file. <hr/> <ul style="list-style-type: none"> • <i>Seed File</i>: Select <i>Upload</i> to load a CSV file that contains token serial numbers, encrypted seeds, and IV values. Note: This option is only available when the <i>Type</i> is <i>Hard Token</i> .

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*.

Approval request

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.

See [My requests on page 141](#) and [Make a request on page 142](#).

My requests

Go to *Approval Request > My Requests* 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*

The screenshot shows the 'My Requests' interface. At the top, there are two donut charts. The first chart, titled 'Request Type', shows 2 total requests, with a green segment representing 'Launcher'. The second chart, titled 'Availability', shows 2 total requests, with a blue segment representing 'Pending' and an orange segment representing 'Expired'. Below the charts is a table with columns: Secret, Request Type, Tier Approval Progress, Start Time, Expiration Time, Duration, and Creation Time. The table contains two rows of data.

Secret	Request Type	Tier Approval Progress	Start Time	Expiration Time	Duration	Creation Time
Expired 1 Log server1#2	Launcher	✓✓	2022-12-22 16:01:00	2022-12-22 17:15:00	1 hour and 14 minutes	2022-12-22 16:01:54
Pending 1 Log server1#4	Launcher	⌚	2022-12-22 18:29:00	2022-12-22 18:59:00	30 minutes	2022-12-22 18:29:02



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 Requests* tab contains the following options:

Create	Select to create a new request. See Make a request on page 142 .
Edit	Select to edit the selected request.
Delete	Select to delete the selected requests.
Search	Enter a search term in the search field, then hit <code>Enter</code> 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 *Folders*, go to the folder where the secret is located, and double-click the secret to open.

You can also go to *Approval Request > My Requests*, 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 50](#).

The *New secret request* window opens.

4. Enter the following information:

Requester	<p>The requester.</p> <p>Note: The option cannot be changed.</p>
Request Type	<p>Select from the following request types:</p> <ul style="list-style-type: none"> • <i>Launcher</i> • <i>Job</i>
Secret	<p>When the <i>Request Type</i> is <i>Launcher</i>, from the dropdown, select a secret. These are secrets with <i>Requires Approval to Launch Secret</i> enabled. See Creating a secret on page 50.</p> <hr/> <p> 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.</p> <hr/> <p> When the <i>Request Type</i> is <i>Launcher</i>, use the search bar to look up a secret with <i>Requires Approval to Launch Secret</i> enabled.</p>
Job	<p>When the <i>Request Type</i> is <i>Job</i>, secret associated with the job is automatically selected. The option becomes non-editable. This is the secret with <i>Requires Approval to Launch Job</i> enabled.</p> <hr/> <p> Not all jobs require approval.</p> <p>When editing a secret, the <i>Requires Approval to Launch Job</i> option in the <i>Secret Setting</i> pane determines which jobs require approval.</p> <hr/> <p>From the dropdown, select a job.</p> <p>Note: The option is only available when the <i>Request Type</i> is <i>Job</i>.</p>
Request Duration	<p>When the <i>Request Type</i> is <i>Launcher</i>, from the dropdown, select a duration of time or select <i>Custom</i> and then enter a date (MM/DD/YYYY) and time range. Alternatively, select the calendar icon and select a start/end date and time.</p> <p>When the <i>Request Type</i> is <i>Job</i>, the start time is the time set in the job. Enter an end date (MM/DD/YYYY) and time.</p>

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 Requests* and *Request Review* tab. See [My requests on page 141](#) and [Request review on page 144](#).

Reviewers specified in [Approval profile on page 146](#) 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 Requests*.

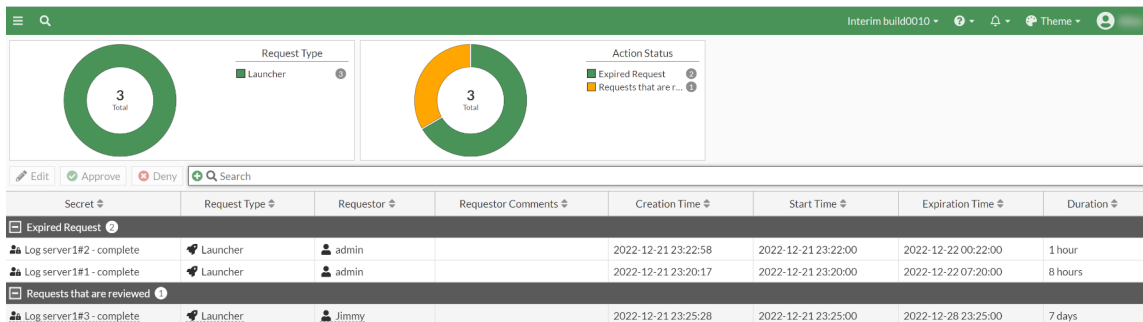


For the approver's email notification, an approver only receives the notification when the request goes to the corresponding tier where the approver is located.

Request review

Go to *Approval Request > Request Review* to see a list of secret requests for review.

The *Request Review* 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 *Request Review* tab contains the following options:

Edit

Select to approve or deny the selected request.

Alternatively, double-click a request to review the request. See [Approve a request on page 145](#).

Approve

Select to approve the selected request.

Deny	Select to deny the selected request.
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 *Approval Request > Request Review*, 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 *Request Review* tab and the status is updated in the [My requests on page 141](#) tab.

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

To see the reviewer comments:

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

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 147](#).

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 146](#).

Approval profile

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

For every approval profile, the following fields are shown:

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

Name	Type	Description	References
Approval_Team	Single Layer		0
test_4	Two Layers		0
test_flow	Single Layer		5



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 148 .
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 <code>Enter</code> 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 *Edit Secret* 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 148](#).
5. Click *Save*.

Create an approval profile





To create an approval request:

1. Go to *Approval Request > Approval Profile*.
2. Select *Create* to create a new approval profile.

The *New Approval Profile* window opens.

The screenshot shows a 'New Approval Profile' dialog box. It has a title bar 'New Approval Profile'. Below the title bar, there are three main sections: 1. 'Name' with a text input field. 2. 'Number of Approval Tiers' with a dropdown menu showing 'One' selected, and 'Two' and 'Three' as options. 3. 'Description' with a text area. Below these is a 'Tier-1 Settings' section. It contains: 1. 'Required number of Approvals' with a text input field containing '1'. 2. 'Approvers' with a '+' button. 3. 'Approver Groups' with a '+' button. At the bottom right of the dialog are 'OK' and 'Cancel' buttons.

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	<p>Select + and from the list, select users in the <i>Select Entries</i> window. The selected users will review the secret request.</p> <p>To add a new user:</p> <ol style="list-style-type: none"> From the <i>Select Entries</i> window, select <i>Create</i>. The <i>New User Definition</i> wizard opens. Follow the steps in Creating a user on page 101, starting step 2 to create a new user.
 Use the search bar to look up a user.	
Approver Groups	<p>Select + and from the list, select user groups in the <i>Select Entries</i> window. The selected user groups will review the secret request.</p> <p>To add a new user group:</p> <ol style="list-style-type: none"> From the <i>Select Entries</i> window, select <i>Create</i>. The <i>Create New User Group</i> window opens. Follow the steps in Creating user groups, starting step 3.
 Use the search bar to look up a user group.	

4. Click OK.

Password changing

Go to *Password Changing* to access the following tabs:

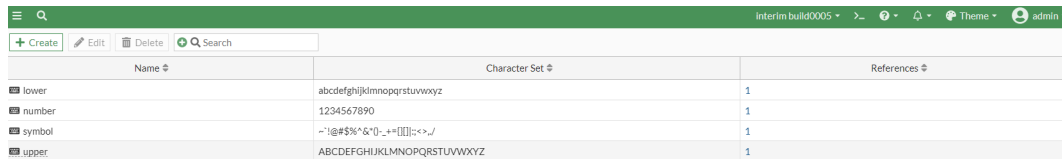
- [Character sets on page 150](#)
- [Password policies on page 151](#)
- [Password changers on page 154](#)

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 151](#).

Character Sets in *Password Changing* displays a list of configured character sets.

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



Name	Character Set	References
lower	abcdefghijklmnopqrstuvwxyz	1
number	1234567890	1
symbol	~!@#\$%^&*()_+=[\]{} :;<.>./	1
upper	ABCDEFGHIJKLMNOPQRSTUVWXYZ	1

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:

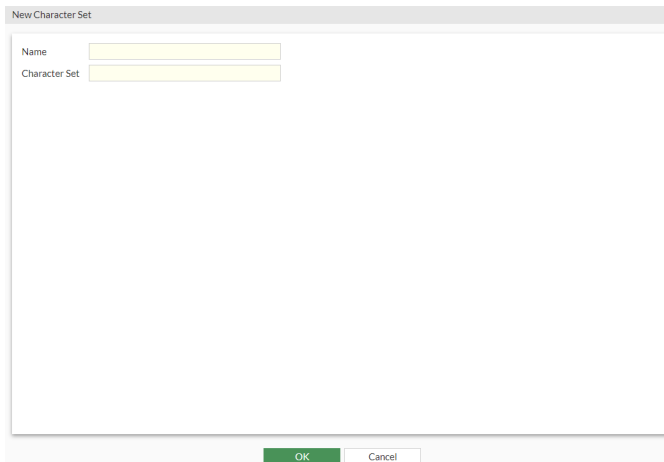
Create	Select to create a new character set. See Creating a character set on page 151 .
Edit	Select to edit the selected character set.
Delete	Select to delete the selected character sets.
Search	Enter a search term in the search field, then hit Enter to search the character sets list. To narrow down your search, see Column filter .

Creating a character set

To create a character set:

1. Go to *Password Changing > 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*.

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 154](#).

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.

Name	Password Requirement	Minimum Length	Maximum Length	References
default	3 lower 3 upper 2 symbol 2 number	10	20	0

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 150](#).

The *Password Policies* tab contains the following options:

Create	Select to create a new password policy. Password policies on page 151 .
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 *Password Changing > Password Policies*
2. Select *Create* to create a new password policy.

The *Create Password Policy* window opens.

Create Password Policy

Name

Minimum Length

Maximum Length

Password Requirements

[+ Create](#) [Edit](#) [Delete](#)

ID	Minimum Number	Character Set
No results		

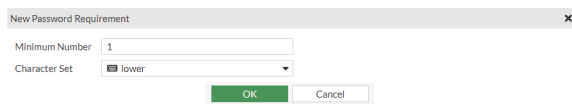
3. Enter the following information:

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 <i>Character Set</i> (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 151 .
 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 153](#).

Applying a password policy to a secret template

To apply a password policy to a secret template:

1. Go to *Secrets > Secret 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 152](#) and [Creating secret templates on page 79](#).
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		1
Cisco-Enable Secret	SSH with Password	Execute > enable	Expect > enable	Association	Association		1
Cisco-Enable Secret Custom	SSH with Password	Expect > Password: Execute > \$PASSWORD	Expect > Password: Execute > \$PASSWORD	Association	Association		0
Cisco-User (SSH Secret)	SSH with Password		Expect > #	Self	Self		1
Cisco-User (SSH) Custom	SSH with Password	Expect > Password: Execute > \$PASSWORD		Self	Self		0
Open LDAPS	Open LDAP			Self	Self		1
SSH Key (FortiProduct)	SSH with Public Key			Self	Self		1
SSH Key (FortiProduct) Custom	SSH with Public Key	Expect > to accept: Execute > a Expect Prompt > Execute > confg global		Self	Self		0
SSH Key (Unix)	SSH with Public Key			Self	Self		1
SSH Key (Unix) Custom	SSH with Public Key	Expect Prompt > Execute > cat Expect Prompt > Execute > mkdir -p .ssh		Self	Self		0
SSH Password (FortiProduct)	SSH with Password			Self	Self		1
SSH Password (FortiProduct) Custom	SSH with Password	Expect > to accept: Execute > a Expect Prompt > Execute > confg global		Self	Self		0
SSH Password (Unix)	SSH with Password			Self	Self		1
SSH Password (Unix) Custom	SSH with Password	Expect Prompt > Execute > password Expect > Current password: Execute > \$PASSWORD		Self	Self		0
Samba	Samba			Self	Self		2

FortiPAM offers the following default password changers:

- Active Directory LDAPS
- Open LDAPS
- SSH Key (FortiProduct)
- SSH Key (Unix)
- SSH Password (FortiProduct)
- SSH Password (Unix)
- Samba



Default password changers cannot be edited.
You can instead clone a default password and edit it.

The *Password Changers* tab contains the following options:

Create	Select to create a new password changer. See Creating a password changer on page 155 .
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 <code>Enter</code> 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 *Password Changing > 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: <ul style="list-style-type: none"> • <i>Active Directory LDAP</i> • <i>Open LDAP</i> • <i>Samba</i> • <i>SSH with Public Key</i> • <i>SSH with Password</i> (default)
New Line Mode	Select from the following options: <ul style="list-style-type: none"> • <i>CR (\r)</i>: Carriage Return (\r) • <i>CRLF (\r\n)</i>: Carriage Return and Line Feed (\r\n) (default) • <i>LF (\n)</i>: Line Feed (\n)
Change Auth Mode	Select from the following two options: <ul style="list-style-type: none"> • <i>Association</i>: Changing password requires credentials from the associated secret. See <i>Associated Secret</i> option when Creating a secret on page 50. • <i>Self</i>: Secret can change its password (default).
Verify Auth Mode	Select from the following two options: <ul style="list-style-type: none"> • <i>Association</i>: Verifying password requires credentials from the associated secret. See <i>Associated Secret</i> option when Creating a secret on page 50. • <i>Self</i>: Secret can verify its password (default).
Description	Optionally, enter a description.
Changers	The password changing procedure. See Changers . <hr/>  The option is available only when the <i>Type</i> is <i>SSH with Public Key</i> or <i>SSH with Password</i> . <hr/>
Verifiers	The password verification procedure. See Verifiers . <hr/>  The option is available only when the <i>Type</i> is <i>SSH with Public Key</i> or <i>SSH with Password</i> . <hr/>

5. Click **OK**.

Changers

1. In step 4 when [Creating a password changer](#), select *Create* in *Changers*. The *New Change Sequence* window opens.

The screenshot shows the 'New Change Sequence' configuration window. It includes the following fields and options:



- Type:** A dropdown menu set to 'Execute'.
- Command:** An empty text input field.
- Execute Action:** Two radio button options: 'Execute command unconditionally' (selected) and 'Execute command on previous match'.
- Critical:** Two radio button options: 'Disable' (selected) and 'Enable'.
- Delay (ms):** A text input field containing the value '50'.
- Description:** An empty text area.

Below the main fields, there is a section titled 'Allowed variables in Command:' which lists several variables with expandable arrows:

- ▶ \$USER
- ▶ \$PASSWORD
- ▶ \$PASSPHRASE
- ▶ \$NEWPASSWORD
- ▶ \$NEW_PUB_KEY
- ▶ \$NEW_PRI_KEY
- ▶ \${0}
- ▶ \$PUB_KEY

At the bottom of the window, there are two buttons: 'OK' and 'Cancel'.

2. Enter the following information:

Type	<p>From the dropdown, select from the following options:</p> <ul style="list-style-type: none"> • <i>Execute</i> • <i>Expect</i> • <i>Expect Prompt</i>
Command	<p>Commands to execute on the password changer.</p> <p>Valid variables are:</p> <ul style="list-style-type: none"> • \$USER • \$PASSWORD • \$PASSPHRASE • \$NEWPASSWD • \$NEW_PUB_KEY • \$NEW_PRI_KEY • \$[0].\$ • \$PUB_KEY <p>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.</p> <hr/> <div style="display: flex; align-items: center;">  <p>Enter \$ to get the list of valid variables.</p> </div> <hr/> <p>Note: The option is only available when the <i>Type</i> is <i>Execute</i>.</p>
Response	<p>The prompted line in target server.</p> <hr/> <div style="display: flex; align-items: center;">  <p>Enter \$ to get the list of valid variables.</p> </div> <hr/> <p>Note: The option is only available when the <i>Type</i> is <i>Expect</i>.</p>
Execute Action	<p>Either select <i>Execute command unconditionally</i> or <i>Execute command on previous match</i>.</p> <p>Note: The option is only available when the <i>Type</i> is <i>Execute</i>.</p>
Expect Action	<p>From the dropdown, select from the following three options:</p> <ul style="list-style-type: none"> • <i>Abort procedure on string not matched</i> • <i>Continue procedure on string not matched</i> • <i>Abort procedure on string matched</i> <p>Note: The option is only available when the <i>Type</i> is <i>Expect</i> or <i>Expect Prompt</i>.</p>
Critical	<p>Enable to indicate that the step is critical.</p>



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 Verify Sequence* window opens.

New Verify Sequence

Type: Execute

Command: [Empty]

Execute Action: Execute command unconditionally
Execute command on previous match

Critical: Disable Enable

Delay (ms): 50

Description: [Empty]

Allowed variables in Command:

- ▶ \$USER
- ▶ \$PASSWORD
- ▶ \$PASSPHRASE
- ▶ \$NEWPASSWD
- ▶ \$NEW_PUB_KEY
- ▶ \$NEW_PRI_KEY
- ▶ \$[]
- ▶ \$PUB_KEY




OK Cancel

2. Enter the following information:

Type

From the dropdown, select from the following options:

- *Execute*
- *Expect*

	<ul style="list-style-type: none"> • <i>Expect Prompt</i>
<p>Command</p>	<p>Commands to execute on the password changer.</p> <p>Valid variables are:</p> <ul style="list-style-type: none"> • \$USER • \$PASSWORD • \$PASSPHRASE • \$NEWPASSWD • \$NEW_PUB_KEY • \$NEW_PRI_KEY • \$[0].\$ • \$PUB_KEY <p>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.</p> <hr/> <div style="display: flex; align-items: center;">  <p>Enter \$ to get the list of valid variables.</p> </div> <hr/> <p>Note: The option is only available when the <i>Type</i> is <i>Execute</i>.</p>
<p>Response</p>	<p>The prompted line in target server.</p> <hr/> <div style="display: flex; align-items: center;">  <p>Enter \$ to get the list of valid variables.</p> </div> <hr/> <p>Note: The option is only available when the <i>Type</i> is <i>Expect</i>.</p>
<p>Execute Action</p>	<p>Either select <i>Execute command unconditionally</i> or <i>Execute command on previous match</i>.</p> <p>Note: The option is only available when the <i>Type</i> is <i>Execute</i>.</p>
<p>Expect Action</p>	<p>From the dropdown, select from the following three options:</p> <ul style="list-style-type: none"> • <i>Abort procedure on string not matched</i> • <i>Continue procedure on string not matched</i> • <i>Abort procedure on string matched</i> <p>Note: The option is only available when the <i>Type</i> is <i>Expect</i> or <i>Expect Prompt</i>.</p>
<p>Critical</p>	<p>Enable to indicate that the step is critical.</p> <hr/> <div style="display: flex; align-items: center;">  <p>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.</p> </div> <hr/>

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 161](#) and [Automatic password verification on page 162](#).

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 *Folders*, 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 *Folders*, 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.

Authentication

Go to *Authentication* to access the following tabs:

- [Addresses on page 163](#)
- [Scheme & Rules on page 171](#)

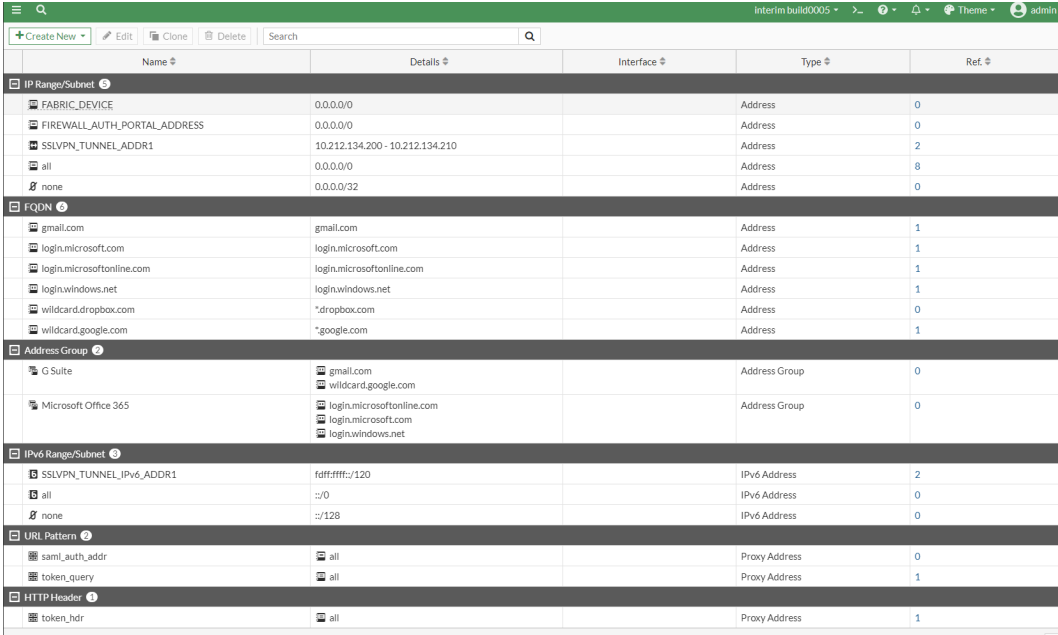
Addresses

The *Addresses* tab in *Authentication* 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.



Name	Details	Interface	Type	Ref.
IP Range/Subnet				
FABRIC_DEVICE	0.0.0.0/0		Address	0
FIREWALL_AUTH_PORTAL_ADDRESS	0.0.0.0/0		Address	0
SSLVPN_TUNNEL_ADDR1	10.212.134.200 - 10.212.134.210		Address	2
all	0.0.0.0/0		Address	8
none	0.0.0.0/32		Address	0
FQDN				
gmail.com	gmail.com		Address	1
login.microsoft.com	login.microsoft.com		Address	1
login.microsoftonline.com	login.microsoftonline.com		Address	1
login.windows.net	login.windows.net		Address	1
wildcard.dropbox.com	*dropbox.com		Address	0
wildcard.google.com	*google.com		Address	1
Address Group				
G Suite	gmail.com wildcard.google.com		Address Group	0
Microsoft Office 365	login.microsoftonline.com login.microsoft.com login.windows.net		Address Group	0
IPv6 Range/Subnet				
SSLVPN_TUNNEL_IPv6_ADDR1	fdffff::/120		IPv6 Address	2
all	:::0		IPv6 Address	0
none	:::128		IPv6 Address	0
URI Pattern				
saml_auth_addr	all		Proxy Address	0
token_query	all		Proxy Address	1
HTTP Header				
token_hdr	all		Proxy Address	1

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 164](#) and [Creating an address group on page 169](#)

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 *Authentication > Addresses*.
2. From the **+Create New** dropdown, select *Address*.

The *New Address* window opens.

3. Enter the following information:

Category	Select from the following options: <ul style="list-style-type: none"> • <i>Address</i> • <i>Proxy Address</i>
Name	Name of the address.
Color	Select <i>Change</i> , and from the color palette choose a color.
Type	From the dropdown, select from the following options when the <i>Category</i> is <i>Address</i> : <ul style="list-style-type: none"> • <i>Subnet</i> (default) • <i>IP Range</i> • <i>FQDN</i> • <i>addr_type_fqdn-group</i> • <i>Geography</i> • <i>Dynamic</i> • <i>Device (MAC Address)</i>

	<p>From the dropdown, select from the following options when the <i>Category</i> is <i>Proxy Address</i>:</p> <ul style="list-style-type: none"> • <i>Host Regex Match</i> • <i>URL Pattern</i> (default) • <i>URL Category</i> • <i>URL List</i> • <i>HTTP Method</i> • <i>User Agent</i> • <i>HTTP Header</i> • <i>Advanced (Source)</i> • <i>Advanced (Destination)</i>
IP/Netmask	<p>Enter the IP address and the netmask.</p> <p>Note: The option is only available when the <i>Category</i> is <i>Address</i> and the <i>Type</i> is <i>Subnet</i>.</p>
IP Range	<p>Enter the IP address range.</p> <p>Note: The option is only available when:</p> <ul style="list-style-type: none"> • <i>Category</i> is <i>Address</i> and the <i>Type</i> is <i>IP Range</i>.
FQDN	<p>Enter the Fully Qualified Domain Name (FQDN).</p> <p>Note: The option is only available when:</p> <ul style="list-style-type: none"> • <i>Category</i> is <i>Address</i> and the <i>Type</i> is <i>FQDN</i>.
Country/Region	<p>From the dropdown, select a country.</p> <p>Note: The option is only available when:</p> <ul style="list-style-type: none"> • <i>Category</i> is <i>Address</i> and the <i>Type</i> is <i>Geography</i>.
Sub Type	<p>From the dropdown, select from the following options:</p> <ul style="list-style-type: none"> • <i>ClearPass</i> • <i>Fabric Connector Address</i> (default) • <i>FortiNAC Tag</i> • <i>FortiVoice Tag</i> • <i>Fortinet Single Sign-On</i> • <i>Switch Controller NAC Policy Tag</i> <hr/> <div style="display: flex; align-items: center;">  <p>To automatically resolve and assign MAC addresses, configure a NAC policy with <i>Switch Controller NAC Policy Tag</i>.</p> </div> <hr/> <p>Note: The option is only available when the <i>Category</i> is <i>Address</i> and the <i>Type</i> is <i>Dynamic</i>.</p>
SDN connector	<p>From the dropdown, select an SDN connector or create a new SDN connector.</p>



Use the search bar to look for an SDN connector.



Use the pen icon next to the SDN connector to edit it.

Note: The option is only available when:

- *Category* is *Address*, *Type* is *Dynamic*, and the *Subtype* is *Fabric Connector Address*.

SPT (System Posture Token)

From the dropdown, select from the following options:

- *Checkup*
- *Healthy*
- *Infected*
- *Quarantine*
- *Transient*
- *Unknown (default)*

Note: The option is only available when the *Category* is *Address*, *Type* is *Dynamic* and the *Subtype* is *ClearPass*.

FSSO Group

Select +, and in *Select Entries*, select FSSO groups or create an FSSO group, click *Close*.

The address for the selected FSSO group is dynamically retrieved.



Use the search bar to look for an FSSO group.



Use the pen icon next to the FSSO group to edit it.

Note: The option is only available when:

- *Category* is *Address*, *Type* is *Dynamic*, and the *Sub Type* is *Fortinet Single Sign-On (FSSO)*.

MAC address

Enter a MAC address. Select + to add a range of MAC addresses.

Note: The option is only available when:

- *Category* is *Address* and the *Type* is *Device (MAC Address)*.

Host

For *Proxy Address*, from the dropdown, select a host or create a host address, address group, or proxy address.



Use the search bar to look for a host.



Use the pen icon next to the host to edit it.

Note: The option is only available when:

- *Category* is *Proxy Address* and *Type* is any option other than *Host Regex Match*.

URL Path Regex

URL path as a regular expression.

Note: The option is only available when the *Category* is *Proxy Address* and the *Type* is *URL Pattern* or *Advanced (Destination)*.

Host Regex Pattern

Host name as a regular expression.

Note: The option is only available when the *Category* is *Proxy Address* and the *Type* is *Host Regex Match*.

URL Category

Select +, and in *Select Entries*, select web filter categories or create a new external connector.



Use the search bar to look for a URL category.

Note: The option is only available when the *Category* is *Proxy Address* and the *Type* is *URL Category* or *Advanced (Destination)*.

URL List

From the dropdown, select a URL list.



Use the search bar to look for a URL list.

Note: The option is only available when the *Category* is *Proxy Address* and the *Type* is *URL List*.

Request Method

Select +, and in *Select Entries*, select methods, and click *Close*.






Use the search bar to look for a method.

Note: The option is only available when the *Category* is *Proxy Address* and the *Type* is *HTTP Method* or *Advanced (Source)*.

User Agent

Select +, and in *Select Entries*, select web browsers.

	 <p>Use the search bar to look for a browser.</p>
	<p>Note: The option is only available when the <i>Category</i> is <i>Proxy Address</i> and the <i>Type</i> is <i>User Agent</i> or <i>Advanced (Source)</i>.</p>
Header Name	<p>Name/Key of the HTTP header.</p> <p>Note: The option is only available when the <i>Category</i> is <i>Proxy Address</i> and the <i>Type</i> is <i>HTTP Header</i>.</p>
Header Regex	<p>HTTP header value as a regular expression.</p> <p>Note: The option is only available when the <i>Category</i> is <i>Proxy Address</i> and the <i>Type</i> is <i>HTTP Header</i>.</p>
HTTP header	<p>HTTP header name and value.</p>
	 <p>Select + to add additional HTTP headers.</p>
	<p>Note: The option is only available when the <i>Category</i> is <i>Proxy Address</i> and the <i>Type</i> is <i>Advanced (Source)</i>.</p>
Interface	<p>From the dropdown, select an interface or create a new interface.</p> <p>Note: By default, <i>any</i> is selected.</p>
	 <p>Use the search bar to look for an interface.</p>
	<p>Note: The option is only available when the <i>Category</i> is <i>Address</i>.</p>
Static route configuration	<p>Enable static route configuration to allow the address to be used in a static route.</p> <p>Note: The option is disabled by default and is only available when the <i>Category</i> is <i>Address</i> and the <i>Type</i> is one of the following:</p> <ul style="list-style-type: none"> • <i>Subnet</i> • <i>IP Range</i> • <i>FQDN</i>
Comments	<p>Optionally, enter comments about the address.</p>

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
```

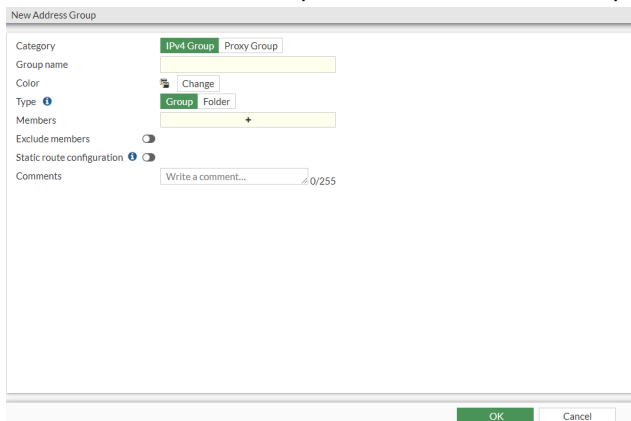


```
set type iprange
set start-ip 10.212.134.200
set end-ip 10.212.134.210
next
end
```

Creating an address group

To create an address group:

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







The screenshot shows the 'New Address Group' configuration window. The window has a title bar 'New Address Group' and a close button. The configuration fields are as follows:

- Category:** A dropdown menu with 'IPv4 Group' selected and 'Proxy Group' as an alternative.
- Group name:** A text input field.
- Color:** A color selection tool with a 'Change' button.
- Type:** A dropdown menu with 'Group' selected and 'Folder' as an alternative.
- Members:** A text input field with a '+' icon to add members.
- Exclude members:** A toggle switch, currently turned off.
- Static route configuration:** A toggle switch with an information icon, currently turned off.
- Comments:** A text input field with the placeholder 'Write a comment...' and a character count '0/255'.

At the bottom of the window, there are 'OK' and 'Cancel' buttons.

3. Enter the following information:

Category	Select from the following options: <ul style="list-style-type: none"> • <i>IPv4 Group</i> • <i>Proxy Group</i>
Group name	Name of the group.
Color	Select <i>Change</i> , and from the color palette choose a color.
Type	For an IPv4 group, select either <i>Group</i> or <i>Folder</i> . For a proxy group, select either <i>Source Group</i> or <i>Destination Group</i> .
	 <p>Members of the address folders can only belong to a single address folder.</p>
Members	Select +, and in <i>Select Entries</i> , select a member or create an address or an address group, click <i>Close</i> .
	 <p>Use the search bar to look for a member.</p>
	 <p>Use the pen icon next to the member to edit it.</p>
Excluded members	Enable, and select + to add members to be excluded or create addresses and address groups to be excluded, click <i>Close</i> . Note: The option is disabled by default and only available when <i>Category</i> is <i>IPv4 Group</i> .
Static route configuration	Enable static route configuration to allow the address group to be used in a static route.
	 <p>All the members of an address group must have static route configuration enabled.</p>
	Note: The option is disabled by default and only available when <i>Category</i> is <i>IPv4 Group</i> .
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-9003cableecb
set member "gmail.com" "wildcard.google.com"
next
end
```

Scheme & Rules

The *Scheme & Rules* tab in *Authentication* displays a list of the configured authentication rules and schemes.

An authentication scheme defines the method of authentication that is applied. By default, *fortipam_auth_scheme* and *fortipam_token_scheme* authentication schemes are available.



In accordance with PAM design, you should avoid changing the default authentication schemes.



Schemes and rules must not be configured by the customers.

Schemes and rules are automatically updated when the following features are configured:

- API users
- LDAP server and users
- RADIUS server and users
- SAML server and users

An authentication rule defines the proxy sources and destinations that require authentication, and which authentication scheme to apply.

For each authentication scheme, the following columns are displayed:

- Name
- Method
- User database
- Reference

Name	Method	User database	Ref.
fortipam_auth_scheme	Form-based	local-admin-db	1
fortipam_token_scheme	Token Code	test_RADIUS_server	2

For each authentication rule, the following columns are displayed:

- Seq #
- Name
- Source Address

- Authentication Scheme
- Comments

Seq #	Name	Source Address	Authentication Scheme	Comments
1	fortipam_token_hdr	token_hdr	fortipam_token_scheme	
2	fortipam_token_query	all	fortipam_token_scheme	
3	fortipam_auth	all	fortipam_auth_scheme	

The *Schemes & Rules* tab contains the following options:

+Create New	From the dropdown, select either <i>Authentication Rule</i> or <i>Authentication Scheme</i> to create an authentication rule or authentication scheme respectively. See Creating an authentication scheme on page 172 and Creating an authentication rule on page 179 .
Edit	Select to edit the selected authentication rule or scheme.
Delete	Select to delete the selected authentication rules or schemes.
Search	Enter a search term in the search field, then hit <code>Enter</code> to search. To narrow down your search, see Column filter .
Refresh	To refresh the contents, click the refresh icon on the bottom-right.



Use the toggle on the top-right to switch between *Authentication Rules* and *Authentication Schemes*.



Changes to the authentication rule sequence applies to both proxy policies and ZTNA rules.

Creating an authentication scheme

To create an authentication scheme:

1. Go to *Authentication > Scheme & Rules*.
2. From the **+Create New** dropdown, select *Authentication Scheme*.

The *New Authentication Scheme* window opens.

New Authentication Scheme

Name

Method +

3. Enter the following information:

Name	Name of the scheme.
Method	Select + , from <i>Select Entries</i> , select one or more of the following options and then click <i>Close</i> :

<i>Basic</i>	Basic HTTP authentication.
<i>Certificate</i>	Client certificate authentication.
<i>Digest</i>	Digest HTTP authentication.
<i>Form-based</i>	Form-based HTTP authentication.
<i>Fortinet Single Sign-On (FSSO)</i>	Fortinet Single Sign-On (FSSO) authentication.
<i>Negotiate</i>	Negotiate authentication.
<i>NTLM</i>	NTLM authentication.
<i>RADIUS Single Sign-On (RSSO)</i>	RADIUS Single Sign-On (RSSO) authentication.
<i>SAML</i>	SAML authentication.
<i>SSH Public Key</i>	Public key based SSH authentication.
<i>Token Code</i>	Token code-based authentication.
<i>x-auth-user</i>	User from HTTP x-authenticated-user header.



Use the search bar to look for a method.

User database

Select +, and in *Select Entries*, select remote servers (LDAP, RADIUS, TACACS+) and user groups then click *Close*.
 You can also create a new remote servers and user groups by selecting *+Create*. See [LDAP servers on page 126](#), [RADIUS servers on page 133](#), and [User groups on page 112](#).



Use the pen icon next to a server or user group to edit it.










User database is only available when the selected methods are either one or combinations of the following:





- *Basic*
- *Digest*
- *Form-based*
- *SAML*
- *SSH Public Key*
- *x-auth-user*

FSSO guest

Enable/disable FSSO-Guest user authentication.

Note: The option is disabled by default.

	<p> FSSO guest is only available when the selected methods are either one or a combination of the following:</p> <ul style="list-style-type: none"> • <i>Basic</i> • <i>Digest</i> • <i>Negotiate</i> • <i>NTLM</i>
<p>Two-factor authentication</p>	<p>Enable/disable two-factor authentication. Note: The option is disabled by default.</p> <p> <i>Two-factor authentication</i> is only available when the selected method is <i>Form-based</i>.</p>
<p>Negotiate NTLM</p>	<p>Enable/disable negotiate authentication for NTLM. Note: The option is enabled by default.</p> <p> <i>Negotiate NTLM</i> is only available when the selected method is <i>Negotiate</i>.</p>
<p>Kerberos keytab</p>	<p>From the dropdown, select a Kerberos Keytab or create a Kerberos Keytab. See Creating a new kerberos keytab on page 175.</p> <p> Use the search bar to look for a Kerberos Keytab.</p> <p> <i>Kerberos keytab</i> is only available when the selected method is <i>Negotiate</i>.</p>
<p>Domain Controller</p>	<p>Enable/disable adding domain controllers, and from the dropdown, select a domain controller or create a domain controller. See Creating a new domain controller on page 176. Note: The option is disabled by default when the <i>Method</i> is <i>Negotiate</i>.</p> <p> Use the search bar to look for a domain controller.</p> <p> <i>Domain Controller</i> is only available when the selected method is <i>Negotiate</i> and/or <i>NTLM</i>.</p>

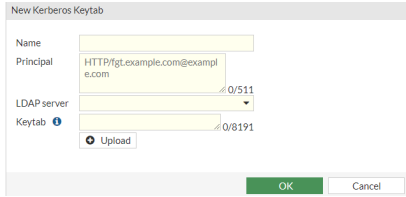
FSSO Agent	<p>Enable/disable using FSSO agent when the <i>Method</i> is <i>Negotiate</i>. From the dropdown, select an FSSO agent or create an FSSO agent. See Creating an FSSO agent on page 177.</p> <p>Note: The option is disabled by default.</p> <hr/> <div style="display: flex; align-items: center;">  <div style="margin-left: 10px;">Use the search bar to look for an FSSO agent.</div> </div> <hr/> <div style="display: flex; align-items: center;">  <div style="margin-left: 10px;"><i>FSSO Agent</i> is only available when the selected method is <i>Negotiate</i>.</div> </div> <hr/>
SAML SSO server	<p>From the dropdown, select a SAML SSO server.</p> <p>Note: The option is only available when the <i>Method</i> is <i>SAML</i>.</p> <hr/> <div style="display: flex; align-items: center;">  <div style="margin-left: 10px;">Use the search bar to look for a SAML SSO server.</div> </div> <hr/>
User database	<p>From the dropdown, select a user database server or create a user database server.</p>
Timeout	<p>SAML authentication timeout in seconds.</p> <p>Note: The option is only available when the <i>Method</i> is <i>SAML</i>.</p>
SAML Timeout	<p>Enter the SAML authentication timeout, in seconds (default = 120).</p> <p>Note: The option is only available when the <i>Method</i> is <i>SAML</i>.</p>
SSH local CA	<p>From the dropdown, select an SSH local CA.</p> <p>Note: The option is only available when the method is <i>SSH Public Key</i>.</p> <hr/> <div style="display: flex; align-items: center;">  <div style="margin-left: 10px;">Use the dropdown to look for an SSH local CA.</div> </div> <hr/>

4. Click **OK**.



Creating a new kerberos keytab

To create a new kerberos keytab:

- In step 3 when [Creating an authentication scheme on page 172](#) where the selected method is *Negotiate*, from the *Kerberos keytab* dropdown, select **+Create**.
The *New Kerberos Keytab* window opens:



2. Enter the following information:

Name	Name of the kerberos keytab.
Principal	Enter the unique identity that Kerberos uses to assign tickets to. Note: Use / to separate components of the principal.
LDAP server	From the dropdown, select an LDAP server or create an LDAP server. See LDAP servers on page 126 .
	 Use the search bar to look for an LDAP server.
	 Use the pen icon next to an LDAP server to edit it.
Keytab	Enter the pre-shared key, and select <i>Upload</i> to locate the Base64 coded keytab file on your local computer.



3. Click *OK*.

Creating a new domain controller

To create a domain controller:

1. In step 3 when [Creating an authentication scheme on page 172](#) where the selected method is *Negotiate* or *NTLM*, from the *Domain Controller* dropdown, select *+Create*.
If the *Method* is set as *Negotiate*, enable *Domain Controller*.

2. Enter the following information:

Name	Name of the domain controller.
IP Address	The IP address of the domain controller.
Port	The port number for the port to be used to communicate with the domain controller (default = 445).
LDAP server	<p>From the dropdown, select an LDAP server or create an LDAP server. See LDAP servers on page 126.</p> <hr/> <div style="display: flex; align-items: center;">  <p>Use the search bar to look for an LDAP server.</p> </div> <hr/> <div style="display: flex; align-items: center;">  <p>Use the pen icon next to an LDAP server to edit it.</p> </div> <hr/>
Domain Name	DNS name of the domain.



3. Click *OK*.

Creating an FSSO agent

To create an FSSO agent:

1. In step 3 when [Creating an authentication scheme on page 172](#) where the selected method is *Negotiate*, enable *FSSO Agent*.
2. From the *FSSO Agent* dropdown, select *+Create*.
The *New External Connector* window opens.
3. Select *FSSO Agent on Windows AD*.

4. In the *Connector Settings* pane, enter the following information:

Name	Name of the FSSO agent.
Primary FSSO agent	The FSSO agent server IP address or name and <i>Password</i> . Select + to add additional FSSO agents.
Trusted SSL certificate	Enable/disable using a trusted SSL certificate. From the dropdown, select a certificate or import a certificate. Note: The option is disabled by default. To import a certificate: <ol style="list-style-type: none"> 1. From the dropdown, select <i>Import</i>. 2. In <i>Upload</i>, select <i>+Upload</i>, and locate the certificate on your local computer. 3. Click <i>OK</i>.
User group source	Select either <i>Collector Agent</i> or <i>Local</i> : <ul style="list-style-type: none"> • <i>Collector Agent</i>: User groups are pushed to the FortiPAM from the collector agent. • <i>Local</i>: User groups are specified in the FortiGate configuration.
LDAP server	From the dropdown, select an LDAP server or create an LDAP server. See LDAP servers on page 126 . Note: The option is only available when the <i>User group source</i> is <i>Local</i> . <hr/>  Use the search bar to look for an LDAP server. <hr/>  Use the pen icon next to an LDAP server to edit it. <hr/>
Proactively retrieve from LDAP server	Enable to configure the search filter and <i>Interval (in minutes)</i> . Note: The option is only available when the <i>User group source</i> is <i>Local</i> , and is disabled by default.
Users/Groups	Click <i>Apply and Refresh</i> to fetch group filters from the collector agent. Note: The option is only available when the <i>User group source</i> is <i>Collector Agent</i> .

5. Click *OK*.

Creating an authentication rule







To create an authentication rule:

1. Go to *Authentication > Scheme & Rules*.
2. From the *+Create New* dropdown, select *Authentication Rule*.
The *Add New Rule* window opens.

The screenshot shows the 'Add New Rule' dialog box. It contains the following fields and controls:

- Name:** A text input field.
- Source Interface:** A dropdown menu.
- Source Address:** A text input field with a plus sign icon.
- Authentication Scheme:** A radio button.
- Comments:** A text input field with the placeholder 'Write a comment...' and a character count of '0/1023'.
- Enable This Rule:** Two radio buttons, 'Enable' (selected) and 'Disable'.
- Buttons:** 'OK' and 'Cancel' buttons at the bottom.

3. Enter the following information:

Name	The name of the authentication rule.
Source Interface	From the dropdown, select a source interface or create an interface.
	 Use the search bar to look for a source interface.
	 Use the pen icon next to a source interface to edit the interface.
Source Address	Select +, and from <i>Select Entries</i> , select source addresses, <i>all</i> or <i>none</i> . You can also create a new source address.
	 Use the search bar to look for a source address.
	 Use the pen icon next to a source address to edit the source address.
Authentication Scheme	Enable <i>Authentication Scheme</i> to use an authentication scheme and then from the dropdown, select which authentication scheme to use. You can also create a new authentication scheme. See Creating an authentication scheme on page 172 .
	 Use the search bar to look for an authentication scheme.
	 Use the pen icon next to an authentication scheme to edit the authentication scheme.
	Note: The option is disabled by default.
Comments	Optionally, enter comments about the authentication rule.
Enable This Rule	Select <i>Enable</i> or <i>Disable</i> to control whether the authentication rule is used or ignored.
	Note: The option is enabled by default.

4. Click *OK*.

System

Go to *System* to manage and configure the basic system options for FortiPAM.

You can also manage and update the firmware for FortiPAM, set up SNMP, HA cluster, manage certificates, configure ZTNA related settings, and automated backup.

System contains the following tabs:

- [Firmware on page 181](#)
- [Settings on page 181](#)
- [SNMP on page 185](#)
- [High availability on page 193](#)
- [Certificates on page 201](#)
- [ZTNA on page 210](#)
- [Backup on page 225](#)

Firmware

The FortiPAM firmware can be upgraded from *System > Firmware*.

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.

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 *System Settings* window opens.

2. In *System Settings*, enter the following information:

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: <ul style="list-style-type: none"> • <i>NTP</i>: The NTP (Network Time Protocol) server (default). • <i>Manual Settings</i>
-----------------	--

Select Server	Select a server from the following two options: <ul style="list-style-type: none"> • <i>FortiGuard</i> (default) • <i>Custom</i>
----------------------	--

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 <i>Set Time</i> is <i>NTP</i> .
Date	Enter the date or select the calendar icon, and from the dropdown, select a date. Note: The option is only available when <i>Set Time</i> is <i>Manual Settings</i> .
Time	Enter the time or select the clock icon, and from the dropdown, select a time. Note: The option is only available when <i>Set Time</i> is <i>Manual Settings</i> .
Setup device as local NTP server	Select <i>True</i> to configure the FortiPAM as a local NTP server (default = <i>False</i>).
Listen on Interfaces	Set the interface or interfaces that the FortiPAM will listen for NTP requests on. Note: The option is only available when <i>Setup device on local NTP server</i> is set as <i>True</i> .

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****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`.

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 269](#).

Debug Logs pane**Debug Logs****Debug Logs**

Select *Download* to export the debug logs to your computer as a text file.

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 = 95, 10 - 100).

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).
	 <p>Enable the toggle or enter 0 for no time limit.</p>
	Note: The option is only available when the <i>Video Storage Mode</i> is <i>Rolling</i> .
Recording Resolution	From the dropdown, select a resolution for the PAM video recordings: <ul style="list-style-type: none"> • 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 (default = 16 Bit Color Depth): <ul style="list-style-type: none"> • 16 Bit Color Depth • 24 Bit Color Depth • 64 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)
Client Port	Enter the port number that FortiPAM uses to connect to FortiClient (default = 9191, 1 - 65536).

3. Click *Apply*.

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 188](#) 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.

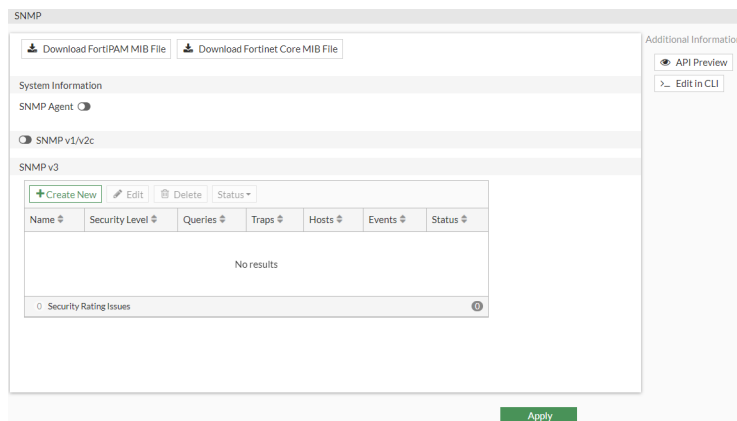


For security reasons, Fortinet recommends that neither “public” nor “private” be used for SNMP community names.



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 188 .
System Information	
SNMP Agent	Enable the FortiPAM SNMP agent. See SNMP agent on page 189 .
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 <i>Create New</i> , the <i>New SNMP Community</i> page opens. See Creating or editing an SNMP community on page 189 .
Edit	Modifies settings within an SNMP community. When you click <i>Edit</i> , the <i>Edit SNMP Community</i> 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 <code>Ctrl</code> or <code>Shift</code> keys and then select <i>Delete</i> .
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 <i>Create New</i> , the <i>Create New SNMP User</i> page opens. See Creating or editing an SNMP user on page 191 .
Edit	Modifies settings within the SNMP v3 user. When you click <i>Edit</i> , the <i>Edit SNMP User</i> 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 <code>Ctrl</code> or <code>Shift</code> keys and then select <i>Delete</i> .
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 185](#).

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.
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: <i>Accept queries and send traps</i> , <i>Accept queries only</i> , or <i>Send traps only</i> .
X	Removes an SNMP manager from the list within the <i>Hosts</i> 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.

The screenshot shows the 'New SNMP User' configuration window. It contains the following sections:

- User Name:** A text input field.
- Enabled:** A radio button set with 'Enabled' selected.
- Security Level:** Two radio buttons: 'No Authentication' (selected) and 'Authentication'.
- Hosts:** A section with 'IP Address' and a port number input field, both with dropdown menus.
- Queries:** A section with 'Enabled' (radio button, selected) and 'Port' (input field, value 161).
- Traps:** A section with 'Enabled' (radio button, selected), 'Local Port' (input field, value 162), and 'Remote Port' (input field, value 162).
- SNMP Events:** A list of events with checkboxes:
 - CPU usage too high
 - Available memory is low
 - Available log space is low
 - Interface IP address changed
 - HA cluster status change
 - HA heartbeat interface failure
 - AV detected virus
 - HA cluster member up
 - HA cluster member down
 - Entity config change (RFC4120)
 - Disconnected from FortiAnalyzer
 - Per-CPU usage is high

At the bottom, there are 'OK' and 'Cancel' buttons.

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:	
<ul style="list-style-type: none"> • <i>No Authentication</i> • <i>Authentication and No Private</i>—Select the authentication algorithm and enter password to use. • <i>Authentication and Private</i>—Select the authentication and encryption algorithm and enter the passwords to use. 	
Authentication/Encryption Algorithm	<p>If the security level is set to <i>Authentication and No Private</i>, you can select from the following authentication algorithms:</p> <ul style="list-style-type: none"> • <i>MD5</i> • <i>SHA1</i> (default) • <i>SHA224</i> • <i>SHA256</i> • <i>SHA384</i> • <i>SHA512</i> <p>If the security level is set to <i>Authentication and Private</i>, you can also select from the following encryption algorithms in addition to authentication algorithms:</p> <ul style="list-style-type: none"> • <i>AES</i> (default) • <i>DES</i> • <i>AES256</i> • <i>AES256 Cisco</i>
Password	If the security level is set to <i>Authentication</i> , select <i>Change</i> and enter a password in the <i>Password</i> 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 <i>Port</i> 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.

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 two FortiPAM devices in the Active-Passive mode for failover protection.

The following shows FortiPAM devices in Active-Passive mode:

Status	Priority	Hostname	Serial No.	Role	System Uptime	Sessions	Throughput
Synchronized	129	FPXVM20220211006	FPXVM20220211006	Primary	4d 23h	0	4.55 Mbps
Synchronized	128	FPAVM20221206010	FPAVM20221206010	Secondary	4d 22h	0	19.00 kbps

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 <i>Standalone</i> or <i>Active-Passive</i> .
	 <p>If you select <i>Standalone</i>, no other options are displayed.</p>
Device priority	<p>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).</p>
	 <p>Since all videos and logs are only stored on the primary device, one FortiPAM should be configured with higher priority.</p> <p>And with override enabled, the primary unit with the highest device priority will always become the primary unit.</p>
	 <p>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.</p>
Cluster Settings	
Group name	Enter a name to identify the cluster.
Password	<p>Select <i>Change</i> 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. When the cluster is operating, you can add a password, if required.</p>
	 <p>Two clusters on the same network must have different passwords.</p>
Monitor interfaces	Select the specific ports to monitor or create new interfaces.
	 <p>Use the search bar to look for an interface.</p>



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 <i>Mode</i> is <i>Active-Passive</i> .	
	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 <i>Unicast Heartbeat</i> 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**.

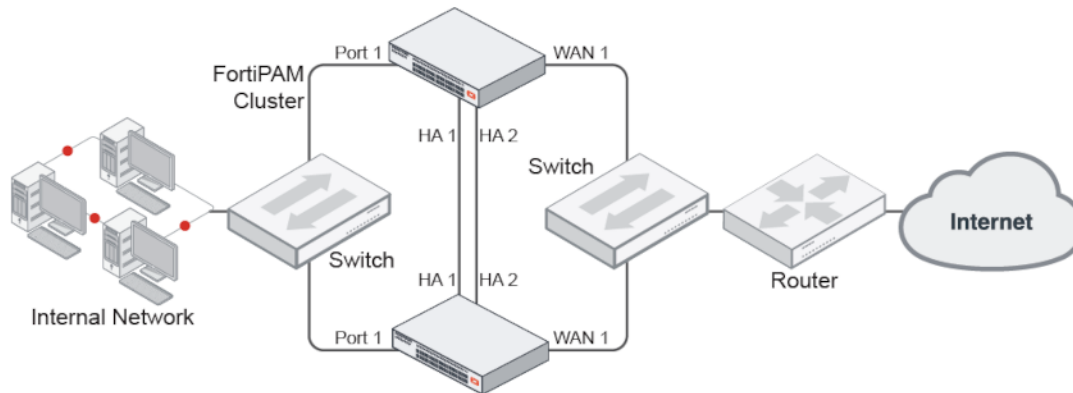
HA failover

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	<i>Active-Passive.</i>
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.

Name	Subject	Comments	Issuer	Expires	Status	Source
Local CA Certificate						
Fortinet_CA_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...	This is the default CA certificate the SSL Inspection will use when genera...	Fortinet	2022/08/30 11:02:36	Valid	Factory
Fortinet_CA_Untrusted	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...	This is the default CA certificate the SSL Inspection will use when genera...	Fortinet	2022/07/05 17:03:49	Valid	Factory
Local Certificate						
Fortinet_Factory	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiProxy, CN = ...	This certificate is embedded in the hardware at the factory and is unique ...	Fortinet	2056/01/18 19:14:07	Valid	Factory
Fortinet_Factory_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiProxy, CN = ...	This certificate is embedded in the hardware at the factory and is unique ...	Fortinet	2038/01/18 19:14:07	Valid	Factory
Fortinet_SSL	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = ...	This certificate is embedded in the hardware at the factory and is unique ...	Fortinet	2024/12/02 10:02:36	Valid	Factory
Fortinet_SSL_DSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = ...	This certificate is embedded in the hardware at the factory and is unique ...	Fortinet	2024/12/02 10:02:38	Valid	Factory
Fortinet_SSL_DSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = ...	This certificate is embedded in the hardware at the factory and is unique ...	Fortinet	2024/12/02 10:02:38	Valid	Factory
Fortinet_SSL_ECDSA256	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = ...	This certificate is embedded in the hardware at the factory and is unique ...	Fortinet	2024/12/02 10:02:38	Valid	Factory
Fortinet_SSL_ECDSA384	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = ...	This certificate is embedded in the hardware at the factory and is unique ...	Fortinet	2024/12/02 10:02:38	Valid	Factory
Fortinet_SSL_ECDSA512	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = ...	This certificate is embedded in the hardware at the factory and is unique ...	Fortinet	2024/12/02 10:02:38	Valid	Factory
Fortinet_SSL_ED448	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = ...	This certificate is embedded in the hardware at the factory and is unique ...	Fortinet	2024/12/02 10:02:38	Valid	Factory
Fortinet_SSL_ED25519	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = ...	This certificate is embedded in the hardware at the factory and is unique ...	Fortinet	2024/12/02 10:02:38	Valid	Factory
Fortinet_SSL_RSA1024	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = ...	This certificate is embedded in the hardware at the factory and is unique ...	Fortinet	2024/12/02 10:02:36	Valid	Factory
Fortinet_SSL_RSA2048	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = ...	This certificate is embedded in the hardware at the factory and is unique ...	Fortinet	2024/12/02 10:02:36	Valid	Factory
Fortinet_SSL_RSA4096	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiGate, CN = ...	This certificate is embedded in the hardware at the factory and is unique ...	Fortinet	2024/12/02 10:02:38	Valid	Factory
Fortinet_WiFi	C = US, ST = California, L = Sunnyvale, O = Fortinet, Inc.; CN = auth-cert...	This certificate is embedded in the firmware and is the same on every uni...	DigiCert Inc	2021/12/25 15:59:59	Expired	Factory
Remote CA Certificate						
Fortinet_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...		Fortinet	2056/05/27 13:27:39	Valid	Factory
Fortinet_CA_Backup	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...		Fortinet	2038/01/19 14:34:39	Valid	Factory
Fortinet_Sub_CA	C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate Aut...		Fortinet	2056/05/27 13:48:33	Valid	Factory
Fortinet_WiFi_CA	C = US, O = DigiCert Inc, CN = DigiCert TLS RSA SHA256 2020 CA1		DigiCert Inc	2030/09/23 16:59:59	Valid	Factory

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 202](#)

- [Generating a CSR \(Certificate Signing Request\) on page 205](#)
- [Importing CA certificate on page 207](#)
- [Uploading a remote certificate on page 208](#)
- [Importing a CRL \(Certificate revocation list\) on page 208](#)

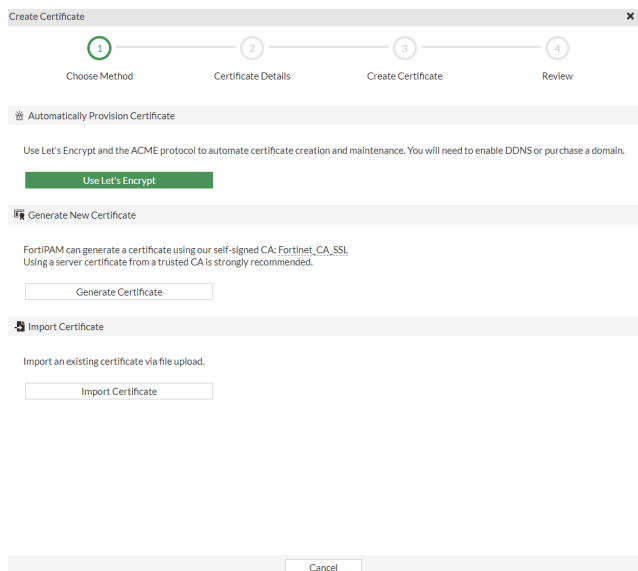
Edit	Select to edit the selected certificate.
Delete	Select to delete the selected certificates.
View Details	Select to see details about the selected certificate.
Download	Select to download the selected certificate.
Search	Use the search bar to look for a certificate.

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.

	<p>Note: The option is only available when the <i>Chosen Method</i> is <i>Generate New Certificate</i>.</p>
Common name	<p>The common name of the certificate. Enter an FQDN or an IPv4 address.</p> <hr/> <div style="display: flex; align-items: center;">  <p>The common name should match the FQDN or the IP address of the primary SSL-VPN interface.</p> </div> <hr/> <p>Note: The option is only available when the <i>Chosen Method</i> is <i>Generate New Certificate</i>.</p>
Subject alternative name	<p>An IP address or FQDN.</p> <p>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.</p> <p>Note: The option is only available when the <i>Chosen Method</i> is <i>Generate New Certificate</i>.</p>
Update Your List of Trusted Certificate Authorities	<p>Select <i>Download CA Certificate</i> to download <code>Fortinet_CA_SSL</code> CA to your computer.</p> <hr/> <div style="display: flex; align-items: center;">  <p><code>Fortinet_CA_SSL</code> is a local CA certificate. To avoid certificate warnings, you must download it and install it on each client machine.</p> </div> <hr/> <p>Note: The option is only available when the <i>Chosen Method</i> is <i>Generate New Certificate</i>.</p>
Import Certificate	
Type	<p>Select from the following three options:</p> <ul style="list-style-type: none"> • <i>Local Certificate</i> • <i>PKCS #12 Certificate</i> • <i>Certificate</i> <p>Note: The option is only available when the <i>Chosen Method</i> is <i>Import Certificate</i>.</p>
Certificate file	<p>Select <i>+Upload</i> and locate the certificate file on your local computer.</p> <p>Note: The option is only available when the <i>Chosen Method</i> is <i>Import Certificate</i> and the <i>Type</i> is either <i>Local Certificate</i> or <i>Certificate</i>.</p>
Certificate with key file	<p>Select <i>+Upload</i> and locate the certificate with key file on your local computer.</p> <p>Note: The option is only available when the <i>Chosen Method</i> is <i>Import Certificate</i> and the <i>Type</i> is <i>PKCS #12 Certificate</i>.</p>
Password	<p>Enter the password.</p> <p>Note: The option is only available when the <i>Chosen Method</i> is <i>Import Certificate</i> and the <i>Type</i> is either <i>PKCS #12 Certificate</i> or <i>Certificate</i>.</p>
Confirm Password	<p>Reenter the password to confirm.</p>

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.
	 <p>Do not include spaces in the certificate to ensure compatibility as a PKCS12 file.</p>
Subject Information	
ID Type	<p>Select the ID type:</p> <ul style="list-style-type: none"> • <i>Host IP</i>: Select if the unit has a static IP address. Enter the device IP address in the <i>IP</i> field (default). • <i>Domain Name</i>: Enter the device domain name or FQDN in the <i>Domain Name</i> field. • <i>E-mail</i>: Enter the email address of the device administrator in the <i>E-mail</i> field.
Optional Information	Optional information to further identify the device.
Organizational Unit	The name of the department.
	 <p>Up to 5 OUs can be added.</p>
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.
	 <p>The option is disabled by default.</p>
E-mail	The contact email address.
Subject Alternative Name	<p>One or more alternative names, separated by commas, for which the certificate is also valid.</p> <p>An alternative name can be: email address, IP address, URI, DNS name, or a directory name.</p> <p>Each name must be preceded by its type, for example: IP:1.2.3.4, or URL: http://your.url.here/.</p>
Password for private key	The password for the private key.

Key Type	Select <i>RSA</i> or <i>Elliptic Curve</i> . Note: The default is <i>RSA</i> .
Key Size	If you selected <i>RSA</i> for the <i>Key Type</i> , select the <i>Key size</i> : <i>1024 Bit</i> , <i>1536 Bit</i> , <i>2048 Bit</i> (default), or <i>4096 Bit</i> .
	 <p>Larger key sizes are more secure but slower to generate.</p>
	If you selected <i>Elliptic Curve</i> for the <i>Key Type</i> , select the <i>Curve Name</i> : <i>secp256r1</i> (default), <i>secp384r1</i> , or <i>secp521r1</i> .
Enrollment Method	Select the enrollment method. <ul style="list-style-type: none"> • <i>File Based</i>: Generate the certificate request (default). • <i>Online SCEP</i>: 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*.

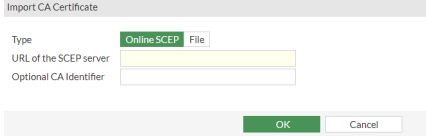
Importing CA certificate

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.



- Enter the following information:

Type	Select either <i>Online SCEP</i> or <i>File</i> .
URL of the SCEP server	The URL of the SCEP server. Note: The option is only available when the <i>Type</i> is <i>Online SCEP</i> .
Optional CA Identifier	Optionally, enter the CA identifier. Note: The option is only available when the <i>Type</i> is <i>Online SCEP</i> .
+Upload	Select and locate the certificate file on your computer. Note: The option is only available when the <i>Type</i> is <i>File</i> .

- 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:

- Go to *System > Certificates*.
- From **+Create/Import**, select *Remote Certificate*.
The *Upload Remote Certificate* window opens.



- Select **+Upload** and locate the certificate file on your computer.
- Click **OK**.

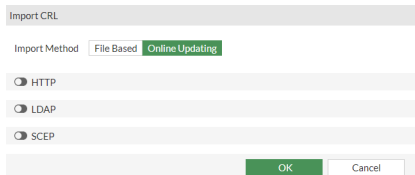
Importing a CRL (Certificate revocation list)

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:

- Go *System > Certificates*.
- 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*.

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 ZTNA rules, ZTNA servers, and ZTNA tags.

The *ZTNA* tab looks like the following:

Name	From	Source	ZTNA Tag	ZTNA Server	Action	Security Profiles	Log	Bytes
FortiPAM_Default	any	all SSO_Guest_Users		fortipam_access_proxy	ACCEPT	deep-inspection	UTM	2.98 MB

The following options are available in all the *ZTNA* tabs:

+Create New	Select to create a ZTNA rule, ZTNA server, or a ZTNA tag depending on the tab you are in. See: <ul style="list-style-type: none"> • Creating a ZTNA rule on page 210 • Creating a ZTNA server on page 214 • Creating a ZTNA tag group on page 219
Edit	Select to edit the selected ZTNA rule, ZTNA server, or a ZTNA tag.
Delete	Select to delete the selected ZTNA rules, ZTNA server, and ZTNA tags.
Search	Use the search bar to look for a ZTNA rule, ZTNA server, or a ZTNA tag.
	 <p>To narrow down your search in the <i>ZTNA Servers</i> and the <i>ZTNA Tags</i> tabs, see Column filter.</p>
Export	From the dropdown, select to export the list of ZTNA 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.

Creating a ZTNA rule

A ZTNA rule is a proxy policy used to enforce access control. ZTNA tags or tag groups can be defined to enforce zero trust role based access. Security profiles can be configured to protect this traffic.

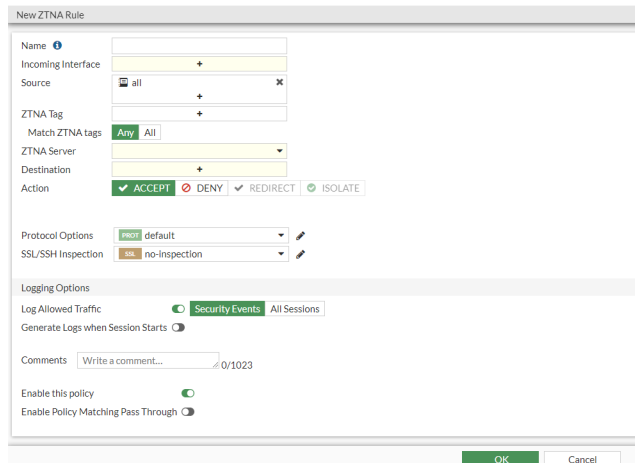


A default *FortiPAM_Default* ZTNA rule is available in the ZTNA rules list.





To configure a ZTNA rule:







1. Go to *System > ZTNA* and select the *ZTNA Rules* tab.
2. Select *+Create New*.





The *New ZTNA Rule* window opens.



3. Enter the following information:

Name	<p>The name of the ZTNA rule.</p> <hr/>  <p>Names are not fixed and can be changed later.</p>
Incoming Interface	<p>Select incoming interfaces or create new interfaces.</p> <hr/>  <p>Use the search bar to look for an interface.</p> <hr/>  <p>Use the pen icon next to the interface to edit it.</p>
Source	<p>Select sources or create new sources (default = all). You can select or create the following types of sources:</p> <ul style="list-style-type: none"> • <i>Address</i> • <i>Address Group</i> • <i>User</i> • <i>User Group</i> <hr/>  <p>Use the search bar to look for a source.</p>

	 <p>Use the pen icon next to the source to edit it.</p>
ZTNA Tag	<p>Add the ZTNA tags or tag groups that are allowed access. ZTNA tags are synchronized from the EMS side.</p>
	 <p>Use the search bar to look for a ZTNA tag.</p>
<p>Creating a ZTNA tag group on page 219</p>	
Match ZTNA tags	<p>If multiple tags are included, select <i>Any</i> or <i>All</i> (default = <i>Any</i>).</p>
ZTNA Server	<p>From the dropdown, select a ZTNA server or create a ZTNA server.</p>
	 <p>Use the search bar to look for a ZTNA server.</p>
	 <p>Use the pen icon next to the server to edit it.</p>
<p>See Creating a ZTNA server on page 214.</p>	
Destination	<p>Select or create a destination.</p> <p>You can select or create the following types of destinations:</p> <ul style="list-style-type: none">• <i>Address</i>• <i>Address Group</i>• <i>User</i>• <i>User Group</i>
	 <p>Use the search bar to look for a destination.</p>
	 <p>Use the pen icon next to a destination to edit it.</p>
Action	<p>Select from the following four actions to execute:</p> <ul style="list-style-type: none">• <i>ACCEPT</i> (default)• <i>DENY</i>
Protocol Options	<p>From the dropdown, select a protocol or create a new protocol.</p>

	 <p>The default protocol is ready only.</p>
	 <p>Use the search bar to look for a protocol.</p>
	<p>Note: The option is only available when <i>Action</i> is set as <i>Accept</i>.</p>
SSL/SSH Inspection	<p>From the dropdown, select an SSL/SSH inspection profile (default = no-inspection).</p>
	 <p>Use the search bar to look for an SSL/SSH inspection profile.</p>
	 <p>Use the pen icon next to the SSL/SSH inspection profile to edit it.</p>
	<p>Note: The option is only available when <i>Action</i> is set as <i>Accept</i>.</p>
Logging Options	
Log Allowed Traffic	<p>Enable to record any log messages about the accepted traffic.</p> <p>Select from the following two options:</p> <ul style="list-style-type: none"> • <i>Security Events</i>: Record only log messages related to security events caused by the accepted traffic (default). • <i>All Sessions</i>: Record all log messages related to all of the accepted traffic. <p>Note: The option is enabled by default.</p> <p>Note: The option is only available when <i>Action</i> is set as <i>Accept</i>.</p>
Generate Logs when Session Starts	<p>Enable to generate logs when the session starts.</p> <p>Note: The option is disabled by default.</p> <p>Note: The option is only available when <i>Log Allowed Traffic</i> is enabled.</p>
Comments	<p>Optionally, enter comments about the ZTNA rule.</p>
Enable this policy	<p>Select to enable the policy.</p> <p>Note: The option is enabled by default.</p>
Enable Policy Matching Pass Through	<p>Enable to make the policy a pass-through policy.</p> <p>When traffic matches a pass-through policy, the firewall continues to the next policy. After FortiPAM tries to match all policies, it will set the last matched passthrough policy as the matched policy.</p> <p>Note: The option is disabled by default.</p>

4. Click *OK*.

Creating a ZTNA server



It is not suggested to create a new ZTNA server on GUI.

To configure a ZTNA server, define the access proxy VIP and the real servers that clients will connect to. The access proxy VIP is the FortiPAM ZTNA gateway that clients make HTTPS connections to. The service/server mappings define the virtual host matching rules and the real server mappings of the HTTPS requests.

To configure a ZTNA server:

1. Go to *System* > *ZTNA* and select the *ZTNA Servers* tab.
2. Select *+Create New*.

The *New ZTNA Server* window opens.

Interim build0012 > > > Theme > admin >

New ZTNA Server

Type **IPv4**

Name

Comments

Client Certificate **Disable** Enable

Network

External Interface

External IP 0.0.0.0

External port 443

SAML

Services and Servers





Default certificate

Service/server mapping

Service	URL	# Real Servers
No results		

OK Cancel

3. Enter the following information:

Type	IPv4 address type used to access the ZTNA server. Note: The option is non-editable.
Name	The name of the server.
Comments	Optionally, enter comments about the server.
Client Certificate	Enable/disable client certificate. Note: The option is disabled by default.
Network	
External interface	From the dropdown, select an external interface or create a new interface. <hr/>  Use the search bar to look for an interface. <hr/>  Use the pen icon next to the interface to edit it. <hr/> Note: The option is only available when the <i>Type</i> is <i>IPv4</i> .
External IP	The external IP address.
External port	The external port number the clients will connect to (default = 443).
SAML	
Note: The option is disabled by default.	
SAML SSO server	From the dropdown, select a SAML SSO server. <hr/>  Use the search bar to look for a SAML SSO server. <hr/> Note: The option is only available when <i>SAML</i> is enabled.
Services and Servers	
Default certificate	From the dropdown, select or create a default certificate. Clients will be presented with this certificate when they connect to the access proxy VIP. <hr/>  Use the search bar to look for a default certificate. <hr/>

Service/servermapping

Select **+Create New** to create a new service/server mapping. See [Creating a service/server mapping on page 216](#).



To edit or delete a service/server mapping, select a service/server mapping and then select *Edit* or *Delete*.

4. Click **OK**.

Creating a service/server mapping

To create a service/server mapping:

1. In step 3 when [Creating a ZTNA server on page 214](#), select **+Create New** in Service/server mapping. The *New Service/Server Mapping* window opens.

New Service/Server Mapping

Type **IPv4**

Service **HTTP** **HTTPS** TCP Forwarding

Virtual Host **Any Host** Specify

Match path by **Substring** Wildcard Regular Expression

Path

Servers



Load balancing **ON**

+ Create New Edit Delete

Address	Port	Status
No results		

OK Cancel

2. Enter the following information:

Type	IPv4 is the IP address type. Note: The option is non-editable.
Service	Select from the following three services: <ul style="list-style-type: none"> • <i>HTTP</i> • <i>HTTPS</i> (default) • <i>TCP Forwarding</i>
Virtual Host	Select from the following two options: <ul style="list-style-type: none"> • <i>Any Host</i> : Any request that resolves to the access proxy VIP will be mapped to your real servers. For example, if both <code>www.example1.com</code> and <code>www.example2.com</code> resolve to the VIP, then both requests are mapped to your real servers. • <i>Specify</i>: Enter the name or IP address of the host that the request must match in <i>Host</i>. For example, if <code>www.example1.com</code> is entered as the host, then only requests to <code>www.example1.com</code> will match. Note: The option is not available when the <i>Service</i> is set as <i>TCP Forwarding</i> .
Match by	Select either <i>Substring</i> or <i>Wildcard</i> based match. Note: The option is only available when the <i>Virtual Host</i> is <i>Specify</i> .
Use certificate	From the dropdown, select a certificate or create a new certificate. <hr/>  Use the search bar to look for a certificate. <hr/> Note: The option is only available when the <i>Virtual Host</i> is <i>Specify</i> .
Match path by	The path can be matched by one of the following three options: <ul style="list-style-type: none"> • <i>Substring</i> • <i>Wildcard</i> • <i>Regular Expression</i> Note: The option is not available when the <i>Service</i> is set as <i>TCP Forwarding</i> .
Path	The path. For example, if the virtual host is specified as <code>www.example1.com</code> , and the path substring is <code>map1</code> , then <code>www.example1/map1</code> will be matched. Note: The option is not available when the <i>Service</i> is set as <i>TCP Forwarding</i> .
Servers	Select <i>+Create New</i> to create a new server. See Creating a server on page 218 . <hr/>  To edit or delete a server, select a server and then click <i>Edit</i> or <i>Delete</i> . <hr/>

Load balancing

Enable and select one of the following load balancing methods:

- *Round Robin*: Distribute to server based round robin order.
- *Weighted*: Distribute to server based on weight.
- *First Alive*: Distribute to the first server that is alive.
- *HTTP Host*: Distribute to server based on the host field in the HTTP header.



The option is only effective when there are multiple servers.

Note: The option disabled by default.

Note: The option is not available when the *Service* is set as *TCP Forwarding*.

3. Click *OK*.

Creating a server

To create a server:

1. In step 2 when [Creating a service/server mapping on page 216](#), select *+Create New*. The *New Server* window opens.

2. In *Type*, select either *IP* or *FQDN*.
3. If the *Type* is *IP*, in *IP*, enter the server IP address.
If the *Type* is set as *FQDN*, from the *Address* dropdown, select an address or create an address.



Use the search bar to look for an address.



Use the pen icon next to the address to edit the address.

4. In *Port*, enter the server port number (default = 443, 1 - 65535).
5. In *Status*, set the status of the server from the following three options:
 - *Active* (default)
 - *Standby*
 - *Disable*
6. Click *OK*.

Creating a ZTNA tag group

After FortiPAM connects to the FortiClient EMS, it automatically synchronizes ZTNA 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 EMS 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 set up EMS in the GUI:

1. Go to *Security Fabric > 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 252](#).



For clients not connected to the same EMS as FortiPAM, configure another access proxy with a different VIP and client certificate disabled to launch secrets without device control successfully.

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

On an EMS server, you can create Zero Trust tagging rules for endpoints 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 firewall policy to control which endpoint has access. See [ZTNA tag control example on page 221](#).

ZTNA tag control - example

To add a ZTNA tag control:

1. Go to *System > ZTNA* and select the *ZTNA Servers* tab.
2. Select the default *fortipam_access_proxy* server and click *Edit*.
3. In *Client Certificate*, select *Enable*.
4. Click *OK*.
After enabling *Client Certificate*, you are required to log in again.
5. In the certificate check pop-up that appears, click *OK*.
6. Log in to FortiPAM.
7. Go to *System > ZTNA* and select the *ZTNA Rules* tab.
8. Select the default *FortiPAM_Default* rule and click *Edit*.
9. In *ZTNA Tag*, add the ZTNA tags or tag groups that are allowed access.
You can choose whether to match all the tags or any by selecting *All* or *Any* for *Match ZTNA tags*.
Only endpoints with the added tags can access FortiPAM.
10. Click *OK*.
On the *ZTNA Tags* tab, you can find all the ZTNA tags from EMS server and create ZTNA tag group.
See [Creating a ZTNA tag group on page 219](#).

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 <---
  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" <---
        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 ZTNA servers and ZTNA rules to achieve it.



GUI only supports basic ZTNA configuration. It is recommended to use CLI to configure additional ZTNA rules (`config firewall policy`) and ZTNA servers (`config firewall access-proxy`).

CLI configuration for a user from endpoint installed with FortiClient - 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. Also, you can set it up to allow access within a certain schedule only.

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

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.


The screenshot shows the 'Edit Automated backup' configuration interface. Key settings include:

- Status:** Enabled (indicated by a green checkmark).
- Backup Type:** Time based trigger (selected over Change based trigger).
- Interval:** 60 Minutes (range 60 - 4294967295).
- Server Type:** HTTPS server (selected over FTP, SFTP, and HTTP).
- Encrypt File:** Disabled (indicated by a red 'X').
- Server Address:** 127.0.0.1
- Server Path:** /backup_test
- Identifier Name:** files
- Username:** toto
- Password:** Encrypted Value
- Filename:** /././././SID.conf
- Limit ID:** Disabled
- Last backup version:** 31453
- Last updated time:** 2022-11-18 16:38:08

 An 'Apply' button is located at the bottom right of the configuration area.

2. Enter the following information:

<p>Status</p>	<p>Enable or disable automatic backup. Note: The option is enabled by default.</p>
<p>Backup Type</p>	<p>Select from the following two options:</p> <ul style="list-style-type: none"> • <i>Time based trigger</i>: FortiPAM sends the backup configuration to the server every <i>Interval</i> minutes. • <i>Change based trigger</i>: FortiPAM checks the configuration every <i>Interval</i> minutes and if the configuration has changed, FortiPAM sends it to the server (default).
<p>Interval</p>	<p>The time interval required in backup, in minutes (default = 60, 60 - 4294967295).</p>
<p>Server Type</p>	<p>Select from the following server types:</p> <ul style="list-style-type: none"> • <i>FTP server</i> • <i>SFTP server</i> • <i>HTTP server</i> • <i>HTTPS server</i> (default)
<div style="display: flex; align-items: center; justify-content: center;">  <p>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.</p> </div>	
<p>Encrypt File</p>	<p>Enable and enter cipher key to encrypt the backup file.</p>
<div style="display: flex; align-items: center; justify-content: center;">  <p>The administrator must enter the same cipher key when restoring the configuration to FortiPAM.</p> </div>	
<p>Note: The option is disabled by default.</p>	

Server Address	The IP address of the server.
Server Path	The path to store the backup file in the server.
Identifier Name	The variable name that server uses to identify the file. Note: Only required for <i>HTTP/HTTPS</i> server type.
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*.

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 server-copyname <string>
  set server-user <string>
  set server-pass <passwd>
  set filename-pattern {$SN $YYYY $MM $DD $hh $mm $ss $ID}
  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: <ul style="list-style-type: none"> time-based: Time based trigger. change-based: Change based trigger (default).
server-type {ftp sftp http https}	Set the server type: <ul style="list-style-type: none"> ftp sftp http https (default)
server-address <string>	Enter the address of file server.
server-path <path>	Enter the path of file server (default = /).
server-copyname <string>	Enter the copy name of the file (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.
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 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 file-field-name "file"
  set server-user "http_user"
  set server-pass QA@fortinet
  set filename-pattern "$SN-$ID.conf"
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.

The screenshot displays the 'System Events' log in a web interface. The main table lists events with columns for Date/Time, Level, User, Message, Log Description, and Log Details. The log shows a series of 'System configuration backed up' events occurring every hour from 2 minutes ago to 19 hours ago. The user for all events is 'daemon_admin'. The message for each event is 'Automatic backup sent the configuration to https://10.59.112.254/upload.php'. The log description is 'System configuration backed up'. The log details panel on the right shows the event type as 'event' and sub-type as 'system'.

Date/Time	Level	User	Message	Log Description	Log Details
2 minutes ago	INFO	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up	General
Hour ago	INFO	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up	Absolute Date/Time: 2023/02/21 10:57:17
2 hours ago	INFO	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up	Time: 10:57:17
3 hours ago	INFO	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up	Warn: root
4 hours ago	INFO	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up	Log Description: System configuration backed up
5 hours ago	INFO	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up	Source
6 hours ago	INFO	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up	User: daemon_admin
7 hours ago	INFO	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up	Action
8 hours ago	INFO	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up	Action: backup
9 hours ago	INFO	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up	Security
10 hours ago	INFO	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up	Level: INFO
11 hours ago	INFO	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up	Event
13 hours ago	INFO	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up	User Interface
14 hours ago	INFO	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up	Message: Automatic backup sent the configuration to https://10.59.112.254/upload.php
15 hours ago	INFO	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up	Other
16 hours ago	INFO	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up	Event Time: 1677005837644200700
17 hours ago	INFO	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up	Timezone: +0800
18 hours ago	INFO	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up	Log ID: 0100032142
19 hours ago	INFO	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up	Type: event
					Sub-Type: system

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, Domain Name System (DNS) options, packet capture, and static routes.

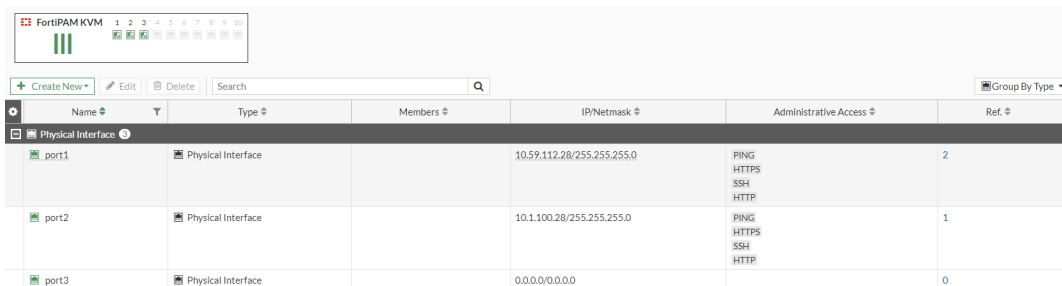
The *Network* tab contains the following tabs:

- [Interfaces on page 231](#)
- [DNS settings on page 235](#)
- [Packet capture on page 238](#)
- [Static routes on page 241](#)

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.



Name	Type	Members	IP/Netmask	Administrative Access	Ref.
port1	Physical Interface		10.59.112.28/255.255.255.0	PING HTTPS SSH HTTP	2
port2	Physical Interface		10.1.100.28/255.255.255.0	PING HTTPS SSH HTTP	1
port3	Physical Interface		0.0.0.0/0.0.0.0		0



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 232 and Creating a zone on page 235 .
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: <ul style="list-style-type: none"> • <i>802.3ad Aggregate</i> • <i>Redundant Interface</i> • <i>VLAN (default)</i>
VLAN protocol	Select either <i>802.1Q</i> or <i>802.1AD</i> . Note: The field is available when <i>Type</i> is set to <i>VLAN</i> .
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.

	 <p>You cannot change the physical interface of a VLAN interface.</p>
	 <p>Use the search bar to look for an interface.</p>
	 <p>Use the pen icon next to an interface to edit the interface.</p>
	<p>Note: The field is available when <i>Type</i> is set to <i>VLAN</i>.</p>
VLAN ID	<p>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.</p> <p>The VLAN ID can be edited after the interface is added.</p> <p>Note: The field is available when <i>Type</i> is set to <i>VLAN</i>.</p>
Interface members	<p>Select members for some interface types.</p> <p>Note: The field is available when <i>Type</i> is set to <i>802.3ad Aggregate</i> or <i>Redundant Interface</i>.</p>
Role	<p>Set the role setting for the interface. Different settings will be shown or hidden when editing an interface depending on the role:</p> <ul style="list-style-type: none"> • <i>LAN</i>: Used to connected to a local network of endpoints. It is default role for new interfaces. • <i>WAN</i>: Used to connected to the internet. When <i>WAN</i> is selected, the <i>Estimated bandwidth</i> setting is available, and <i>Create address object matching subnet</i> is not available. • <i>DMZ</i>: Used to connected to the DMZ. • <i>Undefined</i>: The interface has no specific role. When selected, <i>Create address object matching subnet</i> is not available.
Estimated bandwidth	<p>The estimated WAN bandwidth, in kbps (upstream and downstream).</p> <p>The values can be entered manually, or saved from a speed test executed on the interface. These values are used to estimate WAN usage.</p> <p>Note: The option is only available when the <i>Role</i> is set as <i>WAN</i>.</p>
Address	
Addressing mode	<p>Select the addressing mode for the interface.</p> <ul style="list-style-type: none"> • <i>Manual</i>: Add an IP address and netmask for the interface. • <i>DHCP</i>: Get the interface IP address and other network settings from a DHCP server.
IP/Netmask	<p>If <i>Addressing mode</i> is set to <i>Manual</i>, enter an IPv4 address and subnet mask for the interface.</p>



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. <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  Use the search bar to look for an interface. </div> <div style="border: 1px solid black; padding: 5px; margin-top: 10px;">  Use the pen icon next to an interface to edit the interface. </div>
Comments	Optionally, enter a description about the zone.

4. Click *OK*.

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*.

The screenshot shows the 'DNS Settings' configuration page. It is divided into several sections:

- DNS servers:** Includes a 'Use FortiGuard Servers' button and a 'Specify' button. Below are fields for 'Primary DNS server' (96.45.45.45) and 'Secondary DNS server' (96.45.46.46), each with a '10 ms' response time indicator. A 'Local domain name' field is also present.
- DNS Protocols:** Contains three toggle switches: 'DNS (UDP/53)' (checked), 'TLS (TCP/853)' (unchecked), and 'HTTPS (TCP/443)' (unchecked).
- IPv6 DNS Settings:** Includes fields for 'Primary DNS server' and 'Secondary DNS server', both with empty input boxes.

An 'Apply' button is located at the bottom right of the configuration area.

2. In the *DNS Settings* window, enter the following information:

DNS servers	Select <i>Use FortiGuard Servers</i> or <i>Specify</i> . If you select <i>Specify</i> , 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 <i>DNS servers</i> is <i>Specify</i> .
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 <i>DNS servers</i> is <i>Specify</i> .
Local domain name	The domain name to append to addresses with no domain portion when performing DNS lookups. <hr/>  Select + to add additional local domain names. <hr/>  You can add up to 8 local domain names. <hr/>
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 <i>DNS servers</i> is <i>Specify</i> .
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 <i>DNS servers</i> is <i>Specify</i> .
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 <i>DNS servers</i> is <i>Specify</i> .
SSL certificate	From the dropdown, select an SSL certificate or click <i>Create</i> to import a certificate (default = <code>Fortinet_Factory</code>). 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. <hr/>  Use the search bar to look for an SSL certificate. <hr/>
Server hostname	The host name of the DNS server (default = <code>globalsdns.fortinet.net</code>).



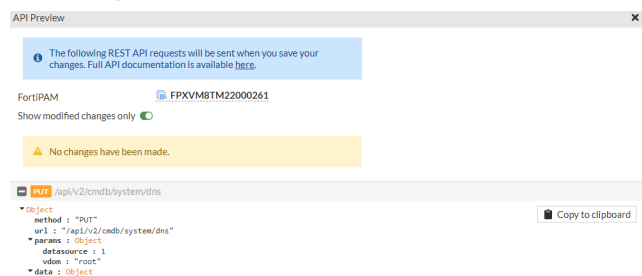
You can add up to 4 server hostnames.

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.

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

Interfaces	Host Filter	Port Filter	VLAN Filter	Protocol Filter	Packets	Max Packet Count	Status
SSL-VPN tunnel interface (ssl.root)					0	4,000	Not Running



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:

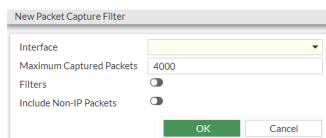
+Create New	Select to create a new packet capture filter. See Creating a packet capture filter on page 239 .
Edit	Select to edit the selected packet capture filter.
Clone	Select to clone the selected packet capture filter.
Delete	Select to delete the selected packet capture filter.
Search	Use the search 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	<p>Select or create a new interface.</p> <hr/> <div style="display: flex; align-items: center;">  <p>Use the search bar to look for an interface.</p> </div> <hr/> <div style="display: flex; align-items: center;">  <p>Use the pen icon next to an interface to edit the interface.</p> </div>
Maximum Captured Packets	<p>Enter how many packets to collect (default = 4000, 1 - 1000000).</p>
Filters	<p>Enable <i>Filters</i>, you can create filters for host names, ports, VLAN identifiers, and protocols.</p> <hr/> <div style="display: flex; align-items: center;">  <p>Use commas to separate items. Use a hyphen to specify a range.</p> </div> <hr/> <p>Note: The option is disabled by default.</p>
Include Non-IP Packets	<p>Select this option if you want to include packets from non-IP protocols.</p> <p>Note: The option is disabled by default.</p>
API Preview	<p>The <i>API Preview</i> 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.</p> <hr/> <div style="display: flex; align-items: center;">  <p>This feature is not available if the user is logged in as an administrator that has read-only GUI permissions.</p> </div>

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.

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.

Destination	Gateway IP	Interface	Status	Comments
IPv4 0.0.0.0/0	10.59.112.1	port1	Enabled	



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 241 .
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.

New Static Route

Destination Subnet

Gateway Address

Interface




Administrative Distance This field is required.

Comments
 0/255

Status
 Enabled Disabled

Advanced Options

3. Enter the following information:

Destination	<p>The destination IP addresses and network masks of packets that the FortiPAM unit intercepts.</p> <p>Enter the IPv4 address and netmask of the new static route.</p>
Gateway Address	<p>The IP addresses of the next-hop routers to which intercepted packets are forwarded.</p> <p>Enter the gateway IP address for those packets that you intend to intercept.</p> <p>Note: <i>Gateway Address</i> is unavailable when the <i>Interface</i> is <i>Blackhole</i>.</p>
Interface	<p>The interface the static route is configured to.</p> <p>Select + and in <i>Select Entries</i>, select the interface or create a new interface.</p> <p>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.</p> <hr/> <div style="display: flex; align-items: center;">  <div style="margin-left: 10px;">Use the search bar to look for an interface.</div> </div> <hr/> <div style="display: flex; align-items: center;">  <div style="margin-left: 10px;">Use the pen icon next to an interface to edit the interface.</div> </div> <hr/>
Administrative Distance	<p>The number of hops the static route has to the configured gateway.</p> <p>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).</p> <p>The route with same distance are considered as equal-cost multi-path (ECMP).</p>
Comments	Optionally, enter a description about the static route.
Status	Enable/disable the static route.
Advanced Options	
Priority	<p>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).</p> <hr/> <div style="display: flex; align-items: center;">  <div style="margin-left: 10px;">Priority can only be customized for statically configured routes. The priority of routes dynamically learned from the routing protocols is always 1.</div> </div> <hr/>

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.

Security profile

The section contains information about configuring FortiPAM security features, including:

- [AntiVirus on page 244](#)

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.

Name	Comments	Ref.
default	Scan files and block viruses.	0



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 246](#).

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.

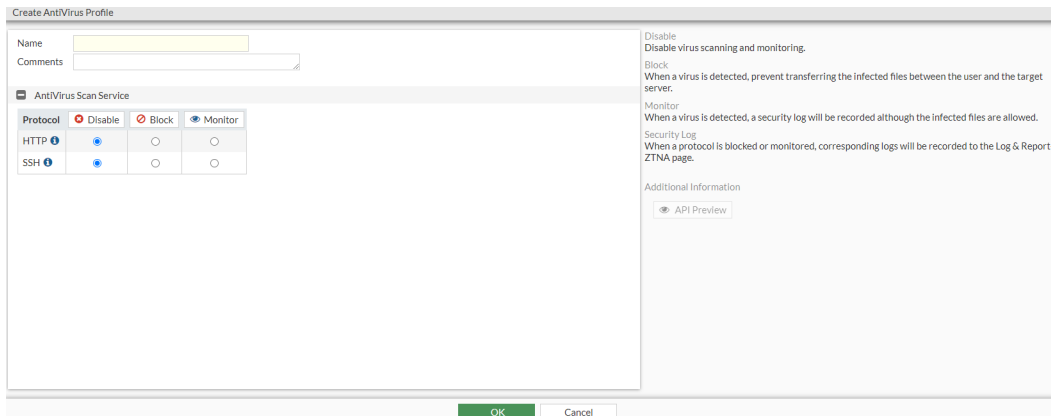
The *AntiVirus* tab contains the following options:

Create New	Select to create a new antivirus profile. See Creating an antivirus profile on page 245 .
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 <code>Enter</code> to search the antivirus profile list.

Creating an antivirus profile

To create an antivirus profile:

1. Go to *Security Profiles > 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 *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. In the *Secret Settings* pane, enable *Antivirus Scan*.
4. From the *Antivirus Profile* dropdown, select an antivirus profile. See [Creating an antivirus profile on page 245](#).
5. Click *Save*.

The screenshot shows the 'Edit Secret' configuration page. The 'Secret Setting' section is expanded, displaying various settings. The 'Antivirus Scan' setting is set to 'Enable', and the 'Antivirus Profile' is set to 'default'. Other settings include 'Automatic Password Changing', 'Automatic Password Verification', 'Session Recording', 'Proxy Mode', 'Tunnel Encryption', 'Requires Checkout', 'Requires Approval to Launch Secret', and 'Requires Approval to Launch Job', all of which are also set to 'Enable'.

The 'General' section shows the following details:

- Name: web-SMB-AD-80.208
- Folder: Windows
- Template: Windows Domain Account (Samba)
- Associated Secret: No associated secret
- Description: (empty)

The 'Fields' table is as follows:

ID	Name	Value
1	Domain-Controller	172.16.40.208
2	Username	admin
3	Password	hidden
4	Domain	fortipam.ca

The 'Secret Setting' section includes the following options:

- Automatic Password Changing: Disable / Enable
- Automatic Password Verification: Disable / Enable
- Session Recording: Disable / Enable
- Proxy Mode: Disable / Enable
- Tunnel Encryption: Disable / Enable
- Antivirus Scan: Disable / Enable
- Antivirus Profile: default
- Requires Checkout: Disable / Enable
- Requires Approval to Launch Secret: Disable / Enable
- Requires Approval to Launch Job: Disable / Enable

At the bottom of the page, there are buttons for 'Save', 'Back', and 'Undo Changes'.

Data loss prevention (DLP) protection for secrets

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
- Credit card and Social Security numbers

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 in the CLI. Note, currently, DLP can only be configured in the CLI and can be applied to file-transfer-based launchers (*WinSCP*, *Web SFTP*, and *Web SMB*).



DLP related configurations can only be set via the CLI.

The following basic filter types can be configured in 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 249](#).
- **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.
- **Credit card and SSN:** The credit card sensor can match the credit card number formats used by American Express, Mastercard, and Visa. It can be used to filter files or messages.
The SSN sensor can be used to filter files or messages for Social Security numbers.

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

```

To configure credit card or SSN 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 {credit-card | ssn}
        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
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

Type	Description
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
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

Type	Description
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.

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 252.

Fabric Connectors

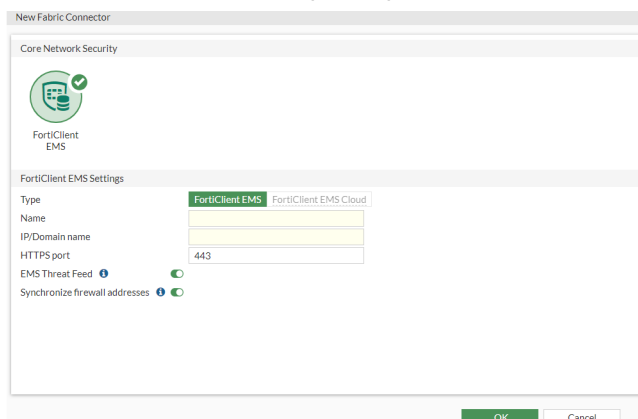
Fabric connectors provide integration with Fortinet products to automate the process of managing dynamic security updates without manual intervention.

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 *Security Fabric > 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:

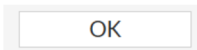
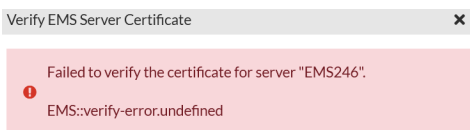
- FortiClient EMS
- FortiClient EMS Cloud



The *FortiClient EMS Cloud* option requires FortiClient EMS Cloud entitlement.

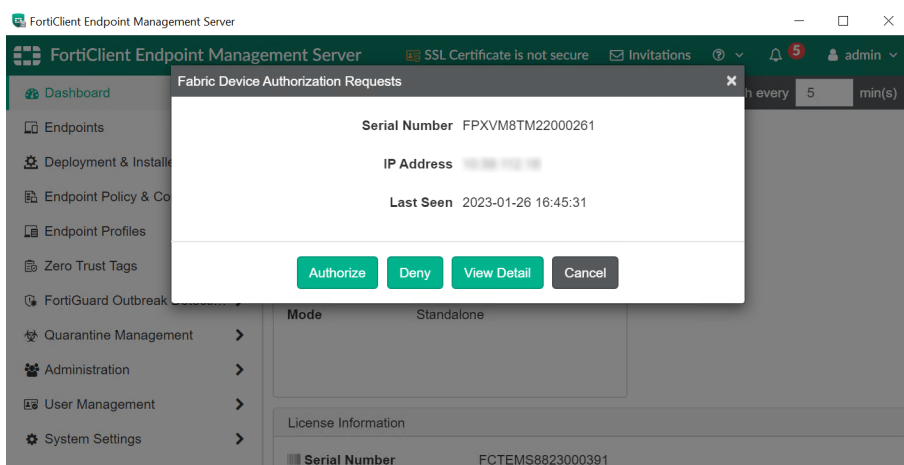
Name	The name of the FortiClient EMS connector.
IP/Domain name	The IP address or the domain name of the FortiClient EMS.
HTTPS port	The HTTPS port number for the FortiClient EMS (default = 443, 1 - 65535).
EMS Threat Feed	Enable to allow FortiPAM to pull FortiClient malware hash from FortiClient EMS. 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.



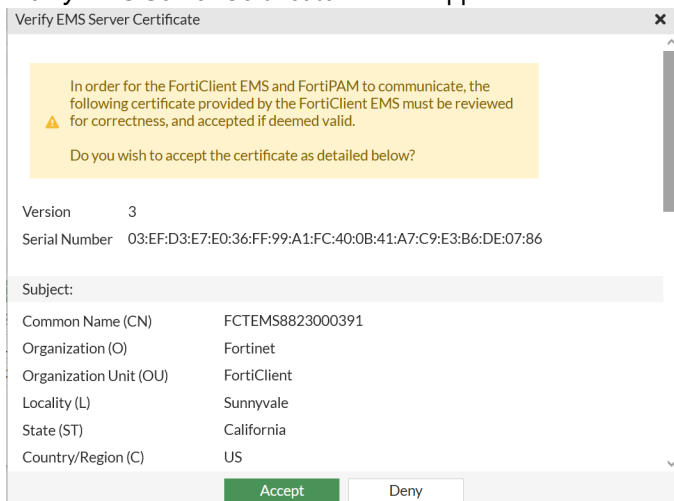
To delete a fabric connector, select *Delete* to delete the selected fabric connector.

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.



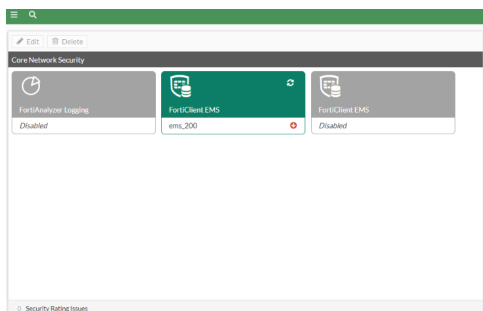
8. In the *Verify EMS Server Certificate* window, select *Accept* to accept the certificate from the EMS-side. FortiPAM is now successfully connected to the EMS server.

FortiAnalyzer logging

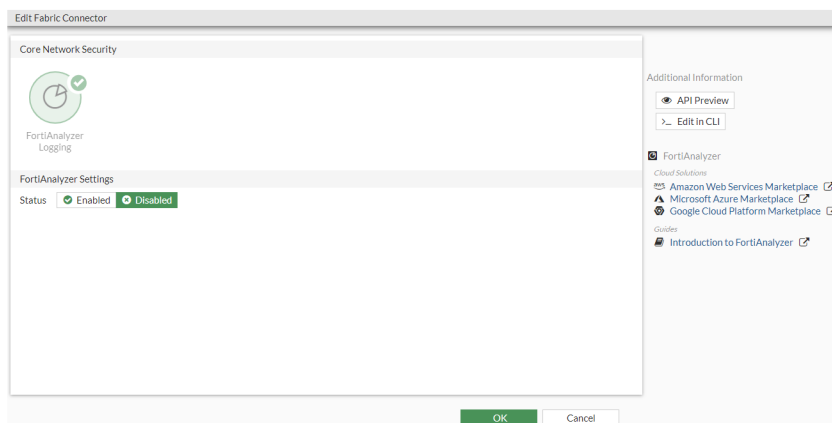
FortiAnalyzer is a remote logging server that helps keep an extra copy of logs and videos from FortiPAM.

To configure FortiAnalyzer logging:

1. Go to *Security Fabric > 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 <i>Test Connectivity</i> to test the connection to the server.
Upload option	The option is set to <i>Store & Upload Logs</i> . Note: The option is non-editable.
Upload interval	Select an upload interval: <ul style="list-style-type: none"> • <i>Daily</i> (default) • <i>Weekly</i> • <i>Monthly</i>
Day	From the dropdown, select a day. Note: The option is only available when the <i>Upload interval</i> is <i>Weekly</i> .
Date	From the dropdown, select a date. Note: The option is only available when the <i>Upload interval</i> is <i>Monthly</i> .
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
```


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:

- [Events on page 257](#)
- [Secret on page 259](#)
- [ZTNA on page 262](#)
- [SSH on page 264](#)
- [Reports on page 264](#)
- [Log settings on page 266](#)
- [Email alert settings on page 269](#)

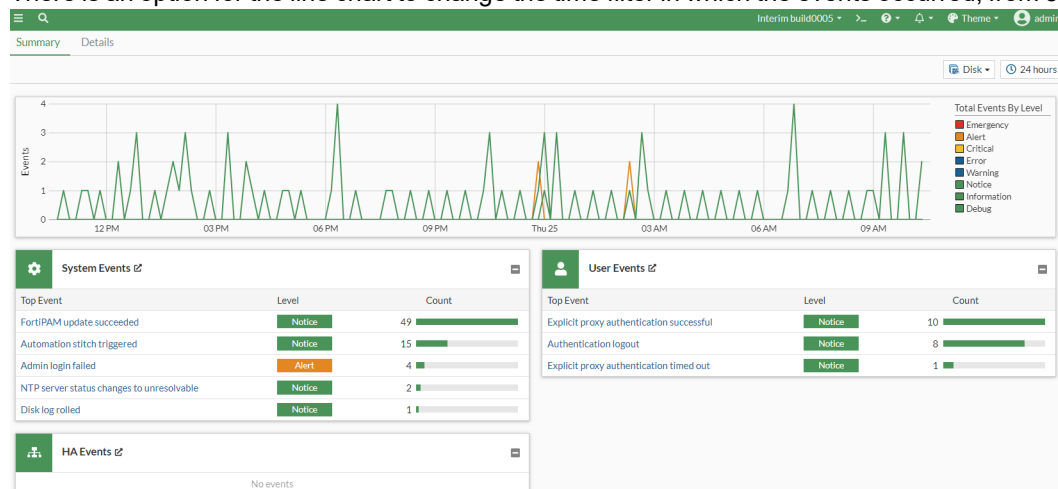
Events

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: <ul style="list-style-type: none"> • 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.

Date/Time	Level	User	Message	Event Type
26 minutes ago	Info		FortiPAM scheduled update fcnl=yes fdnl=yes fsci=yes from 173.243.140.6:443	FortiPAM update
55 minutes ago	Info		FortiPAM scheduled update fcnl=yes fdnl=yes fsci=yes from 173.243.140.6:443	FortiPAM update succeeded
Hour ago	Info		FortiPAM scheduled update fcnl=yes fdnl=yes fsci=yes from 173.243.140.6:443	FortiPAM update succeeded
Hour ago	Info		FortiPAM scheduled update fcnl=yes fdnl=yes fsci=yes from 173.243.140.6:443	FortiPAM update succeeded
2 hours ago	Info		FortiPAM scheduled update fcnl=yes fdnl=yes fsci=yes from 173.243.140.6:443	FortiPAM update succeeded
2 hours ago	Info		FortiPAM scheduled update fcnl=yes fdnl=yes fsci=yes from 173.243.140.6:443	FortiPAM update succeeded
3 hours ago	Info		FortiPAM scheduled update fcnl=yes fdnl=yes fsci=yes from 173.243.140.6:443	FortiPAM update succeeded
3 hours ago	Info		FortiPAM scheduled update fcnl=yes fdnl=yes fsci=yes from 173.243.140.6:443	FortiPAM update succeeded
4 hours ago	Info		stitch:Security Rating Notification is triggered.	Automation stitch triggered
4 hours ago	Info		stitch:Security Rating Notification is triggered.	Automation stitch triggered
4 hours ago	Info		stitch:Security Rating Notification is triggered.	Automation stitch triggered
4 hours ago	Info		FortiPAM scheduled update fcnl=yes fdnl=yes fsci=yes from 173.243.140.6:443	FortiPAM update succeeded
4 hours ago	Info		FortiPAM scheduled update fcnl=yes fdnl=yes fsci=yes from 173.243.140.6:443	FortiPAM update succeeded
5 hours ago	Info		FortiPAM scheduled update fcnl=yes fdnl=yes fsci=yes from 173.243.140.6:443	FortiPAM update succeeded
5 hours ago	Info		FortiPAM scheduled update fcnl=yes fdnl=yes fsci=yes from 173.243.140.6:443	FortiPAM update succeeded
6 hours ago	Info		FortiPAM scheduled update fcnl=yes fdnl=yes fsci=yes from 173.243.140.6:443	FortiPAM update succeeded
6 hours ago	Info		FortiPAM scheduled update fcnl=yes fdnl=yes fsci=yes from 173.243.140.6:443	FortiPAM update succeeded
7 hours ago	Info		FortiPAM scheduled update fcnl=yes fdnl=yes fsci=yes from 173.243.140.6:443	FortiPAM update succeeded
7 hours ago	Info		FortiPAM scheduled update fcnl=yes fdnl=yes fsci=yes from 173.243.140.6:443	FortiPAM update succeeded
8 hours ago	Info		stitch:Security Rating Notification is triggered.	Automation stitch triggered
8 hours ago	Info		stitch:Security Rating Notification is triggered.	Automation stitch triggered
8 hours ago	Info		stitch:Security Rating Notification is triggered.	Automation stitch triggered
8 hours ago	Info		FortiPAM scheduled update fcnl=yes fdnl=yes fsci=yes from 173.243.140.6:443	FortiPAM update succeeded

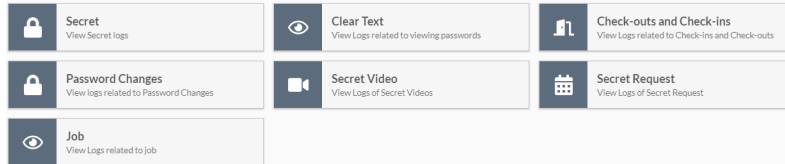
The following options are available in the *Details* tab:

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 <code>Enter</code> . 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 <i>Log & Report</i> page are independent. For example, changing the time frame on the <i>System Events</i> page does not automatically change the time frame on the <i>User Events</i> and <i>HA Events</i> pages.
System Events	From the dropdown, select from the following event types to display: <ul style="list-style-type: none"> • <i>System Events</i> • <i>User Events</i> • <i>HA Events</i>
Log location	Logs sourced from the FortiPAM disk.
Details	Select a log entry and then select <i>Details</i> to see more information about the log.

Secret

Go to *Secret* in *Log & Report* to see logs related to the following:

- [Secret on page 260](#)
- [Clear Text on page 261](#)
- [Check-outs and Check-ins on page 261](#)
- [Password Changes on page 261](#)
- [Secret Video on page 261](#)
- [Secret Request on page 262](#)
- [Job on page 262](#)



The following options are available in the tabs:

Go back to *Secret*.

Back ()

Download log 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

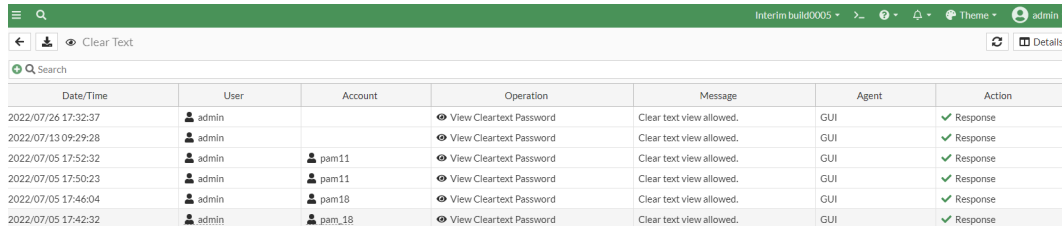
Selecting *Secret* opens all the secret logs. Different subcategories of secret logs are displayed when you click on a secret log.

Date/Time	Token Id	Secret	User	Account	Message	Action	Operation	Launcher	Application Type	Source IP	Destination IP
2022/08/08 16:11:05	2551447021	SVR_101	admin	pam18_1	PAM token is allocated.	Accepted	Start	Web SSH	SSH client	172.17.161.25	10.59.112.28
2022/08/08 16:10:39	2549677532	SVR_101	admin	pam18_1	PAM token is allocated.	Accepted	Start	Web SSH	SSH client	172.17.161.25	10.59.112.28
2022/08/08 16:00:39	2510290068	SVR_101	admin	pam18_1	PAM token is allocated.	Accepted	Start	Web SSH	SSH client	172.17.161.25	10.59.112.28
2022/08/08 15:59:36	2506095731	SVR_101	admin	pam18_1	PAM token is allocated.	Accepted	Start	Web SSH	SSH client	172.17.161.25	10.59.112.28
2022/08/08 15:56:40	2494495767	SVR_101	admin	pam18_1	PAM token is allocated.	Accepted	Start	Web SSH	SSH client	172.17.161.25	10.59.112.28
2022/08/08 15:51:27	2473917282	SVR_101	admin	pam18_1	PAM token is allocated.	Accepted	Start	Web SSH	SSH client	172.17.161.25	10.59.112.28
2022/08/08 15:50:22	2469591864	SVR_101	admin	pam18_1	PAM token is allocated.	Accepted	Start	Web SSH	SSH client	172.17.161.25	10.59.112.28
2022/08/08 15:46:22	2453732012	SVR_101	admin	pam18_1	PAM token is allocated.	Accepted	Start	Web SSH	SSH client	172.17.161.25	10.59.112.28
2022/08/08 15:45:06	2448751229	SVR_101	admin	pam18_1	PAM token is allocated.	Accepted	Start	Web SSH	SSH client	172.17.161.25	10.59.112.28
2022/08/08 15:44:20	2445671009	test_3	admin		PAM token is allocated.	Accepted	Start	Web SSH	SSH client	172.17.161.25	10.59.112.28
2022/08/08 15:43:50	2443639360	test_3	admin		PAM token is allocated.	Accepted	Start	Web SSH	SSH client	172.17.161.25	10.59.112.28
2022/08/05 11:08:04	1552546974	Windows_AD	admin	pam11	PAM token is allocated.	Accepted	Start	Remote Desktop-Windows	Remote desktop	172.30.214.162	10.59.112.28
2022/08/05 10:46:30	1467218808	SVR_101	admin	pam18_1	Video-finished.	Video Finish	Video Finish	PutTY	SSH client	172.16.80.225	10.59.112.28
2022/08/05 10:46:30	1467218808	SVR_101	admin	pam18_1	Uploading.	Video Start	Uploading	PutTY	SSH client	172.16.80.225	10.59.112.28
2022/08/05 10:46:24	1467218808	SVR_101	admin	pam18_1	PAM token is fetched.	Accepted	Fetching	PutTY	SSH client	172.16.80.225	10.59.112.28
2022/08/05 10:46:24	1467218808	SVR_101	admin	pam18_1	PAM token is allocated.	Accepted	Start	PutTY	SSH client	172.16.80.225	10.59.112.28
2022/08/05 10:46:09	1465777002	SVR_101	admin	pam18_1	Video-finished.	Video Finish	Video Finish	Web SSH	SSH client	172.16.80.225	10.59.112.28
2022/08/05 10:46:09	1465777002	SVR_101	admin	pam18_1	Uploading.	Video Start	Uploading	Web SSH	SSH client	172.16.80.225	10.59.112.28
2022/08/05 10:46:07	1465777002	SVR_101	admin	pam18_1	Remote session ended.	Accepted	Connection Closed	Web SSH	SSH client	172.16.80.225	10.1.100.101
2022/08/05 10:46:03	1465777002	SVR_101	admin	pam18_1	PAM token is fetched.	Accepted	Fetching	Web SSH	SSH client	172.16.80.225	10.59.112.28
2022/08/05 10:46:03	1465777002	SVR_101	admin	pam18_1	PAM token is allocated.	Accepted	Start	Web SSH	SSH client	172.16.80.225	10.59.112.28
2022/08/05 10:46:00	1464466261	SVR_101	admin	pam18_1	Video-finished.	Video Finish	Video Finish	PutTY	SSH client	172.16.80.225	10.59.112.28
2022/08/05 10:45:50	1464466261	SVR_101	admin	pam18_1	Uploading.	Video Start	Uploading	PutTY	SSH client	172.16.80.225	10.59.112.28

0% 248 | Updated: 14:54:27

Clear Text

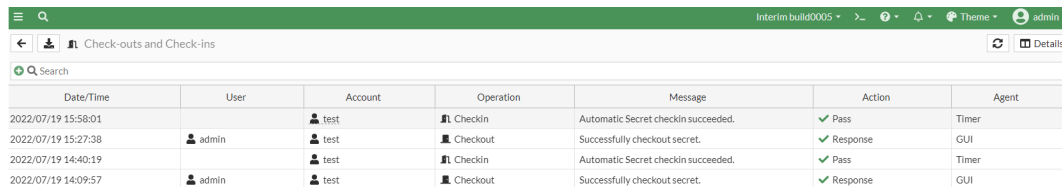
Selecting *Clear Text* shows logs related to viewing passwords. This category of the secret log shows all the information related to the launching of a secret, uploading of a video, termination of a launched session, and status of a FortiPAM token.



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

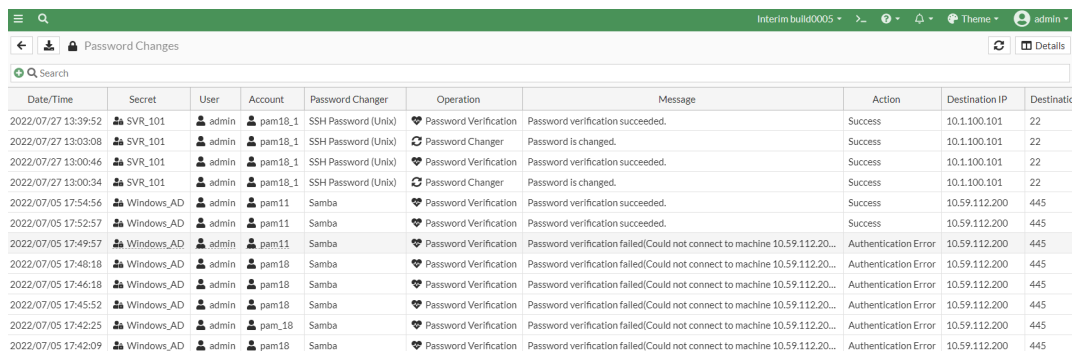
Selecting *Check-outs and Check-ins* shows logs related to password check-ins and check-outs. It displays all the information related to secret check-out and check-in.



Date/Time	User	Account	Operation	Message	Action	Agent
2022/07/19 15:58:01		test	Checkin	Automatic Secret checkin succeeded.	Pass	Timer
2022/07/19 15:27:38	admin	test	Checkout	Successfully checkout secret.	Response	GUI
2022/07/19 14:40:19		test	Checkin	Automatic Secret checkin succeeded.	Pass	Timer
2022/07/19 14:09:57	admin	test	Checkout	Successfully checkout secret.	Response	GUI

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.



Date/Time	Secret	User	Account	Password Changer	Operation	Message	Action	Destination IP	Destination
2022/07/27 13:39:52	SVR_101	admin	pam18_1	SSH Password (Unix)	Password Verification	Password verification succeeded.	Success	10.1.100.101	22
2022/07/27 13:03:08	SVR_101	admin	pam18_1	SSH Password (Unix)	Password Changer	Password is changed.	Success	10.1.100.101	22
2022/07/27 13:00:46	SVR_101	admin	pam18_1	SSH Password (Unix)	Password Verification	Password verification succeeded.	Success	10.1.100.101	22
2022/07/27 13:00:34	SVR_101	admin	pam18_1	SSH Password (Unix)	Password Changer	Password is changed.	Success	10.1.100.101	22
2022/07/05 17:54:56	Windows_AD	admin	pam11	Samba	Password Verification	Password verification succeeded.	Success	10.59.112.200	445
2022/07/05 17:52:57	Windows_AD	admin	pam11	Samba	Password Verification	Password verification succeeded.	Success	10.59.112.200	445
2022/07/05 17:49:57	Windows_AD	admin	pam11	Samba	Password Verification	Password verification failed!(Could not connect to machine 10.59.112.200...	Authentication Error	10.59.112.200	445
2022/07/05 17:48:18	Windows_AD	admin	pam18	Samba	Password Verification	Password verification failed!(Could not connect to machine 10.59.112.200...	Authentication Error	10.59.112.200	445
2022/07/05 17:46:18	Windows_AD	admin	pam18	Samba	Password Verification	Password verification failed!(Could not connect to machine 10.59.112.200...	Authentication Error	10.59.112.200	445
2022/07/05 17:45:52	Windows_AD	admin	pam18	Samba	Password Verification	Password verification failed!(Could not connect to machine 10.59.112.200...	Authentication Error	10.59.112.200	445
2022/07/05 17:42:25	Windows_AD	admin	pam_18	Samba	Password Verification	Password verification failed!(Could not connect to machine 10.59.112.200...	Authentication Error	10.59.112.200	445
2022/07/05 17:42:09	Windows_AD	admin	pam18	Samba	Password Verification	Password verification failed!(Could not connect to machine 10.59.112.200...	Authentication Error	10.59.112.200	445

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.

Date/Time	Token Id	Secret	User	Account	Message	Action	Operation	Launcher	Application Type	Source IP	Destination IP
2022/08/05 10:46:30	1467218808	SVR_101	admin	pam18_1	video-finished.	Video Finish	Video Finish	PUTTY	SSH client	172.16.80.225	10.59.112.28
2022/08/05 10:46:30	1467218808	SVR_101	admin	pam18_1	Uploading.	Video Start	Uploading	PUTTY	SSH client	172.16.80.225	10.59.112.28
2022/08/05 10:46:09	1465777002	SVR_101	admin	pam18_1	video-finished.	Video Finish	Video Finish	Web SSH	SSH client	172.16.80.225	10.59.112.28
2022/08/05 10:46:09	1465777002	SVR_101	admin	pam18_1	Uploading.	Video Start	Uploading	Web SSH	SSH client	172.16.80.225	10.59.112.28
2022/08/05 10:46:00	1464466261	SVR_101	admin	pam18_1	video-finished.	Video Finish	Video Finish	PUTTY	SSH client	172.16.80.225	10.59.112.28
2022/08/05 10:45:50	1464466261	SVR_101	admin	pam18_1	Uploading.	Video Start	Uploading	PUTTY	SSH client	172.16.80.225	10.59.112.28
2022/08/05 10:09:46	1322252844	SVR_101	admin	pam18_1	video-finished.	Video Finish	Video Finish	PUTTY	SSH client	172.16.80.225	10.59.112.28
2022/08/05 10:09:41	1322252844	SVR_101	admin	pam18_1	Uploading.	Video Start	Uploading	PUTTY	SSH client	172.16.80.225	10.59.112.28
2022/08/03 14:30:19	3907314630	SVR_101	admin	pam18_1	video-finished.	Video Finish	Video Finish	PUTTY	SSH client	10.59.112.228	10.59.112.28
2022/08/03 14:30:14	3907314630	SVR_101	admin	pam18_1	Uploading.	Video Start	Uploading	PUTTY	SSH client	10.59.112.228	10.59.112.28
2022/08/03 13:25:03	3554259364	SVR_101	admin	pam18_1	video-finished.	Video Finish	Video Finish	Web SSH	SSH client	172.16.151.57	10.59.112.28
2022/08/03 13:00:19	3554259364	SVR_101	admin	pam18_1	Uploading.	Video Start	Uploading	Web SSH	SSH client	172.16.151.57	10.59.112.28
2022/08/03 10:32:18	2775428305	SVR_101	admin	pam18_1	video-finished.	Video Finish	Video Finish	Web SSH	SSH client	172.16.151.57	10.59.112.28
2022/08/03 09:42:16	2775428305	SVR_101	admin	pam18_1	Uploading.	Video Start	Uploading	Web SSH	SSH client	172.16.151.57	10.59.112.28
2022/08/02 14:48:19	2611454331	SVR_101	admin	pam18_1	Uploading.	Video Start	Uploading	Web SSH	SSH client	172.16.151.57	10.59.112.28
2022/08/02 14:48:02	2533334932	SVR_101	admin	pam18_1	video-finished.	Video Finish	Video Finish	Web SSH	SSH client	172.16.151.57	10.59.112.28
2022/08/02 14:28:29	2533334932	SVR_101	admin	pam18_1	Uploading.	Video Start	Uploading	Web SSH	SSH client	172.16.151.57	10.59.112.28
2022/07/19 14:11:37	503227827	SVR_101	admin	pam18_1	video-finished.	Video Finish	Video Finish	PUTTY	SSH client	172.16.151.57	10.59.112.28
2022/07/19 14:11:27	503227827	SVR_101	admin	pam18_1	Uploading.	Video Start	Uploading	PUTTY	SSH client	172.16.151.57	10.59.112.28
2022/07/13 10:05:04	4215033397	FortiGate	admin	pam18	Uploading.	Video Start	Uploading	Web Launcher	FortiClient Web extension	172.16.151.57	10.59.112.28
2022/07/13 09:48:10	4148186098	FortiGate	admin	pam18	video-finished.	Video Finish	Video Finish	Web Launcher	FortiClient Web extension	172.16.151.57	10.59.112.28
2022/07/13 09:48:05	4148186098	FortiGate	admin	pam18	Uploading.	Video Start	Uploading	Web Launcher	FortiClient Web extension	172.16.151.57	10.59.112.28
2022/07/13 09:18:28	4031006903	FortiGate	admin	pam18	video-finished.	Video Finish	Video Finish	Web Launcher	FortiClient Web extension	172.16.151.57	10.59.112.28

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.

Date/Time	Secret	User	Operation	Start Time	Expired Time	Message	Action
2022/08/18 09:30:32	test_Secret	admin	Request	2022-08-18 09:30:00	2022-08-18 17:30:00	Created secret request.	Pass

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.

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.

Date/Time	Source IP	Access Proxy	Real Server	Service	Result	ZTNA Rule
2022/10/03 13:22:26	172.26.137.3	fortipam_access_proxy	10.59.112.28	HTTPS	Deny: policy violation	1
2022/10/03 13:22:17	172.26.137.3	fortipam_access_proxy	10.59.112.28	HTTPS	Deny: policy violation	1
2022/09/24 14:52:41	admin (172.16.199.82)	fortipam_access_proxy	10.59.112.18	HTTPS	46.82 kB / 0 B	1
2022/09/24 14:52:34	admin (172.16.199.82)	fortipam_access_proxy	127.0.0.1	HTTP	30.71 kB / 15.63 kB	1
2022/09/24 14:52:30	admin (172.16.199.82)	fortipam_access_proxy	10.59.112.18	HTTPS	692 B / 0 B	1
2022/09/24 14:49:43	admin (172.16.199.82)	fortipam_access_proxy	10.59.112.18	HTTPS	2.86 MB / 0 B	1
2022/09/24 14:46:59	admin (172.16.199.82)	fortipam_access_proxy	127.0.0.1	HTTP	39.08 kB / 25.48 kB	1
2022/09/24 14:46:56	admin (172.16.199.82)	fortipam_access_proxy	10.59.112.18	HTTPS	696 B / 0 B	1
2022/09/24 14:46:52	admin (172.16.199.82)	fortipam_access_proxy	10.59.112.18	HTTPS	36.16 kB / 0 B	1
2022/09/24 14:46:48	admin (172.16.199.82)	fortipam_access_proxy	10.59.112.18	HTTPS	197.18 kB / 0 B	1
2022/09/24 14:46:48	admin (172.16.199.82)	fortipam_access_proxy	10.59.112.18	HTTPS	696 B / 0 B	1
2022/09/24 14:46:45	admin (172.16.80.248)	fortipam_access_proxy	10.59.112.200	RDP	77.42 kB / 104.34 kB	1
2022/09/24 14:46:40	admin (172.16.199.82)	fortipam_access_proxy	127.0.0.1	HTTP	103.92 kB / 139.85 kB	1
2022/09/24 14:46:39	admin (172.16.199.82)	fortipam_access_proxy	10.59.112.200	RDP	909 B / 1.85 kB	1
2022/09/24 14:46:37	admin (172.16.199.82)	fortipam_access_proxy	10.59.112.18	HTTPS	688 B / 0 B	1
2022/09/23 17:52:56	admin (172.16.199.5)	fortipam_access_proxy	10.59.112.18	HTTPS	205.88 kB / 0 B	1
2022/09/23 17:52:47	admin (172.16.199.5)	fortipam_access_proxy	127.0.0.1	HTTP	62.12 kB / 67.74 kB	1
2022/09/23 17:52:45	admin (172.16.199.5)	fortipam_access_proxy	10.59.112.18	HTTPS	692 B / 0 B	1
2022/09/23 17:38:43	admin (172.16.80.248)	fortipam_access_proxy	10.59.112.18	HTTPS	497.59 kB / 0 B	1
2022/09/23 17:38:29	admin (172.16.80.248)	fortipam_access_proxy	127.0.0.1	HTTP	97.90 kB / 105.49 kB	1
2022/09/23 17:38:27	admin (172.16.80.248)	fortipam_access_proxy	10.59.112.18	HTTPS	664 B / 0 B	1
2022/09/23 17:37:11	admin (172.16.80.226)	fortipam_access_proxy	10.59.112.18	HTTPS	525.50 kB / 0 B	1
2022/09/23 17:36:57	admin (172.16.80.226)	fortipam_access_proxy	127.0.0.1	HTTP	130.86 kB / 173.41 kB	1
2022/09/23 17:36:55	admin (172.16.80.226)	fortipam_access_proxy	10.59.112.18	HTTPS	696 B / 0 B	1
2022/09/23 17:36:14	admin (172.16.197.145)	fortipam_access_proxy	10.59.112.18	HTTPS	301.48 kB / 0 B	1
2022/09/23 17:36:12	admin (172.16.197.145)	fortipam_access_proxy	10.59.112.200	RDP	75.82 kB / 213.33 kB	1
2022/09/23 17:36:05	admin (172.16.197.145)	fortipam_access_proxy	10.59.112.200	RDP	909 B / 1.85 kB	1
2022/09/23 17:36:05	admin (172.16.197.145)	fortipam_access_proxy	127.0.0.1	HTTP	24.25 kB / 13.37 kB	1
2022/09/23 17:36:03	admin (172.16.197.145)	fortipam_access_proxy	10.59.112.18	HTTPS	688 B / 0 B	1
2022/09/23 17:35:56	admin (172.16.197.145)	fortipam_access_proxy	10.59.112.18	HTTPS	27.30 kB / 0 B	1
2022/09/23 17:35:54	admin (172.16.197.145)	fortipam_access_proxy	127.0.0.1	HTTP	19.09 kB / 12.69 kB	1
2022/09/23 17:35:51	admin (172.16.197.145)	fortipam_access_proxy	10.59.112.18	HTTPS	57.73 kB / 0 B	1
2022/09/23 17:35:50	admin (172.16.197.145)	fortipam_access_proxy	10.59.112.18	HTTPS	692 B / 0 B	1
2022/09/23 17:35:47	admin (172.16.197.145)	fortipam_access_proxy	127.0.0.1	HTTP	19.52 kB / 8.93 kB	1
2022/09/23 17:35:40	admin (172.16.197.145)	fortipam_access_proxy	10.59.112.18	HTTPS	684 B / 0 B	1
2022/09/23 17:35:36	admin (172.16.197.145)	fortipam_access_proxy	10.59.112.18	HTTPS	35.35 kB / 0 B	1
2022/09/23 17:35:30	admin (172.16.197.145)	fortipam_access_proxy	10.59.112.18	HTTPS	692 B / 0 B	1
2022/09/22 22:34:29	admin (172.16.199.42)	fortipam_access_proxy	10.59.112.18	HTTPS	52.61 kB / 0 B	1
2022/09/22 22:34:22	admin (172.16.199.42)	fortipam_access_proxy	127.0.0.1	HTTP	10.01 kB / 3.65 kB	1
2022/09/22 22:34:22	admin (172.16.199.42)	fortipam_access_proxy	10.59.112.18	HTTPS	546.19 kB / 0 B	1
2022/09/22 22:34:19	admin (172.16.199.42)	fortipam_access_proxy	10.59.112.18	HTTPS	668 B / 0 B	1
2022/09/22 22:34:16	admin (172.16.199.42)	fortipam_access_proxy	10.59.112.200	RDP	78.81 kB / 273.57 kB	1
2022/09/22 22:34:08	admin (172.16.199.42)	fortipam_access_proxy	127.0.0.1	HTTP	26.41 kB / 18.20 kB	1
2022/09/22 22:34:07	admin (172.16.199.42)	fortipam_access_proxy	10.59.112.200	RDP	893 B / 1.85 kB	1
2022/09/22 22:34:05	admin (172.16.199.42)	fortipam_access_proxy	10.59.112.18	HTTPS	672 B / 0 B	1
2022/09/22 22:34:00	admin (172.16.199.42)	fortipam_access_proxy	10.59.112.18	HTTPS	948.12 kB / 0 B	1
2022/09/22 22:32:38	admin (172.16.199.42)	fortipam_access_proxy	127.0.0.1	HTTP	38.56 kB / 25.08 kB	1
2022/09/22 22:32:33	admin (172.16.199.42)	fortipam_access_proxy	10.59.112.18	HTTPS	668 B / 0 B	1

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.

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 <i>SSH</i> .
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 <code>Enter</code> to search the secret video list. To narrow down your search, see Column filter .

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.

Name	Data Start	Data End	Size
Schedule-default-2022-08-26-000100	2022/08/25 00:00:00	2022/08/25 23:59:59	412.34 KIB
Schedule-default-2022-08-25-000100	2022/08/24 00:00:00	2022/08/24 23:59:59	412.35 KIB
Schedule-default-2022-08-24-000100	2022/08/23 00:00:00	2022/08/23 23:59:59	412.35 KIB
Schedule-default-2022-08-23-000100	2022/08/22 00:00:00	2022/08/22 23:59:59	414.24 KIB
Schedule-default-2022-08-22-000100	2022/08/21 00:00:00	2022/08/21 23:59:59	412.35 KIB
Schedule-default-2022-08-21-000100	2022/08/20 00:00:00	2022/08/20 23:59:59	412.35 KIB
Schedule-default-2022-08-20-000100	2022/08/19 00:00:00	2022/08/19 23:59:59	412.35 KIB
Schedule-default-2022-08-19-000100	2022/08/18 00:00:00	2022/08/18 23:59:59	413.30 KIB
Schedule-default-2022-08-18-000100	2022/08/17 00:00:00	2022/08/17 23:59:59	412.35 KIB
Schedule-default-2022-08-17-000100	2022/08/16 00:00:00	2022/08/16 23:59:59	412.35 KIB
Schedule-default-2022-08-16-000100	2022/08/15 00:00:00	2022/08/15 23:59:59	412.35 KIB
Schedule-default-2022-08-15-000100	2022/08/14 00:00:00	2022/08/14 23:59:59	412.35 KIB
Schedule-default-2022-08-14-000100	2022/08/13 00:00:00	2022/08/13 23:59:59	412.35 KIB
Schedule-default-2022-08-13-000100	2022/08/12 00:00:00	2022/08/12 23:59:59	412.35 KIB
Schedule-default-2022-08-12-000100	2022/08/11 00:00:00	2022/08/11 23:59:59	412.35 KIB
Schedule-default-2022-08-11-000100	2022/08/10 00:00:00	2022/08/10 23:59:59	412.35 KIB
Schedule-default-2022-08-10-000100	2022/08/09 00:00:00	2022/08/09 23:59:59	419.83 KIB
Schedule-default-2022-08-09-000100	2022/08/08 00:00:00	2022/08/08 23:59:59	416.23 KIB
Schedule-default-2022-08-08-000100	2022/08/07 00:00:00	2022/08/07 23:59:59	412.35 KIB
Schedule-default-2022-08-07-000100	2022/08/06 00:00:00	2022/08/06 23:59:59	412.35 KIB
Schedule-default-2022-08-06-000100	2022/08/05 00:00:00	2022/08/05 23:59:59	420.09 KIB
Schedule-default-2022-08-05-000100	2022/08/04 00:00:00	2022/08/04 23:59:59	416.31 KIB
Schedule-default-2022-08-04-000100	2022/08/03 00:00:00	2022/08/03 23:59:59	420.10 KIB
Schedule-default-2022-08-03-000100	2022/08/02 00:00:00	2022/08/02 23:59:59	418.35 KIB

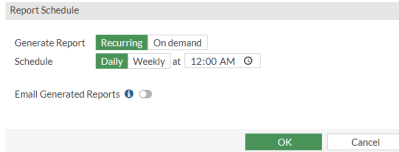
The *Reports* tab contains the following options:

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 <i>Confirm</i> window.
 Regenerating a report may take several minutes.	
Report Schedule	Select to schedule a generating a report. See Schedule generating reports on page 265 .

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 269](#).

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.



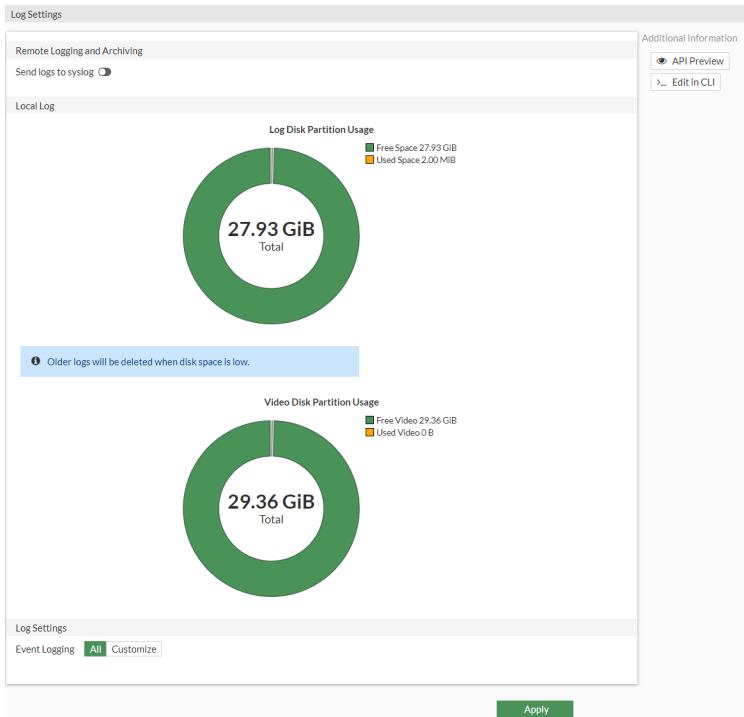
You can change the report attributes from the CLI console only.

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 268](#).

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: <ul style="list-style-type: none"> • <code>legacy-reliable</code>: Legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog). • <code>reliable</code>: Reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP). • <code>udp</code>: 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 = <code>local7</code>): <ul style="list-style-type: none"> • <code>kernel</code>: Kernel messages. • <code>user</code>: Random user-level messages. • <code>mail</code>: Mail system. • <code>daemon</code>: System daemons. • <code>auth</code>: Security/authorization messages. • <code>syslog</code>: Messages generated internally by syslog. • <code>lpr</code>: Line printer subsystem. • <code>news</code>: Network news subsystem. • <code>uucp</code>: Network news subsystem. • <code>cron</code>: Clock daemon.
--	--

	<ul style="list-style-type: none"> • <code>authpriv</code>: Security/authorization messages (private). • <code>ftp</code>: FTP daemon. • <code>ntp</code>: NTP daemon. • <code>audit</code>: Log audit. • <code>alert</code>: Log alert. • <code>clock</code>: Clock daemon. • <code>local0</code> ... <code>local7</code>: Reserved for local use.
<code>source-ip <string></code>	The source IP address of syslog.
<code>format {cef csv default rfc5424}</code>	The log format: <ul style="list-style-type: none"> • <code>cef</code>: CEF (Common Event Format) format. • <code>csv</code>: CSV (Comma Separated Values) format. • <code>default</code>: Syslog format (default). • <code>rfc5424</code>: Syslog RFC5424 format.
<code>priority {default low}</code>	The log transmission priority: <ul style="list-style-type: none"> • <code>default</code>: Set Syslog transmission priority to default (default). • <code>low</code>: Set Syslog transmission priority to low.
<code>max-log-rate <integer></code>	The syslog maximum log rate in MBps (default = 0, 0 - 100000 where 0 = unlimited).
<code>interface-select-method {auto sdwan specify}</code>	Specify how to select outgoing interface to reach the server: <ul style="list-style-type: none"> • <code>auto</code>: Set outgoing interface automatically (default). • <code>sdwan</code>: Set outgoing interface by SD-WAN or policy routing rules. • <code>specify</code>: 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 enable Email alert setting:

1. Go to *Log & Report > Email Alert Settings*, and select *Enable email notification*.

Email Log Setting
 Enable email notification

Glassbreaking Notification General

From
 To Email +

2. In the *Glassbreaking Notification* pane, 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* pane, 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 257](#).
- *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 an email alert when the glass breaking mode is activated:

1. Ensure that *Email Service* is set up in *System > Settings*. See [Settings on page 181](#).
2. Go to *Log & Report > Email Alert Settings*, and select *Enable email notification*.

3. In the *Glassbreaking 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).

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 116](#).



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 272](#).

Related CLI commands:

Command	Description
<code>diagnose wad debug file {enable disable}</code>	Enable/disable dump trace to files.
<code>diagnose wad debug file max_size <size></code>	Set the maximum size for trace files.
<code>diagnose wad debug file overwrite {enable disable}</code>	Allow overwriting when the file reaches maximum size.
<code>diagnose wad debug file clear</code>	Clear all the trace files.
<code>diagnose wad debug file list</code>	Show all trace related file stats.
<code>diagnose wad debug file show {trace_file_name all}</code>	Show a specific or all trace file content.
<code>diagnose wad debug file send tftp <addr> <save_zip_name.tar.gz></code>	Send trace files to TFTP server.
<code>diagnose wad debug file send ftp <save_zip_name.tar.gz> <addr>: [port] [username] [password]</code>	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 <code>/pam api-gateway</code> is displayed, e.g., FortiClient and secret launcher traffic.
tcp-forward	TCP-forward trace. Traffic trace with <code>/tcp api-gateway</code> is displayed, e.g., TCP tunneling information when starting a launcher.
both	Internal FortiPAM and TCP-forward trace. HTTP traffic with <code>/tcp</code> and <code>/pam api-gateway</code> 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

- 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|A| 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
```

- 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:

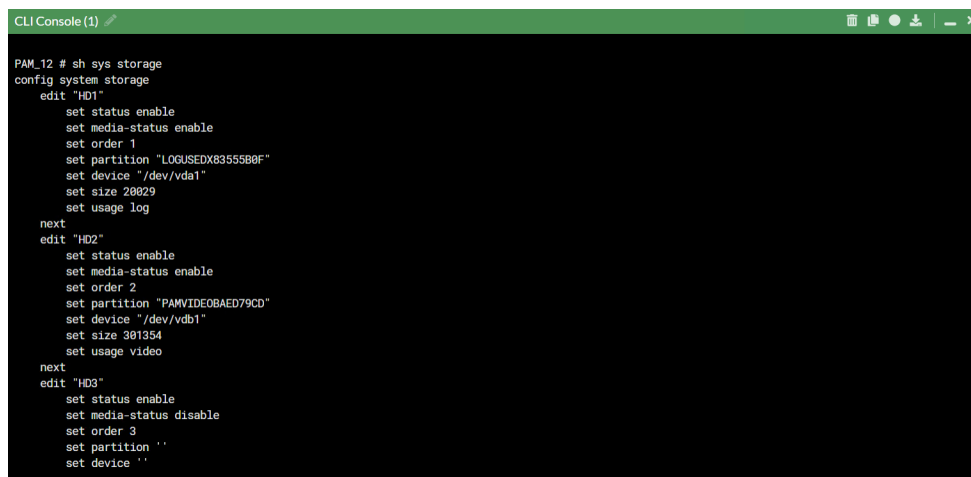
Before opening your virtual machine for the first time you will need to configure two ethernet interfaces.

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 ''
```



```
CLI Console (1)
PAM_12 # sh sys storage
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`.



```
CLI Console (1)
PAM_12 # exec disk list
Disk HD1          ref: 256 20.061B   type: IDE [] dev: /dev/vda
partition ref: 257 19.661B, 19.461B free mounted: Y label: LOGUSEDX83555B0F dev: /dev/vda1 start: 2048
Disk HD2          ref: 16 300.061B  type: IDE [] dev: /dev/vdb
partition ref: 17 294.361B, 293.261B free mounted: Y label: PAMVIDEOBAED79CD dev: /dev/vdb1 start: 2048
PAM_12 #
```

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
```



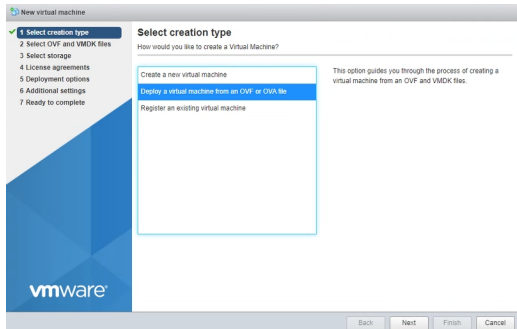
Disk formatting results in the loss of all existing logs and videos.

Appendix B: Installation on VMware

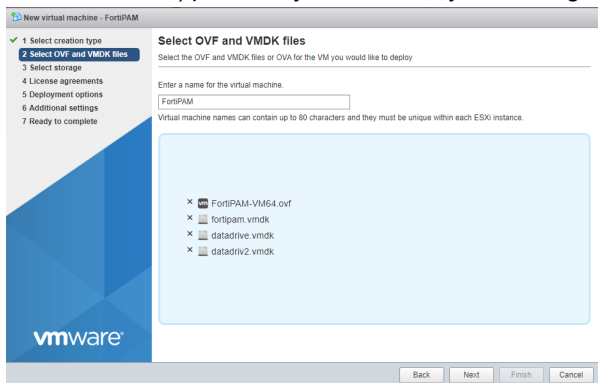
Once you have downloaded the `out.ovf.zip` file and extracted the package contents to a folder on your management computer, you can deploy it into your VMware environment.

To deploy the FortiPAM-VM OVF template:

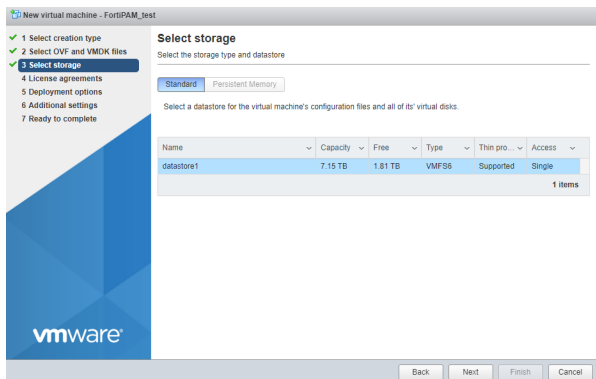
1. Connect to your VMware ESXi server by visiting its URL in your browser. Enter your username and password, and click *Log in*.
2. Select *Create/Register VM*.
The VM creation wizard opens.
3. Select *Deploy a virtual machine from an OVF or OVA file*, and click *Next*.



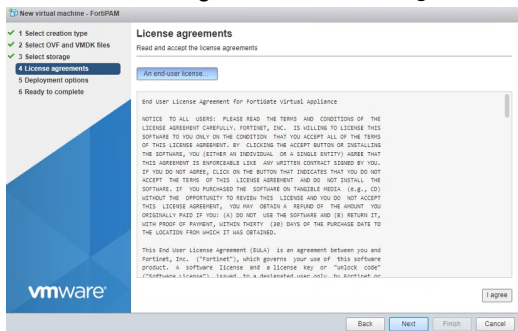
4. Enter a name for your VM and select the files (FortiPAM-VM64.ovf, fortipam.vmdk, datadrive.vmdk, and datadriv2.vmdk) previously extracted to your management computer, and click *Next*.



5. Select which ESXi server's datastore to use for the deployment of FortiPAM-VM, and click *Next*.

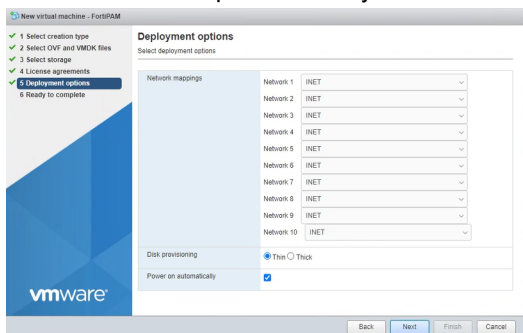


6. Read the licensing terms and click *I agree* and *Next*.



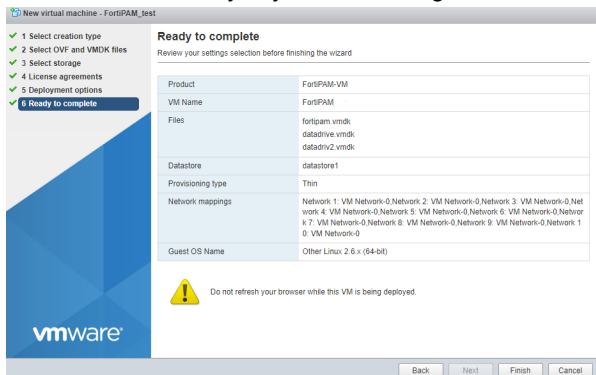
7. Select the appropriate network mappings, disk provisioning, and power on options for your deployment, and click *Next*.

- **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.

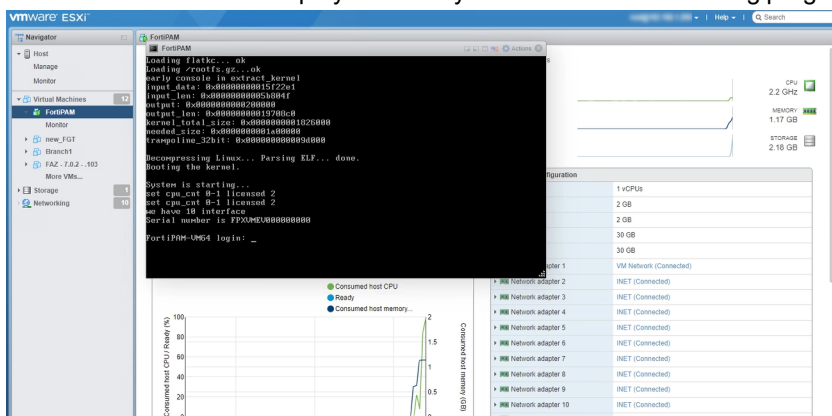


By default, the log disk and video disk size are 30 GB. If you want to change the size, unselect *Power on automatically* to ensure that any disk size change is made before first powering on the VM.

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](#).

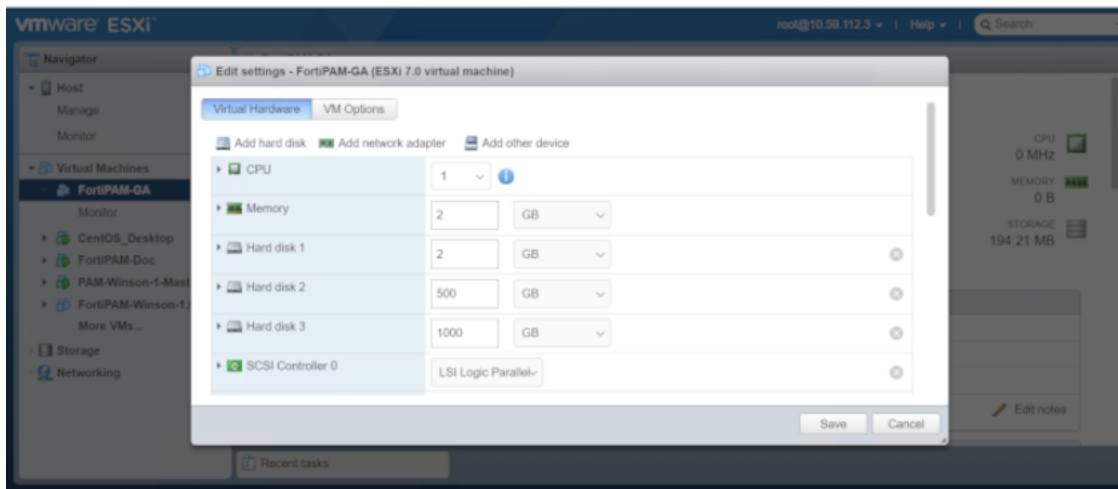
To adjust the log or video disk size:



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. Adjust *Hard disk 2* for log disk size and adjust *Hard disk 3* for video disk size.



- e. 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 ''
```

```

CLI Console (1)
PAM_12 # sh sys storage
config system storage
edit "HD1"
set status enable
set media-status enable
set order 1
set partition "LOGUSEDX8355580F"
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`.

```

CLI Console (1)
PAM_12 # exec disk list
Disk HD1      ref: 256 20.06iB  type: IDE [] dev: /dev/vda
partition ref: 257 19.66iB, 19.46iB free  mounted: Y  label: LOGUSEDX8355580F dev: /dev/vda1 start: 2048
Disk HD2      ref: 16 300.06iB  type: IDE [] dev: /dev/vdb
partition ref: 17 294.36iB, 293.26iB free  mounted: Y  label: PAMVIDEOBAED79CD dev: /dev/vdb1 start: 2048
PAM_12 #

```

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):

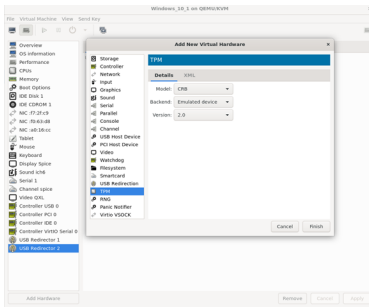
1. In the command line, enter the following commands:

```
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 276](#).
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 vTPM is set up as part of the initial configuration (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.

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
```

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. 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>
```




www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.