Administration Guide

FortiPAM 1.4.2

April 8, 2025
FortiPAM 1.4.2 Administration Guide
74-142-1022359-20250408

TABLE OF CONTENTS

Change Log

Date	Change Description
2025-01-13	Initial release.
2025-02-11	Updated High availability on page 389.
2025-04-08	Updated Gateway on page 124.

What's new in FortiPAM

This section provides a summary of the new features and enhancements in FortiPAM:

- FortiPAM 1.4.2 on page 10
- FortiPAM 1.4.1 on page 10
- FortiPAM 1.4.0 on page 10

Always review the *FortiPAM Release Notes* on the *Fortinet Docs Library* prior to upgrading your device.

FortiPAM 1.4.2

FortiPAM 1.4.2 is a patch release only. There are no new features and enhancements in this release. For more information, see the *FortiPAM 1.4.2 Release Notes* on *Fortinet Docs Library*.

FortiPAM 1.4.1

FortiPAM 1.4.1 is a patch release only. There are no new features and enhancements in this release. For more information, see the *FortiPAM 1.4.1 Release Notes* on *Fortinet Docs Library*.

FortiPAM 1.4.0

The following list contains new and expanded features added in FortiPAM 1.4.0.

Secret/Launch

1001227- Distributed network gateway architecture Reverse mode

The reverse gateway feature extends the distributed architecture functionality.

The introduction of Gateway on page 124 allows accessibility from a FortiPAM located in a public network to a private enterprise network.

Gateway introduced forward type network gateway, i.e., the connection is from FortiPAM to the network gateway and then to the target. This type of in-bound connection can be blocked by an edge or internal firewall and FortiPAM cannot reach the target via the gateway.

To resolve this deployment restriction, FortiPAM supports reverse gateway feature.

The FortiPAM can be reached from a reverse gateway and the reverse gateway makes the first connection to FortiPAM as the control plane connection. This is a persistent connection that uses health checks to detect connection issues and supports reconnection.

New *Type* option when creating a gateway that allows you to configure the gateway as forward or reverse type.

When the *Type* is reverse:

- New *Health Check* options allows you to periodically check if the gateway is still alive.
- Using the new *Gateway ID* option, you can specify the gateway client certificate common name to create a mapping between FortiPAM and the gateway.

A new *Type* column in *Secrets* > *Gateway* that tells you the type of the gateways available, i.e., forward or reverse.

For a reverse gateway, the status is shown on the top-right.

See Gateway on page 124.

994084- Access Target with associated secret credentials

Starting FortiPAM 1.4.0, you can now launch secrets using associated secret credentials not only on Linux and Cisco, but also Windows.

All launchers support launching one secret using another associated secret's credentials. This can be used to store common credential in one secret which can be used by multiple other secrets. This makes the information stored in a secret compact and flexible.

The credential information includes:

- User name
- Password
- Domain
- Public key
- Private key
- Passphrase

The following new options were added when creating or editing a secret in *Secrets* > *Secrets*:

- A new *Launch with Associated Secret Credentials* toggle when *Associated Secret* is enabled in the *General* pane. When the option is enabled, associated secret credential information is used for launching a secret. The credential information stored in the primary secret is not used.

  ⚠ You must ensure that all the required information is stored in the associated secret.

- A new *Auto-Switch Account* option in the *Service Setting* pane when *SSH Service* is enabled and a *Template* is already selected. The option is only available when:
  - *SSH Service* is enabled, i.e., it will only work with SSH launchers.
  - *Launch with Associated Secret Credentials* is enabled in the *General* pane.

  When the *Auto-Switch Account* option is enabled, upon launching the current secret, the secret uses the associated secret (if applicable) and automatically switches to the current account.

When the *Auto-Switch Account* option is disabled, secret launching finishes in the account stored in the associated secret since the credential information was received from the associated secret.

Additionally, *Connect over SSH with* option has been removed.

Note that when both *Launch with Associated Secret Credentials* and *Auto-Switch Account* options are enabled, the same functionality is offered as with the *Connect over SSH with* an associated secret. Launching a secret uses the associated secret credential information to log in and switch to the account stored in the primary secret.

If both *Launch with Associated Secret Credentials* and *Auto-Switch Account* are disabled, the same functionality is offered as with the *Connect over SSH with* itself option. Launching a secret only uses the primary secret for launching. Here, the associated secret provides password for the primary secret without a password, e.g., an SSH secret with keys or a secret with *SSH Auto-Password* enabled and using password changing.

See Creating a secret on page 72.

Also see Connect over SSH on page 90 and Use cases for associated secrets on page 90.

1004629- Customize maximum credential history in a template

A new *Max Record of Credential History* field when configuring a template in *Secret Settings* > *Templates*.

In the new *Max Record of Credential History* field, you can set up the maximum number of credential history to be kept in the database.

See Creating secret templates on page 165.

1000861- Session Monitor refactor based on launch

Starting FortiPAM 1.4.0, the active session monitor is replaced with active launch monitor. One entry represents one launch instead of one session.

Multiple sessions may be made during a single launch. Some launch may still appear in the list even though the launch session is closed.

When the source port is `port 0`, no active TCP connection is attached to the launch.

The *Disconnect* button allows the administrator to terminate a secret launch session. The session attached to the launch is broken.

Two new CLI commands have been added for launch monitor and management.

You can now use the following CLI command to list all the active launches:

```
diagnose wad token list
```

You can use the following CLI command to delete already added launches:

```
diagnose wad token clear <token_id>
```

The `token_id` variable is optional.

⚠ If no `token_id` is given, all the active launches are deleted.

⚠ By deleting active launches, sessions associated with all the launches are broken.

The video connection remains intact until the window is closed.

See Launch session monitor on page 184.

1020348- Warnings for duplicating credentials

Starting FortiPAM 1.4.0, you now receive a secret duplication warning when you create or edit a secret with target address and user name of an existing secret.

This helps avoid password conflicts. If there are duplicate secrets (the same target address and user name) and one secret password is changed, the other secret may not launch as the target password has already been updated.

See Secrets on page 69.

968129, 1006370- Secret service permission

The introduction of launcher permission in secret allows you to customize user with access to only certain types of launchers. This protects some launchers that are more sensetive.

When creating a secret in *Secrets* > *Secrets*:

- The previously available *Secret Setting* pane in *General* is now available as a separate *Secret Setting* tab.
- The ZTNA settings in the *Permission* tab are now available as a separate *ZTNA* pane.
- The *User Permission/Group Permission* table in the *Permission* tab is now available with a new look as a separate pane in the *Permission* tab.

See Creating a secret on page 72.

When creating a folder in *Secrets* > *Personal Folder/Public Folder*:

- The ZTNA settings in the *Permission* tab are now available as a separate *ZTNA* pane.
- The *User Permission/Group Permission* table in the *Permission* tab is now available with a new look as a separate pane in the *Permission* tab.

See Creating a folder on page 139.

When creating a secret template in *Secret Settings* > *Templates*:

- The table listing fields is available with a new look.
- The table listing launchers is available with a new look.
- The *Access* option in the *Permission* tab has been renamed to *Accessibility*.

- *User Permission/Group Permission* in the *Permission* tab have been replaced with *Create Secret* and *Owner* options.

  From the dropdown, you can assign the *Create Secret* and *Owner* permissions to user and user groups.

See Creating secret templates on page 165.

When creating a target in *Secrets* > *Targets*:

- The *Access* option in the *Permission* tab has been renamed to *Accessibility*.
- *User Permission/Group Permission* in the *Permission* tab have been replaced with *Create Secret* and *Owner* options.

  From the dropdown, you can assign the *Create Secret* and *Owner* permissions to user and user groups.

See Creating a target on page 114.

1018981- Three new default SQL templates: Microsoft SQL, MySQL, PostgreSQL

FortiPAM now includes the following three new SQL secret templates:

- *Microsoft SQL*
- *MySQL*
- *PostgreSQL*

This solves the issue of having only one database template entry by creating three new SQL secret database template types from the *Database Server* default template. You can now create more precise database secrets for each specific type.

See Templates on page 161.

971240- Display full folder path

FortiPAM now displays the path to the folder at the top.

You can see the full path of the current folder and jump to a parent folder by clicking the parent folder from the folder path.

Click the predecessor folder from the path breadcrumb to go to the predecessor folder.

Also, the following new GUI changes were introduced:

- The *Go back up one level in the tree* option has been removed.
- The *Open Tree* option is renamed to *Tree*.

See Personal/public folder on page 135.

1021461- Support website login with 2FA(TOTP) and more exact auto filling for web extension

When you launch a secret with web launcher, the extension automatically inputs user name and password to log in to the target website.

However, the web launching feature has the following three limitations:

- When launching to some special website, the extension cannot find the user name or the password field correctly using its predefined key.
- After logging in to a website, the extension tries to fill user name or password into an unrelated field.
- The extension can only fill in user name, password, but 2FA Token is not supported.

In FortiPAM 1.4.0, the web launching feature has been improved with the introduction of auto web filler.

When using a secret template that uses *Web Launcher* as the secret launcher, a new *Web Filler tab* allows you to configure advanced web filler settings, so that extension can locate the correct web elements to patch credential information into.

The following options are available:

- *Authentication path*: The extension checks the URL it visits against the authentication path and applies the configured setting if it is a match. The authentication path can only be part of the desired URL.

  For example, `/#login` can be added instead of `https://fortipam.ca/#login` to allow matching on various sites.
- *Field*: Represents the field from the secret to be patched to the element located by the selector.
  - *Web Element Selector*: Represents the selector for the element in HTML. This can be located with the inspect mode.
  - *Override Path*: Represents if the path should be searched for the selector instead of the authentication path.
  - *Mask*: Represents if there is a mask for the value to be filled in.
- *Token*: The token from the secret is patched to the element located by the selector.
  - *Attribute*: The token value.
  - *Web Element Selector*: Represents the selector for the element in HTML. This can be located with the inspect mode.
  - *Override Path*: Represents if the path should be searched for the selector instead of the authentication path.
  - *Mask*: Represents if there is a mask for the value to be filled in.

Also, more secret fields can be sent to the extension and auto filled during the login process as long as the token is used for 2FA.

The feature needs Microsoft Edge and Google Chrome extension V3.

See Creating secret templates on page 165.

963791- FortiGate web password change

A new *FortiProduct (Web)* default template available in *Secret Settings* > *Templates* for web based products, e.g., FortiGate and FortiProxy.

See Templates on page 161.

The *FortiProduct (Web)* default template includes a new *Web API (Product)* password changer.

See Password changers on page 208.

See Configuring a web FortiProduct secret Example on page 107.

959751- Block copy for web based launching

A new *Block Clipboard* option in the *Secret Setting* tab when creating/editing a secret in *Secrets* > *Secrets* and when creating/editing a secret policy in *Secret Settings* > *Policies*.

When enabled, for the following launchers, you cannot copy content from the launched secret web page:

- *Web Launcher*
- *Web SSH*
- *Web Telnet*
- *Web SMB*
- *Web SFTP*

When enabled, copying content from the remote computer to the local computer is blocked for the following launchers, but does not affect copy/paste on the remote computer itself:

- *Web RDP*
- Native *RDP*

Note that the previously available *Block RDP Clipboard* option in the *Service Setting* tab when creating/editing a secret and in the *New Secret Policy*/*Edit Secret Policy* window when creating/editing a secret policy in *Secret Settings* > *Policies* has been removed.

The feature needs Microsoft Edge and Google Chrome extension V3.

See Creating a secret on page 72 and Creating a policy on page 185.

959751- Support `Ctrl+C/V` for Web RDP session

Starting FortiPAM 1.4.0, you can use copy/paste keyboard shortcuts (`Ctrl + c`/`Ctrl + v`) without the need to first press `F8`.

The `Ctrl + c`/`Ctrl + v` shortcut and right-click to copy/paste functionality are not yet supported on the Mozilla Firefox web browser.

Right-click to copy/paste is not yet supported on Google Chrome and Microsoft Edge web browsers.

The feature needs Microsoft Edge and Google Chrome extension V3.

See Launchers on page 174.

1002904- Secure certificates as secrets

A new default *Certificate Vault* template is introduced in FortiPAM 1.4.0.

With the new default template *Certificate Vault*, you can store certificate with or without corresponding private key and passphrase in FortiPAM. The validity of this certificate will be monitored by FortiPAM.

See Templates on page 161.

Using the new *Certificate Vault* template, you can create secrets to store certificates in *Secrets* > *Secrets*.

The following new options are available when creating a secret using the *Certificate Vault* template:

- *Certificate* field.
- *Log Expiring Certificate* option in the *Secret Setting* tab: Enabling the option generates a log for an expiring certificate.

Disabling *Log Expiring Certificate* stops the generation of log entries for an expiring certificate.

In addition, email alerts for expiring certificates are stopped if you disable this option.

See Creating a secret on page 72.

A new *Certificate* tab in *Log & Report* > *Email Alert Settings*.

Using the new *Certificate* tab, you can now set email alerts for expiring certificates.

See Email alert settings on page 351.

890941- SSH filter Allow mode

In addition to the legacy (Deny) mode, an Allow mode has been added to accept certain commands and deny the rest.

The new Allow mode permits you to configure SSH profiles that will only allow certain SSH pattern commands to be executed while blocking other commands.

The *SSH Filter Profiles* in *Secret Settings* now include the following enhancements:

- Two new modes: *Deny*/*Allow*
  In *Deny* mode, the SSH command patterns configured in the SSH filter profile cannot be used. This means that these commands cannot be executed.

  In *Allow* mode, the SSH command patterns configured in the SSH filter profile can be used. This means that these commands can be executed while other commands will be blocked by FortiPAM.
- New *Log All Unlisted Commands* option.
- When in *Allow* mode, the following commands are available:
  - *Show Allowed List Command*: Customize command that will list all the commands under allowlist anytime.
  - *Shortcut To Run Listed Commands*: Shortcut to quickly run commands within the allowlist, the shortcut is the number within the list shown by *Show Allowed List Command* option.
- New `Exact-match` pattern type applicable to both *Deny* and *Allow* mode.

  This type of pattern will be exact matched on the SSH filter profile.

  See Creating an SSH filter on page 234.

1022441- Ansible lookup plugin integration

For API users with an authentication token, the user gets an exact result with secret ID. Additionally, with the `credential_only` option, you can retrieve credential information for the secret without returning the complete secret information.

The Ansible integration enables user to retrieve secret with ansible playbook, and the secret information obtained through Ansible lookup helps the user to locate the desired secret information.

See *FPAM Ansible Lookup Plugin* to install and use FortiPAM Ansible plugin.

964436- Microsoft SQL Server Management Studio (SSMS) monitoring and logging

When editing a secret target that uses *Microsoft SQL* as the default template, you can enable logging on the SQL server, set the maximum log entry size, and monitor all or a specific database using the new *SQL Log* tab.

See Creating a target on page 114.

1044016- Launcher button refactor

When you open a secret, launchers are now available on the top, listed as icons.

See Creating a secret on page 72 and Launching a secret on page 97.

Additionally:

- When you open a secret that requires check out, the *Check-out Secret* option is now replaced with the *Check-out* ( ) icon.
- When you open a secret to check it in, the *Check-in Secret* option is now replaced with the *Check-in* ( ) icon.

  See Check out and check in a secret on page 98.
- When you open a secret, the *Change Password* option is now available under More options.

  See Change password on page 100.
- When you open a secret, the *Verify Password* option has been replaced with the *Verify* ( ) icon.

  See Verify password on page 104.
- When you open a secret, the *Add/Remove Favorite* option is available under More options.

  See Personal/public folder on page 135.
- When you open a secret that requires you to make a secret access request, the *Make Request* option is now replaced with the *Request* ( ) icon.

  See Make a request on page 145.

1027089, 971921, 1023868- Display privileged account for a target

When setting up a secret as a privileged account for a target, a new tooltip tells you if the target already has a secret set as privileged account. In that case, you cannot set the secret as a privileged account for the target.

See Creating a secret on page 72.

When editing a secret target:

- You can see if the target already has a privileged account set up in the *Privileged Account* field.
- A new *Secret List* tab lists all the secrets associated with this target.

See Creating a target on page 114.

The *Host* column in *Secrets* > *Targets* has been renamed to *Target Address*.

See Targets on page 113.

990047- Print the system time on videos

A new *Video Time Watermark* option in the *Advanced* pane in *System* > *Settings*. The option allows you to add a watermark to the secret videos with time and timezone information.

See Settings on page 373.

A new `video-time-burn` global variable in `secret setting` allows you to include time and timezone information in secret videos.

Limitations:

1. The feature is unavailable when you use the *Fortinet Privileged Access Agent* extension only.
2. The feature is unavailable when you set up secrets using the *Web Account* template.

901040- Approve secret request from email

A new approval link added to the secret approval request email. The approver can use the link to approve or deny the secret access request from the email directly.

To support this, when creating/editing an approval profile in *Secret Settings* > *Approval Profile*, a new *Approval Link Expiry Time* option allows you to set the expiry time for the approve/deny link in the secret approval request email.

Note that the expiry time count starts when the email is sent.

See Create an approval profile on page 200.

1006338- Support ticket number in secret request

You can now create custom fields for an approval profile in *Secret Settings* > *Approval Profile*.

A new *Approval Email Customization* pane when creating or editing an approval profile.

The custom fields capture additional information necessary for the approval process tailored to the specific needs of your organization.

The custom fields are of two types, text/number.

The *Customized Email Template* option has been renamed to *Email Template*.

See Create an approval profile on page 200.

When a user makes a request to launch a secret where an approval profile with custom fields is used, they must specify the required custom fields in the *Fields* pane in the *New secret request* window.

See Make a request on page 145.

See Configuring and accessing a secret that uses an approval profile with custom fields Example on page 110.

1051104- WebTelnet in Secret Service Setting

FortiPAM now supports setting up web *Telnet Service* in the *Service Setting* tab when creating or editing a secret.

See Creating a secret on page 72.

1042899- Windows application filter

Windows application filter is used in Windows server and provides the ability to deny users from installing applications, running certain applications and/or running certain scripts.

Denial is based on directories and usually all executables, scripts, or installers from those directories cannot run.

Exceptions can be added to provide flexibility.

Filters are based on secrets, and different secrets usually have independent filters.

You can add a Windows application filter profile and apply a certain profile to a secret to enable this feature on that secret. FortiPAM generates and maintains a set of application deny rules/filters for that secret.

When a Windows application filter is applied to a secret under a target, a new *Windows Application Filter* tab appears while editing the secret target.

In the new tab, you can see accounts in the secret target, filters applied to accounts, and settings to deactivate/delete all filters.

Prerequisites:

- The host server operates on Windows.
- WinRM is enabled on the host server.
- In FortiPAM, the host server is referred to as "target."
  The target has a privileged account for WinRM access on the host server.
- All secrets whose server information is “Windows” under this target, except for the privileged account, can be used to enable the Windows application filter.

See:

- Window app filter on page 242
- Creating a secret on page 72
- Creating a target on page 114

1025126- User schedule based secret launch

A user configured with a schedule, i.e., the user can log in to FortiPAM depending on its schedule only, will have its launching session terminated when the user session exceeds the time set up in the schedule associated with the user.

A new *Terminate Launching Session* option available when configuring a schedule in *User Management* > *Schedule*.

See Schedule on page 303.

970315- Secret import enhancement

To encourage managing secrets through targets, we now help find existing targets by matching fields— address, domain, or URL.

If non-matching fields are present, the import is considered a duplicate and will not proceed. Otherwise, a new target will be created.

If the secret upload template includes any of the following mandatory fields: *Host*, *Domain*, or *URL*, the corresponding target is modified or created (if applicable).

The new target is created with the naming convention: `import_(Host/Domain/URL).`

The failure to create a target results in the failure to create the corresponding secret.

When importing a secret, FortiPAM first scans if a corresponding target exists by matching *Host*, *URL*, and *Domain*.

If there is a match, FortiPAM chooses the matched target for the secret and creates the secret.

If there is no match, FortiPAM creates a new target automatically first and the target name is `import_[Host/Domain/URL]`. The secret is then created based on the newly created target.

See Uploading secrets using the secret upload template on page 99.

User/Group

936798- Group creation time

A new *Creation Time* column in the following tabs in *User Management*:

- *User Groups*
- *Sponsored Groups*

The *Creation Time* column displays the date and time when a user group or a sponsored group was created.

See User groups on page 269 and Sponsored groups on page 275.

802577- Support single login anytime anywhere

By default, a user account may be used to log in concurrently from multiple locations. For enhanced security, this setting can be disabled by disabling *Concurrent Log-on* in the *Other General Setting* pane in *System* > *Settings*. When you disable the setting, only one session is allowed per user.

See Settings on page 373.

Alternatively, in the CLI console, enter the following commands to disable concurrent login.

```
config system global
 set admin-concurrent disable
end
```

When an admin concurrent session is disabled:

- Additional concurrent admin sessions are blocked while an admin session is active (default)

OR

- FortiPAM automatically terminates any previous sessions when the admin opens a new session.

This behavior can be be changed when the `admin-concurrent` variable is disabled, allowing you to either block additional sessions or terminate (kick out) previous sessions when a new session is opened:

```
config system global
 set admin-concurrent disable
 set admin-new-login-action {block | kick-out} # default = block
end
```

Alternatively, use the *New Log-in Action* option when *Concurrent Log-on* is disabled in *System* > *Settings* to:

- Block additional concurrent admin sessions while an admin session is active (default).
- Terminate any previous sessions when the admin opens a new session.

See Settings on page 373 and Concurrent user sessions on page 434.

System/Log

987628- Automatically backup in-use configuration before restoring a new configuration

FortiPAM automatically backs up the in-use configuration file before restoring a new one to avoid any data loss, e.g., when a wrong password is stored and the encrypted disk fails to open.

See Backup and restore on page 32.

985502- Protect sensitive data with AES256

Starting FortiPAM 1.4.0, AES 256 cryptographic algorithm is used to protect passwords and keys.

902084- FTP support for video/log backup/restore

FortiPAM now supports backing up and restoring video and log files from a remote FTP server.

This displays videos and logs correctly when you want to replace the disks for video and log files.

See Backing up/restoring log and video files using FTP CLI on page 429.

923465- Add filters to the report layout

By using filters, you can now only keep relevant information in the report. The *Add Filter* dropdown shows available filter types for a table.

This helps you filter reports to only keep information that are relevant to you, e.g., secret name, folder, user, etc.

You can add the same or different filters multiple times.

Note that using the same filter generates union (or) results while different filters generate intersection (and) results.

When customizing a report layout in *Log & Report* > *Reports* > *General*, you can add filters for the following tables:

- *User Login*
  - *Top Failure By Reason*

- *Secret Launch*:
  - *Top Success By Secret*
  - *Top Success By Secret and User*
- *Password Change*
  - *Top Success By Secret*
  - *Top Success By Secret and User*
  - *Top Failure By Secret*
  - *Top Failure By Secret and Reason*
  - *Top Failure By Secret, User and Reason*
- *Password Verification*
  - *Top Success By Secret*
  - *Top Success by Secret and User*
  - *Top Failure By Secret*
  - *Top Failure By Secret and Reason*
  - *Top Failure By Secret, User and Reason*
- *Clear Text View*
  - *Top View By Secret*
  - *Top View By Secret and User*

See Layout & schedule on page 338.

949150, 989148, 842754, 901038, 935932- Network Interface GUI refactor

In *Network > Interfaces*:

- A new *Explicit Web Proxy* column is available.
- The *Administrative Access* column has been renamed to *Access*.

See Interfaces on page 357.

Editing an interface has now been simplified.

A new *Service Access Setting* pane is available when editing an interface.

The *ZTNA* tab options previously available in *Settings* are now available when editing an interface.

You can configure ZTNA (firewall policy, access proxy, and VIP) when editing and interface.

Due to the complexity of the ZTNA concept, related settings are available when to *GUI Portal* is enabled while editing an interface.

You can enable the *GUI Portal* toggle to provide external access to FortiPAM. The external access IP can be set in *External IP*. There are two modes for the external IP:

- *Sync with Interface IP*: Under this mode, the external IP address reflects the interface IP address after saving.

  Note: To use *Sync with Interface IP*, `extintf` must be configured to a specific interface in the CLI (not `any`).
- *Customize*: Under this mode, you can set a customized external IP address.

  The default setting is *Sync with Interface IP*.

The service port for external access is on the external IP, with the default port being `443`. The SSL certificate ensures secure authentication access to FortiPAM, with `Fortinet_SSL` as the default certificate.

ZTNA Control restricts access to endpoints with matching ZTNA tags. You can select the validation methods and tags from *ZTNA Tag Validation* and *ZTNA Tags*.

Each interface can have more than one matched external access *GUI Portal* configuration, but the FortiPAM GUI displays the best matched configuration on GUI including its VIP.

If the current interface does not have a matched access portal, you can also create a new access portal on the interface page.

See Editing an interface on page 358.

Additionally, you cannot edit a proxy rule in the GUI anymore.

See ZTNA tags on page 382.

1019879- Show error on the GUI when there is log/video disk failure

The following two types of warning messages are available in the notifications dropdown in the FortiPAM banner on the top-right:

1. When one of the log/video disks or both log and video disks are not mounted properly, the disk is not available, and a warning appears.
2. When the log/video disk encryption status does not match the global disk encryption configuration, then the disk encryption format not matching warning appears.

When you click the warning message, you are sent to the *Log & Report* > *Disk Usage* page for more details on the warnings.

You can click the suggested CLI commands to see more disk status information and suggested solutions.

You must resolve these warnings before performing any task on FortiPAM.

The following lists all the possible warning messages:

Disk not available:

1. `Both the log disk and the video disk are not available.`
2. `The log disk is not available.`
3. `The video disk is not available.`

Disk encryption is not matching:

1. `Disk encryption is enabled but none is in encryption format.`
2. `Disk encryption is enabled but the log disk is not in encryption format.`
3. `Disk encryption is enabled but the video disk is not in encryption format.`
4. `Disk encryption is disabled but both are in encryption format.`
5. `Disk encryption is disabled but the log disk is in encryption format.`
6. `Disk encryption is disabled but the video disk is in encryption format.`

See Disk usage on page 324.

1004932- ACME/LE certificate support

You can now use Let's Encrypt and the ACME protocol to automate certificate creation and maintenance.

See Creating a certificate on page 399.

1014580- Automation stitch for email notifications

Using the new *Automation* tab in *Log & Report*, you can monitor secret activities and system events.

Nine default stitches can be used by enabling and adding your email to action.

You can customize stitches by specifying events and email receivers.

You can add triggers and actions to automation stitches.

See Automation on page 325.

885473- FortiToken Cloud trial support

A one-time 30-day trial FortiToken Cloud license is provided for users to try out the *FortiToken Cloud* 2FA method.

When creating a user in *User Management* > *User List* with *FortiToken Cloud* selected in *Two-Factor Authentication*, you can see the *FortiToken Cloud license* status.

Use the *Activate free trial* option to activate free trial licenses from FortiGuard.

When you go to *System* > *FortiGuard License*, a new entitlement *FortiToken Cloud* is available.

Select *Activate free trial* to activate the free trial with 5 FortiToken Cloud tokens.

The trial license is available for 30 days only. This information is displayed in *System* > *FortiGuard License* and when editing the user.

When in trial or when the license has expired, select *Upgrade* to see instructions on how to add a valid license. The option is available in *System* > *FortiGuard License* and when editing the user.

When the license has expired, you cannot use FortiToken Cloud. *FortiToken Cloud License* then displays *No active license* status when creating/editing the user.

FortiToken Cloud entitlement is marked *Expired* in *System* > *FortiGuard License*.

See Creating a user on page 253 and FortiGuard license on page 434.

1037451, 1052825- Security status on GUI

FortiPAM now displays private data, vTPM, and log/video disk encryption status in the banner and in *System* > *Settings*.

See FortiPAM with TPM on page 47, Settings on page 373, and Configuring log and video disk encryption on page 347.

868067- Log/video disk stats

A new *Disk Usage* tab in *Log & Report* that displays log and video disk usage as charts.

See Disk usage on page 324.

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).

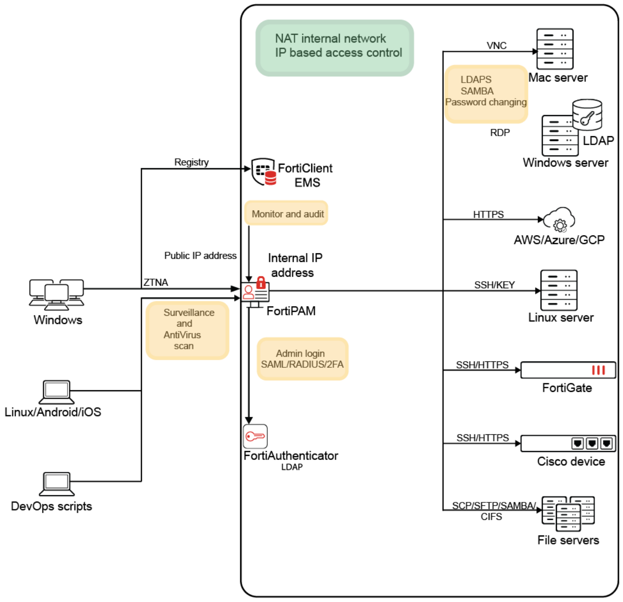
  FortiPAM offers secret permission control to access a target server. Admin users can define common policies and a hierarchical approval system for standard users to access sensitive information. FortiPAM also provides options to control risky user activities such as a user attempting to encrypt the disk.

  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 1.4.2 requires FortiClient 7.4.0 or above to offer the full set of functionalities.

FortiPAM on a NAT internal network



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.

Targets allow a host to have common configuration across secrets.

Classification tags

Classification tags are used to categorize different targets by the OS type or location, e.g., Ubuntu, Windows AD, etc.

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 44 describes basic setup information for getting started with your FortiPAM.
- Licensing on page 51 describes how to register, download, and upload your FortiPAM-VM license.
- Dashboard on page 57 contains widgets providing performance and status information.

- Secrets on page 68 describes features and options related to secrets, targets, gateways, folders, secret and job requests, approval lists, jobs, and discovery.
- Secret settings on page 160 describes features and options related to templates, launchers, policies, classification tags, addresses, dependency updaters, approval profiles, approval email templates, password changers and policies, character sets, antivirus, DLP, DLP file pattern, SSH filter profiles, Windows app filter profiles, event filter profile, and integrity check.
- User management on page 251 describes managing FortiPAM user database.
- Monitoring on page 308 contains information on user logins and active sessions on FortiPAM.
- Log & report on page 312 describes how to view logs and reports on FortiPAM.
- Network on page 357 describes configuring interfaces, static routes, DNS settings, fabric connectors, and packet capture.
- System on page 373 describes managing and configuring basic system settings for FortiPAM. It also contains settings related to ZTNA, HA, certificates, replacement messages, SNMP, automatic backups, firmware, FortiPAM, and FortiGuard licenses.

Using the GUI

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

The following topics are included in this section:

- Banner on page 28
- Tables on page 34

For information about using the dashboards, see Dashboard on page 57.

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 29.
- 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 29.
- *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 30.

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.

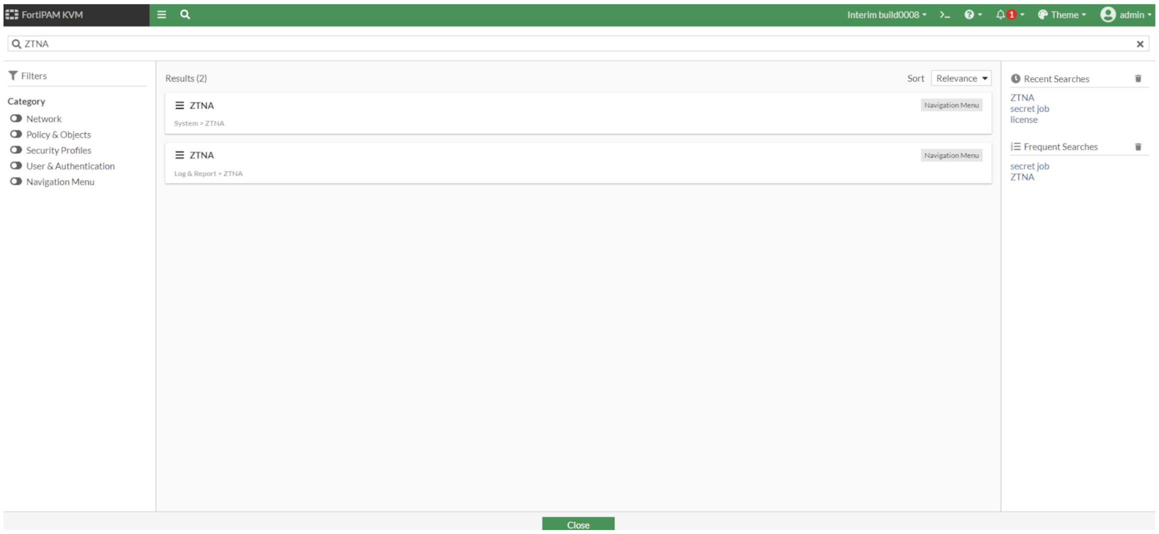
The global search includes the following features:

- 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 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 31.
- Uploading a license. See Licensing on page 51.
- Restoring a configuration. See Backup and restore on page 32.

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

Only the super administrator can change a user 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 353.

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 278.

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

To enter glass breaking mode:

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

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

To disable video recordings when in glass breaking mode:

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

Activate maintenance mode

Suspend all critical processes to allow maintenance related activities.

Uploading a firmware

You can only upload a firmware when in maintenance mode.

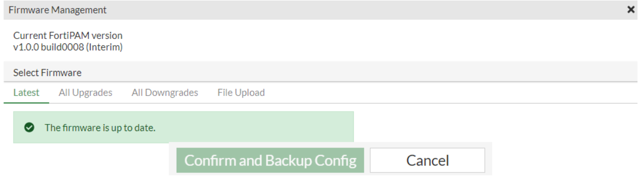
To enter maintenance mode:

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

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

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

To upload a firmware:

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

   Current FortiPAM version
   v1.0.0 build0008 (Interim)
   The firmware is up to date.

   The following options are available:

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

2. Go to *File Upload*:
   a. Select *Browse*, then locate the firmware image on your local computer.
   b. Click *Open*.
3. Click *Confirm and Backup Config*.
   The firmware image uploads from your local computer to the FortiPAM device, which will then reboot. For a short period of time during this reboot, the FortiPAM device is offline and unavailable.

Backup and restore

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

You can encrypt the backup file to prevent tampering.

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

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

When restoring a configuration file, the in-use configuration file is backed up 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 are available at the bottom of the page.

Filters

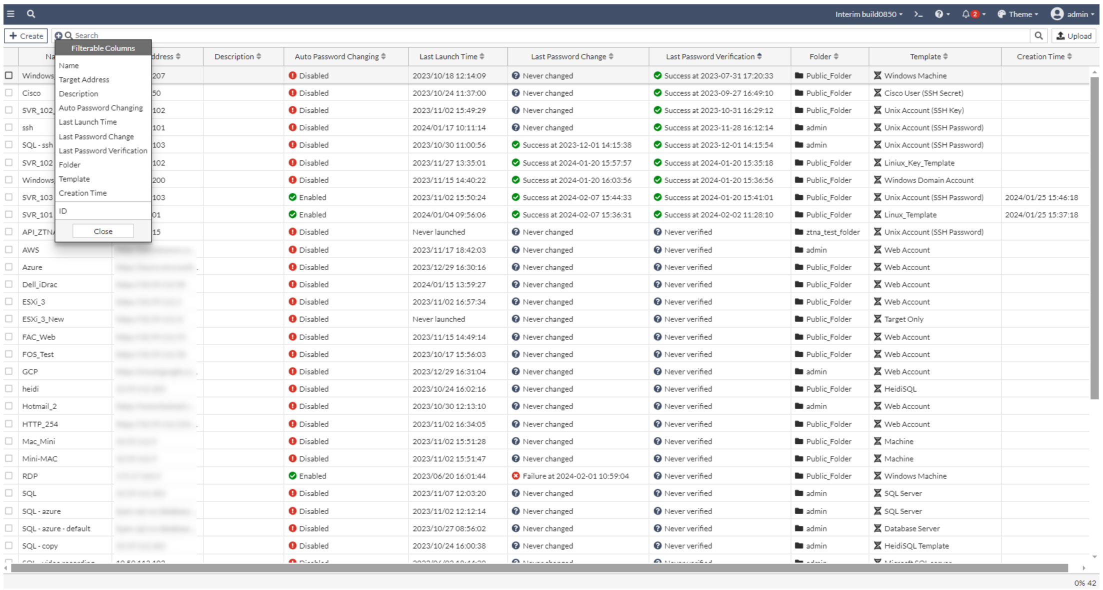
Filters are used to locate a specific set of information or content in a table. They can be particularly useful for locating specific log entries. The filtering options vary, depending on the type of information in the log.

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.

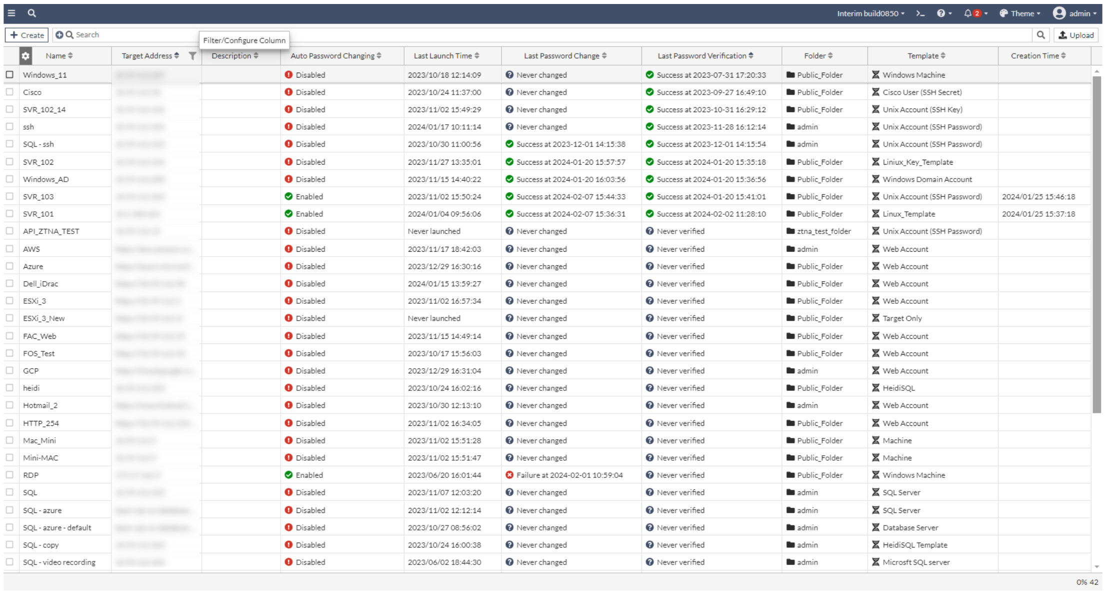
To create a column filter:

1. When available on a GUI page, select + in the search bar.



Na	ddress	Description	Auto Password Changing	Last Launch Time	Last Password Change	Last Password Verification	Folder	Template	Creation Time
Windows	207		Disabled	2023/10/18 12:14:09	Never changed	Success at 2023-07-31 17:20:33	Public_Folder	Windows Machine	
Cisco	50		Disabled	2023/10/24 11:37:00	Never changed	Success at 2023-09-27 16:49:10	Public_Folder	Cisco User (SSH Secret)	
SVR_102	102		Disabled	2023/11/02 15:49:29	Never changed	Success at 2023-10-31 16:29:12	Public_Folder	Unix Account (SSH Key)	
ssh	101		Disabled	2024/01/17 10:11:14	Never changed	Success at 2023-11-28 16:12:14	admin	Unix Account (SSH Password)	
SQL - ssh	103		Disabled	2023/10/30 11:00:56	Success at 2023-12-01 14:15:38	Success at 2023-12-01 14:15:54	admin	Unix Account (SSH Password)	
SVR_102	102		Disabled	2023/11/27 13:35:01	Success at 2024-01-20 15:57:57	Success at 2024-01-20 15:35:18	Public_Folder	Liniux_Key_Template	
Windows	200		Disabled	2023/11/15 14:40:22	Success at 2024-01-20 16:03:56	Success at 2024-01-20 15:36:56	Public_Folder	Windows Domain Account	
SVR_103	103		Enabled	2023/11/02 15:50:24	Success at 2024-02-07 15:44:33	Success at 2024-01-20 15:41:01	Public_Folder	Unix Account (SSH Password)	2024/01/25 15:46:18
SVR_101	01		Enabled	2024/01/04 09:56:06	Success at 2024-02-07 15:36:31	Success at 2024-02-02 11:28:10	Public_Folder	Linux_Template	2024/01/25 15:37:18
API_ZTN	15		Disabled	Never launched	Never changed	Never verified	ztna_test_folder	Unix Account (SSH Password)	
AWS	[redacted]		Disabled	2023/11/17 18:42:03	Never changed	Never verified	admin	Web Account	
Azure	[redacted]		Disabled	2023/12/29 16:30:16	Never changed	Never verified	Public_Folder	Web Account	
Dell_iDrac	[redacted]		Disabled	2024/01/15 13:59:27	Never changed	Never verified	Public_Folder	Web Account	
ESXi_3	[redacted]		Disabled	2023/11/02 16:57:34	Never changed	Never verified	Public_Folder	Web Account	
ESXi_3_New	[redacted]		Disabled	Never launched	Never changed	Never verified	Public_Folder	Target Only	
FAC_Web	[redacted]		Disabled	2023/11/15 14:49:14	Never changed	Never verified	Public_Folder	Web Account	
FOS_Test	[redacted]		Disabled	2023/10/17 15:56:03	Never changed	Never verified	Public_Folder	Web Account	
GCP	[redacted]		Disabled	2023/12/29 16:31:04	Never changed	Never verified	admin	Web Account	
heidi	[redacted]		Disabled	2023/10/24 16:02:16	Never changed	Never verified	Public_Folder	HeidiSQL	
Hotmail_2	[redacted]		Disabled	2023/10/30 12:13:10	Never changed	Never verified	admin	Web Account	
HTTP_254	[redacted]		Disabled	2023/11/02 16:34:05	Never changed	Never verified	Public_Folder	Web Account	
Mac_Mini	[redacted]		Disabled	2023/11/02 15:51:28	Never changed	Never verified	Public_Folder	Machine	
Mini-MAC	[redacted]		Disabled	2023/11/02 15:51:47	Never changed	Never verified	Public_Folder	Machine	
RDP	[redacted]		Enabled	2023/06/20 16:01:44	Failure at 2024-02-01 10:59:04	Never verified	Public_Folder	Windows Machine	
SQL	[redacted]		Disabled	2023/11/07 12:03:20	Never changed	Never verified	admin	SQL Server	
SQL - azure	[redacted]		Disabled	2023/11/02 12:12:14	Never changed	Never verified	admin	SQL Server	
SQL - azure - default	[redacted]		Disabled	2023/10/27 08:56:02	Never changed	Never verified	admin	Database Server	
SQL - copy	[redacted]		Disabled	2023/10/24 16:00:38	Never changed	Never verified	admin	HeidiSQL Template	

Alternatively, select the *Filter/Configure Column (▼)* icon when you hover on the right of the column header, and skip to step 3.

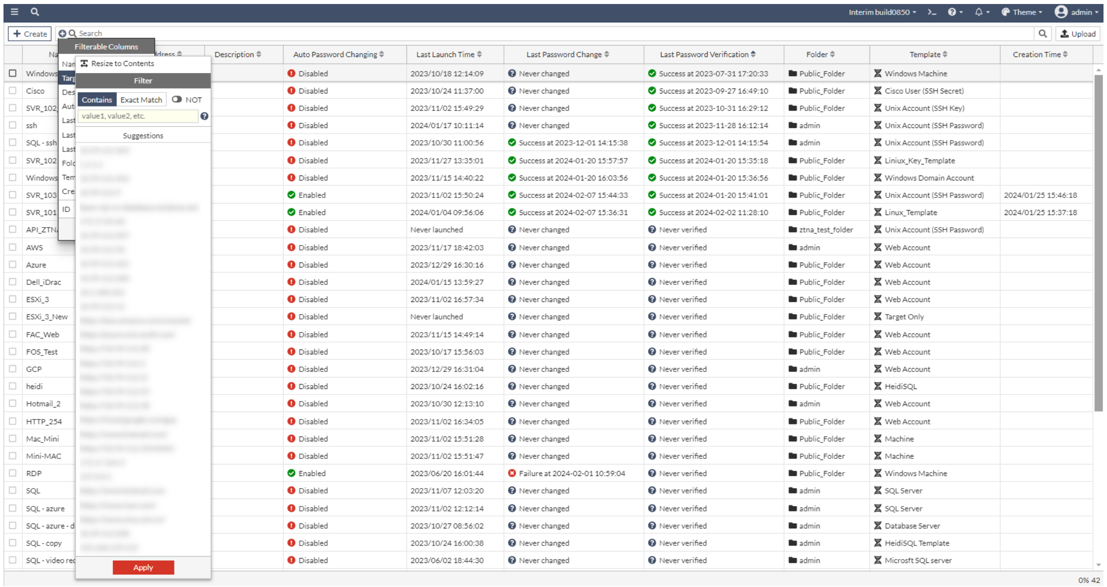


	Name	Target Address	Description	Auto Password Changing	Last Launch Time	Last Password Change	Last Password Verification	Folder	Template	Creation Time
□	Windows_11	[redacted]		Disabled	2023/10/18 12:14:09	Never changed	Success at 2023-07-31 17:20:33	Public_Folder	Windows Machine	
□	Cisco	[redacted]		Disabled	2023/10/24 11:37:00	Never changed	Success at 2023-09-27 16:49:10	Public_Folder	Cisco User (SSH Secret)	
□	SVR_102_14	[redacted]		Disabled	2023/11/02 15:49:29	Never changed	Success at 2023-10-31 16:29:12	Public_Folder	Unix Account (SSH Key)	
□	ssh	[redacted]		Disabled	2024/01/17 10:11:14	Never changed	Success at 2023-11-28 16:12:14	admin	Unix Account (SSH Password)	
□	SQL - ssh	[redacted]		Disabled	2023/10/30 11:00:56	Success at 2023-12-01 14:15:38	Success at 2023-12-01 14:15:54	admin	Unix Account (SSH Password)	
□	SVR_102	[redacted]		Disabled	2023/11/27 13:35:01	Success at 2024-01-20 15:57:57	Success at 2024-01-20 15:35:18	Public_Folder	Liniux_Key_Template	
□	Windows_AD	[redacted]		Disabled	2023/11/15 14:40:22	Success at 2024-01-20 16:03:56	Success at 2024-01-20 15:36:56	Public_Folder	Windows Domain Account	
□	SVR_103	[redacted]		Enabled	2023/11/02 15:50:24	Success at 2024-02-07 15:44:33	Success at 2024-01-20 15:41:01	Public_Folder	Unix Account (SSH Password)	2024/01/25 15:46:18
□	SVR_101	[redacted]		Enabled	2024/01/04 09:56:06	Success at 2024-02-07 15:36:31	Success at 2024-02-02 11:28:10	Public_Folder	Linux_Template	2024/01/25 15:37:18
□	API_ZTNA_TEST	[redacted]		Disabled	Never launched	Never changed	Never verified	ztna_test_folder	Unix Account (SSH Password)	
□	AWS	[redacted]		Disabled	2023/11/17 18:42:03	Never changed	Never verified	admin	Web Account	
□	Azure	[redacted]		Disabled	2023/12/29 16:30:16	Never changed	Never verified	Public_Folder	Web Account	
□	Dell_iDrac	[redacted]		Disabled	2024/01/15 13:59:27	Never changed	Never verified	Public_Folder	Web Account	
□	ESXi_3	[redacted]		Disabled	2023/11/02 16:57:34	Never changed	Never verified	Public_Folder	Web Account	
□	ESXi_3_New	[redacted]		Disabled	Never launched	Never changed	Never verified	Public_Folder	Target Only	
□	FAC_Web	[redacted]		Disabled	2023/11/15 14:49:14	Never changed	Never verified	Public_Folder	Web Account	
□	FOS_Test	[redacted]		Disabled	2023/10/17 15:56:03	Never changed	Never verified	Public_Folder	Web Account	
□	GCP	[redacted]		Disabled	2023/12/29 16:31:04	Never changed	Never verified	admin	Web Account	
□	heidi	[redacted]		Disabled	2023/10/24 16:02:16	Never changed	Never verified	Public_Folder	HeidiSQL	
□	Hotmail_2	[redacted]		Disabled	2023/10/30 12:13:10	Never changed	Never verified	admin	Web Account	
□	HTTP_254	[redacted]		Disabled	2023/11/02 16:34:05	Never changed	Never verified	Public_Folder	Web Account	
□	Mac_Mini	[redacted]		Disabled	2023/11/02 15:51:28	Never changed	Never verified	Public_Folder	Machine	
□	Mini-MAC	[redacted]		Disabled	2023/11/02 15:51:47	Never changed	Never verified	Public_Folder	Machine	
□	RDP	[redacted]		Enabled	2023/06/20 16:01:44	Failure at 2024-02-01 10:59:04	Never verified	Public_Folder	Windows Machine	
□	SQL	[redacted]		Disabled	2023/11/07 12:03:20	Never changed	Never verified	admin	SQL Server	
□	SQL - azure	[redacted]		Disabled	2023/11/02 12:12:14	Never changed	Never verified	admin	SQL Server	
□	SQL - azure - default	[redacted]		Disabled	2023/10/27 08:56:02	Never changed	Never verified	admin	Database Server	
□	SQL - copy	[redacted]		Disabled	2023/10/24 16:00:38	Never changed	Never verified	admin	HeidiSQL Template	
□	SQL - video recording	[redacted]		Disabled	2023/06/02 18:44:30	Never changed	Never verified	admin	Microsft SQL server	

0% 42

When importing users as shown in Importing LDAP users on page 266, the *Filter/Configure Column* (▼) icon is available next to *All Users*.

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*.



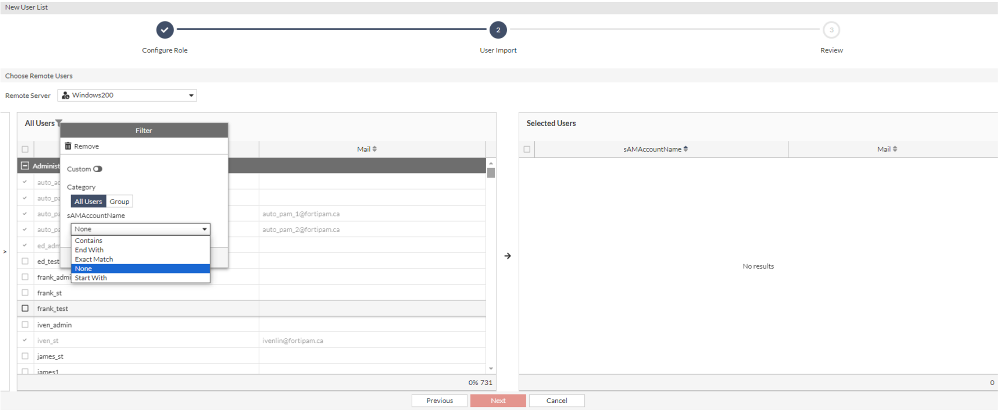
[redacted]

	Na	Description	Auto Password Changing	Last Launch Time	Last Password Change	Last Password Verification	Folder	Template	Creation Time
□	Windows		Disabled	2023/10/18 12:14:09	Never changed	Success at 2023-07-31 17:20:33	Public_Folder	Windows Machine	
□	Cisco		Disabled	2023/10/24 11:37:00	Never changed	Success at 2023-09-27 16:49:10	Public_Folder	Cisco User (SSH Secret)	
□	SVR_102		Disabled	2023/11/02 15:49:29	Never changed	Success at 2023-10-31 16:29:12	Public_Folder	Unix Account (SSH Key)	
□	ssh		Disabled	2024/01/17 10:11:14	Never changed	Success at 2023-11-28 16:12:14	admin	Unix Account (SSH Password)	
□	SQL - ssh		Disabled	2023/10/30 11:00:56	Success at 2023-12-01 14:15:38	Success at 2023-12-01 14:15:54	admin	Unix Account (SSH Password)	
□	SVR_102		Disabled	2023/11/27 13:35:01	Success at 2024-01-20 15:57:57	Success at 2024-01-20 15:35:18	Public_Folder	Liniux_Key_Template	
□	Windows		Disabled	2023/11/15 14:40:22	Success at 2024-01-20 16:03:56	Success at 2024-01-20 15:36:56	Public_Folder	Windows Domain Account	
□	SVR_103		Enabled	2023/11/02 15:50:24	Success at 2024-02-07 15:44:33	Success at 2024-01-20 15:41:01	Public_Folder	Unix Account (SSH Password)	2024/01/25 15:46:18
□	SVR_101		Enabled	2024/01/04 09:56:06	Success at 2024-02-07 15:36:31	Success at 2024-02-02 11:28:10	Public_Folder	Linux_Template	2024/01/25 15:37:18
□	API_ZTN		Disabled	Never launched	Never changed	Never verified	ztna_test_folder	Unix Account (SSH Password)	
□	AWS		Disabled	2023/11/17 18:42:03	Never changed	Never verified	admin	Web Account	
□	Azure		Disabled	2023/12/29 16:30:16	Never changed	Never verified	Public_Folder	Web Account	
□	Dell_iDrac		Disabled	2024/01/15 13:59:27	Never changed	Never verified	Public_Folder	Web Account	
□	ESXi_3		Disabled	2023/11/02 16:57:34	Never changed	Never verified	Public_Folder	Web Account	
□	ESXi_3_New		Disabled	Never launched	Never changed	Never verified	Public_Folder	Target Only	
□	FAC_Web		Disabled	2023/11/15 14:49:14	Never changed	Never verified	Public_Folder	Web Account	
□	FOS_Test		Disabled	2023/10/17 15:56:03	Never changed	Never verified	Public_Folder	Web Account	
□	GCP		Disabled	2023/12/29 16:31:04	Never changed	Never verified	admin	Web Account	
□	heidi		Disabled	2023/10/24 16:02:16	Never changed	Never verified	Public_Folder	HeidiSQL	
□	Hotmail_2		Disabled	2023/10/30 12:13:10	Never changed	Never verified	admin	Web Account	
□	HTTP_254		Disabled	2023/11/02 16:34:05	Never changed	Never verified	Public_Folder	Web Account	
□	Mac_Mini		Disabled	2023/11/02 15:51:28	Never changed	Never verified	Public_Folder	Machine	
□	Mini-MAC		Disabled	2023/11/02 15:51:47	Never changed	Never verified	Public_Folder	Machine	
□	RDP		Enabled	2023/06/20 16:01:44	Failure at 2024-02-01 10:59:04	Never verified	Public_Folder	Windows Machine	
□	SQL		Disabled	2023/11/07 12:03:20	Never changed	Never verified	admin	SQL Server	
□	SQL - azure		Disabled	2023/11/02 12:12:14	Never changed	Never verified	admin	SQL Server	
□	SQL - azure - d		Disabled	2023/10/27 08:56:02	Never changed	Never verified	admin	Database Server	
□	SQL - copy		Disabled	2023/10/24 16:00:38	Never changed	Never verified	admin	HeidiSQL Template	
□	SQL - video rec		Disabled	2023/06/02 18:44:30	Never changed	Never verified	admin	Microsft SQL server	

0% 42

When importing users as shown in Importing LDAP users on page 266, the following options are available for *All Users* and *Group*:

- *Contains*
- *End With*
- *Exact Match*
- *None*
- *Start With*



Remote Server: Windows200

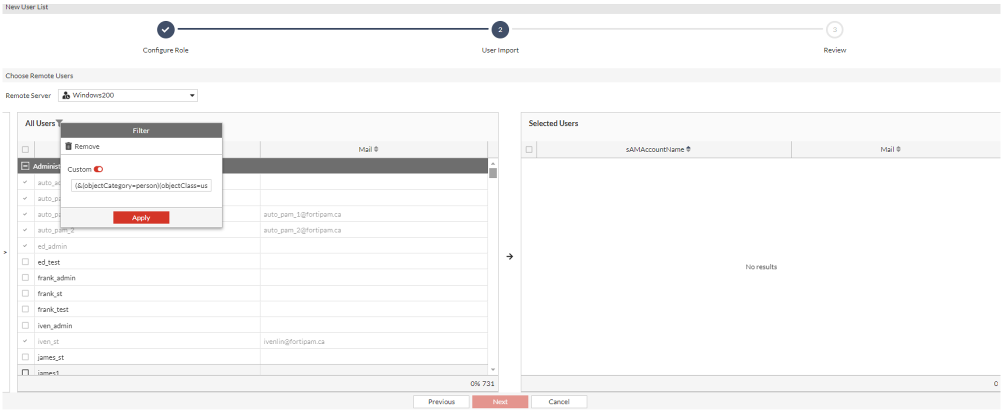
sAMAccountName: None

	Mail
Administ	
auto_ad	
auto_pa	
auto_pa	auto_pam_1@fortipam.ca
auto_pa	auto_pam_2@fortipam.ca
ed_adm	
ed_test	
frank_admi	
frank_st	
frank_test	
iven_admin	
iven_st	ivenlin@fortipam.ca
james_st	
james1	

0% 731

0

You can also create a custom filter by enabling *Custom* and setting up a filter:



Remote Server: Windows200

(&(objectCategory=person)(objectClass=us

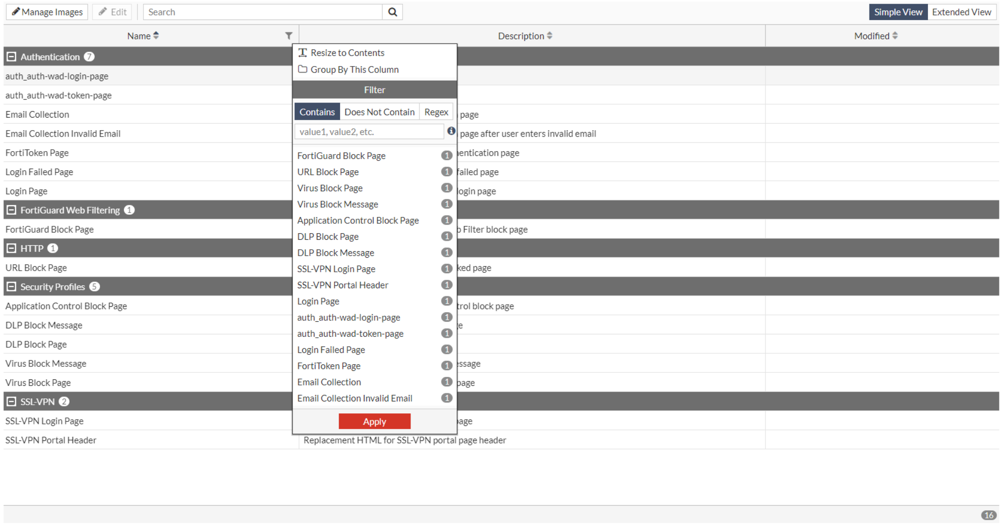
	Mail
Administ	
auto_ad	
auto_pa	
auto_pa	auto_pam_1@fortipam.ca
auto_pam_2	auto_pam_2@fortipam.ca
ed_admin	
ed_test	
frank_admin	
frank_st	
frank_test	
iven_admin	
iven_st	ivenlin@fortipam.ca
james_st	
james1	

0% 731

0

In the *Replacement Message* page, the following options are available:

- *Contains*
- *Does Not Contain*
- *Regex*



Name	Description	Modified
Authentication 7		
auth_auth-wad-login-page		
auth_auth-wad-token-page		
Email Collection	page	
Email Collection Invalid Email	page after user enters invalid email	
FortiToken Page	ıentication page	
Login Failed Page	failed page	
Login Page	login page	
FortiGuard Web Filtering 1		
FortiGuard Block Page	b Filter block page	
HTTP 1		
URL Block Page	ked page	
Security Profiles 5		
Application Control Block Page	trol block page	
DLP Block Message	e	
DLP Block Page		
Virus Block Message	ssage	
Virus Block Page	page	
SSL-VPN 2		
SSL-VPN Login Page	age	
SSL-VPN Portal Header	Replacement HTML for SSL-VPN portal page header	

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.

Alternatively, select *Filter/Configure Column* on the right of the column header, and repeat steps 3 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, Web Telnet, 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 72. Alternatively, see the *Proxy Mode* option when creating or editing a policy. See Creating a policy on page 185.

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.

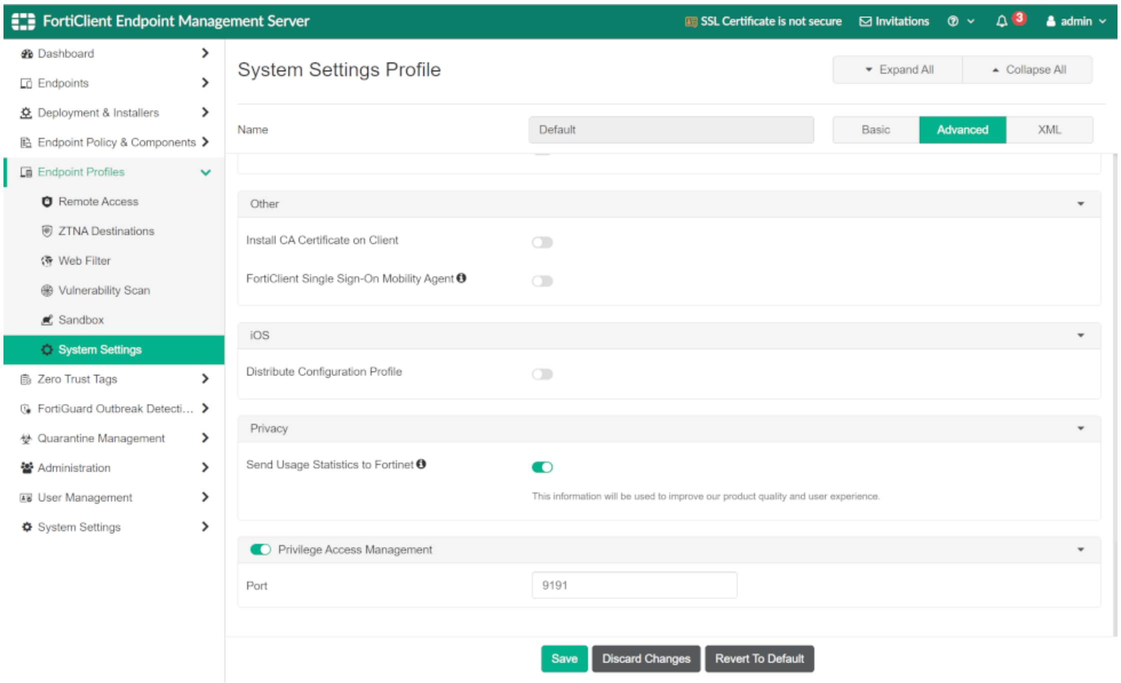
For information on installing FortiPAM browser extension and standalone FortiClient on an air-gapped computer, see Appendix M: FortiPAM browser extension and standalone FortiClient air-gapped installation on page 527.

For information about the over-the-shoulder monitoring (live recording) feature, see Over-the-shoulder monitoring (Live recording) on page 310.

If FortiClient is not available, e.g., a user with Linux or MacOS system, Chrome and Edge extension called *Fortinet Privileged Access Agent* is available on Chrome Web Store and Microsoft Edge Add-ons. On this extension-only setup, web-based launchers and web browsing are supported. The extension can record user activities on the target server.

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

1. If EMS (7.2.0 or later) is available:
   a. **EMS Server**:
      i. Enable *Privilege Access Management*-
         i. Navigate to *Endpoint Profiles* > *System Settings*.
         ii. Edit the *Default System Setting Profiles*.
         iii. Select *Advanced* and enable *Privilege Access Management*.
         iv. In *Port*, enter 9191.
         v. Click *Save*.



Name: Default

Install CA Certificate on Client: off

FortiClient Single Sign-On Mobility Agent: off

Distribute Configuration Profile: off

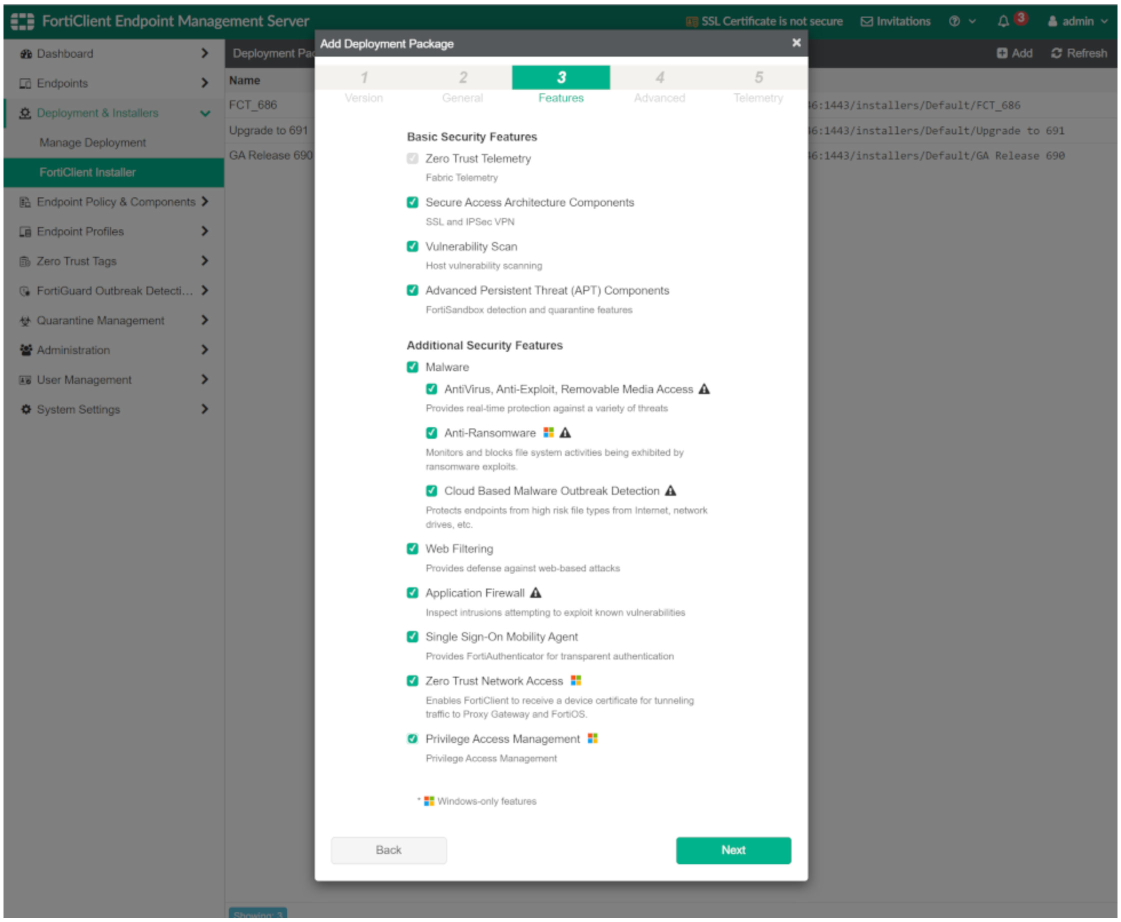
Send Usage Statistics to Fortinet: on

This information will be used to improve our product quality and user experience.

Privilege Access Management: on

Port: 9191

      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.



Add Deployment Package

1 Version | 2 General | 3 Features | 4 Advanced | 5 Telemetry

Basic Security Features

☑ Zero Trust Telemetry
Fabric Telemetry

☑ Secure Access Architecture Components
SSL and IPSec VPN

☑ Vulnerability Scan
Host vulnerability scanning

☑ Advanced Persistent Threat (APT) Components
FortiSandbox detection and quarantine features

Additional Security Features

☑ Malware

☑ AntiVirus, Anti-Exploit, Removable Media Access ⚠
Provides real-time protection against a variety of threats

☑ Anti-Ransomware ⊞ ⚠
Monitors and blocks file system activities being exhibited by ransomware exploits.

☑ Cloud Based Malware Outbreak Detection ⚠
Protects endpoints from high risk file types from Internet, network drives, etc.

☑ Web Filtering
Provides defense against web-based attacks

☑ Application Firewall ⚠
Inspect intrusions attempting to exploit known vulnerabilities

☑ Single Sign-On Mobility Agent
Provides FortiAuthenticator for transparent authentication

☑ Zero Trust Network Access ⊞
Enables FortiClient to receive a device certificate for tunneling traffic to Proxy Gateway and FortiOS.

☑ Privilege Access Management ⊞
Privilege Access Management

* ⊞ Windows-only features

Back | Next

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

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

c. **Linux and MacOS**: Install *Fortinet Privileged Access Agent* extension from the Chrome Web Store or follow the FortiPAM GUI prompt. Then use web-based launchers or web launcher to access the target server.
Note: ZTNA and Native launchers are not supported on extension-only systems.

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

a. **Windows**: After downloading and installing standalone FortiClient (7.2.0 or later) manually, most PAM features are supported.
Note: A standalone installer contains PAM in its filename such as `FortiClientPAMSetup_7.2.0.0xxx_x64.exe`.
Note: ZTNA is not supported.

b. **Linux and MacOS**: Install *Fortinet Privileged Access Agent* extension from the Chrome Web Store or follow the FortiPAM GUI prompt. Then use web-based launchers or web launcher to access the target server.
Note: ZTNA and Native launchers are not supported on extension-only systems.

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

a. **Windows**: Install *Fortinet Privileged Access Agent* extension from the Chrome Web Store or Microsoft Edge Add-ons. Then use web-based launchers or web launcher to access the target server.
Note: ZTNA and Native launchers are not supported on extension-only systems.

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

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

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

Feature availability

The following table lists FortiPAM 1.4.2 feature availability based on the type of deployment being used:

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

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

FortiPAM installation

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

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

The following virtualization environments are supported by FortiPAM 1.4.2:

- VMware ESXi/ ESX 6.5 and above
- KVM
- Microsoft Hyper-V
- Microsoft Azure
- GCP (Google Cloud Platform)
- AWS (Amazon Web Services)

FortiPAM supports both Linux and Windows environments.

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

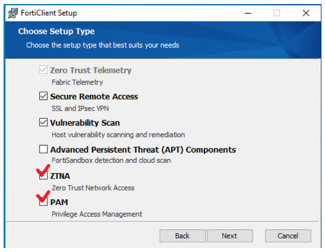
See Installing FortiClient with the FortiPAM feature on page 44 and FortiPAM appliance setup on page 45.

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.



FortiClient Setup

Choose Setup Type

Choose the setup type that best suits your needs

☑ Zero Trust Telemetry
Fabric Telemetry

☑ Secure Remote Access
SSL and IPsec VPN

☑ Vulnerability Scan
Host vulnerability scanning and remediation

☐ Advanced Persistent Threat (APT) Components
FortiSandbox detection and cloud scan

☑ ZTNA
Zero Trust Network Access

☑ PAM
Privilege Access Management

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

3. Reboot the PC.

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

Uninstalling FortiClient

To uninstall FortiClient:

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

FortiPAM appliance setup

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

FortiPAM-VM image installation and initial setup

See Appendix A: Installation on KVM on page 452.

See Appendix B: Installation on VMware on page 455.

See Appendix F: Installation on Hyper-V on page 465.

See Appendix G: Installation on Azure on page 476.

See Appendix J: Installation on AWS on page 492.

See Appendix K: Installation on GCP on page 505.

After FortiPAM is installed, FortiPAM listens using the following default ports:

- **HTTPS GUI**: `443`
- **Web proxy**: `8080`
  (If web proxy is enabled)

Ensure that ports `443` and `8080` are open if using a firewall before FortiPAM.

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 452.

   ```
   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 type physical
         set snmp-index 1
      next
      edit "port2"
         set ip x.x.x.x/x
         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
   ```

When upgrading a FortiPAM instance, use the following CLI command to enable synchronizing the virtual IP address to the IP address of the external interface:

```
Example

 config firewall vip
  set intf-ip-sync enable
  set extintf "port1" #The interface connected to the source network
that receives the packets forwarded to the destination network.
 end
```

When installing a new FortiPAM instance, the synchronization happens automatically.

4. Optionally, enable TPM or vTPM. See FortiPAM with TPM on page 47.
5. Optionally, to encrypt disk to protect logs and videos, see Configuring log and video disk encryption on page 347.
6. On a web browser, go to `https://172.16.xxx.xxx` to access FortiPAM GUI.
   To upload the FortiPAM license file, see Uploading the license file to FortiPAM-VM on page 52.
7. Optionally, enable displaying a login disclaimer message to show the last successful or failed login date and time:

   ```
   config system global
    set post-login-banner enable
   end
   ```

   For a detailed example on setting up the login disclaimer using the CLI console, see Disclaimers via the CLI on page 435.

   To set up the login disclaimer using the GUI, see the *Login Disclaimer* option in *System > Settings*.
8. After logging in to the FortiPAM GUI, go to *Log & Report* > *Email Alert Settings*, and:
   a. Select *Enable Email Notification*.
   b. Add receiver email addresses for critical system notifications in the *Critical System Notification* tab.
      See Email alert settings on page 351 and Email alert when the glass breaking mode is activated example on page 353.

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.

When using (v)TPM and disk encryption:

- On an evaluation license, use 2 GB of memory.
- On a formal license, use 4 GB of memory.

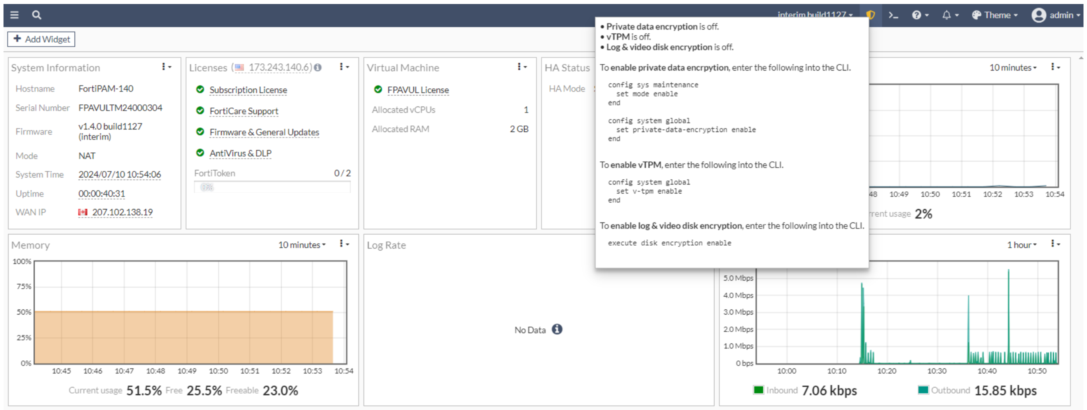
It is suggested that you enable TPM when you initially install FortiPAM.

Do not enable/disable (v)TPM and `private-data-encryption` frequently.

It is suggested that you backup your configuration before you disable or reenable (v)TPM or `private-data-encryption`.

If `private-data-encryption` is changed, backup the new data too.

FortiPAM displays private data, vTPM, and log/video disk encryption status in the banner.



- **Private data encryption** is off.
- **vTPM** is off.
- **Log & video disk encryption** is off.

To **enable private data encrpytion**, enter the following into the CLI.

```
config sys maintenance
  set mode enable
end

config system global
  set private-data-encryption enable
end
```

To **enable vTPM**, enter the following into the CLI.

```
config system global
  set v-tpm enable
end
```

To **enable log & video disk encryption**, enter the following into the CLI.

```
execute disk encryption enable
```

System Information

Hostname	FortiPAM-140
Serial Number	FPAVULTM24000304
Firmware	v1.4.0 build1127 (interim)
Mode	NAT
System Time	2024/07/10 10:54:06
Uptime	00:00:40:31
WAN IP	207.102.138.19

Licenses (173.243.140.6)

- ✓ Subscription License
- ✓ FortiCare Support
- ✓ Firmware & General Updates
- ✓ AntiVirus & DLP

FortiToken 0 / 2

Virtual Machine

- ✓ FPAVUL License

Allocated vCPUs	1
Allocated RAM	2 GB

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 460 and Appendix D: vTPM for FortiPAM on VMware on page 462.

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

To enable vTPM on FortiPAM-VM:

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

```
config system global
  set v-tpm enable
end
```

To enable TPM on FortiPAM-VM:

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

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

```
config sys maintenance
  set mode enable
end
config system global
  set private-data-encryption enable
end
```

```
 Be carefull!!!This operation will refresh all ciphered data!
Backup the current configuration file at first!
Do you want to continue? (y/n)y
Please type your private data encryption key (32 hexadecimal numbers):
0123456789abcdef0123456789abcdef
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
0123456789abcdef0123456789abcdef
Your private data encryption key is accepted.
```

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

To disable TPM:

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

```
config sys maintenance
  set mode enable
end
config system global
  set private-data-encryption disable
end
```

```
Be carefull!!!This operation will refresh all ciphered data!
+Backup the current configuration file at first!
+Do you want to continue? (y/n)y
```

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

To disable vTPM for FortiPAM-VM:

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

```
config system global
  set v-tpm disable
end
```

```
This operation will stop using vTPM module
Do you want to continue? (y/n)y
```

Connecting to target remote systems

Requirements to connect to a target server or PC:

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

Licensing

FortiPAM platforms work in evaluation mode until licensed.

In the evaluation mode:

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

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

Antivirus Scan and DLP are not supported under evaluation license.

Registering and downloading your license

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

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

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

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

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

Uploading the license file to FortiPAM-VM

There are two methods to upload the license file to FortiPAM-VM.

To upload the license via the FortiPAM-VM GUI:

You must be in maintenance mode to be able to upload a license. See Maintenance mode in Admin on page 30.

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.

To upload the license through the public IP address using SCP:

Use the following command:

```
scp <license_file> admin@<public_ip_address>:vmlicense
```

For example:

```
$ scp FPAVULTM23000007.lic admin@52.52.143.64:vmlicense
admin@52.52.143.64's password:
FPAVULTM23000xxx.lic 100% 9128 344.0KB/s 00:00
100-install VM license completed
```

License expiry and renewal

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

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

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

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

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

Follow the procedure as detailed in Renewing FortiPAM-VM license on page 55 to renew FortiPAM-VM license.

License status

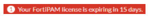
FortiPAM license status can be found in the *Licenses* widget available in *Dashboard* > *Status*. See Licenses widget on page 62.

Email alert for license expiration

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

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

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



Your FortiPAM license is expiring in 15 days.

To set up email alerts for license expiry:

1. Ensure that *Email Service* is set up in *System* > *Settings*. See Settings on page 373.
2. Go to *Log & Report* > *Email Alert Settings*, and select *Enable email notification*.
3. In the *Critical System Notification* tab:
   a. In *From*, enter the email address of the sender.
   b. In *To*, enter the email address of the receiver.
4. Click *Apply*.
   Alternatively, you can add an email address where the notification is sent when creating or editing a user in *User Management* > *User List* (*Configure User Details* tab).

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

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

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

Subscription license

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

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

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

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

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

Advanced Malware Protection (formerly AntiVirus and DLP license)

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

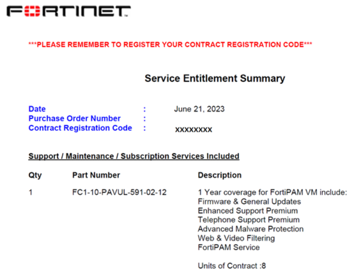
The Advanced Malware Protection (`AVDB & DLP`) licenses are related to the file scanning feature in file launchers. Once the Advanced Malware Protection license expires:

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

Renewing FortiPAM-VM license

To renew FortiPAM-VM license:

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



PLEASE REMEMBER TO REGISTER YOUR CONTRACT REGISTRATION CODE

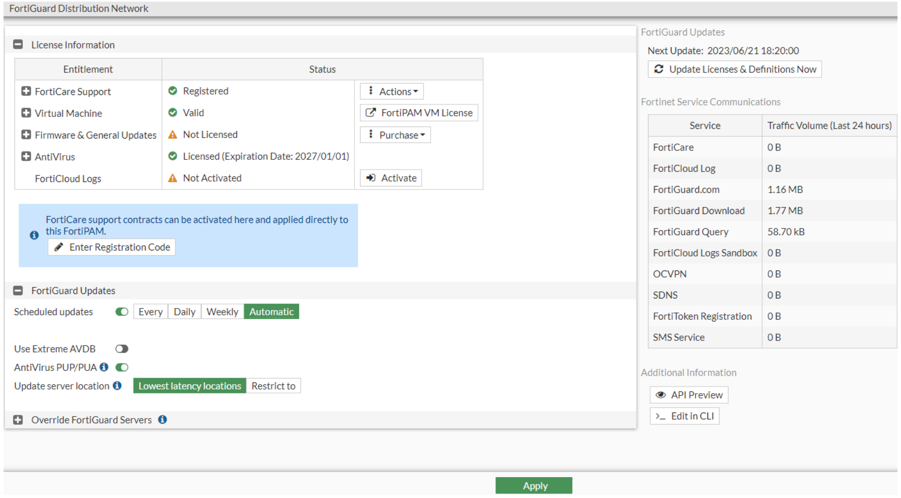
Service Entitlement Summary

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

Support / Maintenance / Subscription Services Included

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

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



FortiGuard Distribution Network

License Information

Entitlement	Status	
FortiCare Support	Registered	Actions
Virtual Machine	Valid	FortiPAM VM License
Firmware & General Updates	Not Licensed	Purchase
AntiVirus	Licensed (Expiration Date: 2027/01/01)	
FortiCloud Logs	Not Activated	Activate

FortiCare support contracts can be activated here and applied directly to this FortiPAM.

FortiGuard Updates

Scheduled updates: Automatic

Use Extreme AVDB: off

AntiVirus PUP/PUA: on

Update server location: Lowest latency locations

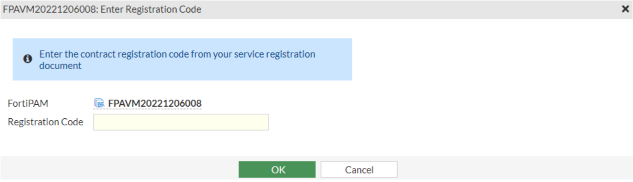
FortiGuard Updates

Next Update: 2023/06/21 18:20:00

Fortinet Service Communications

Service	Traffic Volume (Last 24 hours)
FortiCare	0 B
FortiCloud Log	0 B
FortiGuard.com	1.16 MB
FortiGuard Download	1.77 MB
FortiGuard Query	58.70 kB
FortiCloud Logs Sandbox	0 B
OCVPN	0 B
SDNS	0 B
FortiToken Registration	0 B
SMS Service	0 B

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



FPAVM20221206008: Enter Registration Code

Enter the contract registration code from your service registration document

FortiPAM: FPAVM20221206008
Registration Code:

iii. In *Registration Code*, enter the *Contract Registration Code* that you saved in step 2.

iv. Click *OK*.

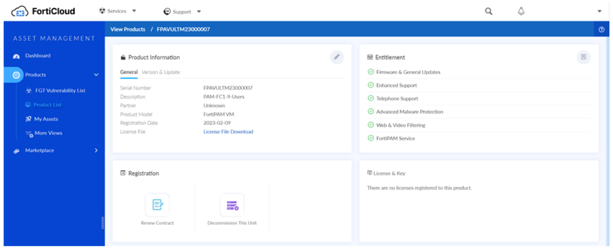
v. Click *Apply*.

b. **Registering directly on FortiCloud**:

i. Go to FortiCloud and create a new account or log in with an existing account.
The *Asset Management* portal opens.

ii. Go to *Products > Product List*.

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



Product Information

General | Version & Update

Serial Number	FPAVULTM23000007
Description	PAM-FC1-9-Users
Partner	Unknown
Product Model	FortiPAM VM
Registration Date	2023-02-09
License File	License File Download

Entitlement

- Firmware & General Updates
- Enhanced Support
- Telephone Support
- Advanced Malware Protection
- Web & Video Filtering
- FortiPAM Service

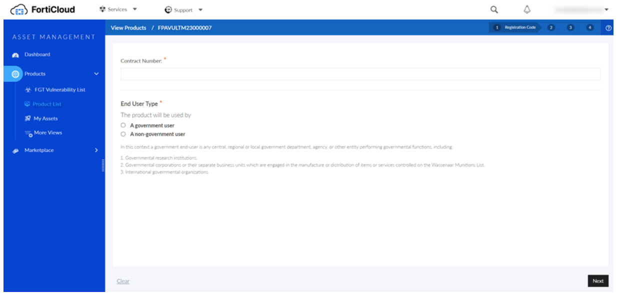
Registration

License & Key

There are no licenses registered to this product.

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

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



Contract Number: *

End User Type *

The product will be used by

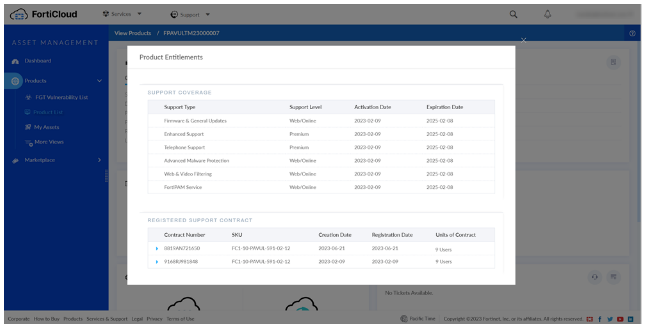
○ A government user
○ A non-government user

In this context a government end-user is any central, regional or local government department, agency, or other entity performing governmental functions, including:

1. Governmental research institutions.
2. Governmental corporations or their separate business units which are engaged in the manufacture or distribution of items or services controlled on the Wassenaar Munitions List.
3. International governmental organizations.

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

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



FortiCloud
Services
Support
ASSET MANAGEMENT
Dashboard
Products
FGT Vulnerability List
Product List
My Assets
More Views
Marketplace
View Products / FPAVULTM23000007
No Tickets Available.
Corporate How to Buy Products Services & Support Legal Privacy Terms of Use
Pacific Time
Copyright ©2023 Fortinet, Inc. or its affiliates. All rights reserved.

Product Entitlements

SUPPORT COVERAGE

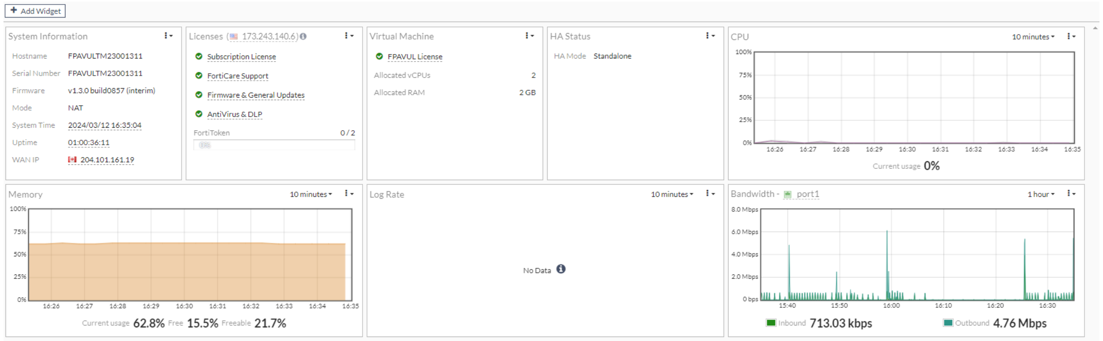
Support Type	Support Level	Activation Date	Expiration Date
Firmware & General Updates	Web/Online	2023-02-09	2025-02-08
Enhanced Support	Premium	2023-02-09	2025-02-08
Telephone Support	Premium	2023-02-09	2025-02-08
Advanced Malware Protection	Web/Online	2023-02-09	2025-02-08
Web & Video Filtering	Web/Online	2023-02-09	2025-02-08
FortiPAM Service	Web/Online	2023-02-09	2025-02-08

REGISTERED SUPPORT CONTRACT

Contract Number	SKU	Creation Date	Registration Date	Units of Contract
8819AN721650	FC1-10-PAVUL-591-02-12	2023-06-21	2023-06-21	9 Users
9168RJ981848	FC1-10-PAVUL-591-02-12	2023-02-09	2023-02-09	9 Users

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.



+ Add Widget

System Information

Hostname FPAVULTM23001311
Serial Number FPAVULTM23001311
Firmware v1.3.0 build0857 (interim)
Mode NAT
System Time 2024/03/12 16:35:04
Uptime 01:00:36:11
WAN IP 204.101.161.19

Licenses (173.243.140.6)

✓ Subscription License
✓ FortiCare Support
✓ Firmware & General Updates
✓ AntiVirus & DLP

FortiToken 0 / 2

Virtual Machine

✓ FPAVUL License
Allocated vCPUs 2
Allocated RAM 2 GB

HA Status

HA Mode Standalone

CPU

Current usage 0%

Memory

Current usage 62.8% Free 15.5% Freeable 21.7%

Log Rate

No Data

Bandwidth - port1

🟩 Inbound 713.03 kbps
🟩 Outbound 4.76 Mbps

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

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

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

System Information	Displays basic information about the FortiPAM system including host name, serial number, firmware version, mode, system time, uptime, and WAN IP address. From this widget you can manually update the FortiPAM firmware to a different release. See Uploading a firmware on page 31 and System information widget on page 60. You can also configure system settings using this widget. For information on system settings, see Settings on page 373.
Licenses	Displays the status of your license and FortiGuard subscriptions. See Licenses widget on page 62.
Virtual Machine	Displays license information, number of allocated vCPUs, and how much RAM has been allocated. See VM license on page 66.
HA status	Displays HA mode. See High availability on page 389.
CPU	The real-time CPU usage is displayed for different time frames. Select the time frame from the dropdown at the top of the widget. Hovering over any point on the graph displays the average CPU usage along with a time stamp.

	To see per core CPU usage, select the CPU widget and click *Show per core CPU usage*.
Memory	Real-time memory usage is displayed for different time frames. Select the time frame from the dropdown at the top of the widget. Hovering over any point on the graph displays the percentage of memory used along with a time stamp.
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 344.
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.

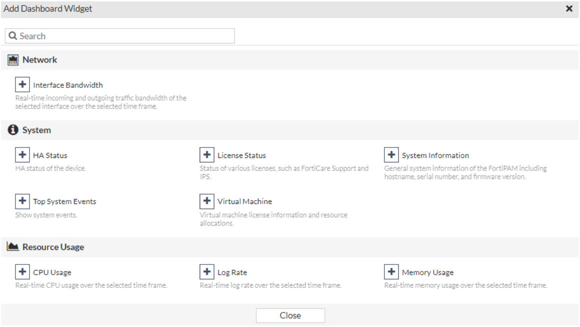
You can add the following *Resource Usage* widgets to the *Dashboard*:

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.

Adding a widget to a dashboard

To add a widget to a dashboard:

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



Add Dashboard Widget ✕

Search

Network

+ Interface Bandwidth
Real-time incoming and outgoing traffic bandwidth of the selected interface over the selected time frame.

System

+ 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.

Resource Usage

+ 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.

Close

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

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

4. Click *Add Widget*.

Widget actions

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

Resize	Select and then select the number of squares you want to extend the widget to.
Settings	Select and then in *Edit Dashboard Widget* - `Widget Name`, specify the *Fabric Member*, interface (if available), and click *OK*. Select from the following options: • *Default*: Uses the current fabric member. • *Specify*: Select a fabric member from the FortiPAM dropdown, i.e., a FortiPAM instance.

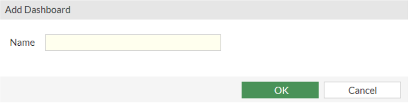
	Choosing a specific fabric member for this widget will override the behavior for the entire dashboard. After this is done, the fabric member selection is on each individual widget. • *Interface*: From the dropdown, select an interface or create a new interface.
Remove	Select *x* to remove the widget.

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

Adding a custom dashboard

To add a custom dashboard:

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

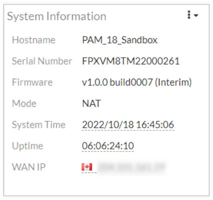
   Add Dashboard

   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 61.
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 31.
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 61.
Uptime	The duration of time FortiPAM has been running since it was last started or restarted.
WAN IP	The WAN IP address and location. Additionally, if the WAN IP is blocked in the FortiGuard server, there is a notification in the notification area, located in the upper right-hand corner of the *Dashboard*. Clicking on the notification opens a window with the relevant blocklist information.

Changing the host name

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

To change the host name:

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

Configuring the system date, time, and time zone

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

To configure the date and time manually:

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

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

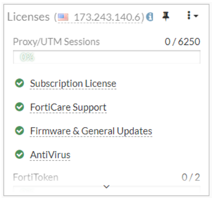
1. Go to *Dashboard* > *Status*.
2. Select the *System Information* widget and then click *Configure settings in System* > *Settings*.
3. From the *Time Zone* dropdown, select a timezone.
4. In *Set Time*, select *NTP*.
5. In *Select Server*, either select *Fortiguard* or *Custom*.
   If you select *Custom*,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

   Custom server details must be configured in the CLI.

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

Licenses widget

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



Licenses (173.243.140.6)

Proxy/UTM Sessions 0 / 6250

0%

✓ Subscription License

✓ FortiCare Support

✓ Firmware & General Updates

✓ AntiVirus

FortiToken 0 / 2

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

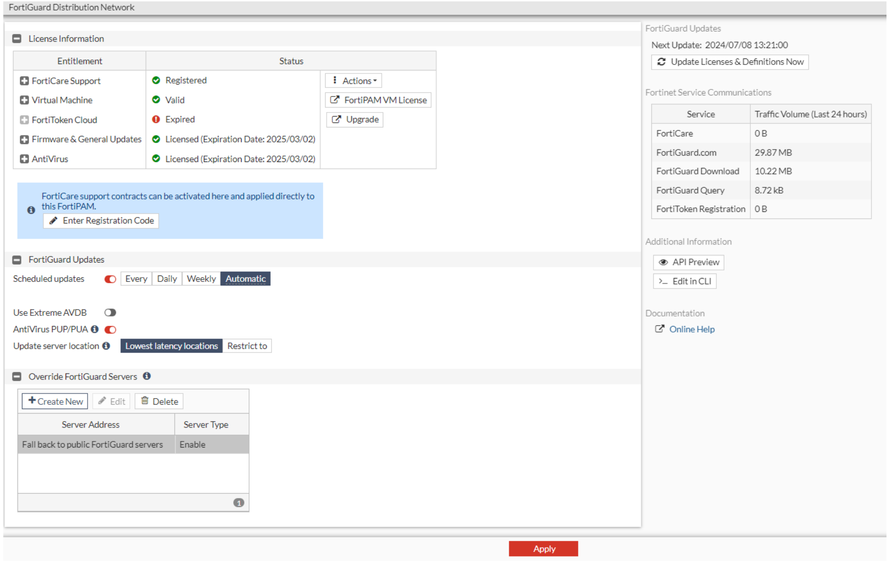
To view details on licenses, see FortiGuard Distribution Network on page 62.

FortiGuard Distribution Network

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

To view and configure FortiGuard connections:

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



FortiGuard Distribution Network

License Information

Entitlement	Status	
FortiCare Support	Registered	Actions
Virtual Machine	Valid	FortiPAM VM License
FortiToken Cloud	Expired	Upgrade
Firmware & General Updates	Licensed (Expiration Date: 2025/03/02)	
AntiVirus	Licensed (Expiration Date: 2025/03/02)	

FortiCare support contracts can be activated here and applied directly to this FortiPAM.

Enter Registration Code

FortiGuard Updates

Scheduled updates: Every | Daily | Weekly | Automatic

Use Extreme AVDB

AntiVirus PUP/PUA

Update server location: Lowest latency locations | Restrict to

Override FortiGuard Servers

Create New | Edit | Delete

Server Address	Server Type
Fall back to public FortiGuard servers	Enable

FortiGuard Updates

Next Update: 2024/07/08 13:21:00

Update Licenses & Definitions Now

Fortinet Service Communications

Service	Traffic Volume (Last 24 hours)
FortiCare	0 B
FortiGuard.com	29.87 MB
FortiGuard Download	10.22 MB
FortiGuard Query	8.72 kB
FortiToken Registration	0 B

Additional Information

API Preview

Edit in CLI

Documentation

Online Help

Apply

3. The following settings are available in the window:

License Information	
FortiCare Support	The availability or status of your unit’s support contract. You can update your registration status by selecting *Enter Registration Code* and loading the license file from a location on your computer. From the *Actions* dropdown: • Select *Login to My Account* to log in to FortiCloud. • Select *Transfer FortiPAM to Another Account* to transfer this FortiPAM device to another FortiCloud account. Fill in the verification details and then review and transfer the device.
Virtual Machine	To upload or check your virtual machine license, select *FortiPAM VM License*. See Uploading a license file.
FortiToken Cloud	Select *Activate free trial* to activate the free trial with 5 FortiToken Cloud tokens. The trial license is available for 30 days only. When in trial or when the license has expired, select *Upgrade* to see instructions on how to add a valid license. You can see the FortiToken Cloud license status. When the license has expired, you cannot use FortiToken Cloud and *FortiToken Cloud* entitlement is marked *Expired* when the license has expired.

Firmware & General Updates

Displays the status of *Application Control Signatures*, *Device & OS Identification*, and *Internet Service Database Definitions*.

To upgrade the database:

1. From the *Actions* dropdown, select *Upgrade Database*.
2. Select *Upload* and locate the application control signatures file from your computer.
3. Select *OK*.

From the *Actions* dropdown, select *View List* to see a list of application control signatures.

To purchase upgrades, select *Enter Registration Code* from the *Purchase* dropdown, enter the *Registration Code* in the new window, and click *OK*.

Antivirus

The FortiGuard AntiVirus Service provides fully automated updates to ensure protection against the latest content level threats. It employs advanced virus, spyware, and heuristic detection engines to prevent both new and evolving threats from gaining access to your network and protects against vulnerabilities.

To renew the AntiVirus service, select *Enter Registration Code* from the *Renew* dropdown, enter the *Registration Code* in the new window, and click *OK*.

FortiCloud Logs

To activate FortiCloud logs:

1. Select *Activate*.
2. Confirm the password of your FortiCloud account.
3. Select from the following domains:
   - *Europe*
   - *US*
   - *Global*
4. Ensure that *Send logs to FortiCloud Logs* is enabled.
5. Click *OK*.

FortiGuard Updates

Scheduled updates

Enable to receive scheduled updates and then select when the updates occur: Every *1-23* hours, *Daily* at a specific hour, or *Weekly* on a specific day at a specific hour, or automatically within every one hour period.

Note: The option is enabled by default.

Use Extreme AVDB

Note: The option is disabled by default.

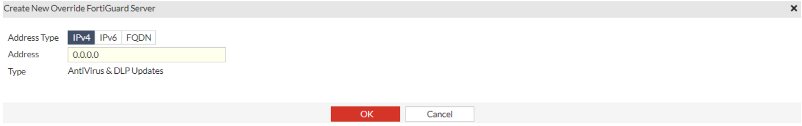
AntiVirus PUP/PUA	Enable antivirus grayware checks for potentially unwanted applications. **Note**: The option is enabled by default.
Update server location	Update the FortiGuard server location to: • *Lowest latency locations* or • Restrict to: • *US only* • *EU only* ⚠ Changing the server location overrides all FortiGuard/FortiCloud/FortiCare servers.
Override FortiGuard Servers By default, the FortiPAM unit updates signature packages and queries rating servers using public FortiGuard servers. You can override this list of servers. You can also disable communication with public FortiGuard servers. See Override FortiGuard Servers on page 65.	

4. Click *Apply*.

Override FortiGuard Servers

To override FortiGuard servers

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



Create New Override FortiGuard Server

Address Type: IPv4 | IPv6 | FQDN

Address: 0.0.0.0

Type: AntiVirus & DLP Updates

2. Enter the following information:

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

3. Click *OK*.

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

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

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

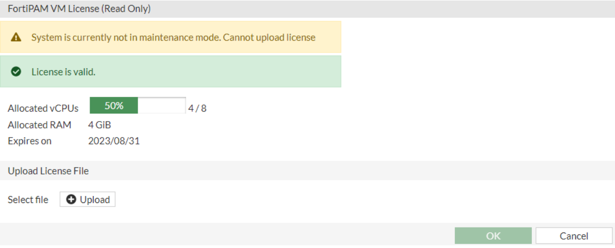
To update the licenses and definition immediately, select *Update Licenses & Definitions Now*.

VM license

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

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

You must be in maintenance mode to be able to upload a license. See Maintenance mode in Admin on page 30.



FortiPAM VM License (Read Only)

⚠ System is currently not in maintenance mode. Cannot upload license

✓ License is valid.

Allocated vCPUs 50% 4 / 8

Allocated RAM 4 GiB

Expires on 2023/08/31

Upload License File

Select file

To upload a license, see Uploading a license.

Secrets

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

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

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

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

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

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

- *Owner*
- *Edit*
- View (Only for users with roles where *View Encrypted Information* is enabled)

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 Telnet, Web RDP, Web VNC, Web SMB, Web SFTP, and Web Account.

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

- Secrets on page 69
- Targets on page 113
- Gateway on page 124
- Personal/public folder on page 135
- My requests list on page 143
- Approval list on page 148
- Job list on page 151
- Discovery on page 154

Secrets

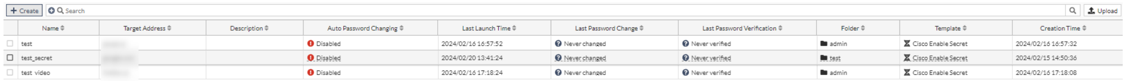
Secrets in *Secrets* displays a list of configured secrets.

To access any of the secrets, you require *Secrets* access.

No matter what permissions the secrets are provided, the secrets are not available anymore if the access control for *Secrets* in the *Role* page is set to *None*. See Role on page 278.

For each secret, the following columns are displayed by default:

- *Name*
- *Target Address*
- *Description*
- *Auto Password Changing*
- *Last Launch Time*
- *Last Password Change*
- *Last Password Verification*
- *Folder*
- *Template*
- *Creation Time*



+ Create | Search | Upload

	Name	Target Address	Description	Auto Password Changing	Last Launch Time	Last Password Change	Last Password Verification	Folder	Template	Creation Time
□	test	[redacted]		Disabled	2024/02/16 16:57:52	Never changed	Never verified	admin	Cisco Enable Secret	2024/02/16 16:57:32
□	test_secret	[redacted]		Disabled	2024/02/20 13:41:24	Never changed	Never verified	test	Cisco Enable Secret	2024/02/15 14:50:36
□	test video	[redacted]		Disabled	2024/02/16 17:18:24	Never changed	Never verified	admin	Cisco Enable Secret	2024/02/16 17:18:08

The *Description* column is not visible by default.

To display the *Description* column, select *Configure Table* icon as you click the header for the left-most column, select *Description* and then click *Apply*.

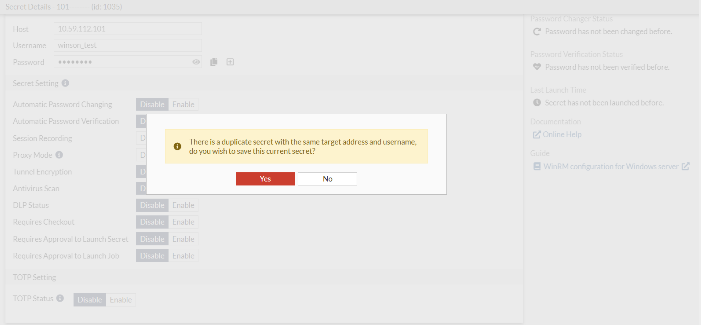
The *Last Password Verification* column gives an overview of the secret password status.

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

Name ⇕

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

The *Secrets List* tab contains the following options:

Create	Select to create a new secret. See Creating a secret on page 72. Starting FortiPAM 1.4.0, you now receive a secret duplication warning when you create or edit a secret with target address and user name of an existing secret. This helps avoid password conflicts. If there are duplicate secrets (the same target address and user name) and one secret password is changed, the other secret may not launch as the target password has already been updated.  Secret Details - 101-------- (id: 1035) Host 10.59.112.101 Username winson_test Password •••••••• Secret Setting Automatic Password Changing: Disable Enable Automatic Password Verification Session Recording Proxy Mode Tunnel Encryption Antivirus Scan DLP Status: Disable Enable Requires Checkout: Disable Enable Requires Approval to Launch Secret: Disable Enable Requires Approval to Launch Job: Disable Enable TOTP Setting TOTP Status: Disable Enable There is a duplicate secret with the same target address and username, do you wish to save this current secret? Yes No Password Changer Status Password has not been changed before. Password Verification Status Password has not been verified before. Last Launch Time Secret has not been launched before. Documentation Online Help Guide WinRM configuration for Windows server
Upload	Select and then select *Upload Secret* to upload secrets using the secret upload template file, or download the secret upload template by selecting *Download Template*. See Uploading secrets using the secret upload template on page 99.
Edit	Select to edit the selected secret.

	When a secret request is approved, the *Launcher Status* timer shows the remaining time till you (as a requester) have access to the secret when you double-click to open the secret in *Secrets* > *Secrets*. When editing a secret, click *Discard Changes* to discard all the changes you made.
Move	Select to move the selected secret.
Delete	Select to delete the selected secrets.
Clone	Select to clone the selected secret.
Add favorite	Select to add the selected secret to the favorite folder.
Remove favorite	Select to remove the selected secret from the favorite folder.
Launch Secret	Launch the selected secret. See Launching a secret on page 97.
Make Request	Make request to launch or perform a job on the secret. Make a request on page 145.
Search	Enter a search term in the search field, then hit `Enter` to search the secrets list. To narrow down your search, see Column filter. The following column filters are available: • *Name* • *Target Address* • *Description* • *Auto Password Changing* • *Last Launch Time* • *Last Password Change* • *Last Password Verification* • *Folder* • *Template* • *Creation Time* • *ID*

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

Creating a secret

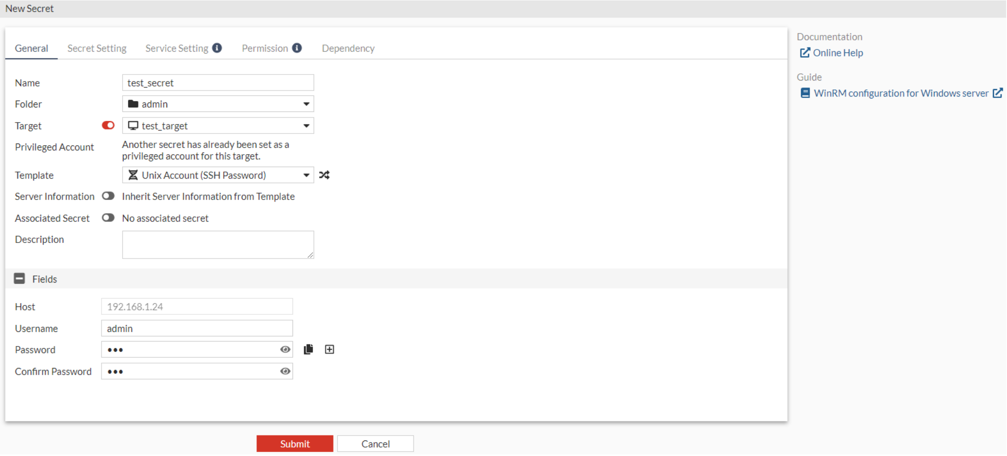
To create a secret:

1. Go to *Secrets* > *Secrets*.
   Alternatively, go to *Personal Folder/Public Folder* in *Secrets*, select *Open Tree*, locate the folder where you intend to add the secret, and click *Open*.

   From the *Create* dropdown, select *Secret*, and skip to step 6.
2. In *Secrets*, 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.

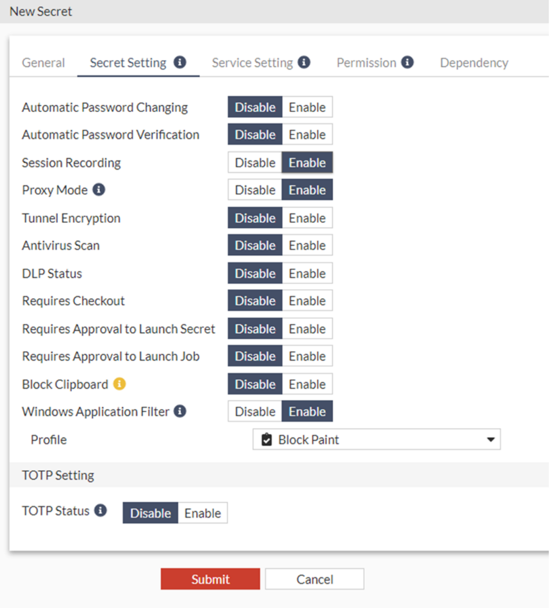
4. Select *Create*.
   The *General* tab opens.



Name: test_secret
Folder: admin
Target: test_target
Privileged Account: Another secret has already been set as a privileged account for this target.
Template: Unix Account (SSH Password)
Server Information: Inherit Server Information from Template
Associated Secret: No associated secret
Description:

Host: 192.168.1.24
Username: admin
Password: •••
Confirm Password: •••

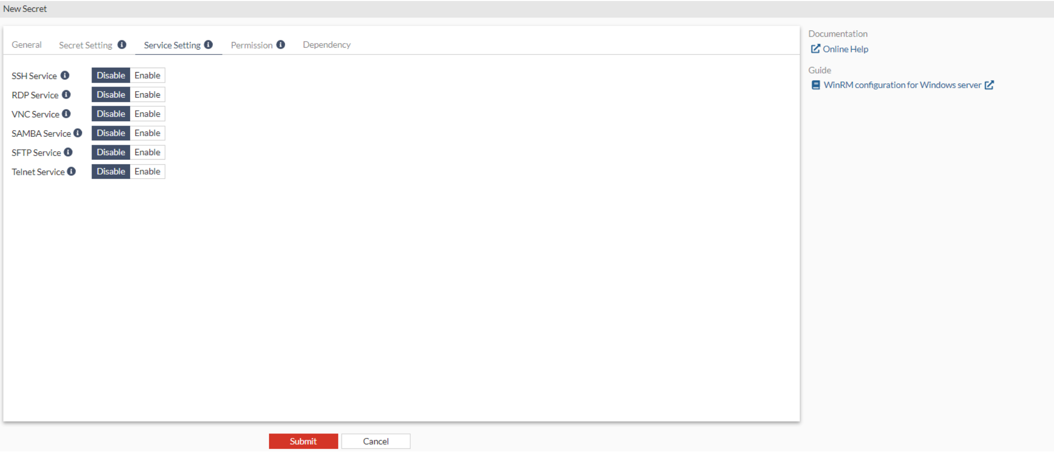
5. To switch to *Secret Setting*, *Service Setting*, *Permission*, or *Dependency* tabs, select the tab.



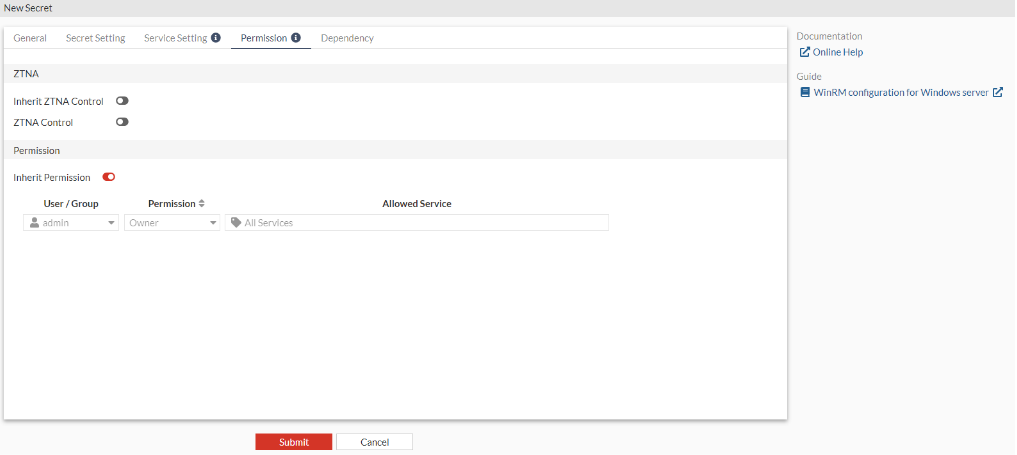
Automatic Password Changing	[✓ Disable] Enable
Automatic Password Verification	[✓ Disable] Enable
Session Recording	Disable [✓ Enable]
Proxy Mode	Disable [✓ Enable]
Tunnel Encryption	[✓ Disable] Enable
Antivirus Scan	[✓ Disable] Enable
DLP Status	[✓ Disable] Enable
Requires Checkout	[✓ Disable] Enable
Requires Approval to Launch Secret	[✓ Disable] Enable
Requires Approval to Launch Job	[✓ Disable] Enable
Block Clipboard	[✓ Disable] Enable
Windows Application Filter	Disable [✓ Enable]
Profile	Block Paint

TOTP Setting

TOTP Status	[✓ Disable] Enable



SSH Service	[✓ Disable] Enable
RDP Service	[✓ Disable] Enable
VNC Service	[✓ Disable] Enable
SAMBA Service	[✓ Disable] Enable
SFTP Service	[✓ Disable] Enable
Telnet Service	[✓ Disable] Enable



ZTNA

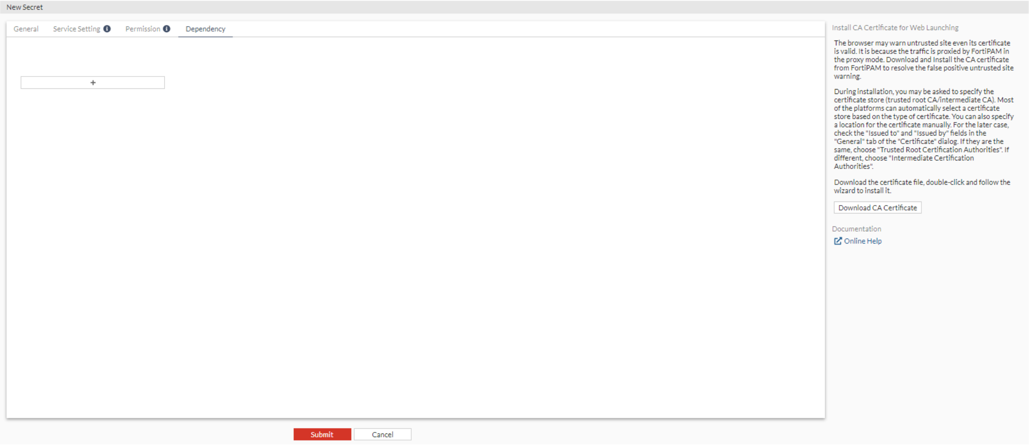
Inherit ZTNA Control ○

ZTNA Control ○

Permission

Inherit Permission ●

User / Group	Permission	Allowed Service
admin	Owner	All Services



Install CA Certificate for Web Launching

The browser may warn untrusted site even its certificate is valid. It is because the traffic is proxied by FortiPAM in the proxy mode. Download and Install the CA certificate from FortiPAM to resolve the false positive untrusted site warning.

During installation, you may be asked to specify the certificate store (trusted root CA/intermediate CA). Most of the platforms can automatically select a certificate store based on the type of certificate. You can also specify a location for the certificate manually. For the later case, check the "Issued to" and "Issued by" fields in the "General" tab of the "Certificate" dialog. If they are the same, choose "Trusted Root Certification Authorities". If different, choose "Intermediate Certification Authorities".

Download the certificate file, double-click and follow the wizard to install it.

Documentation

Online Help

6. Enter the following information:

Name	Name of the secret.
Folder	The folder where the secret is added. See Personal/public folder on page 135. The folder is already selected in step 2. Use the dropdown, if you want to change the folder.
Target	Enable and then from the dropdown, select a target for the new secret being created. In the dropdown, select + to create a new target. See Creating a target on page 114. The *Default Template* from the target will automtaically be used as *Template* for the secret. If the *Default Template* is updated later on, the *Template* for the secret will not be automatically updated. It must be updated by editing the secret. See To change the template after selecting one: on page 75.
Privileged Account	Select *Yes* or *No* to indicate if the secret is for a privilege account. This option is only available when a *Target* is selected. If the target already has a secret set as privileged account, you cannot set a new secret as a privileged account for the target.
Gateway	A gateway is selected if the associated target includes a gateway. A gateway, e.g., a FortiGate or a FortiProxy device, is used when a target is not reachable directly from FortiPAM. It allows you to proxy the connection to the target. See Gateway on page 124.

	The option is non-editable. The option is only available when you select a target with gateway included. See Creating a target on page 114.
Template	From the dropdown, select a template. Select *Create* to create a new template. See Creating secret templates on page 165. **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*.
Server Information	Disable to inherit server information from the *Template*. Enable to select general type of server to which the secret is intended to connect: • *Unix-Like* • *Cisco* • *FortiOS* • *Other*
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. See Use cases for associated secrets on page 90. **Note**: The option is disabled by default.
Launch with Associated Secret Credentials	When the option is enabled, associated secret credential information is used for launching a secret. The credential information stored in the primary secret is not used. You must ensure that all the required information is stored in the associated secret.

The option is only available when *Associated Secret* is enabled.

Description

Optionally, enter a description.

Fields

Enter a value in a field.

For the *Password* field, click the *Generate* button to automatically generate the password following the password policy set in Password policies on page 217.

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.

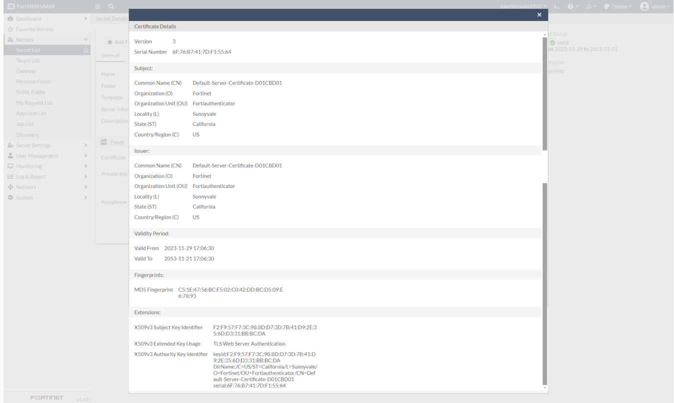
Certificate

You can create secrets to store certificates.

Select *Upload* and from the management computer locate the certificate and select *Open*.

Click the download icon to download the uploaded certificate.

When editing a secret created using the *Certificate Vault* template, click the view icon to view the uploaded certificate.



Certificate Details

Version 3
Serial Number 6F:76:B7:41:7D:F1:55:64

Subject:

Common Name (CN) Default-Server-Certificate-D01CBD01
Organization (O) Fortinet
Organization Unit (OU) Fortiauthenticator
Locality (L) Sunnyvale
State (ST) California
Country/Region (C) US

Issuer:

Common Name (CN) Default-Server-Certificate-D01CBD01
Organization (O) Fortinet
Organization Unit (OU) Fortiauthenticator
Locality (L) Sunnyvale
State (ST) California
Country/Region (C) US

Validity Period:

Valid From 2023-11-29 17:06:30
Valid To 2053-11-21 17:06:30

Fingerprints:

MD5 Fingerprint C5:1E:47:56:BC:F5:02:C0:42:DD:BC:D5:09:E6:78:93

Extensions:

X509v3 Subject Key Identifier F2:F9:57:F7:3C:98:8D:D7:3D:7B:41:D9:2E:35:6D:D3:31:BB:BC:DA
X509v3 Extended Key Usage TLS Web Server Authentication
X509v3 Authority Key Identifier keyid:F2:F9:57:F7:3C:98:8D:D7:3D:7B:41:D9:2E:35:6D:D3:31:BB:BC:DA
DirName:/C=US/ST=California/L=Sunnyvale/O=Fortinet/OU=Fortiauthenticator/CN=Default-Server-Certificate-D01CBD01
serial:6F:76:B7:41:7D:F1:55:64

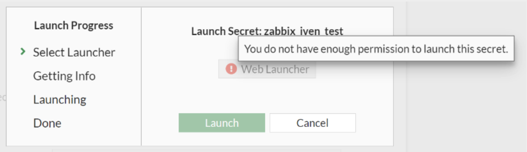
Click the delete icon to delete the uploaded certificate.

	Notes: - The option is only available when the *Template* is *Certificate Vault*. - Other fields for a secret created using the *Certificate Vault* template include *Private-key* and *Passpharse*. You can set email alerts for expiring certificates. See the *Certificate* tab in Email alert settings on page 351.
Launcher	From the list, you can use a launcher to launch the secret.
Secret Setting	

Some settings may not be configurable as they are protected by the policy that applies to the folder where the secret is added.

The owner of the secret must configure password verification and change settings before the secret utilizes the password changer and password verification. However, a user can manually trigger these actions if they have sufficient permissions.

Automatic Password Changing	Enable/disable automatic password changing. When enabled, password changer for secrets is activated to periodically change the password.
Recursive	Displays the password changing schedule based on your selections for the related settings.
Start Time	The date and time when the recurring schedule begins. Enter date (MM/DD/YYYY) and time or select the *Calendar* icon and then select a date and time.
Recurrence	From the dropdown, select from the following three frequencies of recurrence: - *Daily* - *Weekly* - *Monthly*
Repeat every	The number of days/weeks/months after which the password is changed (1-400).
Occurs on	Select from the following days of the month when the password is automatically changed: - *First* - *Second* - *Third* - *Last* - *Last Day* - *Day*

	When you select *Day*, select + to add days of the month when the password is automatically changed. Select days of the week when the password is automatically changed. **Note**: The option is only available when *Recurrence* is set as *Weekly* or *Monthly*.
Automatic Password Verification	Enable/disable automatic password verification. When enabled, password changer for secrets is activated to periodically verify the password, and check if the target server is still available.
Interval (min)	The time interval at which the secret passwords are tested for accuracy, in minutes (default = 60, 5 - 44640).
Start Time	The date and time when the *Interval(min)* begins. Enter date (MM/DD/YYYY) and time or select the *Calendar* icon and then select a date and time.
Session Recording	Enable/disable session recording. When enabled, user action performed on the secret is recorded. The video file is available in the log for users with appropriate permission. See Over-the-shoulder monitoring (Live recording) on page 310.
Proxy Mode	Enable/disable the proxy mode. When enabled, FortiPAM is responsible to proxy the connection from the user to the secret. In the proxy mode: • Web launcher is available to users who have the permission to view the secret password. • Web launcher is disabled for users who do not have the permission to view the secret password. When disabled, the non-proxy (direct) mode is used. See Modes of operation on page 38. 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:  Launch Secret: zabbix_iven_test You do not have enough permission to launch this secret. Launch Progress Select Launcher Getting Info Launching Done Web Launcher Launch Cancel

Web Proxy

Enable/disable the web proxy feature.

When accessing a target using the FortiPAM browser extension, the browser extension sends the browser requests through the FortiPAM web proxy. FortiPAM dynamically operates on the web browser tab's PAC rule (on Google Chrome and Microsoft Edge) to successfully proxy the traffic to FortiPAM based on the configured domain. On Mozilla Firefox, FortiPAM sends the request to the web proxy instead.

FortiPAM scans the incoming web traffic and can replace the password.

> Using web proxy, you do not require FortiClient to launch the proxied web account secret.

To enable the web proxy feature, you must first enable the feature globally for the interface that handles incoming and outgoing traffic using the following CLI commands:

```
config system interface
 edit "port1"
  set explicit-web-proxy enable #must be enabled
 next
end
```

Alternatively, you can enable the feature by enabling *Explicit web proxy* for the interface that handles incoming and outgoing traffic. See Editing an interface on page 358.

Notes:

- The option is only available when *Proxy Mode* is enabled.
- The *Web Proxy* option is inherited from the secret target. See Creating a target on page 114.
- When you edit the *Web Proxy* option, you are editing the *Web Proxy* option available from within the associated secret target.

Tunnel Encryption

Enable/disable tunnel encryption.

When launching a native launcher, FortiClient creates a tunnel between the endpoint and FortiPAM. The protocol stack is HTTP/TLS/TCP.

The HTTP request gives information on the target server then FortiPAM connects to the target server. After that, two protocol options exist for the tunnel between FortiClient and FortiPAM. One is to clear the TLS layer for better throughput and performance. The other is to keep the TLS layer. The launcher's protocol traffic is inside the TLS secure tunnel.

If the launcher's protocol is not secure, like VNC, it is strongly recommended to enable this option so that the traffic is in a secure tunnel.

	When there is an HTTPS Man In The Middle device, e.g., FortiGate or FortiWeb between FortiClient and FortiPAM, you must enable the *Tunnel Encryption* option. Otherwise, the connection will be disconnected, and the launching will fail.
DLP Status	Enable/disable DLP. See Data loss prevention (DLP) protection for secrets on page 225.
DLP Profile	From the dropdown, select a DLP profile.
Antivirus Scan	Enable/disable antivirus scan. When enabled, it enforces an antivirus profile on the secret. See AntiVirus on page 221.
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 98.
Checkout Duration	The checkout duration, in minutes (default = 30, 3 - 120).
Checkin Password Change	Enable/disable automatically changing the password when the user checks in.
Renew Checkout	Enable/disable renewing checkouts.
Max Renew Count	When *Renew Checkout* is enabled, enter the maximum number of renewals allowed for the user with exclusive access to the secret (default = 1, 1 - 5).
Requires Approval to Launch Secret	Enable/disable requiring approval to launch a secret. When enabled, users must request permission from the approvers defined in the approval profile before gaining access. From the dropdown, select an approval profile. Use the search bar to look up an approval profile. Use the pen icon next to the approval profile to edit it. See Make a request on page 145 and Approval flow on page 199.

Requires Approval to Launch Job	When enabled, users must request permission from the approvers defined in the approval profile before executing a job on a secret. From the dropdown, select an approval profile. Use the search bar to look up an approval profile. Use the pen icon next to the approval profile to edit it. See Make a request on page 145 and Approval flow on page 199.
Bypass Approval	Enable/disable secret owners to bypass the secret request/approval process, i.e., secret owners do not require approval to launch secrets they own, given that *Bypass Approval* is enabled. **Note**: The option is disabled by default and only available when *Requires Approval to Launch Job* is enabled.
Block Clipboard	When enabled, for the following launchers, you cannot copy content from the launched secret web page: • *Web Launcher* • *Web SSH* • *Web Telnet* • *Web SMB* • *Web SFTP* When enabled, copying content from the remote computer to the local computer is blocked for the following launchers, but does not affect copy/paste on the remote computer itself: • *Web RDP* • Native *RDP* The feature needs Microsoft Edge and Google Chrome extension V3.
Windows App Filter	Enable and from the *Profile* dropdown select a Windows application filter. See Window app filter on page 242.
Log Expiring Certificate	Enable/disable generating a log for an expiring certificate. **Notes**: • By default, the option is enabled. • The option is only available when the *Template* is *Certificate Vault*.

	Disabling *Log Expiring Certificate* stops the generation of log entries for an expiring certificate. In addition, email alerts for expiring certificates are stopped if you disable this option.
TOTP Setting Enable/disable TOTP (Time-based one-time password) for the secret. TOTP is used when the target server requires TOTP as the 2FA. To configure TOTP settings via the CLI, see Configuring TOTP settings via the secret CLI commands Example on page 92. See Limitations of TOTP on FortiPAM on page 171. **Note**: The option is disabled by default.	
Verification Code with	The verification code issued by: • *3rd Party* (default) • *FortiToken* **Note**: The option is only available when TOTP status is enabled.
Shared Key	The TOTP key from the target server or any other 3rd party authenticator. The TOTP key is usually a binary string and delivered in `base64`/`base32` encoding format. Use the eye icon to hide/unhide the shared key. **Note**: The option is only available when the *Verification Code with* is set as *3rd Party*.
Activation Code	The FortiToken Mobile activation code. When using FortiToken Mobile as the TOTP mobile application, an activation code from the FortiToken Mobile token issuer is required to activate the token. In that case, you must provide the activation token, and FortiPAM then acts as a surrogate for the FortiToken Mobile application. FortiToken TOTP can only be configured via the GUI. **Note**: The option is only available when *Verification Code with* is set as *FortiToken*.
Service Setting Turn on/off the service settings.	

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

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

SSH Service	Enable/disable SSH service. The *SSH Service* toggle controls *Web SSH*, *Web Telnet*, *Web SFTP*, *PuTTY*, and the *WinSCP* launchers. **Note**: *SSH Filter*, *RSA Sign Algorithm*, and *SSH Auto-Password* options are only available when *Template* is already selected.
Use Template Default Port	Use the template default port or disable and enter a port number.
SSH Filter	Enable/disable using an SSH filter profile. See SSH filter profiles on page 234.
SSH Filter Profile	From the dropdown, select an SSH filter profile. **Note**: The option is only available when *SSH Filter* is enabled. Use the search bar to look up an SSH filter profile.
Bypass for owner	Enable/disable allowing secret owners to bypass the SSH command filter (default = disable). Once enabled, secret owners can send otherwise prohibited commands (listed in the SSH filter profile) to the targets. **Note**: The option is only available when *SSH Filter* is enabled.
RSA Sign Algorithm	To improve compatibility with different SSH servers, select a sign in algorithm for RSA-based public key authentication: • *RSA SHA-256 signing algorithm* • *RSA SHA-512 signing algorithm* • *RSA SHA-1 signing algorithm* (default)
SSH Auto-Password	Enable or disable automatically delivering passwords to the server when the user enters privileged commands (e.g., `sudo` in Unix system and `enable` in Cisco devices) in the SSH shell terminal. For secrets using Cisco server info template, an associated secret must be set to enable this feature. **Note**: The option only works when *Proxy Mode* is enabled.
Auto-Switch Account	When enabled, upon launching the current secret, the secret uses the associated secret (if applicable) and automatically switches to the current account. When disabled, secret launching finishes in the account stored in the associated secret since the credential information was received from the associated secret.

	The option is only available when: • *SSH Service* is enabled, i.e., it will only work with SSH launchers. • *Launch with Associated Secret Credentials* is enabled.
RDP Service	Enable/disable RDP service. The *RDP Service* toggle controls *Web RDP* and the *Remote Desktop-Windows* launchers. **Note**: *RDP Security Level*, *RDP Restricted Admin Mode*, and *Keyboard Layout* options are available only when *Template* is already selected.
Use Template Default Port	Use the template default port or disable and enter a port number.
RDP Security Level	Select a security level when establishing a RDP connection to the secret: • *Best Effort* (default): If the server supports NLA, FortiPAM uses NLA to authenticate. Otherwise, FortiPAM conducts standard RDP authentication with the server through RDP over TLS. • *NLA*: Network Level Authentication (CredSSP). When an RDP launcher is launched, FortiPAM is forced to use CredSSP (NLA) to authenticate with the target server. • *RDP*: FortiPAM uses the standard RDP encryption provided by the RDP protocol without using TLS (Web-RDP only). • *TLS*: RDP over TLS. FortiPAM uses secured connection with encryption protocol TLS to connect with the target server.
RDP Auto TOTP	Enable/disable RDP auto Time-based One-time Password (TOTP). **Note**: The option is only available when *RDP Security Level* is set as *TLS*.
RDP Restricted Admin Mode	Enable/disable RDP restricted admin mode. Restricted admin mode prevents the transmission of reusable credentials to the remote system to which you connect using remote desktop. This prevents your credentials from being harvested during the initial connection process if the remote server has been compromised. **Note**: The option is only available when *RDP Security Level* is set as *Best Effort* or *NLA*.
Keyboard Layout	From the dropdown, select a keyboard layout (default = *English, United States*)
RDP Event Filter	Enable/disable using an event filter profile. See Event filter profile on page 240.
RDP Event Filter Profile	From the dropdown, select an event filter profile. **Note**: The option is only available when *RDP Event Filter* is enabled. Use the search bar to look up an event filter profile.

VNC Service	Enable/disable VNC service. The *VNC Service* toggle controls the *Web VNC*, *VNC Viewer*, and *TightVNC* launchers .
Use Template Default Port	Use the template default port or disable and enter a port number. **Note**: The port number you enter is used to connect to the VNC launcher.
Display Number	Enter the display number to be added to the VNC port defined in the template (default = 0). **Notes**: • The display number can only be set if the custom port on the template is the VNC default port, i.e., port `5900`, and the secret uses the default template for VNC. Otherwise, the display number option is the custom port option. • The display number cannot be set with a custom port. • The option is only available when *Use Template Default Port* is enabled.
SAMBA Service	Enable/disable SAMBA service. The *SAMBA Service* toggle controls the *Web SMB* launcher.
Use Template Default Port	Use the template default port or disable and enter a port number.
SFTP Service	Enable/disable SFTP service. The *SFTP Service* toggle controls the *Web SFTP* launcher.
Use Template Default Port	Use the template default port or disable and enter a port number.
Telnet Service	Enable/disable the Telnet service. The *Telnet Service* toggle controls web Telnet.
Use Template Default Port	Use the template default port or disable and enter a port number.
Permission	

By default, secret permission is the same as the folder where they are located.

When customizing secret permission, ensure that you log in with an account with *Owner* or *Edit* permission to the secret or the folder where the secret is located.

ZTNA	
Inherit ZTNA Control	Enable to inherit ZTNA control access permission from the parent folder. By default, secrets in a folder follow the ZTNA control set up in the parent folder. However, when creating or editing a secret you can customize the ZTNA control in the *Secret Permission* tab.
ZTNA Control	Enable to limit the permission of launching by `ztna-ems-tag`.

	You can choose whether to match all the tags or only one of them. The option is only available when *Inherit ZTNA Control* is disabled.
Device Tags	Select + to add ZTNA tags or groups. Use the search bar to look up a ZTNA tag or ZTNA tag group. Only permitted devices with the selected tags are allowed to launch.
Device Match Logic	Define the match logic for the device tags: • *OR*: Devices with any of the selected tags are allowed to launch. • *AND*: Devices must acquire all the selected tags to launch.
Permission	
Inherit Permission	Enable to inherit permissions that apply to the folder where the secret is located. The option is enabled by default.
Permission	The level of user/user group access to the secret. See User Permission on page 88 and Group Permission on page 89.
Target Filter	Enable/disable filtering addresses. When enabled, *Allow*/*Deny* addresses, i.e., create a list of allowed or blocked addresses. Creating allowlist/blocklist helps you improve security by allowing/blocking IP addresses. ⚠ The filter does not apply to the Domain-Controlled address. Select +, from the *Select Entries* list, select addresses, and click *Close*. Use the search bar to look up an address.

Click the delete icon to delete all the addresses and reset the list.

Note:
The option is disabled by default and only available when editing a secret that has one of its fields set as *Domain*.

Dependency

Select + to add a dependency updater.

The secret is used as the credential for the selected target where the service defined in the selected dependency updater runs.

You can add additional dependency updaters by selecting +.

Once the secret password changer successfully rotates the secret password, all the dependencies in the secret are automatically updated.

The following status messages are used:

- `init`: The dependency is newly added or reset by a configuration change.
- `pending`: The dependency is in progress of checking/updating.
- `success`: When *Check* or *Update* succeeds.
- `failure`: When *Check* or *Update* fails.
- `last-update`: The date and time when the latest update or check occured.
  See Updating a service account credential Example on page 197.

See Dependency updater on page 194.

Dependency	From the dropdown, select a dependency updater.

To create a new dependency updater:

1. From the dropdown, select +.
   The *New Dependency Updater* window opens.
2. Follow instructions from step 3 in Creating a dependency updater on page 195 to create a dependency updater.

Use the search bar to look up a dependency updater.

Use the pen icon next to a dependency updater to edit it.

Target	From the dropdown, select a target where the service defined in the selected dependency updater is running. The target must contain a privileged account. **To create a target:** 1. From the dropdown, select +. The *New Secret Target* window opens. 2. Follow the instructions from step 4 in Creating a target on page 114. Use the search bar to look up a target. Use the pen icon next to a target to edit it.

7. Click *Submit*.
   See Launching a secret on page 97 and Example secret configurations example on page 105.

User Permission

1. In step 5 when Creating a secret, in the *Permission* tab, select the user from the *User/Group* dropdown when *Inherit Permission* is disabled.

   To add a new user:
   1. Select + and then select +*User List*.
      The *New User List* wizard opens.
   2. Follow the steps in Creating a user on page 253, starting step 2 to create a new user.

   Use the search bar to look up a user.

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

2. In the *Permission* dropdown, select from the following:
   - *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. In *Allowed Service*, from the *Select Entries* list, select the services, click *Close*.

   Use the search bar to look up a service.

4. Click *Save*.

From the list, click *x* next to a user permission entry to delete it.

Group Permission

1. In step 5 when Creating a secret, in the *Permission* tab, select the user group from the *User/Group* dropdown when *Inherit Permission* is disabled.

   To add a new user group:

   1. Select + and then select +*User Group*.
      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.

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

2. In the *Permission* dropdown, select from the following:
   - *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. In *Allowed Service*, from the *Select Entries* list, select the services, click *Close*.

   Use the search bar to look up a service.

4. Click *Save*.

From the list, click *x* next to a group permission entry to delete it.

Connect over SSH

Note that when both *Launch with Associated Secret Credentials* and *Auto-Switch Account* options are enabled, the same functionality is offered as with the *Connect over SSH with* an associated secret. Launching a secret uses the associated secret credential information to log in and switch to the account stored in the primary secret.

If both *Launch with Associated Secret Credentials* and *Auto-Switch Account* are disabled, the same functionality is offered as with the *Connect over SSH with* itself option. Launching a secret only uses the primary secret for launching. Here, the associated secret provides password for the primary secret without a password, e.g., an SSH secret with keys or a secret with *SSH Auto-Password* enabled and using password changing.

Use cases for associated secrets

The following lists some common use cases for associated secrets:

1. A secret using *Target Only* template which stores the target server IP address can be used as the primary secret. A windows domain secret storing the necessary credential information can be used as the associated secret.

   In this way, multiple target only secrets with different target server IP addresses can associate with the same windows domain secret if they use the same credential information.
2. A *Cisco Enable Secret* template based secret can use a Cisco user secret as its associated secret. The *Cisco Enable Secret* template based secret stores the password whereas the user name and passwords are stored in the *Cisco User (SSH Secret)* template based secret.

   In this case, both *Launch with Associated Secret Credentials* and *Auto-Switch Account* are enabled if you want to stay as an enabled user after the secret launch.
3. A *Cisco User (SSH Secret)* template based secret can use a *Cisco Enable Secret* template based secret as the associated secret.
   The *Cisco Enable Secret* template based secret stores password. The user name and password are stored in the *Cisco User (SSH Secret)* template based secret. Both *Launch with Associated Secret Credentials* and *Auto-Switch Account* are disabled. This way the associated secret provides the password if *SSH Auto-Password* is enabled.

Associated secret related CLI

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

```
config secret database
 edit 2
  set associated-secret 1
  set launch-with {associated-secret | itself}
  set ssh-switch-account {enable | disable}
 next
end
```

Variable	Description
launch-with {associated-secret | itself}	Launching using an associated secret or the secret itself: • `associated-secret`: Use associated secret credential information to launch. • `itself`: Use secret own credential information to launch.
set ssh-switch-account {enable | disable}	Enable to switch to secret account after launching with associated secret using SSH launchers.

Variable	Description
	Disable to remain in the associated secret account after launching with associated secret using SSH launchers. **Note**: The variable is only available when `launch-with` is set as `associated-secret`.

Installing CA certificates for web launching

When you attempt to access a website using the web proxy feature, you may receive a warning about untrusted hosts on the web browser. To resolve this issue, you must download and install a CA certificate signed by FortiPAM.

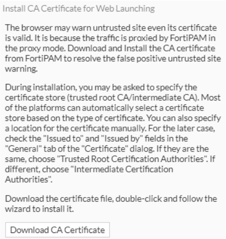
When creating a secret with *Web Proxy* enabled, *Download CA Certificate* button on the top-right allows you to download the CA certificate.

The browser may warn untrusted sites even if its certificate is valid. This is because the traffic is proxied by FortiPAM in the proxy mode. Download and install the CA certificate from FortiPAM to resolve the false positive untrusted site warning.

During installation, you may be asked to specify the certificate store (trusted root CA/intermediate CA). Most platforms can automatically select a certificate store based on the type of certificate. You can also specify a location for the certificate manually. For the latter case, check the *Issued to* and *Issued by* fields in the *General* tab of the *Certificate* dialog. If they are the same, choose *Trusted Root Certification Authorities*. If different, select *Intermediate Certification Authorities*.

- Even if the site is trusted before, you must install the FortiPAM CA certificate to resolve the false positive untrusted site warning.
- If the site is untrusted, you receive the warning about untrusted hosts on the web browser.

Download the certificate file, double-click it, and follow the wizard to install it.



Install CA Certificate for Web Launching

The browser may warn untrusted site even its certificate is valid. It is because the traffic is proxied by FortiPAM in the proxy mode. Download and Install the CA certificate from FortiPAM to resolve the false positive untrusted site warning.

During installation, you may be asked to specify the certificate store (trusted root CA/intermediate CA). Most of the platforms can automatically select a certificate store based on the type of certificate. You can also specify a location for the certificate manually. For the later case, check the "Issued to" and "Issued by" fields in the "General" tab of the "Certificate" dialog. If they are the same, choose "Trusted Root Certification Authorities". If different, choose "Intermediate Certification Authorities".

Download the certificate file, double-click and follow the wizard to install it.

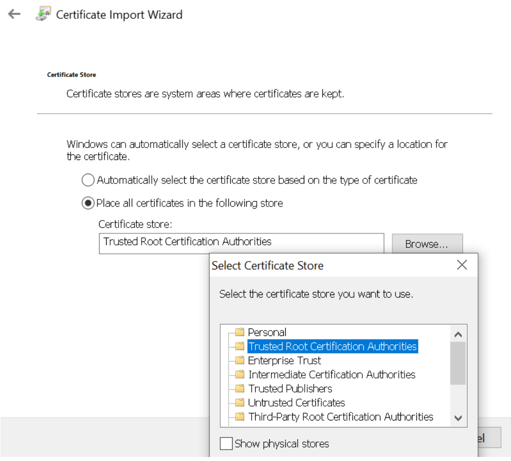
Also, when there are multiple certificates that you need to install, a *Download All CA Certificates* button is available instead.

When downloading multiple certificates, they are made available as a zip file named `CA-Certificates.zip`.

Download and double-click the certificate file to install it by following the installation wizard.

If the CA certificate is root, it must be installed in the trusted root store.

Not all CA certificates should be installed as root CA. If the CA certificate is intermediate, it must be installed in the intermediate store to work correctly.



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

Certificate store: Trusted Root Certification Authorities

Browse...
Select Certificate Store
Select the certificate store you want to use.
Personal
Trusted Root Certification Authorities
Enterprise Trust
Intermediate Certification Authorities
Trusted Publishers
Untrusted Certificates
Third-Party Root Certification Authorities
□ Show physical stores

You can tell the CA type by inspecting the property of the CA, e.g., in Windows, right-click the certificate file and click *Property*. If the *Issued to* and *Issued by* fields are the same, it should be installed as a root CA. Otherwise, it is an intermediate certificate and must be installed in the intermediate store.

Also, Windows can automatically determine the correct CA certificate when you select *Automatically select the certificate store based on the type of certificate*. This is the preferred way of certificate installation.

Configuring TOTP settings via the secret CLI commands - Example

To configure TOTP settings via the CLI:

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

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

To configure TOTP settings via the CLI:

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

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

```
            set shared-key xxxxxxxxxxxx
          end
        end
```

Configuring a secret where the secret owner can bypass the SSH command filter via the CLI- Example

To configure the secret via the CLI:

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

```
 config secret database
  edit 16
   set name "test_SSH_filter"
   set uuid be0204d2-6ea0-51ee-beb9-e0bd958f624c
   set folder 2
   set template "Unix Account (SSH Password)"
   set proxy enable
   set ssh-filter enable #enable SSH filter
   set ssh-filter-profile "test_SSH_filter" #assign an SSH filter
   set bypass-ssh-filter-for-owner enable #enable allowing secret owners to bypass the
SSH command filter
   set ssh-service-status up
   set rdp-serice-status up
   set sftp-service-status up
   config credentials-history
  end
  config field
   edit 1
       set name "Host"
       set value "en.wikipedia.org"
   next
   edit 2
       set name "Username"
       set value "admin"
   next
   edit 3
       set name "Password"
       set value "ENC jdiQCaM/yseJywRX+yz0J+xfA2A="
   next
  end
 next
end
```

Configuring a secret to use dependency via the CLI - Example

To configure a secret to use dependency via the CLI:

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

```
config secret database
 edit 3
  config dependency
   set target "machine-1174"
   set updater "win-mysql-updater"
   set status init
   set last-update 0000-00-00 00:00:00
  end
 next
end
```

MySQL service is running on `machine-1174` that uses the credentials from secret `3`.

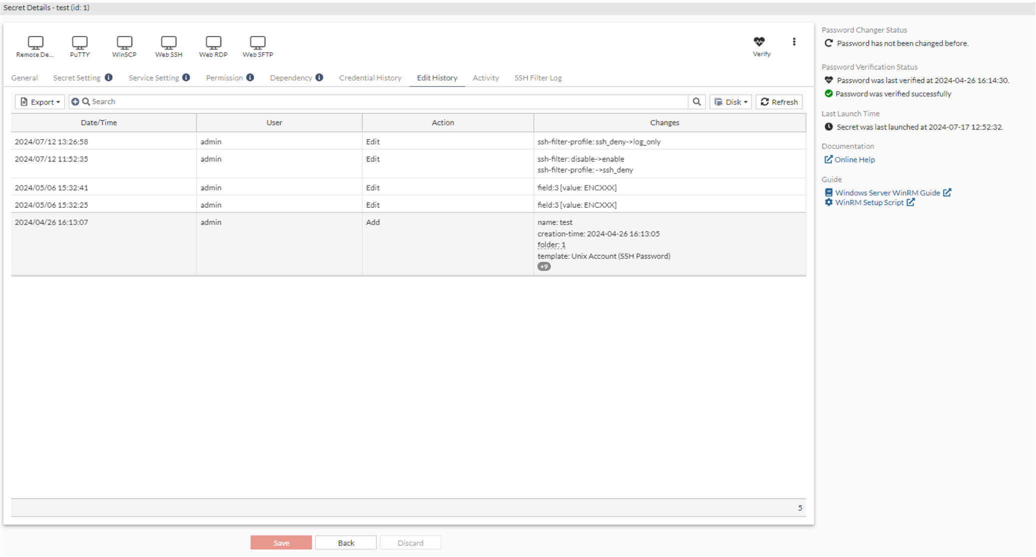
Viewing secret edit history

You must have *View Secret Log* permission to view the secret edit history. See Role on page 278.

You must have at least *View* permission for the secret to see the *Edit History* tab.

To view secret edit history:

1. Go to *Secrets* > *Secrets* and double-click a secret to edit it.
   The *Secret Details* page opens.
2. Select *Edit History* to open the *Edit History* tab.



Date/Time	User	Action	Changes
2024/07/12 13:26:58	admin	Edit	ssh-filter-profile: ssh_deny->log_only
2024/07/12 11:52:35	admin	Edit	ssh-filter: disable->enable ssh-filter-profile: ->ssh_deny
2024/05/06 15:32:41	admin	Edit	field:3 [value: ENCXXX]
2024/05/06 15:32:25	admin	Edit	field:3 [value: ENCXXX]
2024/04/26 16:13:07	admin	Add	name: test creation-time: 2024-04-26 16:13:05 folder: 1 template: Unix Account (SSH Password) +9

Password Changer Status

Password has not been changed before.

Password Verification Status

Password was last verified at 2024-04-26 16:14:30.

Password was verified successfully

Last Launch Time

Secret was last launched at 2024-07-17 12:52:32.

Documentation

Online Help

Guide

Windows Server WinRM Guide

WinRM Setup Script

For each edit history, the following columns are displayed by default:

- *Date/Time*
- *User*
- *Action*
- *Changes*

The *Message* column is not visible by default.

To display the *Message* column, select *Configure Table* icon as you click the header for the left-most column, select *Message* and then click *Apply*.

The following options are available in the *Edit History* tab:

Search	Enter a search term in the search field, then hit `Enter` to search. To narrow down your search, see Column filter.
Disk/FortiAnalyzer	From the dropdown, select from the following two options to retrieve the edit history from: • *Disk* (default) (FortiPAM) • *FortiAnalyzer*
Refresh	To refresh the contents, click the refresh icon.

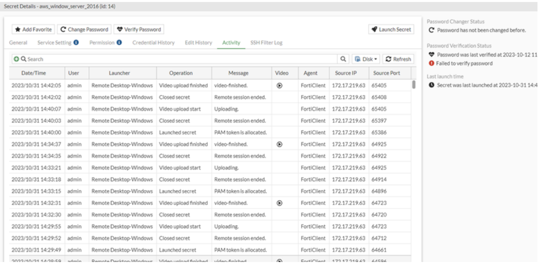
Viewing secret activity

You must have *View Secret Log* permission to view secret activity. See Role on page 278.

You must have at least *View* permission for the secret to see the *Activity* tab.

To view secret activity:

1. Go to *Secrets* > *Secrets* and double-click a secret to edit it.
   The *Secret Details* page opens.
2. Select *Activity* to open the *Activity* tab.



Date/Time	User	Launcher	Operation	Message	Video	Agent	Source IP	Source Port
2023/10/31 14:42:05	admin	Remote Desktop-Windows	Video upload finished	video-finished.	▶	FortiClient	172.17.219.63	65405
2023/10/31 14:42:02	admin	Remote Desktop-Windows	Closed secret	Remote session ended.		FortiClient	172.17.219.63	65408
2023/10/31 14:40:07	admin	Remote Desktop-Windows	Video upload start	Uploading.		FortiClient	172.17.219.63	65405
2023/10/31 14:40:03	admin	Remote Desktop-Windows	Closed secret	Remote session ended.		FortiClient	172.17.219.63	65397
2023/10/31 14:40:00	admin	Remote Desktop-Windows	Launched secret	PAM token is allocated.		FortiClient	172.17.219.63	65386
2023/10/31 14:34:37	admin	Remote Desktop-Windows	Video upload finished	video-finished.	▶	FortiClient	172.17.219.63	64925
2023/10/31 14:34:35	admin	Remote Desktop-Windows	Closed secret	Remote session ended.		FortiClient	172.17.219.63	64922
2023/10/31 14:33:21	admin	Remote Desktop-Windows	Video upload start	Uploading.		FortiClient	172.17.219.63	64925
2023/10/31 14:33:18	admin	Remote Desktop-Windows	Closed secret	Remote session ended.		FortiClient	172.17.219.63	64914
2023/10/31 14:33:15	admin	Remote Desktop-Windows	Launched secret	PAM token is allocated.		FortiClient	172.17.219.63	64896
2023/10/31 14:32:31	admin	Remote Desktop-Windows	Video upload finished	video-finished.	▶	FortiClient	172.17.219.63	64723
2023/10/31 14:32:30	admin	Remote Desktop-Windows	Closed secret	Remote session ended.		FortiClient	172.17.219.63	64720
2023/10/31 14:29:55	admin	Remote Desktop-Windows	Video upload start	Uploading.		FortiClient	172.17.219.63	64723
2023/10/31 14:29:52	admin	Remote Desktop-Windows	Closed secret	Remote session ended.		FortiClient	172.17.219.63	64712
2023/10/31 14:29:49	admin	Remote Desktop-Windows	Launched secret	PAM token is allocated.		FortiClient	172.17.219.63	64661
2023/10/31 14:28:59	admin	Remote Desktop-Windows	Video upload finished	video-finished.	▶	FortiClient	172.17.219.63	64596

Password Changer Status
Password has not been changed before.

Password Verification Status
Password was last verified at 2023-10-12 11
Failed to verify password

Last launch time
Secret was last launched at 2023-10-31 14:4

For each activity entry, the following columns are displayed:

- *Date/Time*
- *User*
- *Launcher*
- *Operation*
- *Message*

- *Video*
- *Agent*
- *Source IP*
- *Source Port*

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

Search	Enter a search term in the search field, then hit `Enter` to search. To narrow down your search, see Column filter.
Disk/FortiAnalyzer	From the dropdown, select from the following two options to retrieve the secret activity from: • *Disk* (default) (FortiPAM) • *FortiAnalyzer*
Refresh	To refresh the contents, click the refresh icon.

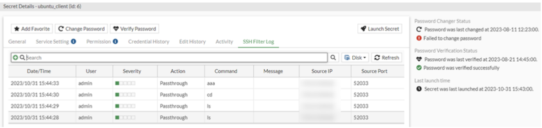
Viewing SSH filter logs for a secret

You must have *View Secret Log* permission to view SSH filter logs for a secret. See Role on page 278.

You must have at least *View* permission for the secret to see the *SSH Filter Log* tab.

To view SSH filter logs for a secret:

1. Go to *Secrets* > *Secrets* and double-click a secret to edit it.
   The *Secret Details* page opens.
2. Select *SSH Filter Log* to open the *SSH Filter Log* tab.



Secret Details - ubuntu_client (id: 6)

Date/Time	User	Severity	Action	Command	Message	Source IP	Source Port
2023/10/31 15:44:33	admin	🟩□□□□	Passthrough	aaa		[redacted]	52033
2023/10/31 15:44:30	admin	🟩□□□□	Passthrough	cd		[redacted]	52033
2023/10/31 15:44:29	admin	🟩□□□□	Passthrough	ls		[redacted]	52033
2023/10/31 15:44:28	admin	🟩□□□□	Passthrough	ls		[redacted]	52033

Password Changer Status
Password was last changed at 2023-08-11 12:23:00.
Failed to change password

Password Verification Status
Password was last verified at 2023-08-21 14:45:00.
Password was verified successfully

Last launch time
Secret was last launched at 2023-10-31 15:43:00.

For each entry, the following tabs columns are displayed:

- *Date/Time*
- *User*
- *Serverity*
- *Action*
- *Command*
- *Message*
- *Source IP*
- *Source Port*

The following options are available in the *SSH Filter Log* tab:

Search	Enter a search term in the search field, then hit `Enter` to search. To narrow down your search, see Column filter.
Disk/FortiAnalyzer	From the dropdown, select from the following two options to retrieve the SSH filter logs from: • *Disk* (default) (FortiPAM) • *FortiAnalyzer*
Refresh	To refresh the contents, click the refresh icon.

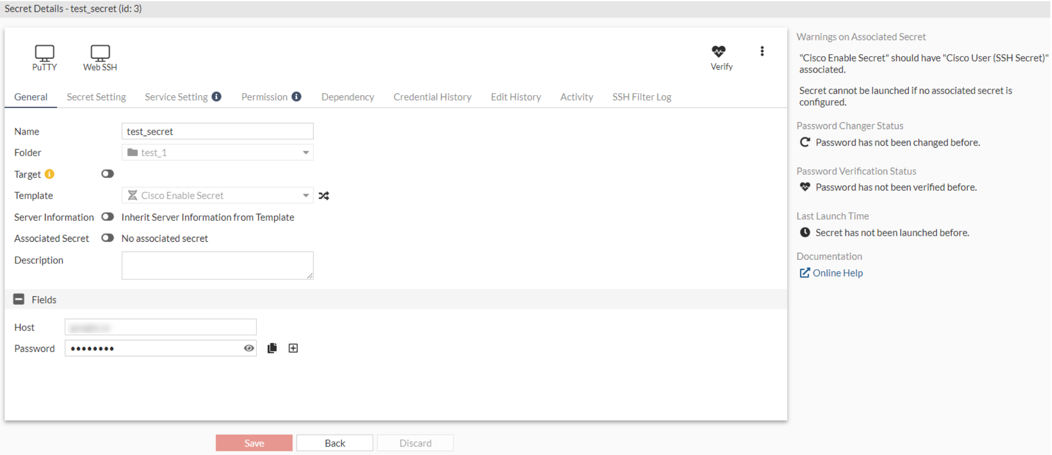
Launching a secret

To launch a secret:

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

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

3. From the top, select a launcher icon to launch the secret.



Secret Details - test_secret (id: 3)

Name: test_secret
Folder: test_1
Target
Template: Cisco Enable Secret
Server Information: Inherit Server Information from Template
Associated Secret: No associated secret
Description

Fields

Host
Password: ••••••••

Warnings on Associated Secret

"Cisco Enable Secret" should have "Cisco User (SSH Secret)" associated.

Secret cannot be launched if no associated secret is configured.

Password Changer Status

Password has not been changed before.

Password Verification Status

Password has not been verified before.

Last Launch Time

Secret has not been launched before.

Documentation

Online Help

> 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 185 and Creating a secret on page 72. Also, see AntiVirus on page 221.
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 225.

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

See Check out and check in a secret on page 98.

Blocklist and allowlist for RDP target IP address restriction

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

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

See the *Target Filter* option in the *Permission* pane when Creating a secret on page 72.

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* > *Secrets*.
2. In *Secrets*, 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 the *Check-out* (🚪) icon to check out the secret.

> If the *Check-out* icon 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 72.

> To ensure accountability, a secret password is only visible to the user with *Edit* or *Owner* permission for the secret the user is checking out.
>
> This is only valid when *Requires Checkout* is enabled in the *Secret Setting* pane when configuring the secret.
>
> See *Requires Checkout* option when Creating a secret on page 72.

To check in a secret:

1. Go to *Secrets* > *Secrets*.
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 the *Check-in* ( ) icon to check in the secret.
   Other approved users can now access the secret.

Uploading secrets using the secret upload template

On the *Secrets* 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.

If the secret upload template includes any of the following mandatory fields: *Host*, *Domain*, or *URL*, the corresponding target is modified or created (if applicable).

The new target is created with the naming convention: `import_(Host/Domain/URL).`

The failure to create a target results in the failure to create the corresponding secret.

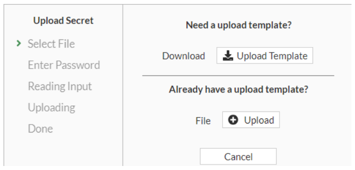
When importing a secret, FortiPAM first scans if a corresponding target exists by matching *Host*, *URL*, and *Domain*.

If there is a match, FortiPAM chooses the matched target for the secret and creates the secret.

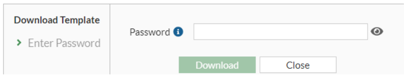
If there is no match, FortiPAM creates a new target automatically first and the target name is `import_[Host/Domain/URL]`. The secret is then created based on the newly created target.

To upload secrets using the secret upload template:

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



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



3. In *Password*, enter a password to encrypt the secret upload template excel file.
   The secret upload template is downloaded on your computer. The file is named `secret_upload_template.xlsm`.
4. Open the secret upload template (`secret_upload_template.xlsm`), enter the password that was used to encrypt the file in step 3, and click *OK*.
   You can now access the secret upload template.

   The secret upload template currently includes the following features:

- Checks template completion when you quit; a warning appears if the template is incomplete.
- Highlights fields that need to be filled in.
- Checks the target address syntax. Currently supports IPv4 addresses and FQDN only.

5. Upon opening the `secret_upload_template.xlsm` file for the first time, enable editing and content for Macros.
6. From the *Secret Template* column, select a supported template.

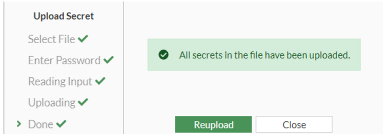
All the default secret templates are supported.

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

7. Fill in the fields highlighted in yellow.

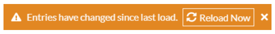
The fields highlighted in red cannot be edited.

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



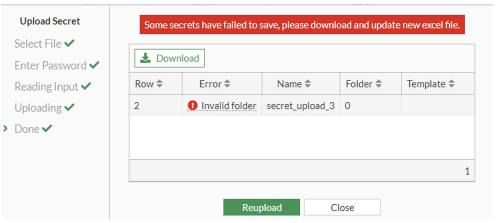
All secrets in the file have been uploaded.

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



Entries have changed since last load.

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



Some secrets have failed to save, please download and update new excel file.

Row	Error	Name	Folder	Template
2	Invalid folder	secret_upload_3	0	

1

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.

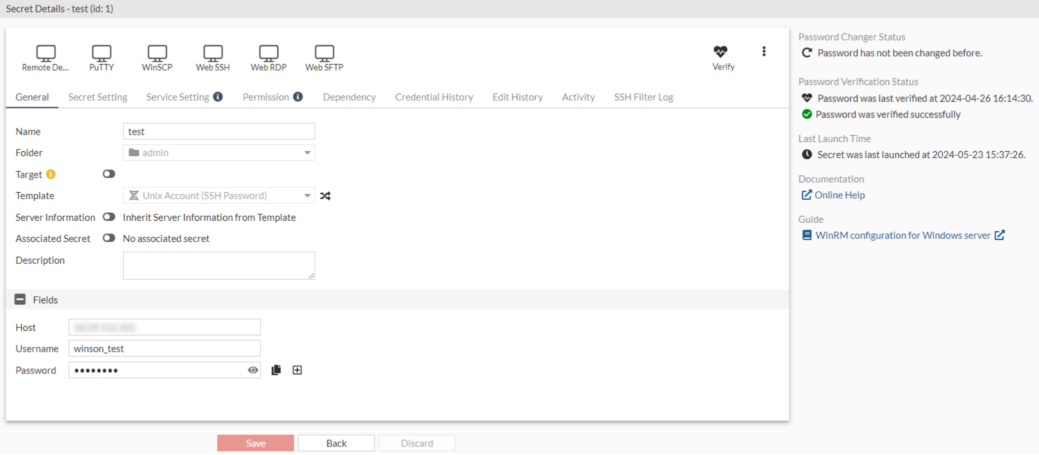
See Automatic password changing on page 216.

To change the password:

1. Go to *Secrets> Secrets*.
2. In *Secrets*, select a secret, and select *Edit*.

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

   The *Secret Details* window opens.



Name: test
Folder: admin
Target
Template: Unix Account (SSH Password)
Server Information: Inherit Server Information from Template
Associated Secret: No associated secret
Description

Host: [redacted]
Username: winson_test
Password: ••••••••

Password Changer Status
Password has not been changed before.

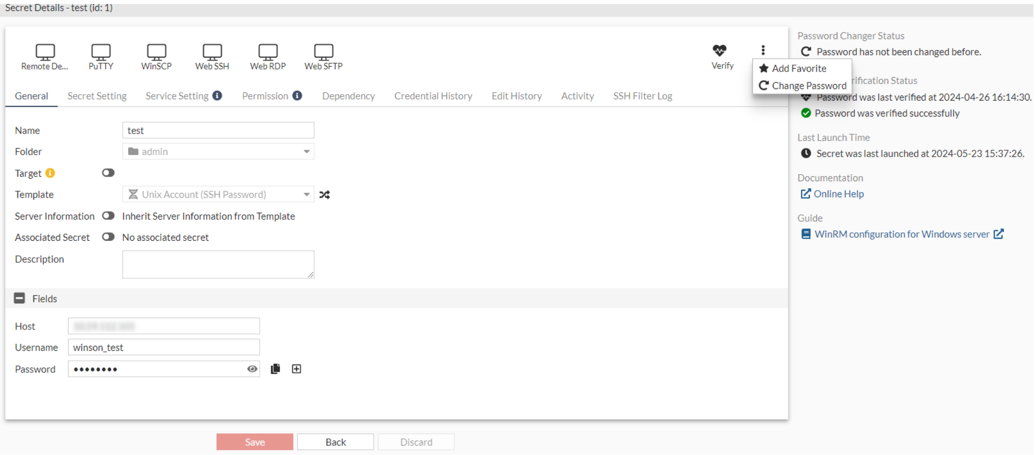
Password Verification Status
Password was last verified at 2024-04-26 16:14:30.
Password was verified successfully

Last Launch Time
Secret was last launched at 2024-05-23 15:37:26.

Documentation
Online Help

Guide
WinRM configuration for Windows server

3. From More options, select *Change Password*.



Name: test
Folder: admin
Target
Template: Unix Account (SSH Password)
Server Information: Inherit Server Information from Template
Associated Secret: No associated secret
Description

Host: [redacted]
Username: winson_test
Password: ••••••••

Password Changer Status
Password has not been changed before.

Password Verification Status
Password was last verified at 2024-04-26 16:14:30.
Password was verified successfully

Last Launch Time
Secret was last launched at 2024-05-23 15:37:26.

Documentation
Online Help

Guide
WinRM configuration for Windows server

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.

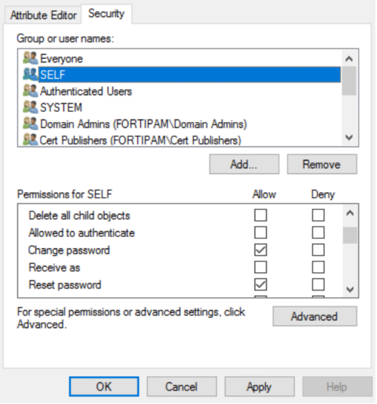
   To be able to successfully change the password manually, the password must follow password requirements set in Password policies on page 217.

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.

For example, in the screenshot below, *Change password* and *Reset password* are allowed for *SELF*, i.e., the user.



Group or user names:

- Everyone
- SELF
- Authenticated Users
- SYSTEM
- Domain Admins (FORTIPAM\Domain Admins)
- Cert Publishers (FORTIPAM\Cert Publishers)

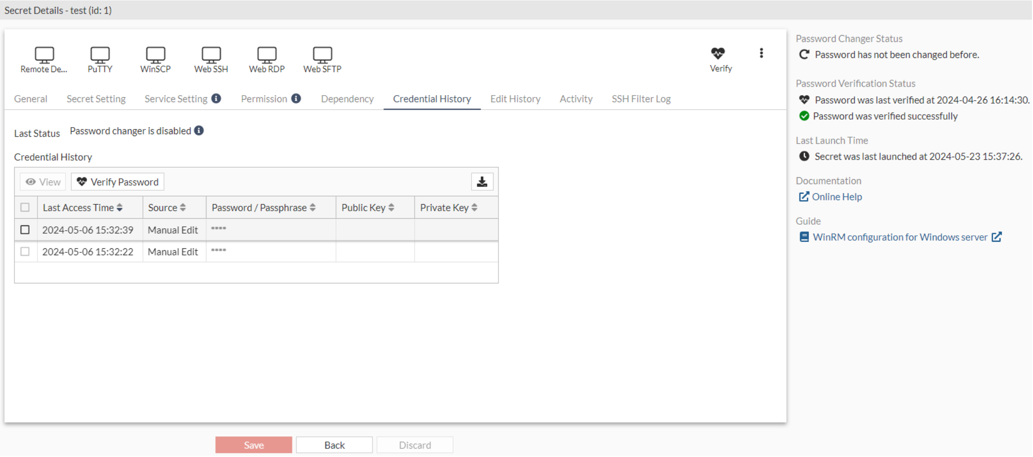
Permissions for SELF	Allow	Deny
Delete all child objects	□	□
Allowed to authenticate	□	□
Change password	☑	□
Receive as	□	□
Reset password	☑	□

For special permissions or advanced settings, click Advanced.

Credential History

FortiPAM retains recent five 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.



Secret Details - test (id: 1)

Last Status Password changer is disabled

Credential History

□	Last Access Time	Source	Password / Passphrase	Public Key	Private Key
□	2024-05-06 15:32:39	Manual Edit	****		
□	2024-05-06 15:32:22	Manual Edit	****		

Password Changer Status
Password has not been changed before.

Password Verification Status
Password was last verified at 2024-04-26 16:14:30.
Password was verified successfully

Last Launch Time
Secret was last launched at 2024-05-23 15:37:26.

Documentation
Online Help

Guide
WinRM configuration for Windows server

To view previous credentials:

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

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

   To clear the last credential used in a failed password change, click *Clear Last Credential*. The last credential used is removed from the credential history.

To restore password using credential history:

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

   The *Secret Details* window opens.
3. Go to the *Credential History* tab.
4. To use the last credential from a failed password change, click *Verify Last Credential*.
   If the password change is successful, a message shows up asking if you want to restore the credential. Click *Yes* to restore the credential.

   To use a previous entry, click the entry row to use and click *Verify Password*. A message appears if the password change is successful.

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

1. On Windows, open *Local Security Policy*.
2. Go to *Local Policies* > *Security Options* > *Network access: Restrict clients allowed to make remote calls to SAM*.
3. Right-click *Network access: Restrict clients allowed to make remote calls to SAM* and select *Properties*.

4. Select *Edit Security...*.
5. Add users to *Group or user names:* in the *Security Settings for Remote Access to SAM* window.
6. Click *OK*.
7. Click *OK*.

Verify password

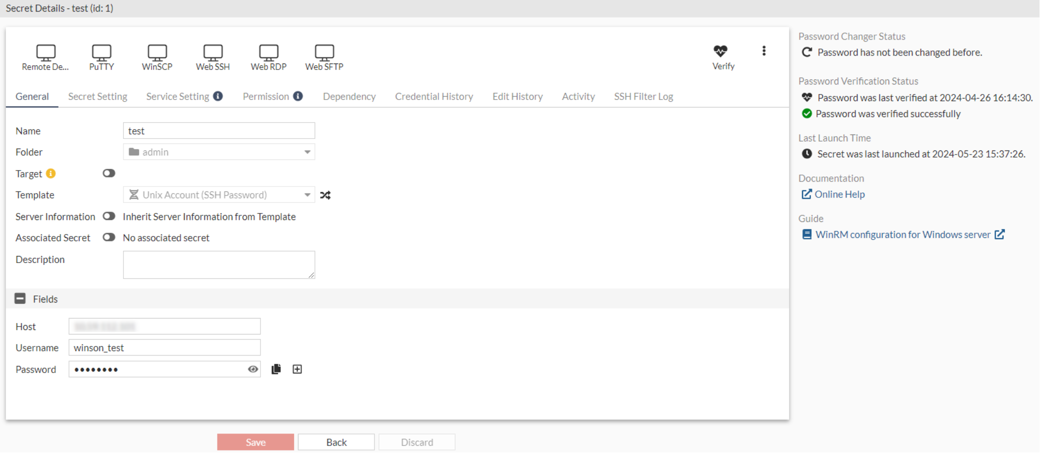
On FortiPAM, you can verify the password in a secret manually to check its accuracy, and confirm if the target server is reachable.

> You can only manually verify passwords every 5 seconds.

> You can also set up a secret to automatically verify the password by enabling *Automatic Password Verification* when creating or editing a secret.
> See Automatic password verification on page 217.

To verify the password:

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



Secret Details - test (id: 1)

Name	test
Folder	admin
Target	
Template	Unix Account (SSH Password)
Server Information	Inherit Server Information from Template
Associated Secret	No associated secret
Description	

Fields

Host	[redacted]
Username	winson_test
Password	••••••••

Password Changer Status
Password has not been changed before.

Password Verification Status
Password was last verified at 2024-04-26 16:14:30.
Password was verified successfully

Last Launch Time
Secret was last launched at 2024-05-23 15:37:26.

Documentation
Online Help

Guide
WinRM configuration for Windows server

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

To configure an SSH key:

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

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

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

   d. *Passphrase*, if any.

5. Ensure that proxy is enabled in the *Secret Setting* pane.

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

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

To configure a Windows AD-LDAP secret:

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

To configure Windows Samba secret:

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

To configure a Cisco secret:

1. Repeat steps 1 to 4 as shown in Configuring an SSH password.
2. Enter a secret name.
3. In the *Template* dropdown, select *Cisco User (SSH Secret)*.
4. In *Fields*, enter information for the following fields:
   a. *Host*
   b. *Username*
   c. *Password*
5. Click *Submit*.
   If the password change feature needs to be used, then one more secret needs to be created for the Cisco enable command:

   a. Repeat steps 1 and 2.
   b. In the *Template* dropdown, select *Cisco Enable Secret*.
   c. In *Fields*, enter information for the following fields:
      i. *Host*
      ii. *Password*
   d. Click *Submit*.
6. Go to the *Service Setting* tab for the Cisco secret that was earlier created (steps 1 - 5).
7. Optionally, enable *SSH Auto-Password*.
8. Go to the *General* tab, and ensure that *Associated Secret* is enabled.
9. In the *Associated Secret* dropdown, select the Cisco enable secret.
10. Click *Save*.

To configure an AWS web account secret:

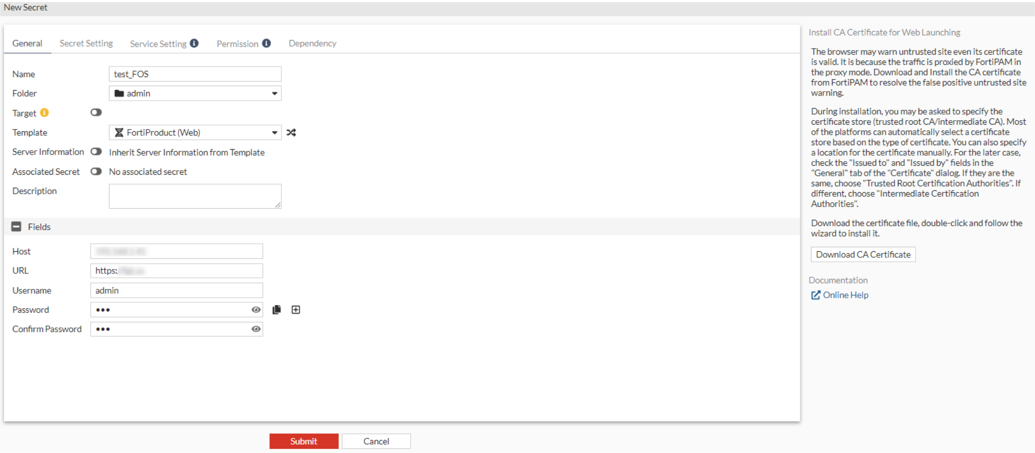
1. Repeat steps 1 to 4 as shown in Configuring an SSH password.
2. Enter a secret name.
3. In the *Template* dropdown, select *AWS Web Account*.
4. In *Fields*, enter information for the following fields:
   a. *URL*
   b. *Username*
   c. *Password*
   d. *AccountID*: Used for IAM accounts.
      For AWS root accounts, the field remains empty. Otherwise, the web extension treats the secret as an IAM account secret impacting the login process.
5. Click *Submit*.

Configuring a web FortiProduct secret - Example

To configure a web FortiProduct secret:

1. Go to *Secrets* > *Secrets*.
2. In *Secrets*, select *Create*.
   The *Create New Secret in:* dialog opens.
3. Select the folder where you intend to add the secret.
4. Select *Create*.
   The *New Secret* window opens.
5. Enter a name for the secret.
6. Disable *Target*.
7. In the *Template* dropdown, select the *FortiProduct (Web)* template.
8. In the *Fields* pane:
   a. In *Host*, enter the IP address or the FQDN of the Fortinet product.
   b. In *URL*, enter the URL of the Fortinet product.
   c. In *Username*, enter the user name.
   d. In *Password*, enter the password.
   e. In *Confirm Password*, reenter the password.

9. Click *Submit*.



New Secret

Name: test_FOS
Folder: admin
Target
Template: FortiProduct (Web)
Server Information: Inherit Server Information from Template
Associated Secret: No associated secret
Description

Fields

Host: [redacted]
URL: https:[redacted]
Username: admin
Password: •••
Confirm Password: •••

Install CA Certificate for Web Launching

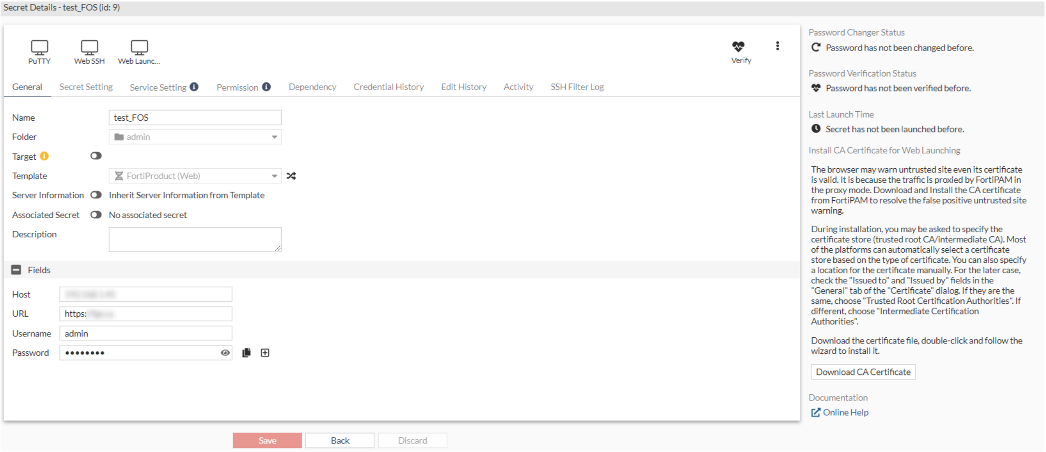
The browser may warn untrusted site even its certificate is valid. It is because the traffic is proxied by FortiPAM in the proxy mode. Download and Install the CA certificate from FortiPAM to resolve the false positive untrusted site warning.

During installation, you may be asked to specify the certificate store (trusted root CA/intermediate CA). Most of the platforms can automatically select a certificate store based on the type of certificate. You can also specify a location for the certificate manually. For the later case, check the "Issued to" and "Issued by" fields in the "General" tab of the "Certificate" dialog. If they are the same, choose "Trusted Root Certification Authorities". If different, choose "Intermediate Certification Authorities".

Download the certificate file, double-click and follow the wizard to install it.

To change or verify the password:

1. Go to *Secrets* > *Secrets*.
2. Double-click the secret created in Configuring a web FortiProduct secret to open it.



Secret Details - test_FOS (id: 9)

Name: test_FOS
Folder: admin
Target
Template: FortiProduct (Web)
Server Information: Inherit Server Information from Template
Associated Secret: No associated secret
Description

Fields

Host: [redacted]
URL: https:[redacted]
Username: admin
Password: ••••••••

Password Changer Status
Password has not been changed before.

Password Verification Status
Password has not been verified before.

Last Launch Time
Secret has not been launched before.

Install CA Certificate for Web Launching

The browser may warn untrusted site even its certificate is valid. It is because the traffic is proxied by FortiPAM in the proxy mode. Download and Install the CA certificate from FortiPAM to resolve the false positive untrusted site warning.

During installation, you may be asked to specify the certificate store (trusted root CA/intermediate CA). Most of the platforms can automatically select a certificate store based on the type of certificate. You can also specify a location for the certificate manually. For the later case, check the "Issued to" and "Issued by" fields in the "General" tab of the "Certificate" dialog. If they are the same, choose "Trusted Root Certification Authorities". If different, choose "Intermediate Certification Authorities".

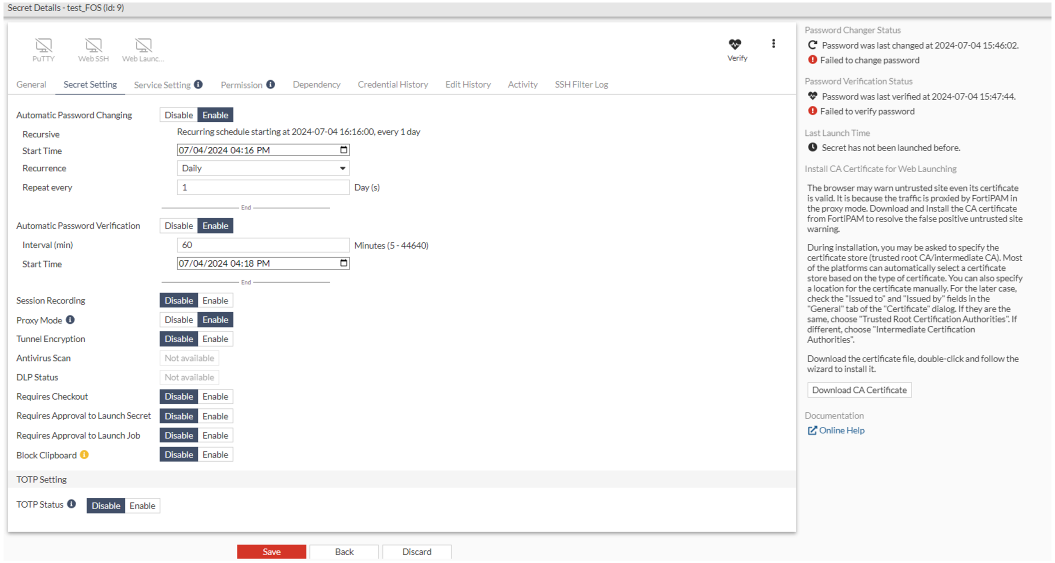
Download the certificate file, double-click and follow the wizard to install it.

3. To change the password, from More options, select *Change Password*:
   The *Generate next password* dialog opens.
   a. In *Generate next password*, select *Randomly*.
   b. Click *OK*.
   c. Click *Save*.
4. To verify the password, select the *Verify* (♥) icon from the top-right.
   Once the password has been verified, *Password Verification Status* shows the date and time when the password was verified and its status.

To schedule a regular password change or verification:

1. Go to *Secrets* > *Secrets*.
2. Double-click the secret created in Configuring a web FortiProduct secret to open it.
3. Go to the *Secret Setting* tab.

4. Enable *Automatic Password Changing*:
   a. In *Start Time*, select the Calendar icon, and select a date and time.
   b. In *Recurrence*, select *Daily*.
   c. In *Repeat every*, enter `1`.
5. Enable *Automatic Password Verification*:
   a. In *Interval*, enter `60`, in minutes.
   b. In *Start Time*, select the Calendar icon, and select a date and time.
6. Click *Save*.



Secret Details - test_FOS (id: 9)

Automatic Password Changing: Disable [✓ Enable]
Recursive: Recurring schedule starting at 2024-07-04 16:16:00, every 1 day
Start Time: 07/04/2024 04:16 PM
Recurrence: Daily
Repeat every: 1 Day (s)
End

Automatic Password Verification: Disable [✓ Enable]
Interval (min): 60 Minutes (5 - 44640)
Start Time: 07/04/2024 04:18 PM
End

Session Recording: [✓ Disable] Enable
Proxy Mode: Disable [✓ Enable]
Tunnel Encryption: [✓ Disable] Enable
Antivirus Scan: Not available
DLP Status: Not available
Requires Checkout: [✓ Disable] Enable
Requires Approval to Launch Secret: [✓ Disable] Enable
Requires Approval to Launch Job: [✓ Disable] Enable
Block Clipboard: [✓ Disable] Enable

TOTP Setting
TOTP Status: [✓ Disable] Enable

Password Changer Status
Password was last changed at 2024-07-04 15:46:02.
Failed to change password

Password Verification Status
Password was last verified at 2024-07-04 15:47:44.
Failed to verify password

Last Launch Time
Secret has not been launched before.

Install CA Certificate for Web Launching

The browser may warn untrusted site even its certificate is valid. It is because the traffic is proxied by FortiPAM in the proxy mode. Download and Install the CA certificate from FortiPAM to resolve the false positive untrusted site warning.

During installation, you may be asked to specify the certificate store (trusted root CA/intermediate CA). Most of the platforms can automatically select a certificate store based on the type of certificate. You can also specify a location for the certificate manually. For the later case, check the "Issued to" and "Issued by" fields in the "General" tab of the "Certificate" dialog. If they are the same, choose "Trusted Root Certification Authorities". If different, choose "Intermediate Certification Authorities".

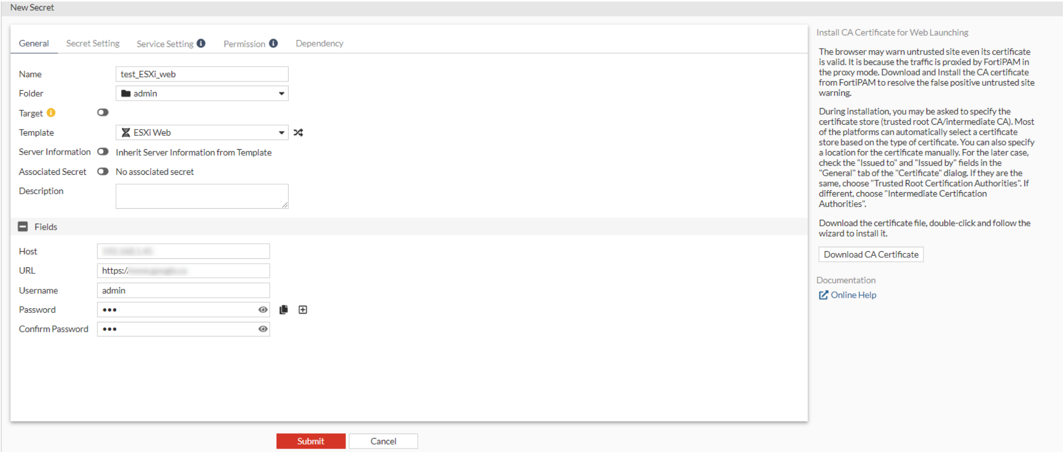
Download the certificate file, double-click and follow the wizard to install it.

Configuring an ESXi web secret - Example

To configure an ESXi web secret:

1. Go to *Secrets* > *Secrets*.
2. In *Secrets*, select *Create*.
   The *Create New Secret in:* dialog opens.
3. Select the folder where you intend to add the secret.
4. Select *Create*.
   The *New Secret* window opens.
5. Enter a name for the secret.
6. Disable *Target*.
7. In the *Template* dropdown, select the *ESXi Web* template.
8. In the *Fields* pane:
   a. In *Host*, enter the IP address or the FQDN of the web-based ESXi server.
   b. In *URL*, enter the URL of the web-based ESXi server.
   c. In *Username*, enter the user name.
   d. In *Password*, enter the password.
   e. In *Confirm Password*, reenter the password.

9. Click *Submit*.



Name: test_ESXi_web
Folder: admin
Target
Template: ESXi Web
Server Information: Inherit Server Information from Template
Associated Secret: No associated secret
Description
Host: [redacted]
URL: https:/[redacted]
Username: admin
Password: •••
Confirm Password: •••

Install CA Certificate for Web Launching

The browser may warn untrusted site even its certificate is valid. It is because the traffic is proxied by FortiPAM in the proxy mode. Download and Install the CA certificate from FortiPAM to resolve the false positive untrusted site warning.

During installation, you may be asked to specify the certificate store (trusted root CA/intermediate CA). Most of the platforms can automatically select a certificate store based on the type of certificate. You can also specify a location for the certificate manually. For the later case, check the "Issued to" and "Issued by" fields in the "General" tab of the "Certificate" dialog. If they are the same, choose "Trusted Root Certification Authorities". If different, choose "Intermediate Certification Authorities".

Download the certificate file, double-click and follow the wizard to install it.

Documentation
Online Help

To change or verify the password or schedule a regular password change or verification, see related instructions in Configuring a web FortiProduct secret Example on page 107.

Configuring and accessing a secret that uses an approval profile with custom fields - Example

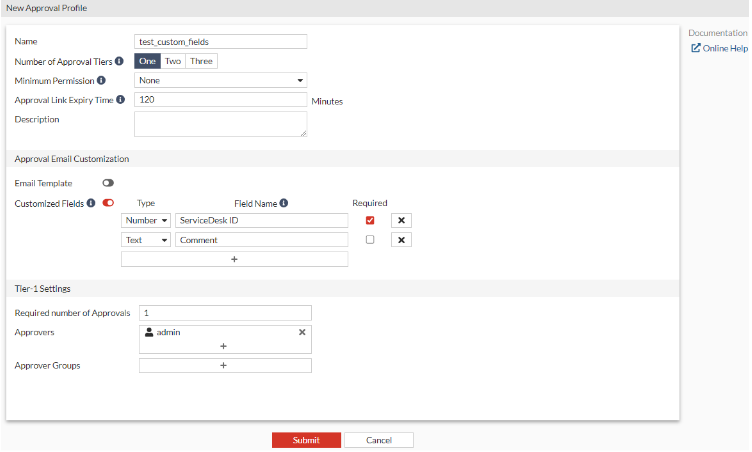
In this example, we request access to a secret where an approval profile is applied that requires custom fields.

To configure an approval profile with custom fields:

1. Go to *Secret Settings* > *Approval Profile* and select *Create*.
   The *New Approval Profile* window opens.
2. In *Name*, enter a name for the approval profile.
3. In *Number of Approval Tiers*, select *One*.
4. In the *Approval Email Customization* pane:
   a. Enable *Customized Fields*.
   b. In *Type*, select *Number*.
   c. In *Field Name*, enter the custom field name.
      This is the name displayed in the *New secret request* window when a user requests access to the secret.
   d. Select *Required* to make the field mandatory.
   e. Select + to add another custom field.
   f. In *Type*, select *Text*.
   g. Enter field name.
   h. Leave *Required* as unselected.
      Two custom fields have been configured, one *ServiceDesk ID* (Number) with *Type* as *Number*, which is mandatory. The field captures a numeric identifier related to a service desk ticket number. Since the field is required, you must enter a valid number before submitting the request.

      The other field is *Comment* (Text). The *Type* is *Text* and the field is optional. The field allows you to provide additional comments for the request.
5. In *Tier-1 Settings*:
   a. Ensure that *Required number of Approvals* is `1`.
   b. In *Approvers* dropdown, select an approver.

6. Click *Submit*.



New Approval Profile

Name	test_custom_fields
Number of Approval Tiers	One (selected) Two Three
Minimum Permission	None
Approval Link Expiry Time	120 Minutes
Description	

Approval Email Customization

Email Template ○

Customized Fields ●

Type	Field Name	Required
Number	ServiceDesk ID	☑
Text	Comment	□

Tier-1 Settings

Required number of Approvals	1
Approvers	admin
Approver Groups	

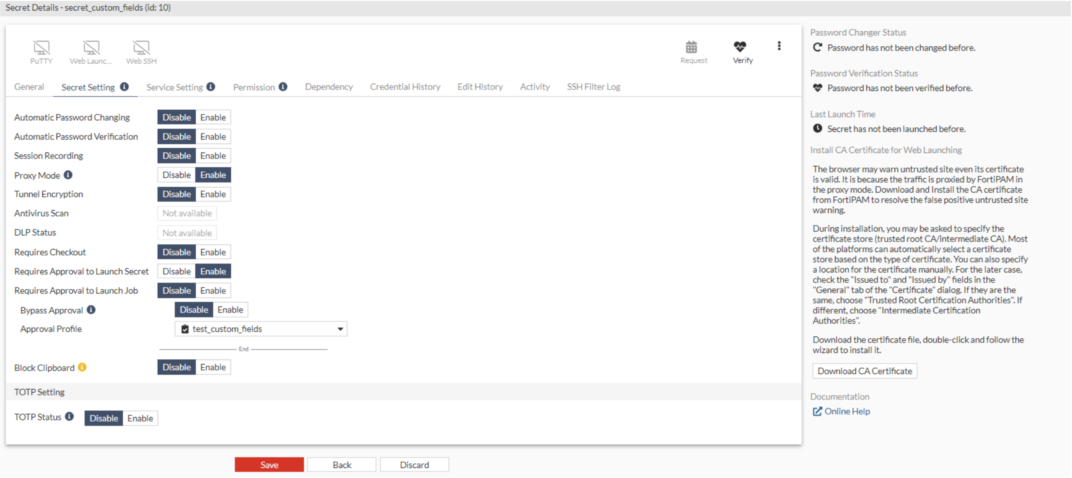
Alternatively, in the CLI console, enter the following commands to create a secret approval profile:

```
config secret approval-profile
 edit "test_apporoval_custom_field"
  set type single
  set first-num 1
  set first-user "admin"
  set description ''
  set remote-group-email disable
  set approver-perm-req none
  set email-template ''
  set email-approval-link-expiry 120
  config field
   edit "ServiceDesk ID"
    set type number
    set mandatory enable
   next
   edit "Comment"
    set type text
    set mandatory disable
   next
  end
 next
end
```

To apply the approval profile to a secret:

1. Go to *Secrets* > *Secrets*.
2. From the list, double-click the secret where you will apply the approval profile created in Creating an approval profile.
   The *Secret Details* window opens.
3. Go to the *Secret Setting* tab, enable *Requires Approval to Launch Secret*, and from the *Approval Profile* dropdown select the approval profile created in Creating an approval profile.

4. Click *Save*.



Automatic Password Changing	Disable
Automatic Password Verification	Disable
Session Recording	Disable
Proxy Mode	Enable
Tunnel Encryption	Disable
Antivirus Scan	Not available
DLP Status	Not available
Requires Checkout	Disable
Requires Approval to Launch Secret	Enable
Requires Approval to Launch Job	Disable
Bypass Approval	Disable
Approval Profile	test_custom_fields
Block Clipboard	Disable
TOTP Setting	
TOTP Status	Disable

Password Changer Status

Password has not been changed before.

Password Verification Status

Password has not been verified before.

Last Launch Time

Secret has not been launched before.

Install CA Certificate for Web Launching

The browser may warn untrusted site even its certificate is valid. It is because the traffic is proxied by FortiPAM in the proxy mode. Download and Install the CA certificate from FortiPAM to resolve the false positive untrusted site warning.

During installation, you may be asked to specify the certificate store (trusted root CA/intermediate CA). Most of the platforms can automatically select a certificate store based on the type of certificate. You can also specify a location for the certificate manually. For the later case, check the "Issued to" and "Issued by" fields in the "General" tab of the "Certificate" dialog. If they are the same, choose "Trusted Root Certification Authorities". If different, choose "Intermediate Certification Authorities".

Download the certificate file, double-click and follow the wizard to install it.

Documentation

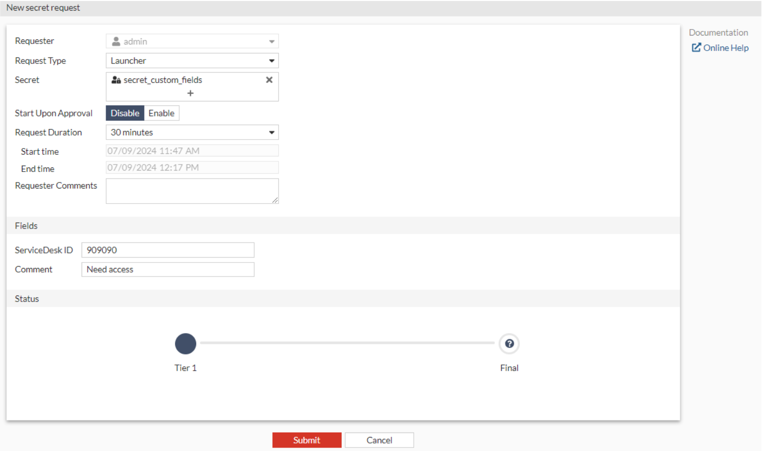
Alternatively, in the CLI console enter the following commands to apply the approval profile to a secret:

```
config secret database
  edit 1
   set name "secret_custom_fields"
   set need-approval enable
   set approval-profile "test_custom_fields"
  next
end
```

To make a secret access request:

1. Go to *Secrets* > *Secrets*.
2. From the list, double-click the secret used in Applying an approval profile to a secret to open it.
3. From the top-right, click the *Request* (▦) icon.
   The *New secret request* window opens.
4. From the *Request Duration* dropdown, select a duration for which you will need access to the secret.
5. In *Fields*, enter the custom fields.
   ServiceDesk ID is the service desk ID for the request. Here, it is `909090`.
   Optionally, enter additional comments for this request.
   These are the custom fields set up in Creating an approval profile.

6. Click *Submit*.



New secret request

Requester admin
Request Type Launcher
Secret secret_custom_fields
Start Upon Approval Disable Enable
Request Duration 30 minutes
Start time 07/09/2024 11:47 AM
End time 07/09/2024 12:17 PM
Requester Comments

Fields

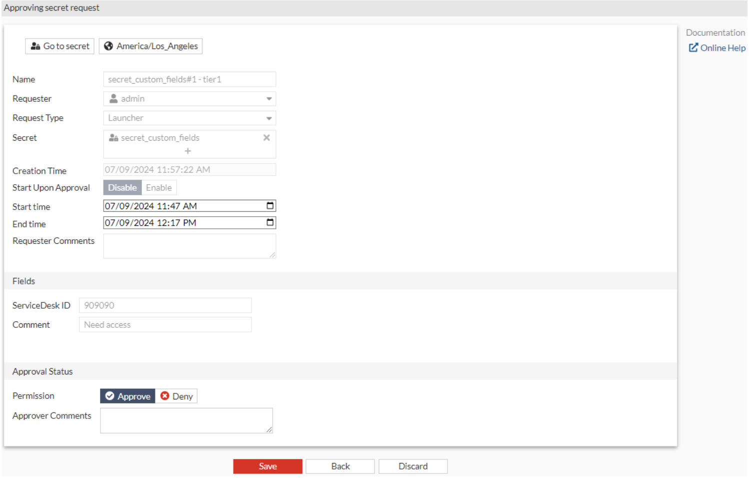
ServiceDesk ID 909090
Comment Need access

Status

Once you have submitted the request, the approver receives an email notification (if set up). Alternatively, when the approver logs in to FortiPAM, a pending request alert is displayed on the banner.

To approve the secret access request:

1. Go to *Secrets* > *Approvals*.
2. From the secret access request in *Waiting for Approval*, double-click to open it.
   The *Approving secret request* window opens.
3. In *Approval Status*, select *Approve*.
4. Optionally, enter comments about the approval in *Approver Comments*.
5. Click *Save*.



Approving secret request

Name secret_custom_fields#1 - tier1
Requester admin
Request Type Launcher
Secret secret_custom_fields
Creation Time 07/09/2024 11:57:22 AM
Start Upon Approval Disable Enable
Start time 07/09/2024 11:47 AM
End time 07/09/2024 12:17 PM
Requester Comments

Fields

ServiceDesk ID 909090
Comment Need access

Approval Status

Permission Approve Deny
Approver Comments

Targets

Go to *Secrets* > *Targets* to create targets.

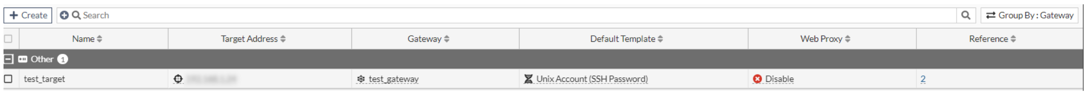
A target is a server/device with a privileged account supporting RDP, SSH, Web, or other admin protocols. Target systems include Windows workstation, Windows domain controller, Web server, Unix server, SQL- server, router, or firewall.

You can create targets for the secrets stored in FortiPAM. One target can be used for multiple secrets, if appropriate.

Using the *Group By* option, you can group group the targets by gateway or tag.

For each target; name, target address, gateway, default template, web proxy, and references are displayed by default when grouped by gateway.

For each target; name, target address, classification tag, default template, web proxy, and references are displayed by default when grouped by tag.



□	Name	Target Address	Gateway	Default Template	Web Proxy	Reference
⊟	Other 1					
□	test_target	[redacted]	test_gateway	Unix Account (SSH Password)	Disable	2

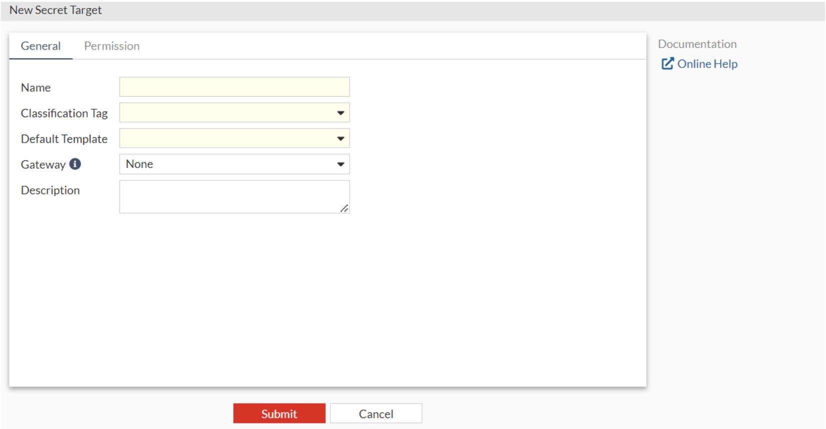
The *Targets* tab contains the following options:

+Create	Select to create a target. See Creating a target on page 114.
Search	Enter a search term in the search field, then hit `Enter` to search the targets. To narrow down your search, see Column filter.
Edit	Select to edit the selected targets.
List Secrets	Select to list the secrets that are using the selected target.
Delete	Select to delete the selected targets.

Creating a target

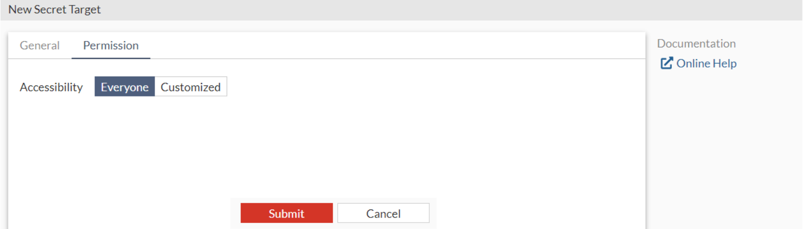
To create a secret target:

1. Go to *Secrets* > *Targets*.
2. Select +*Create*.
   The *New Secret Target* window opens to the *General* tab.


New Secret Target

Name
Classification Tag
Default Template
Gateway: None
Description

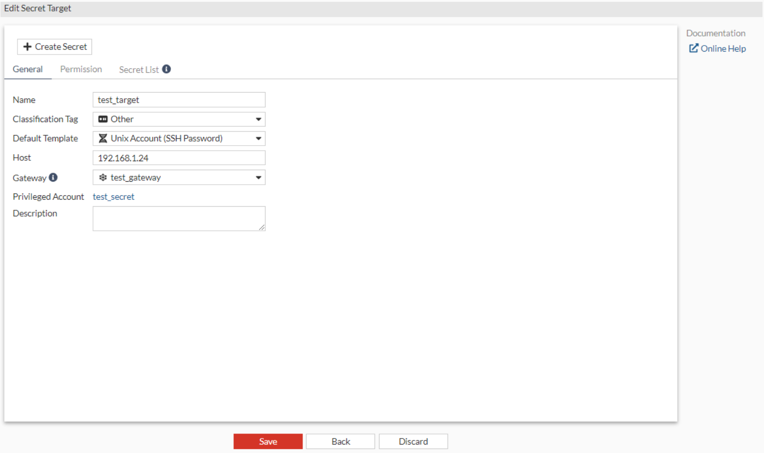
3. Select *Permission* from the top to switch to the *Permission* tab.


New Secret Target

Accessibility: Everyone | Customized

4. Enter the following information:

General	
Name	Name of the target.
Classification Tag	From the dropdown, select a classification tag.
Default Template	From the dropdown, select a secret template. The secret template must include a *Target-Address*, *Domain*, or *URL* field to be included in the dropdown list. If the *Default Template* is changed after the target has been assigned to a secret, the *Template* will not change in the secret. The related secret(s) must be updated, as needed. See Creating a secret on page 72. When editing a secret target that uses *Microsoft SQL* as the default template, you can enable logging on the SQL server, set the maximum log entry size, and monitor all or a specific database using the new *SQL Log* tab. **Limitations:** **1.** Only SSMS client version 19 supported. **2.** Database match is not supported by the Microsoft SQL CLI. See Microsoft SQL server Management Studio (SSMS) monitoring and logging on page 120.
Gateway	From the dropdown, select a gateway (default = *None*).

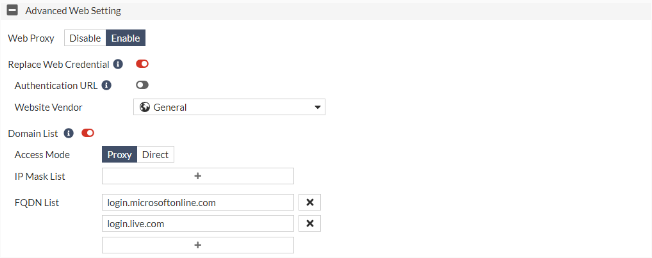
	A gateway, e.g., a FortiGate, FortiProxy, or a FortiPAM device, is used when a target is not reachable directly from FortiPAM. It allows you to proxy the connection to the target. See Gateway on page 124. Use the search bar to look up a gateway.
Privileged Account	When editing a secret target, you can see if the target already has a privileged account.  Edit Secret Target Name: test_target Classification Tag: Other Default Template: Unix Account (SSH Password) Host: 192.168.1.24 Gateway: test_gateway Privileged Account: test_secret Description: + Create Secret General Permission Secret List Documentation Online Help Save Back Discard
Target-Address	The target address. This option is only available when the *Target-Address* field type is included in the selected *Default Template*. If the field is mandatory, it must be included when configuring the target.
Domain	The domain for the server. This option is only available when the *Domain* field type is included in the selected *Default Template*. If the field is mandatory, it must be included when configuring the target.
Common Name	The user ID in the LDAP server. The default is `sAMAccountName`. This option is only available after entering a *Domain*.
DN Search Base	The distinguished name search base in the LDAP server. The default is "CN=users, DC=A, DC=B, DC=C" for A.B.C domain. This option is only available after entering a *Domain*.
LDAPS Minimum SSL Version	From the dropdown, select the minimum SSL version. The default is *Follow system global setting*. This option is only available after entering a *Domain*.
LDAPS Port	The server port. The default is `636`. This option is only available after entering a *Domain*.
WinRM HTTPS	Enable or disable Windows Remote Management (WinRM) over HTTPs.
URL	The URL for the target.

	This option is only available when the *URL* field type is included in the selected *Default Template*. If the field is mandatory, it must be included when configuring the target.
Description	A description for the target.

Advanced Web Setting

These settings are only available in the *General* tab when the *URL* option is populated.

The following shows a configured *Advanced Web Setting* pane.



Advanced Web Setting

Web Proxy: Disable [✓ Enable]

Replace Web Credential: ● (on)

Authentication URL: ○ (off)

Website Vendor: General

Domain List: ● (on)

Access Mode: [✓ Proxy] Direct

IP Mask List: +

FQDN List: login.microsoftonline.com ✕
login.live.com ✕
+

Web Proxy

Enable or disable a web proxy for the target.

When accessing a target using the FortiPAM browser extension, the browser extension sends the browser requests through the FortiPAM web proxy. FortiPAM dynamically operates on the web browser tab's PAC rule (on Google Chrome and Microsoft Edge) to successfully proxy the traffic to FortiPAM based on the configured domain. On Mozilla Firefox, FortiPAM sends the request to the web proxy instead.

FortiPAM scans the incoming web traffic and can replace the password.

> Using web proxy, you do not require FortiClient to launch the proxied web account secret.

To enable the web proxy feature, you must first enable the feature globally for the interface that handles incoming and outgoing traffic using the following CLI commands:

```
config system interface
 edit "port1"
  set explicit-web-proxy enable #must be enabled
 next
end
```

Alternatively, you can enable the feature by enabling *Explicit web proxy* for the interface that handles incoming and outgoing traffic. See Editing an interface on page 358.

Notes:

- The option is disabled by default.
- The *Web Proxy* setting is inherited by the secret using the target. See Creating a secret on page 72.

For more information on the web proxy feature, see Web proxy on page 122.

Replace Web Credential	Enable to replace the website authentication credential. Disable to keep the website credential. The default is disabled.
Authentication URL	Enable and enter the website authentication URL. **Note**: You can enter the authentication URL to prevent deep scanning of all the requests.
Website Vendor	Select from the following two options for web proxy password replacement: • *General* (default) • *vCenter*
Domain List	Enable to create a domain list.
Access Mode	Select *Direct* or *Proxy* for the domain access mode.
IP Mask List	Click + to add a domain to the list. Enter the IP mask. Click *x* to delete a domain from the list.
FQDN List	Click + to add a domain to the list. Enter the fully qualified domain name. Click *x* to delete a domain from the list.
Permission	
Accessibility	Target accessible to: • *Everyone*: All users have *Read/Write* permission for templates (default). • *Customized*: A user permission and a group permission table must be configured.
Create Secret	From the list, select user/user groups with the ability to see and use the target to create secrets. The option is only available when *Accessibility* is set to *Customized*.
Owner	From the list, select user/user groups with the highest possible permission level with the ability to create secrets using the target and to edit and delete the target. Every target must have at least one owner. The option is only available when *Accessibility* is set to *Customized*.

User Permission

1. When creating a secret target, select *Customized* in *Accessibility*.
2. In the *Create Secret* dropdown, select users with the ability to see and use the target to create secrets.

3. In the *Owner* dropdown, select users with the highest possible permission level with the ability to create secrets using the target and to edit and delete the target.
4. Click *Submit*.

From the list, click *x* next to an entry to delete it.

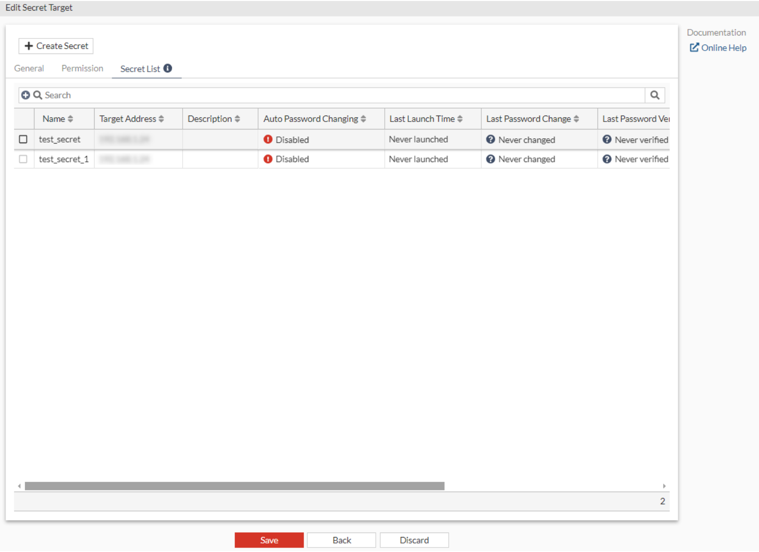
Group Permission

1. When creating a secret target, select *Customized* in *Accessibility*.
2. In the *Create Secret* dropdown, select user groups with the ability to see and use the target to create secrets.
3. In the *Owner* dropdown, select user groups with the highest possible permission level with the ability to create secrets using the target and to edit and delete the target.
4. Click *Submit*.

From the list, click *x* next to an entry to delete it.

Secret list

When editing a secret target, the *Secret List* tab displays all the associated secrets with the secret target.

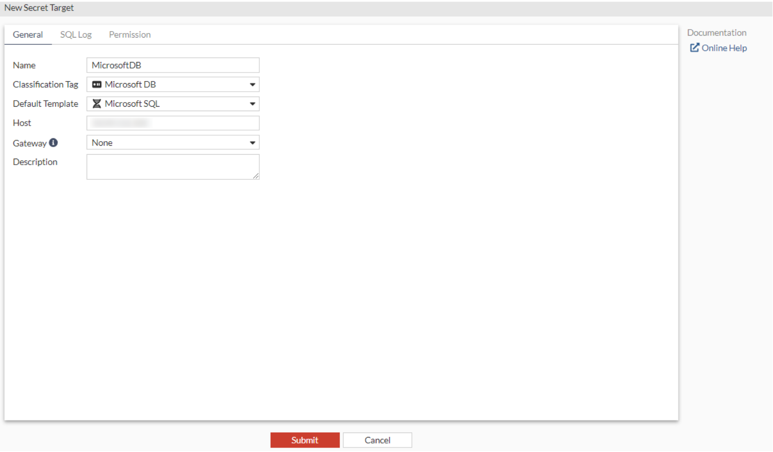


	Name	Target Address	Description	Auto Password Changing	Last Launch Time	Last Password Change	Last Password Ve
□	test_secret	[redacted]		Disabled	Never launched	Never changed	Never verified
□	test_secret_1	[redacted]		Disabled	Never launched	Never changed	Never verified

Microsoft SQL server Management Studio (SSMS) monitoring and logging

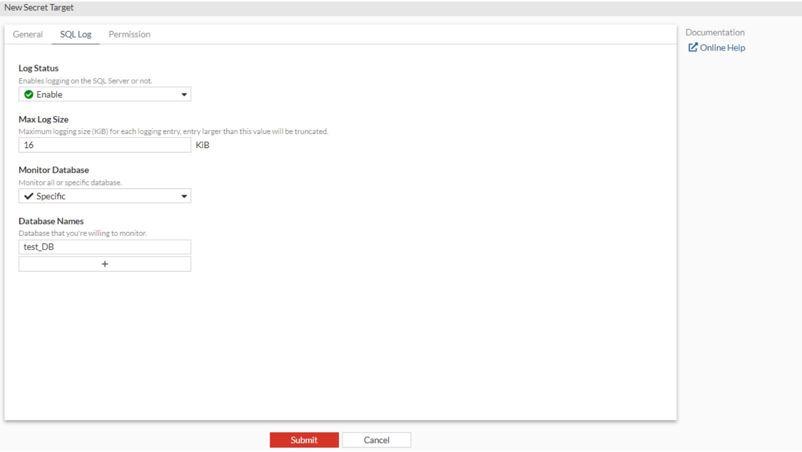
To set up monitoring and logging for the Microsoft SQL server:

1. Go to *Secrets* > *Targets*.
2. Select +*Create*.
   The *New Secret Target* window opens.
3. In the *General* tab:
   a. In *Name*, enter a name for the secret target.
   b. In *Classification Tag*, select a classification tag.
   c. From the *Default Template* dropdown, select *Microsoft SQL* default dropdown.
   d. In *Host*, enter a valid FQDN/IP address.
   e. In *Gateway*, select a gateway to proxy the connection to the target.



Name: MicrosoftDB
Classification Tag: Microsoft DB
Default Template: Microsoft SQL
Host: [redacted]
Gateway: None
Description:

4. In the *SQL* tab:
   a. In *Log Status*, enable to log on the SQL server.
   b. In *Max Log Size*, enter the maximum logging size (in KiB) for each log entry.
      Note: Entries larger than the *Max Log Size* are truncated.
   c. In *Monitor Database*, from the dropdown, select to monitor all or a specific database.
   d. In *Database Name*, enter the database name to be monitored if you are monitoring specific databases.
      Select + to add additional names.



Log Status
Enables logging on the SQL Server or not.
Enable

Max Log Size
Maximum logging size (KiB) for each logging entry, entry larger than this value will be truncated.
16 KiB

Monitor Database
Monitor all or specific database.
Specific

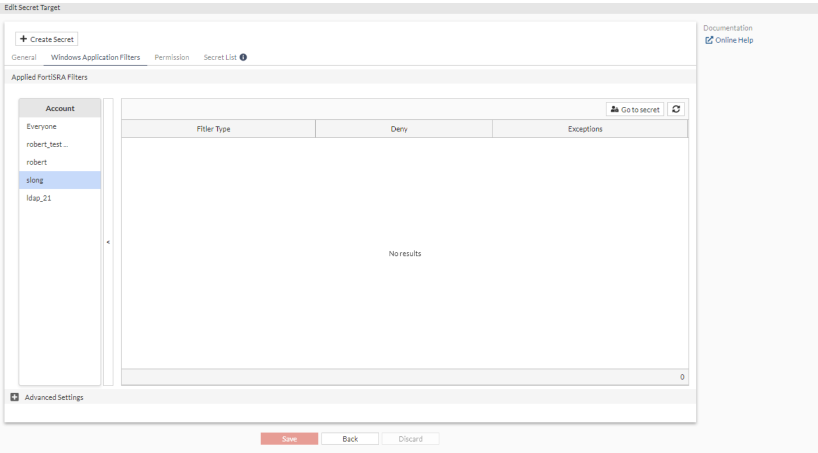
Database Names
Database that you're willing to monitor.
test_DB

5. For the *Permission* tab, see User Permission on page 118 and Group Permission on page 119.
6. Click *Submit*.

Windows application filters

For information on Windows application filters, see Window app filter on page 242.

The *Windows Application Filters* tab appears when a Windows application filter is applied to the secret under a target.



The following options are available:

Account	All the accounts under this target are displayed by their user name, not the secret name. You can select different accounts such as *Everyone* or any other account to see specific filters for each user. *Everyone*: Represents all the users including those not managed by FortiPAM. - Example In the screenshot, two additional accounts are displayed: `robert` and `slong`. • `robert` is the privileged account for this target with no filters. • `slong` is the non-privileged account for this target; it will display corresponding filters if there are any.
Applied FortiPAM Filters	*Filter Table*: Displays the filters applied to the selected account including: • *Filter Type*: Type of filter, e.g., Executable, Script, Installer. • *Deny*: The paths or patterns of applications/scripts/installers to be blocked. • *Exceptions*: Paths or patterns exempted from the deny rule.
Go to secret	Select to go to the specific filter.
Advanced Settings Filters configured on FortiPAM should only effect FortiPAM users from accessing certain files. Note that if you want to stop affecting access for a certain FortiPAM user, you should update the corresponding secret or Windows application filter profile instead. Enter Audit Mode where filters including those set from the server are stored but do not take effect. This allows admin to test if non-FortiPAM users accesses are effected by FortiPAM filters.	

Deactivate All Filters	Temporarily disables all FortiPAM filters under this target impacting all users of this target.
Delete FortiPAM Filters	Permanently removes all FortiPAM filters from the target server.

Web proxy

When accessing a target using the FortiPAM browser extension, the browser extension now sends the browser requests through the FortiPAM web proxy. This enhances security by not delivering credential information to the client.

FortiPAM offers the web proxy feature to dynamically operate on the web browser tab's PAC rule (on Google Chrome and Microsoft Edge) to successfully proxy the traffic to FortiPAM based on the configured domain. On Mozilla Firefox, FortiPAM sends the request to the web proxy instead.

Fortinet Privileged Access Agent 7.2.3 or above is required to support the web proxy feature.

FortiPAM scans the incoming web traffic and can replace the password.

The web proxy feature is supported on both extension only deployment and extension with FortiClient deployment.

This section describes how the web proxy feature on FortiPAM works:

1. You log in to FortiPAM on a browser and launch a web account secret.
2. The FortiPAM browser extension requests session information from the FortiPAM.
3. FortiPAM returns the following:
    a. Web account URL
    b. Web proxy address and the port number
    c. Proxy sub domains
    d. Fake password (if *Replace Web Credential* is enabled for the target associated with the secret)
4. The FortiPAM browser extension adds rules for the browsers and sets the proxy address and the port number.
5. The FortiPAM browser extension creates a new tab that opens the URL (target).
6. FortiPAM receives the proxied web traffic and replaces the fake password during authentication.

Password replacement

If the *Authentication URL* is set up, FortiPAM deepscans to see if fake password was used in the request.

If there is no *Authentication URL* set up, FortiPAM checks each request.

FortiPAM stops checking requests once it has detected and replaced the fake password from a request.

Prerequisites

1. You must manually enable `explicit-web-proxy` for the interface that handles incoming and outgoing traffic:

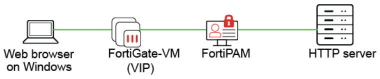
```
config system interface
 edit "port1"
  set explicit-web-proxy enable #must be enabled
 next
end
```

Alternatively, you can enable the feature by enabling *Explicit web proxy* for the interface that handles incoming and outgoing traffic. See Editing an interface on page 358.

2. You must import the related certificate from FortiPAM. Otherwise, the site (target) is not trusted. See Installing CA certificates for web launching on page 91.
3. By default, when using web proxy, port `8080` is the listening port. You can change this using the following CLI commands:

```
config web-proxy explicit-proxy
 edit "web-proxy"
  set status enable
  set interface "any"
  set http-incoming-port 65530 #between 0 - 65535, default = 8080
 next
end
```

4. If the FortiPAM interface cannot be reached from a web browser on Windows as the FortiPAM interface is behind FortiOS, configure a VIP on the FortiOS side to forward to the FortiPAM interface IP and VIP.



You must add the VIP to your DNS server and give it an FQDN.

On the FortiPAM side, add the FQDN to your web proxy configuration using the following CLI commands:

```
config web-proxy global
 set proxy-fqdn [FQDN of FortiOS VIP]
end
```

5. Ensure that the external interface of the firewall VIP is set to the correct port.
If you are on FortiPAM 1.1.0 or above, setting up the external interface of the firewall VIP to the correct port should be done when setting up FortiPAM:

```
config firewall vip
 edit "fortipam_vip"
  set uuid 7b240e68-fa78-51ed-7846-7536d320d9d3
  set type access-proxy
  set extip 172.16.80.209
  set extintf "port2"
  set server-type https
  set extport 443
  set ssl-certificate "Fortinet_SSL"
 next
end
```

See *Configuring the web proxy feature to prevent web credentials from leaking* example in the latest *FortiPAM Examples*.

Gateway

Introduction

FortiPAM supports network gateway for distributed target deployment.

Gateway in *Secrets* displays a list of configured gateways.

Gateway allows accessibility from a FortiPAM located in a public network to a private enterprise network.

You can configure a gateway, e.g., a FortiPAM, a FortiGate, or a FortiProxy device, when a target is not reachable directly from FortiPAM to proxy the connection to the target.

Gateway introduces forward type network gateway, i.e., the connection is from FortiPAM to the network gateway and then to the target. This type of in-bound connection can be blocked by an edge or internal firewall and FortiPAM cannot reach the target via the gateway.

To resolve this deployment restriction, FortiPAM also supports reverse gateway feature.

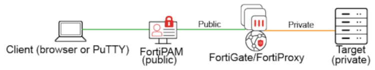
FortiPAM can be reached from a reverse gateway and the reverse gateway makes the first connection to FortiPAM as the control plane connection. This is a persistent connection that uses health checks to detect connection issues and supports reconnection.

Starting FortiOS 7.4.4, FortiPAM gateway is not supported on FortiGate hardware models with 2 GB RAM.

Latest FortiGate version cannot be used to configure a reverse gateway.

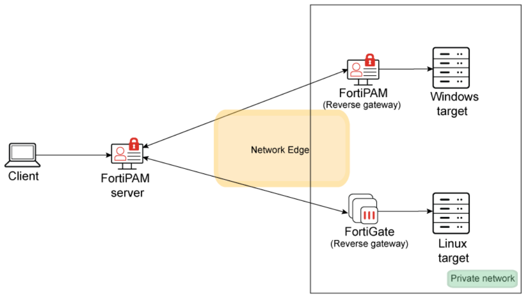
A future FortiGate 7.6.x version will support configuring FortiGate as a reverse gateway.

Forward type



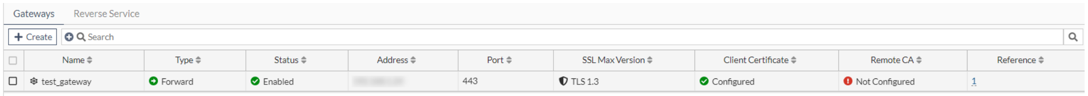
In the forward type scenario, the FortiPAM deployed on a public site cannot reach the target server directly. The target server is in the private enterprise network and deployable at multiple locations. A FortiGate or a FortiProxy device acts as a network gateway. The network gateway can be applied to the target. All connections to the target are now proxied by FortiPAM and the network gateway.

Reverse type



For each gateway, the following columns are displayed by default:

- *Name*
- *Type*
- *Status*
- *Address*
- *Port*
- *SSL Max Version*
- *Client Certificate*
- *Remote CA*
- *Reference*



□	Name ⇕	Type ⇕	Status ⇕	Address ⇕	Port ⇕	SSL Max Version ⇕	Client Certificate ⇕	Remote CA ⇕	Reference ⇕
□	test_gateway	Forward	✓ Enabled	[redacted]	443	TLS 1.3	✓ Configured	! Not Configured	1

The *Gateway* tab contains the following options:

Create	Select to create a new gateway. See Creating a gateway on the FortiPAM GUI on page 126.
Search	Enter a search term in the search field, then hit `Enter` to search the gateway list. To narrow down your search, see Column filter. The following column filters are available: • *Name* • *Type* • *Status* • *Address* • *Port* • *SSL Max Version* • *Client Certificate* • *Remote CA* • *Reference*
Edit	Select to edit the selected gateway.
Delete	Select to delete the selected gateway.

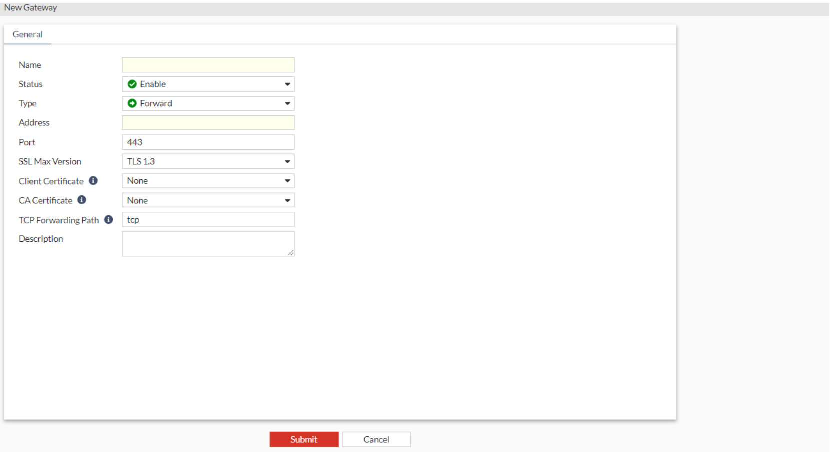
For gateway related CLI configurations, see:

- Creating a gateway on the FortiPAM CLI on page 131
- FortiPAM connects to a target through a FortiProxy acting as the gateway Example on page 133

Creating a gateway on the FortiPAM GUI

To create a gateway:

1. Go to *Secrets* > *Gateway*.
2. In the gateway list, select *Create*.
   The *New Gateway* window opens.



New Gateway

General

Name	
Status	Enable
Type	Forward
Address	
Port	443
SSL Max Version	TLS 1.3
Client Certificate	None
CA Certificate	None
TCP Forwarding Path	tcp
Description	

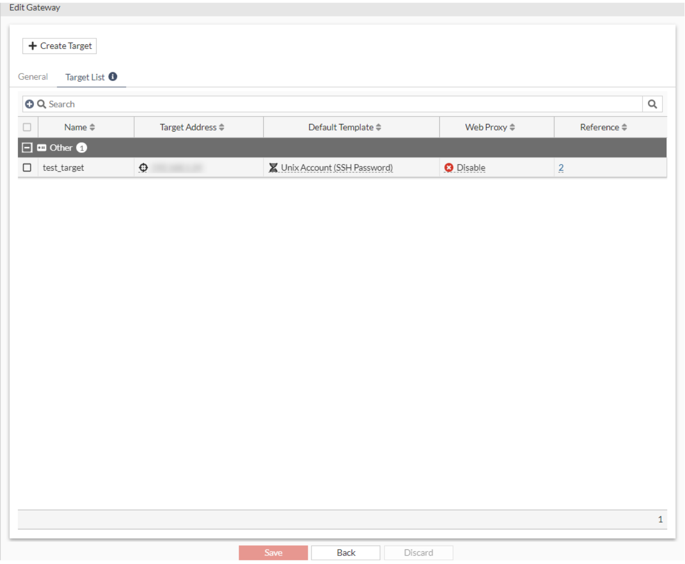
3. Enter the following information:

Name	The name of the gateway.
Status	Enable/disable the gateway (default = *Enable*).
Type	The type of gateway: • *Forward* (default) • *Reverse* To set up a reverse gateway, you must first configure the following: • Reverse service on FortiPAM. See Reverse service on page 128. • Reverse service on the gateway for a reverse connection to the FortiPAM server. See Configuring reverse service on a gateway CLI on page 130. • Traffic proxy on the gateway for forwarding secret launch. See Configuring traffic proxy on gateway CLI on page 130.
Health Check	Enable and enter a time period to periodically check if the gateway is alive, in seconds (default = 60). **Note**: The option is only available when the *Type* is *Reverse*.
Gateway ID	Enter the gateway client certificate common name to create a mapping between FortiPAM and the gateway. **Note**: The option is only available when the *Type* is *Reverse*.
Gateway Address	Enter the gateway IPv4 address. **Note**: The option is only available when the *Type* is *Reverse*.
SNI	Enter the Server Name Indication (SNI) FQDN. **Note**: The option is only available when the *Type* is *Reverse*.
Address	The gateway IP address or FQDN.
Port	The gateway port number (1 - 65535, default = 443).
SSL Max Version	The highest TLS version acceptable from a server: • *TLS 1.1* • *TLS 1.2* • *TLS 1.3* (default) This is the TLS version between FortiPAM and the gateway.
Client Certificate	From the dropdown, select the client certificate for mTLS. This is required if the gateway requests a client certificate.
CA Certificate	From the dropdown, select the CA certificate verification for mTLS. This is used for the gateway certificate verification.
TCP Forwarding Path	The TCP forwarding access proxy path. This is the gateway's URL map for TFAP(TCP Forwarding Application Proxy).
Description	Optionally, enter a description for the gateway.

4. Click *Submit*.

Target list for gateways

When editing a gateway the *Target List* tab displays the targets using the gateway.



□	Name	Target Address	Default Template	Web Proxy	Reference
⊟	Other 1				
□	test_target	[redacted]	Unix Account (SSH Password)	Disable	2

Select +*Create Target* to create a target using the gateway.

Enter a search term in the search field, then hit `Enter` to search the targets.

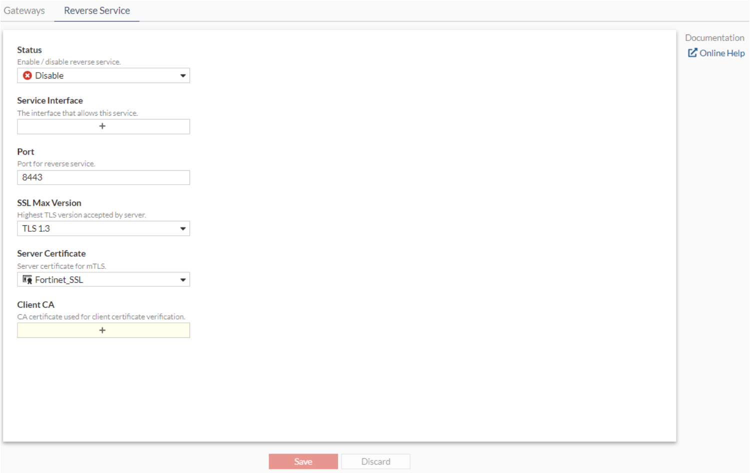
To narrow down your search, see Column filter.

Reverse service

To use the reverse gateway feature, you must first configure reverse service on FortiPAM.

To configure the reverse service:

1. Go to *Secret* > *Gateway*.
2. Select the *Reverse Service* tab.
   The *Reverse Service* tab opens.



Status
Enable / disable reverse service.
Disable

Service Interface
The interface that allows this service.
+

Port
Port for reverse service.
8443

SSL Max Version
Highest TLS version accepted by server.
TLS 1.3

Server Certificate
Server certificate for mTLS.
Fortinet_SSL

Client CA
CA certificate used for client certificate verification.
+

3. Enter the following information:

Status	Enable/disable the reverse service (default = disable).
Service Interface	Select +, from *Select Entries*, select interfaces that allow the reverse service, and click *Close*. The IP address on the selected interface and the port the FortiPAM server listens on to receive the reverse connection from a gateway for the control plane connection. Use the search bar to look up a port.
Port	Enter the port to be used for the reverse service (default = 8443, 1 - 65535).
SSL Max Version	From the dropdown, select the highest TLS version accepted by the server: • *TLS 1.1* • *TLS 1.2* • *TLS 1.3* (default)
Server Certificate	From the dropdown, select a server certificate for control plane mTLS connection (default = `Fortinet_SSL`). Use the search bar to look up a server certificate.
Client CA	Select +, from *Select Entries*, select the CA certificates used for client certificate verification, and click *Close*. Use the search bar to look up a CA certificate.

4. Click *Save*.

Configuring reverse service on a gateway - CLI

We configure the reverse service on the gateway for a reverse connection to the FortiPAM server.

Reverse service can only be configure via the CLI console.

To configure reverse service on a gateway:

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

```
config secret server
 edit "pam_gcp159"
  set status enable
  set address "34.95.41.159" #same as the one on the interface in Service Interface in
Reverse service on page 128
  set port 8443 #same as the one on Port configured in Reverse service on page 128
  set health-check-interval 60
  set set ssl-max-version tls-1.3
  set client-cert "fortipam_gw4.pem"
  set ca "CA_Cert_1"
 next
end
```

Configuring traffic proxy on gateway - CLI

We configure the traffic proxy on the gateway for forwarding secret launch.

Traffic proxy can only be configure via the CLI console.

To configure traffic proxy gateway:

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

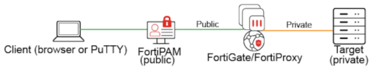
```
config firewall vip
 edit "fortipam_vip_gw"
  set uuid d39c1138-032a-51ef-8508-24d8bb973e7a
  set type access-proxy
  set extip 10.59.112.97
  set extintf "port1"
  set server-type https
  set extport 7443
  set ssl-certificate "Fortinet_SSL"
 next
```

```
end
config firewall access-proxy
 edit "gw_access_proxy"
  set vip "fortipam_vip_gw"
  config api-gateway
   edit 2
    set url-map "/tcp"
    set service tcp-forwarding
    config realservers
     edit 1
      set address "all"
     next
    end
   next
  end
 next
end
config firewall policy
 edit 2
  set type access-proxy
  set uuid 380dc436-032b-51ef-0ef6-a260ec98f34b
  set srcintf "any"
  set srcaddr "all"
  set dstaddr "all"
  set action accept
  set schedule "always"
  set access-proxy "gw_access_proxy"
  set ssl-ssh-profile "deep-inspection"
 next
end
```

`extip` and `extport` in the VIP table are configured in the gateway entry on FortiPAM server to proxy the traffic.

Creating a gateway on the FortiPAM - CLI

FortiPAM now allows configuring a gateway, e.g., a FortiPAM, a FortiGate, or a FortiProxy device, when a target is not reachable directly from FortiPAM to proxy the connection to the target.



To create a gateway:

1. In the CLI console, enter the following commands to configure the gateway:

```
config secret gateway
  edit "test1"
   set status enable #default value
   set type forward #default value
   set address <string>
```

```
    set port 443 #default value
    set sni <string>
    set url-map "tcp" #default value
    set ssl-max-version tls-1.3 #default value
    set client-cert <string>
    set ca <string>
    set description <string>
  next
end
```

Variable	Description
status {enable | disable}	Enable/disable the gateway (default = enable).
type forward	The forward connection mode.
address <string>	The gateway IP address or FQDN.
port <integer>	The gateway port number (1 - 65535, default = 443).
sni <string>	The gateway SNI for TLS. If the `address` is an IP address, the `sni` is the TLS's SNI extension value, which can be used in the gateway for virtual hosting on the same IP address.
url-map <string>	The TCP forwarding access proxy path. This is the gateway's URL map for TFAP(TCP Forwarding Application Proxy).
ssl-max-version {tls-1.1 | tls-1.2 | tls-1.3}	The highest TLS version acceptable from a server (default = tls-1.3). This is the TLS version between FortiPAM and the gateway.
client-cert <string>	The client certificate for mTLS. This is required if the gateway requests a client certificate.
ca <string>	The CA certificate verification for mTLS. This is used for the gateway certificate verification.
description <string>	A description for the gateway.

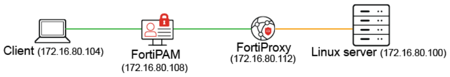
2. In the CLI console, enter the following commands to configure a target with gateway:

```
config secret target
 edit "172.16.80.101"
  set class "Other"
  set templete "Unix Account (SSH Password)"
  set address <string>
  set gateway "test1" #using the gateway created in step 1
  set creation-time <datetime> #syntax yyyy-mm-dd hh:mm:ss, year= 2001-2037
  set web-proxy-status disable
 next
end
```

See FortiPAM connects to a target through a FortiProxy acting as the gateway Example on page 133.

FortiPAM connects to a target through a FortiProxy acting as the gateway - Example

Topology



FortiPAM configuration:

1. In the FortiPAM CLI console, enter the following commands to create the FortiProxy gateway:

```
config secret gateway
 edit test_gateway
  set address "172.16.80.112"
  set port 443
  set url-map "tcp"
  set ssl-max-version tls-1.3
 next
end
```

2. In the FortiPAM CLI console, enter the following commands to create the secret target (Linux server):

```
config secret target
 edit "172.16.80.100"
  set class "Other"
  set template "Unix Account (SSH Password)"
  set address "172.16.80.100"
  set gateway "test_gateway" #from step 1
  set creation-time 2023-11-10 09:34:23
  set web-proxy-status  disable
 next
end
```

FortiProxy configuration:

1. In the FortiProxy CLI console, enter the following commands to configure a VIP:

```
config firewall vip
  edit "test_vip"
   set type access-proxy
   set server-type https
   set extip 172.16.80.112
   set extintf "any"
   set h2-support disable
   set extport 443
   set ssl-certificate "Fortinet_GUI_Server"
   set ssl-min-version tls-1.3
  next
 end
```

2. In the FortiProxy CLI console, enter the following commands to configure an IPv4 access proxy:

```
config firewall access-proxy
 edit "test_access_proxy"
  set vip "test_vip" #from step 1
  set client-cert disable
```

```
    set auth-portal enable
    config api-gateway
     edit 1
      set url-map "/tcp"
      set service tcp-forwarding
      config realservers
       edit 1
        set address "all"
       next
      end
     next
    end
   next
  end
```

3. In the FortiProxy CLI console, enter the following commands to configure a firewall proxy:

```
config firewall policy
 edit 1
  set type access-proxy
  set srcintf "any"
  set srcaddr "all"
  set dstaddr "all"
  set action accept
  set schedule "always"
  set access-proxy "test_access_proxy" #from step 2
 next
end
```

Personal/public folder

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

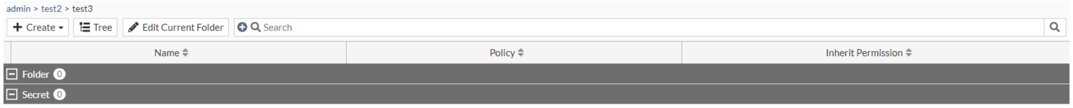
Before you create any secret, you should choose a folder where the secret is added.

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

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

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

The following shows a folder with secrets in it:



Name	Policy	Inherit Permission
⊟ Folder 0		
⊟ Secret 0		

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

Create	From the dropdown, create a secret or a folder. See Creating a secret on page 72 and Creating a folder on page 139.
Tree	Select to open the folder tree. You can use this option to go to a folder. See Opening a folder on page 136.
Edit Current Folder	Edit the current folder.
Search	Enter a search term in the search field, then hit `Enter` to search the folders list. To narrow down your search, see Column filter.
Delete	Delete selected folders or secrets. See Delete a subfolder or a secret.

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

Click the predecessor folder from the path breadcrumb to go to the predecessor folder.

Opening a folder

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

To open a folder:

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

Moving a subfolder

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

To move a subfolder:

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

Moving a secret to a different folder

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

To move a secret:

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

3. Right-click the secret and select *Move*.
   The *Move* window opens.
4. Select the destination folder from the tree and then select *Move*.

Moving multiple secrets to a different folder

To move multiple secrets to a different folder:

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

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

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

Editing a subfolder or a secret:

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

To edit a subfolder or a secret:

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

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

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

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

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

See Creating a folder on page 139 and Creating a secret on page 72.

5. Click *Save*.

Deleting a subfolder or a secret:

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

To delete a subfolder or a secret:

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

   You can only delete an empty folder.

Adding a favorite secret

To add a favorite secret:

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

Removing a secret from favorite

To remove a secret from favorite:

1. Go to *Favorite Secrets* in the tree menu.
2. In the page that lists favorite secrets, right-click a secret and then select *Remove Favorite* to remove the secret from *Favorite Secrets*.

You can now add/remove multiple secrets to/from the favorite list by selecting the secrets, right-clicking on any of the selected secrets, and then selecting either *Add/Remove Favorite*.

Alternatively, having selected the secrets, click *Add/remove Favorite* from the top.

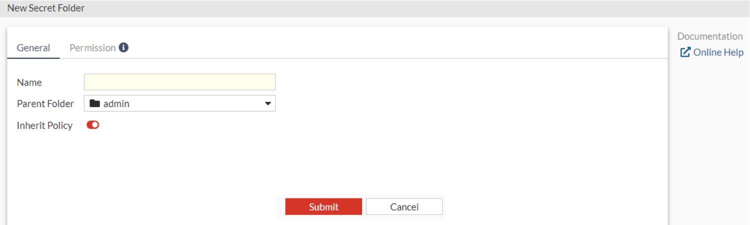
Creating a folder

To create a folder:

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

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

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



Name
Parent Folder: admin
Inherit Policy

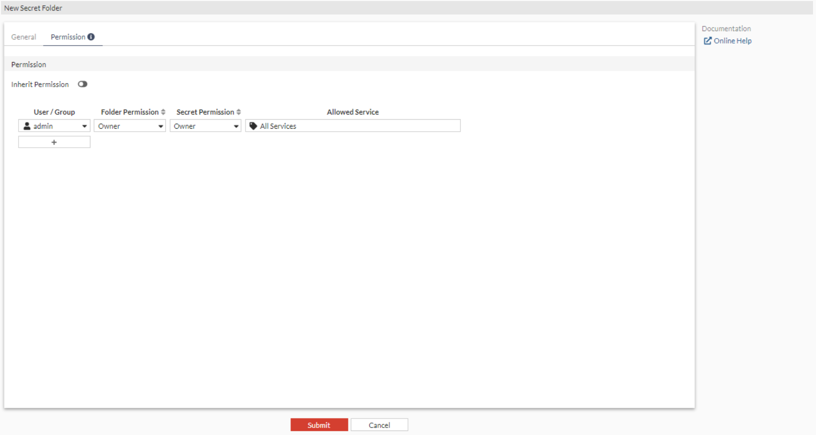
5. Enter the following information:

General	
Name	Name of the folder.
Parent Folder	From the dropdown, select a parent folder or select *Create* to create a new parent folder. The parent folder is set in step 2. The parent folder cannot be changed for a root folder. Use the search bar to look for a folder. Use the pen icon next to the folder to edit it.
Inherit Policy	Enable to inherit policy that applies to the parent folder.

	The option is enabled by default when creating a subfolder. You cannot inherit policy for a root folder.
Secret Policy	From the dropdown, select a policy that applies to the folder or select *Create* to create a new policy. See Creating a policy on page 185. Use the search bar to look for a policy. Use the pen icon next to the policy to edit it. This option is only available when *Inherit Policy* is disabled.

Permission

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



New Secret Folder

Permission

Inherit Permission ○

User / Group	Folder Permission	Secret Permission	Allowed Service
admin	Owner	Owner	All Services

ZTNA

Inherit ZTNA Control	Enable to inherit ZTNA control access permission from the parent folder. When configuring a subfolder, FortiPAM displays the ZTNA control settings from the parent folder.

	By default, secrets in a folder follow the ZTNA control set up in the parent folder. However, when creating or editing a secret you can customize the ZTNA control in the *Secret Permission* tab. See Creating a secret on page 72. The option is enabled by default when creating a subfolder. You cannot inherit ZTNA control access permission for a root folder.
ZTNA Control	Enable to limit access by `ztna-ems-tag`. You can choose whether to match all the tags or only one of them. The option is only available when *Inherit ZTNA Control* is disabled.
Device Tags	Select + to add ZTNA tags or groups. Use the search bar to look up a ZTNA tag or ZTNA tag group. Only permitted devices with the selected tags are allowed to launch.
Device Match Logic	Define the match logic for the device tags: • *OR*: Devices with any of the selected tags are allowed to launch. • *AND*: Devices must acquire all the selected tags to launch.
Inherit Permission	Enable to inherit permission from the parent folder. The option is enabled by default when creating a subfolder. You cannot inherit permission for a root folder. **Note**: The setting can only be disabled if you have the *Owner* permission. Also, the setting cannot be disabled for any subfolder of the personal folder, i.e., the folder generated for every user.
Permission	

The level of user/user group access to the folder and secrets in the folder.
See User Permission on page 142 and Group Permission on page 143.

6. Click *Submit*.

User Permission

To create a user permission:

1. In step 4 when Creating a folder, select the user from the *User/Group* dropdown in the *Permission* pane.

To add a new user:
1. Select + and then select +*User List*.
   The *New User List* wizard opens.
2. Follow the steps in Creating a user on page 253, starting step 2 to create a new user.

Use the search bar to look up a user.

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

2. In the *Folder Permission* dropdown, select from the following:
   - *View*: Ability to view secrets and subfolders in the folder.
   - *Add Secret*: Ability to create new secrets.
   - *Edit*: Ability to create/edit secrets, subfolders, and the folder itself.
   - *Owner*: The highest possible permission level with the ability to create, edit, delete, and move secrets, subfolders, and the folder itself.
3. In the *Secret Permission* dropdown, select from the following:
   - *View*: Ability to view secret details and launch a secret.
   - *Edit*: Ability to create/edit secrets and launch the secrets.
   - *Owner*: The highest possible permission level with the ability to create, edit, delete, move, and launch secrets.
4. In *Allowed Service*, from the *Select Entries* list, select the services, click *Close*.

Use the search bar to look up a service.

5. Click *Submit*.

From the list, click *x* next to a user permission entry to delete it.

Group Permission

To create group permission:

1. In step 4 when Creating a folder, select the user group from the *User/Group* dropdown.

   To add a new user group:
   1. Select + and then select +*User Group*.
      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.

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

2. In the *Folder Permission* dropdown, select from the following:
   - *View*: Ability to view secrets and subfolders in the folder.
   - *Add Secret*: Ability to create new secrets.
   - *Edit*: Ability to create/edit secrets, subfolders, and the folder itself.
   - *Owner*: The highest possible permission level with the ability to create, edit, delete, and move secrets, subfolders, and the folder itself.
3. In the *Secret Permission* dropdown, select from the following:
   - *View*: Ability to view secret details and launch a secret.
   - *Edit*: Ability to create/edit secrets and launch the secrets.
   - *Owner*: The highest possible permission level with the ability to create, edit, delete, move, and launch secrets.
4. In *Allowed Service*, from the *Select Entries* list, select the services, click *Close*.

   Use the search bar to look up a service.

5. Click *Submit*.

   From the list, click *x* next to a group permission entry to delete it.

My requests list

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

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

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

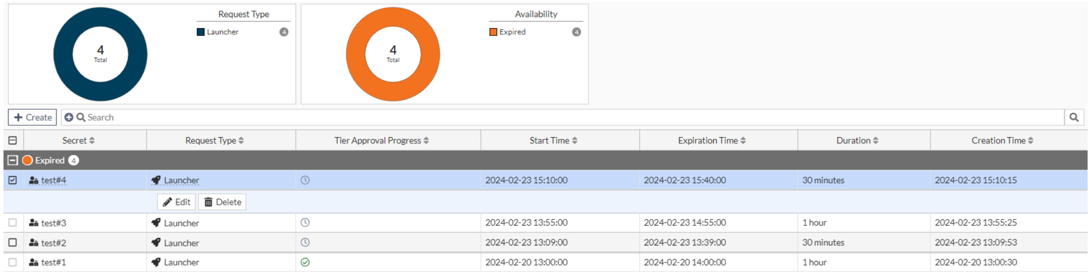
Go to *Secrets* > *My Request List* to see list of secret requests.

The widgets at the top display:

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

For every request the following fields are listed:

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



⊟	Secret	Request Type	Tier Approval Progress	Start Time	Expiration Time	Duration	Creation Time
⊟	Expired 4						
☑	test#4	Launcher	🕓	2024-02-23 15:10:00	2024-02-23 15:40:00	30 minutes	2024-02-23 15:10:15
☐	test#3	Launcher	🕓	2024-02-23 13:55:00	2024-02-23 14:55:00	1 hour	2024-02-23 13:55:25
☐	test#2	Launcher	🕓	2024-02-23 13:09:00	2024-02-23 13:39:00	30 minutes	2024-02-23 13:09:53
☐	test#1	Launcher	✓	2024-02-20 13:00:00	2024-02-20 14:00:00	1 hour	2024-02-20 13:00:30

All requests stay in the list until they are deleted.

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

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

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

Create	Select to create a new request. See Make a request on page 145.
Edit	Select to edit the selected request. When a secret request is approved, the *Launcher Status* timer shows the remaining time till you (as a requester) have access to the secret when you (as a requester) double-click to open the secret request in *Secrets* > *My Request List*.
Delete	Select to delete the selected requests.
Search	Enter a search term in the search field, then hit `Enter` to search the requests list. To narrow down your search, see Column filter.

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

Make a request

To make a request:

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

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

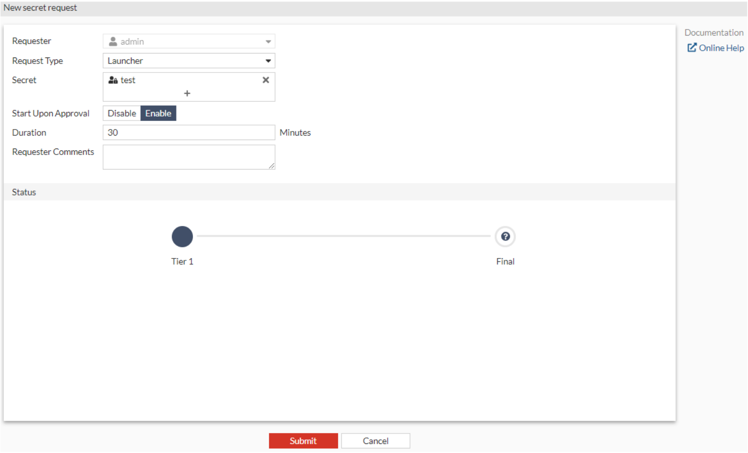
   You can also go to *Secrets* > *My Requests List*, select *Create*, and skip to step 4.

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

3. On the top-right, click the *Request* (▦) icon 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 72.

   The *New secret request* window opens.



New secret request

Requester: admin

Request Type: Launcher

Secret: test

Start Upon Approval: Disable **Enable**

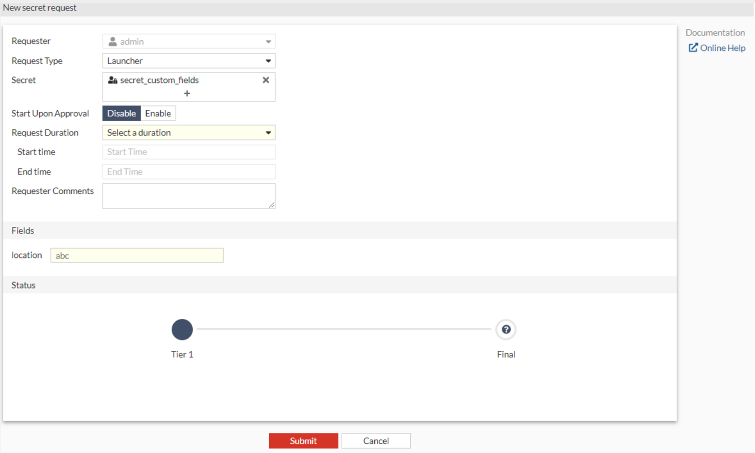
Duration: 30 Minutes

Requester Comments:

Status

4. Enter the following information:

Requester	The requester. **Note**: The option cannot be changed.
Request Type	Select from the following request types: • *Launcher* • *Job*
Secret	When the *Request Type* is *Launcher*, select + and select secrets from the *Select Entries* list. These are secrets with *Requires Approval to Launch Secret* enabled. See Creating a secret on page 72. If available, hover over the secret to see additional information including the folder where the secret is located and the secret template being used for the secret. When the *Request Type* is *Launcher*, use the search bar to look up a secret with *Requires Approval to Launch Secret* enabled.
Job	When the *Request Type* is *Job*, secret associated with the job is automatically selected. The option becomes non-editable. This is the secret with *Requires Approval to Launch Job* enabled. Not all jobs require approval. When editing a secret, the *Requires Approval to Launch Job* option in the *Secret Setting* pane determines which jobs require approval. Select + and select jobs from the *Select Entries* list. **Note**: The option is only available when the *Request Type* is *Job*.
Start Upon Approval	Enable/disable launching a secret once it is approved (default = disable).

	The approver can still override when you get access to the secret and the duration of time you have access to the secret.
Duration	Specify the duration of time you need the secret access for, in minutes (default = 30, minimum = 1). The option is only available when *Start Upon Approval* is enabled.
Request Duration	When the *Request Type* is *Launcher*, from the dropdown, select a duration of time or select *Custom* and then enter a date (MM/DD/YYYY) and time range. Alternatively, select the calendar icon and select a start/end date and time. When the *Request Type* is *Job*, the start time is the latest scheduled time among all selected jobs. Enter an end date (MM/DD/YYYY) and time. The local time of the requestor is displayed.
Request Comments	Optionally, enter comments for the request.
Fields	For a secret request to a secret where an approval profile with custom fields is used, the user must specify the required custom fields in the *Fields* pane.  New secret request Requester: admin Request Type: Launcher Secret: secret_custom_fields Start Upon Approval: Disable Enable Request Duration: Select a duration Start time: Start Time End time: End Time Requester Comments: Fields location: abc Status Documentation Online Help Tier 1 Final Submit Cancel
Status	Current status of the request.

5. Click *Submit*.
   Once the request is submitted, it appears in *My Request List* and *Approval List* tab. See My requests list on page 143 and Approval list on page 148.

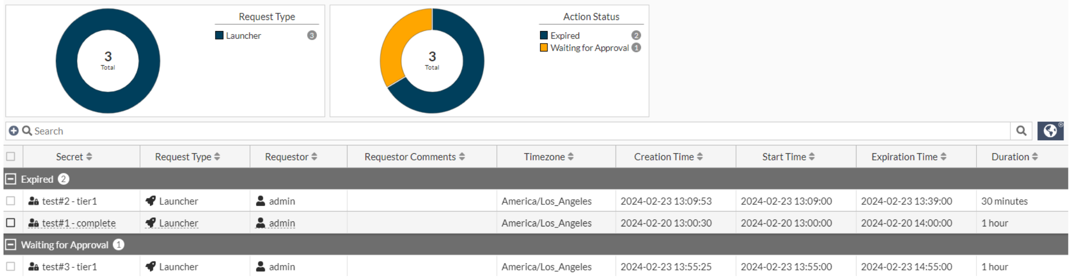
   Reviewers specified in Approval profile on page 199 are sent email notifications so that they can log in to FortiPAM from the email link. If the request is approved or denied, the status of the request changes to *Approved* or *Denied* respectively in *My Request List*.

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

Approval list

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

The *Approval List* tab looks like the following:



□	Secret	Request Type	Requestor	Requestor Comments	Timezone	Creation Time	Start Time	Expiration Time	Duration
Expired 2									
□	test#2 - tier1	Launcher	admin		America/Los_Angeles	2024-02-23 13:09:53	2024-02-23 13:09:00	2024-02-23 13:39:00	30 minutes
□	test#1 - complete	Launcher	admin		America/Los_Angeles	2024-02-20 13:00:30	2024-02-20 13:00:00	2024-02-20 14:00:00	1 hour
Waiting for Approval 1									
□	test#3 - tier1	Launcher	admin		America/Los_Angeles	2024-02-23 13:55:25	2024-02-23 13:55:00	2024-02-23 14:55:00	1 hour

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.

For each secret request, the following columns are displayed by default:

- *Secret*
- *Request Type*
- *Requestor*
- *Requestor Comments*
- *Timezone*
- *Creation Time*
- *Start Time*
- *Expiration Time*
- *Duration*

The *Approval List* tab contains the following options:

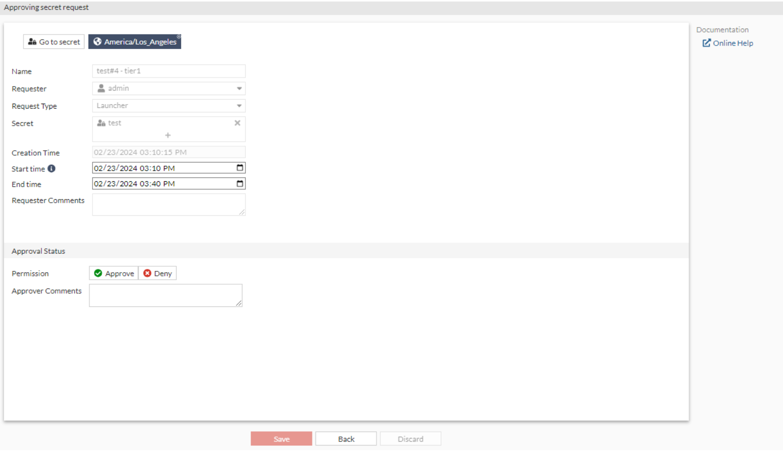
Search	Enter a search term in the search field, then hit `Enter` to search the reviews list. To narrow down your search, see Column filter.

Enable/Disable Requestor Timezone (🌐)	Click to enable/disable the secret access requestor's timezone.
Edit	Select a request and then select *Edit* to approve or deny the selected request. Alternatively, double-click a request to review the request. See Approving a request on page 149. When a secret request is approved, the *Launcher Status* timer shows the remaining time till the requester has access to the secret when you (as an approver) double-click to open the reviewed request in *Secrets* > *Approval List*.
Approve	Select to approve the selected requests. See Reviewing multiple requests on page 150.
Deny	Select to deny the selected requests. See Reviewing multiple requests on page 150.

Approving a request

To approve or deny a secret request:

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



Approving secret request

Go to secret | America/Los_Angeles

Name: test#4 - tier1
Requester: admin
Request Type: Launcher
Secret: test
Creation Time: 02/23/2024 03:10:15 PM
Start time: 02/23/2024 03:10 PM
End time: 02/23/2024 03:40 PM
Requester Comments:

Approval Status

Permission: Approve | Deny
Approver Comments:

By default, the approver's timezone is used.

Click the *Enable Requestor Timezone* option to enable the requestor's timezone and display the requestor's local time.

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

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

      Approver comments are visible to the requester.

3. Click *Save*.

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

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

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

Once a secret request is approved or denied, the request status appears in the *Approval List* tab and the status is updated in the My requests list on page 143 tab.

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

To see the reviewer comments:

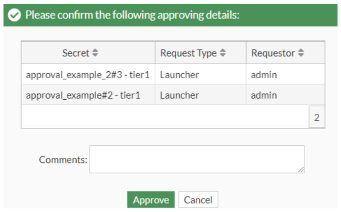
1. Go to *Secrets* > *My Request List*.
2. Double-click the denied request under *Denied/Expired*.
3. Select *View Approvers Comments* to see the reviewer comment.
   Alternatively, go to *Secrets* > *Approval List*, under *Denied/Expired Request*, double-click the request to see the reviewer comments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

Reviewing multiple requests

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

To review multiple requests:

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

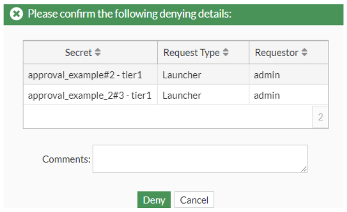


Please confirm the following approving details:

Secret	Request Type	Requestor
approval_example_2#3 - tier1	Launcher	admin
approval_example#2 - tier1	Launcher	admin

2

Comments:



Please confirm the following denying details:

Secret	Request Type	Requestor
approval_example#2 - tier1	Launcher	admin
approval_example_2#3 - tier1	Launcher	admin

2

Comments:

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

Approver comments are visible to the requester.

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

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

Once a secret request is approved or denied, the request status appears in the *Approval List* tab and the status is updated in the My requests list on page 143 tab.

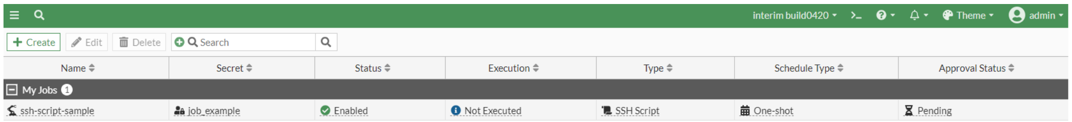
Job list

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

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

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

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



Name	Secret	Status	Execution	Type	Schedule Type	Approval Status
My Jobs 1						
ssh-script-sample	job_example	Enabled	Not Executed	SSH Script	One-shot	Pending

Jobs are not executed when FortiPAM is in maintenance mode.

The *Job List* tab contains the following options:

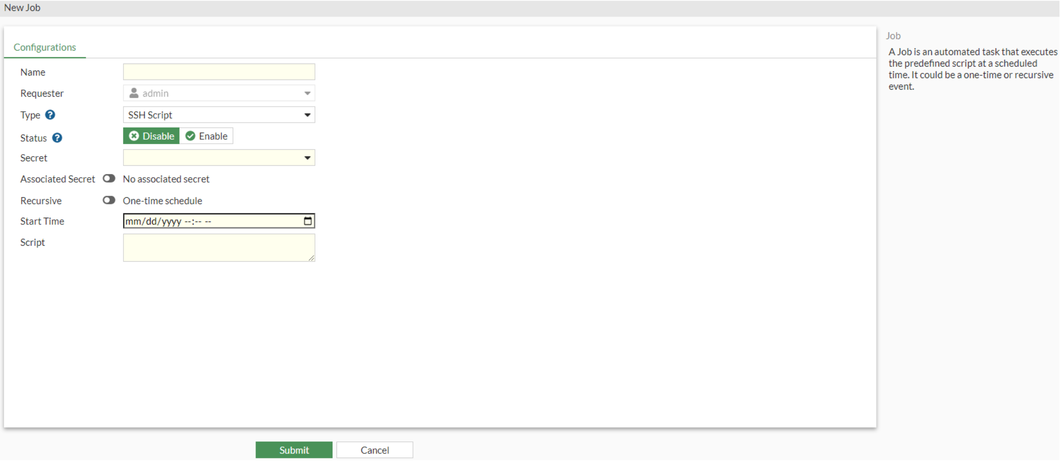
+Create	Select to create a job. See Creating a job on page 152.
Edit	Select to edit the selected job.
Delete	Select to delete the selected jobs.
Search	Enter a search term in the search field, then hit `Enter` to search the jobs list. To narrow down your search, see Column filter.

Creating a job

To create a job:

1. Go to *Secrets* > *Job List*.
2. Select +*Create*.

   The *New Job* window opens.



Name:
Requester: admin
Type: SSH Script
Status: Disable | Enable
Secret:
Associated Secret: No associated secret
Recursive: One-time schedule
Start Time: mm/dd/yyyy --:-- --
Script:

Job

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

3. Enter the following information:

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

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

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

4. Click *Submit*.

When editing a job, select the *Make Request* option from the top to make a request to perform a job on the secret associated with the job. See Make a request on page 145.

When editing a job, select the *Log* tabs to see logs related to the job. See Log & report on page 312.

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

Discovery

Discovery in *Secrets* displays a list of configured discovery entries.

Discovery is the process where FortiPAM scans an environment to find accounts and other associated resources. Once the accounts and the resources are found, they can be automatically imported to FortiPAM for centralized management.

Discovery helps provide a better overview of the existing accounts in an Active Directory. The automatic import feature saves time.

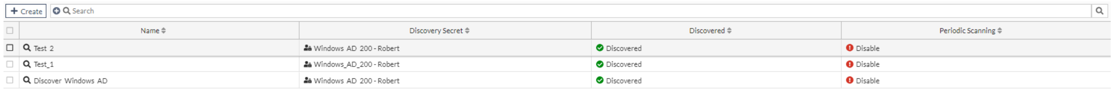
Users with the *Secret Discovery* permission for their role are able to see the *Discovery* tab in *Secrets*.

See Role on page 278.

Do not use the CLI console to configure discovery.

The following columns are available in the *Discovery* tab:

- *Name*
- *Discovery Secret*
- *Discovered*
- *Periodic Scanning*



□	Name	Discovery Secret	Discovered	Periodic Scanning
□	Test 2	Windows AD 200 - Robert	✓ Discovered	! Disable
□	Test_1	Windows_AD_200 - Robert	✓ Discovered	! Disable
□	Discover Windows AD	Windows AD 200 - Robert	✓ Discovered	! Disable

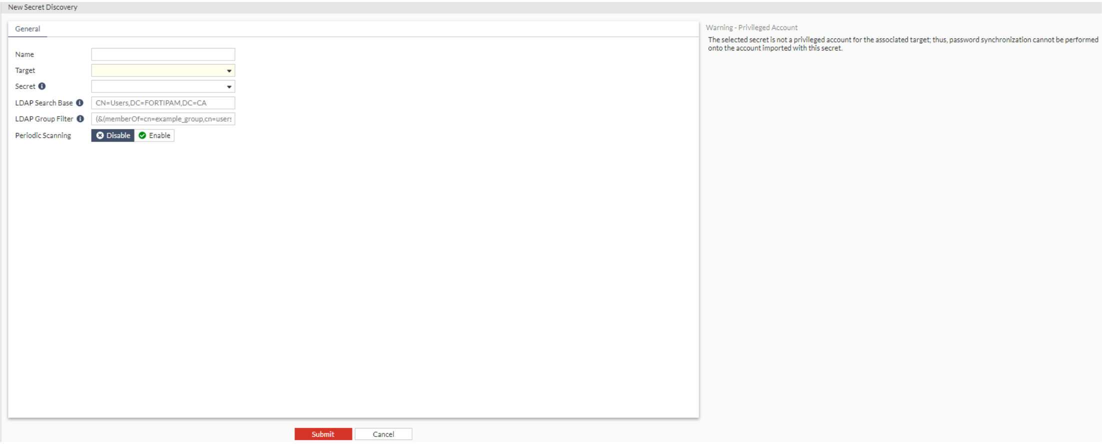
The *Discovery* tab contains the following options:

Create	Select to create a new discovery entry. See Creating discovery entry on page 155.
Search	Enter a search term in the search field, then hit `Enter` to search the discovery list. To narrow down your search, see Column filter.
Edit	Select to edit the selected discovery entry.
Delete	Select to delete the selected discovery entries.
Clear Selection	Select to clear the currently selected discovery entries from selection.

Creating discovery entry

To create a discovery entry:

1. Go to *Secrets* > *Discovery*.
2. In the *Discovery* tab, select *Create*.
   The *New Secret Discovery* tab opens.



Name	
Target	
Secret	
LDAP Search Base	CN=Users,DC=FORTIPAM,DC=CA
LDAP Group Filter	(&(memberOf=cn=example_group,cn=users
Periodic Scanning	● Disable ○ Enable

Warning - Privileged Account

The selected secret is not a privileged account for the associated target; thus, password synchronization cannot be performed onto the account imported with this secret.

3. Enter the following information:

Name	The name of the discovery entry.
Target	From the dropdown, select a target, e.g., a secret target for the Domain Controller. **To create a new target:** 1. From the dropdown, select +. The *New Secret Target* window opens. 2. Follow the steps in Creating a target on page 114, starting step 4.

	From the search bar look up a target. Use the pen icon next to the target to edit it.
Secret	From the dropdown, select a secret that is using the selected target to perform discovery. The account of the selected secret is used to perform discovery on the selected target. This is generally a privileged account. **To create a new secret:** **1.** From the dropdown, select +. The *New Secret* window opens. **2.** Follow the steps in Creating a secret on page 72, starting step 6. From the search bar look up a secret. Use the pen icon next to the secret to edit it.
LDAP Search Base	Enter the LDAP search base. Search base denotes the location in the directory where the search for a particular directory object begins, e.g., `CN = Users,DC=FORTINET,DC=COM`.
LDAP Group Filter	Enter the LDAP group filter. Standard LDAP filters to the LDAP search. Only the accounts that match the specified group filters are discovered, e.g., `(&(memberOf=cn=HR_GRP,cn=users,dc=fortinet,dc=com)(memberOf=cn=DEV_GRP,cn=users,dc=fortinet,dc=com))`.

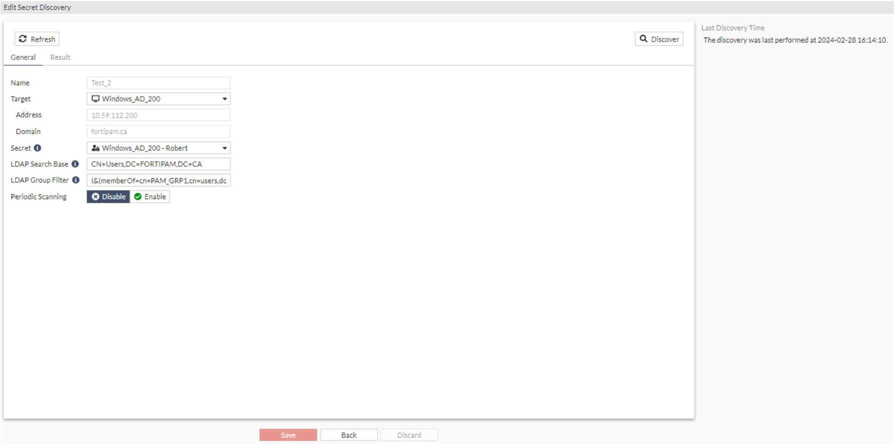
	LDAP Group Filter is an optional configuration. Leave the field empty if you do not want to apply LDAP filters to the search.
Periodic Scanning	Enable/disable periodic scanning (default = disable). If you disable the setting, you can later manually click *Discover* in the *Edit Secret Discovery* page to trigger discovery.

4. Click *Submit*.

Manual discovery

To perform manual discovery:

1. Go to *Secrets* > *Discovery*.
2. In the *Discovery* tab, select a discovery entry and then select *Edit*.
   The *Edit Secret Discovery* window opens.



Edit Secret Discovery

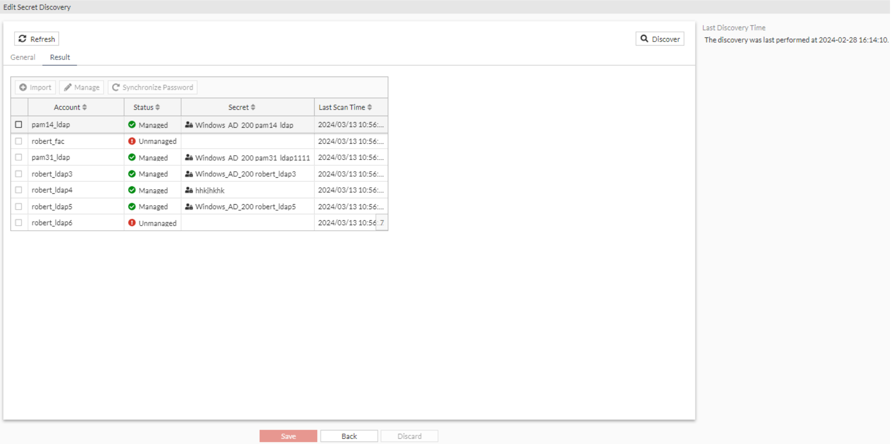
Name	Test_2
Target	Windows_AD_200
Address	10.59.112.200
Domain	fortipam.ca
Secret	Windows_AD_200 - Robert
LDAP Search Base	CN=Users,DC=FORTIPAM,DC=CA
LDAP Group Filter	(&(memberOf=cn=PAM_GRP1,cn=users,dc
Periodic Scanning	● Disable ○ Enable

Last Discovery Time

The discovery was last performed at 2024-02-28 16:14:10.

3. Form the right, click *Discover* to trigger a one-time discovery.

4. In the *Results* tab, you can see the discovered accounts.



Last Discovery Time
The discovery was last performed at 2024-02-28 16:14:10.

	Account	Status	Secret	Last Scan Time
□	pam14_ldap	Managed	Windows_AD_200 pam14_ldap	2024/03/13 10:56:...
□	robert_fac	Unmanaged		2024/03/13 10:56:...
□	pam31_ldap	Managed	Windows_AD_200 pam31_ldap1111	2024/03/13 10:56:...
□	robert_ldap3	Managed	Windows_AD_200 robert_ldap3	2024/03/13 10:56:...
□	robert_ldap4	Managed	hhkjhkhk	2024/03/13 10:56:...
□	robert_ldap5	Managed	Windows_AD_200 robert_ldap5	2024/03/13 10:56:...
□	robert_ldap6	Unmanaged		2024/03/13 10:56

5. Select the unmanaged account and select *Import* to import the selected account as a secret to FortiPAM.

The *Status* of an account indicates if it is managed by FortiPAM:

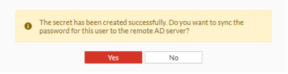
- *Managed*: Account is managed by FortiPAM.
- *Unmanaged*: Account is not managed by FortiPAM.

If an account is already managed by FortiPAM, you can see the corresponding secret in the *Secret* column.

Double-click a managed account to open the *Manage Account* window. Here, you can edit the secret.

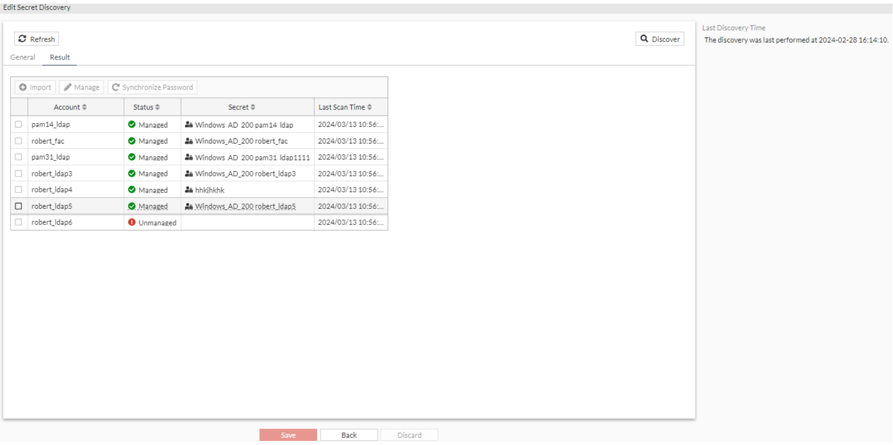
FortiPAM detects if it manages an account by looking for all the secrets that are currently using the discovery target.

6. In the *Import Account* window:
   a. Enter the password of the AD account.
      If you know the password, enter the password in the *Password* field.
      Alternatively, click + to automatically generate a random password.
   b. In *Confirm Password*, enter the password again to confirm the password.
      Alternatively, click *Copy to clipboard* option and then paste the password.
7. Click *Submit*.
   A dialog appears confirming the creation of the secret.



The secret has been created successfully. Do you want to sync the password for this user to the remote AD server?

8. Click *Yes* if you want to sync the password of the account to the remote AD server.
   The account is imported as a secret and the *Results* tab is updated.



Last Discovery Time

The discovery was last performed at 2024-02-28 16:14:10.

	Account	Status	Secret	Last Scan Time
□	pam14_ldap	✓ Managed	Windows AD 200 pam14 ldap	2024/03/13 10:56:...
□	robert_fac	✓ Managed	Windows_AD_200 robert_fac	2024/03/13 10:56:...
□	pam31_ldap	✓ Managed	Windows AD 200 pam31 ldap1111	2024/03/13 10:56:...
□	robert_ldap3	✓ Managed	Windows_AD_200 robert_ldap3	2024/03/13 10:56:...
□	robert_ldap4	✓ Managed	hhkjhkhk	2024/03/13 10:56:...
□	robert_ldap5	✓ Managed	Windows_AD_200 robert_ldap5	2024/03/13 10:56:...
□	robert_ldap6	! Unmanaged		2024/03/13 10:56:...

Secret settings

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

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

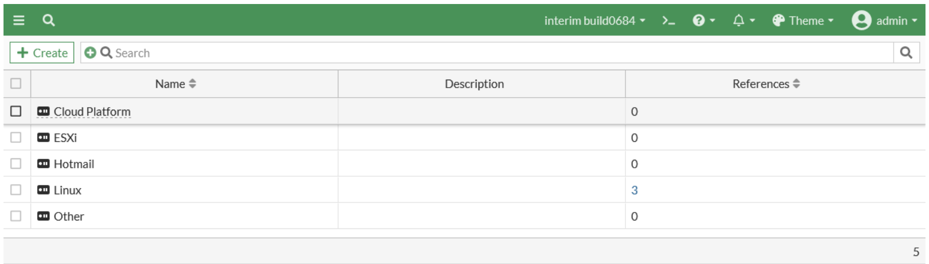
- Classification tags on page 160
- Templates on page 161
- Launchers on page 174
- Policies on page 184
- Addresses on page 191
- Dependency updater on page 194
- Approval profile on page 199
- Approval email template on page 203
- Password changers on page 208
- Password policies on page 217
- Character sets on page 220
- AntiVirus on page 221
- Data loss prevention (DLP) protection for secrets on page 225
- DLP file pattern on page 232
- SSH filter profiles on page 234
- Window app filter on page 242
- Event filter profile on page 240
- Integrity check on page 247

Classification tags

Go to *Secret Settings* > *Classification Tag* to configure classification tags.

A classification tag can be used to classify targets. To add a classification tag to a target, see Creating a target on page 114.

For each classification tag; name, description, and number of references are displayed. Click the number of references to display where the classification tag is used. You can *Edit* or *Delete* these objects if you have permissions to do so.



	Name	Description	References
□	Cloud Platform		0
□	ESXi		0
□	Hotmail		0
□	Linux		3
□	Other		0

5

The *Classification Tag* tab contains the following options:

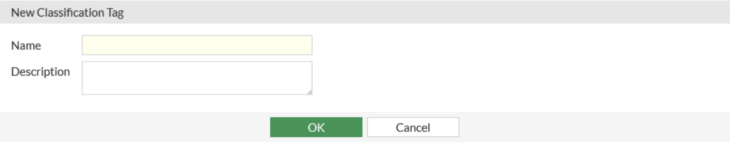
+Create	Select to create a classification tag. See Creating a classification tag on page 161.
Edit	Select to edit the selected classification tag.
Delete	Select to delete the selected classification tags.
Search	Enter a search term in the search field, then hit `Enter` to search the jobs list. To narrow down your search, see Column filter.

Creating a classification tag

To create a classification tag:

1. Go to *Secret Settings* > *Classification Tag*.
2. Select +*Create*.

   The *New Classification Tag* window opens.



3. Enter the following information:

Name	Name of the classification tag.
Description	A description for the classification tag.

4. Click *OK*.

Templates

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

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

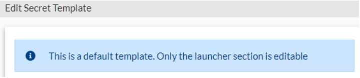
Secret templates allow configuring the fields a secret requires, as well as the types of launchers that are allowed for the secrets. A password changer can also be configured to automatically change a secret's passwords. See Password changers on page 208.

FortiPAM provides the following default templates:

Cisco User (SSH Secret)	A basic template for a Cisco SSH account.
Certificate Vault	A basic template designed to save certificate and its key.
FortiProduct (Web)	A basic template for web based products, e.g., FortiGate and FortiProxy.
MySQL	A basic template for a MySQL database server account.
Machine	A basic template for a general machine, with all default launchers.

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

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



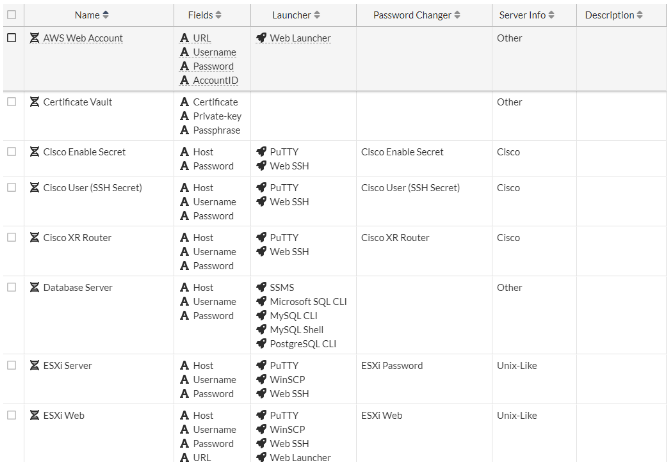
Edit Secret Template

This is a default template. Only the launcher section is editable

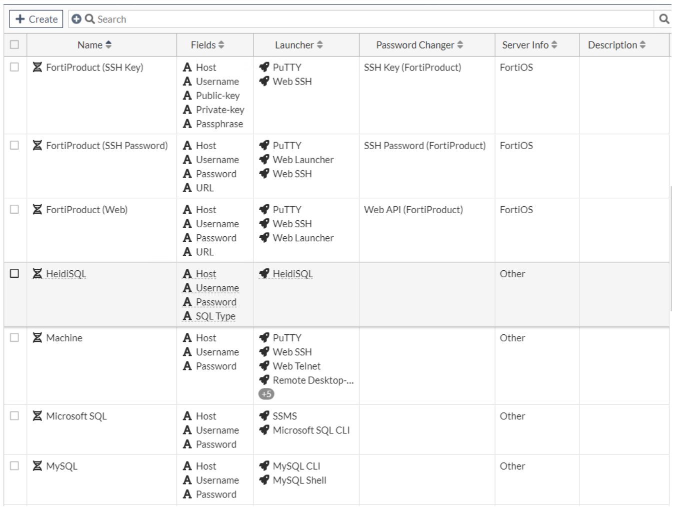
The following default templates have *Server Information* set to *Unix-Like*:

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

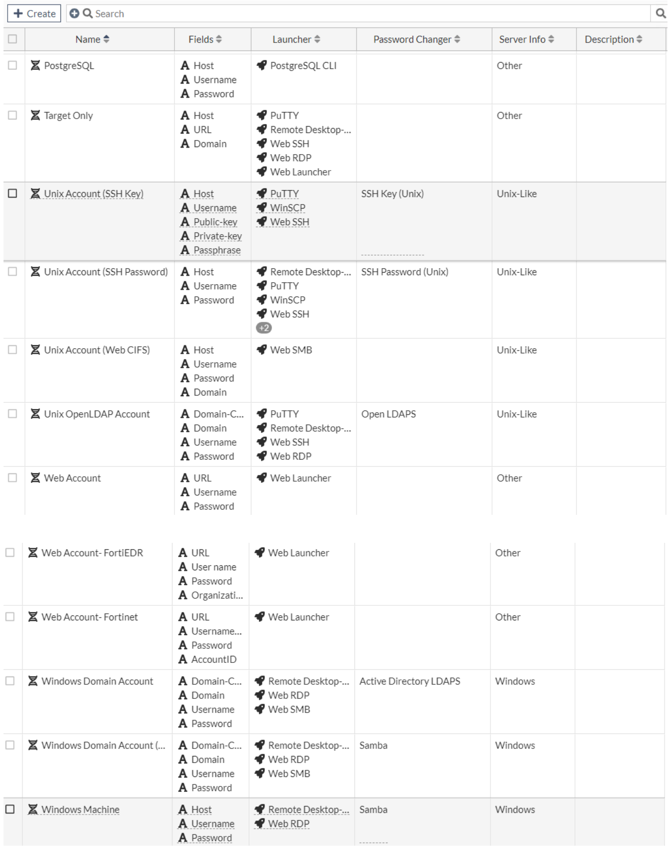
For each template; name, fields, launcher, password changer, server info, and description are displayed.



□	Name	Fields	Launcher	Password Changer	Server Info	Description
□	AWS Web Account	URL Username Password AccountID	Web Launcher		Other	
□	Certificate Vault	Certificate Private-key Passphrase			Other	
□	Cisco Enable Secret	Host Password	PuTTY Web SSH	Cisco Enable Secret	Cisco	
□	Cisco User (SSH Secret)	Host Username Password	PuTTY Web SSH	Cisco User (SSH Secret)	Cisco	
□	Cisco XR Router	Host Username Password	PuTTY Web SSH	Cisco XR Router	Cisco	
□	Database Server	Host Username Password	SSMS Microsoft SQL CLI MySQL CLI MySQL Shell PostgreSQL CLI		Other	
□	ESXi Server	Host Username Password	PuTTY WinSCP Web SSH	ESXi Password	Unix-Like	
□	ESXi Web	Host Username Password URL	PuTTY WinSCP Web SSH Web Launcher	ESXi Web	Unix-Like	



□	Name	Fields	Launcher	Password Changer	Server Info	Description
□	FortiProduct (SSH Key)	Host Username Public-key Private-key Passphrase	PuTTY Web SSH	SSH Key (FortiProduct)	FortiOS	
□	FortiProduct (SSH Password)	Host Username Password URL	PuTTY Web Launcher Web SSH	SSH Password (FortiProduct)	FortiOS	
□	FortiProduct (Web)	Host Username Password URL	PuTTY Web SSH Web Launcher	Web API (FortiProduct)	FortiOS	
□	HeidiSQL	Host Username Password SQL Type	HeidiSQL		Other	
□	Machine	Host Username Password	PuTTY Web SSH Web Telnet Remote Desktop-... +5		Other	
□	Microsoft SQL	Host Username Password	SSMS Microsoft SQL CLI		Other	
□	MySQL	Host Username Password	MySQL CLI MySQL Shell		Other	



+ Create | Search

□	Name	Fields	Launcher	Password Changer	Server Info	Description
□	PostgreSQL	Host Username Password	PostgreSQL CLI		Other	
□	Target Only	Host URL Domain	PuTTY Remote Desktop-... Web SSH Web RDP Web Launcher		Other	
□	Unix Account (SSH Key)	Host Username Public-key Private-key Passphrase	PuTTY WinSCP Web SSH	SSH Key (Unix)	Unix-Like	
□	Unix Account (SSH Password)	Host Username Password	Remote Desktop-... PuTTY WinSCP Web SSH +2	SSH Password (Unix)	Unix-Like	
□	Unix Account (Web CIFS)	Host Username Password Domain	Web SMB		Unix-Like	
□	Unix OpenLDAP Account	Domain-C... Domain Username Password	PuTTY Remote Desktop-... Web SSH Web RDP	Open LDAPS	Unix-Like	
□	Web Account	URL Username Password	Web Launcher		Other	
□	Web Account- FortiEDR	URL User name Password Organizati...	Web Launcher		Other	
□	Web Account- Fortinet	URL Username... Password AccountID	Web Launcher		Other	
□	Windows Domain Account	Domain-C... Domain Username Password	Remote Desktop-... Web RDP Web SMB	Active Directory LDAPS	Windows	
□	Windows Domain Account (...	Domain-C... Domain Username Password	Remote Desktop-... Web RDP Web SMB	Samba	Windows	
□	Windows Machine	Host Username Password	Remote Desktop-... Web RDP	Samba	Windows	

The secret templates list contains the following options:

Create	Select to create a new template. See Creating secret templates on page 165.
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.

For *Windows Domain Account*, *Windows Machine*, and *Windows Domain Account (Samba)* secret templates, it is recommended that you manually change the *Server Info* to *Windows* in the CLI console.

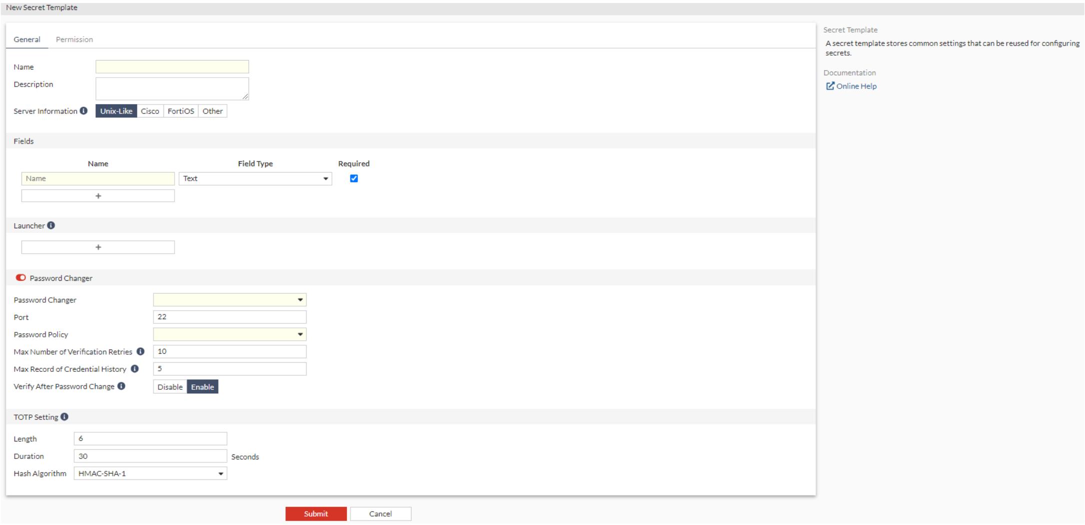
- Example

```
config secret template
 edit Windows Domain Account
  set server-info Windows
end
```

Creating secret templates

To create a secret template:

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



New Secret Template

General | Permission

Name:

Description:

Server Information: [Unix-Like] Cisco FortiOS Other

Fields

Name	Field Type	Required
Name	Text	☑
+		

Launcher

+

Password Changer

Password Changer:

Port: 22

Password Policy:

Max Number of Verification Retries: 10

Max Record of Credential History: 5

Verify After Password Change: Disable [Enable]

TOTP Setting

Length: 6

Duration: 30 Seconds

Hash Algorithm: HMAC-SHA-1

Submit Cancel

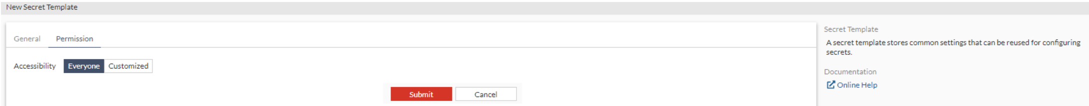
Secret Template

A secret template stores common settings that can be reused for configuring secrets.

Documentation

Online Help

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



New Secret Template

General | Permission

Accessibility: [Everyone] Customized

Submit Cancel

Secret Template

A secret template stores common settings that can be reused for configuring secrets.

Documentation

Online Help

4. Enter the following information:

General	
Name	Name of the template.
Description	Optionally, enter a description.
Server Information	The general type of server to which the template is intended to connect: - *Unix-Like* - *Cisco* - *FortiOS* - *Other*
Fields	Secrets require fields to enter the secret related information. To add new fields, select + and enter the following information: **Name** — The name of the field. **Field Type** — From the dropdown, select a field type: - *Target-Address:* A target address field. - *Domain:* A domain field.

<table>
<tr>
<td></td>
<td>
<table>
<tr>
<td></td>
<td>

- *URL:* A URL field.
- *Username:* A username field.
- *Password:* A password field.
- *Public-Key:* A public-key field.
- *Private-Key:* A private-key field.
- *Passphrase:* A passphrase fields.
- *Text:* A text field.

</td>
</tr>
<tr>
<td><b>Required</b></td>
<td>Enable to make this field required or disable if this field will be optional.
<b>Note</b>: By default, all fields are marked as required.</td>
</tr>
</table>

From the list, click *x* next to a field entry to delete it.
</td>
</tr>
<tr>
<td><b>Launcher</b></td>
<td>
Launcher helps you access a target server. See Launchers on page 174.

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 + and enter the following information:

You can add up to a maximum of 20 launchers.

When you select *Web Launcher* as the secret launcher, a new *Web Filler* tab allows you to configure advanced web filler settings, so that extension can locate the correct web elements to patch credential information into.
See Auto web filler on page 172.

<table>
<tr>
<td><b>Launcher</b></td>
<td>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 +.
Enter the following information and click *Submit*:</td>
</tr>
</table>
</td>
</tr>
</table>

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

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

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

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

	Client Software	Enable to select a client software entry from the dropdown. See Integrity check on page 247. Use the search bar to look up a client software entry. **Note**: The option is disabled by default.
	Initial Commands	Configure initializing the environment. See Creating a new launcher command.
	Clean Commands	Configure cleaning the environment. See Creating a new launcher command.
Launcher Port	The launcher port number. The port number will be mapped to the launcher variable `` `$PORT` ``. The minimum allowed value is `1`.	
Integrity Check	Enable/disable integrity check. For information on integrity check, see Integrity check on page 247.	

	The *Integrity Check* option can only be edited if you choose a launcher in the *Launcher Name* option with a client software entry enabled and selected. **Note**: The option is disabled by default. From the list, click *x* next to a launcher to delete it.
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 210. 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 218. Use the search for to look up a password policy. Use the pen icon next to a password policy to edit it.
Max Number of Verification Retries	The maximum number of retries allowed after which the connection fails (default = 10).

Max Record of Credential History	The maximum number of credential history to be kept in the database (default = 5).
Verify After Password Change	When enabled, whenever secrets with the template conducts a password change, a verification of the newly changed password is ran. **Note**: The option is enabled by default.
TOTP Setting TOTP (Time-based one-time password) settings. The TOTP configuration from a secret template can be inherited by all the secrets using this template. When configuring the secret, you can override the secret template TOTP configuration. See *TOTP Setting* in Creating a secret on page 72. See Limitations of TOTP on FortiPAM on page 171.	
Length	The length of the TOTP (default = 6, 4 - 9).
Duration	The duration for which the TOTP is valid, in seconds (default = 30, 30 - 90).
Hash Algorithm	Select from the following hash algorithms for TOTP: • *HMAC-SHA-1* (default) • *HMAC-SHA-256* • *HMAC-SHA-512*
Permission Template access control settings.	
Accessibility	Template accessible to: • *Everyone*: All users have *Read/Write* permission for templates (default). • *Customized*: A user permission and a group permission table must be configured.
Create Secret	From the list, select user/user groups with the ability to see and use the template to create secrets. The option is only available when *Accessibility* is set to *Customized*.
Owner	From the list, select user/user groups with the highest possible permission level and with the ability to create, edit, and delete templates. Every template must have at least one owner. The option is only available when *Accessibility* is set to *Customized*.

5. Click *Submit*.

User Permission

1. In Step 3, when Creating secret templates on page 165, select *Customized* in *Accessibility*.
2. In the *Create Secret* dropdown, select users with the ability to see and use the template to create secrets.
3. In the *Owner* dropdown, select users with the highest possible permission level and with the ability to create, edit, and delete templates.
4. Click *Submit*.

From the list, click *x* next to an entry to delete it.

Group Permission

1. In Step 3, when Creating secret templates on page 165, select *Customized* in *Accessibility*.
2. In the *Create Secret* dropdown, select user groups with the ability to see and use the template to create secrets.
3. In the *Owner* dropdown, select user groups with the highest possible permission level and with the ability to create, edit, and delete templates.
4. Click *Submit*.

From the list, click *x* next to an entry to delete it.

Configuring TOTP settings via the secret template CLI commands - Example

To configure TOTP settings via the CLI:

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

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

Limitations of TOTP on FortiPAM

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

Auto web filler

When you launch a secret with web launcher, the extension automatically inputs user name and password to log in to the target website.

However, the web launching feature has the following three limitations:

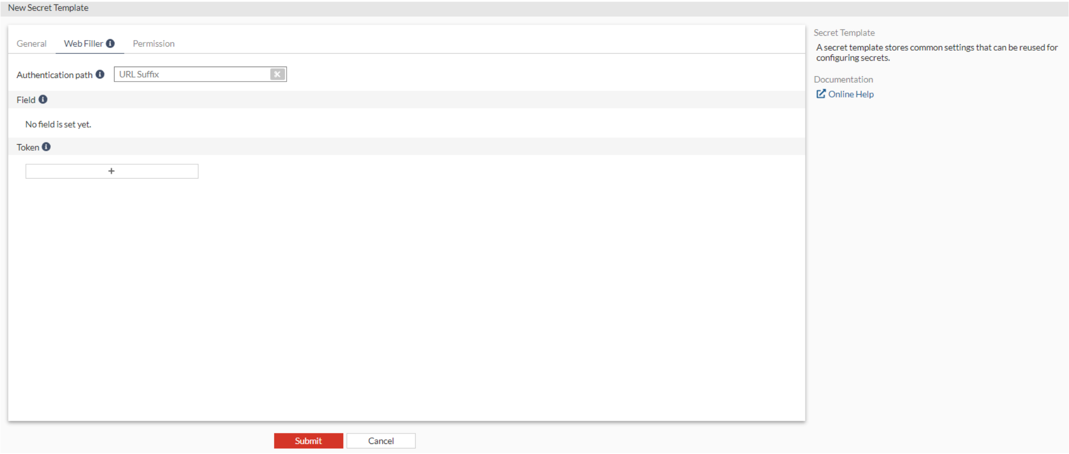
- When launching to some special website, the extension cannot find the user name or the password field correctly using its predefined key.
- After logging in to a website, the extension tries to fill user name or password into an unrelated field.
- The extension can only fill in user name, password, but 2FA Token is not supported.

Using auto web filler, these issues with web launching have been fixed.

The feature needs Microsoft Edge and Google Chrome extension V3.

To configure auto web filler for the web launcher:

1. When configuring a secret template as shown in Creating a secret template, select *Web Launche*r as the *Launcher*. A new *Web Filler* tab is available.
2. Go to the *Web Filler* tab.



New Secret Template

Authentication path: URL Suffix

Field

No field is set yet.

Token

Secret Template

A secret template stores common settings that can be reused for configuring secrets.

Documentation

3. Enter the following information:

Authentication path	The authentication path URL suffix. This is the login page of a website. The extension checks the URL that it visits against the authentication path and applies the configured setting if it is a match, The authentication path can only be part of the desired URL. For example, `/#login` can be added instead of `https://fortipam.ca/#login` to allow matching on various sites.
Field	The field from the secret to be patched to the element located by the selector. The field can be user name/ password. It refers to the user name/password value in a secret configuration. • *Web Element Selector*: Represents the selector for the element in HTML. This can be located with the inspect mode. The field defines how to locate the user name/password fields on the login page. • *Override Path*: Represents if the path should be searched for the selector instead of the authentication path. By default, this is empty. This means the user name/password fields are located in the page added in *Authentication path*. If the page to enter user name/password is different than the one mentioned in *Authentication path*, fill in with user name/password page path. • *Mask*: Represents if there is a mask for the value to be filled in. If enabled, enter the value in the mask format. Also, more secret fields can be sent to the extension and auto filled during the login process as long as the token is used for 2FA.
Token	The token from the secret is patched to the element located by the selector. • *Attribute*: The token value. • *Web Element Selector*: Represents the selector for the element in HTML. This can be located with the inspect mode. The field defines the page path to locate the token. • *Override Path*: Represents if the path should be searched for the selector instead of the authentication path. By default, this is empty. This means the token field is located in the page added in *Authentication path*. If the page to enter the token is different than the one mentioned in *Authentication path*, fill in with token page path. • *Mask*: Represents if there is a mask for the value to be filled in. If enabled, enter the value in the mask format.

4. The *General* and *Permission* tabs can be configured as shown in Creating a secret template.

Launchers

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

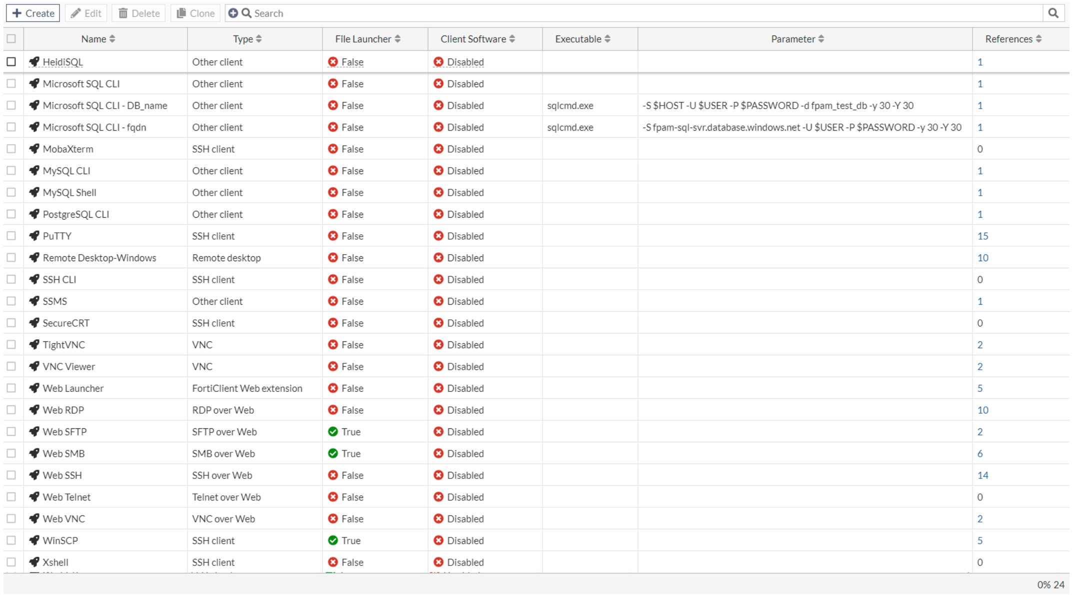
A secret launcher stores an executable and the parameters needed to start a connection to a target.

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

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

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

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



□	Name	Type	File Launcher	Client Software	Executable	Parameter	References
□	HeidiSQL	Other client	☒ False	☒ Disabled			1
□	Microsoft SQL CLI	Other client	☒ False	☒ Disabled			1
□	Microsoft SQL CLI - DB_name	Other client	☒ False	☒ Disabled	sqlcmd.exe	-S $HOST -U $USER -P $PASSWORD -d fpam_test_db -y 30 -Y 30	1
□	Microsoft SQL CLI - fqdn	Other client	☒ False	☒ Disabled	sqlcmd.exe	-S fpam-sql-svr.database.windows.net -U $USER -P $PASSWORD -y 30 -Y 30	1
□	MobaXterm	SSH client	☒ False	☒ Disabled			0
□	MySQL CLI	Other client	☒ False	☒ Disabled			1
□	MySQL Shell	Other client	☒ False	☒ Disabled			1
□	PostgreSQL CLI	Other client	☒ False	☒ Disabled			1
□	PuTTY	SSH client	☒ False	☒ Disabled			15
□	Remote Desktop-Windows	Remote desktop	☒ False	☒ Disabled			10
□	SSH CLI	SSH client	☒ False	☒ Disabled			0
□	SSMS	Other client	☒ False	☒ Disabled			1
□	SecureCRT	SSH client	☒ False	☒ Disabled			0
□	TightVNC	VNC	☒ False	☒ Disabled			2
□	VNC Viewer	VNC	☒ False	☒ Disabled			2
□	Web Launcher	FortiClient Web extension	☒ False	☒ Disabled			5
□	Web RDP	RDP over Web	☒ False	☒ Disabled			10
□	Web SFTP	SFTP over Web	✓ True	☒ Disabled			2
□	Web SMB	SMB over Web	✓ True	☒ Disabled			6
□	Web SSH	SSH over Web	☒ False	☒ Disabled			14
□	Web Telnet	Telnet over Web	☒ False	☒ Disabled			0
□	Web VNC	VNC over Web	☒ False	☒ Disabled			2
□	WinSCP	SSH client	✓ True	☒ Disabled			5
□	Xshell	SSH client	☒ False	☒ Disabled			0

0% 24

The following default launchers are available in FortiPAM:

- *HeidiSQL*: An SQL GUI launcher that supports `mssql`, `psql`, and `mysql`.
- *Microsoft SQL CLI*: A MSSQL CLI launcher for `sqlcmd.exe`.
- *MobaXterm*: An SSH client using MobaXterm.
- *MySQL CLI*: A MYSQL CLI launcher for `mysql.exe`.
- *MySQL Shell*: A MYSQL CLI launcher for `mysqlsh.exe`.
- *PostgreSQL CLI*: A PostgreSQL CLI launcher for `psql.exe`.

To use `psql.exe`:

- You must add the application path to the PATH environment variable in the system, e.g., `C:\Program Files\PostgreSQL\<version>\bin`.
- Restart FortiClient.

PostgreSQL CLI default launcher is connected to postgres by default.

To switch the database:

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

- *PuTTY*: A basic SSH client using PuTTY.
- *Remote Desktop- Windows*: A basic RDP client using remote desktop.
- *SSH CLI*: An SSH CLI launcher for `ssh.exe`.
- *SSMS*: An MSSQL GUI launcher.

You must open SSMS locally at least once (it does not require connecting to the database) to set up the initial software cache; otherwise, the SSMS launcher fails.

- *SecureCRT*: An SSH client using SecureCRT.
- *TightVNC*: A basic VNC client using TightVNC.

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

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

For secrets created for a target with *Web Proxy* enabled:

- *Web Launcher* is available to users with *View*, *Edit*, or *Owner* permission for the secret.

For secrets not created for a target or for secrets created for a target with *Web Proxy* disabled:

- *Web Launcher* is unavailable to users with *View* permission for the secret, as the password can be retrieved using browser dev tools.
- *Web Launcher* is only available to users with *Edit* or *Owner* permission for the secret.

For information on setting up folder and secret permissions, see Creating a folder on page 139 and Creating a secret on page 72.

- *Web RDP*: A basic browser based RDP launcher.

  Copy from Local to Remote or vice versa:

  a. Select the text and hit `Ctrl + c`.

  b. To paste, on the Local or the Remote system, hit `Ctrl + v`.

You can use copy/paste keyboard shortcuts (`Ctrl + c`/ `Ctrl + v`) without the need to first press `F8`.

The `Ctrl + c`/ `Ctrl + v` shortcut and right-click to copy/paste functionality are not yet supported on the Mozilla Firefox web browser.

Right-click to copy/paste is not yet supported on Google Chrome and Microsoft Edge web browsers.

The feature needs Microsoft Edge and Google Chrome extension V3.

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

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

- *Web Telnet*: A basic browser based Telnet web launcher.
- *Web VNC*: A basic browser based VNC web launcher.
- *WinSCP*: A basic WinSCP client using SSH.
- *Xshell*: An SSH client using Xshell.
- *FortiClient Web extension FortiClient Web Launcher*
- *RDP over Web RDP over Web Launcher*
- *SSH over Web SSH over Web Launcher*
- *VNC over Web VNC over Web Launcher*
- *SMB over Web SMB over Web Launcher*
- *SFTP over Web SFTP over Web Launcher*

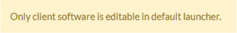
The following launchers should not be used for customized launcher:

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

These launchers will be removed in a future FortiPAM version.

Chrome, Edge, and Firefox are the supported browsers.

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



Only client software is editable in default launcher.

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

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

- PuTTY
- WinSCP
- RDP

- VNC Viewer
- TightVNC

The *Launchers* tab contains the following options:

Create	Select to create a new launcher.Creating a launcher on page 178Creating a launcher on page 178.
Edit	Select to edit the selected launcher.
Delete	Select to delete the selected launchers.
Clone	Select to clone the selected launcher.
Search	Enter a search term in the search field, then hit `Enter` to search the launchers list. To narrow down your search, see Column filter.

Preconfiguration for MobaXterm, Xshell, and SecureCRT

Before you use FortiPAM to launch secrets in MobaXterm, Xshell, or SecureCRT, ensure that these applications are correctly installed and configured on your local endpoint (user machine).

Execute each application independently to confirm that it operates correctly. Pay close attention to any initial setup or configuration prompts that may appear during the first launch. It is essential to have all the necessary configurations in place for the applications to run smoothly.

This preconfiguration step is essential to avoid issues or disruptions when using these secrets within FortiPAM. If you encounter problems during the initial manual launch, please resolve them before integrating FortiPAM with these applications.

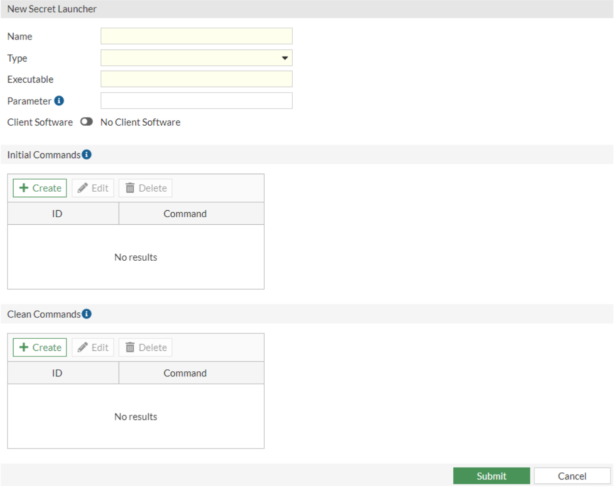
Once you have verified that these applications work correctly on your endpoint, you can seamlessly integrate them with FortiPAM for enhanced access control and security.

Creating a launcher

To create a launcher:

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

3. The *New Secret Launcher* window opens.



4. Enter the following information:

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

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

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

- `$VNCPASSWORD`

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

- `$PASSPHRASE`

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

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

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

- `$TMPFILE`

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

User input variables are:

- `$TARGET`

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

- Example

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

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

or

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

Note:

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

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

	When there is space in the path, double quotes must be used with backslash: `-l $USER -pw $PASSWORD $HOST -m "C:\Program Files\cmd.txt"`
Client Software	Enable to select a client software entry from the dropdown. See Integrity check on page 247. Use the search bar to look up a client software entry. **Note**: The option is disabled by default.
Initial Commands Configure initializing the environment. See Creating a new launcher command on page 181.	
Clean Commands Configure cleaning the environment. See Creating a new launcher command on page 181.	

5. Click *Submit*.

Non-proxy environment

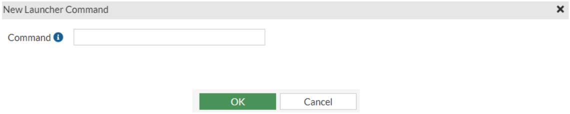
When using launchers with non-proxy mode, launchers may require the environment to be initialized beforehand. You may specify this with init-commands and clean-commands.

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:$HOST:$PORT /noConsentPrompt"
      set type rdp
      config init-commands
         edit 1
            set cmd "cmdkey /generic:$HOST /user:$USER /pass:$PASSWORD"
         next
      end
      config clean-commands
         edit 1
            set cmd "cmdkey /del:$HOST"
         next
      end
   next
end
```

Example secret configurations with launchers - example

To configure a secret with Web SSH launcher:

1. Go to *Secrets* > *Secrets*.
2. In *Secrets*, 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 165 to create a new template:
   Note: Ensure that the template uses *Web SSH* as its launcher.
   a. *Unix Account (SSH Password)*
   b. *Unix Account (SSH Key)*
   c. *FortiProduct (SSH Password)*

   Unix Account (SSH Password), *Unix Account (SSH Key)*, and *FortiProduct(SSH Password)* secret templates are preconfigured with *Web SSH* launcher.

7. In *Fields*, enter the required information.
8. Click *Submit*.

9. In *Secrets*, 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 165 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 165 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*.

Launch session monitor

The active session monitor is replaced with active launch monitor. One entry represents one launch instead of one session.

Multiple sessions may be made during a single launch. Some launch may still appear in the list even though the launch session is closed.

When the source port is `port 0`, no active TCP connection is attached to the launch.

The *Disconnect* button allows the administrator to terminate a secret launch session. The session attached to the token is broken.

You can use the following CLI command to list all the active launches:

```
diagnose wad token list
```

You can use the following CLI command to delete already added launches:

```
diagnose wad token clear <token_id>
```

The `token_id` variable is optional.

If no `token_id` is given, all the active launches are deleted.

By deleting active launches, sessions associated with all the launches are broken.

The video connection remains intact until the window is closed.

Policies

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

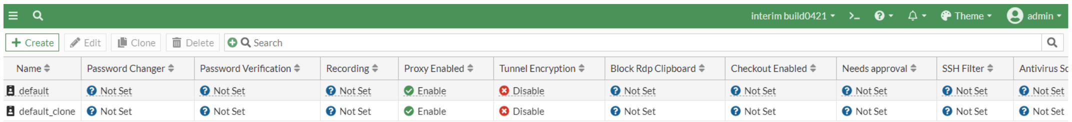
Policies in *Secret Settings* displays a list of secret policies.

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

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

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

The *Policies* tab looks like the following:



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

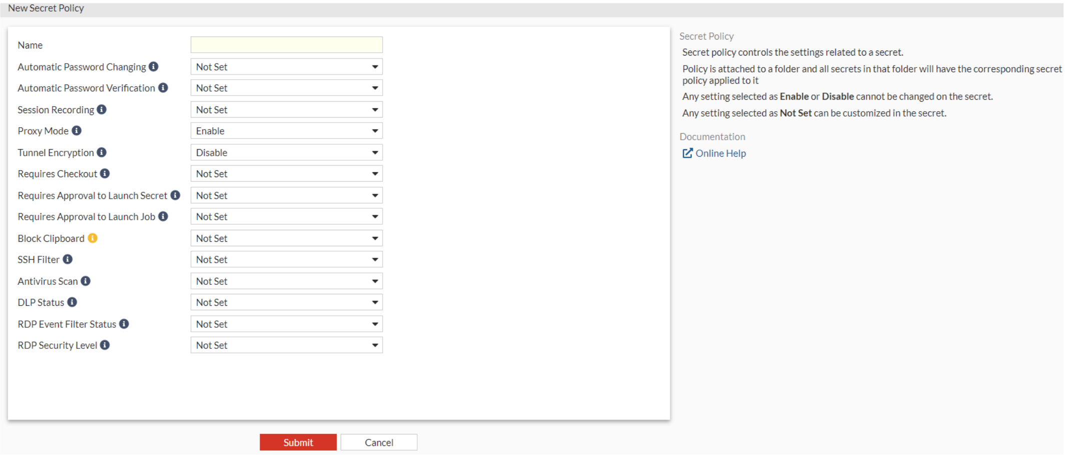
The *Policies* list contains the following options:

Create	Select to create a policy. See Creating a policy on page 185.
Edit	Select to edit the selected policy.
Clone	Select to clone the selected policy.
Delete	Select to delete the selected policies. The default secret policy cannot be deleted.
Search	Enter a search term in the search field, then hit `Enter` to search the policies list. To narrow down your search, see Column filter.

Creating a policy

To create a policy:

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


New Secret Policy

Name	
Automatic Password Changing	Not Set
Automatic Password Verification	Not Set
Session Recording	Not Set
Proxy Mode	Enable
Tunnel Encryption	Disable
Requires Checkout	Not Set
Requires Approval to Launch Secret	Not Set
Requires Approval to Launch Job	Not Set
Block Clipboard	Not Set
SSH Filter	Not Set
Antivirus Scan	Not Set
DLP Status	Not Set
RDP Event Filter Status	Not Set
RDP Security Level	Not Set

Secret Policy

Secret policy controls the settings related to a secret.

Policy is attached to a folder and all secrets in that folder will have the corresponding secret policy applied to it

Any setting selected as **Enable** or **Disable** cannot be changed on the secret.

Any setting selected as **Not Set** can be customized in the secret.

Documentation

Online Help

3. Enter the following information:

Name	Name of the policy.
Automatic Password Changing	Select *Enable*, *Disable*, or *Not Set*. When enabled, password changer for secrets is activated to periodically change the password.
Recursive	Displays the password changing schedule based on your selections for the related settings.
Start Time	The date and time when the *Change Interval (min)* begins. Enter date (MM/DD/YYYY) and time or select the *Calendar* icon and then select a date and time.
Recurrence	From the dropdown, select from the following three frequencies of recurrence: • *Daily* • *Weekly* • *Monthly*
Repeat every	The number of days/weeks/months after which the password is changed (1-400).
Occurs on	Select from the following days of the month when the password is automatically changed: • *First* • *Second* • *Third* • *Last* • *Last Day* • *Day* Select days of the week when the password is automatically changed. When you select *Day*, select + to add days of the month when the password is automatically changed. **Note**: The option is only available when *Recurrence* is set as *Weekly* or *Monthly*.

Editable in Secret	Enable/disable users from customizing the password change schedule in the secret.
Automatic Password Verification	Select *Enable*, *Disable*, or *Not Set*. When enabled, password changer for secrets is activated to periodically verify the password.
Verification Interval (min)	The time interval at which the secrets are tested for accuracy, in minutes (default = 60, 5 - 44640).
Start Time	The date and time when the *Interval(min)* begins. Enter date (MM/DD/YYYY) and time or select the *Calendar* icon and then select a date and time.
Editable in Secret	When enabled, you can customize the password verification schedule in the secret.
Session Recording	Select *Enable*, *Disable*, or *Not Set*. When enabled, user action performed on the secret is recorded. The video file is available in the log for users with appropriate permission.
Proxy Mode	Select *Enable*, *Disable*, or *Not Set*. When enabled, FortiPAM is responsible to proxy the connection from the user to the secret. When disabled, the non-proxy (direct) mode is used. See Modes of operation on page 38.
Tunnel Encryption	Select *Enable*, *Disable*, or *Not Set*. When launching a native launcher, FortiClient creates a tunnel between the endpoint and FortiPAM. The protocol stack is HTTP/TLS/TCP. The HTTP request gives information on the target server then FortiPAM connects to the target server. After that, two protocol options exist for the tunnel between FortiClient and FortiPAM. One is to clear the TLS layer for better throughput and performance. The other is to keep the TLS layer. The launcher's protocol traffic is inside the TLS secure tunnel. If the launcher's protocol is not secure, like VNC, it is strongly recommended to enable this option so that the traffic is in a secure tunnel. When there is an HTTPS Man In The Middle device, e.g., FortiGate or FortiWeb between FortiClient and FortiPAM, you must enable the *Tunnel Encryption* option. Otherwise, the connection will be disconnected, and the launching will fail. When set to *Not Set*, secrets using the policy can have the option set as either *Enable* or *Disable*.

	When the option is enabled or disabled, all the secrets using this policy have the same setting for this option as set in the policy.
Requires Checkout	Select *Enable*, *Disable*, or *Not Set*. When enabled, users are forced to check out the secret before gaining access. At a given time, only one user can check out a secret. Other approved users must wait for the secret to be checked in or wait for the checkout duration to lapse before accessing the secret. See Check out and check in a secret on page 98.
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 145 and Approval flow on page 199.
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 145 and Approval flow on page 199.
Approval Profile	From the dropdown, select an approval profile, or select *Create* to create a new approval profile. See Approval profile on page 199. Use the search bar to look up an approval profile. Use the pen icon next to the approval profile to edit it.
Block Clipboard	Select *Enable*, *Disable*, or *Not Set*. When enabled, for the following launchers, you cannot copy content from the launched secret web page: • *Web Launcher* • *Web SSH* • *Web Telnet* • *Web SMB* • *Web SFTP*

	When enabled, copying content from the remote computer to the local computer is blocked for the following launchers, but does not affect copy/paste on the remote computer itself: - *Web RDP* - Native *RDP* The feature needs Microsoft Edge and Google Chrome extension V3.
SSH Filter	Select *Enable*, *Disable*, or *Not Set*. When enabled, commands defined in the SSH profile to be executed on the secret are blocked.
SSH Filter Profile	From the dropdown, select an SSH filter profile.
Bypass For Owner	Enable/disable allowing secret owners to bypass the SSH command filter (default = disable). Once enabled, secret owners can send otherwise prohibited commands (listed in the SSH filter profile) to the targets. **Note**: The option is only available when *SSH Filter* is enabled.
Antivirus Scan	Select *Enable*, *Disable*, or *Not Set*. When enabled, it enforces an antivirus profile on the secret. See AntiVirus on page 221.
Antivirus Profile	From the dropdown, select an antivirus profile.
DLP Status	Select *Enable*, *Disable*, or *Not Set*. When enabled, it enforces a particular DLP profile on the secret.
DLP Filter Profile	From the dropdown, select a DLP filter profile.
RDP Event Filter Status	Select *Enable*, *Disable*, or *Not Set*. When enabled, it enforces a particular event filter profile on the secret.
RDP Event Filter Profile	From the dropdown, select an RDP filter profile.
RDP Security Level	Select a security level when establishing a RDP connection to the secret: - *Best Effort*: If the server supports NLA, FortiPAM uses NLA to authenticate. Otherwise, FortiPAM conducts standard RDP authentication with the server through RDP over TLS. - *NLA*: Network Level Authentication (CredSSP). When an RDP launcher is launched, FortiPAM is forced to use CredSSP (NLA) to authenticate with the target server. - *Not Set* - *RDP*: FortiPAM uses the standard RDP encryption provided by the RDP protocol without using TLS (Web-RDP only). - *TLS*: RDP over TLS. FortiPAM uses secured connection with encryption protocol TLS to

	connect with the target server.
RDP Auto TOTP	Enable/disable RDP auto Time-based One-time Password (TOTP). **Note**: The option is only available when *RDP Security Level* is set as *TLS*.
RDP Restricted Admin Mode	Enable/disable RDP restricted admin mode. Restricted admin mode prevents the transmission of reusable credentials to the remote system to which you connect using remote desktop. This prevents your credentials from being harvested during the initial connection process if the remote server has been compromised. **Note**: The option is only available when *RDP Security Level* is set as *Best Effort* or *NLA*.

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

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

For example - example:

While setting up a policy:

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

4. Click *Submit*.

See Applying a policy to a folder on page 190.

Configuring a secret policy where the secret owner can bypass the SSH command filter - example

To configure the secret policy:

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

```
 config secret policy
  edit "default"
   set ssh-filter enable
   set block-rdp-clipboard disable
   set bypass-ssh-filter-for-owner enable #enable allowing secret owners to bypass the
SSH command filter
  next
 end
```

Applying a policy to a folder

To apply a policy to a folder:

1. Go to a folder in *Secrets* > *Personal Folder/Public Folder*.
2. Either select *Edit Current Folder* to edit the folder and skip to step 5, or from the *Create* dropdown, select *Folder*.
3. Enter the name of the folder.

4. From the *Parent Folder* dropdown, select a folder.
5. Enable *Inherit Policy*, so that the folder follows the parent folder policy.

   > ⚠ You cannot inherit policy for a root folder.

   If *Inherit Policy* is disabled, from the *Secret Policy* dropdown, select a policy profile.
   Select *Create* to create a new secret policy. See Creating a policy on page 185.

   > Use the search bar to look up a policy.

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

6. Click *Save/Submit*.

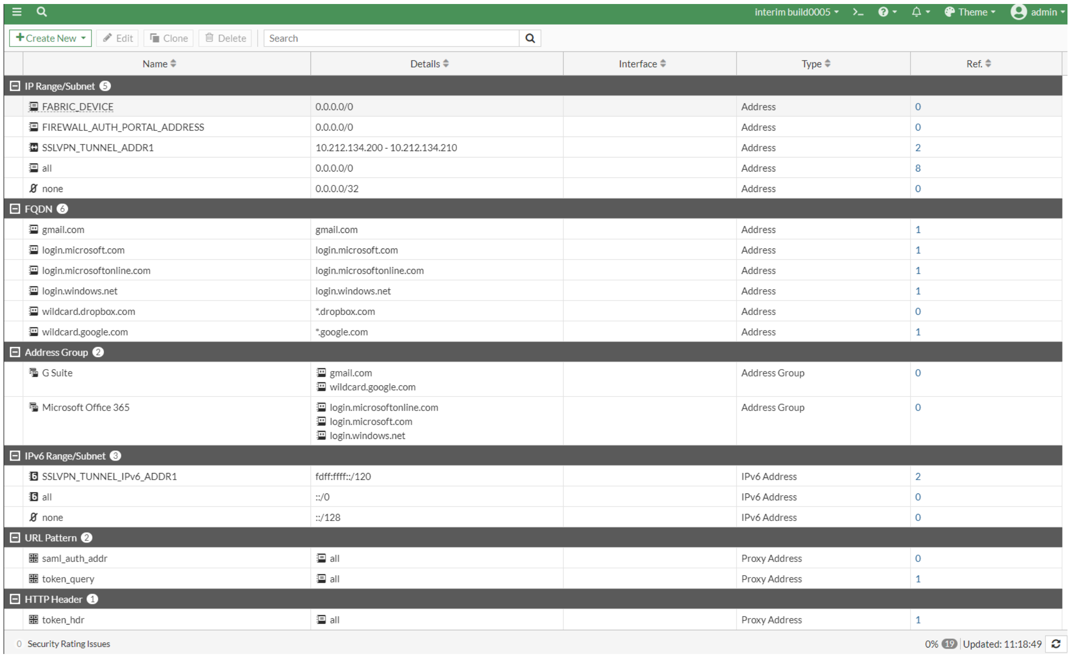
Addresses

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

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

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

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



Name	Details	Interface	Type	Ref.
IP Range/Subnet 5				
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 6				
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 2				
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 3				
SSLVPN_TUNNEL_IPv6_ADDR1	fdff:ffff::/120		IPv6 Address	2
all	::/0		IPv6 Address	0
none	::/128		IPv6 Address	0
URL Pattern 2				
saml_auth_addr	all		Proxy Address	0
token_query	all		Proxy Address	1
HTTP Header 1				
token_hdr	all		Proxy Address	1

0 Security Rating Issues

0% 19 Updated: 11:18:49

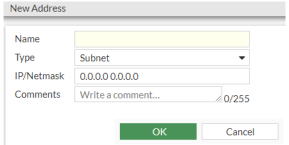
The *Addresses* tab contains the following options:

+Create New	From the dropdown, select *Address* or *Address Group* to create an address or an address group. See Creating an address on page 192 and Creating an address group on page 193
Edit	Select to edit the selected address or address group.
Clone	Select to clone the selected address or address group.
Delete	Select to delete the selected addresses or address groups.
Search	Enter a search term in the search field, then hit `Enter` to search the list. To narrow down your search, see Column filter.
Refresh	To refresh the contents, click the refresh icon on the bottom-right.

Creating an address

To create an address:

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



New Address

Name

Type: Subnet

IP/Netmask: 0.0.0.0 0.0.0.0

Comments: Write a comment... 0/255

3. Enter the following information:

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

4. Click *OK*.

Creating an address using the CLI - example

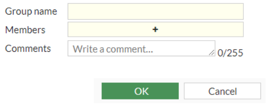
1. Enter the following commands in the CLI console:

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

Creating an address group

To create an address group:

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



3. Enter the following information:

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

4. Click *OK*.

Creating an address group using the CLI - example

1. Enter the following commands in the CLI console:

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

Dependency updater

Service accounts

A service account is a non-human privileged account that an operating system uses to run applications, automated services, virtual machine instances, and other background processes.

A service account provides a way to assign an identity and permissions to a computer program or process that performs a specialized task.

Service accounts have privileges that allow extensive access to system resources either locally or across the domain.

While service accounts can be created manually, they are often preinstalled and preconfigured as part of an operating system or another software program.

Service accounts pose a greater risk compared to other privileged accounts as they can potentially enable bad actors to hide in plain sight by operating under the cloak of a valid program. Many such programs run continuously, giving attackers persistent access.

Cybercriminals who hack a service account can elevate privileges to gain ever more access. Adopting a phantom identity allows them to roam freely through corporate IT networks and cloud environments without arousing suspicions.

Updating service accounts

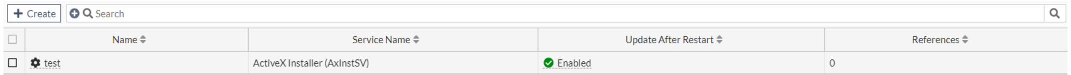
If a service running on a machine relies on a credential managed by FortiPAM, the dependency updater feature offers the ability to update the service credential immediately after FortiPAM changes the credential. FortiPAM ensures that the service does not fail during authentication.

Dependency Updater in *Secret Settings* displays a list of dependency updaters.

A dependency updater defines the service identifier and its type.

For every dependency updater, the following columns are displayed by default:

- *Name*
- *Service Name*
- *Update After Restart*
- *References*



□	Name	Service Name	Update After Restart	References
□	test	ActiveX Installer (AxInstSV)	✓ Enabled	0

The *Dependency Updater* tab contains the following options:

Create	Select to create a new dependency updater. See Creating a dependency updater on page 195.
Search	Enter a search term in the search field, then hit `Enter` to search the dependency updater list. To narrow down your search, see Column filter.
Edit	Select to edit the selected dependency updater.
Delete	Select to delete the selected the selected dependency updaters.
Clear Selection	Select to clear the currently selected dependency updater entries from selection.

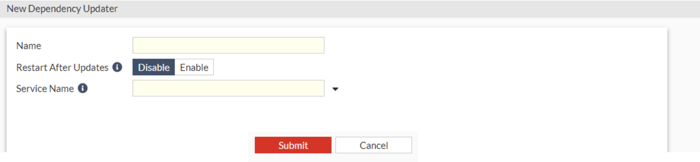
For updating the Windows server, WinRM service must be configured on the target machine, and there must be a privileged account for the target machine in FortiPAM.

See Updating a service account credential Example on page 197.

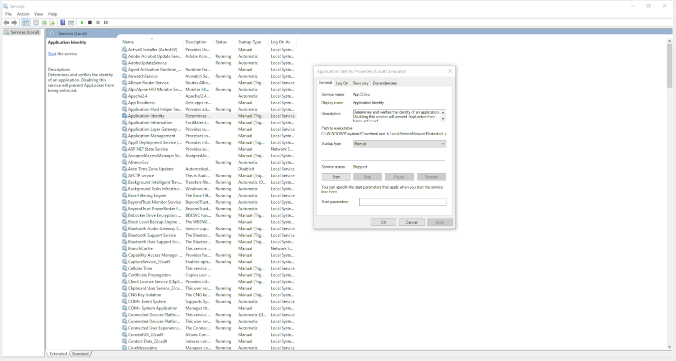
Creating a dependency updater

To create a dependency updater:

1. Go to *Secret Settings* > *Dependency Updater*.
2. Select *Create*.
   The *New Dependency Updater* window opens.



3. Enter the following information:

Name	The name of the dependency updater.
Restart After Updates	Enable/disable restarting the service after updating the service credentials (default = disable).
Service Name	Enter a service name or from the dropdown, select a service. On Windows, the Service *Display name* is different from the *Service name*. For example, in *Services* on Windows, when you double-click *Application Identity*, you see that the *Service name* is *AppIDSvc*. 

4. Click *Submit*.

Configuring dependency updater via the CLI commands - Example

To configure dependency updater via the CLI commands:

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

```
config secret dependency-updater
 edit 'win-mysql-updater'
  set  type win-service
  set  restart disable
  set service-name 'MySQL80'
 next
end
```

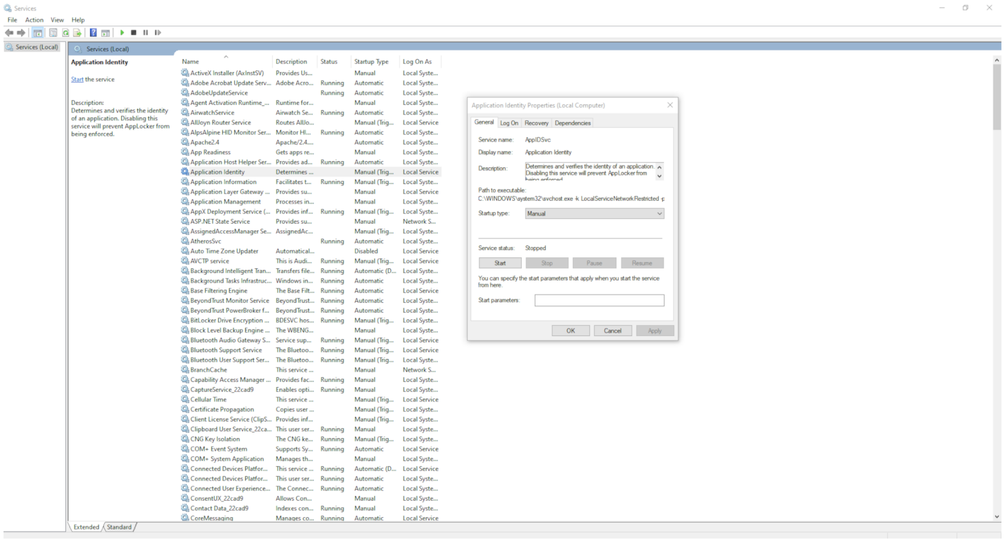
Updating a service account credential - Example

To update a service account credential:

1. Go to *Secret Settings* > *Dependency Updater*.
2. Select *Create*.
   The *New Dependency Updater* window opens.
3. In *Name*, enter a name for the dependency updater.
4. Set *Restart After Updates* to *Disable*.
   If you intend to restart the service each time after updating the service credential, set *Restart After Updates* to *Enable*.
5. In the *Service Name* dropdown, select *Application Identity*.

On Windows, the Service *Display name* is different from the *Service name*.

For example, in *Services* on Windows, when you double-click *Application Identity*, you see that the *Service name* is *AppIDSvc*.



Application Identity

Start the service

Description:
Determines and verifies the identity of an application. Disabling this service will prevent AppLocker from being enforced.

Name	Description	Status	Startup Type	Log On As
ActiveX Installer (AxInstSV)	Provides Us...		Manual	Local Syste...
Adobe Acrobat Update Serv...	Adobe Acro...	Running	Automatic	Local Syste...
AdobeUpdateService		Running	Automatic	Local Syste...
Agent Activation Runtime_...	Runtime for...		Manual	Local Syste...
AirwatchService	Airwatch Se...	Running	Automatic	Local Syste...
AllJoyn Router Service	Routes AllJo...		Manual (Trig...	Local Service
AlpsAlpine HID Monitor Ser...	Monitor HI...	Running	Automatic	Local Syste...
Apache2.4	Apache/2.4....		Automatic	Local Syste...
App Readiness	Gets apps re...		Manual	Local Syste...
Application Host Helper Ser...	Provides ad...	Running	Automatic	Local Syste...
Application Identity	Determines ...		Manual (Trig...	Local Service
Application Information	Facilitates t...	Running	Manual (Trig...	Local Syste...
Application Layer Gateway ...	Provides su...		Manual	Local Service
Application Management	Processes in...		Manual	Local Syste...
AppX Deployment Service (...	Provides inf...	Running	Manual (Trig...	Local Syste...
ASP.NET State Service	Provides su...		Manual	Network S...
AssignedAccessManager Se...	AssignedAc...		Manual (Trig...	Local Syste...
AtherosSvc		Running	Automatic	Local Syste...
Auto Time Zone Updater	Automatical...		Disabled	Local Service
AVCTP service	This is Audi...	Running	Manual (Trig...	Local Service
Background Intelligent Tran...	Transfers file...	Running	Automatic (D...	Local Syste...
Background Tasks Infrastruc...	Windows in...	Running	Automatic	Local Syste...
Base Filtering Engine	The Base Filt...	Running	Automatic	Local Service
BeyondTrust Monitor Service	BeyondTrust...	Running	Automatic	Local Syste...
BeyondTrust PowerBroker f...	BeyondTrust...	Running	Automatic	Local Syste...
BitLocker Drive Encryption ...	BDESVC hos...	Running	Manual (Trig...	Local Syste...
Block Level Backup Engine ...	The WBENG...		Manual	Local Syste...
Bluetooth Audio Gateway S...	Service sup...	Running	Manual (Trig...	Local Service
Bluetooth Support Service	The Bluetoo...	Running	Manual (Trig...	Local Service
Bluetooth User Support Ser...	The Bluetoo...	Running	Manual (Trig...	Local Syste...
BranchCache	This service ...		Manual	Network S...
Capability Access Manager ...	Provides fac...	Running	Manual	Local Syste...
CaptureService_22cad9	Enables opti...	Running	Manual	Local Syste...
Cellular Time	This service ...		Manual (Trig...	Local Service
Certificate Propagation	Copies user ...		Manual (Trig...	Local Syste...
Client License Service (ClipS...	Provides inf...		Manual (Trig...	Local Syste...
Clipboard User Service_22ca...	This user ser...	Running	Manual	Local Syste...
CNG Key Isolation	The CNG ke...	Running	Manual (Trig...	Local Syste...
COM+ Event System	Supports Sy...	Running	Automatic	Local Service
COM+ System Application	Manages th...		Manual	Local Syste...
Connected Devices Platfor...	This service ...	Running	Automatic (D...	Local Service
Connected Devices Platfor...	This user ser...	Running	Automatic	Local Syste...
Connected User Experience...	The Connec...	Running	Automatic	Local Syste...
ConsentUX_22cad9	Allows Con...		Manual	Local Syste...
Contact Data_22cad9	Indexes con...	Running	Manual	Local Syste...
CoreMessaging	Manages co...	Running	Automatic	Local Service

Application Identity Properties (Local Computer)

General | Log On | Recovery | Dependencies

Service name: AppIDSvc

Display name: Application Identity

Description: Determines and verifies the identity of an application. Disabling this service will prevent AppLocker from being enforced.

Path to executable:
C:\WINDOWS\system32\svchost.exe -k LocalServiceNetworkRestricted -p

Startup type: Manual

Service status: Stopped

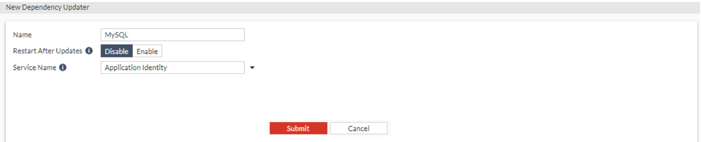
Start | Stop | Pause | Resume

You can specify the start parameters that apply when you start the service from here.

Start parameters:

OK | Cancel | Apply

6. Click *Submit*.



New Dependency Updater

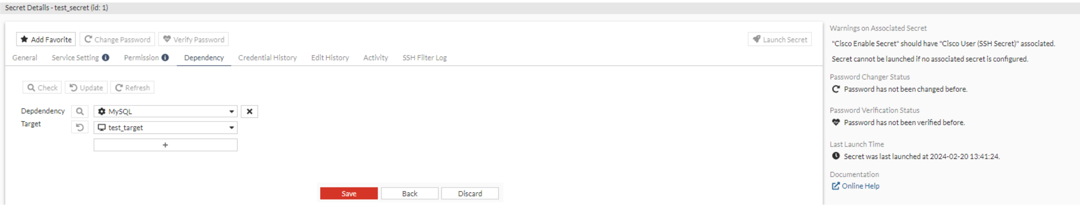
Name: MySQL

Restart After Updates: Disable | Enable (Disable selected)

Service Name: Application Identity

7. Go to *Secrets* > *Secrets*.
8. Double-click the secret that you intend to use as the credential for a target where the service defined in the dependency updater runs.
9. Select the *Dependency* tab.
10. Select +.
11. From the *Dependency* dropdown, select the dependency updater created earlier.
12. From the *Target* dropdown, select a target.

13. Click *Save*.



Secret Details - test_secret (id: 1)

Depdendency Target: MySQL, test_target

Warnings on Associated Secret
"Cisco Enable Secret" should have "Cisco User (SSH Secret)" associated.
Secret cannot be launched if no associated secret is configured.

Password Changer Status
Password has not been changed before.

Password Verification Status
Password has not been verified before.

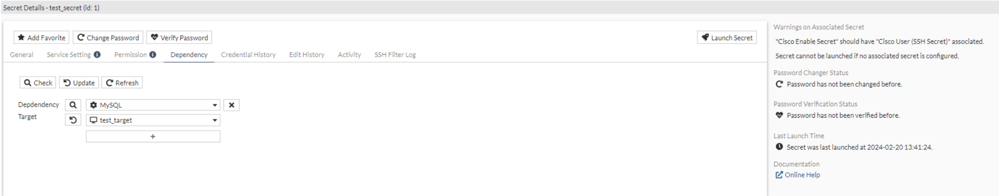
Last Launch Time
Secret was last launched at 2024-02-20 13:41:24.

Documentation

Once the secret password changer successfully rotates the secret password, all the dependencies in the secret are automatically updated.

To update an individual dependency, click the *Update Dependency* (⟲) icon on the left of each dependency when editing a secret.

If needed, you can update all the dependencies by selecting *Update* from the top when editing the secret.



Secret Details - test_secret (id: 1)

Depdendency Target: MySQL, test_target

Warnings on Associated Secret
"Cisco Enable Secret" should have "Cisco User (SSH Secret)" associated.
Secret cannot be launched if no associated secret is configured.

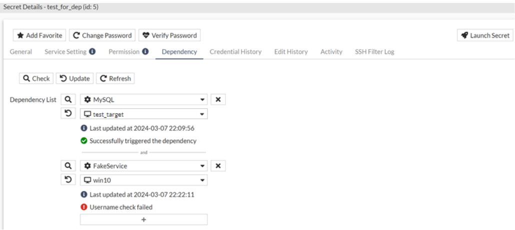
Password Changer Status
Password has not been changed before.

Password Verification Status
Password has not been verified before.

Last Launch Time
Secret was last launched at 2024-02-20 13:41:24.

Documentation

Click the *Check Dependency* (🔍) icon on the left of each dependency to check if the service is running or not, and whether the service is running with the particular secret user name.



Secret Details - test_for_dep (id: 5)

Dependency List: MySQL, test_target
Last updated at 2024-03-07 22:09:56
Successfully triggered the dependency

FakeService, win10
Last updated at 2024-03-07 22:22:11
Username check failed

To check all the dependencies in a secret, select *Check* from the top when editing a secret.

To sync the current status of the dependencies, select *Refresh* from the top when editing a secret.

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 200.

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.

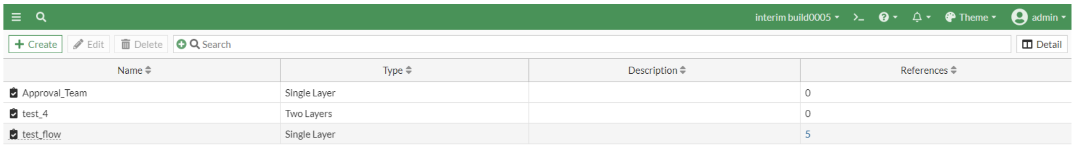
See Approval profile on page 199.

Approval profile

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

For every approval profile, the following fields are shown:

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



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 200.
Edit	Select to edit the selected approval profile.
Delete	Select to delete the selected profiles.
Search	Enter a search term in the search field, then hit `Enter` to search the approval profiles list. To narrow down your search, see Column filter.
Details	Select to see details of the selected approval profile.

Enabling approval profiles for a secret

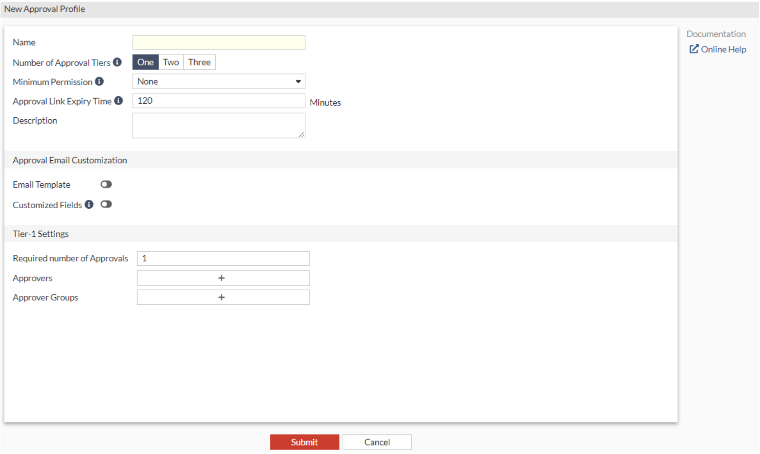
To enable approval profile:

1. Go *Secrets* > *Secrets*.
2. In *Secrets*, select a secret and then select *Edit*.
   The *Secret Details* window opens.
3. In the *Secret Setting* pane, enable *Requires Approval to Launch Secret* to require users to request permission from the approvers defined in the approval profile for secret launching.
   Alternatively, enable *Requires Approval to Launch Job* to require users to request permission from the approvers defined in the approval profile for job execution.
4. In the *Approval Profile* dropdown, select an approval profile, or select *Create* to create a new approval profile. See Create an approval profile on page 200.
5. Click *Save*.

Create an approval profile

To create an approval request:

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



New Approval Profile

Name

Number of Approval Tiers: One | Two | Three

Minimum Permission: None

Approval Link Expiry Time: 120 Minutes

Description

Approval Email Customization

Email Template

Customized Fields

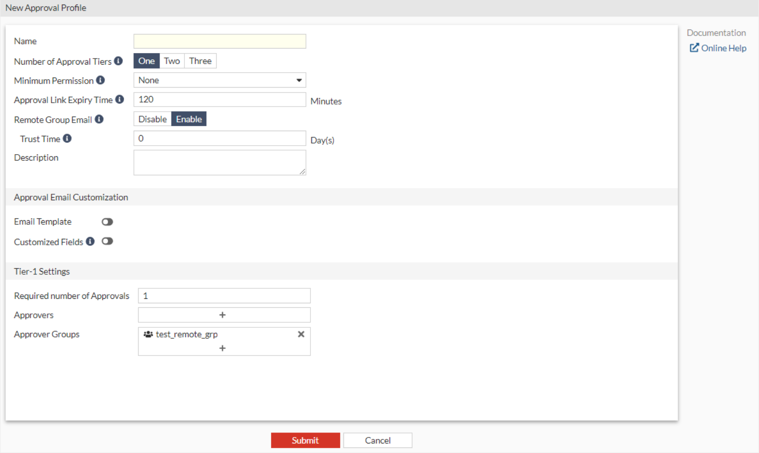
Tier-1 Settings

Required number of Approvals: 1

Approvers

Approver Groups

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: - *One* (default) - *Two* - *Three*
Minimum Permission	From the dropdown, select the minimum secret permission required by the approver to view the secret request: - *None* (default) - *List* - *View* - *Edit* - *Owner*
Approval Link Expiry Time	The expiry time for the approve/deny link in the secret approval request email, in minutes (30 - 600, default = 120). The expiry time count starts when the email is sent.
Remote Group Email	Enabling ensures that members of an approver group receive email notification when an access request is sent for a secret where *Requires Approval to Launch Secret* (see Creating a secret on page 72) is enabled and an approval profile is selected with at least one remote user group as an approver (default = disable). The option appears when you select at least one remote use r group in *Approver Groups*.  New Approval Profile Name Number of Approval Tiers: [✓ One] Two Three Minimum Permission: None Approval Link Expiry Time: 120 Minutes Remote Group Email: Disable [✓ Enable] Trust Time: 0 Day(s) Description Approval Email Customization Email Template ○ Customized Fields ○ Tier-1 Settings Required number of Approvals: 1 Approvers: + Approver Groups: test_remote_grp ✕ +

	Trust Time Controls how frequently the remote user needs to log in to FortiPAM to receive the approver email notification. Enter the number of days from the access request creation time a remote user belonging to the remote user group in *Approver Groups* logs in to FortiPAM (0 - 30, default = 0). **Note**: 0 means no login requirements. For example, when *Trust Time* is `5`, a remote user belonging to the remote user group selected in *Approver Groups* must have logged in to FortiPAM at least once within five days from the access request creation time to receive the approver email notification. The field appears when *Remote Group Email* is enabled. *Trust Time* filters out remote users who are not disabled/removed on FortiPAM but are removed from the IdP. If the approving user logs in to FortiPAM before the access request expires, the user can still approve the access request, but no email notification is sent.
Description	Optionally, enter a description.
Approval Email Customization	
Email Template	Enable, and from the dropdown, select a customized email template. See Approval email template on page 203. Use the search bar to look up a custom email template.
Customized Fields	Enable and add text/number as fields. Select + to add additional fields. The custom fields capture additional information necessary for the approval process tailored to the specific needs of your organization. Select *Required* next to the field to make the field mandatory. **Note**: The option is disabled by default.

Tier-1 Settings	
	Tier 2 and 3 options are same as tier 1.
Required number of Approvals	The minimum number of approvals required. The number of user or user groups reviewing a secret request as part of an approval profile must be at least equal to the number of approvals required to pass the request to the next tier or approve it.
Approvers	Select + and from the list, select users in the *Select Entries* window. The selected users will review the secret request. **To add a new user:** **1.** From the *Select Entries* window, select *Create*. The *New User List* wizard opens. **2.** Follow the steps in Creating a user on page 253, starting step 2 to create a new user. Use the search bar to look up a user.
Approver Groups	Select + and from the list, select user groups in the *Select Entries* window. The selected user groups will review the secret request. **To add a new user group:** **1.** From the *Select Entries* window, select *Create*. The *Create New User Group* window opens. **2.** Follow the steps in Creating user groups, starting step 3. Use the search bar to look up a user group.

4. Click *Submit*.

Approval email template

Approval Email Template in *Secret Settings* displays a list of secret approval request email templates.

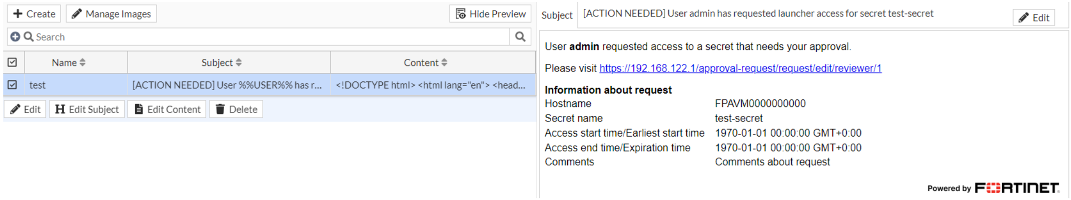
You can create a custom email template for the secret approval request email sent to the approvers.

Custom email templates can be created in the GUI or the CLI console.

For every approval email template, the following columns are displayed by default:

- *Name*
- *Subject*
- *Content*

When you select an email template, a preview of the selected email template is displayed on the right.



☑	Name	Subject	Content
☑	test	[ACTION NEEDED] User %%USER%% has r...	<!DOCTYPE html> <html lang="en"> <head...

Subject [ACTION NEEDED] User admin has requested launcher access for secret test-secret

User **admin** requested access to a secret that needs your approval.

Please visit https://192.168.122.1/approval-request/request/edit/reviewer/1

Information about request

Hostname	FPAVM0000000000
Secret name	test-secret
Access start time/Earliest start time	1970-01-01 00:00:00 GMT+0:00
Access end time/Expiration time	1970-01-01 00:00:00 GMT+0:00
Comments	Comments about request

Approval email template list contains the following options:

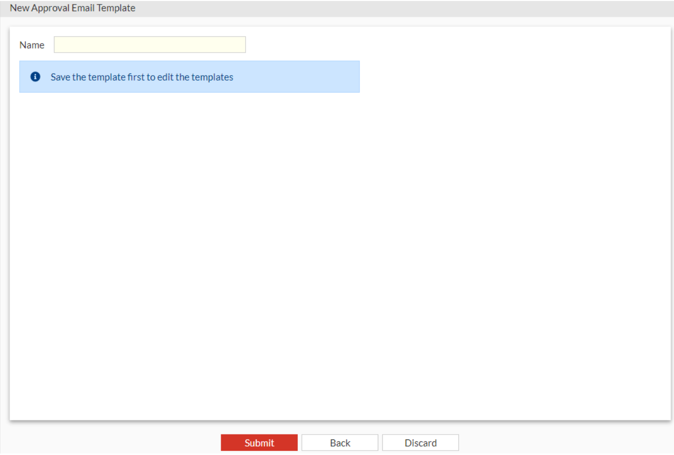
Create	Select to create an approval email template. See Creating an approval email template on page 205.
Manage Images	Select to view the available images and their respective tags and add new images. By default, images are embedded in the approval email template instead of using a URL. See Managing images on page 413.
Hide/Show Preview	Select to hide or show the selected approval email template preview.
Search	Enter a search term in the search field, then hit `Enter` to search the approval email template list. To narrow down your search, see Column filter.
Edit	Select to edit the selected approval email template.
Edit Subject	Select to edit the subject of the selected approval email template.
Edit Content	Select to edit the content of the selected approval email template.
Delete	Select to delete the selected approval email template.

To create an approval email template using the CLI console, see Creating an approval email template using the CLI on page 207.

Creating an approval email template

To create an approval email template:

1. Go to *Secret Settings* > *Approval Email Template*.
2. Select *Create*.
   The *New Approval Email Template* window opens.



New Approval Email Template

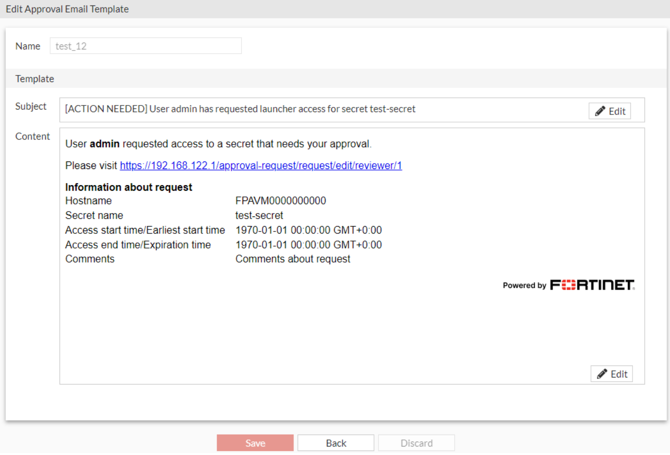
Name

Save the template first to edit the templates

3. In *Name*, enter a name for the approval email template.
4. Click *Submit*.

> You must save the approval email template first to be able to edit the template.

The *Edit Approval Email Template* window opens.



Edit Approval Email Template

Name test_12

Template

Subject [ACTION NEEDED] User admin has requested launcher access for secret test-secret

Content

User **admin** requested access to a secret that needs your approval.

Please visit https://192.168.122.1/approval-request/request/edit/reviewer/1

Information about request

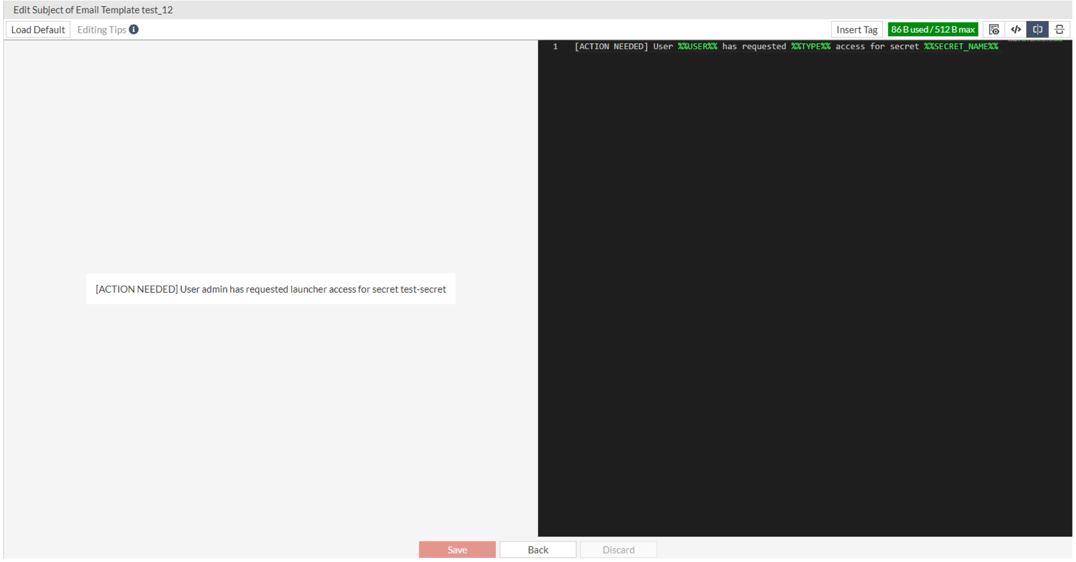
Hostname	FPAVM0000000000
Secret name	test-secret
Access start time/Earliest start time	1970-01-01 00:00:00 GMT+0:00
Access end time/Expiration time	1970-01-01 00:00:00 GMT+0:00
Comments	Comments about request

Powered by FORTINET

5. In the *Template* pane:
   a. In *Subject*, select *Edit*.
      The *Edit Subject of Email Template* `Name` window opens.

The subject must be text only.

By default, the preview and the plain text code are displayed as a horizontally split screen.



```
[ACTION NEEDED] User %%USER%% has requested %%TYPE%% access for secret %%SECRET_NAME%%
```

[ACTION NEEDED] User admin has requested launcher access for secret test-secret

Click the insert buttons to add variable, image tags, or:

- Enter `%%` to show all the available variables.
- Hit `Ctrl + Space` to display the auto-completion pane.
- Use the preview pane to preview the changes in realtime.

Select *Load Default* to load the default entry.

From the options on the right, select:

- *Preview* (🗔): Preview the subject.
- *Editor* (</>): Open the plain text code editor.
- *Horizontal Split* (◫): Editor and preview screens are horizontally split.
- *Vertical Split* (⊟): Editor and preview screens are vertically split.

b. Edit the plain text code.

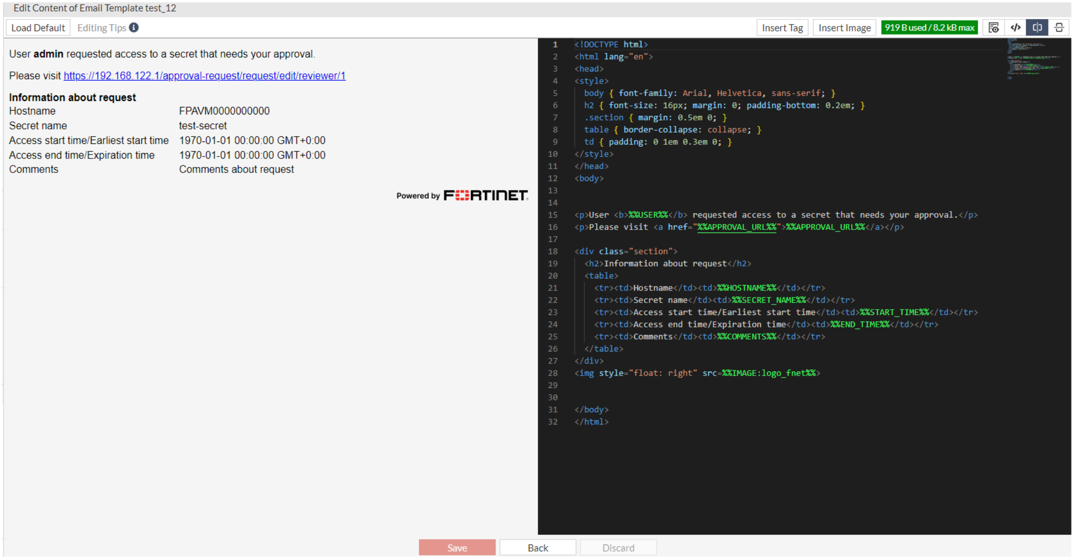
c. **To insert a tag:**

   i. In the plain text code where you intend to add a tag, select *Insert Tag*. Alternatively, enter `%%` to show all the variables.

   ii. From the list that appears, select a tag.

d. Click *Save*.

e. In *Content*, select *Edit*.
The *Edit Content of Email Template* `Name` window opens.



User **admin** requested access to a secret that needs your approval.

Please visit https://192.168.122.1/approval-request/request/edit/reviewer/1

Information about request

Hostname	FPAVM0000000000
Secret name	test-secret
Access start time/Earliest start time	1970-01-01 00:00:00 GMT+0:00
Access end time/Expiration time	1970-01-01 00:00:00 GMT+0:00
Comments	Comments about request

Powered by FORTINET

```
<!DOCTYPE html>
<html lang="en">
<head>
<style>
  body { font-family: Arial, Helvetica, sans-serif; }
  h2 { font-size: 16px; margin: 0; padding-bottom: 0.2em; }
  .section { margin: 0.5em 0; }
  table { border-collapse: collapse; }
  td { padding: 0 1em 0.3em 0; }
</style>
</head>
<body>


<p>User <b>%%USER%%</b> requested access to a secret that needs your approval.</p>
<p>Please visit <a href="%%APPROVAL_URL%%">%%APPROVAL_URL%%</a></p>

<div class="section">
  <h2>Information about request</h2>
  <table>
    <tr><td>Hostname</td><td>%%HOSTNAME%%</td></tr>
    <tr><td>Secret name</td><td>%%SECRET_NAME%%</td></tr>
    <tr><td>Access start time/Earliest start time</td><td>%%START_TIME%%</td></tr>
    <tr><td>Access end time/Expiration time</td><td>%%END_TIME%%</td></tr>
    <tr><td>Comments</td><td>%%COMMENTS%%</td></tr>
  </table>
</div>
<img style="float: right" src=%%IMAGE:logo_fnet%%>


</body>
</html>
```

f. Edit the plain text code.

g. To insert tag, follow step c.

h. **To insert an image:**

   i. In the plain text code where you intend to add an image, select *Insert Image*.
   The cursor goes to `%%IMAGE:`, a list of all the images with preview appears.

   Alternatively, enter `%%IMAGE:`.

   ii. Select an image from the list.

   The email maximum size is 192 KB, including all images. If the email is too large, FortiPAM truncates it to fit within the size limit.

i. Click *Save*.

6. Click *Save*.

The approval email template can now be added to an approval profile. See Create an approval profile on page 200.

Creating an approval email template using the CLI

To create an approval email template:

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

```
config secret approval-email-template
 edit "test-template"
```

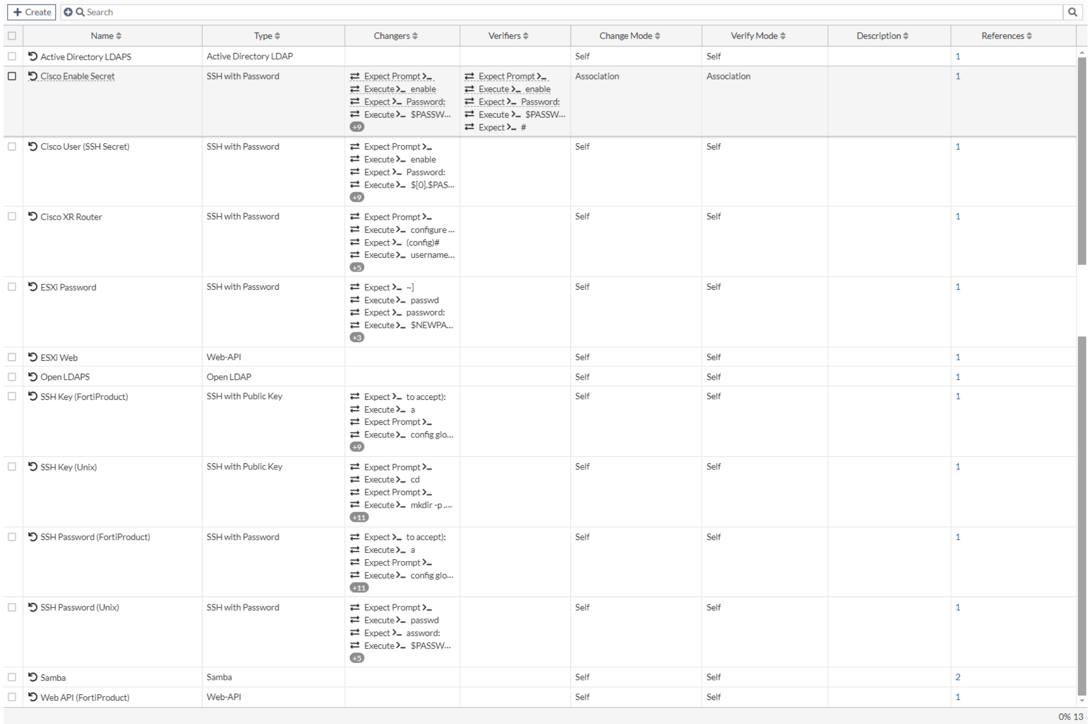
```
        set subject "User %%USER%% has requested access to secret %%SECRET_ID%%"
        set content "TEST EMAIL
Approval url: %%APPROVAL_URL%%
Request id: %%REQUEST_ID%%
Secret url: %%SECRET_URL%%
Secret id: %%SECRET_ID%%
Secret name: %%SECRET_NAME%%
Job name: %%JOB_NAME%%
Start time: %%START_TIME%%
End time: %%END_TIME%%
Hostname: %%HOSTNAME%%
User: %%USER%%
"
    next
 end
```

Variable	Description
`%%TYPE%%`	`launcher` or `job` depending on the type of the request.
`%%APPROVAL_URL%%`	The URL to access the secret approval page to approve/deny the request.
`%%REQUEST_ID%%`	The request ID in the configuration management database.
`%%SECRET_URL%%`	The URL to access secret information.
`%%SECRET_ID%%`	The secret ID in the configuration management database.
`%%SECRET_NAME%%`	The name of the secret.
`%%JOB_NAME%%`	The name of the job (empty for a secret request).
`%%START_TIME%%`	The time allowed to begin launching the secret or the earliest execution time for the job request.
`%%END_TIME%%`	The time after which you cannot launch the secret or the request approval expiration time for the job request.
`%%HOSTNAME%%`	FortiPAM name/ID.
`%%COMMENTS%%`	Comments by the requester.
`%%USER%%`	User name.
`%%IMAGE:`	Custom image.

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.



+ Create | Search

□	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	⇄ Expect Prompt >_ ⇄ Execute >_ enable ⇄ Expect >_ Password: ⇄ Execute >_ $PASSW... +9	⇄ Expect Prompt >_ ⇄ Execute >_ enable ⇄ Expect >_ Password: ⇄ Execute >_ $PASSW... ⇄ Expect >_ #	Association	Association		1
□	Cisco User (SSH Secret)	SSH with Password	⇄ Expect Prompt >_ ⇄ Execute >_ enable ⇄ Expect >_ Password: ⇄ Execute >_ $[0].$PAS... +9		Self	Self		1
□	Cisco XR Router	SSH with Password	⇄ Expect Prompt >_ ⇄ Execute >_ configure ... ⇄ Expect >_ (config)# ⇄ Execute >_ username... +5		Self	Self		1
□	ESXi Password	SSH with Password	⇄ Expect >_ ~] ⇄ Execute >_ passwd ⇄ Expect >_ password: ⇄ Execute >_ $NEWPA... +3		Self	Self		1
□	ESXi Web	Web-API			Self	Self		1
□	Open LDAPS	Open LDAP			Self	Self		1
□	SSH Key (FortiProduct)	SSH with Public Key	⇄ Expect >_ to accept): ⇄ Execute >_ a ⇄ Expect Prompt >_ ⇄ Execute >_ config glo... +9		Self	Self		1
□	SSH Key (Unix)	SSH with Public Key	⇄ Expect Prompt >_ ⇄ Execute >_ cd ⇄ Expect Prompt >_ ⇄ Execute >_ mkdir -p .... +11		Self	Self		1
□	SSH Password (FortiProduct)	SSH with Password	⇄ Expect >_ to accept): ⇄ Execute >_ a ⇄ Expect Prompt >_ ⇄ Execute >_ config glo... +11		Self	Self		1
□	SSH Password (Unix)	SSH with Password	⇄ Expect Prompt >_ ⇄ Execute >_ passwd ⇄ Expect >_ assword: ⇄ Execute >_ $PASSW... +5		Self	Self		1
□	Samba	Samba			Self	Self		2
□	Web API (FortiProduct)	Web-API			Self	Self		1

0% 13

FortiPAM offers the following default password changers:

- Active Directory LDAPS
- Cisco Enable Secret
- Cisco User (SSH Secret)
- Cisco XR Router
- ESXi Password
- ESXi Web
- Open LDAPS
- SSH Key (FortiProduct)
- SSH Key (Unix)
- SSH Password (FortiProduct)
- SSH Password (Unix)
- Samba
- Web API (FortiProduct)

Default password changers cannot be edited.

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

For LDAPS password changer and verification, the minimum SSL/TLS version and the target server port number used by LDAPS can be set using the following CLI commands, provided the secret has an associated target:

```
 config secret target
  edit target_name
   set ldaps-min-ssl-version {default | SSLv3 | TLSv1 | TLSv1.1 | TLSv1.2 | TLSv1.3}
   set ldaps-port <integer>
  end
end
```

If there is no associated target with the secret or `ldaps-min-ssl-version` is set to `default`, the minimum SSL/TLS version used follows `system > global > ssl-min-proto-version`.

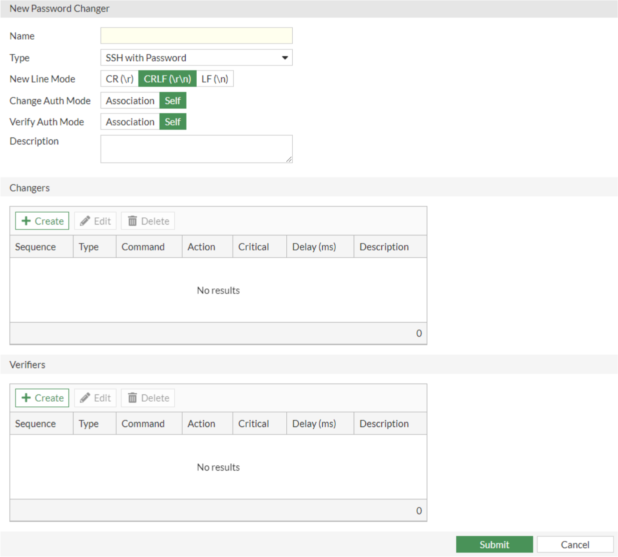
The *Password Changers* tab in *Secret Settings* contains the following options:

Create	Select to create a new password changer. See Creating a password changer on page 210.
Edit	Select to edit the selected password changer.
Delete	Select to delete the selected password changers.
Clone	Select to clone the selected password changer.
Search	Enter a search term in the search field, then hit `Enter` to search the password changers list. To narrow down your search, see Column filter.

Creating a password changer

To create a password changer:

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



New Password Changer

Name	
Type	SSH with Password
New Line Mode	CR (\r) [✓ CRLF (\r\n)] LF (\n)
Change Auth Mode	Association [✓ Self]
Verify Auth Mode	Association [✓ Self]
Description	

Changers

Sequence	Type	Command	Action	Critical	Delay (ms)	Description
No results						

0

Verifiers

Sequence	Type	Command	Action	Critical	Delay (ms)	Description
No results						

0

4. Enter the following information:

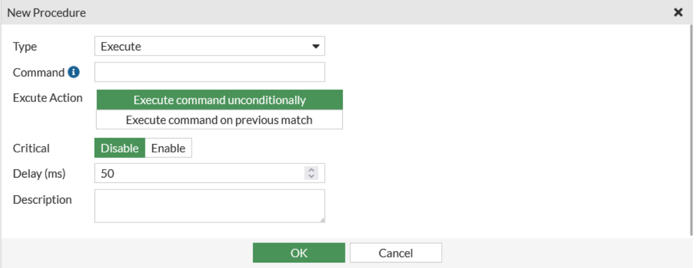
Name	The name of the password changer.
Type	From the dropdown, select a type: • *Active Directory LDAP* • *Open LDAP* • *Samba* • *SSH with Public Key* • *SSH with Password* (default)
New Line Mode	Select from the following options: • *CR (\r)*: Carriage Return (\r) • *CRLF (\r\n)*: Carriage Return and Line Feed (\r\n) (default) • *LF (\n)*: Line Feed (\n)
Change Auth Mode	Select from the following two options: • *Association*: Changing password requires credentials from the associated secret. See *Associated Secret* option when Creating a secret on page 72. • *Self*: Secret can change its password (default).
Verify Auth Mode	Select from the following two options: • *Association*: Verifying password requires credentials from the associated secret. See *Associated Secret* option when Creating a secret on page 72. • *Self*: Secret can verify its password (default).
Description	Optionally, enter a description.
Changers	The password changing procedure. See Changers.

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

5. Click *Submit*.

Changers

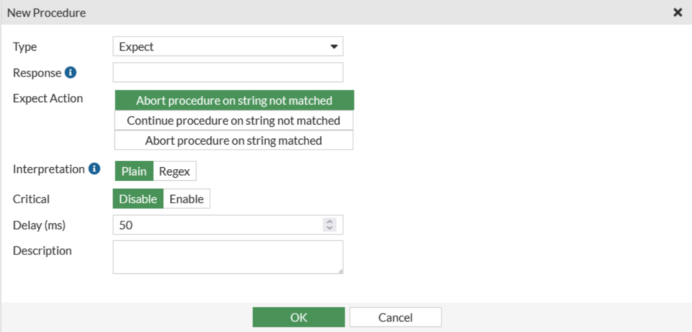
1. In step 4 when Creating a password changer, select *Create* in *Changers*.
   The *New Procedure* window opens. By default, the *Type* is *Execute*.



New Procedure

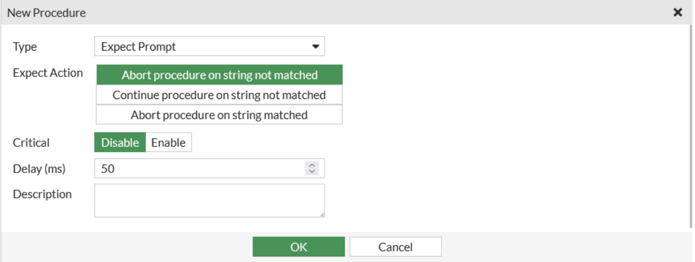
Type	Execute
Command	
Excute Action	Execute command unconditionally Execute command on previous match
Critical	Disable Enable
Delay (ms)	50
Description	

   Different configuration options are available according to the *Type* selected.



New Procedure

Type	Expect
Response	
Expect Action	Abort procedure on string not matched Continue procedure on string not matched Abort procedure on string matched
Interpretation	Plain Regex
Critical	Disable Enable
Delay (ms)	50
Description	



New Procedure

Type	Expect Prompt
Expect Action	Abort procedure on string not matched Continue procedure on string not matched Abort procedure on string matched
Critical	Disable Enable
Delay (ms)	50
Description	

2. Enter the following information:

Type	From the dropdown, select from the following options:

	• *Execute* • *Expect* • *Expect Prompt*
Command	Commands to execute on the password changer. Valid variables are: • `$USER` • `$PASSWORD` • `$PASSPHRASE` • `$NEWPASSWD` • `$NEW_PUB_KEY` • `$NEW_PRI_KEY` • `$[0].$` • `$PUB_KEY` **Note**: `$[0].$` could be used when an associated secret is used. In this case, `$[0].$USER` means the username of the associated secret. `$[0].$PASSWORD` means the password of the associated secret. Enter `$` to get the list of valid variables. **Note**: The option is only available when the *Type* is *Execute*.
Response	The prompted line in target server. Enter `$` to get the list of valid variables. **Note**: The option is only available when the *Type* is *Expect*.
Execute Action	Either select *Execute command unconditionally* or *Execute command on previous match*. **Note**: The option is only available when the *Type* is *Execute*.
Expect Action	From the dropdown, select from the following three options: • *Abort procedure on string not matched* • *Continue procedure on string not matched* • *Abort procedure on string matched* **Note**: The option is only available when the *Type* is *Expect* or *Expect Prompt*.
Interpretation:	Select the method to interpret the expect string. • *Plain*: Interpret the expect string as a plain command. • *Regex*: Interpret the expect string as a regular expression. For example, if the response is "`Current password:`", then all of "`Current`", "`password`", "`rent`" will succeed to match. **Note**: The option is only available when the *Type* is *Expect*.

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

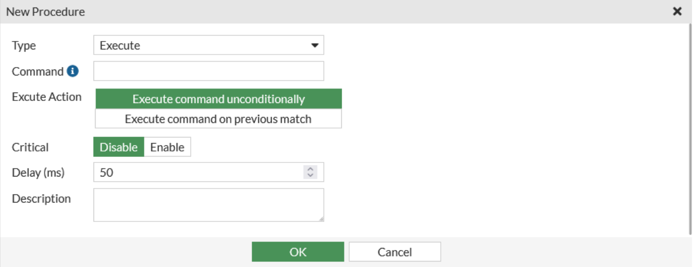
To reorder the changer sequence, drag from the sequence number and then drop.

3. Click *OK*.

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

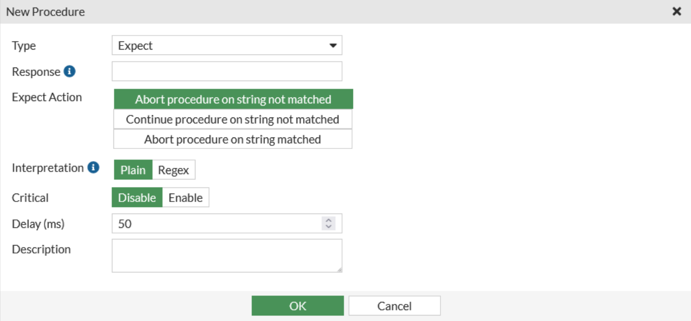
Verifiers

1. In step 4 when Creating a password changer, select *Create* in *Verifiers*.
   The *New Procedure* window opens. By default, the *Type* is *Execute*.

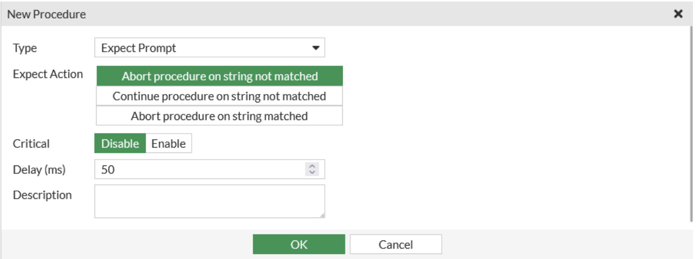


Type: Execute
Command:
Excute Action: [✓ Execute command unconditionally] Execute command on previous match
Critical: [✓ Disable] Enable
Delay (ms): 50
Description:

Different configuration options are available according to the *Type* selected.



Type: Expect
Response:
Expect Action: [✓ Abort procedure on string not matched] Continue procedure on string not matched Abort procedure on string matched
Interpretation: [✓ Plain] Regex
Critical: [✓ Disable] Enable
Delay (ms): 50
Description:



Type: Expect Prompt

Expect Action: Abort procedure on string not matched / Continue procedure on string not matched / Abort procedure on string matched

Critical: Disable Enable

Delay (ms): 50

Description

2. Enter the following information:

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

	• *Continue procedure on string not matched* • *Abort procedure on string matched* **Note**: The option is only available when the *Type* is *Expect* or *Expect Prompt*.
Critical	Enable to indicate that the step is critical. Password verification is successful when all steps before the critical step are passed. Steps after the critical step are optional, password verifier ignores the optional steps if they fail.
Delay	The maximum waiting time for the current action, in ms (default = 50, 50 - 20000).
Description	Optionally, enter a description.

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

3. Click *OK*.

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

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

See Automatic password changing on page 216 and Automatic password verification on page 217.

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* > *Secrets*.
   Alternatively, go to *Secrets* > *Personal Folder/Public Folder*, and select the folder where the secret is located.
2. Double-click the secret to edit it.
3. In the *Secret Setting* pane:
   a. Enable *Automatic Password Changing*.
   b. In *Start Time*, enter the date and time when the recurring schedule begins. Alternatively, select the *Calendar* icon and then select a date and time.
   c. In *Recurrence*, select from the following three frequencies of recurrence:
      i. *Daily*
      ii. *Weekly*
      iii. *Monthly*
   d. In *Repeat every*, enter the number of days/weeks/months after which the password is changed.

e. In *Occurs on*, select from the following days of the month when the password is automatically changed:

i. *First*

ii. *Second*

iii. *Third*

iv. *Last*

v. *Last Day*

vi. *Day*

When you select *Day*, select + to add days of the month when the password is automatically changed.

Select days of the week when the password is automatically changed.

Note: The *Occurs on* option is only available when *Recurrence* is set as *Weekly* or *Monthly*.

The automatic password changing schedule is displayed in *Recursive*.

4. Click *Save*.

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

Automatic password verification

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

To automatically verify the password:

1. Go to *Secrets* > *Secrets*.
   Alternatively, go to *Secrets* > *Personal Folder/Public Folder*, and select the folder where the secret is located.
2. Double-click the secret to edit it.
3. In the *Secret Setting* pane:

   a. Enable *Automatic Password Verification*.

   b. In *Interval (min)*, enter the time interval at which the password is verified.

   c. In *Start Time*, enter a date and time.
   Alternatively, select the calendar icon, and select a date and time.
4. Click *Save*.

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

Password policies

Using a secure password is vital to prevent unauthorized access. FortiPAM allows you to create password policy for secret passwords generated by the password changer. See Password changers on page 208.

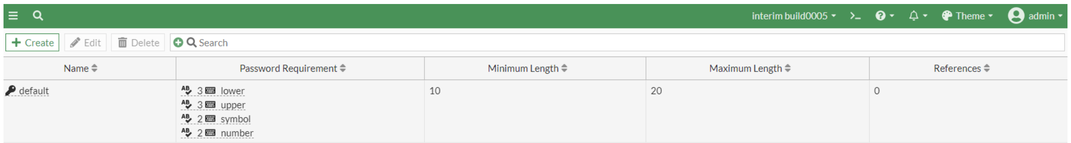
With password policies, you can enforce specific criteria for a new password, including:

- 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 220.

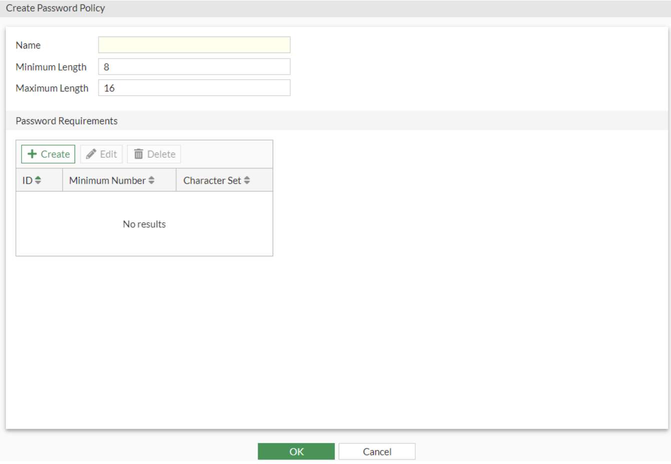
The *Password Policies* tab contains the following options:

Create	Select to create a new password policy. Password policies on page 217.
Edit	Select to edit the selected password policy.
Delete	Select to delete the selected password policies.
Search	Enter a search term in the search field, then hit `Enter` to search the password policies list. To narrow down your search, see Column filter.

Creating a password policy

To create a password policy:

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



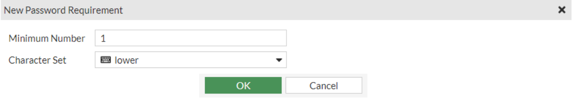
3. Enter the following information:

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

4. Click *OK*.

Password Requirements

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



2. Enter the following information:

Minimum Number	The minimum number of characters from the *Character Set* (default = 1).
Character Set	From the dropdown, select a character set or create a new character set (default = lower). See Creating a character set on page 221. 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 220.

Applying a password policy to a secret template

To apply a password policy to a secret template:

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

Default templates cannot be modified.

Administrators can clone a default template and then select a password policy.

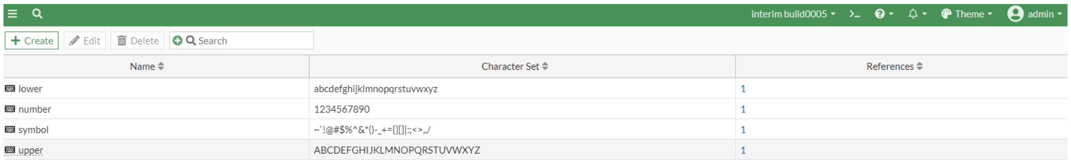
3. In the *Password Changer* pane, from the *Password Policy* dropdown, select a password policy or create a new password policy. See Creating a password policy on page 218 and Creating secret templates on page 165.
4. Click *Save*.

Character sets

A character set is a group of varied characters used in password policies. Character sets provide building blocks for passwords. See Password policies on page 217.

Character Sets in *Secret Settings* 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:

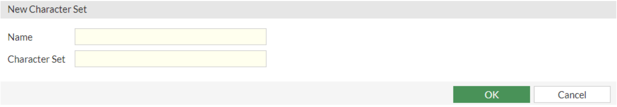
- *symbol*: contains some special characters.
- *number*: contains all numbers.
- *lower*: contains all lowercase English letters.
- *upper*: contains all uppercase English letters.

The *Character Sets* tab contains the following options:

Create	Select to create a new character set. See Creating a character set on page 221.
Edit	Select to edit the selected character set.
Delete	Select to delete the selected character sets.
Search	Enter a search term in the search field, then hit `Enter` to search the character sets list. To narrow down your search, see Column filter.

Creating a character set

To create a character set:

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

3. Enter the following information:

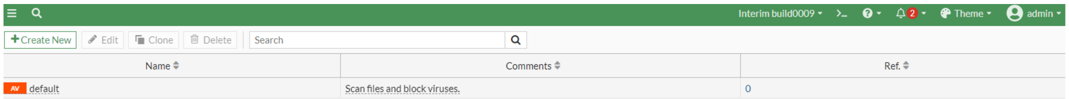
Name	The name of the character set.
Character Set	The character set.

4. Click *OK*.

AntiVirus

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

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



Name	Comments	Ref.
AV 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 224.

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.

In the FortiPAM CLI console, use the following command to enable FortiSandbox:

```
config system fortisandbox
 set status enable
 set email <string> #notifier email address
end
```

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.

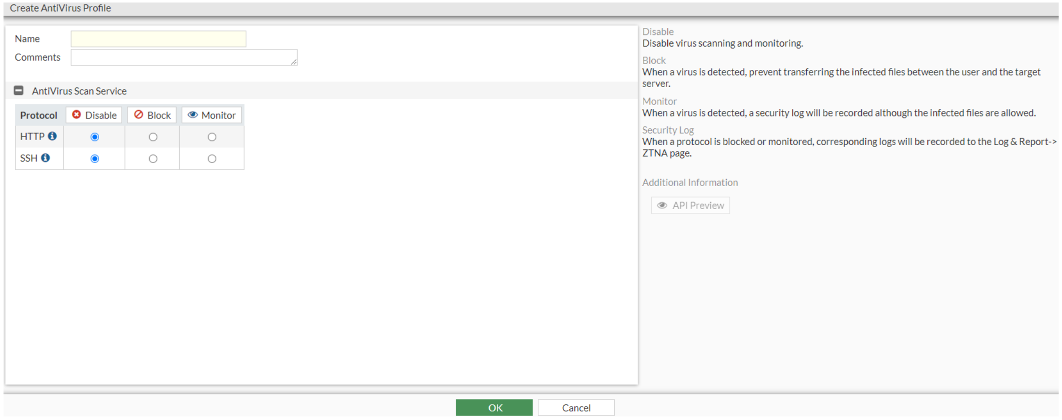
The *AntiVirus* tab contains the following options:

Create New	Select to create a new antivirus profile. See Creating an antivirus profile on page 222.
Edit	Select to edit the selected antivirus profile.
Clone	Select to clone the selected antivirus profile.
Delete	Select to delete the selected antivirus profiles.
Search	Enter a search term in the search field, then hit `Enter` to search the antivirus profile list.

Creating an antivirus profile

To create an antivirus profile:

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



Create AntiVirus Profile

Name

Comments

AntiVirus Scan Service

Protocol	Disable	Block	Monitor
HTTP	●	○	○
SSH	●	○	○

Disable
Disable virus scanning and monitoring.

Block
When a virus is detected, prevent transferring the infected files between the user and the target server.

Monitor
When a virus is detected, a security log will be recorded although the infected files are allowed.

Security Log
When a protocol is blocked or monitored, corresponding logs will be recorded to the Log & Report-> ZTNA page.

Additional Information

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
```

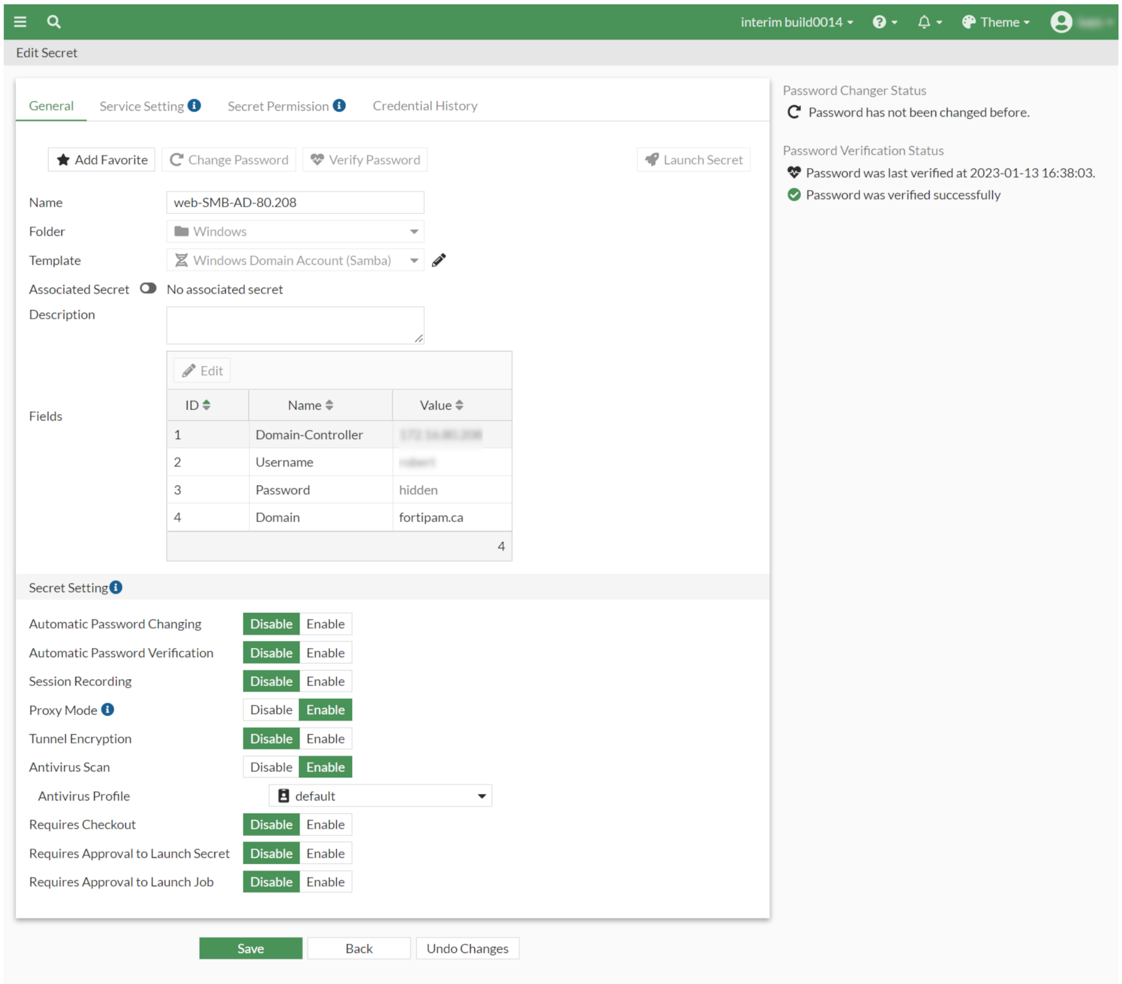
Enabling antivirus scan in a secret

To enable antivirus scan in a secret:

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

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

3. In the *Secret Setting* pane, enable *Antivirus Scan*.
4. From the *Antivirus Profile* dropdown, select an antivirus profile. See Creating an antivirus profile on page 222.
5. Click *Save*.



Password Changer Status
Password has not been changed before.

Password Verification Status
Password was last verified at 2023-01-13 16:38:03.
Password was verified successfully

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

Fields

ID	Name	Value
1	Domain-Controller	[redacted]
2	Username	[redacted]
3	Password	hidden
4	Domain	fortipam.ca

4

Secret Setting

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

Data loss prevention (DLP) protection for secrets

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

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

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

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

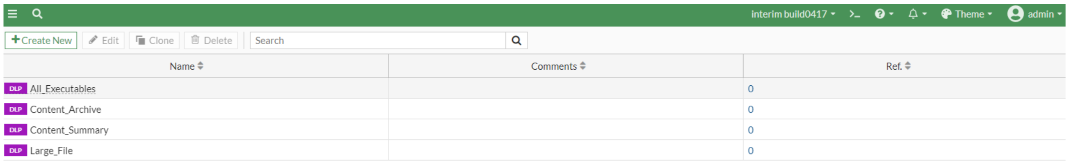
DLP is primarily used to stop sensitive data from leaving your network. DLP can also prevent unwanted data from entering your network and archive some or all of the content that passes through the FortiPAM. DLP archiving is configured per filter, which allows a single sensor to archive only the required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

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

- **File type and name**: A file type filter allows you to block, allow, log, or quarantine based on the file type specified in the file filter list. See Supported file types on page 230.
- **File size**: A file size filter checks for files that exceed the specific size and performs the DLP sensor's configured action on them.
- **Regular expression**: A regular expression filter filters files or messages based on the configured regular expression pattern.

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

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



Name	Comments	Ref.
DLP All_Executables		0
DLP Content_Archive		0
DLP Content_Summary		0
DLP Large_File		0

FortiPAM offers the following preconfigured DLP sensors:

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

You cannot delete the default DLP sensors.

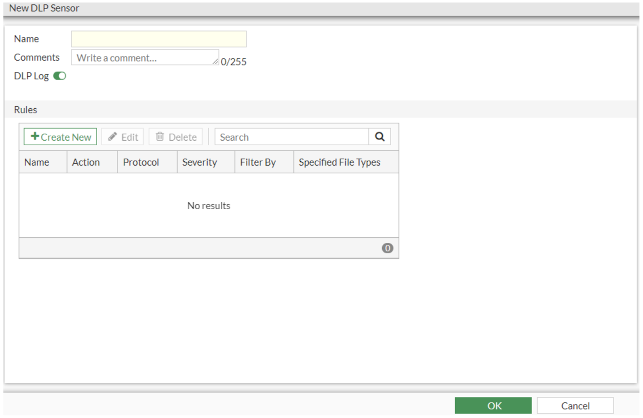
The *Data Leak Prevention* tab contains the following options:

Create New	Select to create a new DLP sensor. See Creating a DLP sensor on page 226.
Edit	Select to edit the selected DLP sensor.
Clone	Select to clone the selected DLP sensor.
Delete	Select to delete the selected DLP sensors.
Search	Search the DLP sensors list.

Creating a DLP sensor

To create a DLP sensor:

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



New DLP Sensor

Name

Comments Write a comment... 0/255

DLP Log

Rules

Name	Action	Protocol	Severity	Filter By	Specified File Types
No results					

3. Enter the following information:

Name	Name of the DLP sensor.
Comments	Optionally, enter a description for the DLP sensor.
DLP Log	Enable to generate a log entry when data matches the configured patterns. The option is enabled by default.
Rules	Create or edit DLP filter rules. See Creating DLP filter rules on page 227.

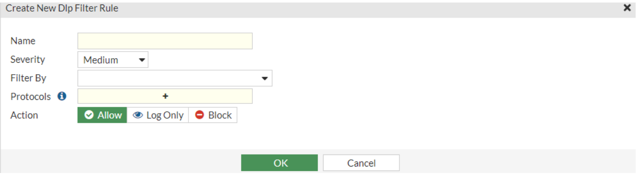
4. Click *OK*.

Creating DLP filter rules

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

To create a DLP filter rule:

1. In step 2 when Creating a DLP sensor on page 226, select *Create New* in *Rules*.
   The *Create New Dlp Filter Rule* window opens.



Create New Dlp Filter Rule

Name

Severity: Medium

Filter By

Protocols

Action: Allow

2. Enter the following information:

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

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

3. Click *OK*.

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

DLP via the CLI - Example

To configure a file type and name filter:

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

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

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

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

To configure a file size filtering:

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

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

To configure regular expression filtering:

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

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

Supported file types

The following file types are supported in DLP profiles:

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

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

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

*This file type is only available in DLP profiles.

DLP file pattern

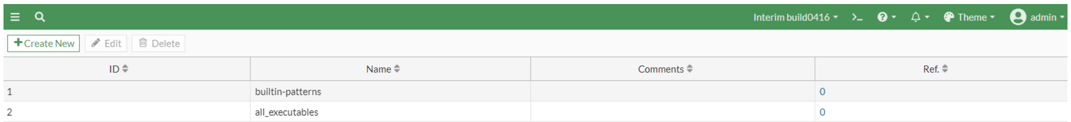
DLP file patterns match selected file types and file patterns. They are used as DLP filter rules in DLP sensors.

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

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

The *Ref.* column displays the number of times the object is referenced to other objects.

To view the location of the referenced object, select the number in *Ref.*; the *Object Usage* window opens and displays the various locations of the referenced object.



ID	Name	Comments	Ref.
1	builtin-patterns		0
2	all_executables		0

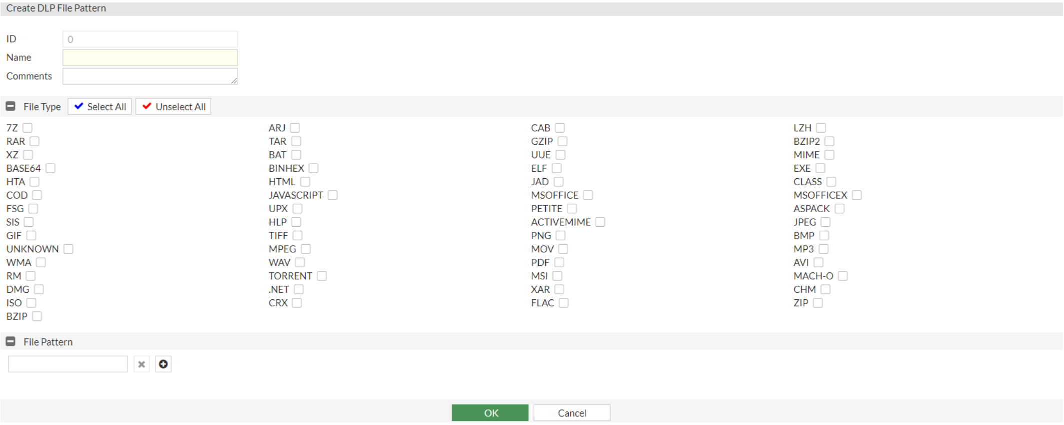
The *DLP File Pattern* tab contains the following options:

Create New	Create a DLP file pattern. See Creating a DLP file pattern on page 233.
Edit	Select to edit the selected DLP file pattern.
Delete	Select to delete the selected DLP file patterns.

Creating a DLP file pattern

To create a DLP file pattern:

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



ID 0

Name

Comments

7Z ☐
RAR ☐
XZ ☐
BASE64 ☐
HTA ☐
COD ☐
FSG ☐
SIS ☐
GIF ☐
UNKNOWN ☐
WMA ☐
RM ☐
DMG ☐
ISO ☐
BZIP ☐

ARJ ☐
TAR ☐
BAT ☐
BINHEX ☐
HTML ☐
JAVASCRIPT ☐
UPX ☐
HLP ☐
TIFF ☐
MPEG ☐
WAV ☐
TORRENT ☐
.NET ☐
CRX ☐

CAB ☐
GZIP ☐
UUE ☐
ELF ☐
JAD ☐
MSOFFICE ☐
PETITE ☐
ACTIVEMIME ☐
PNG ☐
MOV ☐
PDF ☐
MSI ☐
XAR ☐
FLAC ☐

LZH ☐
BZIP2 ☐
MIME ☐
EXE ☐
CLASS ☐
MSOFFICEX ☐
ASPACK ☐
JPEG ☐
BMP ☐
MP3 ☐
AVI ☐
MACH-O ☐
CHM ☐
ZIP ☐

3. Enter the following information:

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

4. Click *OK*.

SSH filter profiles

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

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

For each SSH profile; name, mode, shell commands, block channel, log activity, log all unlisted commands, and references are displayed by default.

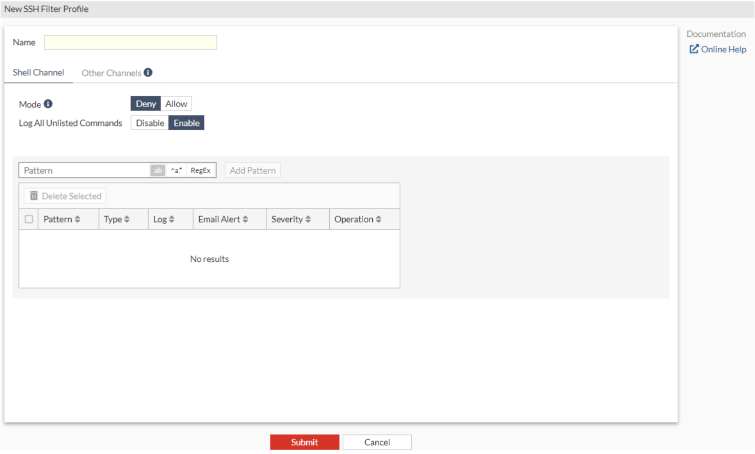
The *SSH Filter Profiles* tab contains the following options:

Create	Select to create a new SSH filter profile. See Creating an SSH filter on page 234.
Edit	Select to edit the selected SSH filter profile.
Delete	Select to delete the selected SSH filter profiles.
Search	Enter a search term in the search field, then hit `Enter` to search the SSH filter profiles list. To narrow down your search, see Column filter.

Creating an SSH filter

To create an SSH filter profile:

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



New SSH Filter Profile

Name

Mode [✓ Deny] Allow

Log All Unlisted Commands Disable [✓ Enable]

☐	Pattern	Type	Log	Email Alert	Severity	Operation

No results

3. Enter the following information:

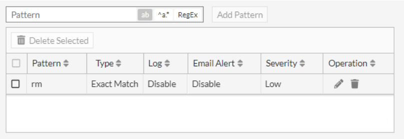
Name	Name of the SSH filter.
Shell Channel	
Mode	Select from the following two options: • *Deny*: The SSH command patterns configured in the SSH filter profile cannot be used. This means that these commands cannot be executed. • *Allow*: The SSH command patterns configured in the SSH filter profile can be used. This means that these commands can be executed while other commands will be blocked by FortiPAM.
Show Allowed List Command	Customize command that will list all the commands under allowlist anytime. **Note**: The option is only available when *Mode* is *Allow*.
Shortcut To Run Listed Commands	Shortcut to quickly run commands within the allowlist, the shortcut is the number within the list shown by *Show Allowed List Command* option (default = disable). **Note**: The option is only available when *Mode* is *Allow*.
Log All Unlisted Commands	Enable/disable logging all the unlisted commands (default = enable).
Shell commands can be created to block a command in the SSH terminal. See Adding a pattern.	
	Select shell commands from the list then select *Delete Selected* to delete the commands .
Other Channels Use this tab for advanced settings. **Note**: Settings in the tab require setting up a custom launcher.	
Block Channel	Select from the SSH blocking options (multiple options may be selected): • *X11*: X server forwarding • *SSH execution* • *Port forwarding* • *Tunnel forwarding* • *SFTP* • *SCP* • *Unknown channel*: Unknown channel (any channel other than the six listed here and the shell channel.)
Log Activity	SSH logging options. These are log activities related to selected channels regardless of the blocking status (multiple options may be selected): • *X11*: X server forwarding • *SSH execution* • *Port forwarding*

- *Tunnel forwarding*
- *SFTP*
- *SCP*
- *Unknown channel*

4. Click *Submit*.

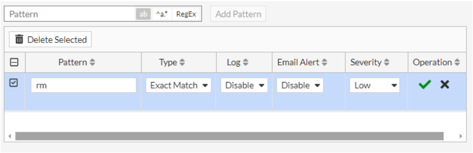
To add a pattern:

1. When editing an SSH filter profile, in the *New SSH Filter Profile* window:
   a. In the *Pattern* field, select from *Exact Match*, *Start with single word*, or *Use Regular Expression*.
   b. Enter a pattern.
   c. Click *Add Pattern*.
      The pattern is added to the list.



☐	Pattern	Type	Log	Email Alert	Severity	Operation
☐	rm	Exact Match	Disable	Disable	Low	

   d. From the pattern list, select the pen icon to edit the pattern.



⊟	Pattern	Type	Log	Email Alert	Severity	Operation
☑	rm	Exact Match ▾	Disable ▾	Disable ▾	Low ▾	✓ ✗

   e. You can edit the following options: *Type*, *Log*, *Email Alert*, and *Severity*.
      - *Type*:
        - *Start with*
        - *Regex*
        - *Exact Match*
   f. Click *Submit*.

Configuring SSH filter profile in the CLI console

To configure SSH filter profile in the CLI console:

1. In the CLI console, enter the following commands to set up an SSH filter in the *Deny* mode:

```
config ssh-filter profile
 edit "deny_prf"
  set restricted-mode disable # deny mode
  config shell-commands
   edit 1
    set pattern "rm"
    set log enable
    set alert enable
   next
   edit 2
    set pattern "ping 8.8.8.8"
    set exact-match enable
```

```
        set log enable
        set alert enable
        set severity critical
      next
     end
    next
   end
```

2. In the CLI console, enter the following commands to set up an SSH filter in the *Allow* mode:

```
    config ssh-filter profile
     edit "allow_prf"
      set restricted-mode enable # allow mode
      set shortcut-input enable
      config shell-commands
       edit 1
        set pattern "whoami"
        set exact-match enable
        set log enable
        set alert enable
        set severity low
       next
       edit 2
        set pattern "ls"
        set log enable
        set severity low
       next
       edit 3
        set pattern "ifconfig virbr0"
        set exact-match enable
        set log enable
        set severity low
       next
      end
    next
   end
```

If you are upgrading from FortiPAM 1.3.0 or below where the SSH filter profile is set with `Action = Allow`, entries are not shown in the new pattern table.

These entries will not block other commands; however, the new *Allow* mode does block other commands.

All the entries (including the old entries) can be viewed using the following CLI command:

```
 config ssh-filter profile
```

In the CLI console, you can still configure `Action = Allow` for some SSH shell patterns to log command activities, but this does not block other commands.

```
 config ssh-filter profile
  edit "ssh_block_allow"
   set block x11 exec port-forward tun-forward sftp unknown
   unset log
   set restricted-mode disable # Deny Mode default
   set default-command-log disable
   config shell-commands
    edit 1
     set type simple
     set pattern "ps"
     set exact-match disable
     set action allow #allow pattern 'ps'
     set log enable   #enable log this ssh pattern activities
     set alert enable #enable email alert this ssh pattern activities
     set severity critical
    next
   end
  next
 end
```

Adding SSH filter to secret

To add SSH filter to a secret:

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

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

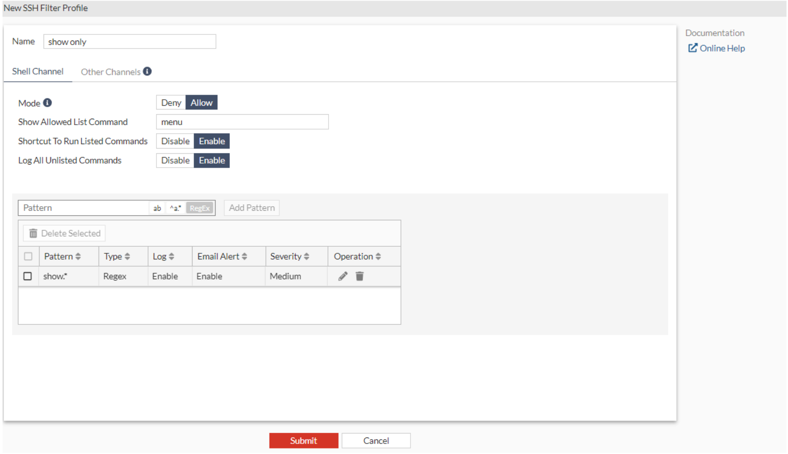
3. In *Service Setting* tab, ensure that *SSH Service* is enabled.
4. Enable *SSH Filter* and then select an SSH filter profile from the *SSH Filter Profile* dropdown.
5. Click *Save*.

Example SSH filter profiles - example

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

1. Go to *Secret Settings* > *SSH Filter Profiles*.
2. In *SSH Filter Profiles*, select *Create*.
   The *New SSH Filter Profile* window opens.
3. Enter a name for the SSH filter profile. In this example, the SSH filter profile is named `show only`.
4. In *Mode*, select *Allow*.
5. Leave *Show Allowed List Command* in the default state, i.e., `menu`.
6. Enable *Shortcut To Run Listed Commands*.
7. Enable *Log All Unlisted Commands*.
8. Add a pattern:
   a. In the *Pattern* field, select *RegEx*, and enter `show.*`.
   b. Select *Add Pattern*.
   c. Click the pen icon to edit the pattern, and:
      i. Enable *Log*.
      ii. Enable *Email Alert*.
      iii. Set *Severity* to *Medium*.
      iv. Select the green check mark.

9. Click *Submit*.



Name: show only

Mode: Deny [✓ Allow]

Show Allowed List Command: menu

Shortcut To Run Listed Commands: Disable [✓ Enable]

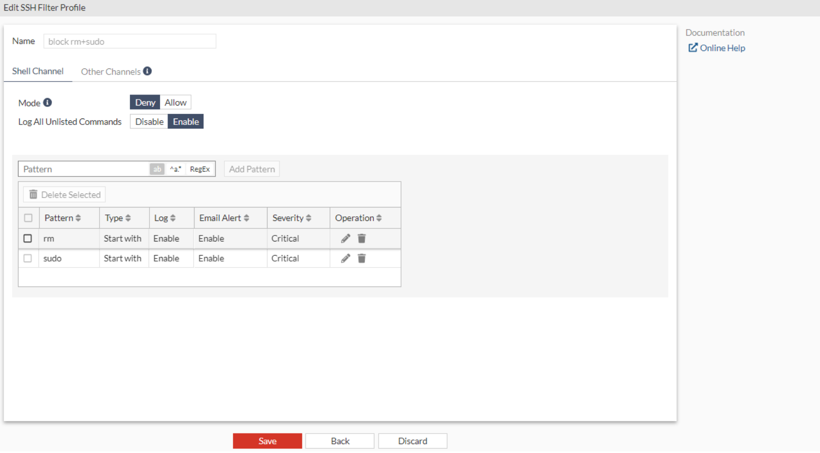
Log All Unlisted Commands: Disable [✓ Enable]

□	Pattern	Type	Log	Email Alert	Severity	Operation
□	show.*	Regex	Enable	Enable	Medium	✎ 🗑

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

1. Go to *Secret Settings* > *SSH Filter Profiles*.
2. In *SSH Filter Profiles*, select *Create*.
   The *New SSH Filter Profile* window opens.
3. Enter a name for the SSH filter profile. In this example, the SSH filter profile is named `block rm+sudo`.
4. Enable *Log All Unlisted Commands*.
5. Add a pattern:
   a. In the *Pattern* field, select *Start with single word*, and enter `rm`.
   b. Select *Add Pattern*.
6. Add another pattern:
   a. In the *Pattern* field, select select *Start with single word*, and enter `sudo`.
   b. Select *Add Pattern*.
7. Click the pen icon to edit the patterns, and:
   a. Enable *Log*.
   b. Enable *Email Alert*.
   c. Set *Severity* to *Critical*.
   d. Select the green check mark.
8. Follow step 7 to edit the other pattern.

9. Click *Submit*.



Edit SSH Filter Profile

Name: block rm+sudo

Mode: Deny | Allow

Log All Unlisted Commands: Disable | Enable

□	Pattern	Type	Log	Email Alert	Severity	Operation
□	rm	Start with	Enable	Enable	Critical	
□	sudo	Start with	Enable	Enable	Critical	

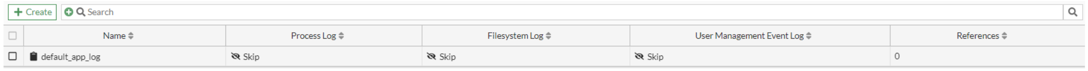
Event filter profile

The *Event Filter Profile* tab in *Secret Settings* displays a list of event filter profiles.

Using event filter profiles, FortiPAM can retrieve specific logs for events that occurred during an RDP session from a target.

The feature is agentless and relies on FortiPAM configuration, the WinRM service status, and the window audit policy on the target remote machine.

For each event filter profile; name, process log, file system log, user management event log, and references are displayed.



□	Name	Process Log	Filesystem Log	User Management Event Log	References
□	default_app_log	Skip	Skip	Skip	0

A default *default_app_log* event filter profile is available.

The *Event Filter Profile* tab contains the following options:

Create	Select to create a new event filter profile. See Creating an event filter profile on page 241.
Edit	Select to edit the selected event filter profile.
Delete	Select to delete the selected event filter profiles.
Search	Enter a search term in the search field, then hit `Enter` to search the event filter profiles list. To narrow down your search, see Column filter.

Creating an event filter profile

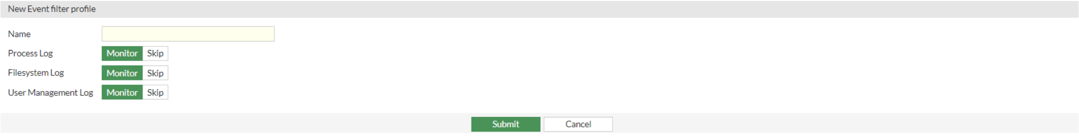
A secret event filter profile defines event categories pulled from the remote Windows server. Currently, users can monitor the following categories:

- Process related events, such as starting an application or terminating an existing application
- File system related events such as creating, accessing, and deleting a file
- User management related events such as creating a user.

Setting up an event filter profile requires that the server has enabled WinRM service and related audit policies, see Appendix L: WinRM configuration for Windows server on page 519.

To create an event filter profile:

1. Go to *Secret Settings* > *Event Filter Profile*.
2. In *Event Filter Profile*, select *Create*.
   The *New Event filter profile* window opens.



New Event filter profile

Name

Process Log: Monitor | Skip

Filesystem Log: Monitor | Skip

User Management Log: Monitor | Skip

3. Enter the following information:

Name	Name of the event filter profile.
Process Log	Monitor/skip the process log (default = *Monitor*).
Filesystem Log	Monitor/skip the file system event log (default = *Monitor*).
User Management Log	Monitor/skip the user management event log (default = *Monitor*).

4. Click *Submit*.

Event filter profile via the CLI - Example

1. In the CLI console, use the following commands to configure the event filter profile:

```
config secret event-filter-profile
 edit "default_app_log"
  set process-log {enable | disable}  #Enable/disable pulling activity log
  set filesystem-log {enable | disable}  #Enable/disable pulling activity log
  set user-management {enable | disable}  #Enable/disable pulling activity log
 next
end
```

2. In the CLI console, use the following commands to enable or disable the event filter for the policy or secret.

```
config secret policy
 edit default
  set event-filter {not-set | disable | enable}
  set event-filter-profile "default_app_log"
```

```
    end
   end
  config secret database
   edit sec_1
    set event-filter {not-set | disable | enable}
    set event-filter-profile "default_app_log"
   end
  end
```

3. The launched secret requires a target with a privileged account with WinRM (Windows remote management) privilege.
   Enable or disable `winrm-https` in the secret target using the following CLI commands:

   ```
   config secret target
    edit "3-84-141-197"
     set class "Other"
     set template "Windows Domain Account"
     set address "ec2-3-84-141-197.compute-1.amazonaws.com"
     set creation-time 2023-10-12 11:28:57
     set winrm-https {enable | disable} #Enable
     set access customized
     config user-permission
      edit 1
       set user-name "admin"
       set permission owner
      next
     end
     set web-proxy-status disable
    next
   end
   ```

   For information on WinRM configuration for Windows server, see Appendix L: WinRM configuration for Windows server on page 519.

Limitations

The RDP log retrieving feature currently only works on RDP sessions proxied by FortiPAM with video recording enabled.

Window app filter

The Windows Application Filter is a powerful security feature designed for Windows servers, providing administrators with the ability to control and restrict the installation and execution of applications and scripts.

This feature is essential for maintaining a secure and stable server environment by preventing unauthorized software from running.

Go to *Secret Settings* > *Windows App Filter Profiles* to see a list of Windows app filter profiles.

The following columns are displayed by default:

- *Name*
- *Filters Total Count*
- *Reference*

The *Windows App Filter Profiles* tab contains the following options:

Create	Select to create a new secret. See Creating a Windows app filter profile on page 244.
Search	Enter a search term in the search field, then hit `Enter` to search the Windows app filter profiles list. To narrow down your search, see Column filter.
Edit	Select to edit the selected Web app filter profiles.
Delete	Select to delete the selected Web app filter profiles.

Key features

1. Executable, script, and installer control:
   - Three types of pattern are supported in Windows app filter. Each profile filter stands for a particular deny pattern for certain types.
     - *Executable*: Executable files such as `.exe`, `.com`, and any portable executable files.
     - *Script*: Scripts such as `.ps1`, `.bat`, `.cmd`, `.vbs`, and `.js`.
     - *Installer*: Windows installer files such as `.msi`, `.mst`, and `.msp`.
2. Directory based restrictions:
   - Comprehensive coverage: Block any executable, script, or installer from designated directories.
   - Exceptions management: Add exceptions to allow specific applications or scripts to run, providing necessary flexibility.
3. Profile based management:
   a. Custom Profiles: Administrators can create and manage Windows app filter profiles tailored to specific needs.
   b. Secret-Based Application: Apply different profiles to different secrets.

Benefits of using Windows App Filter

1. Enhanced security: Prevents unauthorized and potentially harmful software from running on your server.
2. Policy flexibility: Allows for detailed and flexible control over which applications, scripts, and installers can be executed, tailored to your organization's specific needs.
3. Simplified management: Integrates with FortiPAM for easy management.
4. Reduced risk: Minimizes the attack surface by controlling the execution of applications and scripts, reducing the risk of security breaches.

Limitations

The Windows application filter has the following limitations:

1. If the secret template requires a domain and the combined length of the domain and user name exceeds 96 characters, the feature may not function properly.

Workaround: No workaround. Keep the domain and the user name length under the limit.

2. If you enable Windows application filter and later decide to not use it, disabling the option in secret settings or deleting the secret does not remote the rules from the remote server. This means you are still restricted.

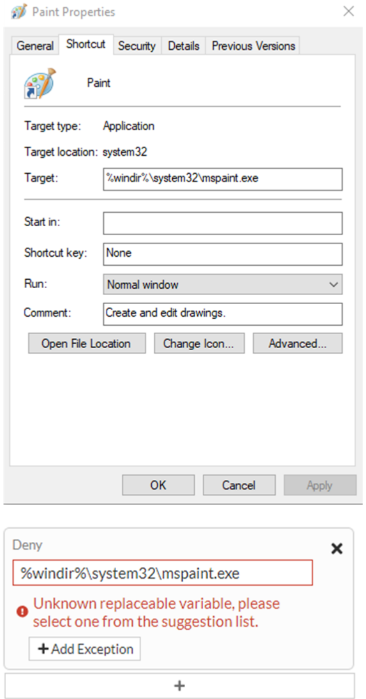
   Workaround 1: Create an empty Windows application filter profile without any filters and apply it to the secret. The rules are updated on the next launch.

   Workaround 2: Disable the Windows application filter for the secret, go to the target, select the *Windows Application Filters* tab, click *Delete FortiPAM Filters* in the *Advanced Settings* pane.

   See Creating a target on page 114.

   If **Workaround 2** is used, all profiles for the target are deleted. This impacts active sessions as they will have no filters and no restrictions till the next launch.

3. Occasionally, copying a specific path from the remote server to the FortiPAM Windows application filter fields results in error.



Target type: Application

Target location: system32

Target: %windir%\system32\mspaint.exe

Start in:

Shortcut key: None

Run: Normal window

Comment: Create and edit drawings.

%windir%\system32\mspaint.exe

Unknown replaceable variable, please select one from the suggestion list.

This occurs because the feature's regulation requires all the characters in the replaceable variables to be uppercase.

Workaround: You must manually convert the variable to uppercase.

Creating a Windows app filter profile

The Windows app filter profile interface is designed to help you control which applications and files users can run on Windows servers.

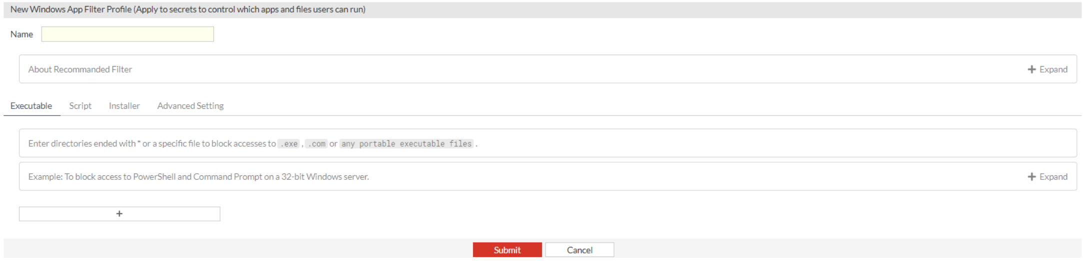
This interface allows for the creation and management of profiles that enforce security policies by restricting access to certain executables, scripts, and installers.

Prerequisites

1. The host server operates on Windows.
2. WinRM is enabled on the host server.
3. In FortiPAM, the host server is referred to as "target."
   The target has a privileged account for WinRM access on the host server.
4. All secrets whose server information is “Windows” under this target, except for the privileged account, can be used to enable the Windows application filter.

To create a Windows app filter profile:

1. Go to *Secret Settings* > *Windows App Filter Profiles*.
2. Select Create.
   The *New Windows App Filter Profile (Apply to secrets to control which apps and files users can run) window* opens.



New Windows App Filter Profile (Apply to secrets to control which apps and files users can run)

Name

About Recommanded Filter

Enter directories ended with * or a specific file to block accesses to `.exe` , `.com` or `any portable executable files` .

Example: To block access to PowerShell and Command Prompt on a 32-bit Windows server.

3. Enter the following information:

Name	The name of the Windows app filter profile. This helps identify and manage different profiles.
About Recommended Filter	Offers guidance on setting up filters, recommending the restriction of access exclusively to application storage and system files directories. The wildcard * blocks all interactions, with exceptions for `%PROGRAMFILES%\*` and `%WINDIR%\*` to permit access to Program Files and `C:\Windows` directories.

Executable

Enter directories ending in `*` or a specific file to block access to `.exe`, `.com`, or any portable executable file.

Deny (Recommend)

Pre-filled with the wildcard `*` to block all executable files.

Exceptions

List of directories where executable files are allowed ,e.g., `%PROGRAMFILES%\*`, `%WINDIR%\*`.

Add Exceptions

Use the *Add Exception* button to include additional paths where execution is permitted.

Deny

Define specific paths to block. Click *Add Exception* to permit specific directories or files within the blocked paths.

- Example

To block access to PowerShell and Command Prompt on a 32 bit Windows server, use:

Deny

```
C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe%SYSTEM32%\WindowsPowerShell\
v1.0\powershell_ise.exe%SYSTEM32%\cmd.exe
```

Script

Enter directories ending in `*` or a specific file to block access to `.ps1`, `.bat`, `.cmd`, `.vbs`, or `.js` files.

- *.ps1*: Powershell scripts
- *.bat*: Batch files
- *.cmd*: Command scripts
- *.vbs*: VBScript files
- *.js*: Javascript files

Using `*` at the end of a directory path ensures that all scripts within that directory are blocked.
Similar to *Executable*, you can set *Deny*.

Installer

Enter directories ending in `*` or a specific file to block accesses to `.msi` , `.msp`, or `.mst` files.

- *.msi*: Windows installer package
- *.msp*: Windows installer patch
- *.mst*: Windows installer transform

Deny (Recommend)

Pre-filled with the wildcard `*` to block all installer files.

Exceptions

List of directories where installer files are allowed ,e.g., `%PROGRAMFILES%\*`, `%WINDIR%\*`.

Add Exceptions

Use the *Add Exception* button to include additional paths where execution is permitted.

Deny

Define specific paths to block. Click *Add Exception* to permit specific directories or files within the blocked paths.

Advanced Settings

Offers the ability to control the refresh interval for profile checks and updates.

This guarantees that even in the absence of profile changes, FortiPAM continues to update the rule on the remote server, ensuring the rule remains current.

Consequently, multiple methods exist to initiate the rules update upon the launch of the secret session.

- The policy changes.
- The secret settings change.
- The target settings change.
- The Windows app filter profile changes.
- The refresh period is up.

Refresh Period	The time period at which the system checks and marks if the profile has been modified during each refresh period, in minutes (default = 30). When launching a secret with this profile, the filters are only updated if the profile is marked as modified.

4. Click *Submit*.

Integrity check

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

Client software integrity check requires FortiPAM 1.1 and FortiClient 7.2.2.

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

Using integrity check prevents launching of corrupt executables.

The following two types of integrity checks are available:

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

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

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

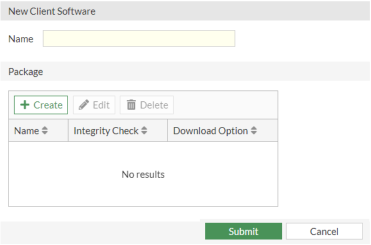
The *Integrity Check* tab contains the following options:

Create	Select to create a client software entry for integrity check. See Creating a client software entry for integrity check on page 248.
Edit	Select to edit the selected client software entry.
Delete	Select to delete the selected client software entries.
Search	Enter a search term in the search field, then hit `Enter` to search the client software entry list. To narrow down your search, see Column filter.

Creating a client software entry for integrity check

To create a client software entry for integrity check:

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



2. Enter the following information:

Name	The name of the client software entry.
Package Configure client software packages. See Creating client software packages on page 248.	

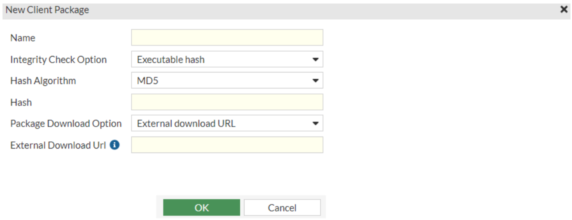
While creating a client software entry for integrity check, you can either store the software package locally, i.e., on the FortiPAM disk or provide an external URL to the package for downloading.

3. Click *Submit*.

Creating client software packages

To create a client software package

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



New Client Package

Name	
Integrity Check Option	Executable hash
Hash Algorithm	MD5
Hash	
Package Download Option	External download URL
External Download Url	

2. Enter the following information:

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

3. Click *OK*.

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

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

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

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

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

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

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

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

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

User management

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

- User list on page 251
- User groups on page 269
- Sponsored groups on page 275
- Role on page 278
- LDAP servers on page 290
- SAML Single Sign-On (SSO) on page 293
- RADIUS servers on page 301
- Auto provision rules on page 297
- Schedule on page 303
- FortiTokens on page 305

User list

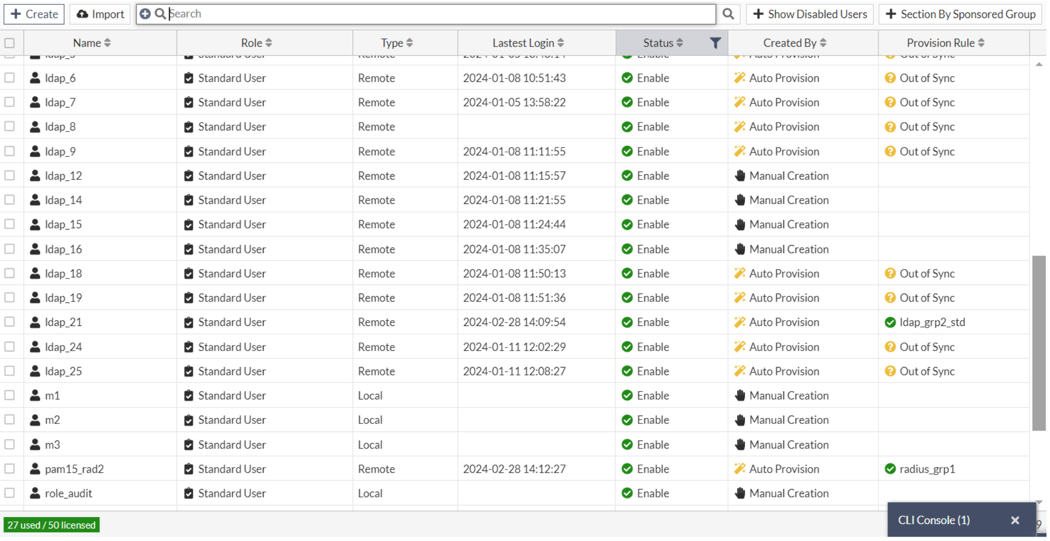
User List in *User Management* displays a list of FortiPAM users listed by their role types.

For each user, the following columns are displayed:

- *Name*
- *Sponsored Group*
- *Role*
- *Type*
- *Latest Login*
- *Status*
- *Two-factor Authentication*
- *References*
- *Created By*

By default, FortiPAM only lists enabled users.

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



□	Name	Role	Type	Lastest Login	Status	Created By	Provision Rule
□	ldap_6	Standard User	Remote	2024-01-08 10:51:43	✓ Enable	Auto Provision	? Out of Sync
□	ldap_7	Standard User	Remote	2024-01-05 13:58:22	✓ Enable	Auto Provision	? Out of Sync
□	ldap_8	Standard User	Remote		✓ Enable	Auto Provision	? Out of Sync
□	ldap_9	Standard User	Remote	2024-01-08 11:11:55	✓ Enable	Auto Provision	? Out of Sync
□	ldap_12	Standard User	Remote	2024-01-08 11:15:57	✓ Enable	Manual Creation	
□	ldap_14	Standard User	Remote	2024-01-08 11:21:55	✓ Enable	Manual Creation	
□	ldap_15	Standard User	Remote	2024-01-08 11:24:44	✓ Enable	Manual Creation	
□	ldap_16	Standard User	Remote	2024-01-08 11:35:07	✓ Enable	Manual Creation	
□	ldap_18	Standard User	Remote	2024-01-08 11:50:13	✓ Enable	Auto Provision	? Out of Sync
□	ldap_19	Standard User	Remote	2024-01-08 11:51:36	✓ Enable	Auto Provision	? Out of Sync
□	ldap_21	Standard User	Remote	2024-02-28 14:09:54	✓ Enable	Auto Provision	✓ ldap_grp2_std
□	ldap_24	Standard User	Remote	2024-01-11 12:02:29	✓ Enable	Auto Provision	? Out of Sync
□	ldap_25	Standard User	Remote	2024-01-11 12:08:27	✓ Enable	Auto Provision	? Out of Sync
□	m1	Standard User	Local		✓ Enable	Manual Creation	
□	m2	Standard User	Local		✓ Enable	Manual Creation	
□	m3	Standard User	Local		✓ Enable	Manual Creation	
□	pam15_rad2	Standard User	Remote	2024-02-28 14:12:27	✓ Enable	Auto Provision	✓ radius_grp1
□	role_audit	Standard User	Local		✓ Enable	Manual Creation	

27 used / 50 licensed

The user list contains the following options:

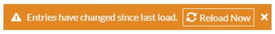
Create	Select to create a new user. See Creating a user on page 253.
Import	Select to import remote LDAP users from an LDAP server. See Importing LDAP users on page 266.
Edit	Select to edit the selected user account.
Disable	Select to disable the selected user account or accounts.
Delete	Select to delete the selected user account or accounts. See Deleting a user.
Search	Enter a search term in the search field, then hit `Enter` to search the user list. To narrow down your search, see Column filter.
Show/Hide Disabled Users	Select to show or hide disabled users.
Section By Sponsored Group/Default	Select to section the user list by sponsored groups or by default sections.

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

Out-of-sync users do not occupy license seats.

To enable/disable a user:

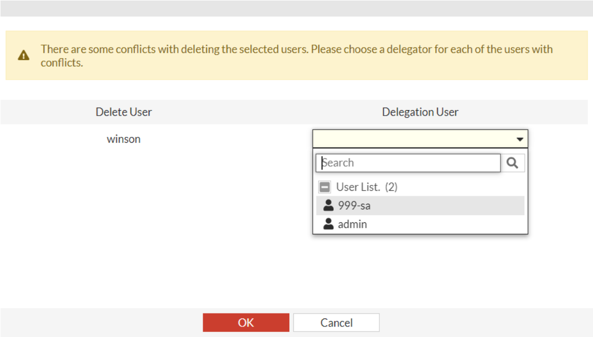
1. Right-click a user from the user list and then select *Enable/Disable* from *Set status*.
2. To refresh the user list, select *Reload Now* from the message that appears on the bottom-right.



Entries have changed since last load.

To delete a user:

1. Right-click a user from the user list and then select *Delete*.
   A user that does not solely own any public resource is deleted.
2. If the deleted user owns public resources, e.g., secrets, user groups, or folders, a delegation window appears.



There are some conflicts with deleting the selected users. Please choose a delegator for each of the users with conflicts.

Delete User	Delegation User
winson	

3. In the delegation window, from the *Delegation User* dropdown, select a user who will own the resources once the user owning the resource is deleted.
4. Click *OK*.

The deleted user's personal folder, personal subfolders, secrets, requests, and jobs are all removed on deletion.

Only public resources are delegated to the user selected in *Delegation User*.

Another user must be given ownership of a secret, template, target, or group, if the deleted user is the only owner for the resource (or the only member in a group).

Another user must be given ownership of the folder, if the deleted user is the only owner of the folder and secrets within the folder.

Approved and currently running secret jobs must be delegated to another user when the owner is deleted.

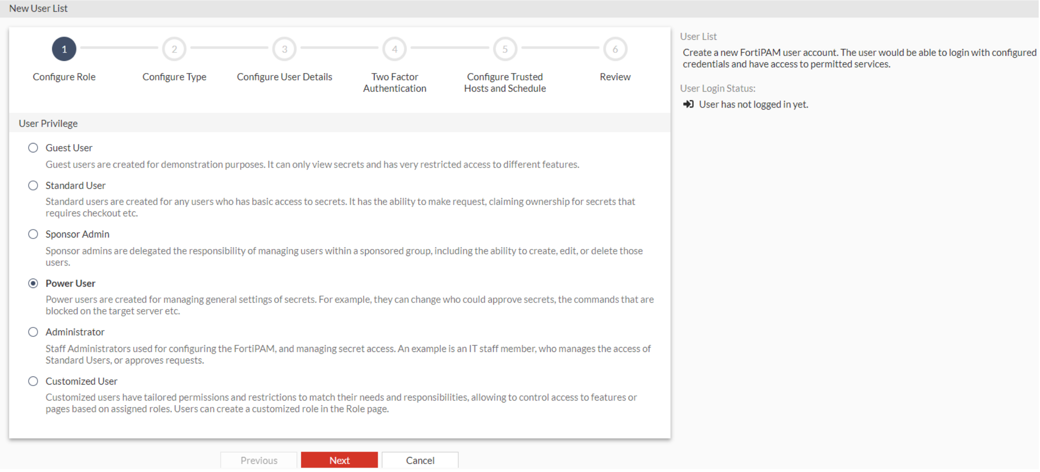
Creating a user

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 List*, and select *Create*
   The *New User List* wizard is launched.



User Privilege

○ 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.

○ Sponsor Admin
Sponsor admins are delegated the responsibility of managing users within a sponsored group, including the ability to create, edit, or delete those users.

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

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

○ Customized User
Customized users have tailored permissions and restrictions to match their needs and responsibilities, allowing to control access to features or pages based on assigned roles. Users can create a customized role in the Role page.

User List
Create a new FortiPAM user account. The user would be able to login with configured credentials and have access to permitted services.

User Login Status:
User has not logged in yet.

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

Configure Role	
User Privilege	Select from the following user role types: • *Guest User* • *Standard User* • *Sponsor Admin* • *Power User* • *Administrator* • *Customized User* For *Sponsor Admin*, select a sponsor admin role and a sponsored group. Sponsor admins can only manage users within their assigned sponsored group. For more information about sponsored groups, see Sponsored groups on page 275. For *Administrator*, select from one of the available administrator roles from the *Choose an Administrator Role* dropdown. For *Customized User*, select from one of the available custom roles from the *Choose a custom defined Role* dropdown. The sponsor admin/administrator/custom role decides what a sponsor admin, administrator, or customized user can see. Depending on the nature of the administrator work, access level, or seniority, you can allow them to view and configure as much or as little as required. Use the search bar to look for an administrator/custom role.

For information on the user types and their roles, see Users in FortiPAM on page 258 and Role on page 278.

Configure Type

User Type

Select a user type:

- *Local User*

  To change the local user password, see Admin on page 30.

- *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.

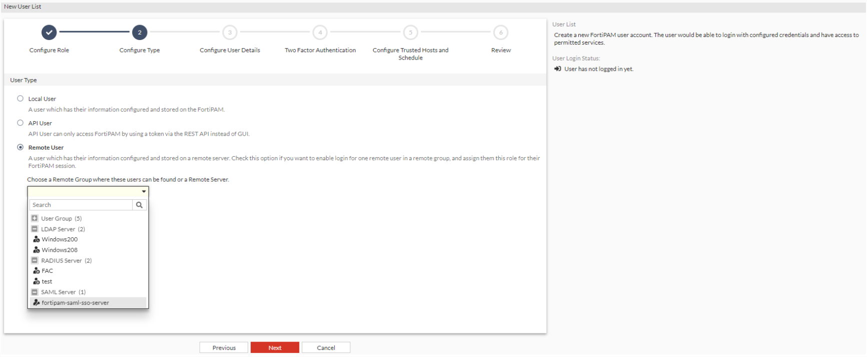
For *Remote User*, select a remote group where the user is found from the *Choose a Remote Group where these users can be found or a Remote Server* dropdown. See User groups on page 269.

Use the search bar to look for a remote group.

For information on the user types, see Users in FortiPAM on page 258.

Or

For *Remote User*, select a remote server where the user resides from the *Choose a Remote Group where these users can be found or a Remote Server* dropdown. See LDAP servers on page 290, SAML Single Sign-On (SSO) on page 293, and RADIUS servers on page 301.



New User List

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

User Type

○ 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.

Choose a Remote Group where these users can be found or a Remote Server.

User List

Create a new FortiPAM user account. The user would be able to login with configured credentials and have access to permitted services.

User Login Status:

User has not logged in yet.

Use the search bar to look for a remote server.

	In the *Choose a Remote Group where these users can be found or a Remote Server* dropdown, remote user groups and remote servers are mutually exclusive, i.e., only one can be selected.
Force SAML Login	Enable/disable forced SAML login (default = disable). **Note**: This option must be enabled when creating a SAML user.
Configure User Details	
Username	The username. Do not use `< > ( ) # " ' `` characters in the username.
Password	The password. **Note**: This option is only available when the user type is local.
Confirm Password	Enter the password again to confirm. **Note**: This option is only available when the user type is local.
Status	Enable/disable user login to FortiPAM. When you attempt to create a new user that exceeds the licensed seats, the *Status* option in the *Configure User Details* tab cannot be enabled. As you hover over the *Enable* button, a tooltip appears, alerting you that the user cannot be enabled as you have exceeded your license seat. **Note**: The option is not available when the user type is an API user.
Comments	Optionally, enter comments about the user.
Two Factor Authentication	
Email address	The email address. **Note**: This option is mandatory for all authentication types.
Critical System Email Alert	Enable/disable sending critical system alerts via email. **Note**: The option is disabled by default.
General Email Alert	Enable/disable sending general alerts via email. **Note**: The option is disabled by default.
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.

	Specify the type of user authentication used: • *FortiToken* • *FortiToken Cloud*: • *FortiToken Cloud License*: Displays the FortiToken Cloud license status. Use the *Activate free trial* option to activate free trial with 5 FortiToken Cloud tokens. The trial license is available for 30 days only. When in trial or when the license has expired, select *Upgrade* to see instructions on how to add a valid license. When the license has expired, you cannot use FortiToken Cloud. *FortiToken Cloud License* then displays *No active license* status. See 2FA with FortiToken Cloud example on page 259. • *Email* (default) SMS based two factor authentication is not supported in FortiPAM 1.4.2.
Token	From the dropdown, select a token. **Note**: The option is mandatory and only available when the *Authentication Type* is *FortiToken*.
Configure Trusted Hosts	
IPv4 Trusted Hosts	Trusted IPv4 addresses users use to connect to FortiPAM. Use + button to add a new IPv4 address and *x* to delete an added IPv4 address.
Configure the schedule for which the user can connect to the FortiPAM	Enable/disable configuring the login schedule for the users. From the dropdown, select a schedule. See Schedule on page 303. **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 List*.
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.
- *Sponsor Admin*: For managing users assigned to their sponsored group(s). This includes creating, editing, and deleting users assigned to their sponsored group(s). Sponsor admins can only access logs and reports for their specific users, groups, and secrets.

  The *Sponsor Admin* user has *View Secret Log* and *View Secret Video* permissions by default.

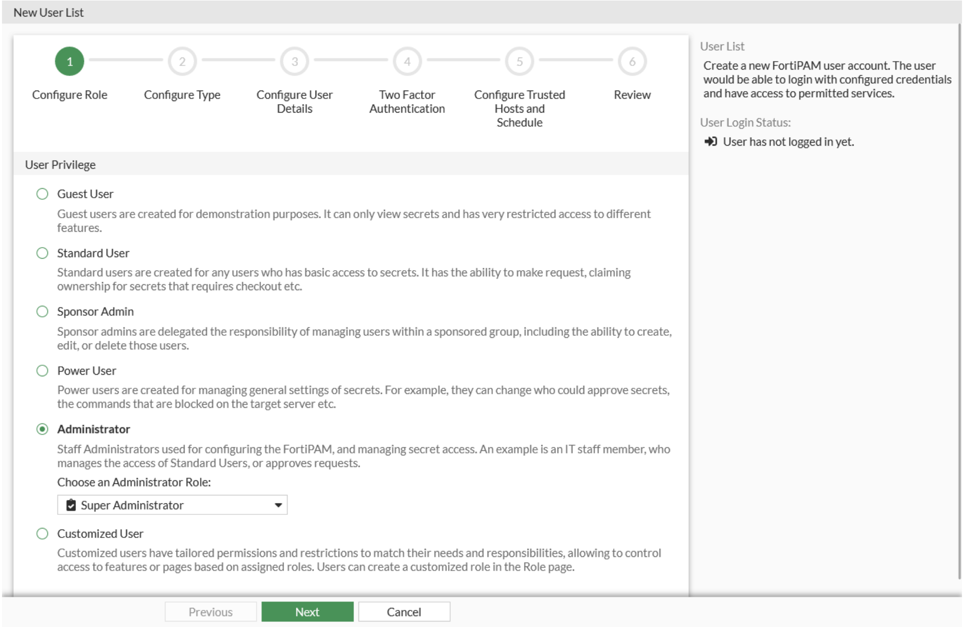
  For information on *View Secret Log* and *View Secret Video* permissions, see Role on page 278.
- *Power User*: For managing general secret settings, e.g., a power user can change who approves secrets, commands blocked on the target server, etc.
- *Administrator*: Staff administrators used for configuring 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 278.
- *Customized User*: Customized users have tailored permissions and restrictions to match their needs and responsibilities, allowing them to control access to features or pages based on assigned roles. You can create a customized role in Role.

  See Creating a user on page 253.

2FA with FortiToken Cloud - example

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

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



New User List

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

User Privilege

○ 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.

○ Sponsor Admin
Sponsor admins are delegated the responsibility of managing users within a sponsored group, including the ability to create, edit, or delete those users.

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

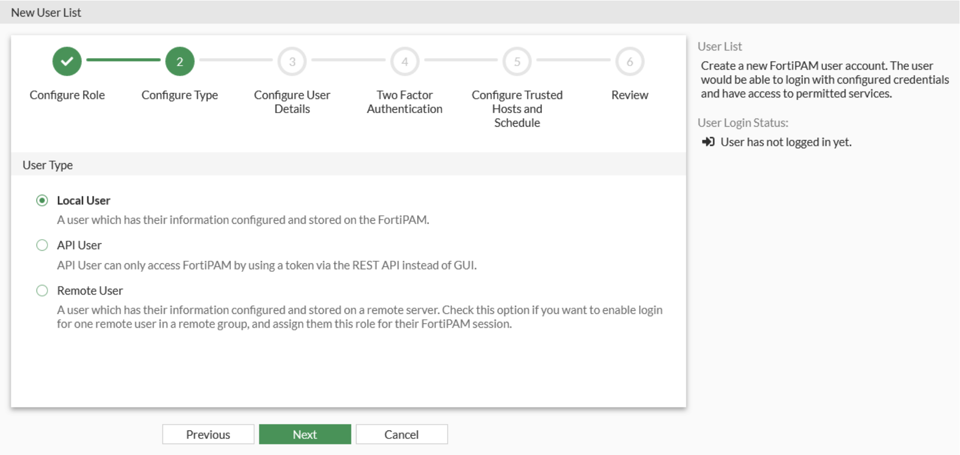
● Administrator
Staff Administrators used for configuring the FortiPAM, and managing secret access. An example is an IT staff member, who manages the access of Standard Users, or approves requests.
Choose an Administrator Role: Super Administrator

○ Customized User
Customized users have tailored permissions and restrictions to match their needs and responsibilities, allowing to control access to features or pages based on assigned roles. Users can create a customized role in the Role page.

User List
Create a new FortiPAM user account. The user would be able to login with configured credentials and have access to permitted services.

User Login Status:
User has not logged in yet.

3. Click *Next*.
4. In *Configure Type*, select either *Local User* or *Remote User*.
   In this example, *Local User* is selected.



New User List

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

User Type

● 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.

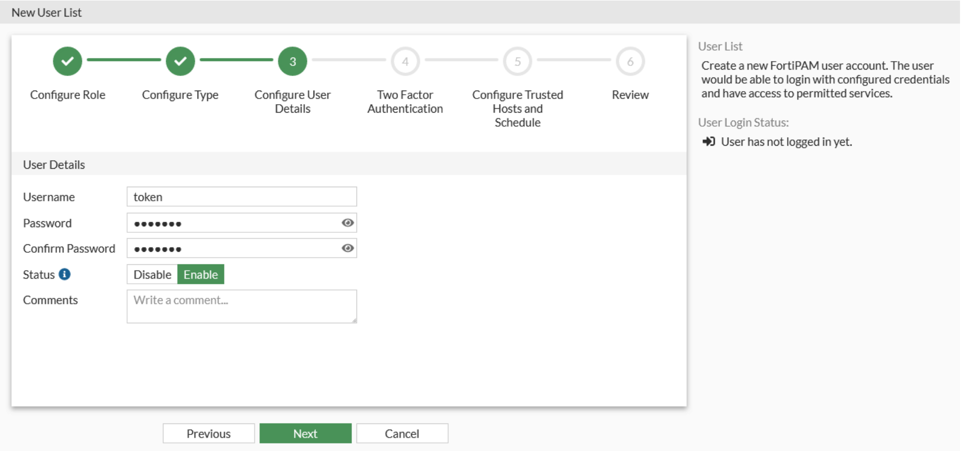
User List
Create a new FortiPAM user account. The user would be able to login with configured credentials and have access to permitted services.

User Login Status:
User has not logged in yet.

For *Remote User*, select a remote group where the user is found. See User groups on page 269.

5. Click *Next*.
6. In *Configure User Details*:
   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.



User List

Create a new FortiPAM user account. The user would be able to login with configured credentials and have access to permitted services.

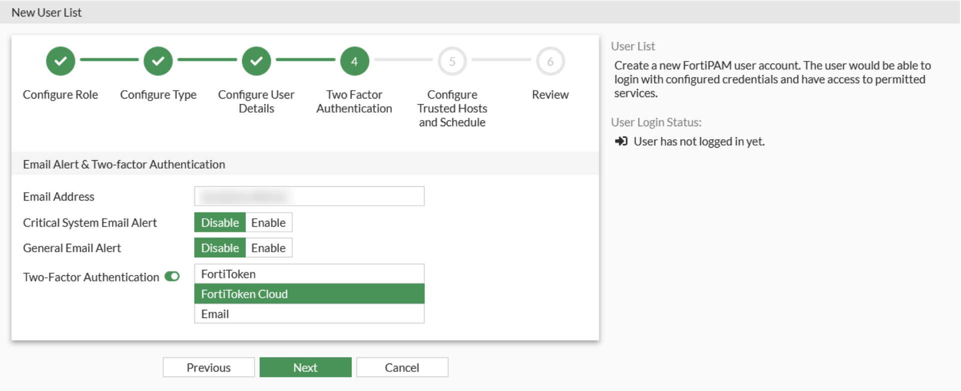
User Login Status:

User has not logged in yet.

User Details

Username	token
Password	•••••••
Confirm Password	•••••••
Status	Disable [✓ Enable]
Comments	Write a comment...

7. Click *Next*.
8. In *Two Factor Authentication*:
   a. In *Email address*, enter the user email address where the activation code for FortiToken Cloud is sent.
   b. Enable *Two-Factor Authentication*, and select *FortiToken Cloud*.



User List

Create a new FortiPAM user account. The user would be able to login with configured credentials and have access to permitted services.

User Login Status:

User has not logged in yet.

Email Alert & Two-factor Authentication

Email Address	[redacted]
Critical System Email Alert	[✓ Disable] Enable
General Email Alert	[✓ Disable] Enable
Two-Factor Authentication	● FortiToken [✓ FortiToken Cloud] Email

   c. Click *Next*.
9. Click *Next*.
10. In the *Review* tab, verify the information you entered and click *Submit* to create the user.
11. You will receive an email with the subject *Activation for FortiToken Cloud*, activate the token in your FortiToken Mobile application by scanning the QR code or manually input the activation code in the email.
12. From the user dropdown on the top-right, select *Logout*.
13. On the login screen, enter the username and password for the user you just created, and select *Continue*.
14. 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 type physical
      set snmp-index 1
   next
end
```

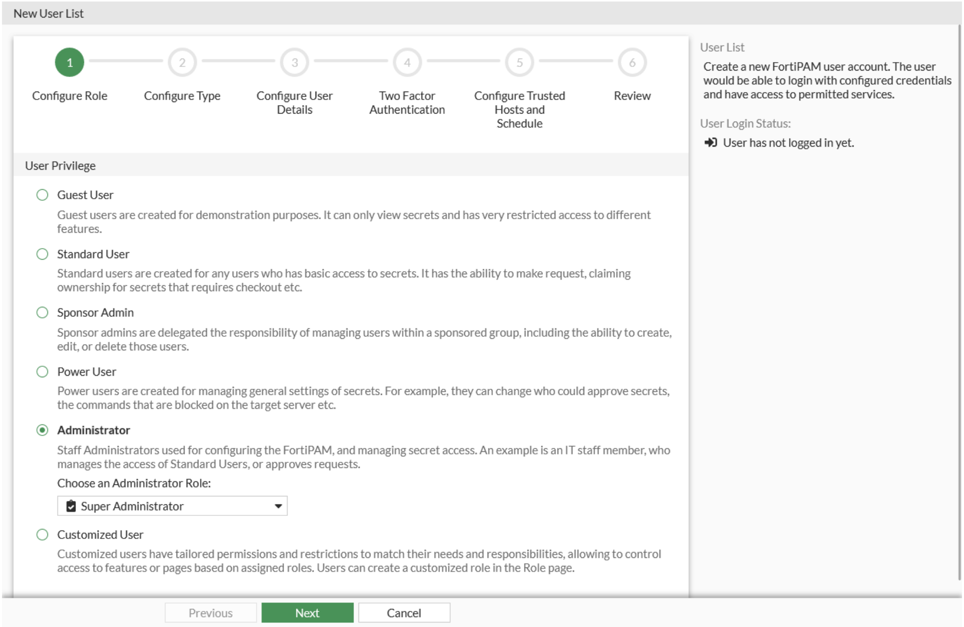
CLI configuration to set up a virtual IP address for FortiPAM - example:

```
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 List*, and select *Create*.
   The *New User List* wizard is launched.
2. In *Choose a User Role type*, select *Administrator*, and from the *Choose an Administrator Role* dropdown, select *Super Administrator*.



User Privilege

○ 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.

○ Sponsor Admin
Sponsor admins are delegated the responsibility of managing users within a sponsored group, including the ability to create, edit, or delete those users.

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

● Administrator
Staff Administrators used for configuring the FortiPAM, and managing secret access. An example is an IT staff member, who manages the access of Standard Users, or approves requests.
Choose an Administrator Role:
Super Administrator

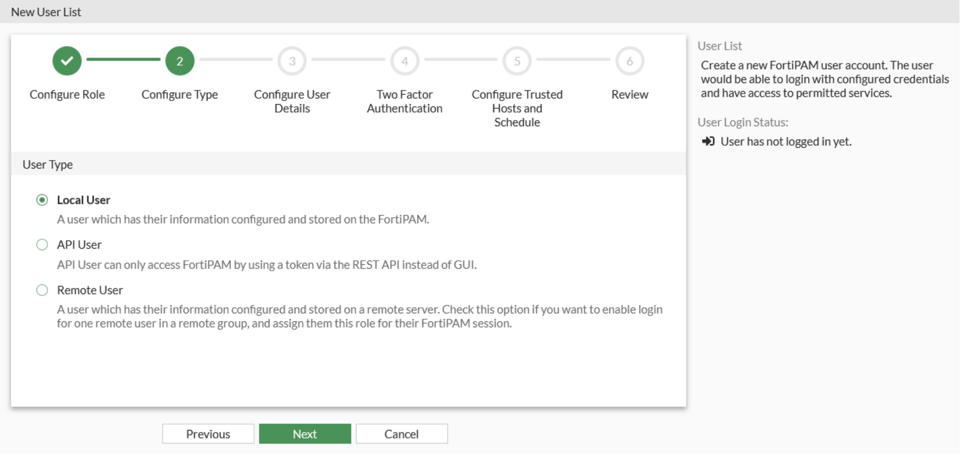
○ Customized User
Customized users have tailored permissions and restrictions to match their needs and responsibilities, allowing to control access to features or pages based on assigned roles. Users can create a customized role in the Role page.

User List
Create a new FortiPAM user account. The user would be able to login with configured credentials and have access to permitted services.

User Login Status:
User has not logged in yet.

3. Click *Next*.

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



User Type

● 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.

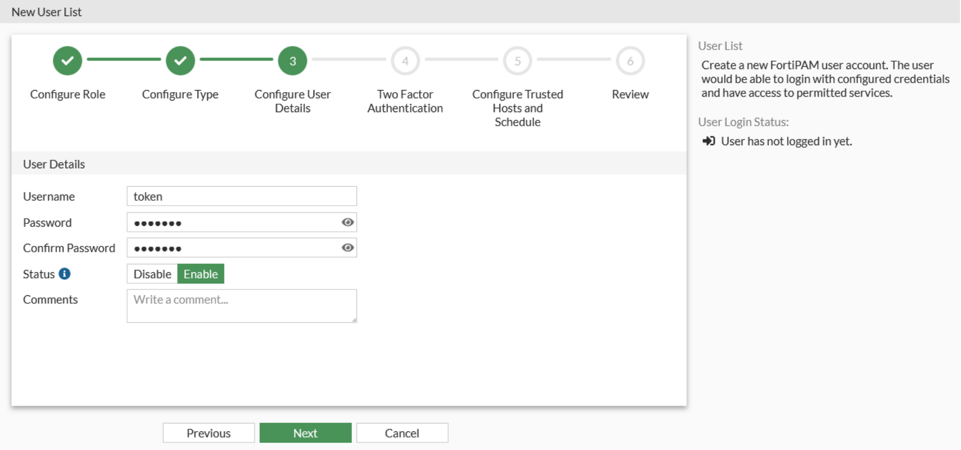
○ Remote User
A user which has their information configured and stored on a remote server. Check this option if you want to enable login for one remote user in a remote group, and assign them this role for their FortiPAM session.

User List
Create a new FortiPAM user account. The user would be able to login with configured credentials and have access to permitted services.

User Login Status:
User has not logged in yet.

For *Remote User*, select a remote group where the user is found. See User groups on page 269.

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.



User Details

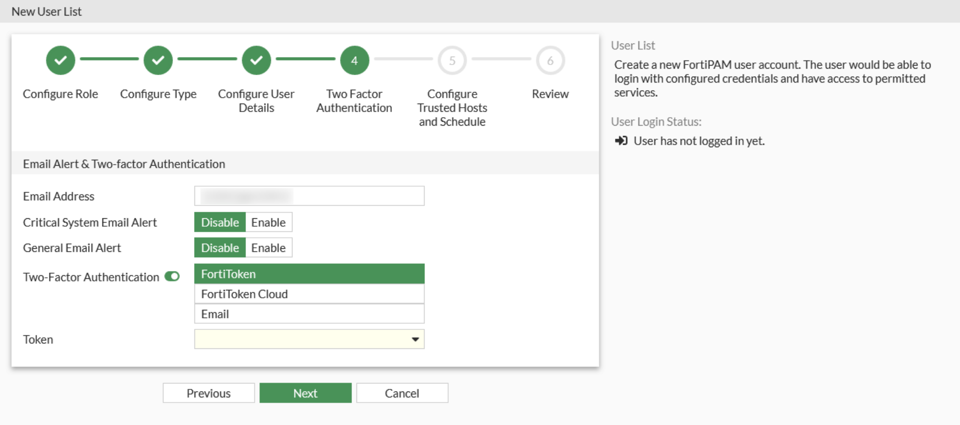
Username	token
Password	•••••••
Confirm Password	•••••••
Status	Disable [✓ Enable]
Comments	Write a comment...

User List
Create a new FortiPAM user account. The user would be able to login with configured credentials and have access to permitted services.

User Login Status:
User has not logged in yet.

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

c. From the *Token* dropdown, select a FortiToken.



User List

Create a new FortiPAM user account. The user would be able to login with configured credentials and have access to permitted services.

User Login Status:

User has not logged in yet.

Email Alert & Two-factor Authentication

Email Address	[redacted]
Critical System Email Alert	[✓ Disable] Enable
General Email Alert	[✓ Disable] Enable
Two-Factor Authentication ●	[✓ FortiToken] FortiToken Cloud Email
Token	

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 265.

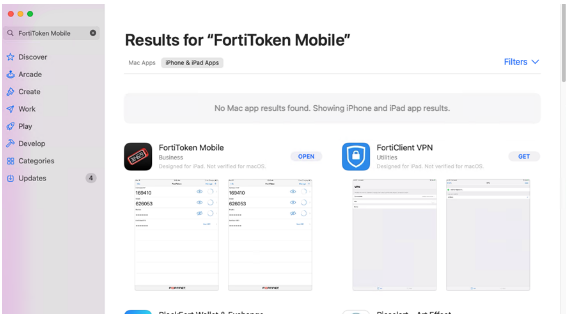
CLI configuration to set up a user with FortiToken as the authentication type - example:

```
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
```

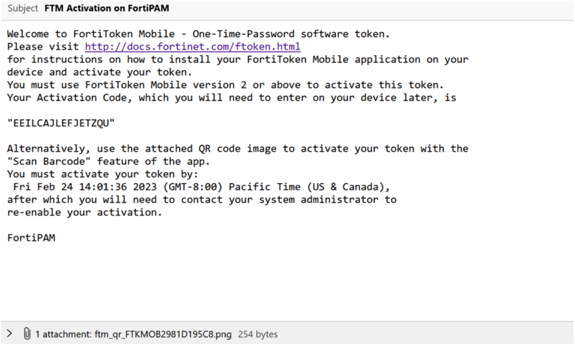
Setting up FortiToken Mobile

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*.

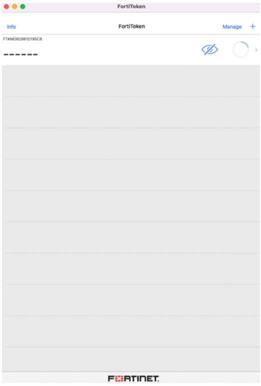


Subject **FTM Activation on FortiPAM**

```
Welcome to FortiToken Mobile - One-Time-Password software token.
Please visit http://docs.fortinet.com/ftoken.html
for instructions on how to install your FortiToken Mobile application on your
device and activate your token.
You must use FortiToken Mobile version 2 or above to activate this token.
Your Activation Code, which you will need to enter on your device later, is

"EEILCAJLEFJETZQU"

Alternatively, use the attached QR code image to activate your token with the
"Scan Barcode" feature of the app.
You must activate your token by:
 Fri Feb 24 14:01:36 2023 (GMT-8:00) Pacific Time (US & Canada),
after which you will need to contact your system administrator to
re-enable your activation.

FortiPAM
```

1 attachment: ftm_qr_FTKMOB2981D195C8.png 254 bytes

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

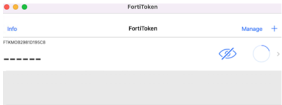


4. There are two ways to add a token to the FortiToken Mobile application:
   a. **Scan QR code**: If your device supports QR code recognition, select + in the FortiToken Mobile home screen and point your device camera at the QR code attached to the activation email.

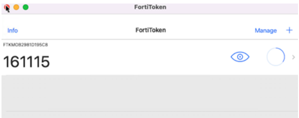
b. **Enter Manually**:
   i. Select + and then select *Enter Manually* from the bottom.
   ii. Select *Fortinet* and enter *Name* and *Key*.

> *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.

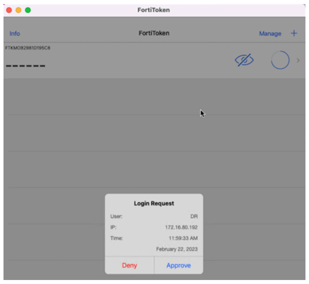
   iii. Click *Done*.
   FortiToken Mobile communicates with the secure provisioning server to activate your token. The token is now displayed in the token list view.



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*.



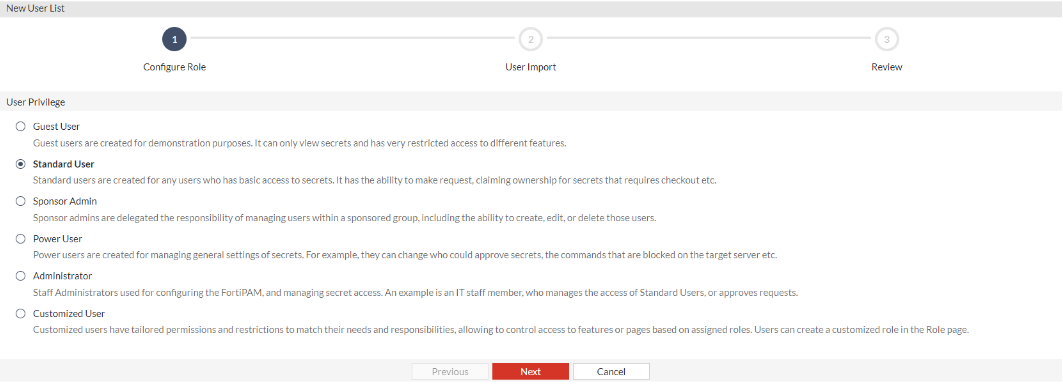
Login Request

User: DR
IP: 172.16.80.192
Time: 11:59:33 AM February 22, 2023

Importing LDAP users

To import LDAP users:

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


New User List

User Privilege

○ 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.

○ Sponsor Admin
Sponsor admins are delegated the responsibility of managing users within a sponsored group, including the ability to create, edit, or delete those users.

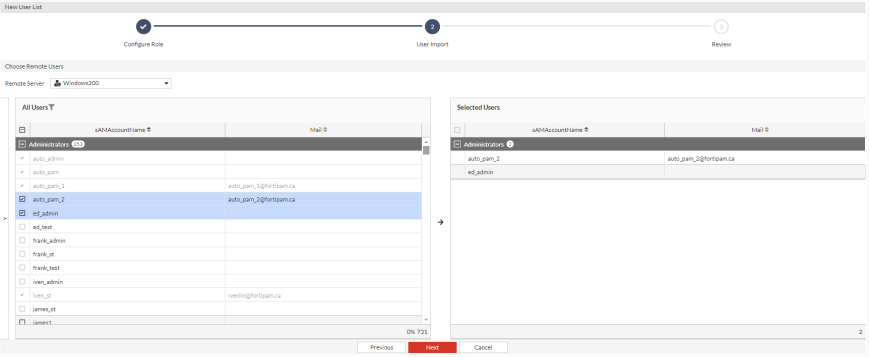
○ Power User
Power users are created for managing general settings of secrets. For example, they can change who could approve secrets, the commands that are blocked on the target server etc.

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

○ Customized User
Customized users have tailored permissions and restrictions to match their needs and responsibilities, allowing to control access to features or pages based on assigned roles. Users can create a customized role in the Role page.

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

Configure Role	
User Privilege	Select from the following user role type: • *Guest User* • *Standard User* • *Sponsor Admin* • *Power User* • *Administrator* • *Customized User* For *Sponsor Admin*, select a sponsor admin role and a sponsored group. Sponsor admins can only manage users within their assigned sponsored group. For more information about sponsored groups, see Sponsored groups on page 275. For *Administrator*, select from one of the available administrator roles from the *Choose an Administrator Role* dropdown. For *Customized User*, select from one of the available custom roles from the *Choose a custom defined Role* dropdown. Use the search bar to look for the following: • Sponsor admin role and group • Administrator role • Custom role For information on the user types and their roles, see Users in FortiPAM on page 258 and Role on page 278.
User Import	
Remote Server	From the dropdown, select a remote LDAP server. In the dropdown, select + to create a new remote LDAP server. See LDAP servers on page 290. Use the search bar to look for a remote LDAP server. Hover over a remote LDAP server name to see details about the remote LDAP server. Click > on the left to open *LDAP DB Structure* and choose a node.



Remote Server: Windows200

All Users

⊟	sAMAccountName	Mail
⊟	Administrators 253	
✓	auto_admin	
✓	auto_pam	
✓	auto_pam_1	auto_pam_1@fortipam.ca
☑	auto_pam_2	auto_pam_2@fortipam.ca
☑	ed_admin	
□	ed_test	
□	frank_admin	
□	frank_st	
□	frank_test	
□	iven_admin	
✓	iven_st	ivenlin@fortipam.ca
□	james_st	
□	james1	

0% 731

Selected Users

□	sAMAccountName	Mail
⊟	Administrators 2	
	auto_pam_2	auto_pam_2@fortipam.ca
	ed_admin	

2

By default, *LDAP DB Structure* is hidden.

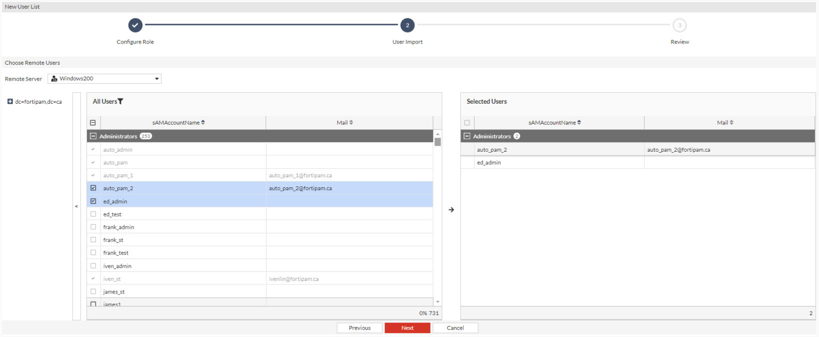
In the *All Users* table:

- All the users in the selected remote LDAP server show up.
- To select all the users, select the checkbox in the header.
- To only select some users, select the checkbox before the users.

To define a filter to match username or group, see Filters on page 34 in Tables on page 34.

For other column related settings, see Column settings on page 37 in Tables on page 34.

- Selected users from *All Users* are displayed in the *Selected Users* table.



Remote Server: Windows200

All Users

⊟	sAMAccountName	Mail
⊟	Administrators 253	
✓	auto_admin	
✓	auto_pam	
✓	auto_pam_1	auto_pam_1@fortipam.ca
☑	auto_pam_2	auto_pam_2@fortipam.ca
☑	ed_admin	
□	ed_test	
□	frank_admin	
□	frank_st	
□	frank_test	
□	iven_admin	
✓	iven_st	ivenlin@fortipam.ca
□	james_st	
□	james1	

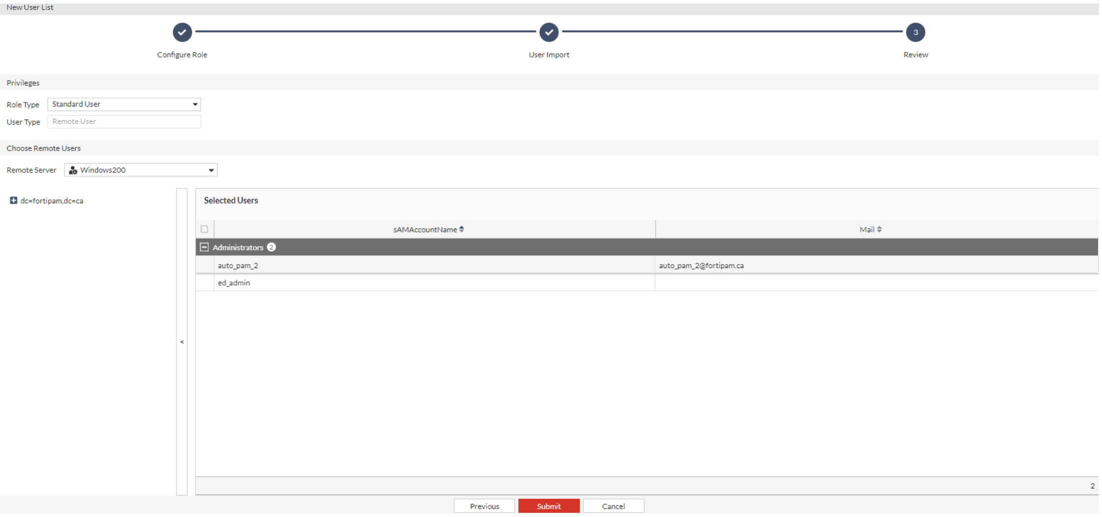
0% 731

Selected Users

□	sAMAccountName	Mail
⊟	Administrators 2	
	auto_pam_2	auto_pam_2@fortipam.ca
	ed_admin	

2

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



Role Type: Standard User

User Type: Remote User

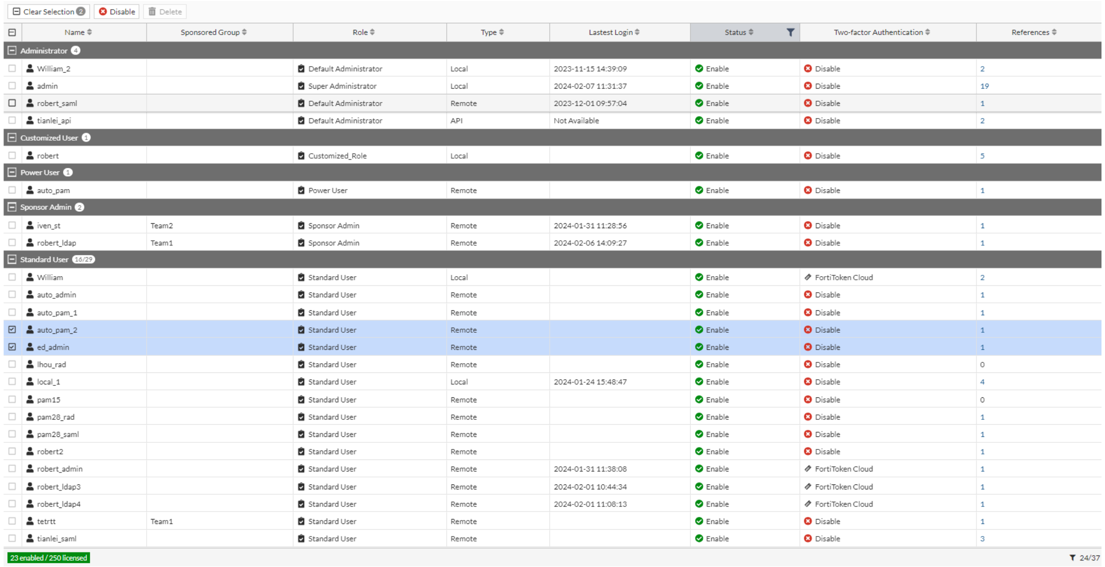
Remote Server: Windows200

dc=fortipam,dc=ca

□	sAMAccountName	Mail
Administrators 2		
	auto_pam_2	auto_pam_2@fortipam.ca
	ed_admin	

2

The imported users are listed in *User Management > User List*.



□	Name	Sponsored Group	Role	Type	Lastest Login	Status	Two-factor Authentication	References
Administrator 4								
□	William_2		Default Administrator	Local	2023-11-15 14:39:09	Enable	Disable	2
□	admin		Super Administrator	Local	2024-02-07 11:31:37	Enable	Disable	19
□	robert_saml		Default Administrator	Remote	2023-12-01 09:57:04	Enable	Disable	1
□	tianlei_api		Default Administrator	API	Not Available	Enable	Disable	2
Customized User 1								
□	robert		Customized_Role	Local		Enable	Disable	5
Power User 1								
□	auto_pam		Power User	Remote		Enable	Disable	1
Sponsor Admin 2								
□	iven_st	Team2	Sponsor Admin	Remote	2024-01-31 11:28:56	Enable	Disable	1
□	robert_ldap	Team1	Sponsor Admin	Remote	2024-02-06 14:09:27	Enable	Disable	1
Standard User 16/29								
□	William		Standard User	Local		Enable	FortiToken Cloud	2
□	auto_admin		Standard User	Remote		Enable	Disable	1
□	auto_pam_1		Standard User	Remote		Enable	Disable	1
☑	auto_pam_2		Standard User	Remote		Enable	Disable	1
☑	ed_admin		Standard User	Remote		Enable	Disable	1
□	lhou_rad		Standard User	Remote		Enable	Disable	0
□	local_1		Standard User	Local	2024-01-24 15:48:47	Enable	Disable	4
□	pam15		Standard User	Remote		Enable	Disable	0
□	pam28_rad		Standard User	Remote		Enable	Disable	1
□	pam28_saml		Standard User	Remote		Enable	Disable	1
□	robert2		Standard User	Remote		Enable	Disable	1
□	robert_admin		Standard User	Remote	2024-01-31 11:38:08	Enable	FortiToken Cloud	1
□	robert_ldap3		Standard User	Remote	2024-02-01 10:44:34	Enable	FortiToken Cloud	1
□	robert_ldap4		Standard User	Remote	2024-02-01 11:08:13	Enable	FortiToken Cloud	1
□	tetrtt	Team1	Standard User	Remote		Enable	Disable	1
□	tianlei_saml		Standard User	Remote		Enable	Disable	3

23 enabled / 250 licensed

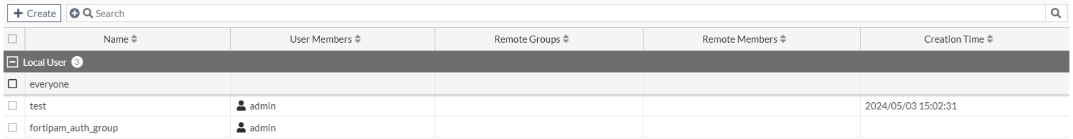
24/37

User groups

User Groups in *User Management* displays a list of user groups.

The following two default user groups are available:

- *everyone*: By default, every user belongs to this user group.
- *fortipam_auth_group*: By default, the *Super Administrator* admin user belongs to this user group. Users can be added or removed from this user group.



	Name	User Members	Remote Groups	Remote Members	Creation Time
⊟ Local User 3					
□	everyone				
□	test	admin			2024/05/03 15:02:31
□	fortipam_auth_group	admin			

The following columns are available in the *User Groups* window:

- *Name*
- *User Members*
- *Remote Groups*
- *Remote Members*
- *Creation Time*: Displays the date and time when a user group was created.

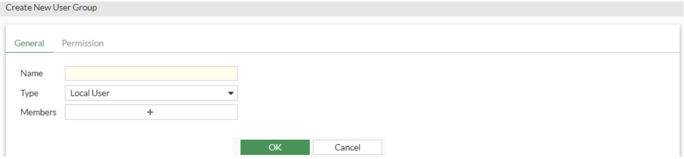
Users can be assigned to groups during user account configuration, or by creating or editing the groups to add users to it.

The *User Groups* tab contains the following options:

Create	Select to create a new user group.
Edit	Select to edit the selected user group.
Delete	Select to delete the selected user groups.
Search	Enter a search term in the search field, then hit `Enter` to search the user groups list. To narrow down your search, see Column filter.

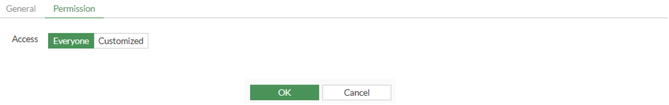
To create a new user group:

1. Go to *User Management* > *User Groups*.
2. Select *Create* to create a new user group.
   The *General* tab in the *Create New User Group window* opens.



Name:
Type: Local User
Members:

3. To switch to the *Permission* tab, select the tab.



Access: Everyone | Customized

4. In the *General* tab, enter the following information:

Name	Name of the group.
Type	Select the type of the group: • *Remote* • *Local User*
Members	Select + to add existing members to the user group from the list and select *Close*, or in the *Select Entries* window, select + to create a new user.

	See Creating a user on page 253. Use the search bar to look for a user.
Remote Groups	By adding a remote server to the user group, the group will contain all user accounts on that server. Optionally, a specific user group on the remote server can be included to restrict the scope to that group. See Creating Remote Groups. **Note:** This pane is available only when the *Type* is *Remote*. Select remote groups from the list and select *Delete* to delete the remote groups. Select a remote group from the list and select *Edit* to edit the remote group.

5. Switch to the *Permission* tab and enter the following information:

Access	Select from the following two options: • *Everyone*: All the members of the user group have complete access to the user group. • *Customized*: Customize the level of access for members in the user group.
User Permission	The level of user access to the user group. See User Permission on page 273. **Note**: The option is only available when *Access* is set to *Customized*.

6. 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 290.

      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 301.

   c. Optionally, if a SAML server is selected, select +, and enter group names in *Groups*.

      At least one SAML server must be already configured.

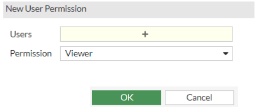
3. Click *OK* to save changes to group match.

Alternatively, use the CLI commands to create a user group.

User Permission

To set up user permission:

1. In step 5 when Creating a user group, provided that *Access* is set to *Customized*, select *Create* in *User Permission*. The *New User Permission* window opens.



New User Permission

Users +

Permission Viewer

2. Enter the following information:

Users	Select + and from the list, select users in the *Select Entries* window. **To add a new user:** 1. From the *Select Entries* window, select + and then select +*UserList*. The *New User List* wizard open. 2. Follow the steps in Creating a user on page 253, starting step 2 to create a new user. Use the search bar to look up a user. Use the pen icon next to a user to edit it.
Permission	From the dropdown, select an option: - *Viewer*: Ability to view the user group. - *Owner*: The highest possible permission level with the ability to create, edit, and delete user groups.

3. Click *OK*.

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
```

Auto provision rules

Auto Provision Rules in *User Management* displays a list of auto provision rules for remote users.

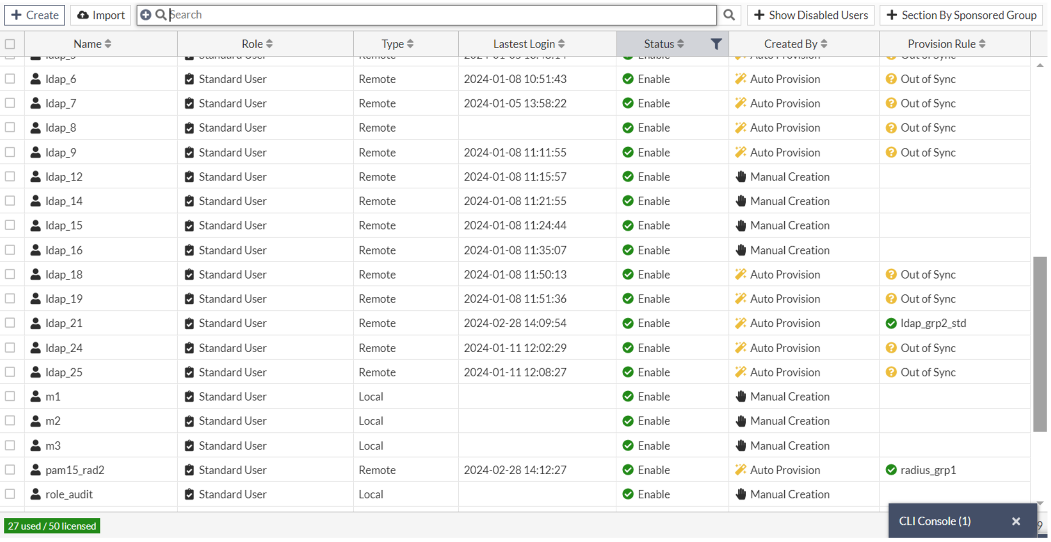
Based on the predefined auto provision rules, remote users can be auto provisioned upon their first successful login without requiring the manual creation of a user in the system prior to login:

- You create an auto provision rule for remote users (LDAP, RADIUS, or SAML).
- The user is created automatically on the first successful login.

FortiPAM allows you to automatically sync up users based on group membership without limiting the authentication protocol (LDAP, RADIUS, or SAML).

The auto provision rule includes information about the remote user group and users' role (access profile) on auto provision. The type of role depends on the user's group membership.

Based on the group, FortiPAM decides if the user can log in to FortiPAM and the type of permission the user is granted. Once the user logs in, the user is automatically created and listed in *User Management* > *User List*.



☐	Name	Role	Type	Lastest Login	Status	Created By	Provision Rule
☐	ldap_6	Standard User	Remote	2024-01-08 10:51:43	✓ Enable	Auto Provision	? Out of Sync
☐	ldap_7	Standard User	Remote	2024-01-05 13:58:22	✓ Enable	Auto Provision	? Out of Sync
☐	ldap_8	Standard User	Remote		✓ Enable	Auto Provision	? Out of Sync
☐	ldap_9	Standard User	Remote	2024-01-08 11:11:55	✓ Enable	Auto Provision	? Out of Sync
☐	ldap_12	Standard User	Remote	2024-01-08 11:15:57	✓ Enable	Manual Creation	
☐	ldap_14	Standard User	Remote	2024-01-08 11:21:55	✓ Enable	Manual Creation	
☐	ldap_15	Standard User	Remote	2024-01-08 11:24:44	✓ Enable	Manual Creation	
☐	ldap_16	Standard User	Remote	2024-01-08 11:35:07	✓ Enable	Manual Creation	
☐	ldap_18	Standard User	Remote	2024-01-08 11:50:13	✓ Enable	Auto Provision	? Out of Sync
☐	ldap_19	Standard User	Remote	2024-01-08 11:51:36	✓ Enable	Auto Provision	? Out of Sync
☐	ldap_21	Standard User	Remote	2024-02-28 14:09:54	✓ Enable	Auto Provision	✓ ldap_grp2_std
☐	ldap_24	Standard User	Remote	2024-01-11 12:02:29	✓ Enable	Auto Provision	? Out of Sync
☐	ldap_25	Standard User	Remote	2024-01-11 12:08:27	✓ Enable	Auto Provision	? Out of Sync
☐	m1	Standard User	Local		✓ Enable	Manual Creation	
☐	m2	Standard User	Local		✓ Enable	Manual Creation	
☐	m3	Standard User	Local		✓ Enable	Manual Creation	
☐	pam15_rad2	Standard User	Remote	2024-02-28 14:12:27	✓ Enable	Auto Provision	✓ radius_grp1
☐	role_audit	Standard User	Local		✓ Enable	Manual Creation	

The order of the rules impacts the login matching. First, the rule is matched from top to bottom.

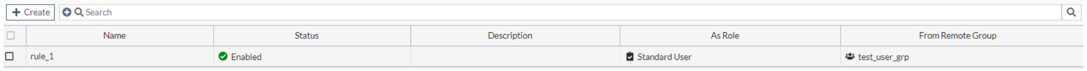
The rules can be reordered by dragging a rule up/down from the left-most row.

Disabling or deleting a rule, or changing the *From Remote Group* setting for a rule results in users becoming out-of-sync, which means the current user might not match any rule until the next successful login.

Out-of-sync users do not occupy license seats.

For each auto provision rule, the following columns are displayed by default:

- *Name*
- *Status*
- *Description*
- *As Role*
- *From Remote Group*



□	Name	Status	Description	As Role	From Remote Group
□	rule_1	✓ Enabled		Standard User	test_user_grp

The *Auto Provision Rules* tab contains the following options:

Create	Select to create a new auto provision rule. See Creating an auto provision rule on page 298.
Search	Enter a search term in the search field, then hit `Enter` to search the auto provision rules list. To narrow down your search, see Column filter.
Edit	Select to edit the selected auto provision rule.
Enable/Disable	Select to enable/disable the selected auto provision rule.
Delete	Select to delete the selected auto provision rule.
List Provisioned Users	Select to see the list of provisioned users in a new window for the selected auto provision rule.

To set up auto provisioning rule using the CLI, see Setting up remote user auto provisioning using the CLI on page 300.

Sponsored groups

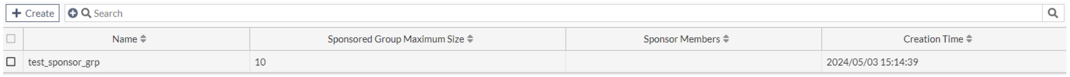
Super administrators can create sponsored groups, defining a maximum number of users for each group. These groups can then have sponsor admins assigned to them. Those sponsor admins can only access logs for their specific secrets. This includes creating, editing, disabling, and deleting users within their sponsored group.

Super administrators can assign the sponsor admin role and sponsored group when creating or editing users. Multiple sponsor admins can be assigned to a single sponsored group.

The sponsor role benefits the customers needing more visibility on the contractors' users. It aims to manage those contractors efficiently and balance the administrators' workload by designating sponsor admins managing sponsored groups.

Sponsored Groups in *User Management* displays a list of sponsored groups.

For each sponsored group; name, maximum number of users, members, and the creation time are shown.



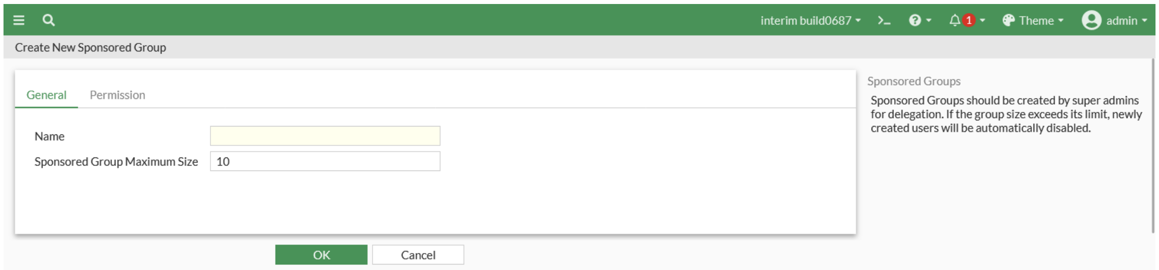
	Name	Sponsored Group Maximum Size	Sponsor Members	Creation Time
□	test_sponsor_grp	10		2024/05/03 15:14:39

The *Sponsored Groups* tab contains the following options:

Create	Select to create a new sponsored group.
Edit	Select to edit the selected sponsored group.
Delete	Select to delete the selected sponsored groups.
Search	Enter a search term in the search field, then hit `Enter` to search the sponsored groups list. To narrow down your search, see Column filter.

To create a new sponsored group:

1. Go to *User Management* > *Sponsored Groups*.
2. Select *Create* to create a new user group.
   The *General* tab in the *Create New Sponsored Group* window opens.



Create New Sponsored Group

Name	
Sponsored Group Maximum Size	10

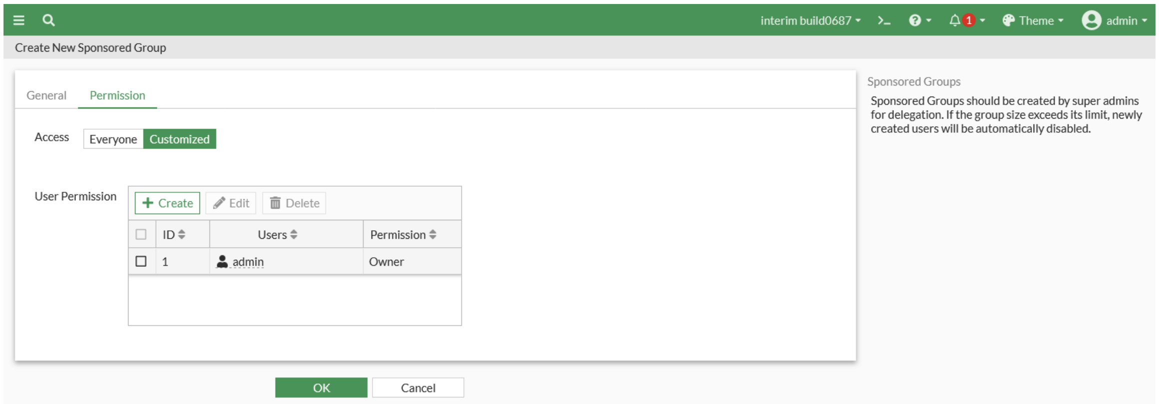
Sponsored Groups

Sponsored Groups should be created by super admins for delegation. If the group size exceeds its limit, newly created users will be automatically disabled.

3. In the *General* tab, enter the following information:

Name	Name of the group.
Sponsored Group Maximum Size	Enter the maximum number of users that can be assigned to the sponsored group.

4. To switch to the *Permission* tab, select the tab.



ID	Users	Permission
1	admin	Owner

Sponsored Groups

Sponsored Groups should be created by super admins for delegation. If the group size exceeds its limit, newly created users will be automatically disabled.

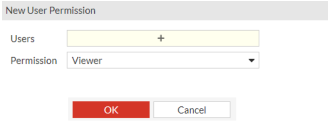
5. In the *Permission* tab, enter the following information:

Access	Select from the following two options: • *Everyone*: All the members of the sponsored group have complete access to the sponsored group. • *Customized*: Customize the level of access for members in the sponsored group.
User Permission	The level of user access to the sponsored group. See User Permission on page 277. **Note**: The option is only available when *Access* is set to *Customized*.

6. Click *OK*.

User Permission

1. In step 4 when Creating a sponsored group, with *Customized* selected in *Access*, select *Create* in *User Permission*. The *New User Permission* window opens.



Permission: Viewer

2. Enter the following information:

Users	Select + and from the list, select users in the *Select Entries* window. **To add a new user:** 1. From the *Select Entries* window, select +, and then select +*User List*. The *New User List* wizard opens. 2. Follow the steps in Creating a user on page 253, starting step 2 to create a new user. Use the search bar to look up a user. Use the pen icon next to a user to edit it.
Permission	From the dropdown, select an option: • *Viewer*: Ability to view the sponsored group. • *Owner*: The highest possible permission level with the ability to create, edit, disable, and delete users within the sponsored group.

3. Click *OK*.

Role

Roles or access profiles define what a user can do when logged into FortiPAM.

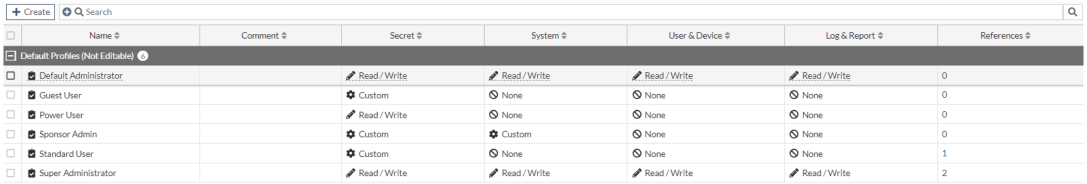
When a new user is created, it must have a specific role. See Creating a user on page 253.

When you create a standard user, a default normal user role is assigned to the new user automatically.

When setting up an administrator, administrator roles can be selected from the *Choose an Adminstrator Role* dropdown. See Creating a user on page 253.

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) 6						
□	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
□	Sponsor Admin		Custom	Custom	None	None	0
□	Standard User		Custom	None	None	None	1
□	Super Administrator		Read / Write	Read / Write	Read / Write	Read / Write	2

There are six 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.
- *Sponsor Admin*: For managing users assigned to their sponsored group. This includes creating, editing, and deleting users assigned to their sponsored group. Sponsor admins can only access logs and reports for their specific users, groups, and secrets.

  The sponsored group is selected when creating the sponsor admin user.

  The *Sponsor Admin* user has *View Secret Log* and *View Secret Video* permissions by default.
- *Standard User*: Logs in, makes requests for resources, and connect to the privileged resources.

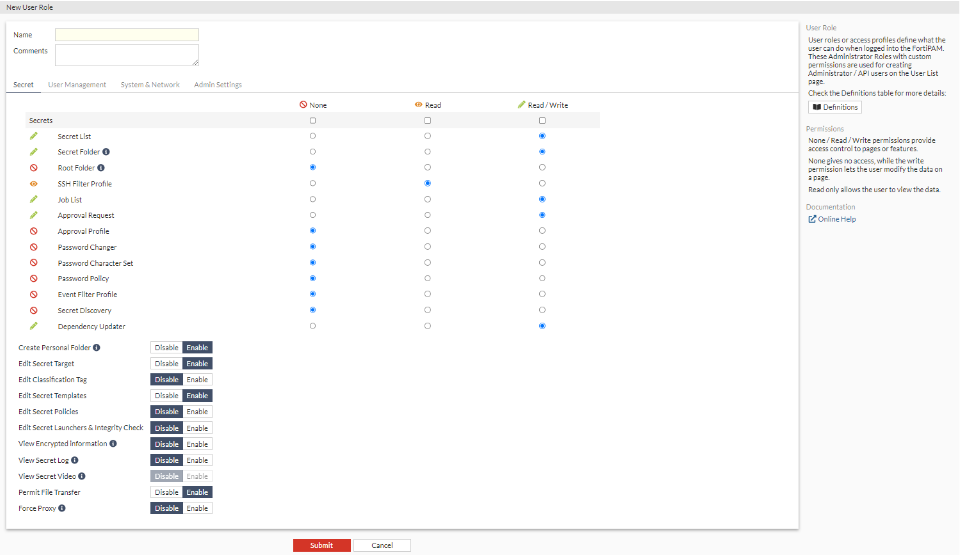
  Users with *Standard User* role do not have the privilege to manage FortiPAM devices.
- *Super Administrator*: Privilege to manage and monitor the FortiPAM device.

  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.



New User Role

Name

Comments

		None	Read	Read / Write
Secrets		□	□	□
✎	Secret List	○	○	●
✎	Secret Folder	○	○	●
⃠	Root Folder	●	○	○
👁	SSH Filter Profile	○	●	○
✎	Job List	○	○	●
✎	Approval Request	○	○	●
⃠	Approval Profile	●	○	○
⃠	Password Changer	●	○	○
⃠	Password Character Set	●	○	○
⃠	Password Policy	●	○	○
⃠	Event Filter Profile	●	○	○
⃠	Secret Discovery	●	○	○
✎	Dependency Updater	○	○	●

Create Personal Folder	Disable [✓ Enable]
Edit Secret Target	Disable [✓ Enable]
Edit Classification Tag	[✓ Disable] Enable
Edit Secret Templates	Disable [✓ Enable]
Edit Secret Policies	[✓ Disable] Enable
Edit Secret Launchers & Integrity Check	[✓ Disable] Enable
View Encrypted information	[✓ Disable] Enable
View Secret Log	[✓ Disable] Enable
View Secret Video	[✓ Disable] Enable
Permit File Transfer	Disable [✓ Enable]
Force Proxy	[✓ Disable] Enable

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 List 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.

Documentation

   Pages and features are organized and separated into different access controls.

   There are two types of access controls:

   - *Radio*: Provides *None*, *Read*, and *Read/Write* access.
   - *Switch*: Enable/disable a feature.

   For each feature, select from the following access levels:

   - *None*
   - *Read*: View access.

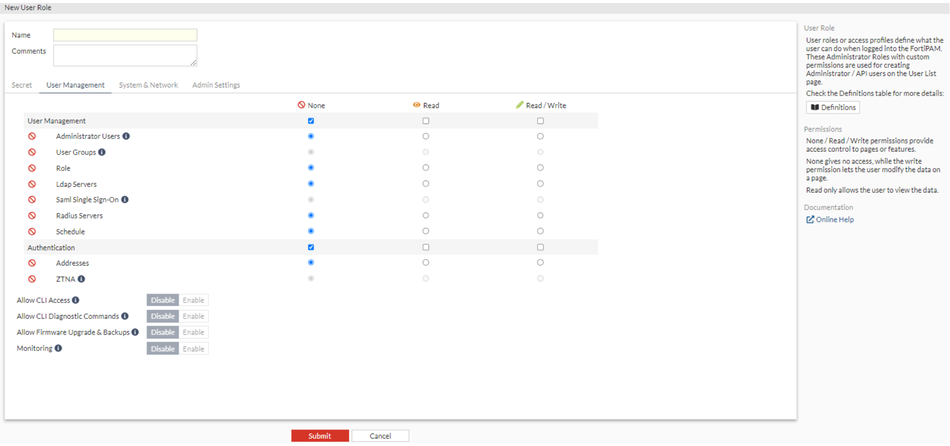
     Note: When an administrator has only read access to a feature, the administrator can access the GUI page and can use the `get` and `show` CLI command for that feature, but cannot make changes to the configuration.
   - *Read/Write*: View, change, and execute access.

2. Enter the following information:

Name	The name of the role.
Comment	Optionally, enter comments about the role.
Secret Select *None*, *Read*, or *Read/Write* to set access level globally for all the secret features.	
Secret List	Set the access level for *Secrets* page. It also controls whether pages: *Secret Templates*, *Policies* and *Launchers* can be viewed.
Secret Folder	Set the access level for *Folders*. **Note**: You can restrict the corresponding folder and secret permissions under a specific secret.
Root Folder	Permission to create folders in *Root*.

	Note: The *Secret Folder* must be set to at least *Read* permission to enable accessing the root folder.
SSH Filter Profile	Set the access level for *SSH Filter Profiles* page.
Job List	Set the access level for *Jobs List* page.
Approval Request	Set the access level for *My Request* and *Request Review* page in *Approval Request*.
Approval Profile	Set the access level for *Approval Profile* page in *Approval Flow*.
Password Changer	Set the access level for *Password Changers* page in *Password Changing*.
Password Character Set	Set the access level for *Character Sets* page in *Password Changing*.
Password Policy	Set the access level for *Password Policies* page in *Password Changing*.
Event Filter Profile	Set the access level for *Event Filter Profile* page.
Secret Discovery	Set the access level for the *Discovery* page.
Dependency Updater	
Create Personal Folder	Enable/disable creating a personal folder right after the user is created. **Note**: The *Secret Folder* permission must be *Read/Write*.
Edit Secret Target	Enable/disable editing the targets.
Edit Classification Tag	Enable/disable editing the *Classification Tag* page.
Edit Secret Templates	Enable/disable editing the *Templates* page.
Edit Secret Policies	Enable/disable editing the *Policies* page.
Edit Secret Launchers & Integrity Check	Enable/disable editing the *Launchers* and the *Integrity Check* pages.
View Encrypted 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.
View Secret Log	Enable/disable viewing secret modification history, launch activity logs, and SSH filter logs (for SSH launcher) in the *Secret Details* page when editing/viewing a secret in *Secrets* > *Secrets*. When enabled, the following tabs are available when editing/viewing a secret: • *Edit History* • *Activity* • *SSH Filter Log*
View Secret Video	Enable/disable viewing secret launch videos. **Note**: The option is only available when *View Secret Log* is enabled.
Permit File Transfer	Enable/disable permitting file transfer.
Force Proxy	Enable/disable launching secrets in the proxy mode. **Note**: The option is disabled by default.

3. Select the *User Management* tab.
   The *User Management* tab opens.



New User Role

Name

Comments

Secret | User Management | System & Network | Admin Settings

	None	Read	Read / Write
User Management	☑	□	□
Administrator Users	●	○	○
User Groups	○	○	○
Role	●	○	○
Ldap Servers	●	○	○
Saml Single Sign-On	○	○	○
Radius Servers	●	○	○
Schedule	●	○	○
Authentication	☑	□	□
Addresses	●	○	○
ZTNA	○	○	○

Allow CLI Access: [✓ Disable] Enable

Allow CLI Diagnostic Commands: [✓ Disable] Enable

Allow Firmware Upgrade & Backups: [✓ Disable] Enable

Monitoring: [✓ Disable] Enable

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 List page.

Check the Definitions table for more details:

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.

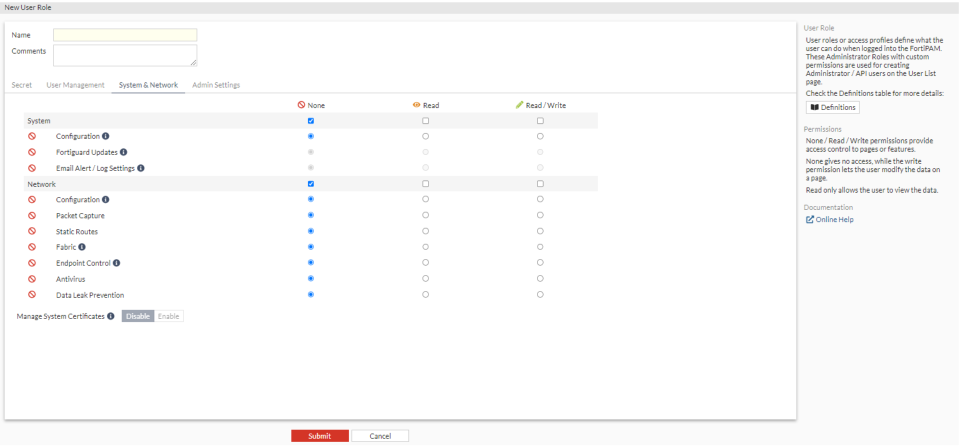
Read only allows the user to view the data.

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 List* page in *User Management* and the *Backup* page in *System*.
User Groups	Set the access level for *User Groups* page in *User Management*. **Note**: *Ldap Servers*, *Saml Single Sign-On*, and *Radius Servers* must be set to at least *Read* permission to access *User Groups*.
Role	Set the access level for *Role* page in *User Management*.
Ldap Servers	Set the access level for *Ldap Servers* page in *User Management*. **Note**: *Scheme & Rules* must be set to at least *Read* permission to access LDAP servers.
Saml Single Sign-On	Set the access level for *Saml Single Sign-On* page in *User Management*. **Note**: *Addresses* and *Scheme & Rules* must be set to at least *Read* permission to access SAML servers.
Radius Servers	Set the access level for *Radius Servers* page in *User Management*. **Note**: *Scheme & Rules* must be set to at least *Read* permission to access RADIUS servers.
Schedule	Set the access level for *Schedule* page in *User Management*.
Authentication Select *None*, *Read*, or *Read/Write* to set access level globally for all the authentication features.	
Addresses	Set the access level for *Addresses* page in *Authentication*.
ZTNA	Set the access level for *ZTNA* page in *System*. **Note**: This requires the same permission as *Schedule* and *Addresses*. - Examples • If all required permissions are *Read/ Write*, the ZTNA can only be either

	None or *Read/Write*. • If *Schedule* is set to *Read* and the rest is set to *Read/Write*, *ZTNA* can only be *None*.
Allow CLI Access	Enable/disable CLI access. **Note**: The *Administrator Users* must be set to *Write* permission to have CLI access.
Allow CLI Diagnostic Commands	Enable/disable access to diagnostic CLI commands. **Note**: *System Configuration* must be set to *Write* permission to manage system certificates. ⚠ The role must have *Allow CLI Access* enabled to access the diagnostic commands.
Allow Firmware Upgrade & Backups	Enable/disable permission to use firmware upgrades and configuration backup features.
Monitoring	Enable/disable access to the pages under *Monitoring*. Note: This requires the same permission as *User Groups*, *Ldap Servers*, *Saml Single Sign-On*, and *Radius Servers*.

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	☑	□	□
Configuration	●	○	○
Fortiguard Updates	●	○	○
Email Alert / Log Settings	●	○	○
Network	☑	□	□
Configuration	●	○	○
Packet Capture	●	○	○
Static Routes	●	○	○
Fabric	●	○	○
Endpoint Control	●	○	○
Antivirus	●	○	○
Data Leak Prevention	●	○	○

Manage System Certificates: Disable | Enable

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 List 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.

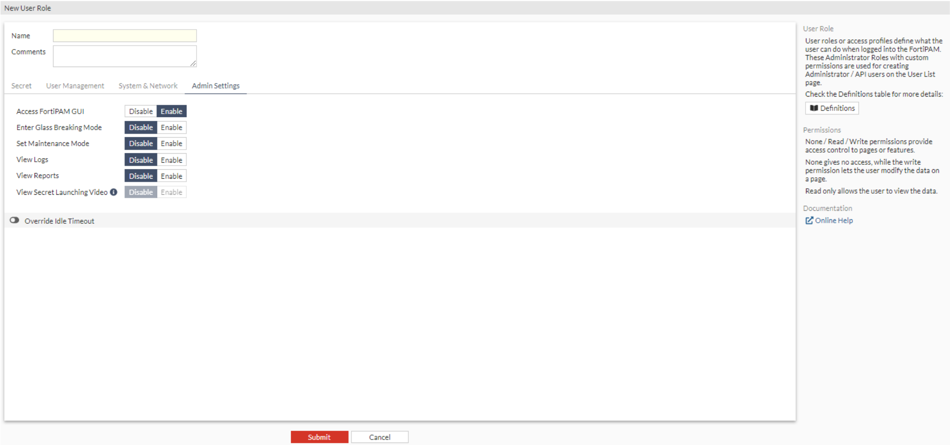
Documentation

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*.
Antivirus	Set the access level for the *AntiVirus* page in *Secret Settings*. If the access level is set to *Read* or *None*, *Use Extreme AVDB* and *AntiVirus PUP/PUA* in FortiGuard license on page 434 are either disabled or shown as *Not Available*. **Note**: This also controls the *AntiVirus* settings in the *ForitGuard License* page in *System*.
Data Leak Prevention	Set the access level for the *Data Leak Prevention* and *DLP File Pattern* pages in *Secret Settings*.
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.



Name

Comments

Access FortiPAM GUI Disable [✓ Enable]

Enter Glass Breaking Mode [✓ Disable] Enable

Set Maintenance Mode [✓ Disable] Enable

View Logs [✓ Disable] Enable

View Reports [✓ Disable] Enable

View Secret Launching Video [✓ Disable] Enable

○ Override Idle Timeout

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 List 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.

Documentation

8. Enter the following information:

Access FortiPAM GUI	Enable/disable accessing FortiPAM GUI.
Enter Glass Breaking Mode	Enable/disable glass breaking mode. **Note**: The glass breaking mode gives you access to all secrets in the system.
Set Maintenance Mode	Enable/disable maintenance mode. Note: Suspend all critical processes to allow maintenance related activities.
View Logs	Enable/disable viewing *Events*, *Secrets*, *ZTNA*, and *SSH* logs in *Log & Report*.
View Reports	Enable/disable viewing *Reports* in *Log & Report*.
View Secret Launching Video	Enable/disable viewing playback videos in *Secret Video*. **Note**: *View Logs* must be enabled since the secret videos are available in *Log & Report* > *Secret* page.
Override Idle Timeout Enable to override the idle timeout.	
Never Timeout	Enable to never timeout. **Note**: The option is disabled by default.
Offline	Set the time after which the user with the role goes offline, in minutes (1 - 480, default = 10).

9. Click *Submit*.

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 *Secrets* page. It also controls whether pages: *Secret Templates*, *Policies* and *Launchers* can be viewed.
Secret Folder	Controls the access to *Folders*. **Note**: You can restrict the corresponding folder and secret permissions under a specific folder and secret.
Root Folder	Permission to create folders in *Root*.
SSH Filter Profile	Access to the *SSH Filter Profiles* page.
Job List	Access to the *Job List* page.
Approval Request	Access to the *My Request* and *Request Review* page in *Approval Request*.

Access Control	Definition
Approval Profile	Access to the *Approval Profile* page in *Approval Flow*.
Password Changer	Access to *Password Changers* page in *Password Changing*.
Password Character Set	Access to *Character Sets* page in *Password Changing*.
Password Policy	Access to *Password Policies* page in *Password Changing*.
Event Filter Profile	Enable/disable creating event filter profiles.
Create Personal Folder	Enable/disable creating a personal folder right after the user is created.
Edit Secret Target	Enable/disable editing secret targets.
Edit Classification Tag	Enable/disable editing the *Classification Tag* page.
Edit Secret Templates	Enable/disable editing the *Secret Templates* page.
Edit Secret Policies	Enable/disable editing the *Policies* page.
Edit Secret Launchers & Integrity Check	Enable/disable editing the *Secret Launchers* and the *Integrity Check* pages.
View Encrypted information	Enable/disable viewing the secret password, passphrase, and ssh-key. This requires *Read/Write* permission for the *Secret List*.
View Secret Log	Enable/disable viewing secret logs (*Edit History*, *Activity*, and *SSH Filter Log* tabs) when editing a secret (*Secret Details* window).
View Secret Video	Enable/disable viewing secret video when editing a secret (*Secret Details* window). **Note**: This only takes effect when *View Secret Log* is already enabled.
Permit File Transfer	Enable/disable launching file launchers. These are designated to send files.
Force Proxy	Enable/disable forcing user with this account profile to always launch with proxy.
User Management	
Administrator Users	Access to the *User List* page in *User Management* and the *Backup* page in *System*.
User Groups	Access to the *User Groups* page in *User Management*.
Role	Access to the *Role* page in *User Management*.
Ldap Servers	Access to the *Ldap Servers* page in *User Management*.
Saml Single Sign-On	Access to the *Saml Single Sign-On* page in *User Management*.
Radius Servers	Access to the *Radius Servers* page in *User Management*.
Schedule	Access to the *Schedule* page in *User Management*.
Allow CLI Access	Enable/disable CLI access.
Allow CLI Diagnostic Commands	Enable/disable access to diagnostic CLI commands.

Access Control	Definition
Allow Firmware Upgrade & Backups	Enable/disable permission to use firmware and configuration backup features.
Monitoring	Access to pages in *Monitoring*. **Note**: This requires the same permission as *User Groups*, *Ldap Servers*, *Saml Single Sign-On*, and *Radius Servers*.
Authentication	
Addresses	Access to the *Addresses* page.
ZTNA	Access to the *ZTNA* page in *System*. ZTNA requires the same permission as *Schedule* and *Addresses*. Examples - Example: • If all the required permissions are *Read/Write*, ZTNA can be either *None* or *Read/Write*. • If *Schedule* is set to *Read* and the rest is *Read/Write*, *ZTNA* is *None*.
Network	
Configuration	Access to the *Interfaces* page in *Network*.
Packet Capture	Access to the *Packet Capture* page in *Network*.
Static Routes	Access to the *Static Routes* page in *Network*.
Fabric	Access to the *FortiAnalyzer Logging* card on the *Fabric Connectors* page in *Security Fabric*.
Endpoint Control	Access to the *FortiClient EMS* card on the *Fabric Connectors* page in *Security Fabric*.
Antivirus	Access to the *AntiVirus* page. **Notes**: • This also controls the *Antivirus* settings in the *FortiGuard Distribution Network* page. • Use Extreme AVDB and AntiVirus PUP/PUA settings in the *FortiGuard Distribution Network* page are disabled or shown as unavailable if the role has Read-Only or no access permission.
Data Leak Prevention	Access to the *Data Leak Prevention* and the *DLP File Pattern* pages.
Manage System Certificates	Enable/disable accessing the *Certificates* page in *System*.
System	
Configuration	Access to: • *DNS Settings* in *Network*. • *SNMP*, *Settings*, and *HA* pages in *System*. • VM License uploading; *System Reboot*, and *Shutdown* settings. • *Configuration Revisions* and *Scripts*.
FortiGuard Updates	Access to the *FortiGuard* page from *Dashboard*.
Email Alert/Log Settings	Access to *Email Alert Settings* and *Log Settings* in *Log & Report*.

Access Control	Definition
Admin Settings	
Access FortiPAM GUI	Enable/disable accessing FortiPAM GUI.
Enter Glass Breaking Mode	Enable/disable glass breaking mode.
Set Maintenance Mode	Enable/disable maintenance mode.
View Logs	Enable/disable viewing *Events*, *Secrets*, *ZTNA*, and *SSH* logs in *Log & Report*.
View Reports	Enable/disable viewing *Reports* in *Log & Report*.
View Secret Launching Video	Enable/disable viewing playback videos in *Secret Video*.

Log permissions

Use the following chart to confirm the level of log access depending on user/user group permission for the secret and log permission for the role that applies to the user:

Secret Permission				Role Permission			Result		
List	View	Edit	Owner	View Secret Log	View Secret Video	View Global Log	Log from Secret	Video from Secret	Global Log
✓						✓	NO	NO	YES
	✓					✓	Yes	Yes	Yes
		✓				✓	Yes	Yes	Yes
			✓			✓	Yes	Yes	Yes
✓				✓			No	No	No
	✓			✓			Yes	No	No
		✓		✓			Yes	No	No
			✓	✓			Yes	No	No
✓				✓	✓		No	No	No
	✓			✓	✓		Yes	Yes	No
		✓		✓	✓		Yes	Yes	No
			✓	✓	✓		Yes	Yes	No
✓							No	No	No
	✓						No	No	No
		✓					No	No	No
			✓				No	No	No

Sponsor Admin									
List	**View**	**Edit**	**Owner**	**View Secret Log**	**View Secret Video**	**View Global Log**	**Log from Secret**	**Video from Secret**	**Global Log**
✓				✓	✓		No	No	No
	✓			✓	✓		Yes	Yes	No
		✓		✓	✓		Yes	Yes	No
			✓	✓	✓		Yes	Yes	No

Notes:

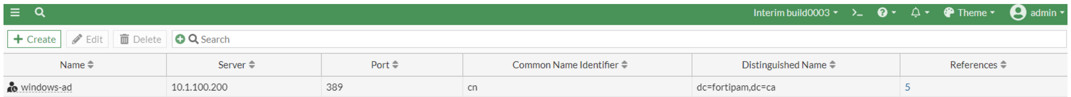
- For users with *View Secret Log* and *View Secret Video* permissions without global log access, at least *View* permission is the precondition to check logs from the *Secret Details* window. Users with global log access can bypass the precondition.
- The *Sponsor Admin* user has *View Secret Log* and *View Secret Video* permissions by default.

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.



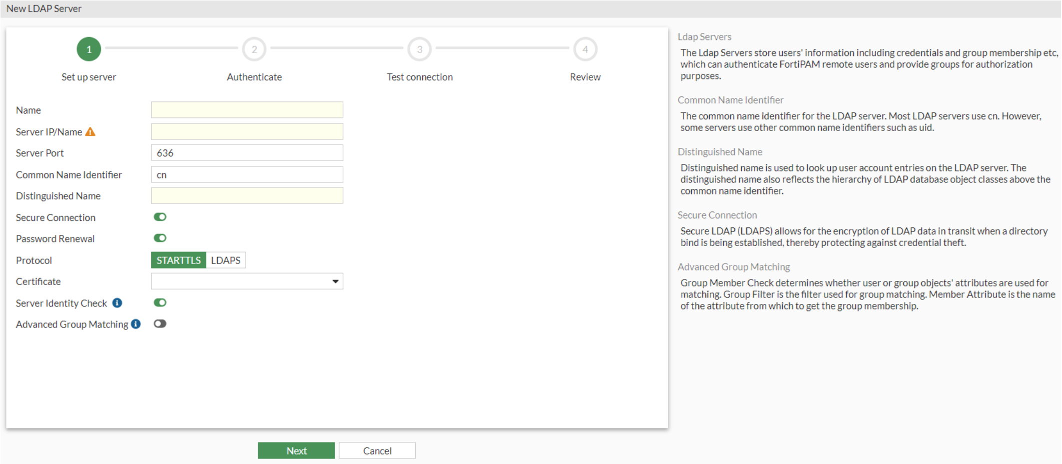
Name	Server	Port	Common Name Identifier	Distinguished Name	References
windows-ad	10.1.100.200	389	cn	dc=fortipam,dc=ca	5

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.



Name:
Server IP/Name:
Server Port: 636
Common Name Identifier: cn
Distinguished Name:
Secure Connection: ●
Password Renewal: ●
Protocol: [✓ STARTTLS] LDAPS
Certificate:
Server Identity Check: ●
Advanced Group Matching: ○

Ldap Servers

The Ldap Servers store users' information including credentials and group membership etc, which can authenticate FortiPAM remote users and provide groups for authorization purposes.

Common Name Identifier

The common name identifier for the LDAP server. Most LDAP servers use cn. However, some servers use other common name identifiers such as uid.

Distinguished Name

Distinguished name is used to look up user account entries on the LDAP server. The distinguished name also reflects the hierarchy of LDAP database object classes above the common name identifier.

Secure Connection

Secure LDAP (LDAPS) allows for the encryption of LDAP data in transit when a directory bind is being established, thereby protecting against credential theft.

Advanced Group Matching

Group Member Check determines whether user or group objects' attributes are used for matching. Group Filter is the filter used for group matching. Member Attribute is the name of the attribute from which to get the group membership.

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

Set up server	
Name	Name of the server.
Server IP/name	The IP address or FQDN for this remote server.
Server Port	The port number for LDAP traffic (default = 636).
Common Name Identifier	The common name identifier for the LDAP server. Most LDAP servers use `cn`. However, some servers use other common name identifiers such as `UID`. (default = `cn`).
Distinguished Name	The distinguished name is used to look up entries on the LDAP server. The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier.
Secure Connection	Enable to use a secure LDAP server connection for authentication. Secure LDAP (LDAPS) allows for the encryption of LDAP data in transit when a directory bind is being established, thereby protecting against credential theft. **Note**: This option is enabled by default.
Password Renewal	Enable to allow LDAP users to renew passwords. **Note**: This option is only available when *Secure Connection* is enabled. **Note**: This option is enabled by default.
Protocol	When *Secure Connection* is enabled, select either *LDAPS* or *STARTTLS* (default).
Certificate	When *Secure Connection* is enabled, select the certificate from the dropdown. Use the search bar to look up a certificate.
Server Identity Check	Enable to verify server domain name/IP address against the server certificate.

	Note: This option is only available when *Secure Connection* is enabled. **Note**: This option is enabled by default.
Advanced Group Matching	Group member check determines whether user or group objects' attributes are used for matching. Group Filter is the filter used for group matching. Member attribute is the name of the attribute from which to get the group membership. Depending on the LDAP server, you may need to configure additional properties to ensure LDAP groups are correctly matched. **Note**: The option is disabled by default.
Group Member Check	From the dropdown, select a group member check option (default = `Ldap::grp::member::check:user-attr`).
Group Filter	Enter the group filter for group matching.
Group Search Base	Enter the search base used for searching a group.
Member Attribute	Specify the value for this attribute. This value must match the attribute of the group in LDAP server. All users part of the LDAP group with the attribute matching the attribute will inherit the administrative permissions specified for this group (default = `memberof`).
Authenticate	
Username	The username.
Password	The password.

3. Click *Test connection* to test the connection to the LDAP server.

   Test connection is only available to users who have *Write* permission for *Ldap Servers*. See Role on page 278.

   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 269.
3. Configuring the administrator account. See Creating a user on page 253.

SAML Single Sign-On (SSO)

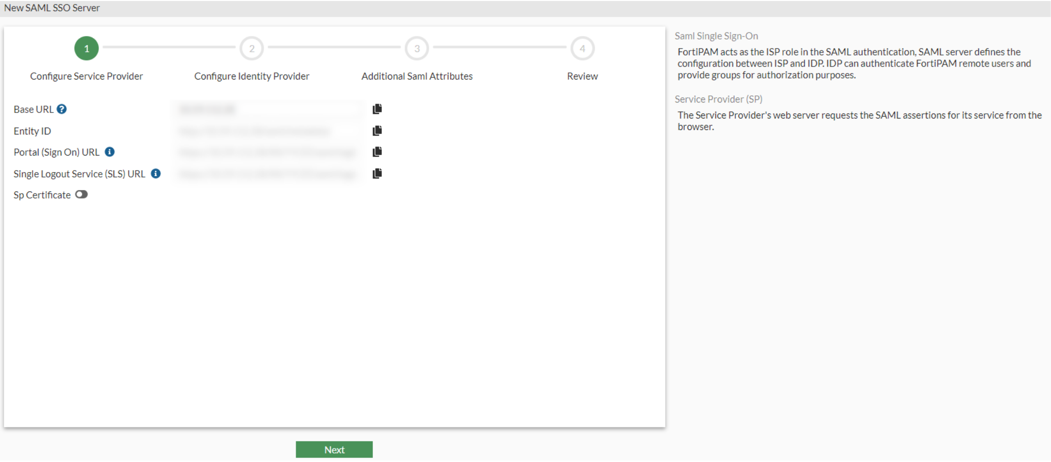
SAML SSO can be configured in *User Management*.

FortiPAM acts as the SP in SAML authentication. The SAML server defines the configuration between SP and IdP. An IdP can authenticate FortiPAM remote users and provide groups for authorization.

To create a SAML SSO server:

Before creating the SAML SSO server, you must add the SAML user as a remote user.
See Creating a user on page 253.
Alternatively, you can automatically provision the remote SAML user.
See Creating an auto provision rule on page 298.

1. Go to *User Management* > *Saml Single Sign-On*.


New SAML SSO Server
1
Configure Service Provider
2
Configure Identity Provider
3
Additional Saml Attributes
4
Review
Base URL
Entity ID
Portal (Sign On) URL
Single Logout Service (SLS) URL
Sp Certificate
Next

Base URL [redacted]

Entity ID [redacted]

Portal (Sign On) URL [redacted]

Single Logout Service (SLS) URL [redacted]

Saml Single Sign-On

FortiPAM acts as the ISP role in the SAML authentication, SAML server defines the configuration between ISP and IDP. IDP can authenticate FortiPAM remote users and provide groups for authorization purposes.

Service Provider (SP)

The Service Provider's web server requests the SAML assertions for its service from the browser.

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

Configure Service Provider	
Base URL	The URL where the Identity Provider (IdP) sends SAML authentication requests. **Note**: The address should be WAN-accessible and can be an IP address or an FQDN. **Note**: To include a port, append it after a colon. For example: `200.1.1.1.:443`.
Entity ID	Enter the SP entity ID.
Portal (Sign On) URL	The SAML service provider login URL. The URL is used to initiate a single sign-on. **Note**: Not all IdPs require a *Portal (Sign On) URL*. **Note**: The *Portal (Sign On) URL* is alternatively referred to as the Portal URL or the Sign On URL.
Single Logout Service (SLS) URL	The SP Single Logout Service (SLS) logout URL. The IdP sends the logout response to this URL. **Note**: The *Single Logout Service (SLS) URL* is alternatively referred to as the SLS URL, Single Logout Service URL, or the Logout URL.
Sp Certificate	Enable this option and import the SP certificate for authentication request signing by the SP. **Note**: This option is disabled by default.
Configure Identity Provider An IdP provides SAML assertions for the service provider and redirects the user's browser back to the service provider web server.	
Log in to the IdP to find the following information.	

Type	Select either *Fortinet Product* or a *Custom* IdP.
IdP Address	The IdP address. **Note**: This option is only available when the *Type* is *Fortinet Product*.
Prefix	Enter the IdP prefix. **Note**: The prefix is appended to the end of the IdP URLs. **Note**: This option is only available when the *Type* is *Fortinet Product*.
IdP Certificate	Select a server certificate to use for the SP. ⚠ Whenever the configuration changes on the IdP, you need to upload the new certificate reflecting the changes.
IdP entity ID	The IdP's entity ID, for example: `http://www.example.com/saml-idp/xxx/metadata/` **Note**: This option is only available when the *Type* is *Custom*.
IdP single sign-on URL	The IdP's login URL, for example: `http://www.example.com/saml-idp/xxx/login/` **Note**: This option is only available when the *Type* is *Custom*.
IdP single logout URL	The IdP's logout URL, for example: `http://www.example.com/saml-idp/xxx/logout/` **Note**: This option is only available when the *Type* is *Custom*.
Additional Saml Attributes FortiPAM looks for the attributes to verify authentication attempts. Configure your IdP to include the attributes in the SAML attribute statement.	
Attribute used to identify users	Enter the SAML attribute used to identify the users.
Attribute used to identify groups	Enter the SAML attribute used to identify the groups.
AD FS claim	Enable AD FS claim. **Note**: This option is disabled by default.
User claim type	From the dropdown, select a user claim type (default = `User Principal Name`).
Group claim type	From the dropdown, select a group claim type (default = `User Group`).

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

Use the pen icon to edit tabs.

Alternatively, use the CLI commands to configure an IdP.

CLI configuration to set up a SAML IdP - example**:**

```
config user saml
   edit <SAML Name>
      set entity-id "http://<PAM_VIP>/saml/metadata/"
      set single-sign-on-url "https://<PAM_VIP>/XX/YY/ZZ/saml/login/"
      set single-logout-url "https://<PAM_VIP>/remote/saml/logout/"
      set idp-entity-id "http://<iDP URL>/<idp_entity_id>"
      set idp-single-sign-on-url "https://<iDP_URL>/<sign_on_url>"
      set idp-single-logout-url "https://<iDP_URL>/<sign_out_url>"
      set idp-cert <iDP Certificate>
      set user-name "username"
      set group-name "group"
      set digest-method sha256
   next
end
config firewall access-proxy
   edit "fortipam_access_proxy"
      set vip "fortipam_vip"
      config api-gateway
         edit 4
            set service samlsp
            set saml-server "fortipam-saml-sso-server"
         next
      end
   next
end
config authentication scheme
   edit "fortipam_saml_auth_scheme"
      set method saml
      set saml-server "fortipam-saml-sso-server"
   next
end
config authentication rule
   edit "fortipam_saml_auth_rule" #Create a new rule and move it above the default
         "fortipam_auth" rule.
      set srcaddr "all"
      set dstaddr "saml_auth_addr"
      set ip-based disable
      set active-auth-method "fortipam_saml_auth_scheme"
      set web-auth-cookie enable
   next
   edit "fortipam_auth"
      set srcaddr "all"
      set ip-based disable
      set active-auth-method "fortipam_auth_scheme"
      set web-auth-cookie enable
   next
end
```

CLI configuration to enable SAML authentication on the login page - example

```
config system global
   set saml-authentication enable
end
```

To log in to FortiPAM as a SAML user:

1. On the login page, from the *Local* dropdown, select *SAML*.
2. Select *Continue* to open the SAML login page.
3. Enter the username and password to log in to FortiPAM.

Auto provision rules

Auto Provision Rules in *User Management* displays a list of auto provision rules for remote users.

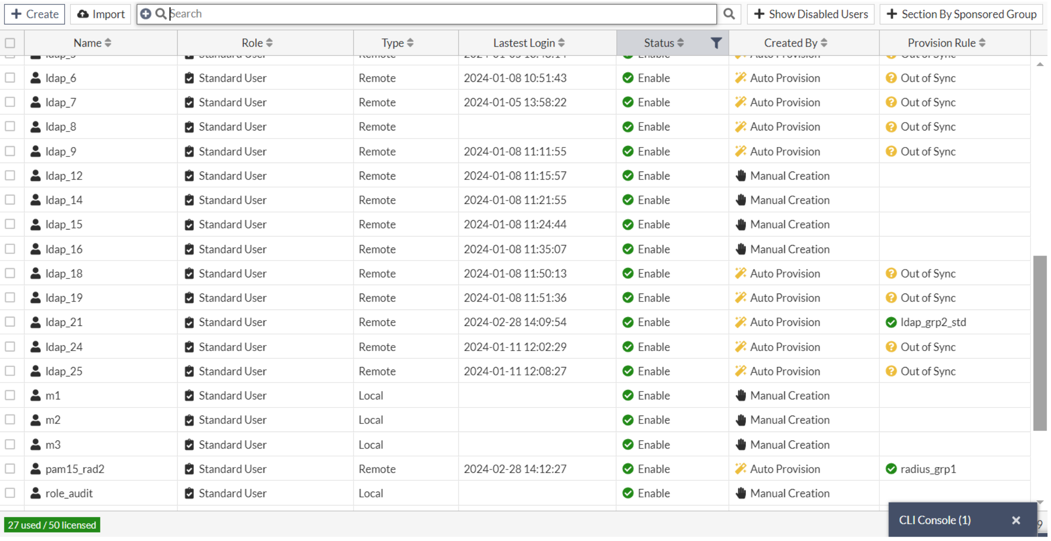
Based on the predefined auto provision rules, remote users can be auto provisioned upon their first successful login without requiring the manual creation of a user in the system prior to login:

- You create an auto provision rule for remote users (LDAP, RADIUS, or SAML).
- The user is created automatically on the first successful login.

FortiPAM allows you to automatically sync up users based on group membership without limiting the authentication protocol (LDAP, RADIUS, or SAML).

The auto provision rule includes information about the remote user group and users' role (access profile) on auto provision. The type of role depends on the user's group membership.

Based on the group, FortiPAM decides if the user can log in to FortiPAM and the type of permission the user is granted. Once the user logs in, the user is automatically created and listed in *User Management* > *User List*.



□	Name	Role	Type	Lastest Login	Status	Created By	Provision Rule
□	ldap_6	Standard User	Remote	2024-01-08 10:51:43	✓ Enable	Auto Provision	? Out of Sync
□	ldap_7	Standard User	Remote	2024-01-05 13:58:22	✓ Enable	Auto Provision	? Out of Sync
□	ldap_8	Standard User	Remote		✓ Enable	Auto Provision	? Out of Sync
□	ldap_9	Standard User	Remote	2024-01-08 11:11:55	✓ Enable	Auto Provision	? Out of Sync
□	ldap_12	Standard User	Remote	2024-01-08 11:15:57	✓ Enable	Manual Creation	
□	ldap_14	Standard User	Remote	2024-01-08 11:21:55	✓ Enable	Manual Creation	
□	ldap_15	Standard User	Remote	2024-01-08 11:24:44	✓ Enable	Manual Creation	
□	ldap_16	Standard User	Remote	2024-01-08 11:35:07	✓ Enable	Manual Creation	
□	ldap_18	Standard User	Remote	2024-01-08 11:50:13	✓ Enable	Auto Provision	? Out of Sync
□	ldap_19	Standard User	Remote	2024-01-08 11:51:36	✓ Enable	Auto Provision	? Out of Sync
□	ldap_21	Standard User	Remote	2024-02-28 14:09:54	✓ Enable	Auto Provision	✓ ldap_grp2_std
□	ldap_24	Standard User	Remote	2024-01-11 12:02:29	✓ Enable	Auto Provision	? Out of Sync
□	ldap_25	Standard User	Remote	2024-01-11 12:08:27	✓ Enable	Auto Provision	? Out of Sync
□	m1	Standard User	Local		✓ Enable	Manual Creation	
□	m2	Standard User	Local		✓ Enable	Manual Creation	
□	m3	Standard User	Local		✓ Enable	Manual Creation	
□	pam15_rad2	Standard User	Remote	2024-02-28 14:12:27	✓ Enable	Auto Provision	✓ radius_grp1
□	role_audit	Standard User	Local		✓ Enable	Manual Creation	

The order of the rules impacts the login matching. First, the rule is matched from top to bottom.

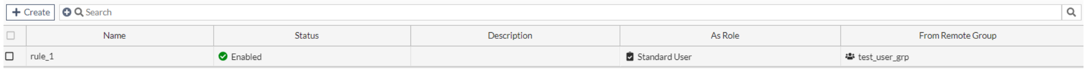
The rules can be reordered by dragging a rule up/down from the left-most row.

Disabling or deleting a rule, or changing the *From Remote Group* setting for a rule results in users becoming out-of-sync, which means the current user might not match any rule until the next successful login.

Out-of-sync users do not occupy license seats.

For each auto provision rule, the following columns are displayed by default:

- *Name*
- *Status*
- *Description*
- *As Role*
- *From Remote Group*



☐	Name	Status	Description	As Role	From Remote Group
☐	rule_1	✓ Enabled		Standard User	test_user_grp

The *Auto Provision Rules* tab contains the following options:

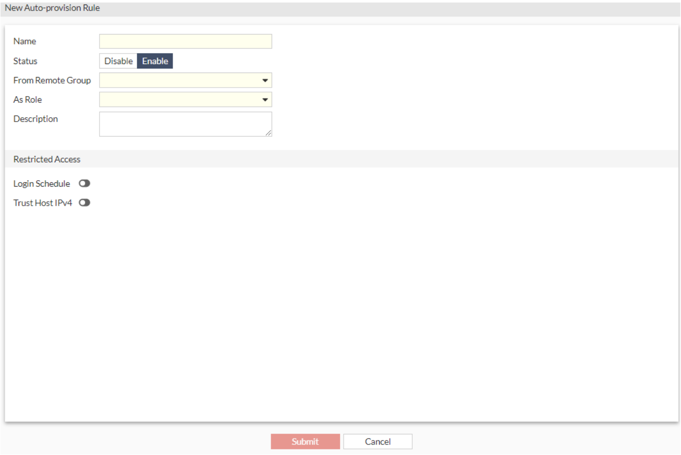
Create	Select to create a new auto provision rule. See Creating an auto provision rule on page 298.
Search	Enter a search term in the search field, then hit `Enter` to search the auto provision rules list. To narrow down your search, see Column filter.
Edit	Select to edit the selected auto provision rule.
Enable/Disable	Select to enable/disable the selected auto provision rule.
Delete	Select to delete the selected auto provision rule.
List Provisioned Users	Select to see the list of provisioned users in a new window for the selected auto provision rule.

To set up auto provisioning rule using the CLI, see Setting up remote user auto provisioning using the CLI on page 300.

Creating an auto provision rule

To create an auto provision rule:

1. Go to *User Management* > *Auto Provision Rules*.
2. In the auto provision rules list, select *Create*.
   The *New Auto-provision Rule* window opens.



New Auto-provision Rule

Name

Status Disable Enable

From Remote Group

As Role

Description

Restricted Access

Login Schedule

Trust Host IPv4

Submit Cancel

3. Enter the following information:

Name	The name of the auto provision rule.
Status	Enable/disable the auto provision rule (default = enable).
From Remote Group	From the dropdown, select the remote user group from where to auto provision users. **To create a new remote group:** 1. Select +. The *Create New User Group* window opens. 2. Follow the steps in Creating a remote user group, starting step 4 to create a new remote user group. Use the search bar to look up a remote user group.
As Role	From the dropdown, select a role (access profile) that is assigned to the user on successful login. **To create a new user role:** 1. Select +. The *New User Role* window opens. 2. Follow the steps in *To create a role* in Role on page 278, to create a new user role. Use the search bar to look up a user role.
Description	Optionally, enter a description about the auto provision rule.

Restricted Access	
Login Schedule	Enable, and from the dropdown, select a login schedule. This is the schedule when auto provisioned users are allowed to log in. **Note**: The option is disabled by default. Use the search bar to look up a schedule. See Schedule on page 303.
Trust Host IPv4	Enable, and from the dropdown, select trusted IPv4 addresses users use to connect to FortiPAM. **Note**: The option is disabled by default. Use + button to add a new IPv4 address and *x* to delete an added IPv4 address.

4. Click *Submit*.

Setting up remote user auto provisioning using the CLI

To set up remote user auto provisioning:

1. In the CLI console, enter the following commands to configure a user group:

```
config user group
 edit "test_user_grp"
  set member "test_ldap_server" #LDAP server set as the member
  config match
   edit 1
    set server-name "test_ldap_server"
    set group-name "cn=PAM_Group,cn=users,dc=fortipam,dc=ca"
   next
  end
 next
end
```

2. In the CLI console, enter the following commands to configure an auto provision rule:

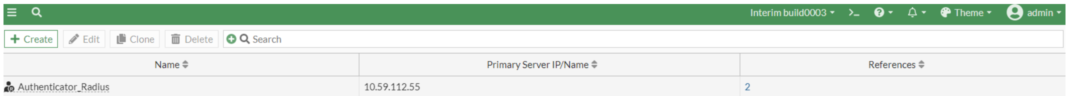
```
config user auto-provision-rule
 edit "test_rule"
  set status enable
  set remote-group "test_user_grp" #user group created in step 1
  set accprofile "pam_standard_user" #user role
 next
end
```

When a user from the `test_user_grp` user group logs in to FortiPAM, the user is automatically created with the *Standard User* role and listed in *User Management* > *User List*.

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.



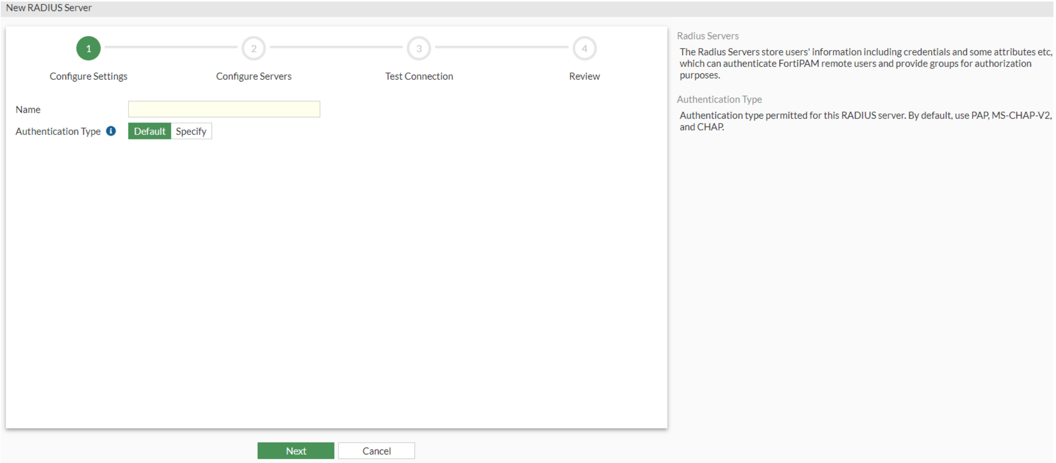
Name	Primary Server IP/Name	References
Authenticator_Radius	10.59.112.55	2

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.



Name
Authentication Type: Default

Radius Servers

The Radius Servers store users' information including credentials and some attributes etc, which can authenticate FortiPAM remote users and provide groups for authorization purposes.

Authentication Type

Authentication type permitted for this RADIUS server. By default, use PAP, MS-CHAP-V2, and CHAP.

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
```

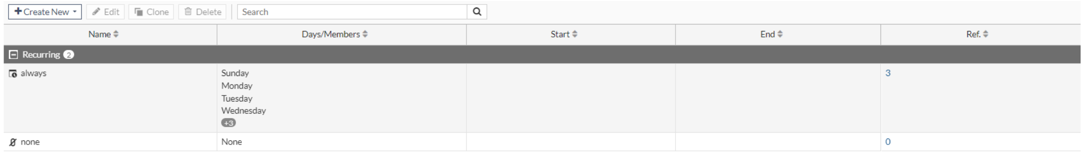
Setting up RADIUS authentication includes the following steps:

1. Configure the RADIUS server. Configuring a RADIUS server.
2. Adding the RADIUS server to a user group. User groups on page 269.
3. Configuring a RADIUS user. Creating a user on page 253.

Schedule

Schedule can be configured in *User Management*.

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



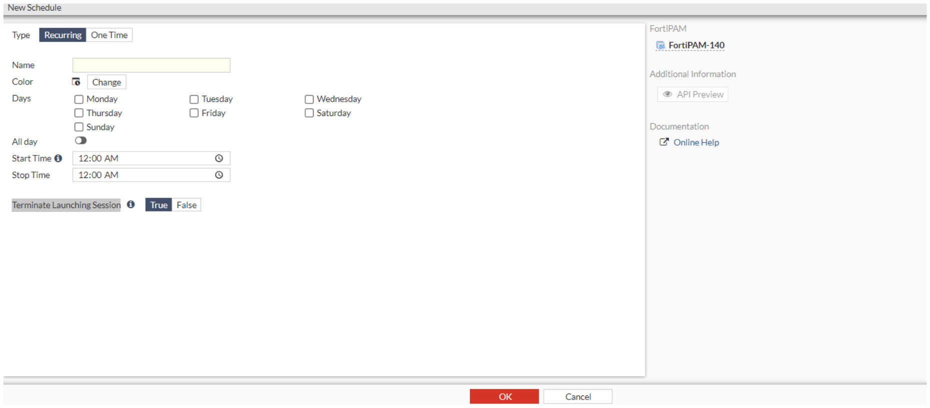
Name	Days/Members	Start	End	Ref.
Recurring 2				
always	Sunday Monday Tuesday Wednesday +3			3
none	None			0

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.



Type: Recurring | One Time

Name:

Color:

Days: □ Monday □ Tuesday □ Wednesday □ Thursday □ Friday □ Saturday □ Sunday

All day

Start Time: 12:00 AM

Stop Time: 12:00 AM

Terminate Launching Session: True | False

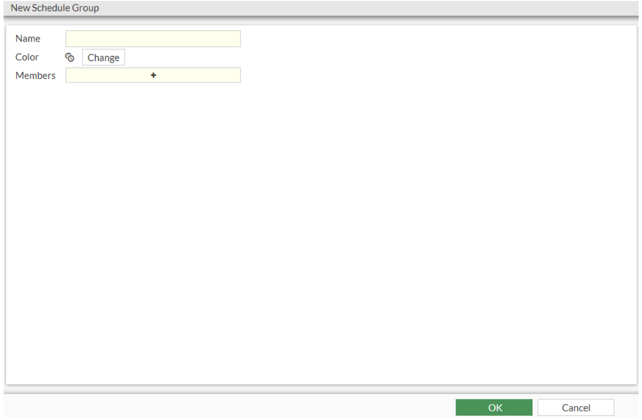
3. In the *New Schedule* window, enter the following information:

Type	Select either *Recurring* or *One Time*.
Name	The name of the schedule.
Color	Select *Change* and then select a color.
Days	Select the days of the week when the schedule applies. **Note**: This option is only available when the *Type* is *Recurring*.
All day	Enable to apply the schedule all day. **Note**: This option is only available when the *Type* is *Recurring*.
Start Date	Enter the start date and time. Alternatively, select the calendar icon and then select a date. Similarly, select the clock icon and then select a time. **Note**: This option is only available when the *Type* is *One Time*.
Start Time	Enter the start time. Alternatively, select the clock icon and then select a start time. **Note**: This option is only available when the *Type* is *Recurring* and *All day* is disabled.
End Date	Enter the end date and time. Alternatively, select the calendar icon and then select a date. Similarly, select the clock icon and then select a time. **Note**: This option is only available when the *Type* is *One Time*.
Stop Time	Enter the stop time. Alternatively, select the clock icon and then select a stop time. If the stop time is set earlier than the start time, the stop time is the same time the next day. **Note**: This option is only available when *Type* is *Recurring* and *All day* is disabled.
Pre-expiration event log	Select to create an event log *Number of days* before the *End Date*. **Note**: This option is only available when the *Type* is *One Time*.
Number of days before	Enter the number of days (1 - 100, default = 3). **Note**: This option is only available when the *Type* is *One Time* and *Pre-expiration event log* is enabled.
Terminate Launching Session	Launching session terminated when the user session exceeds the time set up in the schedule associated with the user. Set as *True*/*False* (default = *True*).

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.



New Schedule Group

Name

Color

Members

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

Name	The name of the schedule group.
Color	Select *Change* and then select a color.
Members	From the dropdown, select +, and in *Select Entries*, select members. If a new schedule is required, select *Create* then select the type of schedule to create a new schedule. Use the search bar to look for members. Use the pen icon next to a schedule to edit the scheudle.

4. Click *Close*
5. Click *OK*.

FortiTokens

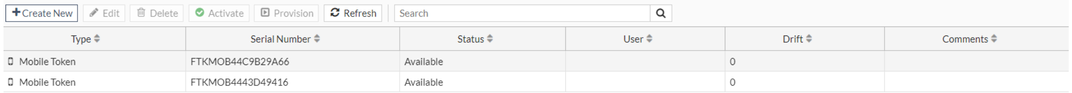
Go to *User Management* > *FortiTokens* to view a list of configured FortiTokens.

To access the *FortiTokens* page, you require *Read* or higher permission to *User Groups*, *Ldap Servers*, *Saml Single Sign-On*, and *Radius Servers*. See Role on page 278.

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.



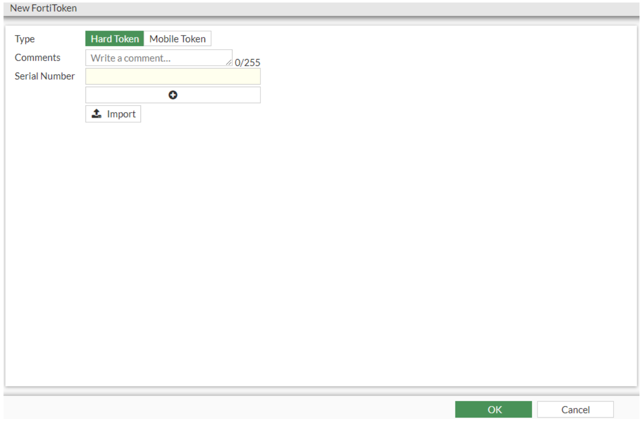
Type	Serial Number	Status	User	Drift	Comments
Mobile Token	FTKMOB44C9B29A66	Available		0	
Mobile Token	FTKMOB4443D49416	Available		0	

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.



2. Enter the following information:

Type	The token type: • *Hard Token* • *Mobile Token*
Comments	Optionally, enter comments about the token. **Note**: This option is only available when the *Type* is *Hard Token*.
Serial Number	The FortiToken serial number. To add multiple FortiTokens, select + and enter a new serial number. **Note**: This option is only available when the *Type* is *Hard Token*.
Activation Code	The activation code. **Note**: This option is only available when the *Type* is *Mobile Token*.
Import	Select the option to import multiple tokens by selecting one of the following and clicking *OK*: • *Serial Number File*: Select *Upload* to load a CSV file that contains token serial numbers. FortiToken devices have a serial number barcode on the m used to create the import file. • *Seed File*: Select *Upload* to load a CSV file that contains token serial numbers, encrypted seeds, and IV values. **Note**: This option is only available when the *Type* is *Hard Token*.

3. Click *OK*.

Monitoring FortiTokens

You can also view the list of FortiTokens, their status, token clock drift, and which user they are assigned to from the FortiToken list found at *User Management* > *FortiTokens*.

Monitoring

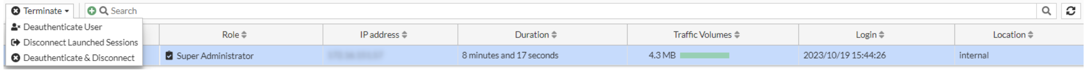
Go to *Monitoring* to access the following tabs:

- User monitor on page 308
- Active sessions on page 308

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, timestamp of when they logged in last, and the location from where they have 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, role, IP address, duration, traffic volume, the last login date and time, and location are displayed.



Role	IP address	Duration	Traffic Volumes	Login	Location
Super Administrator	[redacted]	8 minutes and 17 seconds	4.3 MB	2023/10/19 15:44:26	internal

The *User Monitor* tab contains the following options:

Terminate	From the dropdown, select from the following options for a selected user: • *Deauthenticate User*: Kick out a logged in FortiPAM user. • *Disconnect Launched Sessions*: Terminate all the launched secret sessions associated with the user. • *Deauthenticate & Disconnect*: Kick out a logged in FortiPAM user and all the launched secret sessions associated with the user.
Search	Enter a search term in the search field, then hit `Enter` to search the user monitor list. To narrow down your search, see Column filter.
Refresh	To refresh the contents, click the refresh icon.

Active sessions

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

Additionally, a *Disconnect* button is available when you select a secret session. Using the *Disconnect* button, you can terminate the selected launched secret session. 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 *Disconnect* button to protect the integrity of the secret.

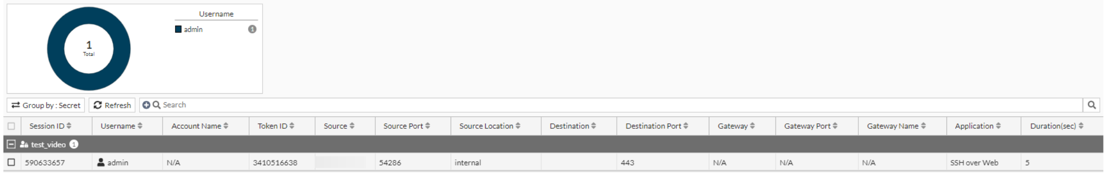
Disconnecting native non-proxy sessions is currently not supported.

On the top, the following widget is displayed:

- *Username*: displays the total count of the users using secrets.

For every session, the following columns are displayed by default:

- *Session ID*
- *Username*
- *Account Name*
- *Token ID*
- *Source*
- *Source Port*
- *Source Location*
- *Destination*: The actual target server IP address.
- *Destination Port*
- *Gateway*: The gateway IP address.
- *Gateway Port*
- *Gateway Name*: The gateway name.
- *Application*
- *Duration (sec)*

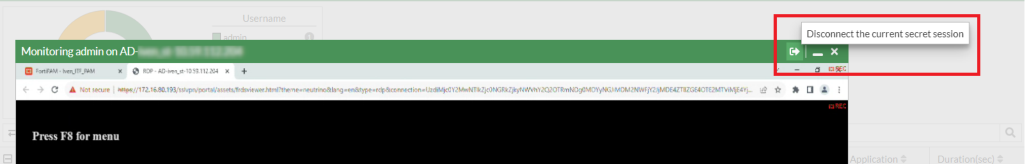


□	Session ID	Username	Account Name	Token ID	Source	Source Port	Source Location	Destination	Destination Port	Gateway	Gateway Port	Gateway Name	Application	Duration(sec)
⊟ test_video 1														
□	590633657	admin	N/A	3410516638	[redacted]	54286	internal		443	N/A	N/A	N/A	SSH over Web	5

The *Active Sessions* tab contains the following options:

Group by	Select to group the active sessions by either username or secret.
Refresh	To refresh the contents, click the refresh icon.
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.

For an active secret session, you can terminate the session by clicking *Disconnect the current secret session* as you live stream the session.


Disconnect the current secret session
Monitoring admin on AD-[redacted]
FortiPAM - Iven_ITF_PAM
RDP - AD-iven_st-10.59.112.204
Not secure
https://172.16.80.193/sslvpn/portal/assets/frdsviewer.html?theme=neutrino&lang=en&type=rdp&connection=UzdiMjc0Y2MwNTlkZjc0NGRkZjkyNWVhY2Q2OTRmNDg0MDYyNGJiMOM2NWFjY2JjMDE4ZTllZGE4OTE2MTViMjE4Yj...
REC
Press F8 for menu
Username
admin
Application
Duration(sec)

For information on over-the-shoulder monitoring, see Over-the-shoulder monitoring (Live recording) on page 310.

Over-the-shoulder monitoring (Live recording)

FortiPAM allows administrators to monitor the user session and actions in real-time.

Prerequisites:

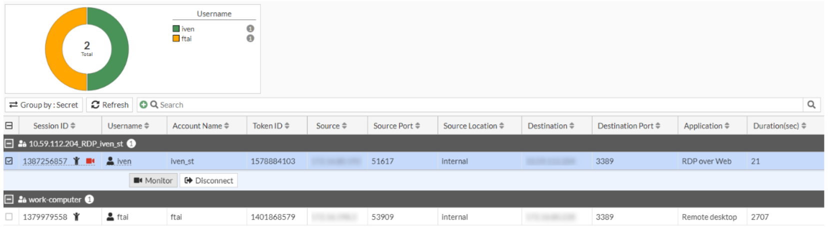
- *Fortinet Privileged Access Agent* 7.2.3 or above is required to support over-the-shoulder monitoring.
- When you launch a secret with *Session Recording* enabled, and given that *Live Recording* is enabled in the *Advanced* tab in *System* > *Settings*, you can monitor the user session in real-time.

> To ensure seamless real-time video recording and transmission to FortiPAM, consider the following system resource guidelines for launching multiple concurrent sessions:
> - CPU: 8 logical processors
> - Memory: 16 GB

To monitor the user secret session in real-time:

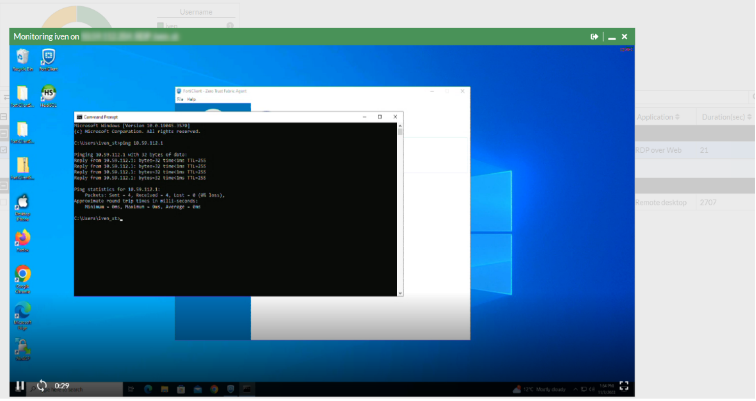
1. Go to *Monitoring* > *Active Sessions*.
2. Select the secret session and click *Monitor*.

> Secret sessions with a red video recording icon are ready to be live-streamed.



	Session ID	Username	Account Name	Token ID	Source	Source Port	Source Location	Destination	Destination Port	Application	Duration(sec)
⊟ 10.59.112.204_RDP_iven_st 1											
☑	1387256857	iven	iven_st	1578884103	[redacted]	51617	internal	[redacted]	3389	RDP over Web	21
⊟ work-computer 1											
□	1379979558	ftai	ftai	1401868579	[redacted]	53909	internal	[redacted]	3389	Remote desktop	2707

A new window opens. The window displays user activity in real-time.


Monitoring iven on [redacted]
FortiClient
HeidiSQL
FortiClient - Zero Trust Fabric Agent
File Help
Command Prompt
0:29

```
Microsoft Windows [Version 10.0.19045.3570]
(c) Microsoft Corporation. All rights reserved.

C:\Users\iven_st>ping 10.59.112.1

Pinging 10.59.112.1 with 32 bytes of data:
Reply from 10.59.112.1: bytes=32 time<1ms TTL=255
Reply from 10.59.112.1: bytes=32 time<1ms TTL=255
Reply from 10.59.112.1: bytes=32 time<1ms TTL=255
Reply from 10.59.112.1: bytes=32 time<1ms TTL=255

Ping statistics for 10.59.112.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\iven_st>_
```

You can terminate an active session by clicking *Disconnect the current secret session* icon on the top-right as you live stream the session.

Log & report

Logging and reporting are valuable components to help you understand what is happening on your network and to inform you about network activities, such as system and user events.

Reports show the recorded activity in a more readable format. A report gathers all the log information that it needs, then presents it in a graphical format with a customizable design and automatically generated charts showing what is happening on the network.

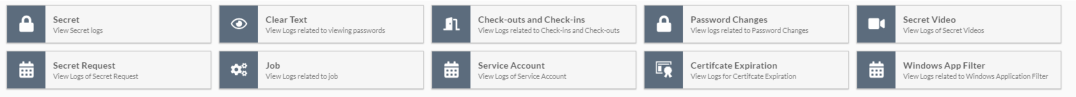
Go to *Log & Report* to access the following tabs:

- Secret on page 312
- Events on page 317
- ZTNA on page 319
- SSH on page 320
- Antivirus on page 322
- Date leak prevention on page 323
- Disk usage on page 324
- Automation on page 325
- Reports on page 336
- Log settings on page 344
- Email alert settings on page 351
- Debug settings on page 353

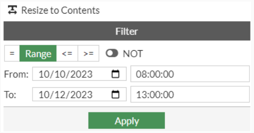
Secret

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

- Secret on page 314
- Clear Text on page 314
- Check-outs and Check-ins on page 314
- Password Changes on page 315
- Secret Video on page 315
- Secret Request on page 316
- Job on page 316
- Service Account on page 316
- Certificate Expiration on page 316
- Windows App Filter on page 316

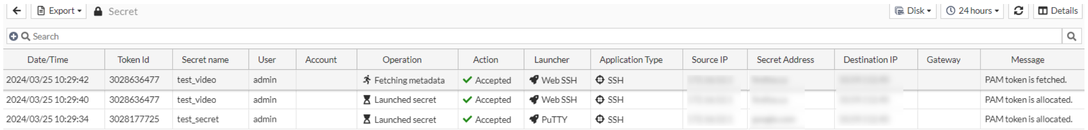

Secret
View Secret logs
Clear Text
View Logs related to viewing passwords
Check-outs and Check-ins
View Logs related to Check-ins and Check-outs
Password Changes
View logs related to Password Changes
Secret Video
View Logs of Secret Videos
Secret Request
View Logs of Secret Request
Job
View Logs related to job
Service Account
View Logs of Service Account
Certifcate Expiration
View Logs for Certifcate Expiration
Windows App Filter
View Logs related to Windows Application Filter

The following options are available in the tabs:

Back (←)	Go back to *Secret*.
Export	From the *Export* dropdown, select to export the logs in the following three formats: - *JSON*: Export the selected secret session log to your computer as a JSON file named as *secret-xyz-YYYY_MM_DD.json* - *CSV*: Export the selected secret session log to your computer as a CSV file named as *secret-xyz-YYYY_MM_DD.csv* - *TEXT*: Export the selected secret session log to your computer as a text file named as *secret-xyz-YYYY_MM_DD.txt*
Log location	Select a source from where to retrieve logs: - *Disk* (default) (FortiPAM) - *FortiAnalyzer* See FortiAnalyzer logging on page 369 for setting up FortiAnalyzer as the remote logging server.
Time frame	From the dropdown, select from the following time filters: - *5 minutes* - *1 hour* - *24 hours* - *7 days* - *Custom* - *View All* **Custom filter** **1.** From the dropdown, select *Custom*. **2.** In the window that opens, you can set combinations of `=`, `Range`, `<=`, `>=`, and `NOT`. **3.** Enter a date and time. **4.** Click *Apply*. For example, to create a range filter that filters and displays all the logs between 8:00 AM on 10th October, 2023 to 1:00 PM on 12th October 2023, we set up a filter that looks like the following:  Resize to Contents Filter = Range <= >= NOT Apply From: 10/10/2023 08:00:00 To: 10/12/2023 13:00:00
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 name	User	Account	Operation	Action	Launcher	Application Type	Source IP	Secret Address	Destination IP	Gateway	Message
2024/03/25 10:29:42	3028636477	test_video	admin		Fetching metadata	✓ Accepted	Web SSH	SSH	[redacted]	[redacted]	[redacted]		PAM token is fetched.
2024/03/25 10:29:40	3028636477	test_video	admin		Launched secret	✓ Accepted	Web SSH	SSH	[redacted]	[redacted]	[redacted]		PAM token is allocated.
2024/03/25 10:29:34	3028177725	test_secret	admin		Launched secret	✓ Accepted	PuTTY	SSH	[redacted]	[redacted]	[redacted]		PAM token is allocated.

where:

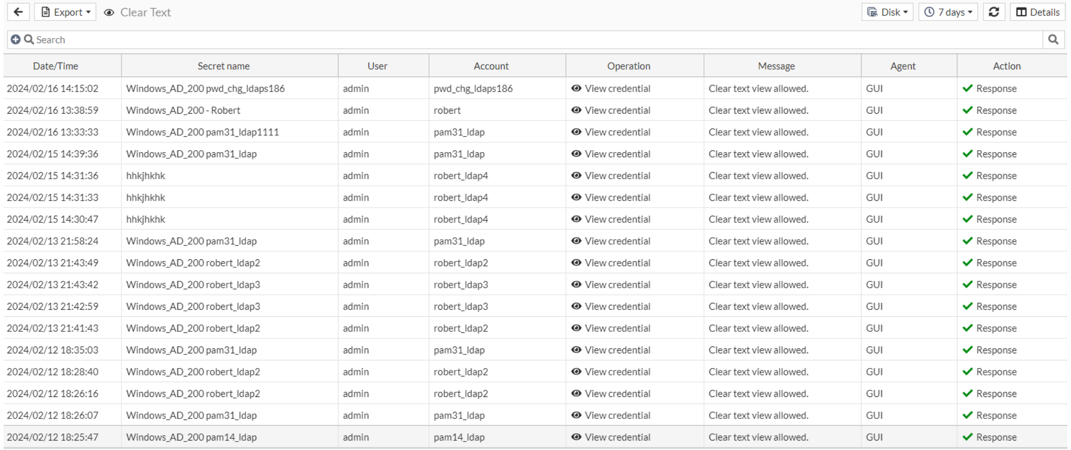
- *Secret Address*: The IP address or FQDN of the actual target server.
- *Gateway*: The gateway name for the secret.
- *Destination IP*: The next hop IP address. If the next hop is FortiPAM, this is the IP address of FortiPAM.

  If the next hop is the actual target server, this is the IP address of the actual target server.

  If the next hop is a gateway, this is the IP address of the gateway.

Clear Text

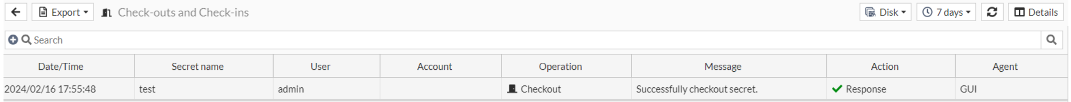
Selecting *Clear Text* shows logs related to viewing passwords. This category of the secret log shows all the information related to the launching of a secret, uploading of a video, termination of a launched session, and status of a FortiPAM token.



Date/Time	Secret name	User	Account	Operation	Message	Agent	Action
2024/02/16 14:15:02	Windows_AD_200 pwd_chg_ldaps186	admin	pwd_chg_ldaps186	View credential	Clear text view allowed.	GUI	✓ Response
2024/02/16 13:38:59	Windows_AD_200 - Robert	admin	robert	View credential	Clear text view allowed.	GUI	✓ Response
2024/02/16 13:33:33	Windows_AD_200 pam31_ldap1111	admin	pam31_ldap	View credential	Clear text view allowed.	GUI	✓ Response
2024/02/15 14:39:36	Windows_AD_200 pam31_ldap	admin	pam31_ldap	View credential	Clear text view allowed.	GUI	✓ Response
2024/02/15 14:31:36	hhkjhkhk	admin	robert_ldap4	View credential	Clear text view allowed.	GUI	✓ Response
2024/02/15 14:31:33	hhkjhkhk	admin	robert_ldap4	View credential	Clear text view allowed.	GUI	✓ Response
2024/02/15 14:30:47	hhkjhkhk	admin	robert_ldap4	View credential	Clear text view allowed.	GUI	✓ Response
2024/02/13 21:58:24	Windows_AD_200 pam31_ldap	admin	pam31_ldap	View credential	Clear text view allowed.	GUI	✓ Response
2024/02/13 21:43:49	Windows_AD_200 robert_ldap2	admin	robert_ldap2	View credential	Clear text view allowed.	GUI	✓ Response
2024/02/13 21:43:42	Windows_AD_200 robert_ldap3	admin	robert_ldap3	View credential	Clear text view allowed.	GUI	✓ Response
2024/02/13 21:42:59	Windows_AD_200 robert_ldap3	admin	robert_ldap3	View credential	Clear text view allowed.	GUI	✓ Response
2024/02/13 21:41:43	Windows_AD_200 robert_ldap2	admin	robert_ldap2	View credential	Clear text view allowed.	GUI	✓ Response
2024/02/12 18:35:03	Windows_AD_200 pam31_ldap	admin	pam31_ldap	View credential	Clear text view allowed.	GUI	✓ Response
2024/02/12 18:28:40	Windows_AD_200 robert_ldap2	admin	robert_ldap2	View credential	Clear text view allowed.	GUI	✓ Response
2024/02/12 18:26:16	Windows_AD_200 robert_ldap2	admin	robert_ldap2	View credential	Clear text view allowed.	GUI	✓ Response
2024/02/12 18:26:07	Windows_AD_200 pam31_ldap	admin	pam31_ldap	View credential	Clear text view allowed.	GUI	✓ Response
2024/02/12 18:25:47	Windows_AD_200 pam14_ldap	admin	pam14_ldap	View credential	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.

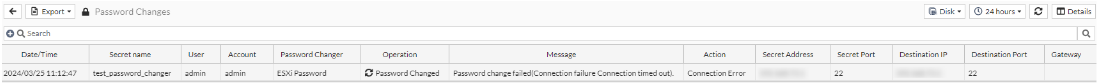


← | Export ▾ | Check-outs and Check-ins | Disk ▾ | 7 days ▾ | Details
Search

Date/Time	Secret name	User	Account	Operation	Message	Action	Agent
2024/02/16 17:55:48	test	admin		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.

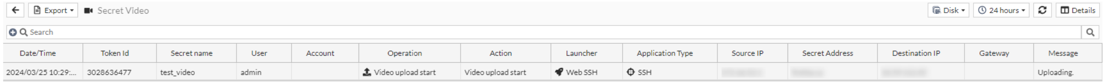


Date/Time	Secret name	User	Account	Password Changer	Operation	Message	Action	Secret Address	Secret Port	Destination IP	Destination Port	Gateway
2024/03/25 11:12:47	test_password_changer	admin	admin	ESXi Password	Password Changed	Password change failed(Connection failure Connection timed out).	Connection Error	[redacted]	22	[redacted]	22	

For some column descriptions, see Secret on page 314.

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.

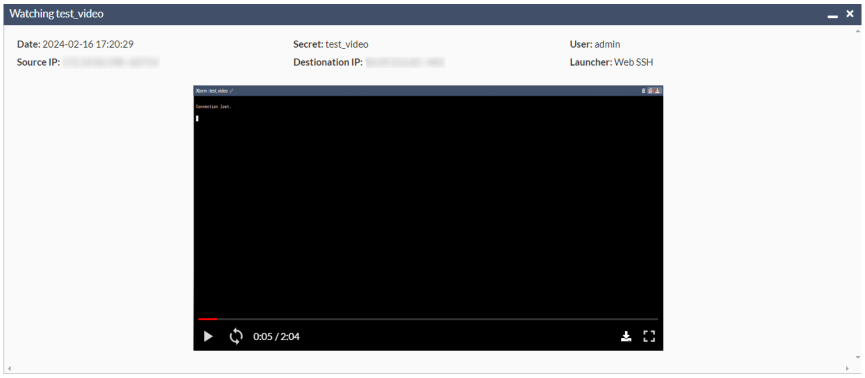


Date/Time	Token Id	Secret name	User	Account	Operation	Action	Launcher	Application Type	Source IP	Secret Address	Destination IP	Gateway	Message
2024/03/25 10:29:...	3028636477	test_video	admin		Video upload start	Video upload start	Web SSH	SSH	[redacted]	[redacted]	[redacted]		Uploading.

To view a recorded video of a launched secret:

1. Select the log with the operation labelled as *Video upload finished*, then click the *Details* button located at the right of the menu.
   Alternatively, double-click the log labelled as *Video upload finished*.

   The video player opens, and the secret video is automatically played.



Date: 2024-02-16 17:20:29
Source IP: [redacted]
Secret: test_video
Destionation IP: [redacted]
User: admin
Launcher: Web SSH

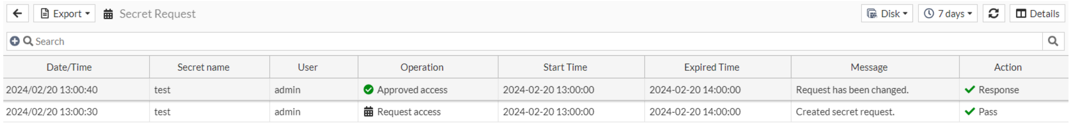
```
Connection lost.
```

To download a recorded video of a launched secret:

1. Select the log with the operation labelled as *Video upload finished*, then click the *Details* button located at the right of the menu.
   Alternatively, double-click the log labelled as *Video upload finished*.
2. From the window that opens, select the download icon (⭳) to save the secret video on your computer in `WebM` format.

Secret Request

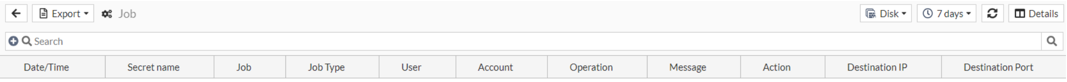
Selecting *Secret Request* shows logs related to secret requests. This category of the secret log shows all the information related to a secret that requires secret approval. It indicates when a request is submitted for a secret or when a request is approved or denied.



Date/Time	Secret name	User	Operation	Start Time	Expired Time	Message	Action
2024/02/20 13:00:40	test	admin	Approved access	2024-02-20 13:00:00	2024-02-20 14:00:00	Request has been changed.	✓ Response
2024/02/20 13:00:30	test	admin	Request access	2024-02-20 13:00:00	2024-02-20 14:00:00	Created secret request.	✓ Pass

Job

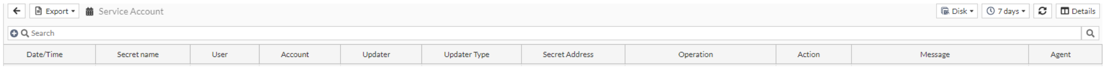
Selecting *Job* shows all logs related to jobs. This category of secret log keeps track of all the events related to an execution of a job on a secret. This includes the job name, the user who initiated the job, the type of the job, and whether the job is executed successfully.



Date/Time	Secret name	Job	Job Type	User	Account	Operation	Message	Action	Destination IP	Destination Port

Service Account

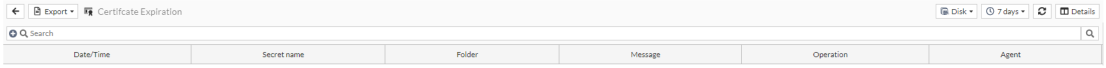
Selecting *Service Account* shows all the logs related to service accounts. This category of the secret log shows information related to updating credentials related to a service account.



Date/Time	Secret name	User	Account	Updater	Updater Type	Secret Address	Operation	Action	Message	Agent

Certificate Expiration

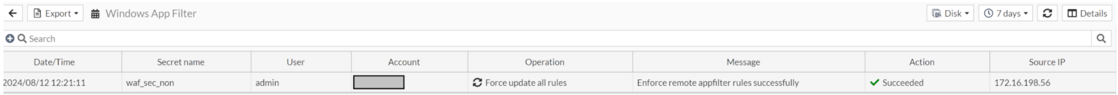
Selecting *Certificate Expiration* shows all the logs related to *Certificate Vault* secret. This category of the secret log shows information related to the certificate status.



Date/Time	Secret name	Folder	Message	Operation	Agent

Windows App Filter

Selecting *Windows App Filter* shows all the logs related to the secret configured with Windows application filter profile. This category of the secret log shows information related to the Windows application filter activities.

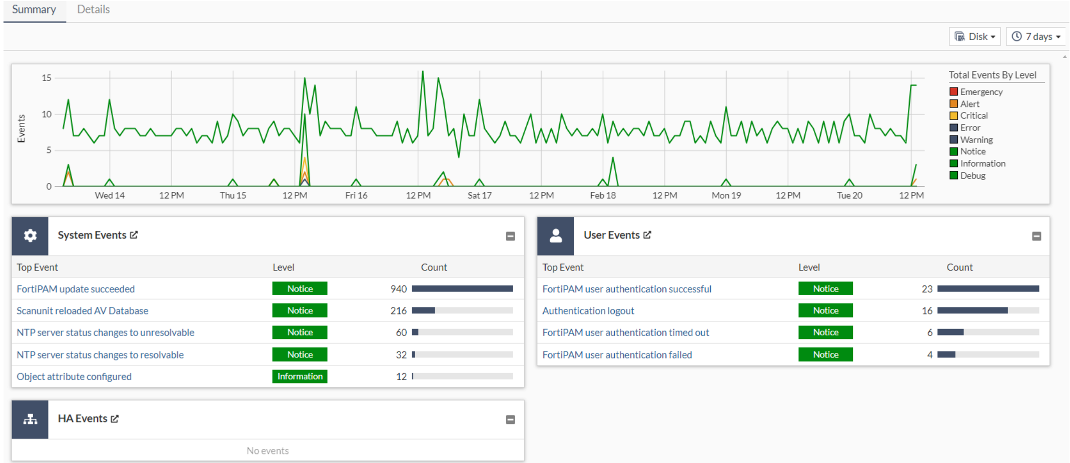


Date/Time	Secret name	User	Account	Operation	Message	Action	Source IP
2024/08/12 12:21:11	waf_sec_non	admin	[redacted]	Force update all rules	Enforce remote appfilter rules successfully	✓ Succeeded	172.16.198.56

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.



System Events

Top Event	Level	Count
FortiPAM update succeeded	Notice	940
Scanunit reloaded AV Database	Notice	216
NTP server status changes to unresolvable	Notice	60
NTP server status changes to resolvable	Notice	32
Object attribute configured	Information	12

User Events

Top Event	Level	Count
FortiPAM user authentication successful	Notice	23
Authentication logout	Notice	16
FortiPAM user authentication timed out	Notice	6
FortiPAM user authentication failed	Notice	4

HA Events

No events

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:

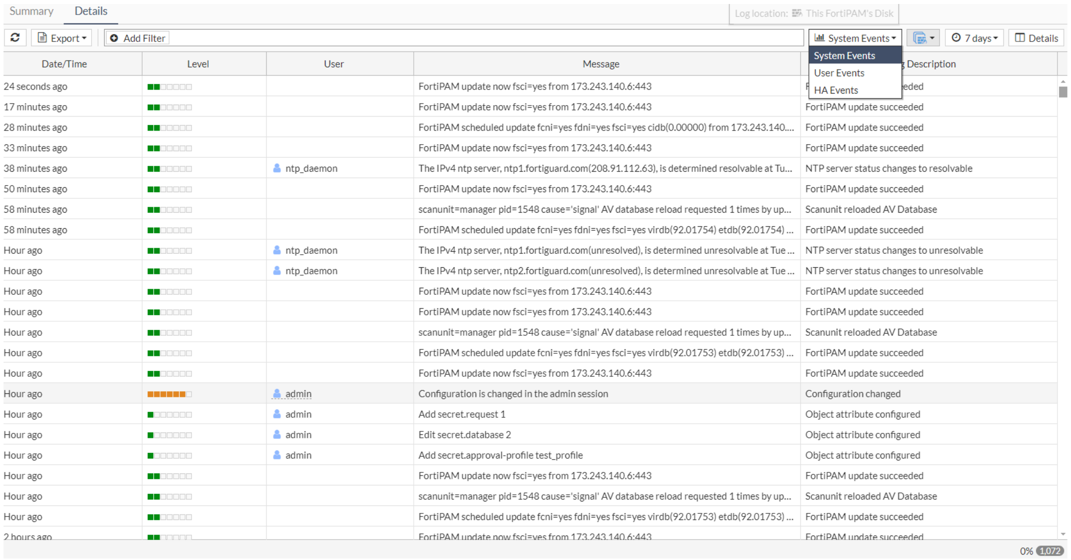
Log location	Logs sourced from the FortiPAM disk only.
Time frame	From the dropdown, select from the following time filters: • *5 minutes* • *1 hour*

	- *24 hours* - *7 days*
System Events	Top system events by count.
User Events	Top user events by count.
HA Events	Top HA events by count.

In *System Events*, *User Events*, or *HA Events* widgets, select an event to open the corresponding details tab with all the logs for the event listed in a table.

- *Details*

The tab displays the related information of each log for a specific event type. The event type can be toggled with the event type dropdown located right of the search bar. Different filters can be added, such as date/time to filter logs in a time range.



Date/Time	Level	User	Message	Description
24 seconds ago	🟩🟩⬜⬜⬜⬜⬜		FortiPAM update now fsci=yes from 173.243.140.6:443	F eded
17 minutes ago	🟩🟩⬜⬜⬜⬜⬜		FortiPAM update now fsci=yes from 173.243.140.6:443	FortiPAM update succeeded
28 minutes ago	🟩🟩⬜⬜⬜⬜⬜		FortiPAM scheduled update fcni=yes fdni=yes fsci=yes cidb(0.00000) from 173.243.140....	FortiPAM update succeeded
33 minutes ago	🟩🟩⬜⬜⬜⬜⬜		FortiPAM update now fsci=yes from 173.243.140.6:443	FortiPAM update succeeded
38 minutes ago	🟩🟩⬜⬜⬜⬜⬜	ntp_daemon	The IPv4 ntp server, ntp1.fortiguard.com(208.91.112.63), is determined resolvable at Tu...	NTP server status changes to resolvable
50 minutes ago	🟩🟩⬜⬜⬜⬜⬜		FortiPAM update now fsci=yes from 173.243.140.6:443	FortiPAM update succeeded
58 minutes ago	🟩🟩⬜⬜⬜⬜⬜		scanunit=manager pid=1548 cause='signal' AV database reload requested 1 times by up...	Scanunit reloaded AV Database
58 minutes ago	🟩🟩⬜⬜⬜⬜⬜		FortiPAM scheduled update fcni=yes fdni=yes fsci=yes virdb(92.01754) etdb(92.01754) ...	FortiPAM update succeeded
Hour ago	🟩🟩⬜⬜⬜⬜⬜	ntp_daemon	The IPv4 ntp server, ntp1.fortiguard.com(unresolved), is determined unresolvable at Tue ...	NTP server status changes to unresolvable
Hour ago	🟩🟩⬜⬜⬜⬜⬜	ntp_daemon	The IPv4 ntp server, ntp2.fortiguard.com(unresolved), is determined unresolvable at Tue ...	NTP server status changes to unresolvable
Hour ago	🟩🟩⬜⬜⬜⬜⬜		FortiPAM update now fsci=yes from 173.243.140.6:443	FortiPAM update succeeded
Hour ago	🟩🟩⬜⬜⬜⬜⬜		FortiPAM update now fsci=yes from 173.243.140.6:443	FortiPAM update succeeded
Hour ago	🟩🟩⬜⬜⬜⬜⬜		scanunit=manager pid=1548 cause='signal' AV database reload requested 1 times by up...	Scanunit reloaded AV Database
Hour ago	🟩🟩⬜⬜⬜⬜⬜		FortiPAM scheduled update fcni=yes fdni=yes fsci=yes virdb(92.01753) etdb(92.01753) ...	FortiPAM update succeeded
Hour ago	🟩🟩⬜⬜⬜⬜⬜		FortiPAM update now fsci=yes from 173.243.140.6:443	FortiPAM update succeeded
Hour ago	🟧🟧🟧🟧🟧🟧⬜	admin	Configuration is changed in the admin session	Configuration changed
Hour ago	🟩⬜⬜⬜⬜⬜⬜	admin	Add secret.request 1	Object attribute configured
Hour ago	🟩⬜⬜⬜⬜⬜⬜	admin	Edit secret.database 2	Object attribute configured
Hour ago	🟩⬜⬜⬜⬜⬜⬜	admin	Add secret.approval-profile test_profile	Object attribute configured
Hour ago	🟩🟩⬜⬜⬜⬜⬜		FortiPAM update now fsci=yes from 173.243.140.6:443	FortiPAM update succeeded
Hour ago	🟩🟩⬜⬜⬜⬜⬜		scanunit=manager pid=1548 cause='signal' AV database reload requested 1 times by up...	Scanunit reloaded AV Database
Hour ago	🟩🟩⬜⬜⬜⬜⬜		FortiPAM scheduled update fcni=yes fdni=yes fsci=yes virdb(92.01753) etdb(92.01753) ...	FortiPAM update succeeded
2 hours ago	🟩🟩⬜⬜⬜⬜⬜		FortiPAM update now fsci=yes from 173.243.140.6:443	FortiPAM update succeeded

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

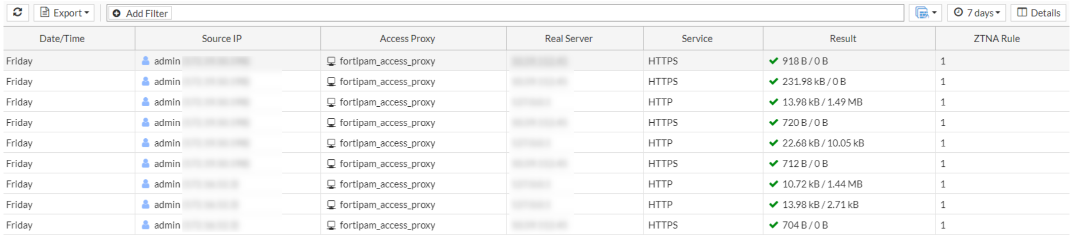
Refresh	To refresh the contents, click the refresh icon.
Export	From the *Export* dropdown, select to export the logs in the following three formats: - *JSON*: Export the selected log to your computer as a JSON file - *CSV*: Export the selected log to your computer as a CSV file - *TEXT*: Export the selected 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.

	Time frame settings for each *Log & Report* page are independent. For example, changing the time frame on the *System Events* page does not automatically change the time frame on the *User Events* and *HA Events* pages.
System Events	From the dropdown, select from the following event types to display: • *System Events* • *User Events* • *HA Events*
Log location	Select a source from where to retrieve logs: • *Disk* (default) (FortiPAM) • *FortiAnalyzer*
Time frame	From the dropdown, select from the following time filters: • *5 minutes* • *1 hour* • *24 hours* • *7 days* • *Custom* • *View All* **Custom filter** **1.** From the dropdown, select *Custom*. **2.** Click the search bar. **3.** Select `<=`, `>=`, or `A-B` (date and time range). **4.** Depending on your selection in step 3, enter a date and time or a date and time range. **5.** Hit `Enter`.
Details	Select a log entry and then select *Details* to see more information about the log.

ZTNA

Go to ZTNA in *Log & Report* to see ZTNA related logs.

The ZTNA log keeps track of ZTNA related traffics. This can include when a ZTNA rule cannot be matched, an API gateway cannot be matched, or when a secret configured with device permission fails to connect.



Date/Time	Source IP	Access Proxy	Real Server	Service	Result	ZTNA Rule
Friday	admin [redacted]	fortipam_access_proxy	[redacted]	HTTPS	✓ 918 B / 0 B	1
Friday	admin [redacted]	fortipam_access_proxy	[redacted]	HTTPS	✓ 231.98 kB / 0 B	1
Friday	admin [redacted]	fortipam_access_proxy	[redacted]	HTTP	✓ 13.98 kB / 1.49 MB	1
Friday	admin [redacted]	fortipam_access_proxy	[redacted]	HTTPS	✓ 720 B / 0 B	1
Friday	admin [redacted]	fortipam_access_proxy	[redacted]	HTTP	✓ 22.68 kB / 10.05 kB	1
Friday	admin [redacted]	fortipam_access_proxy	[redacted]	HTTPS	✓ 712 B / 0 B	1
Friday	admin [redacted]	fortipam_access_proxy	[redacted]	HTTP	✓ 10.72 kB / 1.44 MB	1
Friday	admin [redacted]	fortipam_access_proxy	[redacted]	HTTP	✓ 13.98 kB / 2.71 kB	1
Friday	admin [redacted]	fortipam_access_proxy	[redacted]	HTTPS	✓ 704 B / 0 B	1

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

Refresh	To refresh the contents, click the refresh icon.
Export	From the *Export* dropdown, select to export the ZTNA logs in the following three formats: • *JSON*: Export the selected ZTNA log to your computer as a JSON file • *CSV*: Export the selected ZTNA log to your computer as a CSV file • *TEXT*: 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	Select a source from where to retrieve logs: • *Disk* (default) (FortiPAM) • *FortiAnalyzer*
Time frame	From the dropdown, select from the following time filters: • *5 minutes* • *1 hour* • *24 hours* • *7 days* • *Custom* • *View All* See Custom filter on page 319, for an example on how to set up custom filters.
Details	Select to see details for the selected log entry.

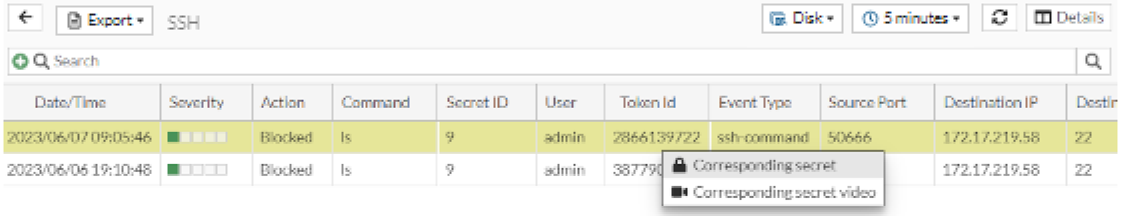
SSH

Go to *SSH* in *Log & Report* to see SSH related logs.

For each SSH log, the following columns are displayed:

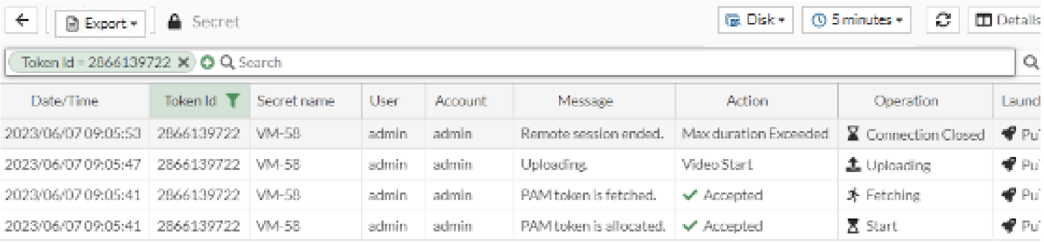
- Date/time
- Severity
- Action
- Command
- Secret ID
- User
- Token Id
- Event Type
- Group
- Source Port
- Destination IP

- Destination Port
- Protocol

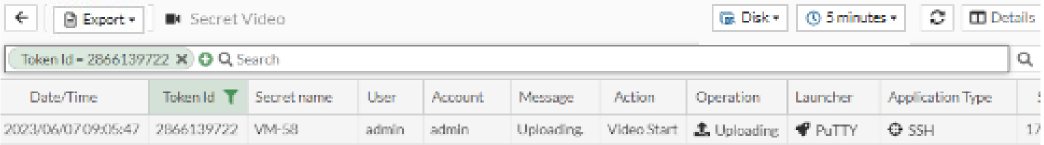


Date/Time	Severity	Action	Command	Secret ID	User	Token Id	Event Type	Source Port	Destination IP	Destir
2023/06/07 09:05:46	■□□□□	Blocked	ls	9	admin	2866139722	ssh-command	50666	172.17.219.58	22
2023/06/06 19:10:48	■□□□□	Blocked	ls	9	admin	38779			172.17.219.58	22

Selecting the *Corresponding secret* or the *Corresponding secret video* buttons when you right-click an SSH log takes you to the corresponding secret log or the secret video log, respectively.



Date/Time	Token Id	Secret name	User	Account	Message	Action	Operation	Laund
2023/06/07 09:05:53	2866139722	VM-58	admin	admin	Remote session ended.	Max duration Exceeded	Connection Closed	Pu
2023/06/07 09:05:47	2866139722	VM-58	admin	admin	Uploading.	Video Start	Uploading	Pu
2023/06/07 09:05:41	2866139722	VM-58	admin	admin	PAM token is fetched.	✓ Accepted	Fetching	Pu
2023/06/07 09:05:41	2866139722	VM-58	admin	admin	PAM token is allocated.	✓ Accepted	Start	Pu



Date/Time	Token Id	Secret name	User	Account	Message	Action	Operation	Launcher	Application Type	
2023/06/07 09:05:47	2866139722	VM-58	admin	admin	Uploading.	Video Start	Uploading	PuTTY	SSH	17

The SSH log keeps track of all the events related to the SSH filter profile. It contains information such as the severity of a command, the destination IP and port used to execute the command, and the action associated with the log. The action may be *Blocked*, indicating the command has been blocked from executing on the secret or *Passthrough*, representing it is allowed to execute on the secret.

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

Back (←)	Go back to *SSH*.
Export	From the *Export* dropdown, select to export the SSH logs in the following three formats: • *JSON*: Export the selected SSH log to your computer as a JSON file named as *secret-xyz-YYYY_MM_DD.json* • *CSV*: Export the selected SSH log to your computer as a CSV file named as *secret-xyz-YYYY_MM_DD.csv* • *TEXT*: Export the selected SSH log to your computer as a text file named as *secret-xyz-YYYY_MM_DD.txt*
Log location	Select a source from where to retrieve logs: • *Disk* (default) (FortiPAM) • *FortiAnalyzer*

Time frame	From the dropdown, select from the following time filters: • *5 minutes* • *1 hour* • *24 hours* • *7 days* • *Custom* See Custom filter on page 313 for an example on how to set up custom filters. • *View All*
Refresh	To refresh the contents, click the refresh icon.
Details	Select to see details for the selected log entry.
Search	Enter a search term in the search field, then hit `Enter` to search the secret video list. To narrow down your search, see Column filter.

Antivirus

Go to *Log & Report* > *Antivirus* to see logs related to antivirus.

The antivirus log records when, during the antivirus scanning process, the FortiPAM unit finds a match within the antivirus profile, which includes the presence of a virus or grayware signature.

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

Refresh	To refresh the contents, click the refresh icon.
Export	From the *Export* dropdown, select to export the antivirus logs in the following three formats: • *JSON*: Export the selected antivirus log to your computer as a JSON file • *CSV*: Export the selected antivirus log to your computer as a CSV file • *TEXT*: Export the selected antivirus 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	Select a source from where to retrieve logs: • *Disk* (default) (FortiPAM) • *FortiAnalyzer*
Time frame	From the dropdown, select from the following time filters: • *5 minutes* • *1 hour* • *24 hours* • *7 days*

	- *Custom* See Custom filter on page 319, for an example on how to set up custom filters. - *View All*
Details	Select to see details for the selected log entry.

Date leak prevention

Go to *Log & Report* > *Data Leak Prevention* to see logs related to DLP.

The data leak prevention (DLP) log provides valuable information about the sensitive data trying to get through to your network as well as any unwanted data trying to get into your network.

The following options are available in the *Data Leak Prevention* tab:

Refresh	To refresh the contents, click the refresh icon.
Export	From the *Export* dropdown, select to export the DLP logs in the following three formats: - *JSON*: Export the selected DLP log to your computer as a JSON file - *CSV*: Export the selected DLP log to your computer as a CSV file - *TEXT*: Export the selected DLP 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	Select a source from where to retrieve logs: - *Disk* (default) (FortiPAM) - *FortiAnalyzer*
Time frame	From the dropdown, select from the following time filters: - *5 minutes* - *1 hour* - *24 hours* - *7 days* - *Custom* See Custom filter on page 319, for an example on how to set up custom filters. - *View All*
Details	Select to see details for the selected log entry.

Disk usage

Go to *Log & Report* > *Disk Usage* to see log and video disk usage information.

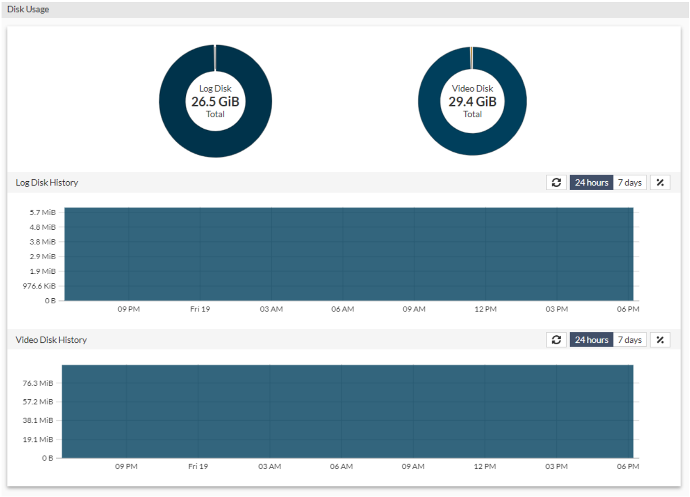
Use the refresh icon to refresh the data in *Log Disk History* and *Video History Disk*.

You can switch between *24 hours* or *7 days* view for *Log Disk History* and *Video Disk History*.

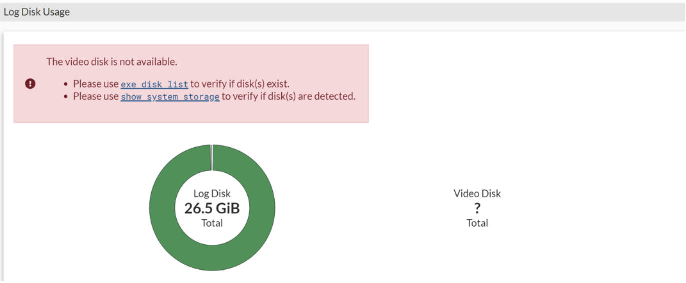
By default:

- *Log Disk History* is displayed as usage vs time.
- *Video Disk History* is displayed as usage vs time.

You can switch the view to percent usage vs time by selecting *%* icon.



When the video disk is unavailable, the following warning is displayed:

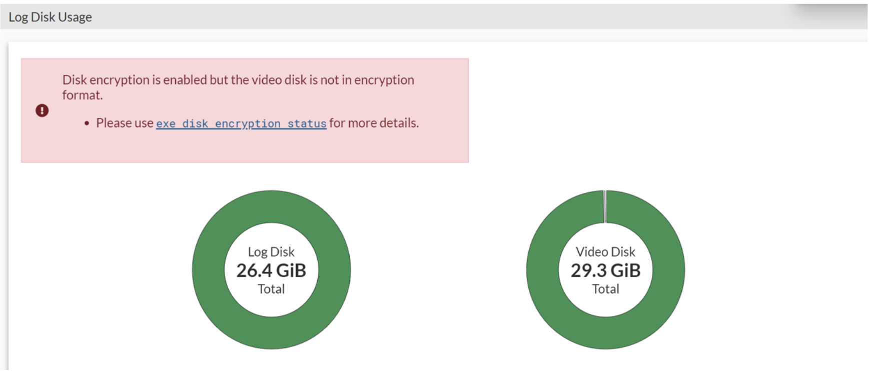


The video disk is not available.

- Please use `exe disk list` to verify if disk(s) exist.
- Please use `show system storage` to verify if disk(s) are detected.

A similar warning is displayed when the log disk is unavailable.

When disk encryption is enabled but the video disk is not in encryption format, the following warning is displayed:



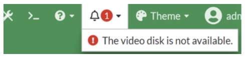
Log Disk Usage

Disk encryption is enabled but the video disk is not in encryption format.

- Please use exe disk encryption status for more details.

You can click the suggested CLI commands to see more disk status information and suggested solutions.

The warning messages originally appear in the notifications dropdown in the FortiPAM banner on the top-right.



The video disk is not available.

You must resolve disk related warnings before performing any task on FortiPAM.

The following lists all the possible warning messages:

Disk not available:

1. Both the log disk and the video disk are not available.
2. The log disk is not available.
3. The video disk is not available.

Disk encryption is not matching:

1. Disk encryption is enabled but none is in encryption format.
2. Disk encryption is enabled but the log disk is not in encryption format.
3. Disk encryption is enabled but the video disk is not in encryption format.
4. Disk encryption is disabled but both are in encryption format.
5. Disk encryption is disabled but the log disk is in encryption format.
6. Disk encryption is disabled but the video disk is in encryption format.

Automation

Go to *Automation* in *Log & Report* to see automation related tabs.

You can monitor secret activities and system events.

See:

- Stitch on page 326
- Trigger on page 333

- Action on page 335

Stitch

Go to *Log & Report* > *Automation* and select the *Stitch* tab to see the automation stitches.

Automation stitches automate the activities between the different components in the Security Fabric, which decreases the response times to security events. Events from any source in the Security Fabric can be monitored, and action responses can be set up to any destination.

The automation settings can be synchronized within the Security Fabric, or can only apply to an individual FortiPAM in the Security Fabric. Automation stitches can only be created on the root FortiPAM in a Security Fabric.

Automation stitches can also be used on FortiPAM devices that are not part of a Security Fabric.

An automation stitch consists of two parts: the trigger and the actions. The trigger is the condition or event on the FortiPAM that activates the action, for example, a specific log, or a failed log in attempt. The action is what the FortiPAM does in response to the trigger.

For each automation stitch, the following columns are displayed by default:

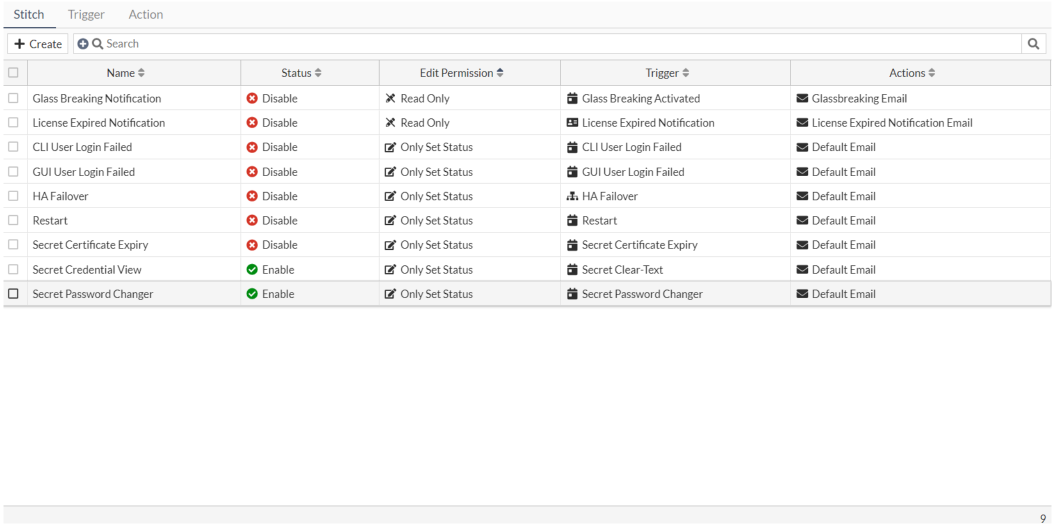
- *Name*
- *Status*
- *Edit Permission*
- *Trigger*
- *Actions*

By default, nine stitches are available:

- *Glass Breaking Notification*
- *License Expired Notification*
- *CLI User Login Failed*
- *GUI User Login Failed*
- *HA Failover*
- *Restart*
- *Secret Certificate Expiry*
- *Secret Credential View*
- *Secret Password Changer*

To use a default automation stitch:

1. Check the action being used by the automation stitch.
2. From the *Action* tab, double-click the action to edit it.
3. Update the recipient email address.



	Name	Status	Edit Permission	Trigger	Actions
□	Glass Breaking Notification	Disable	Read Only	Glass Breaking Activated	Glassbreaking Email
□	License Expired Notification	Disable	Read Only	License Expired Notification	License Expired Notification Email
□	CLI User Login Failed	Disable	Only Set Status	CLI User Login Failed	Default Email
□	GUI User Login Failed	Disable	Only Set Status	GUI User Login Failed	Default Email
□	HA Failover	Disable	Only Set Status	HA Failover	Default Email
□	Restart	Disable	Only Set Status	Restart	Default Email
□	Secret Certificate Expiry	Disable	Only Set Status	Secret Certificate Expiry	Default Email
□	Secret Credential View	Enable	Only Set Status	Secret Clear-Text	Default Email
□	Secret Password Changer	Enable	Only Set Status	Secret Password Changer	Default Email

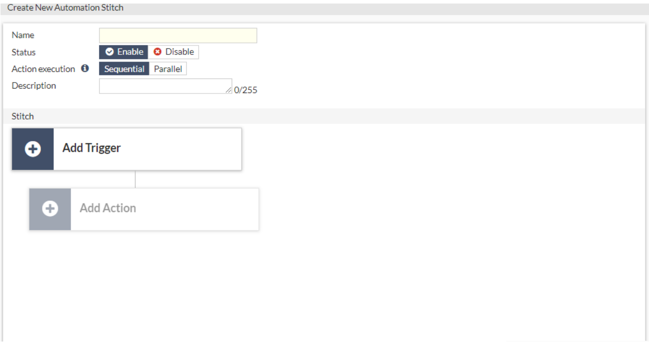
The *Stitch* tab contains the following options:

Create	Select to create a new automation stitch. See Creating an automation stitch on page 328.
Search	Enter a search term in the search field, then hit `Enter`to search the stitches list. To narrow down your search, see Column filter. The following column filters are available: • *Name* • *Status* • *Edit Permission* • *Trigger* • *Actions* • *Description* • *Last Triggered* • *Trigger Count*
Edit	Select to edit the selected automation stitch. **Note**: You cannot edit the default automation stitches.
Enable/Disable	Select to enable/disable the selected automation stitch.
Clone	Select to clone the selected automation stitch.
Delete	Select to delete the selected automation stitch. **Note**: You cannot delete the default automation stitches.

Creating an automation stitch

To create an automation stitch:

1. Go to *Log & Report > Automation*.
2. In the *Stitch* tab, select *Create*.
   The *Create New Automation Stitch* window opens.



3. Enter the following information:

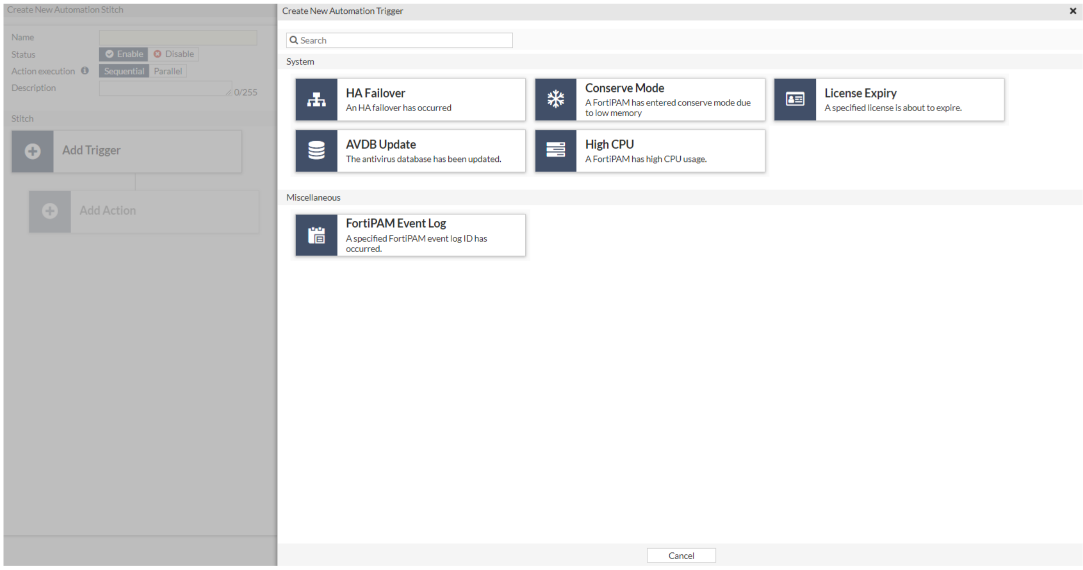
Name	The name of the automation stitch.
Status	Enable/disable the automation stitch.
Action execution	Select from the following two options: • *Sequential*: Actions execute one after another with a delay (if specified). If one action fails, the action chain stops (default). • *Parallel*: All actions execute immediately when the stitch is triggered. Action parameters do not work with parallel execution.
Description	Optionally, add a description for the automation stitch.
Stitch	
Add Trigger	Select, from *Select Entries*, select to add a trigger, and click *Apply*. From the search bar, look up a trigger. Use the pen icon next to a trigger to edit it. You can create new triggers. See Creating new triggers on page 329.
Add Action	Select, from *Select Entries*, select to add an action, and click *Apply*. From the search bar, look up an action. Use the pen icon next to an action to edit it. You can create new actions. See Creating new actions on page 331.

4. Click *OK*.

Creating new triggers

To create a new trigger:

1. In step 3 when Creating an automation stitch, select *Add Trigger*.
2. From *Select Entries*, select *Create*.
   The *Create New Automation Trigger* window opens.


Create New Automation Stitch
Name
Status
Enable
Disable
Action execution
Sequential
Parallel
Description
0/255
Stitch
Add Trigger
Add Action
Create New Automation Trigger
Search
System
HA Failover
An HA failover has occurred
Conserve Mode
A FortiPAM has entered conserve mode due to low memory
License Expiry
A specified license is about to expire.
AVDB Update
The antivirus database has been updated.
High CPU
A FortiPAM has high CPU usage.
Miscellaneous
FortiPAM Event Log
A specified FortiPAM event log ID has occurred.
Cancel

3. From the following options, select one:
   - *System*
     - *HA Failover*: An HA failover occurred.
     - *Conserve Mode*: FortiPAM enters conserve mode due to low memory.
     - *License Expiry*: A specified license is about to expire.
     - *AVDB Update*: The antivirus database is updated.
     - *High CPU*: FortiPAM high CPU usage.
   - *Miscellaneous*
     - *FortiPAM Event Log*: A specified FortiPAM event log ID occurred.

From the search bar, look up a trigger category.

4. Enter the following information:

Name	The name of the of the trigger.
Description	Optionally, enter a description.
License Expiry **Note**: The pane is only available when the *License Expiry* is selected from the category.	
License	Select from the following: • *FortiCare Support* • *FortiGuard AntiVirus* • *FortiGuard Management Service* • *FortiGuard Logs* • *FortiPAM Subscription* • *Any*
FortiPAM Event Log	

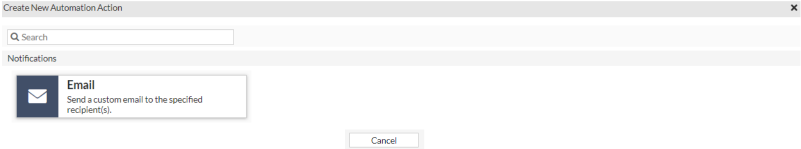
Note: The pane is only available the *FortiPAM Event Log* is selected from the category.	
Event	Select +, from *Select Entries*, select an event. From the search bar, look up an event.
Field filter (s)	Select +, enter field name.
Value	Enter a field value.

5. Click *OK*.

Creating new actions

To create a new action:

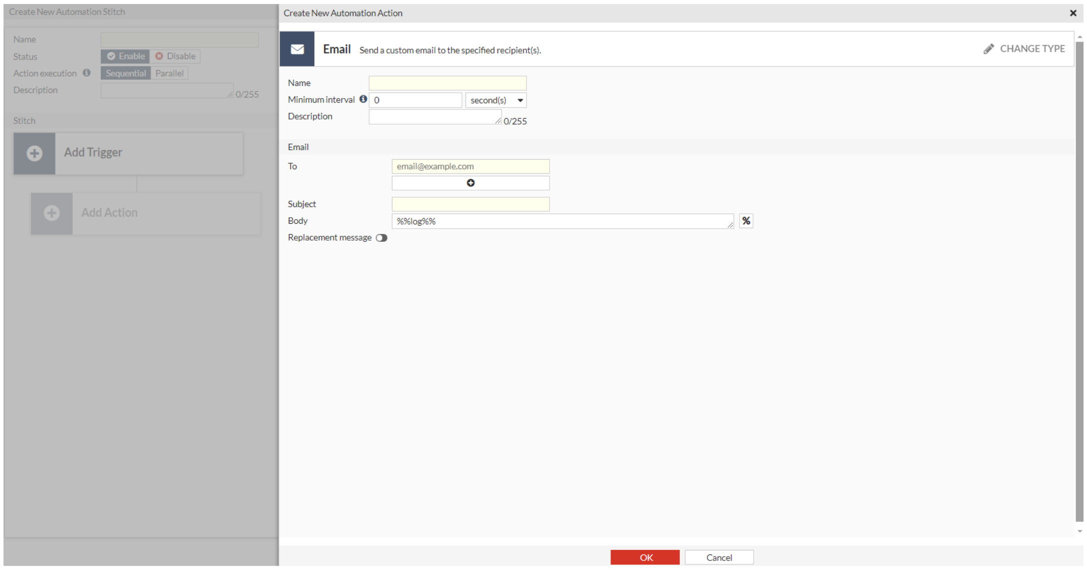
1. In step 3 when Creating an automation stitch, select *Add Action*.
2. From *Select Entries*, select *Create*.
   The *Create New Automation Action* window opens.



Create New Automation Action

3. From the *Notifications* pane, select *Email*.
   Selecting *Email* allows you to send custom emails to the specified recipients.

   An updated *Create New Automation Action* window opens.



Create New Automation Stitch

Name
Status: Enable | Disable
Action execution: Sequential | Parallel
Description 0/255

Stitch

Create New Automation Action

Email Send a custom email to the specified recipient(s).

Name
Minimum interval: 0 second(s)
Description 0/255

Email
To: email@example.com
Subject
Body: %%log%%
Replacement message

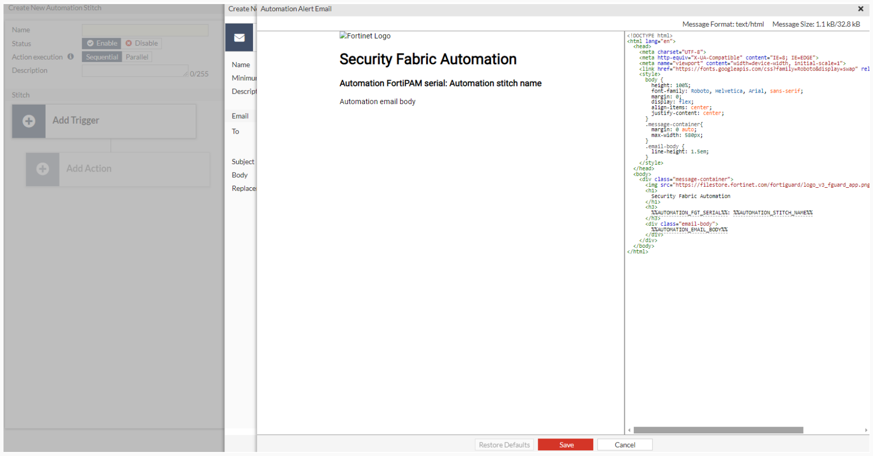
4. Enter the following information:

Name	The name of the automation action.

<table>
<tr><td><b>Minimum interval</b></td><td>Enter a time interval in hour(s)/minute(s)/second(s)
Action triggered once within the time interval.</td></tr>
<tr><td><b>Description</b></td><td>Optionally, enter a description.</td></tr>
<tr><td><b>Email</b></td><td></td></tr>
<tr><td><b>To</b></td><td>Enter the recipient email address.
Select + to add additional recipients.</td></tr>
<tr><td><b>Subject</b></td><td>Enter a subject for the email.</td></tr>
<tr><td><b>Body</b></td><td>Enter the message for the email.
<b>Note</b>: The field can use parameters from logs or previous action results.
Wrapping the parameter with <code>%%</code> replaces the expression with the JSON value for that parameter.
Click <code>%</code> to see examples on how to add parameters to the body.
Click <i>Return</i> to return to the previous window.
- Examples
<table>
<tr><td><code>%%log%%</code></td><td>All fields from the log or FortiAnalyzer event triggering this stitch.</td></tr>
<tr><td><code>%%results%%</code></td><td>The complete result from previous action, such as CLI script.</td></tr>
<tr><td><code>%%results.source%%</code></td><td>The "source" property from the previous action.</td></tr>
<tr><td><code>%%results[aws_ban_ip].source%%</code></td><td>The "source" property from the results of a previous action named "aws_ban_ip".</td></tr>
<tr><td><code>%%results.sources.1%%</code></td><td>The first index value in the array "sources" from the previous action.</td></tr>
<tr><td><code>%%results.email.from%%</code></td><td>The "from" property of an email object from the previous action.</td></tr>
<tr><td><code>%%log.srcip%%</code></td><td>The "srcip" field from the log or FortiAnalyzer event triggering this stitch.</td></tr>
</table></td></tr>
<tr><td><b>Replacement message</b></td><td>Enable and click <i>Edit</i> to add a replacement message:
Click <code>%</code> to see examples on how to add parameters to the body.
Click <i>Return</i> to return to the previous window.</td></tr>
</table>

For examples on adding parameters to replacement message, see Examples on page 332.

A new window opens:



Security Fabric Automation

Automation FortiPAM serial: Automation stitch name

Automation email body

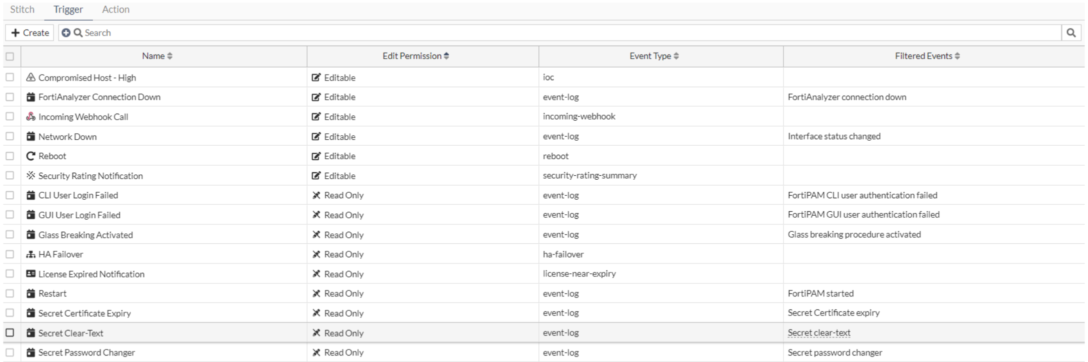
```
<!DOCTYPE html>
<html lang="en">
  <head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=8; IE=EDGE">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <link href="https://fonts.googleapis.com/css?family=Roboto&display=swap" rel
    <style>
      body {
        height: 100%;
        font-family: Roboto, Helvetica, Arial, sans-serif;
        margin: 0;
        display: flex;
        align-items: center;
        justify-content: center;
      }
      .message-container{
        margin: 0 auto;
        max-width: 580px;
      }
      .email-body {
        line-height: 1.5em;
      }
    </style>
  </head>
  <body>
    <div class="message-container">
      <img src="https://filestore.fortinet.com/fortiguard/logo_v3_fguard_app.png
      <h1>
        Security Fabric Automation
      </h1>
      <h3>
        %%AUTOMATION_FGT_SERIAL%%: %%AUTOMATION_STITCH_NAME%%
      </h3>
      <div class="email-body">
        %%AUTOMATION_EMAIL_BODY%%
      </div>
    </div>
  </body>
</html>
```

1. You can edit the replacement message by editing the HTML code. The preview appears in the left window.
2. Click *Save*.
   Click *Restore Defaults* if you want to restore the default replacement message.

5. Click *OK*.

Trigger

Go to *Log & Report* > *Automation* and select the *Trigger* tab to see the triggers.



□	Name	Edit Permission	Event Type	Filtered Events
□	Compromised Host - High	Editable	ioc	
□	FortiAnalyzer Connection Down	Editable	event-log	FortiAnalyzer connection down
□	Incoming Webhook Call	Editable	incoming-webhook	
□	Network Down	Editable	event-log	Interface status changed
□	Reboot	Editable	reboot	
□	Security Rating Notification	Editable	security-rating-summary	
□	CLI User Login Failed	Read Only	event-log	FortiPAM CLI user authentication failed
□	GUI User Login Failed	Read Only	event-log	FortiPAM GUI user authentication failed
□	Glass Breaking Activated	Read Only	event-log	Glass breaking procedure activated
□	HA Failover	Read Only	ha-failover	
□	License Expired Notification	Read Only	license-near-expiry	
□	Restart	Read Only	event-log	FortiPAM started
□	Secret Certificate Expiry	Read Only	event-log	Secret Certificate expiry
□	Secret Clear-Text	Read Only	event-log	Secret clear-text
□	Secret Password Changer	Read Only	event-log	Secret password changer

For each trigger, the following columns are displayed by default:

- *Name*
- *Edit Permission*
- *Event Type*
- *Filtered Events*

The following describes the default triggers:

Trigger	Description
Compromised Host	An indicator of compromise (IoC) is detected on a host endpoint. The threat level must be selected and can be Medium or High. If Medium is selected, both medium and high level threats are included. Additional actions are available only for Compromised Host triggers: • Access Layer Quarantine • FortiClient Quarantine • VMware NSX Security Tag • IP Ban
FortiAnalyzer Connection Down	An event has occurred on a specific Fabric connector.
Incoming Webhook Call	An incoming webhook has been triggered.
Network Down	A network connection is down.
Reboot	FortiPAM rebooting.
Security Rating Notification	Security rating report available.
CLI User Login Failed	SSH login failed event trigger.
GUI User Login Failed	GUI login failed event trigger.
Glass Breaking Activated	When a user activates the glass breaking mode.
HA Failover	An HA failover has occurred.
License Expired Notification	When a license is near expiration.
Restart	System restarts.
Secret Certificate Expiry	The secret certificate expiry event trigger.
Secret Clear-Text	The secret credential clear text event trigger.
Secret Password Changer	The secret password changing event trigger.

The *Trigger* tab contains the following options:

Create	Select to create a new trigger. See Creating a trigger on page 335.
Search	Enter a search term in the search field, then hit `Enter`to search triggers list. To narrow down your search, see Column filter. The following column filters are available: • *Name* • *Edit Permission* • *Event Type* • *Filtered Events* • *Description* • *References*

	• *Trigger Type*
Edit	Select to edit the selected trigger.
Clone	Select to clone the selected trigger.
Delete	Select to delete the selected trigger.

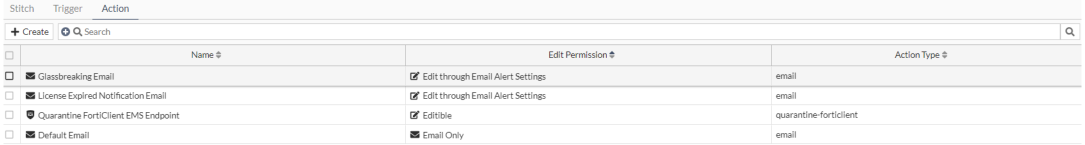
Creating a trigger

To create a trigger:

1. Go to *Log & Report > Automation* and select the *Trigger* tab.
2. In the *Trigger* tab, select *Create*.
   The *Create New Automation Trigger* window opens.
3. Follow from steps 3 in Creating new triggers on page 329.

Action

Go to *Log & Report > Automation* and select the *Action* tab to see the actions.



☐	Name	Edit Permission	Action Type
☐	Glassbreaking Email	Edit through Email Alert Settings	email
☐	License Expired Notification Email	Edit through Email Alert Settings	email
☐	Quarantine FortiClient EMS Endpoint	Editible	quarantine-forticlient
☐	Default Email	Email Only	email

The following four default actions are available:

- *Glassbreaking Email*
- *License Expired Notification Email*
- *Quarantine FortiClient EMS Endpoint*
- *Default Email*

For each action, the following columns are displayed by default:

- *Name*
- *Edit Permission*
- *Action Type*

The *Action* tab contains the following options:

Create	Select to create a new action. See Creating an action on page 336.
Search	Enter a search term in the search field, then hit `Enter`to search actions list. To narrow down your search, see Column filter. The following column filters are available: • *Name* • *Edit Permission* • *Action Type*

	• *Description* • *Last Triggered* • *References* • *Trigger Count*
Edit	Select to edit the selected action.
Clone	Select to clone the selected action.
Delete	Select to delete the selected action.

Creating an action

To create an action:

1. Go to *Log & Report* > *Automation* and select the *Action* tab.
2. In the *Action* tab, select *Create*.
   The *Create New Automation Action* window opens.
3. Follow from steps 3 in Creating new actions on page 331.

Reports

Go to *Log & Reports* > *Reports* to access the following:

- General on page 336
- Secret audit on page 343

General

In *General*, you can generate and view general FortiPAM reports. You can also customize the report layout and schedule the generation of reports.

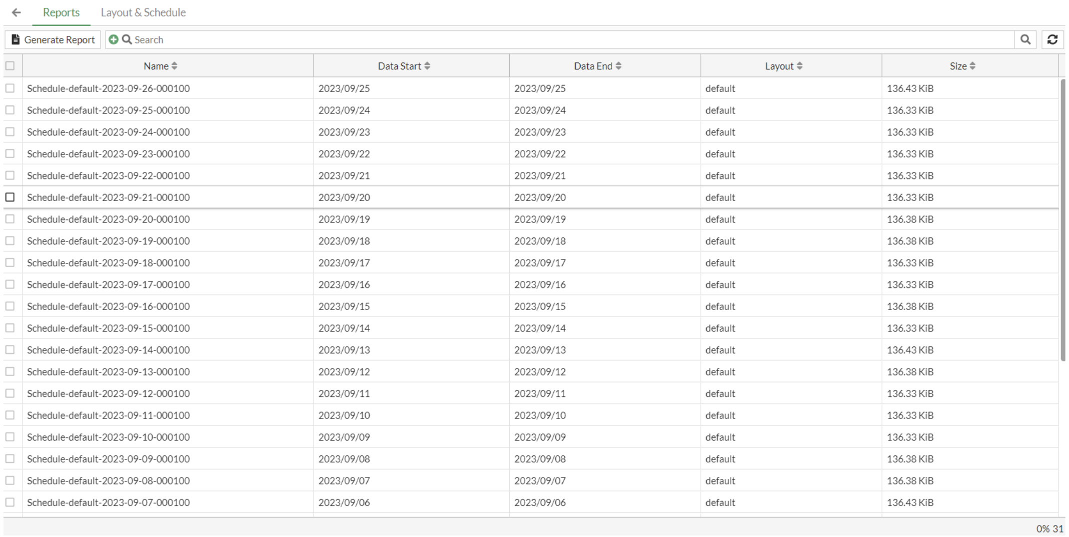
The following two tabs are available in *General*:

- Reports on page 336
- Layout & schedule on page 338

Reports

Reports displays a list of audit reports generated to comply with audit requirements.

For each report entry; name, data start, data end, layout, and the size are displayed.



□	Name	Data Start	Data End	Layout	Size
□	Schedule-default-2023-09-26-000100	2023/09/25	2023/09/25	default	136.43 KiB
□	Schedule-default-2023-09-25-000100	2023/09/24	2023/09/24	default	136.33 KiB
□	Schedule-default-2023-09-24-000100	2023/09/23	2023/09/23	default	136.33 KiB
□	Schedule-default-2023-09-23-000100	2023/09/22	2023/09/22	default	136.33 KiB
□	Schedule-default-2023-09-22-000100	2023/09/21	2023/09/21	default	136.33 KiB
□	Schedule-default-2023-09-21-000100	2023/09/20	2023/09/20	default	136.33 KiB
□	Schedule-default-2023-09-20-000100	2023/09/19	2023/09/19	default	136.38 KiB
□	Schedule-default-2023-09-19-000100	2023/09/18	2023/09/18	default	136.38 KiB
□	Schedule-default-2023-09-18-000100	2023/09/17	2023/09/17	default	136.33 KiB
□	Schedule-default-2023-09-17-000100	2023/09/16	2023/09/16	default	136.33 KiB
□	Schedule-default-2023-09-16-000100	2023/09/15	2023/09/15	default	136.38 KiB
□	Schedule-default-2023-09-15-000100	2023/09/14	2023/09/14	default	136.33 KiB
□	Schedule-default-2023-09-14-000100	2023/09/13	2023/09/13	default	136.43 KiB
□	Schedule-default-2023-09-13-000100	2023/09/12	2023/09/12	default	136.38 KiB
□	Schedule-default-2023-09-12-000100	2023/09/11	2023/09/11	default	136.33 KiB
□	Schedule-default-2023-09-11-000100	2023/09/10	2023/09/10	default	136.33 KiB
□	Schedule-default-2023-09-10-000100	2023/09/09	2023/09/09	default	136.33 KiB
□	Schedule-default-2023-09-09-000100	2023/09/08	2023/09/08	default	136.38 KiB
□	Schedule-default-2023-09-08-000100	2023/09/07	2023/09/07	default	136.38 KiB
□	Schedule-default-2023-09-07-000100	2023/09/06	2023/09/06	default	136.43 KiB

0% 31

A report generated using the default layout includes:

- 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

The *Reports* tab contains the following options:

Generate Report	Select *Generate Report*, from the *Layout* dropdown select a report layout, and click *OK*.

	Use the search bar to look up a report layout.
Search	Enter a search term in the search field, then hit `Enter` to search the reports list. To narrow down your search, see Column filter.
Refresh	To refresh the contents, click the refresh icon.

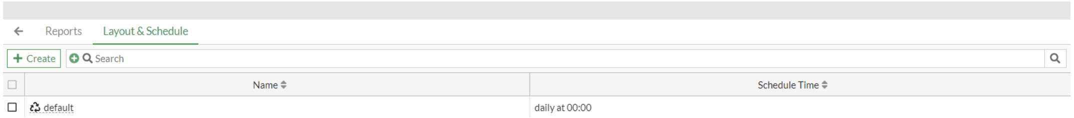
The following options are available for each of the generated report:

View	Select to view the selected report.
Download	Select to export the selected report to your computer as a pdf file.
Delete	Select to delete the selected reports.

Layout & schedule

FortiPAM allows you to customize reports to display attributes according to your preference and schedule generation of reports.

The *Layout & Schedule* tab looks like the following:



	Name	Schedule Time
□	default	daily at 00:00

A *default* layout and schedule is available.

The default layout and schedule generates a comprehensive report daily at 12:00 AM (midnight) with information on user login, system, and secret.

This report is only available on FortiPAM and is not sent out as an email.

By using filters, you now only keep relevant information in the report. The *Add Filter* dropdown shows available filter types for a table.

You can add the same or different filters multiple times.

Note that using the same filter generates union (or) results while different filters generate intersection (and) results.

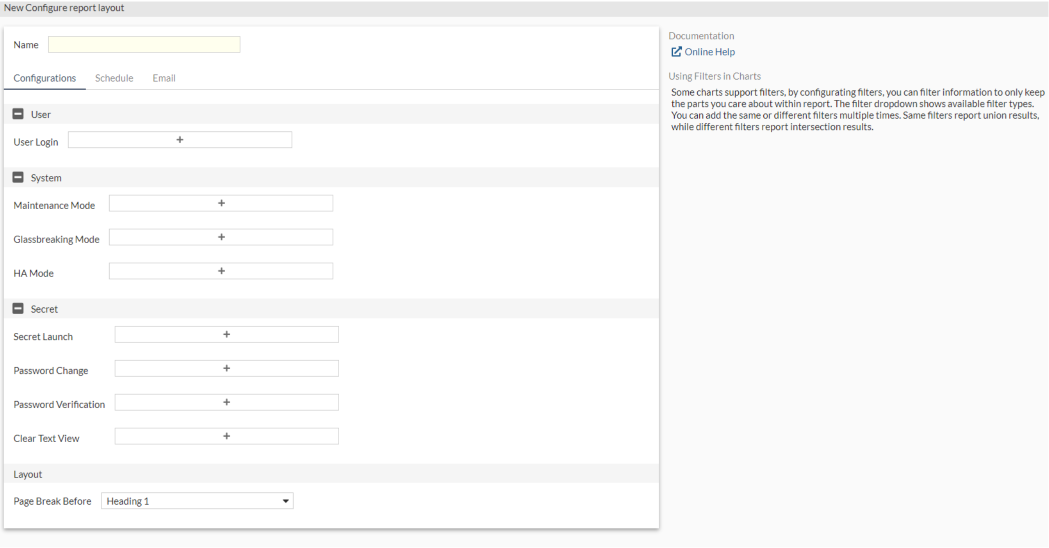
The *Layout & Schedule* tab contains the following options:

Create	Select to create a new report layout and schedule. See Creating a report layout and schedule on page 339.
Search	Enter a search term in the search field, then hit `Enter` to search the layout and schedule list. To narrow down your search, see Column filter.

Creating a report layout and schedule

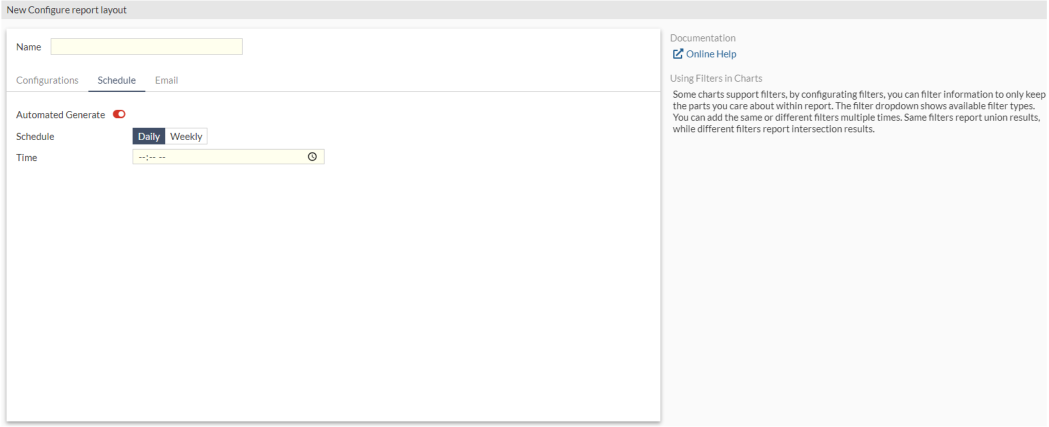
To create a report layout and schedule:

1. Go to *Log & Report* > *Reports* and select *General*.
2. Switch to the *Layout & Schedule* tab and select *Create*.
   The *New Configure report layout* window opens.

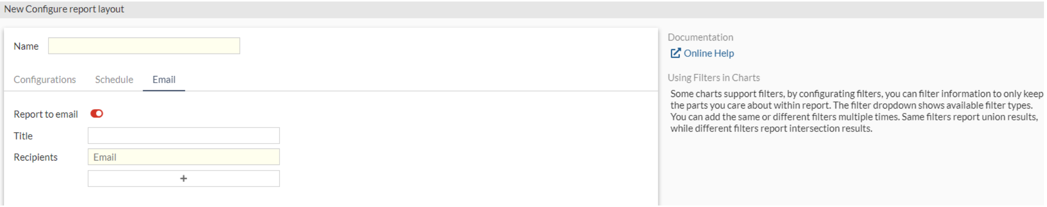


Some charts support filters, by configurating filters, you can filter information to only keep the parts you care about within report. The filter dropdown shows available filter types. You can add the same or different filters multiple times. Same filters report union results, while different filters report intersection results.

3. To switch to either *Schedule* and *Email* tab, select the tab.



Some charts support filters, by configurating filters, you can filter information to only keep the parts you care about within report. The filter dropdown shows available filter types. You can add the same or different filters multiple times. Same filters report union results, while different filters report intersection results.



Some charts support filters, by configurating filters, you can filter information to only keep the parts you care about within report. The filter dropdown shows available filter types. You can add the same or different filters multiple times. Same filters report union results, while different filters report intersection results.

4. Enter the following information:

Name	The name of the custom report layout and schedule.

	Only alphanumeric characters are allowed.
Configurations The report layout configurations.	
User Login	Select +, and from the dropdown, select a table to add: • *Summary* • *Top Success* • *Top Failure* • *Top Failure By Reason* For additional tables, select + and from the dropdown, select a table. You can add filters for the *Top Failure By Reason* table.
Maintenance Mode	Select +, and from the dropdown, select a table to add: • *Summary* • *Top Activations By User* For additional tables, select + and from the dropdown, select a table.
Glassbreaking Mode	Select +, and from the dropdown, select a table to add: • *Summary* • *Top Activations By User* For additional tables, select + and from the dropdown, select a table.
HA Mode	Select +, and from the dropdown, select a table to add: • *Summary* For additional tables, select + and from the dropdown, select a table.
Secret Launch	Select +, and from the dropdown, select a table to add: • *Summary* • *Top Success By Secret* • *Top Success By Secret and User* For additional tables, select + and from the dropdown, select a table. You can add filters for the following tables: • *Top Success By Secret*: Filter by *Secret*, *Target*, and *Folder*. • *Top Success By Secret and User*: Filter by *Secret*, *Target*, *Folder*, and *User*.
Password Change	Select +, and from the dropdown, select a table to add: • *Summary* • *Top Success By Secret* • *Top Success By Secret and User*

	• *Top Failure By Secret* • *Top Failure By Secret and Reason* • *Top Failure By Secret, User and Reason* For additional tables, select + and from the dropdown, select a table. You can add filters for the following tables: • *Top Success By Secret*: Filter by *Secret*, *Target*, and *Folder*. • *Top Success by Secret and User*: Filter by *Secret*, *Target*, *Folder*, and *User*. • *Top Failure By Secret*: Filter by *Secret*, *Target*, and *Folder*. • *Top Failure By Secret and Reason*: Filter by *Secret*, *Target*, *Folder*, and *Reason*. • *Top Failure By Secret, User and Reason*: Filter by *Secret*, *Target*, *Folder*, *User*, and *Reason*.
Password Verification	Select +, and from the dropdown, select a table to add: • *Summary* • *Top Success By Secret* • *Top Success By Secret and User* • *Top Failure By Secret* • *Top Failure By Secret and Reason* • *Top Failure By Secret, User and Reason* For additional tables, select + and from the dropdown, select a table. You can add filters for the following tables: • *Top Success By Secret*: Filter by *Secret*, *Target*, and *Folder*. • *Top Success by Secret and User*: Filter by *Secret*, *Target*, *Folder*, and *User*. • *Top Failure By Secret*: Filter by *Secret*, *Target*, and *Folder*. • *Top Failure By Secret and Reason*: Filter by *Secret*, *Target*, *Folder*, and *Reasons*. • *Top Failure By Secret, User and Reason*: Filter by *Secret*, *Target*, *Folder*, *User*, and *Reason*.
Clear Text View	Select +, and from the dropdown, select a table to add: • *Summary* • *Top View By Secret* • *Top View By Secret and User* For additional tables, select + and from the dropdown, select a table. You can add filters for the following tables: • *Top View By Secret*: Filter by *Secret*, *Target*, and *Folder*. • *Top View By Secret and User*: Filter by *Secret*, *Target*, *Folder*, and *User*.

Page Break Before	Add a page break before one of the following heading levels: • *Heading 1* (default) • *Heading 2* • *Heading 3*
Schedule Schedule for generating reports.	
Automated Generate	Enable/disable scheduled report generation. **Note**: The option is disabled by default.
Schedule	Select a frequency for automatic scheduled report generation: • *Daily* (default) • *Weekly*
Day	Select a day of the week. **Note**: The option is only available when *Schedule* is *Weekly*.
Time	Enter the time or select the clock icon and then select the time from the dropdown.
Email Report related email alerts.	
Report to Email	Enable/disable sending reports to the specified email. ⚠ Before enabling the option, you must configure an email messaging server in *System* > *Settings* and set up *Email Alert Settings*. See Email alert settings on page 351 **Note**: The option is disabled by default.
Title	The email subject starts with the title entered here.
Recipients	The recipient email addresses. Select + to include additional email addresses.

5. Click *Submit*.

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.
```

CLI configuration to add filters to a table - example

```
config report layout
 edit default
  config body-item #Configure report body items.
  edit 2023 #Secret Launch- Top Success By Secret and User.
  config parameters
   edit 1
    set name "secret" #Add filter for the secret.
    set value "test_secret" #Secret name.
   next
   edit 2
    set name "user"
    set value "test_user"
   next
  end
 end
end
```

Secret audit

Secret Audit displays a list secret audit reports.

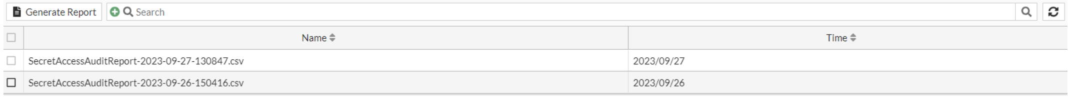
Secret audit reports make it easier for the management to understand the permission distribution of each secret in the system so that when users change, they can accurately and quickly grasp the addition and deletion of permissions. At the same time, it also allows auditors to globally observe the distribution of permissions of each user and the apparent ownership of each key.

A secret audit report contains the following information about each secret:

- target server
- user account accessing the secret
- folder where the secret resides
- secret name
- user/user group with access to the secret
- secret access permission level for the user accessing the secret

For each report entry; the report name and the date when the report was generated is displayed.

The report name follows the following naming convention:
`SecretAccessAuditReport-YYYY-MM-DD-HHMMSS.csv`



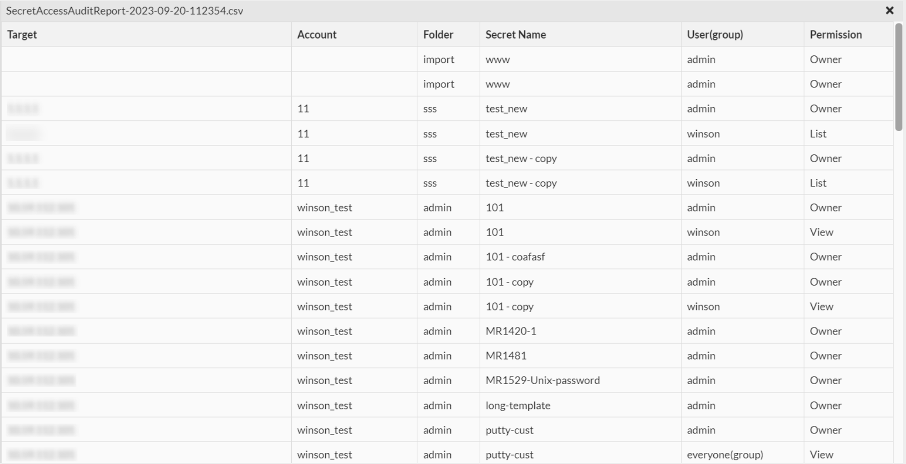
☐	Name	Time
☐	SecretAccessAuditReport-2023-09-27-130847.csv	2023/09/27
☐	SecretAccessAuditReport-2023-09-26-150416.csv	2023/09/26

The *Secret Audit* tab includes the following options:

Generate Report	Select *Generate Report* to generate a new secret audit report.

Search	Enter a search term in the search field, then hit `Enter` to search the reports list. To narrow down your search, see Column filter.
Refresh	To refresh the contents, click the refresh icon.

The following options are available for each of the generated report:

<table>
<tr><td><b>View</b></td><td>Select to view the selected report.
When viewed from within FortiPAM, a secret audit report looks like the following:

SecretAccessAuditReport-2023-09-20-112354.csv
<table>
<tr><th>Target</th><th>Account</th><th>Folder</th><th>Secret Name</th><th>User(group)</th><th>Permission</th></tr>
<tr><td></td><td></td><td>import</td><td>www</td><td>admin</td><td>Owner</td></tr>
<tr><td></td><td></td><td>import</td><td>www</td><td>admin</td><td>Owner</td></tr>
<tr><td>[redacted]</td><td>11</td><td>sss</td><td>test_new</td><td>admin</td><td>Owner</td></tr>
<tr><td>[redacted]</td><td>11</td><td>sss</td><td>test_new</td><td>winson</td><td>List</td></tr>
<tr><td>[redacted]</td><td>11</td><td>sss</td><td>test_new - copy</td><td>admin</td><td>Owner</td></tr>
<tr><td>[redacted]</td><td>11</td><td>sss</td><td>test_new - copy</td><td>winson</td><td>List</td></tr>
<tr><td>[redacted]</td><td>winson_test</td><td>admin</td><td>101</td><td>admin</td><td>Owner</td></tr>
<tr><td>[redacted]</td><td>winson_test</td><td>admin</td><td>101</td><td>winson</td><td>View</td></tr>
<tr><td>[redacted]</td><td>winson_test</td><td>admin</td><td>101 - coafasf</td><td>admin</td><td>Owner</td></tr>
<tr><td>[redacted]</td><td>winson_test</td><td>admin</td><td>101 - copy</td><td>admin</td><td>Owner</td></tr>
<tr><td>[redacted]</td><td>winson_test</td><td>admin</td><td>101 - copy</td><td>winson</td><td>View</td></tr>
<tr><td>[redacted]</td><td>winson_test</td><td>admin</td><td>MR1420-1</td><td>admin</td><td>Owner</td></tr>
<tr><td>[redacted]</td><td>winson_test</td><td>admin</td><td>MR1481</td><td>admin</td><td>Owner</td></tr>
<tr><td>[redacted]</td><td>winson_test</td><td>admin</td><td>MR1529-Unix-password</td><td>admin</td><td>Owner</td></tr>
<tr><td>[redacted]</td><td>winson_test</td><td>admin</td><td>long-template</td><td>admin</td><td>Owner</td></tr>
<tr><td>[redacted]</td><td>winson_test</td><td>admin</td><td>putty-cust</td><td>admin</td><td>Owner</td></tr>
<tr><td>[redacted]</td><td>winson_test</td><td>admin</td><td>putty-cust</td><td>everyone(group)</td><td>View</td></tr>
</table>
</td></tr>
<tr><td><b>Download</b></td><td>Select to export the selected report to your computer as a csv file.</td></tr>
<tr><td><b>Delete</b></td><td>Select to delete the selected reports.</td></tr>
</table>

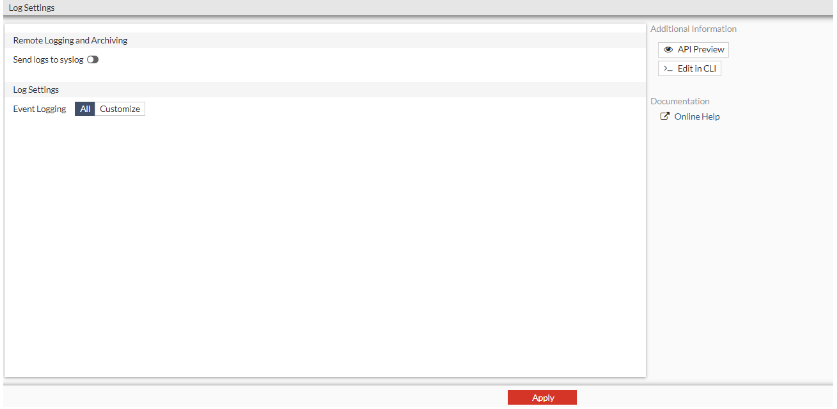
CLI configuration to generate secret audit report - example

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

```
execute audit secret-access
```

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. When enabled, enter the IP address/FQDN for the syslog. See Configuring parameters to send logs to syslog server on page 346. **Note**: The option is disabled by default.
Log Settings	
Event Logging	By default, the system logs all the events: system activity, user activity, and HA. You can customize event logging by selecting *Customize* and then unselecting options under *Customize*. **Note**: No event logs are recorded and displayed on the *Log & Report* > *Events* page for unselected events.

Older logs are deleted when disk space is low.

Disabling disk storage

Although it is not suggested that you disable the disk storage, FortiPAM allows you to disable the disk storage via the CLI.

To disable disk storage:

If you intend to disable the disk storage, ensure that the memory storage is enabled to make the log pages work correctly:

```
config log memory setting
   set status enable
end
```

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

```
config log disk setting
   set status disable
end
```

Configuring parameters to send logs to syslog server

To configure parameters to send logs to syslog server:

1. Go to *Log & Report > Log Settings*.
2. In *Additional Information*, select *Edit in CLI*.
   The CLI console opens.
3. Use the following parameters:

status {enable | disable}	Enable/disable remote syslog logging (default = disable).
The following parameters are only available when the `status` is set as `enable`.	
server <string>	Address of the remote syslog server.
mode {legacy-reliable | reliable | udp}	The remote syslog logging mode: • `legacy-reliable`: Legacy reliable syslogging by RFC3195 (Reliable Delivery for Syslog). • `reliable`: Reliable syslogging by RFC6587 (Transmission of Syslog Messages over TCP). • `udp`: syslogging over UDP (default).
port <integer>	The server listening port number (default = 514, 0 - 65535).
facility {kernel | user | mail | daemon | auth | syslog | lpr | news | uucp | cron | authpriv | ftp | ntp | audit | alert | clock | local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7}	The remote syslog facility (default = `local7`): • `kernel`: Kernel messages. • `user`: Random user-level messages. • `mail`: Mail system. • `daemon`: System daemons. • `auth`: Security/authorization messages. • `syslog`: Messages generated internally by syslog. • `lpr`: Line printer subsystem. • `news`: Network news subsystem. • `uucp`: Network news subsystem. • `cron`: Clock daemon. • `authpriv`: Security/authorization messages (private). • `ftp`: FTP daemon. • `ntp`: NTP daemon. • `audit`: Log audit. • `alert`: Log alert. • `clock`: Clock daemon. • `local0 ... local7`: Reserved for local use.
source-ip <string>	The source IP address of syslog.
format {cef | csv | default | rfc5424}	The log format: • `cef`: CEF (Common Event Format) format. • `csv`: CSV (Comma Separated Values) format. • `default`: Syslog format (default).

	• `rfc5424`: Syslog RFC5424 format.
priority {default | low}	The log transmission priority: • `default`: Set Syslog transmission priority to default (default). • `low`: Set Syslog transmission priority to low.
max-log-rate <integer>	The syslog maximum log rate in MBps (default = 0, 0 - 100000 where 0 = unlimited).
interface-select-method {auto | sdwan | specify}	Specify how to select outgoing interface to reach the server: • `auto`: Set outgoing interface automatically (default). • `sdwan`: Set outgoing interface by SD-WAN or policy routing rules. • `specify`: Set outgoing interface manually.

4. After adjusting the parameters, click *x* to close the CLI console.

Configuring log and video disk encryption

FortiPAM allows you to encrypt disk to protect logs and videos. Turning on disk encryption on log and video disks is akin to putting a solid lock on a chest of sensitive information. This keeps all the data safe by making it unreadable to anyone without a unique key or password. If someone tries to steal or get into the storage devices without permission, they cannot open and access the disk content. This is a crucial defence against any potential leaks or breaches.

When using (v)TPM and disk encryption:

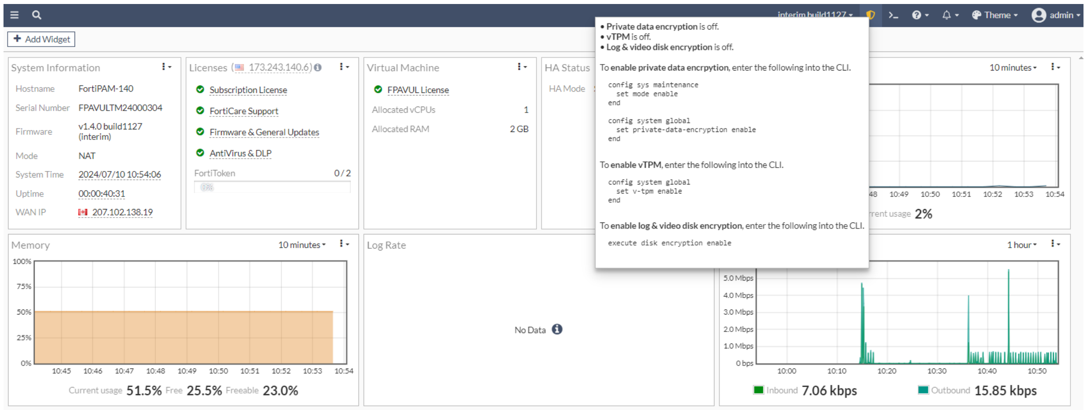
- On an evaluation license, use 2 GB of memory.
- On a formal license, use 4 GB of memory.

Disks can only be encrypted using the CLI console.

Enabling/disabling disk encryption erases all the existing logs and videos.

When log and video disk is encrypted, read/write on disk is slower.

FortiPAM displays private data, vTPM, and log/video disk encryption status in the banner.



System Information

Hostname FortiPAM-140
Serial Number FPAVULTM24000304
Firmware v1.4.0 build1127 (interim)
Mode NAT
System Time 2024/07/10 10:54:06
Uptime 00:00:40:31
WAN IP 207.102.138.19

Allocated vCPUs 1
Allocated RAM 2 GB

- **Private data encryption** is off.
- **vTPM** is off.
- **Log & video disk encryption** is off.

To **enable private data encrpytion**, enter the following into the CLI.

```
config sys maintenance
  set mode enable
end

config system global
  set private-data-encryption enable
end
```

To **enable vTPM**, enter the following into the CLI.

```
config system global
  set v-tpm enable
end
```

To **enable log & video disk encryption**, enter the following into the CLI.

```
execute disk encryption enable
```

CLI commands for disk encryption

```
execute disk encryption {enable | disable}
execute disk encryption log
execute disk encryption status
execute disk encryption video
```

Command	Description
execute disk encryption enable	Enable disk encryption on log and video disk. **Note**: The option is only available when disk encryption is disabled.
execute disk encryption disable	Disable disk encryption on log and video disk. **Note**: The option is only available when disk encryption is enabled.
execute disk encryption log	Check the log disk encryption status.
execute disk encryption status	Check the disk encryption status.
execute disk encryption video	check the video disk encryption status.

To encrypt log and video disks:

1. Enable maintenance mode. See Enable maintenance mode.
   In the CLI console, enter the following commands:

   ```
   config system maintenance
    set mode enable
   end
   ```

   Note: Disk operations are only allowed when the device is in maintenance mode.
2. In the CLI console, enter the following command:

   ```
   execute disk encryption enable
   Change disk encryption setting will erase all data in log and video disk.
   And system will reboot!
   Do you want to continue (y/n)y

   Add into disk encryption list: /dev/vda1 LOGUSEDXEAE02C3F
   ```

```
 Add into disk encryption list: /dev/vdb1 PAMVIDEOC5E34481

 Performing encrypt on the requested disk(s) and rebooting, please wait...

 Encrypting the disk...
  - unmounting /data2 :  ok
  - unmounting /var/log :  ok
  - unmounting /var/storage/HD2-PAMVIDEOC5E34481 :  ok
  Formatting /dev/mapper/dm_log ...
  Disk encryption is enabled on /dev/vda1 dm_log
  Formatting /dev/mapper/dm_video ...
  Disk encryption is enabled on /dev/vdb1 dm_video

  The system is going down NOW !!

Please stand by while rebooting the system.
[  528.501700] reboot: Restarting system

System is starting...
we have 2 interfaces
Serial number is FPAVUL2022103101

FPAVUL2022103101 login:
```

FortiPAM encrypts and formats both the log and video disks. All the content in log and video disk are erased and FortiPAM reboots.

FortiPAM only supports one log and one video disk.

Disk encryption cannot be enabled when there are more than one log or more than one video disk.

You must check the system storage using `configure system storage` and set unused storage status to disable.

3. FortiPAM then automatically generates a random `disk-encryption-password` and enables `disk-encryption`.

```
 config secret setting
  set disk-encryption enable
  set disk-encryption-password ENC
r7Z4a0307If/m+mqnl3p/XVypR6bde1bSTgx4nlmj5ml81/7giR7qHeEMcs7Kg+8sxUHMnR+ezp6HFG3S9yiaPEO
5lR4RzAxyp5CxvBCcr9WuNCwemr8P+lYOMj56Qaq897xykbd3c+0l+xgeRjNeHwmWo8KWEiRoVop9iQ1RUqO1FKy
zYmuJy0y5U8Rnv4TGqZpNw==
 end
```

`disk-encryption-password` and `disk-encryption` cannot be set manually.

4. In an HA setup, disk encryption configuration is not synced. All the HA members should have disk encryption configured before joining the cluster. Each HA member uses a different encryption password.

You must back up the system configuration of each member of an HA cluster.

To disable disk encryption:

1. Enable maintenance mode. See Enabling maintenance mode.
2. In the CLI console of a FortiPAM device where disk encryption is enabled, enter the following command to disable disk encryption:

```
execute disk encryption disable
Change disk encryption setting will erase all data in log and video disk.
And system will reboot!
Do you want to continue? (y/n)y

Add into disk decryption list: /dev/vda1 dm_log LOGUSEDXEAE02C3F
Add into disk decryption list: /dev/vdb1 dm_video PAMVIDEOC5E34481

Performing decrypt on the requested disk(s) and rebooting, please wait...

Decrypting the disk...
- unmounting /data2 :  ok
- unmounting /var/log :  ok
Add into format list: /dev/vda1 LOGUSEDXEAE02C3F
Add into format list: /dev/vdb1 PAMVIDEOC5E34481

Formatting the disk...
Formatting /dev/vda1 label LOGUSEDXEAE02C3F ... done
Formatting /dev/vdb1 label PAMVIDEOC5E34481 ... done

The system is going down NOW !!

Please stand by while rebooting the system.
[  117.836312] reboot: Restarting system

System is starting...
we have 2 interfaces
Serial number is FPAVUL2022103101

FPAVUL2022103101 login:
```

FortiPAM decrypts and formats log and video disks. All the content in log and video disk are erased and FortiPAM reboots. FortiPAM then automatically removes `disk-encryption-password` and sets `disk-encryption` to disable.

For troubleshooting, see Troubleshooting log and video disk encryption issues on page 442.

Email alert settings

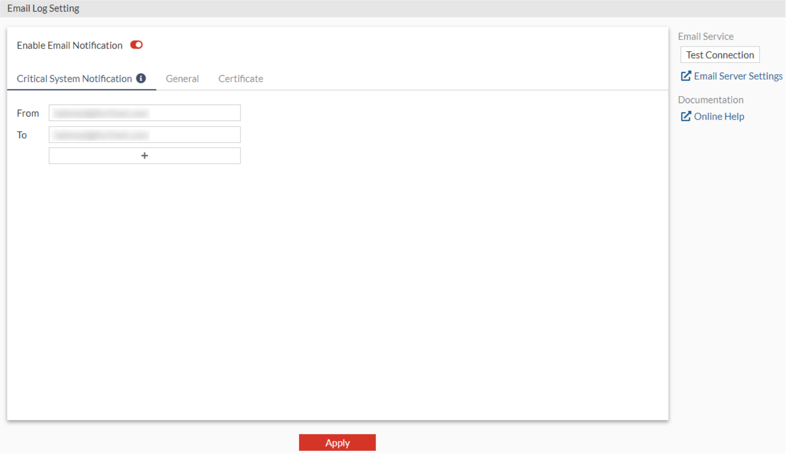
Enabling *Email Alert Settings* allows FortiPAM to send alert emails to administrators.

To configure a mail service:

1. Go to *System* > *Settings*.
2. You can set up the email service from the *Email Service* pane. See Settings on page 373.
   By default, the Fortinet mail server is used. You can set up a custom email server by enabling *Use custom settings* in the *Email Service* pane and configuring the related settings.

To enable Email alert setting:

1. Go to *Log & Report* > *Email Alert Settings*, and select *Enable email notification*.
   The following three tabs are available:
   - *Critical System Notification*: Includes setting up glass breaking and license expiring notifications.
   - *General*
   - *Certificate*



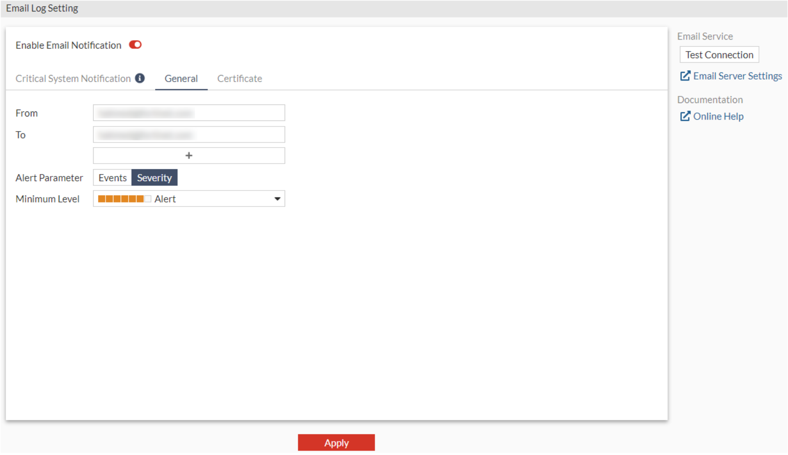
Email Log Setting

Enable Email Notification

Critical System Notification | General | Certificate

From [redacted]

To [redacted]



Email Log Setting

Enable Email Notification

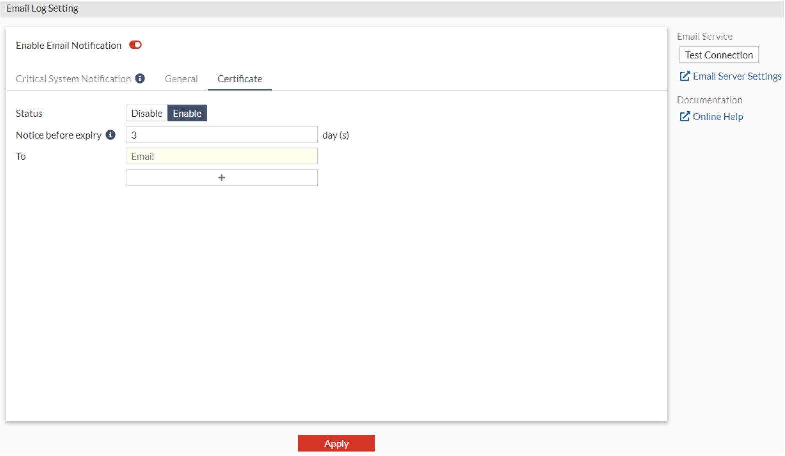
Critical System Notification | General | Certificate

From [redacted]

To [redacted]

Alert Parameter: Events | Severity

Minimum Level: Alert



Enable Email Notification ●

Status: Disable [✓ Enable]

Notice before expiry: 3 day (s)

To: Email

+

2. In the *Critical System Notification* tab, enter the following information:

From	The email address of the sender.
To	The email address of the receiver. Select + to add additional email addresses.

3. In the *General* tab, enter the following information:

From	The email address of the sender. fortipam@example.com
To	The email address of the receiver. admin1@example.com admin2@example.com Select + to add additional email addresses.
Alert parameter	Select from the following two options: • *Events*: Alerts are sent when an event occurs, e.g., system or user events. See Events on page 317. • *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. In the *Certificate* tab, enter the following information to set alerts for expiring certificates:

Status	Enable/disable sending alerts for expiring certificates. **Note**: The option is enabled by default.
Notice before expiry	The number of days before the certificate expiry, alerts are sent, in days (default = 3).
To	The email address of the receiver. Select + to add additional email addresses.

5. Click *Apply*.

Email alert when the glass breaking mode is activated - example

To set up email alerts when the glass breaking mode is activated:

1. Ensure that *Email Service* is set up in *System* > *Settings*. See Settings on page 373.
2. Go to *Log & Report* > *Email Alert Settings*, and select *Enable email notification*.
3. In the *Critical System Notification* tab:
   a. In *From*, enter the email address of the sender.
   b. In *To*, enter the email address of the receiver.
4. Click *Apply*.

Setting up an email alert for glass breaking excludes other important notifications, e.g., administrative change (configuration and HA status) and security (virus detection).

Debug settings

Customer Support may request a copy of your debug logs for troubleshooting.

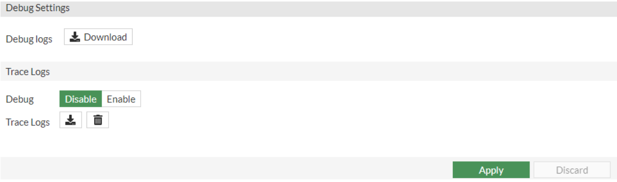
Go to *Log & Report* > *Debug Settings* and click *Download* in the *Debug Settings* pane to download the debug logs for troubleshooting.

Trace logs

FortiPAM trace GUI tool is available in the *Trace Logs* pane in *Log & Report* > *Debug Settings*.

To set up and download trace logs:

1. Go to *Log & Report* > *Debug Settings*.
   The *Debug Settings* window opens.



2. In the *Trace Logs* pane, enter the following information:

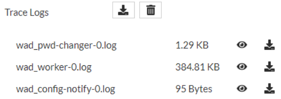
Debug	Enable/disable trace logs. **Note**: The option is disabled by default.
Category	Select + and then select categories to trace from the *Select Entries* window. Click *Close* once you have selected all the required trace categories. Use the search bar to look up a trace category. **Note**: The option is only available when *Debug* is enabled.
Debug Level	From the dropdown, select a debug level for the trace: • *Verbose* • *Info* (default) • *Warning* • *Error* **Note**: The option is only available when *Debug* is enabled.
Filter	From the dropdown, select a filter: • *None* (default) • *Internal* • *TCP Forwarding* • *Both* See FortiPAM HTTP filter on page 439. **Note**: The option is only available when *Debug* is enabled.
Overwrite	Enable/disable overwriting when the file reaches maximum size. **Note**:

	- The option is disabled by default. - The option is only available when *Debug* is enabled.
Drop Unknown Session	Enable to drop unknown sessions. See FortiPAM HTTP filter on page 439. **Note**: - The option is disabled by default. - The option is only available when *Debug* is enabled.
Maximum File Size	The maximum size for each trace log file, in MB (default = 1, 1 - 10). **Note**: The option is only available when *Debug* is enabled.
Trace Logs	Select from the following two options: - ⬇: Download all the trace logs. - 🗑: Clear all the log traces.

3. Click *Apply*.

   When FortiPAM is recording trace logs, a list of the logs appears in *Trace Logs*. You can download or view a trace log by clicking the eye or the download icon next to the trace log.

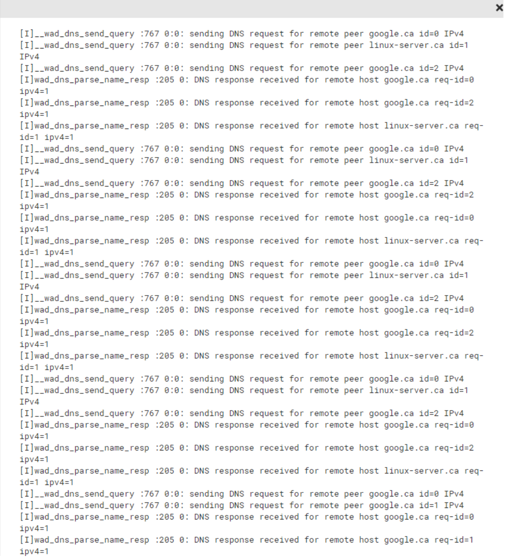
> Viewing does not stop the trace recording, but downloading turns off the trace recording.



Trace Logs ⬇ 🗑

wad_pwd-changer-0.log	1.29 KB	👁	⬇
wad_worker-0.log	384.81 KB	👁	⬇
wad_config-notify-0.log	95 Bytes	👁	⬇

When you click the eye icon next to a trace log, you can view it.



```
[I]__wad_dns_send_query :767 0:0: sending DNS request for remote peer google.ca id=0 IPv4
[I]__wad_dns_send_query :767 0:0: sending DNS request for remote peer linux-server.ca id=1
IPv4
[I]__wad_dns_send_query :767 0:0: sending DNS request for remote peer google.ca id=2 IPv4
[I]wad_dns_parse_name_resp :205 0: DNS response received for remote host google.ca req-id=0
ipv4=1
[I]wad_dns_parse_name_resp :205 0: DNS response received for remote host google.ca req-id=2
ipv4=1
[I]wad_dns_parse_name_resp :205 0: DNS response received for remote host linux-server.ca req-
id=1 ipv4=1
[I]__wad_dns_send_query :767 0:0: sending DNS request for remote peer google.ca id=0 IPv4
[I]__wad_dns_send_query :767 0:0: sending DNS request for remote peer linux-server.ca id=1
IPv4
[I]__wad_dns_send_query :767 0:0: sending DNS request for remote peer google.ca id=2 IPv4
[I]wad_dns_parse_name_resp :205 0: DNS response received for remote host google.ca req-id=2
ipv4=1
[I]wad_dns_parse_name_resp :205 0: DNS response received for remote host google.ca req-id=0
ipv4=1
[I]wad_dns_parse_name_resp :205 0: DNS response received for remote host linux-server.ca req-
id=1 ipv4=1
[I]__wad_dns_send_query :767 0:0: sending DNS request for remote peer google.ca id=0 IPv4
[I]__wad_dns_send_query :767 0:0: sending DNS request for remote peer linux-server.ca id=1
IPv4
[I]__wad_dns_send_query :767 0:0: sending DNS request for remote peer google.ca id=2 IPv4
[I]wad_dns_parse_name_resp :205 0: DNS response received for remote host google.ca req-id=0
ipv4=1
[I]wad_dns_parse_name_resp :205 0: DNS response received for remote host google.ca req-id=2
ipv4=1
[I]wad_dns_parse_name_resp :205 0: DNS response received for remote host linux-server.ca req-
id=1 ipv4=1
[I]__wad_dns_send_query :767 0:0: sending DNS request for remote peer google.ca id=0 IPv4
[I]__wad_dns_send_query :767 0:0: sending DNS request for remote peer linux-server.ca id=1
IPv4
[I]__wad_dns_send_query :767 0:0: sending DNS request for remote peer google.ca id=2 IPv4
[I]wad_dns_parse_name_resp :205 0: DNS response received for remote host google.ca req-id=0
ipv4=1
[I]wad_dns_parse_name_resp :205 0: DNS response received for remote host google.ca req-id=2
ipv4=1
[I]wad_dns_parse_name_resp :205 0: DNS response received for remote host linux-server.ca req-
id=1 ipv4=1
[I]__wad_dns_send_query :767 0:0: sending DNS request for remote peer google.ca id=0 IPv4
[I]__wad_dns_send_query :767 0:0: sending DNS request for remote peer google.ca id=1 IPv4
[I]wad_dns_parse_name_resp :205 0: DNS response received for remote host google.ca req-id=0
ipv4=1
[I]wad_dns_parse_name_resp :205 0: DNS response received for remote host google.ca req-id=1
ipv4=1
```

4. When the diagnostic is finished, disable *Debug* to stop recording.

Automation trigger settings

FortiPAM can be configured to perform actions when an event log is triggered. This is in the system automation table.

Automation trigger settings can only be configured via the CLI.

Automation trigger settings via the CLI - Example

To configure automation trigger settings:

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

```
config system automation-trigger
 edit "fold_chg"
  set event-type event-log
  set logid 44547 44548 #from the log id "0100044547". Remove the first 5 digits
(category/subcategory prefix)
  set category 1 #first 2 digits of the log ID "01"
  set logic and
  config fields
   edit 1
    set match regex
    set name "msg"
    set value "E*t"
   next
   edit 2
    set name "user"
    set value "u1"
   next
  end
 next
end
```

If the field is set to match regex, it uses the regular expression to match the field with the `value _name_`. Otherwise, it uses the default match, using `_*_` character as a wildcard.

If the logic is set to `_and_`, all fields must match to trigger the action. Otherwise, if it is set to `_or_`, any field matching triggers the action.

Network

Go to *Network* to configure network related settings for FortiPAM.

The menu provides features for configuring and viewing basic network settings, such as the unit interfaces, static routes, Domain Name System (DNS) options, fabric connectors, and packet capture.

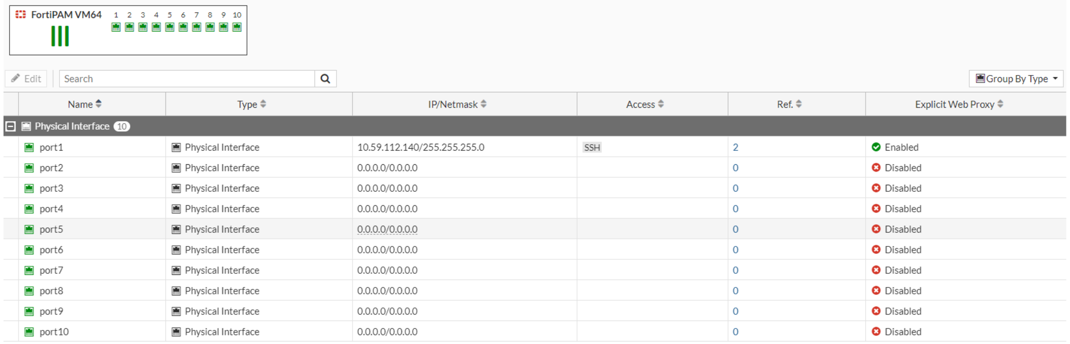
The *Network* tab contains the following tabs:

- Interfaces on page 357
- Static routes on page 361
- DNS settings on page 364
- Fabric Connectors on page 366
- Packet capture on page 371

Interfaces

In *Network* > *Interfaces*, you can configure the interfaces that handle incoming and outgoing traffic.

By default, each interface's name, type, IP/netmask, access, references, and explicit web proxy are displayed.



Name	Type	IP/Netmask	Access	Ref.	Explicit Web Proxy
Physical Interface 10					
port1	Physical Interface	10.59.112.140/255.255.255.0	SSH	2	✓ Enabled
port2	Physical Interface	0.0.0.0/0.0.0.0		0	✗ Disabled
port3	Physical Interface	0.0.0.0/0.0.0.0		0	✗ Disabled
port4	Physical Interface	0.0.0.0/0.0.0.0		0	✗ Disabled
port5	Physical Interface	0.0.0.0/0.0.0.0		0	✗ Disabled
port6	Physical Interface	0.0.0.0/0.0.0.0		0	✗ Disabled
port7	Physical Interface	0.0.0.0/0.0.0.0		0	✗ Disabled
port8	Physical Interface	0.0.0.0/0.0.0.0		0	✗ Disabled
port9	Physical Interface	0.0.0.0/0.0.0.0		0	✗ Disabled
port10	Physical Interface	0.0.0.0/0.0.0.0		0	✗ Disabled

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.

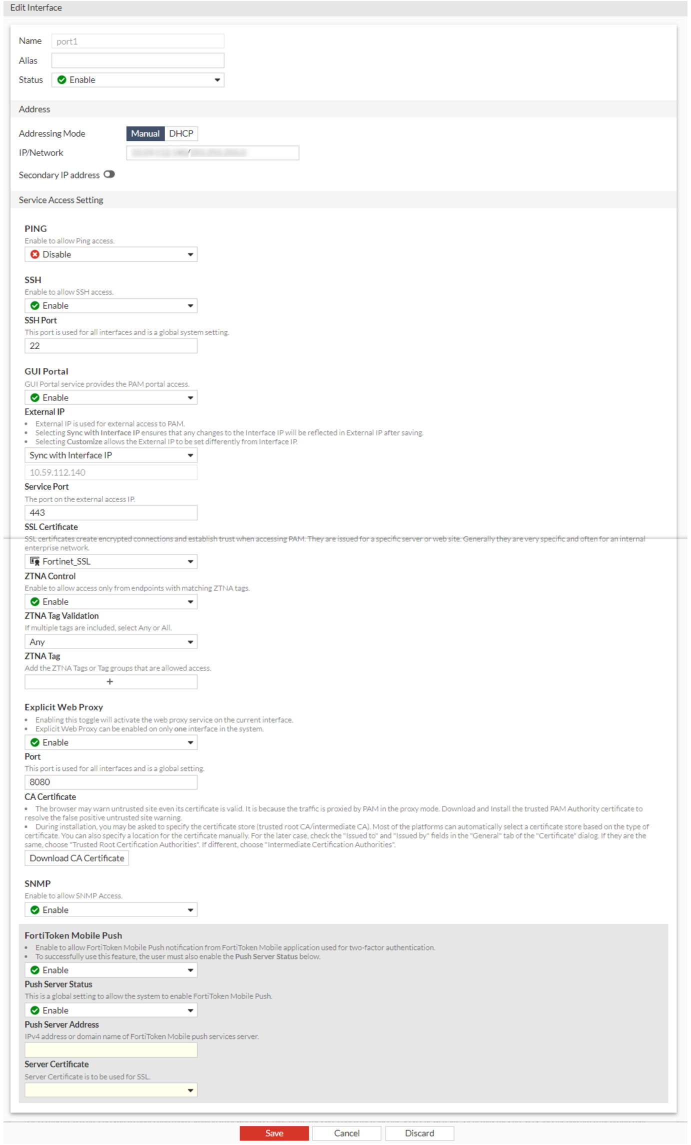
The following options are available in the *Interface* tab:

Edit	Select to edit the selected interface. See Editing an interface on page 358.
Search	Use the search bar to look for an interface.
Group By Type	From the dropdown, group the list of interfaces 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.

Editing an interface

To edit an interface:

1. Go to *Network* > *Interfaces*.
2. Double-click an interface to edit it
   The *Edit Interface* window opens.



Edit Interface

Name: port1
Alias:
Status: Enable

Address

Addressing Mode: Manual | DHCP
IP/Network: [redacted]
Secondary IP address

Service Access Setting

PING
Enable to allow Ping access.
Disable

SSH
Enable to allow SSH access.
Enable
SSH Port
This port is used for all interfaces and is a global system setting.
22

GUI Portal
GUI Portal service provides the PAM portal access.
Enable
External IP
- External IP is used for external access to PAM.
- Selecting **Sync with Interface IP** ensures that any changes to the Interface IP will be reflected in External IP after saving.
- Selecting **Customize** allows the External IP to be set differently from Interface IP.

Sync with Interface IP
10.59.112.140
Service Port
The port on the external access IP.
443
SSL Certificate
SSL certificates create encrypted connections and establish trust when accessing PAM. They are issued for a specific server or web site. Generally they are very specific and often for an internal enterprise network.
Fortinet_SSL
ZTNA Control
Enable to allow access only from endpoints with matching ZTNA tags.
Enable
ZTNA Tag Validation
If multiple tags are included, select Any or All.
Any
ZTNA Tag
Add the ZTNA Tags or Tag groups that are allowed access.
+

Explicit Web Proxy
- Enabling this toggle will activate the web proxy service on the current interface.
- Explicit Web Proxy can be enabled on only **one** interface in the system.

Enable
Port
This port is used for all interfaces and is a global setting.
8080
CA Certificate
- The browser may warn untrusted site even its certificate is valid. It is because the traffic is proxied by PAM in the proxy mode. Download and Install the trusted PAM Authority certificate to resolve the false positive untrusted site warning.
- During installation, you may be asked to specify the certificate store (trusted root CA/intermediate CA). Most of the platforms can automatically select a certificate store based on the type of certificate. You can also specify a location for the certificate manually. For the later case, check the "Issued to" and "Issued by" fields in the "General" tab of the "Certificate" dialog. If they are the same, choose "Trusted Root Certification Authorities". If different, choose "Intermediate Certification Authorities".

SNMP
Enable to allow SNMP Access.
Enable

FortiToken Mobile Push
- Enable to allow FortiToken Mobile Push notification from FortiToken Mobile application used for two-factor authentication.
- To successfully use this feature, the user must also enable the **Push Server Status** below.

Enable
Push Server Status
This is a global setting to allow the system to enable FortiToken Mobile Push.
Enable
Push Server Address
IPv4 address or domain name of FortiToken Mobile push services server.

Server Certificate
Server Certificate is to be used for SSL.

3. Enter the following information:

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.
Status	From the dropdown, enable/disable the interface.

Address	
Addressing Mode	Select the addressing mode for the interface. • *Manual*: Add an IP address and netmask for the interface. • *DHCP*: Get the interface IP address and other network settings from a DHCP server.
IP/Network	If *Addressing mode* is set to *Manual*, enter an IPv4 address and subnet mask for the interface. ⚠ FortiPAM interfaces cannot have IP addresses on the same subnet. **Note**: The option is only available when the *Addressing mode* is *Manual*.
Retrieve default gateway from server	Enable to retrieve the default gateway from the server. The default gateway is added to the static routing table. **Note**: The option is enabled by default. **Note**: The option is only available when the *Addressing mode* is *DHCP*.
Distance	Enter the administrative distance for the default gateway retrieved from the DHCP server (default = 5, 1 - 255). *Distance* specifies the relative priority of a route when there are multiple routes to the same destination. A lower administrative distance indicates a more preferred route. **Note**: The option is only available when *Retrieve default gateway from server* is enabled.
Secondary IP address	Add additional IPv4 addresses to this interface and select from *PING*, *SSH*, *SNMP*, and *FTM*. **Note**: The option is disabled by default. **Note**: The option is only available when the *Addressing mode* is *Manual*.
Service Access Setting By default, all the options are disabled.	
PING	From the dropdown, enable to allow PING access.
SSH	From the dropdown, enable to allow SSH access.
SSH Port	Enter the SSH port used for all the interfaces (a global system setting). **Note**: The option is only available when *SSH* is enabled.
GUI Portal	From the dropdown, enable the GUI portal. The GUI portal service provides the FortiPAM portal access. Each interface can have more than one matched external access *GUI Portal* configuration, but the FortiPAM GUI displays the best matched configuration on GUI including its VIP. If the current interface does not have a matched access portal, you can also create a new access portal on the interface page.

External IP	The external IP address is used for external access to FortiPAM. Selecting *Sync with Interface IP* ensures that any changes to the interface IP address will be reflected in external IP address after saving. **Note**: To use *Sync with Interface IP*, `extintf` must be configured to a specific interface in the CLI (not `any`). Selecting *Customize* allows the external IP address to be set differently from the interface IP address. **Note**: The option is only available when *GUI Portal* is enabled.
Service Port	Enter the port number on the external access IP address. **Note**: The option is only available when *GUI Portal* is enabled.
SSL Certificate	From the dropdown, select an SSL certificate. SSL certificates create encrypted connections and establish trust when accessing FortiPAM. They are issued for a specific server or web site. Generally, they are very specific and often used for an internal enterprise network. **Note**: The option is only available when *GUI Portal* is enabled.
ZTNA Control	Enable to allow access only from endpoints with matching ZTNA tags. **Note**: The option is only available when *GUI Portal* is enabled.
ZTNA Tag Validation	If multiple tags are included, select *Any* or *All*. **Note**: The option is only available when *ZTNA Control* is enabled.
ZTNA Tag	Select +, from *Select Entries*, add ZTNA tags or tag groups that are allowed access to FortiPAM. **Note**: The option is only available when *ZTNA Control* is enabled.
Explicit Web Proxy	From the dropdown, enable to activate the web proxy service on the current interface. **Note**: Explicit web proxy can be enabled on only one interface in the system.
Port	The port number for all interfaces (a global setting). **Note**: The option is only available when *Explicit Web Proxy* is enabled.
CA Certificate	The browser may warn untrusted sites even if its certificate is valid. This is because the traffic is proxied by FortiPAM in the proxy mode. Download and install the trusted FortiPAM authority certificate to resolve the false positive untrusted site warning. During installation, you may be asked to specify the certificate store (trusted root CA/intermediate CA). Most platforms can automatically select a certificate store based on the type of certificate. You can also specify a location for the certificate manually. For the latter case, check the *Issued to* and *Issued by* fields in the *General* tab of the *Certificate* dialog. If they are the same, choose *Trusted Root Certification Authorities*. If different, select *Intermediate Certification Authorities*.

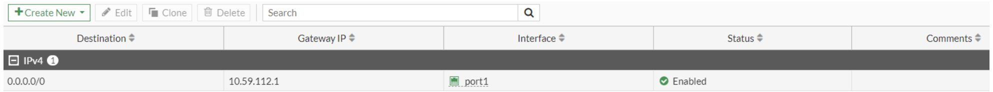
	Note: The option is only available when *Explicit Web Proxy* is enabled.
SNMP	From the dropdown, enable to allow SNMP access.
FortiToken Mobile Push	From the dropdown, enable to allow FortiToken Mobile Push notification from FortiToken Mobile application used for 2FA. **Note**: To successfully use *FortiToken Mobile Push*, you must also enable *Push Server Status*.
Push Server Status	Enable/disable FortiToken Mobile push (a global setting).
Push Server Address	The IPv4 address or domain name of the FortiToken Mobile push services server. **Note**: The option is only available when *Push Server Status* is enabled.
Server Certificate	From the dropdown, select the server certificate to be used for SSL. **Note**: The option is only available when *Push Server Status* is enabled.

4. Click *Save*.

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 1				
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.

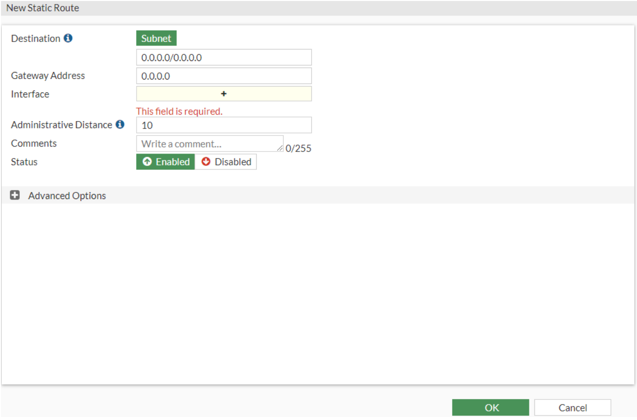
The following options are available in the *Static Routes* tab:

+Create New	From the dropdown, select to create an IPv4 static route. See Creating an IPv4 static route on page 362.
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 0.0.0.0/0.0.0.0
Gateway Address	0.0.0.0
Interface	+ This field is required.
Administrative Distance	10
Comments	Write a comment... 0/255
Status	Enabled Disabled

3. Enter the following information:

Destination	The destination IP addresses and network masks of packets that the FortiPAM unit intercepts. Enter the IPv4 address and netmask of the new static route.
Gateway Address	The IP addresses of the next-hop routers to which intercepted packets are forwarded. Enter the gateway IP address for those packets that you intend to intercept. **Note**: *Gateway Address* is unavailable when the *Interface* is *Blackhole*.
Interface	The interface the static route is configured to. Select + and in *Select Entries*, select the interface or create a new interface. A blackhole route is a route that drops all traffic sent to it. Blackhole routes are used to dispose of packets instead of responding to suspicious inquiries. This provides added security since the originator will not discover any information from the target network. Blackhole routes can also limit traffic on a subnet. If some subnet addresses are not in use, traffic to those addresses, which may be valid or malicious, can be directed to a blackhole for added security and to reduce traffic on the subnet. Use the search bar to look for an interface. Use the pen icon next to an interface to edit the interface.
Administrative Distance	The number of hops the static route has to the configured gateway. The administrative distance is used to determine the cost of the route. Smaller distances are considered "better" route that should be used when multiple paths exist to the same destination (default = 10, 1 - 255). The route with same distance are considered as equal-cost multi-path (ECMP).
Comments	Optionally, enter a description about the static route.
Status	Enable/disable the static route.
Advanced Options	
Priority	A number for the priority of the static route. Routes with a larger number will have a lower priority. Routes with the same priority are considered as ECMP (default = 1 when creating an IPv4 static route, 1 - 65535). Priority can only be customized for statically configured route s. The priority of routes dynamically learned from the routing protocols is always 1.

API Preview	The *API Preview* allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. The feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

4. Click *OK*.

To use API preview:

1. Click *API Preview*.
   The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* (enabled by default) to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

DNS settings

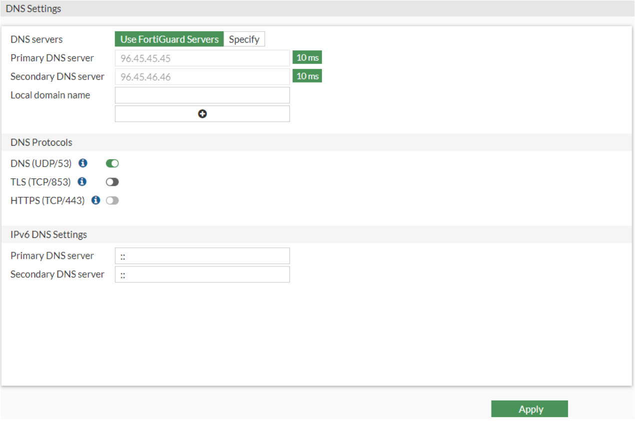
Domain name system (DNS) is used by devices to locate websites by mapping a domain name to a website’s IP address.

You can specify the IP addresses of the DNS servers to which your FortiPAM unit connects.

To configure DNS settings, go to *Network > DNS Settings*.

To configure DNS settings:

1. Go to *Network > DNS Settings*.



DNS Settings

DNS servers: Use FortiGuard Servers | Specify
Primary DNS server: 96.45.45.45 (10 ms)
Secondary DNS server: 96.45.46.46 (10 ms)
Local domain name:

DNS Protocols

DNS (UDP/53): enabled
TLS (TCP/853): disabled
HTTPS (TCP/443): disabled

IPv6 DNS Settings

Primary DNS server: ::
Secondary DNS server: ::

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

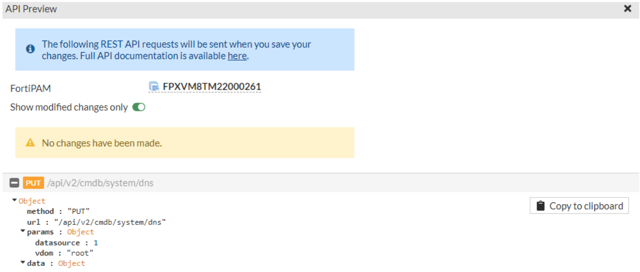
DNS servers	Select *Use FortiGuard Severs* or *Specify*. If you select *Specify*, enter the IP addresses for the primary and secondary DNS servers.
Primary DNS server	Enter the IPv4 or IPv6 address for the primary DNS server. **Note**: For an IPv4 address, the option is only available to edit when *DNS servers* is *Specify*.
Secondary DNS server	Enter the IPv4 or IPv6 address for the secondary DNS server. **Note**: For an IPv4 address, the option is only available to edit when *DNS servers* is *Specify*.
Local domain name	The domain name to append to addresses with no domain portion when performing DNS lookups. Select + to add additional local domain names. You can add up to 8 local domain names.
DNS Protocols	
DNS (UDP/53)	Enable or disable the use of clear-text DNS over port 53. **Note**: The option is disabled by default and only available to edit when *DNS servers* is *Specify*.
TLS (TCP/853)	Enable or disable the use of DNS over TLS (DoT). **Note**: The option is enabled by default and only available to edit when *DNS servers* is *Specify*.
HTTPS (TCP/443)	Enable or disable the use of DNS over HTTPS (DoH). **Note**: The option is disabled by default and only available to edit when *DNS servers* is *Specify*.
SSL certificate	From the dropdown, select an SSL certificate or click *Create* to import a certificate (default = `Fortinet_Factory`). SSL certificate is used by the DNS proxy as a DNS server so that the DNS proxy can provide service over TLS as well as normal UDP/TCP. Use the search bar to look for an SSL certificate.
Server hostname	The host name of the DNS server (default = `globalsdns.fortinet.net`).

You can add up to 4 server hostnames.

3. Click *Apply*.

To use API preview:

1. Click *API Preview*.
   The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.



The following REST API requests will be sent when you save your changes. Full API documentation is available here.

FortiPAM FPXVM8TM22000261

Show modified changes only

No changes have been made.

PUT /api/v2/cmdb/system/dns

```
▾Object
   method : "PUT"
   url : "/api/v2/cmdb/system/dns"
  ▾params : Object
     datasource : 1
     vdom : "root"
  ▾data : Object
```

2. Enable *Show modified changes only* (enabled by default) to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Security fabric

The Security Fabric allows your network to automatically see and dynamically isolate affected devices, partition network segments, update rules, push out new policies, and remove malware.

The Security Fabric is designed to cover the entire attack surface and provide you with complete visibility into your network. It allows you to collect, share, and correlate threat intelligence between security and network devices, centrally manage and orchestrate policies, automatically synchronize resources to enforce policies, and coordinate a response to threats detected anywhere across the extended network. The unified management interface provides you with cooperative security alerts, recommendations, audit reports, and full policy control across the Security Fabric that will give you confidence that your network is secure.

See Fabric Connectors on page 366.

Fabric Connectors

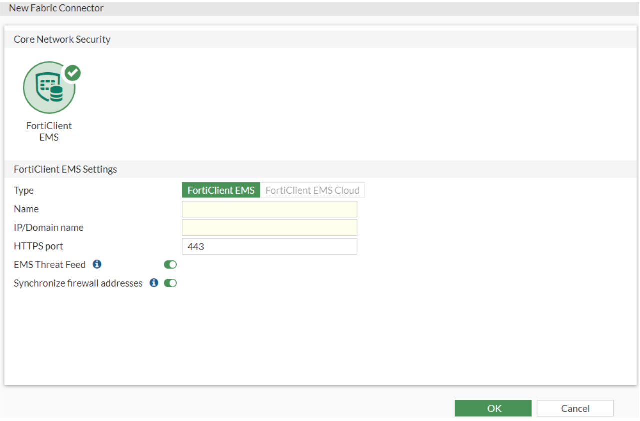
Fabric connectors provide integration with Fortinet products to automate the process of managing dynamic security updates without manual intervention.

In HA and DR setup, the EMS configuration, such as server name and IP, can be synced to secondary and DR nodes. However, secondary and DR nodes need to be authorized by EMS individually. It is recommended that after configuring

HA, admin test failover, log in to the new primary, and follow the same procedure to authorize secondary and DR nodes on the EMS server.

To create a FortiClient EMS fabric connector:

1. Go to *Network > Fabric Connectors*.
2. In the *Core Network Security* pane, select *FortiClient EMS* and then select *Edit*.
   The *New Fabric Connector* pane opens.



New Fabric Connector

Core Network Security

FortiClient EMS

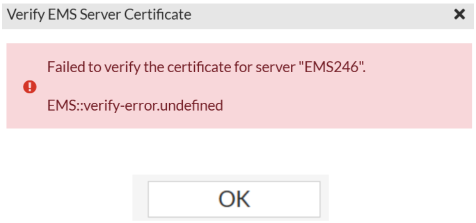
FortiClient EMS Settings

Type: FortiClient EMS | FortiClient EMS Cloud
Name
IP/Domain name
HTTPS port: 443
EMS Threat Feed
Synchronize firewall addresses

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.



Verify EMS Server Certificate

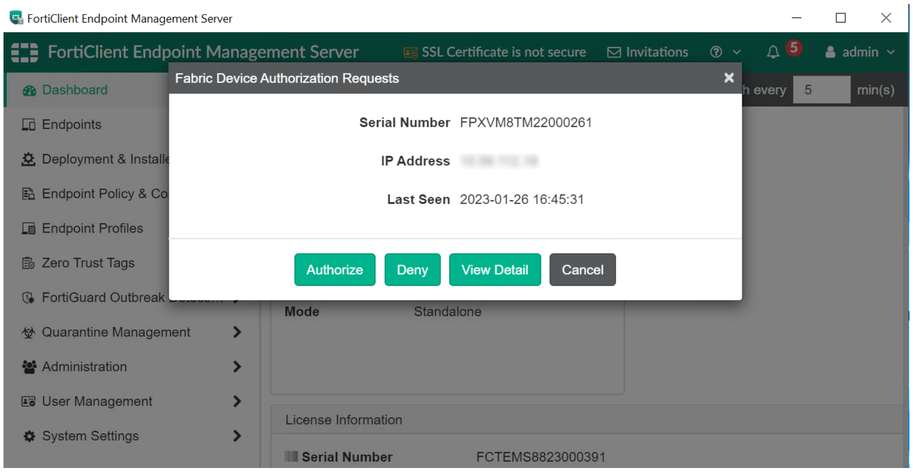
Failed to verify the certificate for server "EMS246".

EMS::verify-error.undefined

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.



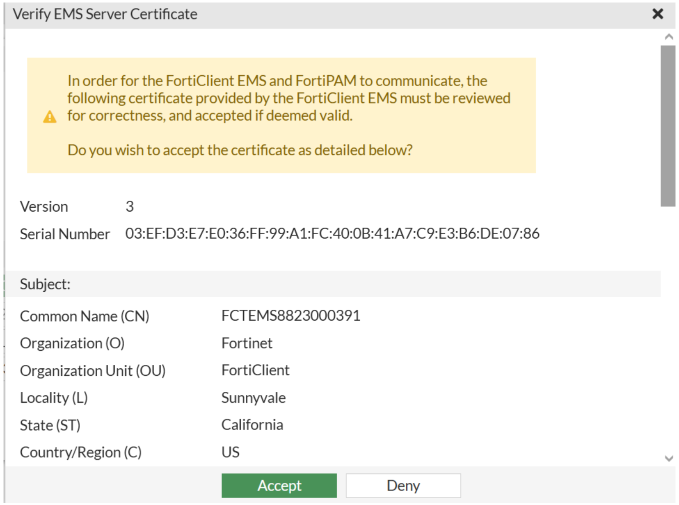
Fabric Device Authorization Requests

Serial Number	FPXVM8TM22000261
IP Address	[redacted]
Last Seen	2023-01-26 16:45:31

Mode	Standalone
Serial Number	FCTEMS8823000391

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.



Verify EMS Server Certificate

In order for the FortiClient EMS and FortiPAM to communicate, the following certificate provided by the FortiClient EMS must be reviewed for correctness, and accepted if deemed valid.

Do you wish to accept the certificate as detailed below?

Version	3
Serial Number	03:EF:D3:E7:E0:36:FF:99:A1:FC:40:0B:41:A7:C9:E3:B6:DE:07:86

Subject:

Common Name (CN)	FCTEMS8823000391
Organization (O)	Fortinet
Organization Unit (OU)	FortiClient
Locality (L)	Sunnyvale
State (ST)	California
Country/Region (C)	US

8. In the *Verify EMS Server Certificate* window, select *Accept* to accept the certificate from the EMS-side.

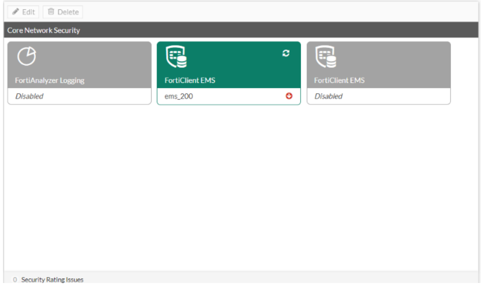
   FortiPAM is now successfully connected to the EMS server.

FortiAnalyzer logging

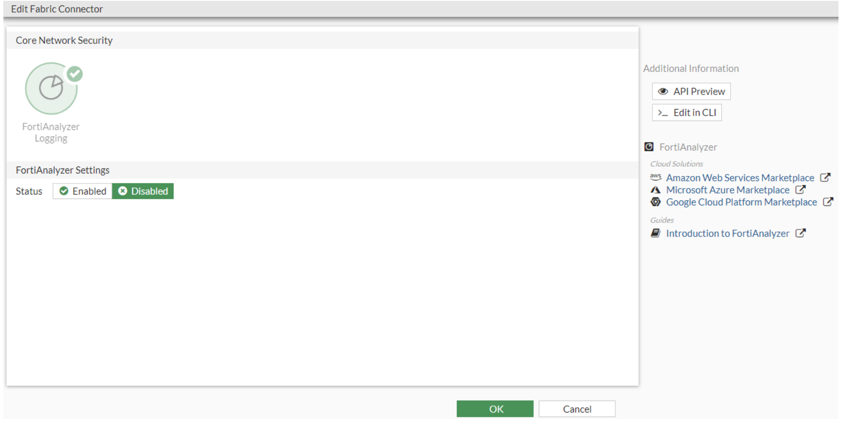
FortiAnalyzer is a remote logging server that helps keep an additional copy of logs from FortiPAM.

To configure FortiAnalyzer logging:

1. Go to *Network > Fabric Connectors*.
   Core Network Security opens.



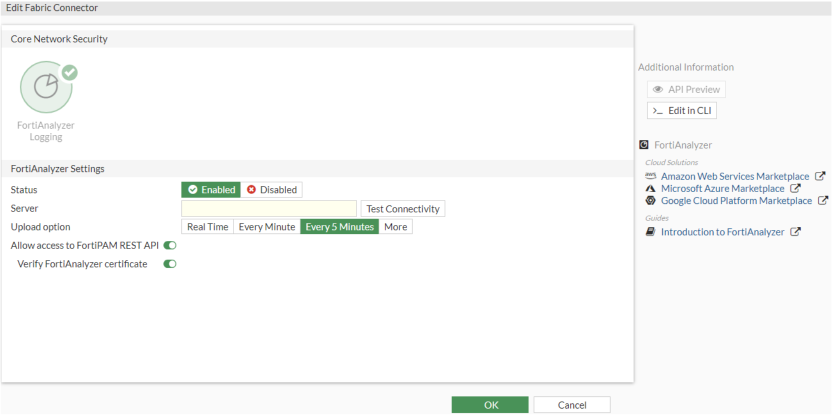
2. Select *FortiAnalyzer Logging* and select *Edit*.
   The *Edit Fabric Connector* window opens.



FortiAnalyzer Settings

Status: Enabled [✓ Disabled]

3. In the *FortiAnalyzer Settings* pane, set the *Status* as *Enabled*.
   You now see new options in the *Edit Fabric Connector* window.



FortiAnalyzer Settings

Status: [✓ Enabled] Disabled

Server:

Upload option: Real Time, Every Minute, [✓ Every 5 Minutes], More

Allow access to FortiPAM REST API: ●

Verify FortiAnalyzer certificate: ●

4. Enter the following information:

Server	Enter the server IP address or the FQDN. Select *Test Connectivity* to test the connection to the server.
Upload option	Select an upload interval: • *Real Time* • *Every Minute* • *Every 5 Minute* (default) • *More*
Upload interval	Select an upload interval: • *Daily* (default) • *Weekly* • *Monthly* **Note**: The option is only available when the *Upload option* is set to *More*.
Day	From the dropdown, select a day. **Note**: The option is only available when the *Upload interval* is *Weekly*.
Date	Enter a date for the month. **Note**: The option is only available when the *Upload interval* is *Monthly*.
Time	Enter a time or select the clock icon to select a time.
Allow access to FortiPAM REST API	Enable/disable FortiPAM REST API access (default = enable).
Verify FortiAnalyzer certificate	Enable/disable verifying the FortiAnalyzer certificate (default = enable). **Note**: The option is only available when *Allow access to FortiPAM REST API* is enabled.

5. Click *OK*.
6. In the window that opens, verify the FortiAnalyzer serial number and click *Accept*.
7. Check the *FortiAnalyzer Status*. If the connection is unauthorized, click *Authorize* to log in to FortiAnalyzer and authorize FortiPAM.
   After establishing a connection between FortiPAM and FortiAnalyzer, subsequent logs are accessible in the corresponding FortiAnalyzer.

When reviewing logs in *Log & Report*, you can choose *FortiAnalyzer* as the log source. See Log & report on page 312.

To configure FortiAnalyzer logging via the CLI - Example

```
config log fortianalyzer setting
  set status enable
  set server faz.fortipam.ca
end
```

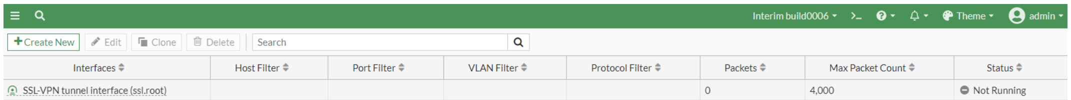
Packet capture

You can create a filter on an interface to capture a specified number of packets to examine.

Go to *Network* > *Packet Capture* to see existing packet capture filters.

For each packet capture filter the following are displayed:

- Interfaces
- Host filter
- Post filter
- VLAN filter
- Protocol filter
- Packets
- Maximum packet count
- Status



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.

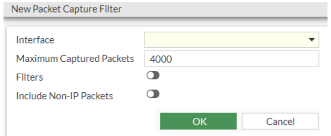
The following options are available in the *Packet Capture* tab:

+Create New	Select to create a new packet capture filter. See Creating a packet capture filter on page 371.
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.



New Packet Capture Filter

Interface:
Maximum Captured Packets: 4000
Filters: ○
Include Non-IP Packets: ○

3. Enter the following information:

Interface	Select or create a new interface. Use the search bar to look for an interface. Use the pen icon next to an interface to edit the interface.
Maximum Captured Packets	Enter how many packets to collect (default = 4000, 1 - 1000000).
Filters	Enable *Filters*, you can create filters for host names, ports, VLAN identifiers, and protocols. Use commas to separate items. Use a hyphen to specify a range. **Note**: The option is disabled by default.
Include Non-IP Packets	Select this option if you want to include packets from non-IP protocols. **Note**: The option is disabled by default.
API Preview	The *API Preview* allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. This feature is not available if the user is logged in as an 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.

System

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

You can also manage certificates, edit replacement messages, set up HA cluster and SNMP, and configure ZTNA related settings, automated backup, firmware upgrades, FortiPAM and FortiGuard licenses.

System contains the following tabs:

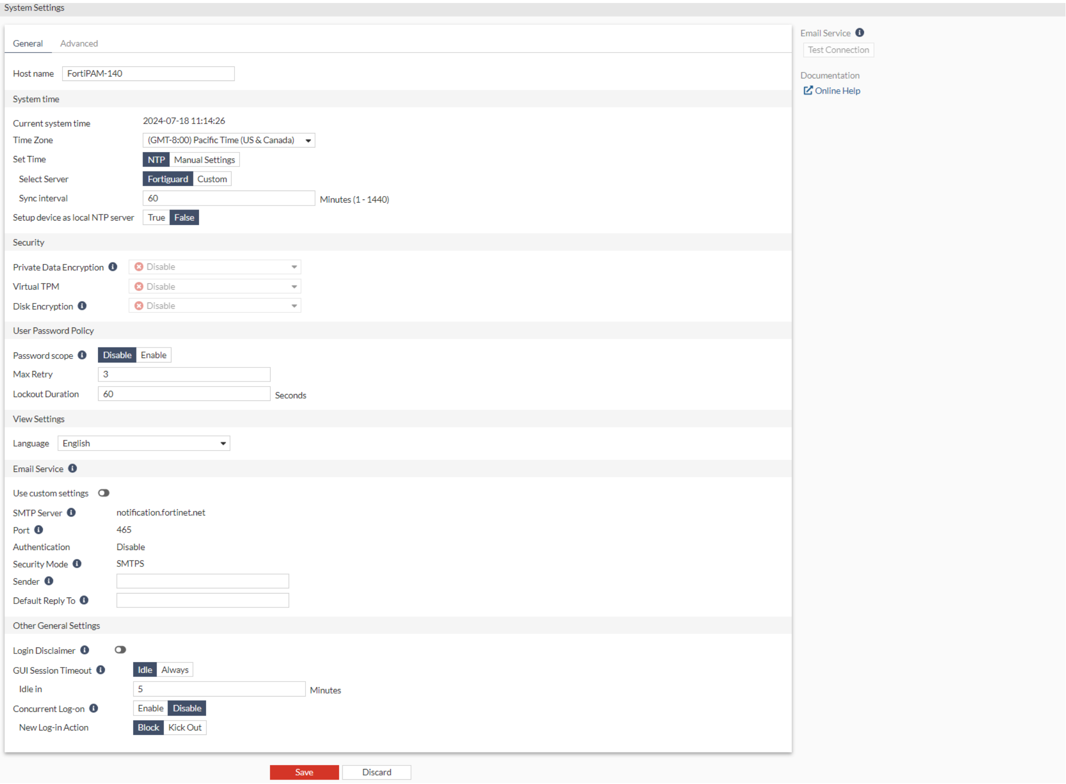
- Settings on page 373
- ZTNA tags on page 382
- High availability on page 389
- Certificates on page 398
- Replacement messages on page 408
- SNMP on page 416
- Backup on page 423
- Firmware on page 432
- FortiPAM license on page 433
- FortiGuard license on page 434

Settings

Go to *System* > *Settings* to access system configuration that you can update after installing FortiPAM.

To update System Settings:

1. Go to *System* > *Settings*.
   The *General* tab in the *System Settings* window opens.



System Settings

General | Advanced

Host name: FortiPAM-140

System time

Current system time: 2024-07-18 11:14:26

Time Zone: (GMT-8:00) Pacific Time (US & Canada)

Set Time: NTP | Manual Settings

Select Server: Fortiguard | Custom

Sync interval: 60 Minutes (1 - 1440)

Setup device as local NTP server: True | False

Security

Private Data Encryption: Disable

Virtual TPM: Disable

Disk Encryption: Disable

User Password Policy

Password scope: Disable | Enable

Max Retry: 3

Lockout Duration: 60 Seconds

View Settings

Language: English

Email Service

Use custom settings

SMTP Server: notification.fortinet.net

Port: 465

Authentication: Disable

Security Mode: SMTPS

Sender:

Default Reply To:

Other General Settings

Login Disclaimer

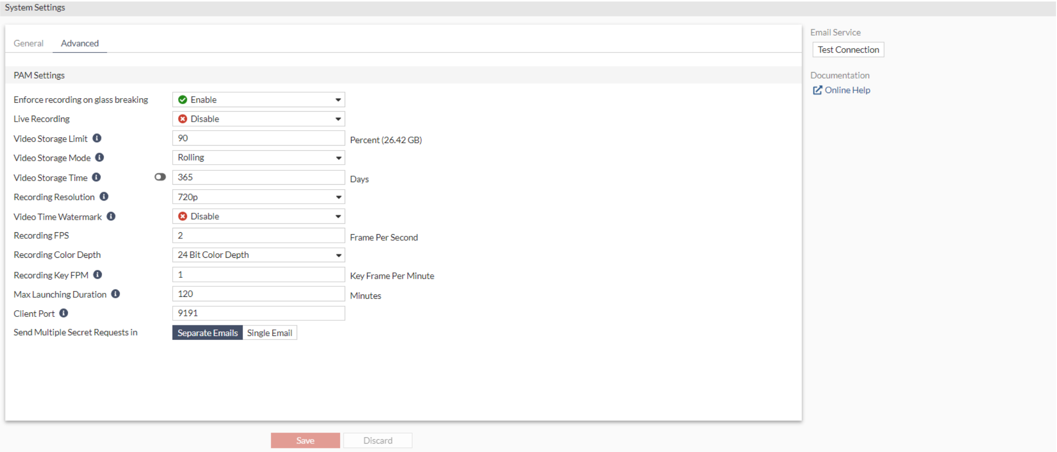
GUI Session Timeout: Idle | Always

Idle in: 5 Minutes

Concurrent Log-on: Enable | Disable

New Log-in Action: Block | Kick Out

2. To switch to the *Advanced* tab, select *Advanced*.



System Settings

General | Advanced

PAM Settings

Enforce recording on glass breaking: Enable

Live Recording: Disable

Video Storage Limit: 90 Percent (26.42 GB)

Video Storage Mode: Rolling

Video Storage Time: 365 Days

Recording Resolution: 720p

Video Time Watermark: Disable

Recording FPS: 2 Frame Per Second

Recording Color Depth: 24 Bit Color Depth

Recording Key FPM: 1 Key Frame Per Minute

Max Launching Duration: 120 Minutes

Client Port: 9191

Send Multiple Secret Requests in: Separate Emails | Single Email

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

General tab

Host name	The identifying name assigned to this FortiPAM unit.

System time pane

System time	

Current system time	The current date and time on the FortiPAM internal clock or NTP servers.
Time Zone	From the dropdown, select a timezone.
Set Time	Select from the following options: • *NTP*: The NTP (Network Time Protocol) server (default). • *Manual Settings*
Select Server	Select a server from the following two options: • *FortiGuard* (default) • *Custom* **Note**: The option is only available when *Set Time* is *NTP*.
Custom Server IP Address	The custom server IP address. Custom NTP server details must be configured via the CLI. **Note**: The option is only available when *Set Time* is *NTP* and the *Select Server* is *Custom*.
Sync internal	Enter how often, in minutes, that the device synchronizes its time with the NTP server (default = 60, 1 - 1440). **Note**: The option is only available when *Set Time* is *NTP*.
Date	Enter the date or select the calendar icon, and from the dropdown, select a date. **Note**: The option is only available when *Set Time* is *Manual Settings*.
Time	Enter the time or select the clock icon, and from the dropdown, select a time. **Note**: The option is only available when *Set Time* is *Manual Settings*.
Setup device as local NTP server	Select *True* to configure the FortiPAM as a local NTP server (default = *False*).
Listen on Interfaces	Set the interface or interfaces that the FortiPAM will listen for NTP requests on. **Note**: The option is only available when *Setup device on local NTP server* is set as *True*.

Security

Private Data Encryption	Enable/disable encrypting secret credentials and other sensitive data with a private key. It is suggested that you backup your configuration before you disable or reenable (v)TPM or `private-data-encryption`. **Note**: Only the status is shown. Use the CLI to configure private data encryption. See Secure password storage on page 448.
Virtual TPM	Enable/disable vTPM. **Note**: Only the status is shown. Use the CLI to configure vTPM.

	See FortiPAM with TPM on page 47.
Disk Encryption	Enable/disable log and video disk encryption. **Note**: Only the status is shown. Use the CLI to change log/video disk encryption. See Configuring log and video disk encryption on page 347.

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).
Max Retry	Enter the maximum number of allowed failed login attempts (default = 3, 1 - 10).
Lockout Duration	Specify the length of the lockout period, in seconds (default = 60, 1 - 2147483647). **Note**: After the lockout duration expires, the *Max Retry* number applies again.

View Settings pane

View Settings	
Language	From the dropdown, select a language.

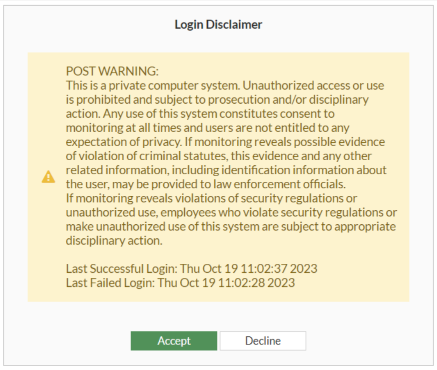
Email Service pane

Email Service See Testing the email service connection example on page 380.	
Use custom settings	Enable to edit options in the *Email Service* pane.
SMTP Server	The SMTP server IP address or the hostname, e.g., `smtp.example.com` and `notification.fortinet.net`.
Port	The recipient port number.

	The default port value depends on the chosen *Security Mode*. For *None* and *STARTTLS*, the default value is 25. For *SMTPS*, the default value is 465.
Authentication	If required by the email server, enable authentication. If enabled, enter the *Username* and *Password*.
Security Mode	Set the connection security mode used by the email server: • *None* • *SMTPS* (default) • *STARTTLS*
Sender	Enter the email address used to send emails. For the email to be sent, depending on the *SMTP Server* used and *Authentication* being enabled, the *Sender* email address may be required to be a specific email address. If the *Sender* email address is incorrect, the email is not sent.
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 351.

Other General Settings pane

Login Disclaimer	Enable/disable displaying a disclaimer message once a user successfully logs in. Once enabled, enter a disclaimer in the text box. Alternatively, you can use the default login disclaimer.

	Last Successful Login displays when the last successful login has occurred. *Last Failed Login* displays when the last failed login has occured.  Login Disclaimer POST WARNING: This is a private computer system. Unauthorized access or use is prohibited and subject to prosecution and/or disciplinary action. Any use of this system constitutes consent to monitoring at all times and users are not entitled to any expectation of privacy. If monitoring reveals possible evidence of violation of criminal statutes, this evidence and any other related information, including identification information about the user, may be provided to law enforcement officials. If monitoring reveals violations of security regulations or unauthorized use, employees who violate security regulations or make unauthorized use of this system are subject to appropriate disciplinary action. Last Successful Login: Thu Oct 19 11:02:37 2023 Last Failed Login: Thu Oct 19 11:02:28 2023 Click the eye icon to preview the login disclaimer. **Note**: The option is disabled by default.
GUI Session Timeout	Select from the following two options: • *Idle*: Enforce timeout after the entered time in *Idle in* has elapsed, in minutes (default = 5, 1 - 480). • *Always*: Enforce user logout after the entered time in *Force logout in* has elapsed, in minutes (default = 480, 5 - 480). A shorter *GUI Session Timeout* duration is more secure.
Concurrent Log-on	A concurrent session occurs when multiple users access FortiPAM using the same account from different locations or web browsers. Select from the following two options: • *Enable*: Enable user concurrent login. • *Disable*: Disable user concurrent login. **Note**: The option is enabled by default. Once disabled, concurrent logins are disallowed.
New Log-in Action	Select from the following two options when an admin concurrent session is disabled: • *Block*: Additional concurrent admin sessions are blocked while an admin

	session is active (default). • *Kick Out*: Terminate (kick out) previous sessions when a new admin session is opened. **Note**: The option is only available when *Concurrent Log-on* is disabled. For information on related CLI commands, see Concurrent user sessions on page 434.

Advanced tab

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).
Live Recording	Enable/disable live recording (default = disable). ⚠ Before downgrading from FortiPAM version 1.2.x to 1.1.x, disable *Live Recording*. Otherwise, you cannot replay videos on FortiPAM 1.1.x. See Over-the-shoulder monitoring (Live recording) on page 310.
Video Storage Limit	The maximum percentage of the video disk partition size that can be used for storing FortiPAM session video recordings (default = 90, 10 - 90).
Video Storage Mode	From the dropdown, select a PAM session video recording storage mode (default = *Rolling*): • *Rolling*: Evict the oldest PAM video recording within the *Video Storage Time* when the video storage limit is reached. • *Stop*: Stop storing new PAM video recordings when the disk quota is full.
Video Storage Time	The number of days for which a video is stored. Video files are removed from FortiPAM once the time has elapsed (default = 365, 0 - 36500). 🛠 Enable the toggle or enter `0` for no time limit. **Note**: The option is only available when the *Video Storage Mode* is *Rolling*.
Recording Resolution	From the dropdown, select a resolution for the PAM video recordings: • *480p* • *720p* (default) • *1080p*
Video Time Watermark	Enable/disable adding a watermark to the secret videos with time and timezone information (default = disable).

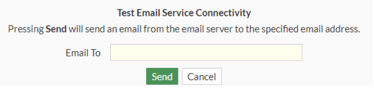
Recording FPS	Enter the PAM video recording frame rate (default = 2, 1 - 15).
Recording Color Depth	From the dropdown, select a color depth: • *24 Bit Color Depth* (default) • *32 Bit Color Depth*
Recording Key FPM	Enter the PAM video recording key frame rate per minute (default = 1, 1 - 60).
Max Launching Duration	Enter the maximum duration for all the secret launching sessions, in minutes (default = 120, 1 - 10000).
Client Port	Enter the port number that FortiPAM uses to connect to FortiClient (default = 9191, 1 - 65536).
Send Multiple Secret Requests in	When sending multiple secret request notifications to a reviewer: • *Separate Emails*: Send the secret request notifications as separate emails (default). • *Single Email*: Send the secret request notifications as a single email.
Period	Enter the time interval at which multiple secret request notifications are sent, in seconds (default = 60, 60 - 600). **Note**: The option is only available when *Send Multiple Secret Requests in* is set to *Single Email*.

4. Click *Save*.

Testing the email service connection - example

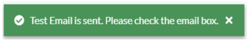
To test the email service connection:

1. Go to *System* > *Settings*.
   In this example, we use the default Fortinet mail server (`notification.fortinet.net`).
2. In the *Email Service* pane:
   a. In *Default Reply To*, enter the email address that is used to send emails.
3. Click *Apply*.
   To configure alert emails, see Email alert settings on page 351.
4. Once the email service settings have been set up, click *Test Connection* from the top-right.
   The *Test Email Service Connectivity* dialog opens.

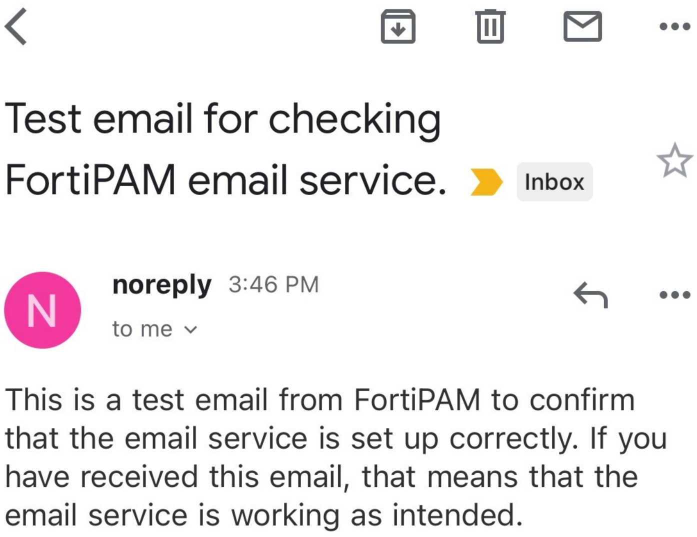

Test Email Service Connectivity

Pressing **Send** will send an email from the email server to the specified email address.

5. In *Email To*, enter an email address where the test email is sent to.
6. Click *Send*.
   Once the email is successfully sent, you see the following message on the bottom-right:


Test Email is sent. Please check the email box.

The test email looks like the following:



Test email for checking FortiPAM email service. Inbox

noreply 3:46 PM

to me

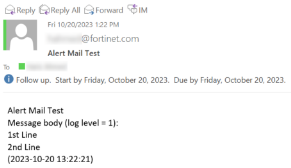
This is a test email from FortiPAM to confirm that the email service is set up correctly. If you have received this email, that means that the email service is working as intended.

To test the email service connection via the CLI:

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

   ```
   diagnose log alertmail test
   ```

   If the email service is correctly setup, you should receive a test email that looks like the following:

   Fri 10/20/2023 1:22 PM

   [redacted]@fortinet.com

   Alert Mail Test

   To [redacted]

   Follow up. Start by Friday, October 20, 2023. Due by Friday, October 20, 2023.

   Alert Mail Test
   Message body (log level = 1):
   1st Line
   2nd Line
   (2023-10-20 13:22:21)

2. If you do not receive the test email:
   1. In the CLI console, enter the following CLI commands to collect the debug logs:

      ```
      diagnose debug reset
      diagnose debug enable
      diagnose debug console timestamp enable
      diagnose debug application alertmail -1
      ```

   2. In the CLI console, enter the following CLI command to send a test email:

      ```
      diagnose log alertmail test
      ```

   3. In the CLI console, enter the following CLI commands to disable debugging:

      ```
      diagnose debug disable
      diagnose debug reset
      ```

3. To save the output, select *Download* from the top-right of the CLI window or use PuTTY to log the output.

How FortiPAM chooses the sender email address

1. FortiPAM uses the sender email address in *Log & Report* > *Email Alert Settings* to send alert emails.
2. FortiPAM uses the sender email address from the *Email Service* pane in *System* > *Settings*.

3. A concatenation of `system.email-server.user` and `system.email-server.server` (`user@server`).
4. The default email (`fortipam@fortinet.com`).

ZTNA tags

For an introduction to Zero Trust Network Access (ZTNA), see Zero Trust Network Access introduction in the FortiOS Admin Guide.

In *System* > *ZTNA Tags*, you can set up proxy rules and ZTNA tags.

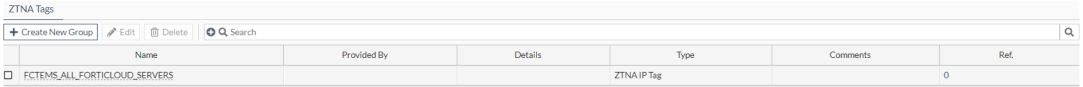
ZTNA servers can only be set using the CLI command:

- `config firewall access-proxy`

New proxy rules can only be created using the CLI command:

- `config firewall policy`

The *ZTNA Tags* tab looks like the following:



	Name	Provided By	Details	Type	Comments	Ref.
□	FCTEMS_ALL_FORTICLOUD_SERVERS			ZTNA IP Tag		0

The following options are available in the *ZTNA Tags* tab:

+Create New Group	Select to create a ZTNA tag group. See Creating a ZTNA tag group on page 382
Edit	Select to edit the selected tag group.
Delete	Select to delete the selected tag groups.
Search	Use the search bar to look for a tag. To narrow down your search in the *ZTNA Tags* tab, see Column filter.
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 tag group

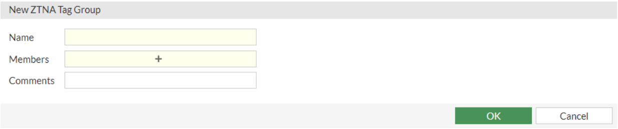
After FortiPAM connects to the FortiClient EMS, it automatically synchronizes ZTNA tags.

ZTNA tags related information is listed in the ZTNA tags list. You can customize ZTNA tag groups to categorize user access based on multiple tags.

Hover over a tag name to see more information about the tag, such as its resolved address.

To create a ZTNA group:

1. Go to *System* > *ZTNA Tags*.
2. Select +*Create New Group*.
   The *New ZTNA Tag Group* window opens.



New ZTNA Tag Group

Name

Members +

Comments

3. In *Name*, enter a name for the group.
4. In *Members*, select +, and from the *Select Entries* window, select members or create new members.

   Use the search bar to look for a member.

5. Optionally, enter comments about the ZTNA tag group.
6. Click *OK*.

ZTNA user control

When ZTNA control is set up on FortiPAM, you can only connect to FortiPAM and launch a secret from the endpoint PC with allowed ZTNA tags. The endpoint PC must install FortiClient and connect to the same EMS server.

To use the FortiPAM ZTNA control feature:

- You must connect to the same EMS server for the client where the FortiClient runs.
- You must enable `ztna-status` when configuring a proxy rule (`config firewall policy`).
- You must configure another access proxy with a different VIP and client certificate disabled to launch secrets without ZTNA control successfully for clients not connected to the same EMS as FortiPAM.

In FortiClient EMS 7.2.x, you must set the `<gateways_enabled>` flag to `1` to enable proxy based connections.

In FortiClient EMS 7.4.x and later, you do not need to set the `<gateways_enabled>` flag for accessing proxy based connections using FortiPAM.

To set up EMS in the GUI:

1. Go to *Network* > *Fabric Connectors*.
2. Select *FortiClient EMS* and click *Edit*.
3. In *Name*, enter the EMS name.
4. In *IP/Domain name*, enter the IP address or the domain name of the EMS.
5. In *HTTPS port*, enter the HTTPS port for the EMS.

6. Click *OK*.

Refer to *FortiClient EMS Status* to check the status of the FortiClient EMS.

If there is an error connecting to the EMS server, log in to the EMS server, authorize FortiPAM in *Administration* > *Fabric Device*, and click *Accept* in *Verify EMS Server Certificate*.

For more information, see Fabric Connectors on page 366.

To set EMS using the CLI:

1. In the CLI console, enter the following commands to configure an EMS:

```
config endpoint-control fctems
   edit "ems_200"
      set server "10.59.112.200"
   next
end
```

2. After adding an EMS server, the CLI asks you to verify using `execute fctems verify ems_200`.

- example

```
execute fctems verify ems_200
   Subject: C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = FortiClient, CN
         = FCTEMS8822002925, emailAddress = support@fortinet.com
   Issuer: C = US, ST = California, L = Sunnyvale, O = Fortinet, OU = Certificate
         Authority, CN = support, emailAddress = support@fortinet.com
   Valid from: 2022-04-25 18:17:42 GMT
   Valid to: 2038-01-19 03:14:07 GMT
   Fingerprint: 35:12:95:DA:A5:2E:20:F9:8F:99:88:75:25:BC:D8:A3
   Root CA: No
   Version: 3
   Serial Num:
   a4:35:c8
   Extensions:
   Name: X509v3 Basic Constraints
   Critical: no
   Content:
   CA:FALSE
EMS configuration needs user to confirm server certificate.
Do you wish to add the above certificate to trusted remote certificates? (y/n)y
Certificate successfully configured and verified.
```

If authentication is denied, log in to the EMS server and authorize FortiPAM in *Administration* > *Fabric Device*.

Using EMS tag for endpoint control

You can create Zero Trust tagging rules for endpoints on an EMS server based on operating system versions, logged-in domains, running processes, and other criteria. EMS uses the rules to dynamically group endpoints with different tags. FortiPAM can use these ZTNA tags in proxy rules (firewall policy) to control which endpoint has access to FortiPAM. For this, at least one FortiClient EMS must be added in *Network* > *Fabric Connectors*, and FortiPAM must be successfully connected to this EMS server.

FortiClient EMS is a security management solution that enables scalable and centralized management of endpoints. See ZTNA tag control example on page 385.

ZTNA tag control - example

To add ZTNA tag control using the CLI:

In the access proxy, `client-cert` must be enabled. You can use `ztna-ems-tag` to give FortiPAM access to endpoints with this tag.

1. In the CLI console enter the following commands:

```
config firewall access-proxy
   edit "fortipam_access_proxy"
      set vip "fortipam_vip"
      set client-cert enable #Must be enabled
      config api-gateway
         edit 1
            set url-map "/pam"
            set service pam-service
         next
         edit 2
            set url-map "/tcp"
            set service tcp-forwarding
            config realservers
               edit 1
                  set address "all"
               next
            end
         next
         edit 3
            set service gui
            config realservers
               edit 1
                  set ip 127.0.0.1
                  set port 80
               next
            end
         next
      end
   next
end
config firewall policy
   edit 1
      set type access-proxy
      set name "FortiPAM_Default"
      set srcintf "any"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set access-proxy "fortipam_access_proxy"
      set ztna-ems-tag "FCTEMS8822002925_pam-ems-tag-office" #Only endpoints with this
         tag can access FortiPAM
      set utm-status enable
      set groups "SSO_Guest_Users"
```

```
     set ssl-ssh-profile "deep-inspection"
   next
end
```

ZTNA-based FortiPAM access control

When ZTNA control is enforced on FortiPAM, devices without FortiClient installed cannot access FortiPAM.

> If you want to grant access to the user using the browser extension-only solution, you can create multiple proxy rules to achieve this. See CLI configuration for a user with browser extension-only solution example on page 388.

Enable ZTNA control to only allow endpoints with selected tags to access FortiPAM

To enable ZTNA control:

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

```
 config firewall policy
  edit 1
   set type access-proxy
   set ztna-status enable
   set name "FortiPAM_Default"
   set srcintf "any"
   set srcaddr "all"
   set dstaddr "all"
   set action accept
   set schedule "always"
   set access-proxy "fortipam_access_proxy"
   set ztna-ems-tag "FCTEMS8822002925_pam-ems-tag-office" #Only endpoints with this tag
can access FortiPAM
   set utm-status enable
   set groups "SSO_Guest_Users"
   set ssl-ssh-profile "deep-inspection"
  next
 end
```

2. From the user dropdown on the top-right, select *Logout*.
3. When attempting to log in, a certificate check appears on the browser.
   Click *OK* to proceed with logging in to FortiPAM.

CLI configuration for a user from endpoint installed with FortiClient (multiple proxy rules) - example

In this example, a user from an endpoint installed with FortiClient can access FortiPAM via VIP `192.168.1.109` provided that the endpoint contains `FCTEMS8822008307_Office_Windows_PC` or `FCTEMS8822008307_MIS_Team` ZTNA tag.

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

```
config firewall vip
   edit "fortipam_vip"
```

```
      set type access-proxy
      set extip 192.168.1.109
      set extintf "any"
      set server-type https
      set extport 443
      set ssl-certificate "Fortinet_SSL"
   next
end
config firewall access-proxy
   edit "fortipam_access_proxy"
      set vip "fortipam_vip"
      set client-cert enable
      config api-gateway
         edit 1
            set url-map "/pam"
            set service pam-service
         next
         edit 2
            set url-map "/tcp"
            set service tcp-forwarding
            config realservers
               edit 1
                  set address "all"
               next
            end
         next
         edit 3
            set service gui
            config realservers
               edit 1
                  set ip 127.0.0.1
                  set port 80
               next
            end
         next
      end
   next
end
config firewall policy
   edit 1
      set type access-proxy
      set name "FortiPAM_Default"
      set srcintf "any"
      set srcaddr "all"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set access-proxy "fortipam_access_proxy"
      set ztna-ems-tag "FCTEMS8822008307_Office_Windows_PC" "FCTEMS8822008307_MIS_
            Team"
         set groups "SSO_Guest_Users"
         set ssl-ssh-profile "deep-inspection"
   next
end
```

CLI configuration for a user with browser extension-only solution - example

In this example, users with IP address `192.168.1.2` access FortiPAM via the VIP `192.168.1.108` from an endpoint with no FortiClient installed or no match with the ZTNA policy in the previous example.

The firewall policy is more restrictive than the previous example and allows fewer source addresses. Two VIPs are required for this setup. Also, you can set it up to allow access within a certain schedule only.

The `access-proxy` setting links to the name of the corresponding firewall access-proxy. The VIP setting links to the name of the corresponding firewall VIP. The VIP represents the FortiPAM ZTNA gateway to which clients make HTTPS connections. The service/server mappings define the virtual host matching rules and the actual server mappings of the HTTPS requests. When creating an access proxy, it is recommended to copy the default access proxy and modify only the VIP and `client-cert` settings to ensure proper configuration.

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

```
config firewall vip
   edit "fortipam_vip-no-ztna"
      set type access-proxy
      set extip 192.168.1.108
      set extintf "any"
      set server-type https
      set extport 443
      set ssl-certificate "Fortinet_SSL"
   next
end
config firewall access-proxy
   edit "fortipam_access_proxy-no-ztna"
      set vip "fortipam_vip-no-ztna"
      config api-gateway
         edit 1
            set url-map "/pam"
            set service pam-service
         next
         edit 2
            set url-map "/tcp"
            set service tcp-forwarding
            config realservers
               edit 1
                  set address "all"
               next
            end
         next
         edit 3
            set service gui
            config realservers
               edit 1
                  set ip 127.0.0.1
                  set port 80
               next
            end
         next
      end
   next
end
config firewall address
   edit "192.168.1.2"
```

```
      set subnet 192.168.1.2 255.255.255.255
   next
end
config firewall policy
   edit 2
      set type access-proxy
      set name "no ZTNA"
      set srcintf "any"
      set srcaddr "192.168.1.2"
      set dstaddr "all"
      set action accept
      set schedule "always"
      set access-proxy "fortipam_access_proxy-no-ztna"
      set groups "SSO_Guest_Users"
      set ssl-ssh-profile "deep-inspection"
   next
end
```

High availability

Multiple FortiPAM units can operate as an high availability (HA) cluster to provide even higher reliability.

FortiPAM can operate in Active-Passive HA mode.

Active-Passive: Clustered fail-over mode where all of the configuration is synchronized between the devices.

PAM configurations, such as users and secrets, are automatically synced to secondary devices to ensure PAM services can be operated or recovered when the primary device is down. All tasks are handled by the primary device as long as system events and logs are only recorded on the primary device.

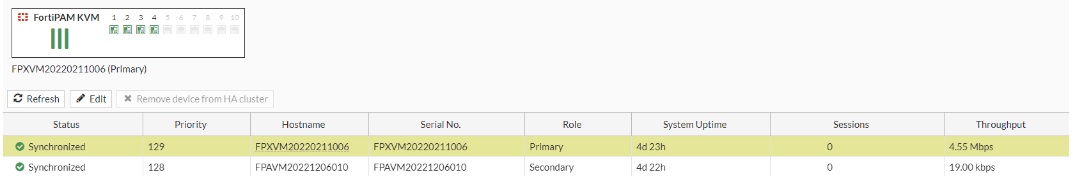
Your FortiPAM device can be configured as a standalone unit, or you can configure up to three FortiPAM devices in HA, one Active and up to two Passive mode devices, for failover protection and/or disaster recovery.

HA requires an additional license for each cluster unit with the same number of seats as you have for the primary FortiPAM. Each FortiPAM device in HA must be the same device model and version number.

Logs recorded in HA are not synchronized between the primary and the secondary unit's disks. Further, secret videos recorded in HA mode are not available from FortiAnalyzer.

FortiPAM displays the device's serial number that exclusively contains the log records.

The following shows FortiPAM devices in Active-Passive mode:



FPXVM20220211006 (Primary)

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 *Standalone* or *Active-Passive*. If you select *Standalone*, no other options are displayed.
Device priority	You can set a different device priority for each cluster member to control the order in which cluster units become the primary unit (HA primary) when the primary unit fails. The device with the highest device priority becomes the primary unit (default = 128, 0 - 255). Since all videos and logs are only stored on the primary device, one FortiPAM should be configured with higher priority. And with override enabled, the primary unit with the highest device priority will always become the primary unit. The override setting and device priority value are not synchronized to all cluster units. You must enable override and adjust device priority manually and separately for each cluster unit.
Cluster Settings	

Group name	Enter a name to identify the cluster.
Password	Select *Change* to enter a password to identify the HA cluster. The maximum password length is 15 characters. The password must be the same for all cluster FortiPAM units before the FortiPAM units can form the HA cluster. It is suggested that you add a password to protect the HA cluster Different HA clusters on the same network must have different group names. When configuring HA clusters in the CLI, different HA clusters on the same network must have different `group-id` and `group-name`.
Monitor interfaces	Select the specific ports to monitor or create new interfaces. Use the search bar to look for an interface. Use the pen icon next to the interface to edit it. If a monitored interface fails or is disconnected from its network, the interface leaves the cluster and a link failover occurs. The link failover causes the cluster to reroute the traffic being processed by that interface to the same interface of another cluster that still has a connection to the network. This other cluster becomes the new primary unit.
Heartbeat interfaces	Select to enable or disable the HA heartbeat communication for each interface in the cluster and then set the heartbeat interface priority. You can also create new interfaces. Use the search bar to look for an interface. Use the pen icon next to the interface to edit it. The heartbeat interface with the highest priority processes all heartbeat traffic. You must select at least one heartbeat interface. If the interface functioning as the heartbeat fails, the heartbeat is transferred to another interface configured as a heartbeat interface. If heartbeat communication is interrupted, the cluster stops processing traffic. Priority ranges from 0 to 512.

	Heartbeat interfaces should use dedicated interfaces and not share the VIP interface.

Management Interface Reservation

Enable or disable the management interface reservation.

Note: The option is disabled by default.

You can provide direct management access to individual cluster units by reserving a management interface as part of the HA configuration. After this management interface is reserved, you can configure a different IP address, administrative access, and other interface settings for this interface for each cluster unit. You can also specify static routing settings for this interface. Then by connecting this interface of each cluster unit to your network, you can manage each cluster unit separately from a different IP address.

Only by using SSH can you access a FortiPAM node via HA management interface reservation.

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

There are two options for setting up the HA heartbeat: unicast and broadcast.

Broadcast is the default HA heartbeat configuration. However, the broadcast configuration is not ideal for the VM platform because it requires special host settings. In most cases, the unicast configuration is preferable.

Enable the unicast HA heartbeat in virtual machine (VM) environments that do not support broadcast communication.

Note: The option is disabled by default.

Note: The pane is only available when the *Mode* is *Active-Passive*.

When disabling this option to change from HA unicast to broadcast, you must reboot all units in the cluster for the change to take effect.

When the broadcast mode is used, as a best practice, isolate the heartbeat devices from the user network by connecting the heartbeat devices to a dedicated switch not connected to any network.
The heartbeat packet contains sensitive information about the cluster configuration and may use a considerable amount of bandwidth.
If the cluster consists of two FortiPAM devices, connect the heartbeat device interfaces back to back using a crossover cable.
If there are more than two FortiPAM devices, each heartbeat interface should be connected to a dedicated switch.
For example, in a three member HA cluster with two heartbeat interfaces, there are two switches, one switch dedicated to each interface.

Peer IP	Enter the IP address of the HA heartbeat interface of the other FortiPAM-VM in the HA cluster. **Note**: The option is only available when *Unicast Heartbeat* is enabled.
Override	Enable to use the primary server by default whenever it is available. **Note**: The option is enabled by default.

3. Click *OK*.

HA failover

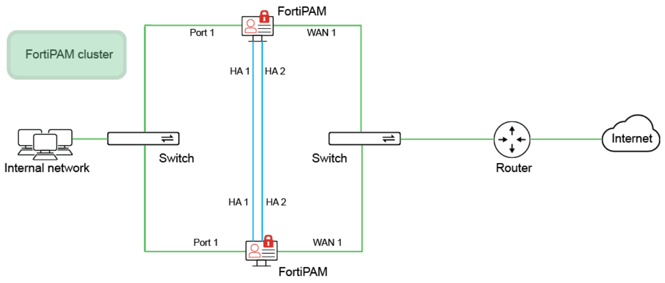
When primary FortiPAM is down, secondary will take the primary role and permanently enter maintenance mode. Under maintenance mode, all critical processes will be temporarily suspended.

The administrator can bring up the original primary device or disable maintenance mode on the new primary device to resume all FortiPAM features.

HA active-passive cluster setup

An HA Active-Passive (A-P) cluster can be set up using the GUI or CLI.

This example uses the following network topology:

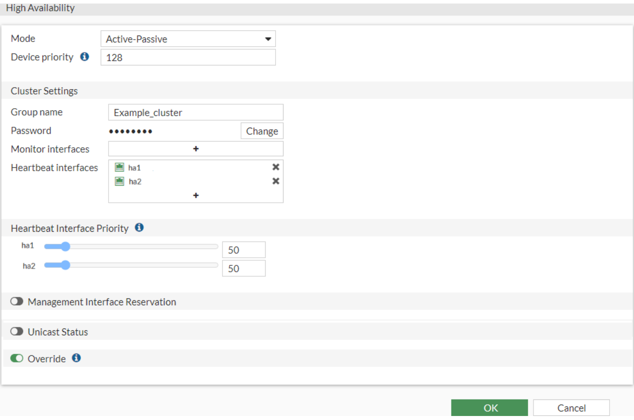


To set up an HA A-P cluster using the GUI:

1. Make all the necessary connections as shown in the topology diagram.
2. Log into one of the FortiPAM devices.
3. Go to *System* > *HA* and set the following options:

Mode	*Active-Passive*.
Device priority	128 or higher.
Group name	Example_cluster.
Heartbeat interfaces	ha1 and ha2.

Except for the device priority, these settings must be the same on all FortiPAM devices in the cluster.



High Availability

Mode: Active-Passive
Device priority: 128

Cluster Settings

Group name: Example_cluster
Password: ••••••••
Monitor interfaces:
Heartbeat interfaces: ha1, ha2

Heartbeat Interface Priority

ha1: 50
ha2: 50

○ Management Interface Reservation

○ Unicast Status

● Override

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 32.

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 31.
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.

When `firewall.vip` is configured in the system's `vdom-exception` list, configuration changes related to the interface GUI portal must be manually applied on the secondary and DR nodes. This is especially important for changes involving enabling the GUI portal on another interface, setting an external IP address, adjusting the service port, and configuring the SSL certificate. Otherwise, HA synchronization will fail due to "firewall.policy" and "firewall access-proxy" being out of sync.

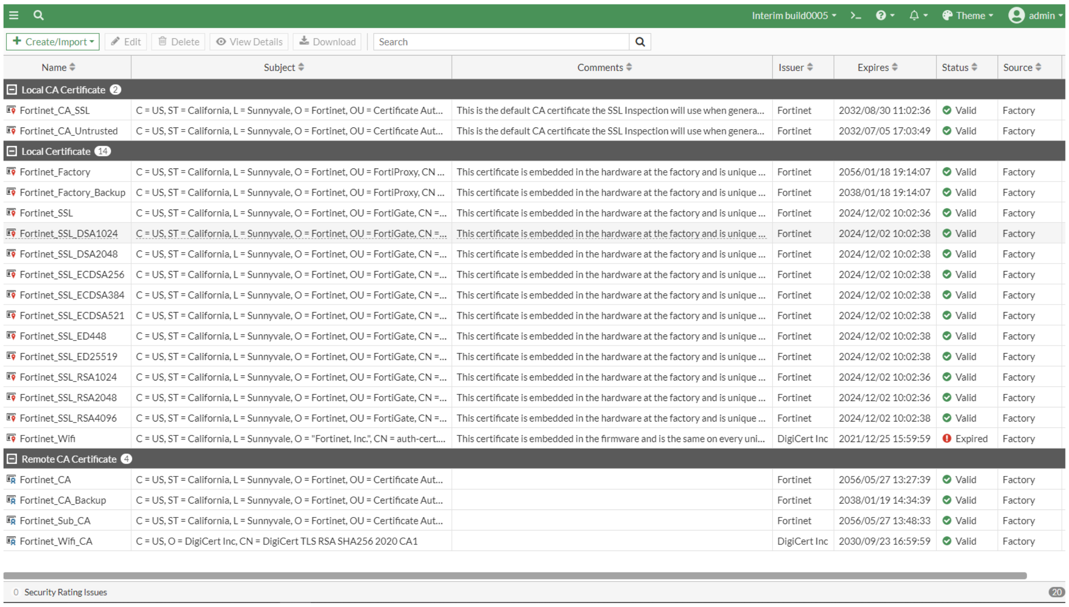
For example: After enabling the GUI portal on another interface, such as "port2," on the primary node, the following firewall VIP configuration is automatically created:

```
config firewall vip
   edit "port2_auto_create_vip"
      set type access-proxy
      set extip 10.1.100.63
      set extintf "port2"
      set server-type https
      set extport 443
      set ssl-certificate "Fortinet_SSL"
   next
end
```

Manually copy and paste the above configuration to the secondary and DR nodes. Modify `extip` and any related settings if a different subnet is used on the DR node.

Certificates

Go to *System* > *Certificates* to manage certificates.



Name	Subject	Comments	Issuer	Expires	Status	Source
Local CA Certificate 2						
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	2032/08/30 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	2032/07/05 17:03:49	✓ Valid	Factory
Local Certificate 14						
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_ECDSA521	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 4						
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

0 Security Rating Issues

20

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.

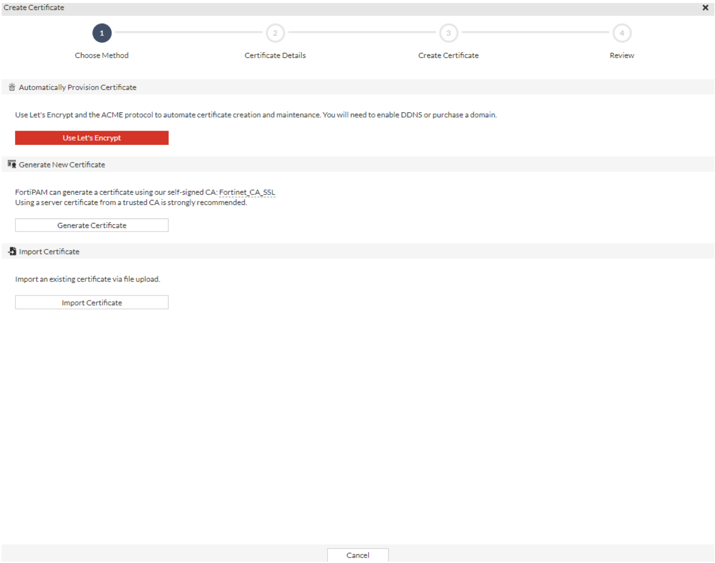
The *Certificates* tab contains the following options:

+Create/Import	From the dropdown, select *Certificate*, *Generate CSR*, *CA Certificate*, *Remote Certificate*, and *CRL*. See: • Creating a certificate on page 399 • Generating a CSR (Certificate Signing Request) on page 402 • Importing CA certificate on page 405 • Uploading a remote certificate on page 406 • Importing a CRL (Certificate revocation list) on page 406
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.



Use Let's Encrypt and the ACME protocol to automate certificate creation and maintenance. You will need to enable DDNS or purchase a domain.

FortiPAM can generate a certificate using our self-signed CA: Fortinet_CA_SSL
Using a server certificate from a trusted CA is strongly recommended.

Import an existing certificate via file upload.

3. Enter the following information:

Choose Method	
Automatically Provision Certificate	Select *Use Let's Encrypt* to automatically create a certificate using the ACME protocol with Let's Encrypt service. You will need to enable DDNS or purchase a domain.
Generate New Certificate	Select *Generate Certificate* to generate a certificate using the self-signed `Fortinet_CA_SSL` CA. Using a server certificate from a trusted CA is strongly recommended.
Import Certificate	Select *Import Certificate* to import an existing certificate by uploading the file.
Certificate Details Enter the certificate details and click *Create* to create a certificate.	
Automatically Provision Certificate	The certificate will be automatically provisioned using the ACME protocol with the Let's Encrypt service. It is the easiest way to install a trusted certificate.
Certificate name	The name of the certificate.
Domain	The public FQDN of FortiPAM. **Note**: The option is only available when the *Chosen Method* is *Automatically Provision Certificate*.
Email	The email address. **Note**: The option is only available when the *Chosen Method* is *Automatically Provision Certificate*.
Set ACME Interface	If this is the first time enrolling a server certificate with Let's Encrypt on this FortiPAM unit, the *Set ACME Interface* pane opens. **Note**: The options in the pane are only available when the *Chosen Method* is *Automatically Provision Certificate*.
ACME Interface	Select + and from *Select Entries*, select ports, or create new interfaces on which the ACME client will listen for challenges to provision and renew certificates. Click *OK* when you have selected interfaces. Use the search bar to look for an interface.

	Use the pen icon next to the interface to edit it.
Generate New Certificate	
Certificate authority	The certificate authority. **Note**: The option is only available when the *Chosen Method* is *Generate New Certificate*.
Common name	The common name of the certificate. Enter an FQDN or an IPv4 address. The common name should match the FQDN or the IP address of the primary SSL-VPN interface. **Note**: The option is only available when the *Chosen Method* is *Generate New Certificate*.
Subject alternative name	An IP address or FQDN. Subject alternative names (SAN) allow you to protect multiple host names with a single SSL certificate. SAN is part of the X.509 certificate standard. **Note**: The option is only available when the *Chosen Method* is *Generate New Certificate*.
Update Your List of Trusted Certificate Authorities	Select *Download CA Certificate* to download `Fortinet_CA_SSL` CA to your computer. `Fortinet_CA_SSL` is a local CA certificate. To avoid certificate warnings, you must download it and install it on each client machine. **Note**: The option is only available when the *Chosen Method* is *Generate New Certificate*.
Import Certificate	
Type	Select from the following three options: • *Local Certificate* • *PKCS #12 Certificate* • *Certificate* **Note**: The option is only available when the *Chosen Method* is *Import Certificate*.
Certificate file	Select *+Upload* and locate the certificate file on your local computer. **Note**: The option is only available when the *Chosen Method* is *Import Certificate* and the *Type* is either *Local Certificate* or *Certificate*.
Certificate with key file	Select *+Upload* and locate the certificate with key file on your local computer.

	Note: The option is only available when the *Chosen Method* is *Import Certificate* and the *Type* is *PKCS #12 Certificate*.
Password	Enter the password. **Note**: The option is only available when the *Chosen Method* is *Import Certificate* and the *Type* is either *PKCS #12 Certificate* or *Certificate*.
Confirm Password	Reenter the password to confirm. **Note**: The option is only available when the *Chosen Method* is *Import Certificate* and the *Type* is *PKCS #12 Certificate* or *Certificate*.
Key file	Select *+Upload* and locate the key file on your local computer. **Note**: The option is only available when the *Chosen Method* is *Import Certificate* and the *Type* is *Certificate*.
Review Enable *ACME log* to see logs related to the certificate created using the ACME protocol. **Note**: The option is only available when *Chosen Method* is *Automatically Provision Certificate*.	
Update Your List of Trusted Certificate Authorities	If you have not already downloaded the `Fortinet_CA_SSL` CA to your computer, select *Download CA Certificate* to download it. **Note**: The option is only available when the *Chosen Method* is *Generate New Certificate*.

4. Click *OK*.

Generating a CSR (Certificate Signing Request)

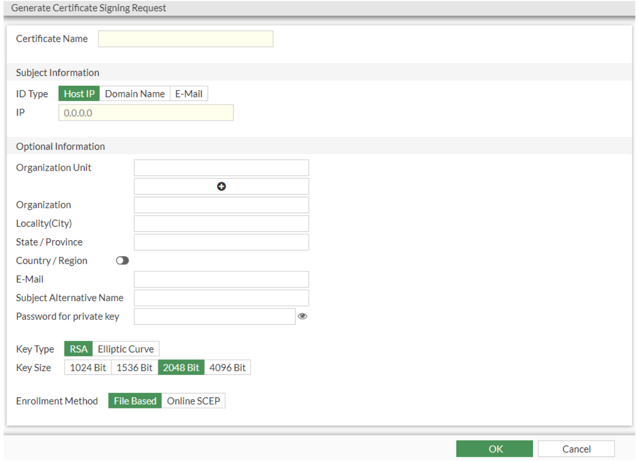
Whether you create certificates locally or obtain them from an external certificate service, you need to generate a Certificate Signing Request (CSR).

When a CSR is generated, a private and public key pair is created for FortiPAM. The generated request includes the public key of the device, and information such as the unit’s public static IP address, domain name, or email address. The device private key remains confidential on the unit.

After the request is submitted to a CA, the CA verifies the information and register the contact information on a digital certificate that contains a serial number, an expiration date, and the public key of the CA. The CA then signs the certificate, after which you can install the certificate on FortiPAM.

To generate a CSR:

1. Go to *System* > *Certificates*.
2. From +*Create/Import*, select *Generate CSR*.
   The *Generate Certificate Signing Request* window opens.



Generate Certificate Signing Request

Certificate Name

Subject Information

ID Type: Host IP

IP: 0.0.0.0

Optional Information

Organization Unit

Organization

Locality(City)

State / Province

Country / Region

E-Mail

Subject Alternative Name

Password for private key

Key Type: RSA

Key Size: 2048 Bit

Enrollment Method: File Based

3. Enter the following information:

Certificate Name	Enter a unique name for the certificate request, such as the host name or the serial number of the device. Do not include spaces in the certificate to ensure compatibility as a PKCS12 file.
Subject Information	
ID Type	Select the ID type: • *Host IP*: Select if the unit has a static IP address. Enter the device IP address in the *IP* field (default). • *Domain Name*: Enter the device domain name or FQDN in the *Domain Name* field. • *E-mail*: Enter the email address of the device administrator in the *E-mail* field.
Optional Information Optional information to further identify the device.	
Organizational Unit	The name of the department. Up to 5 OUs can be added.
Organization	The legal name of the company or organization.
Locality (City)	The name of the city where the unit is located.
State/Province	The name of the state or province where the unit is located.
Country/Region	Enable and then enter the country where the unit is located. Select from the dropdown. The option is disabled by default.
E-mail	The contact email address.
Subject Alternative Name	One or more alternative names, separated by commas, for which the certificate is also valid. An alternative name can be: email address, IP address, URI, DNS name, or a directory name. Each name must be preceded by its type, for example: IP:`1.2.3.4`, or URL: `http://your.url.here/`.
Password for private key	The password for the private key.

Key Type	Select *RSA* or *Elliptic Curve*. **Note**: The default is RSA.
Key Size	If you selected *RSA* for the *Key Type*, select the *Key size*: *1024 Bit*, *1536 Bit*, *2048 Bit* (default), or *4096 Bit*. ⚠ Larger key sizes are more secure but slower to generate. If you selected *Elliptic Curve* for the *Key Type*, select the *Curve Name*: *secp256r1* (default), *secp384r1*, or *secp521r1*.
Enrollment Method	Select the enrollment method. • *File Based*: Generate the certificate request (default). • *Online SCEP*: Obtain a signed, Simple Certificate Enrollment Protocol (SCEP) based certificate automatically over the network. Enter the CA server URL and challenge password in their respective fields.

4. Click *OK*.

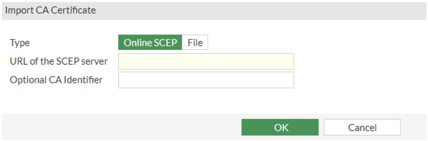
Importing CA certificate

CA root certificates are similar to local certificates, however they apply to a broader range of addresses or to whole company; they are one step higher up in the organizational chain. Using the local certificate example, a CA root certificate would be issued for all of `www.example.com` instead of just the smaller single web page.

You can import a CA certificate to FortiPAM.

To import a CA certificate:

1. Go to *System* > *Certificates*.
2. From *+Create/Import*, select *CA Certificate*.
   The *Import CA Certificate* window opens.



3. Enter the following information:

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

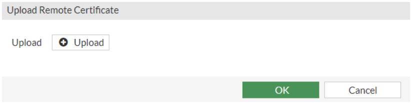
4. Click *OK*.

Uploading a remote certificate

Remote certificates are public certificates without a private key. Remote certificates can be uploaded to the FortiPAM unit.

To upload a remote certificate:

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



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

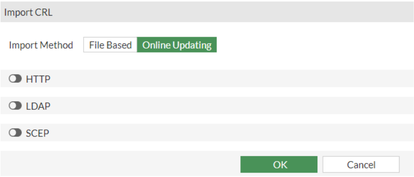
Importing a CRL (Certificate revocation list)

Certificate revocation list (CRL) is a list of certificates that have been revoked and are no longer usable. This list includes certificates that have expired, been stolen, or otherwise compromised. If your certificate is on this list, it will not be accepted. CRLs are maintained by the CA that issues the certificates and includes the date and time when the next CRL will be issued as well as a sequence number to help ensure you have the most current version of the CRL.

CRLs can be imported to FortiPAM.

To import a CRL:

1. Go *System* > *Certificates*.
2. From *+Create/Import*, select *CRL*.
   The *Import CRL* window opens.



3. Enter the following information:

Imported Method	Select either *File Based* or *Online Updating*.
+Upload	Select and locate the certificate file on your computer. **Note**: The option is only available when the *Imported Method* is *File Based*.

HTTP

Enable HTTP updating and enter the *URL of the HTTP server*.

Note: The option disabled by default.

Note: The pane is only available when the *Imported Method* is *Online Updating*.

LDAP

Enable LDAP updating and select an LDAP server from the dropdown or create a new one.

Use the search bar to look for an LDAP server.

Use the pen icon next to an LDAP server to edit the server.

Enter the *Username* and the *Password*.

Note: The option disabled by default.

Note: The pane is only available when the *Imported Method* is *Online Updating*.

SCEP

Enable SCEP updating and select a local certificate or create a new certificate for SCEP communication for the online CRL.

Use the search bar to look for a certificate.

Enter the *URL of the SCEP server*.

Note: The option disabled by default.

Note: The pane is only available when the *Imported Method* is *Online Updating*.

4. Click *OK*.

Replacement messages

Replacement Messages in *System* displays a list of replacement messages.

You can customize the appearance of some web pages to fit your style requirements, e.g., the login page can be customized to include organization name and logo.

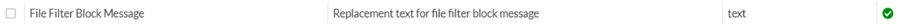
There are two types of replacement messages in FortiPAM:

- **Plain text**: Simpler customization where only the text content can be changed.
- **HTML**: Supports advanced customization.

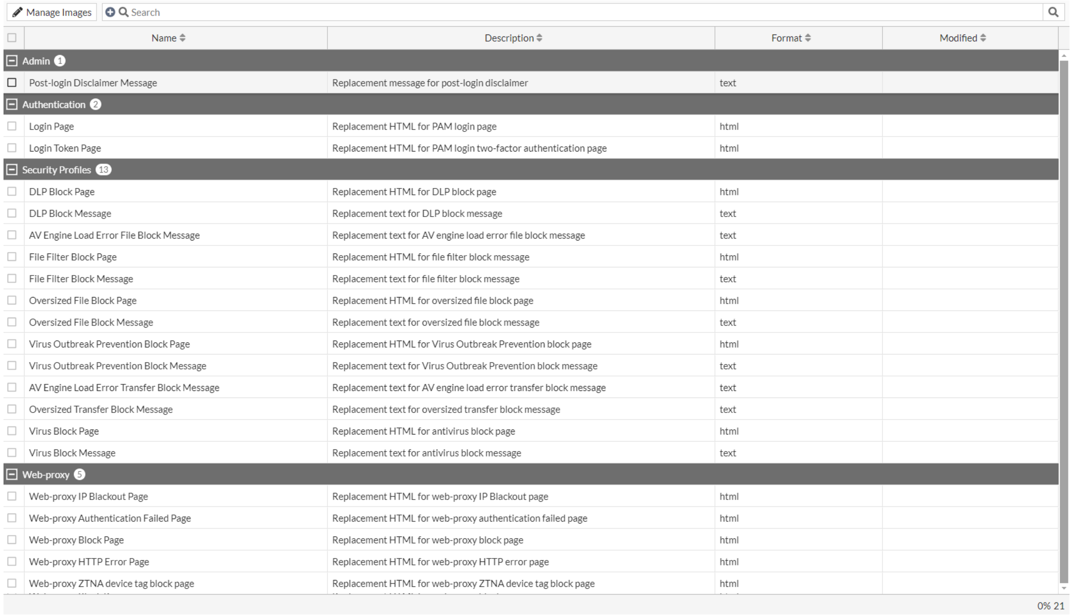
  You can customize text, re-layout or apply styles to the web components using CSS and insert images using image tags.

For every replacement message, the following columns are displayed:

- *Name*
- *Description*
- *Format*
- *Modified*: If a default replacement message is edited, a green check mark is displayed in the *Modified* column.



□	File Filter Block Message	Replacement text for file filter block message	text	✓



□	Name	Description	Format	Modified
⊟	Admin 1			
□	Post-login Disclaimer Message	Replacement message for post-login disclaimer	text	
⊟	Authentication 2			
□	Login Page	Replacement HTML for PAM login page	html	
□	Login Token Page	Replacement HTML for PAM login two-factor authentication page	html	
⊟	Security Profiles 13			
□	DLP Block Page	Replacement HTML for DLP block page	html	
□	DLP Block Message	Replacement text for DLP block message	text	
□	AV Engine Load Error File Block Message	Replacement text for AV engine load error file block message	text	
□	File Filter Block Page	Replacement HTML for file filter block message	html	
□	File Filter Block Message	Replacement text for file filter block message	text	
□	Oversized File Block Page	Replacement HTML for oversized file block page	html	
□	Oversized File Block Message	Replacement text for oversized file block message	text	
□	Virus Outbreak Prevention Block Page	Replacement HTML for Virus Outbreak Prevention block page	html	
□	Virus Outbreak Prevention Block Message	Replacement text for Virus Outbreak Prevention block message	text	
□	AV Engine Load Error Transfer Block Message	Replacement text for AV engine load error transfer block message	text	
□	Oversized Transfer Block Message	Replacement text for oversized transfer block message	text	
□	Virus Block Page	Replacement HTML for antivirus block page	html	
□	Virus Block Message	Replacement text for antivirus block message	text	
⊟	Web-proxy 5			
□	Web-proxy IP Blackout Page	Replacement HTML for web-proxy IP Blackout page	html	
□	Web-proxy Authentication Failed Page	Replacement HTML for web-proxy authentication failed page	html	
□	Web-proxy Block Page	Replacement HTML for web-proxy block page	html	
□	Web-proxy HTTP Error Page	Replacement HTML for web-proxy HTTP error page	html	
□	Web-proxy ZTNA device tag block page	Replacement HTML for web-proxy ZTNA device tag block page	html	

- The following options are available in *Replacement Messages*:

Manage Images	Select to view the available images and their respective tags and add new images. By default, images are embedded in replacement messages instead of using a URL. See Managing images on page 413.
Search	Enter a search term in the search field, then hit `Enter` to search the replacement messages list. To narrow down your search, see Column filter.
Edit	Select to edit the selected replacement message. See Editing a replacement message on page 411.

To define a filter, see Filters on page 34 in Tables on page 34.

For column related settings, see Column settings on page 37 in Tables on page 34.

Tags

Dynamic values can be inserted to replacement message templates to provide additional information. This can be achieved by inserting tags (template variables) to the replacement message template (`%%<VARIABLE_NAME>%%`).

For example, in the *Post-login Disclaimer Message*, tags `%%LAST_SUCCESSFUL_LOGIN%%` and `%%LAST_FAILED_LOGIN%%` are present:

```
POST WARNING:
This is a private computer system. Unauthorized access or use
is prohibited and subject to prosecution and/or disciplinary
action.
...
...

%%LAST_SUCCESSFUL_LOGIN%%
%%LAST_FAILED_LOGIN%%
```

When the message is displayed to the user, these variables are replaced with the correct information.

For example:

```
POST WARNING:
This is a private computer system. Unauthorized access or use
is prohibited and subject to prosecution and/or disciplinary
action.
...
...

Last Successful Login: Thu Feb 22 13:46:28 2024
Last Failed Login: Thu Feb 22 13:46:28 2024
```

Both the HTML and the plain text template support `%%<VARIABLE_NAME>%%` variable.

Further, there is a special variable for inserting images (`%%IMAGE:<IMAGE_NAME>%%`), which can only be used in the HTML message format. When an image URL is required as part of a replacement message, the image tag can be used.

Note that when using the image tag, double quotation marks should not be used.

For example:

The following image tag is correct:

```
<img src=%%IMAGE:logo_fnet%%>
```

The following image tag is incorrect:

```
<img src="%%IMAGE:logo_fnet%%">
```

Another example:

```
<style>
  .logo {
    background-image: url(%%IMAGE:logo_fnet%%);  #correct
  }
.bad-logo {
  background-image: url("%%IMAGE:logo_fnet%%"); #incorrect #Don't use ""
</style>
```

For information on managing images, see Managing images on page 413.

Replacement messages descriptions

The following table outlines all the messages that can be customized and their descriptions.

Admin

Post-login Disclaimer Message	Replacement message for the post-login disclaimer.

Authentication

Login Page	Replacement HTML for the FortiPAM login page.
Login Token Page	Replacement HTML for the FortiPAM login two-factor authentication page.

Security Profiles

DLP Block Page	Replacement HTML for the DLP block page.
DLP Block Message	Replacement text for the DLP block message.
AV Engine Load Error File Block Message	Replacement text for the AV engine load error file block message.
File Filter Block Page	Replacement HTML for the file filter block message.

File Filter Block Message	Replacement text for the file filter block message.
Oversized File Block Page	Replacement HTML for the oversized file block page.
Oversized File Block Message	Replacement text for the oversized file block message.
Virus Outbreak Prevention Block Page	Replacement HTML for the Virus Outbreak Prevention block page.
Virus Outbreak Prevention Block Message	Replacement text for the Virus Outbreak Prevention block message.
AV Engine Load Error Transfer Block Message	Replacement text for the AV engine load error transfer block message.
Oversized Transfer Block Message	Replacement text for the oversized transfer block message.
Virus Block Page	Replacement HTML for the AntiVirus block page.
Virus Block Message	Replacement text for the AntiVirus block message.

Web Proxy

Web-proxy IP Blackout Page	Replacement HTML for the web proxy IP Blackout page.
Web-proxy Authentication Failed Page	Replacement HTML for the web proxy authentication failed page.
Web-proxy Block Page	Replacement HTML for the web proxy block page.
Web-proxy HTTP Error Page	Replacement HTML for the web proxy HTTP error page.
Web-proxy ZTNA device tag block page	Replacement HTML for the web proxy ZTNA device tag block page.

Editing a replacement message

Editor features

There are two panes in the replacement message editor in *System > Replacement Messages*:

- *Preview*
- *Editor*

Depending on the display layout that you select from the right, the panes can be hidden or arranged differently. See step 3 in *To edit a replacement message*.

Any change that you make in the editor pane is reflected instantly in the preview pane.

The code editor supports:

- Syntax highlighting
  HTML tags, attributes, embedded CSS, and embedded Javascript are colored differently to make it easier to understand the replacement message.

Variables, e.g., `%%<VARIABLE_NAME>%%` are highlighted. Variable color indicates validity, e.g., green indicates a valid variable and red indicates error, i.e., the variable was not found.

- Semantic-aware code folding

  The replacement message code can be collapsed based on the code hierarchy.
- Hover over the HTML tag to see additional information.

  For example, hovering over `%%<VARIABLE_NAME>%%` tag gives the example value.

  Hovering on an image tag `%%IMAGE:logo_fnet%%` gives you a preview of the image.
- Code suggestion.

  A suggestion is triggered when you insert a text. The suggestion includes HTML tags, attributes, and variables.

  A suggestion pane opens when `%%` is entered. As you enter more characters the suggestion is filtered. Use up and down arrow to navigate the list. Hit enter to accept a suggestion.
- Click the arrow beside the line number to expand or collapse.
- Use *Load Default* from the top-left to restore the content to its default value.
- Use *Insert Tag* to insert `%%` at the current position of the cursor and trigger suggestions.
- User *Insert Image* to insert the image tag at the current position of the cursor and trigger suggestions.

  The *Insert Image* button is only displayed for HTML type replacement messages.
- The *html* or *text* tag indicates the type of the message.
- *? used / ? max* indicates the current message length and the maximum message length.

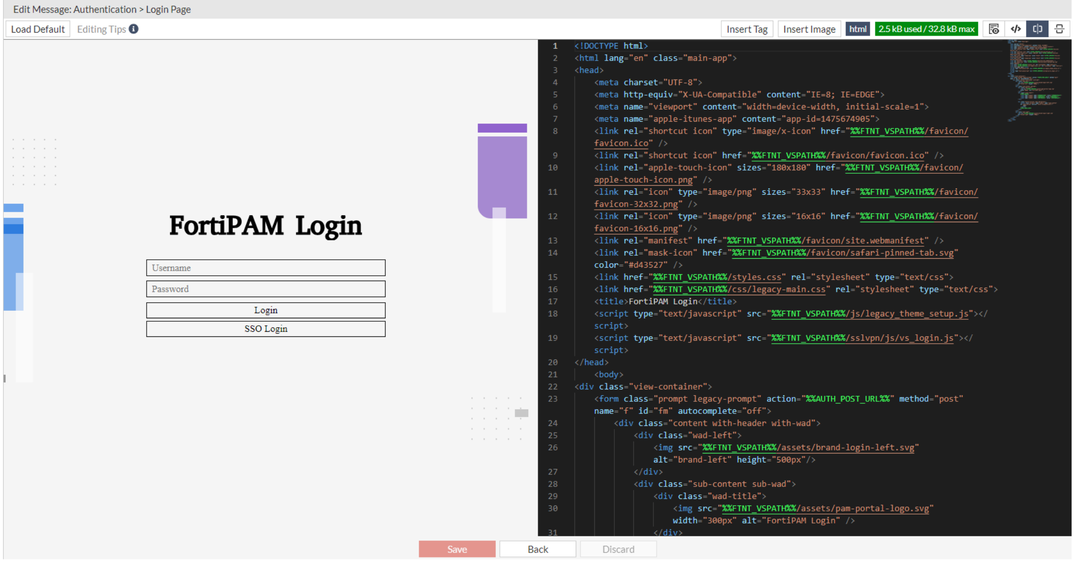
A replacement message cannot exceed the maximum size.

To edit a replacement message:

1. Go to *System > Replacement Messages*.
2. In the *Replacement Messages* tab, select a message in the replacement message list and then select *Edit*.

   The *Edit Message* page opens.

   Here, the *Login Page* replacement message was selected.



```
<!DOCTYPE html>
<html lang="en" class="main-app">
<head>
    <meta charset="UTF-8">
    <meta http-equiv="X-UA-Compatible" content="IE=8; IE=EDGE">
    <meta name="viewport" content="width=device-width, initial-scale=1">
    <meta name="apple-itunes-app" content="app-id=1475674905">
    <link rel="shortcut icon" type="image/x-icon" href="%%FTNT_VSPATH%%/favicon/favicon.ico" />
    <link rel="shortcut icon" href="%%FTNT_VSPATH%%/favicon/favicon.ico" />
    <link rel="apple-touch-icon" sizes="180x180" href="%%FTNT_VSPATH%%/favicon/apple-touch-icon.png" />
    <link rel="icon" type="image/png" sizes="33x33" href="%%FTNT_VSPATH%%/favicon/favicon-32x32.png" />
    <link rel="icon" type="image/png" sizes="16x16" href="%%FTNT_VSPATH%%/favicon/favicon-16x16.png" />
    <link rel="manifest" href="%%FTNT_VSPATH%%/favicon/site.webmanifest" />
    <link rel="mask-icon" href="%%FTNT_VSPATH%%/favicon/safari-pinned-tab.svg" color="#d43527" />
    <link href="%%FTNT_VSPATH%%/styles.css" rel="stylesheet" type="text/css">
    <link href="%%FTNT_VSPATH%%/css/legacy-main.css" rel="stylesheet" type="text/css">
    <title>FortiPAM Login</title>
    <script type="text/javascript" src="%%FTNT_VSPATH%%/js/legacy_theme_setup.js"></script>
    <script type="text/javascript" src="%%FTNT_VSPATH%%/sslvpn/js/vs_login.js"></script>
</head>
    <body>
<div class="view-container">
    <form class="prompt legacy-prompt" action="%%AUTH_POST_URL%%" method="post" name="f" id="fm" autocomplete="off">
        <div class="content with-header with-wad">
            <div class="wad-left">
                <img src="%%FTNT_VSPATH%%/assets/brand-login-left.svg" alt="brand-left" height="500px"/>
            </div>
            <div class="sub-content sub-wad">
                <div class="wad-title">
                    <img src="%%FTNT_VSPATH%%/assets/pam-portal-logo.svg" width="300px" alt="FortiPAM Login" />
                </div>
```

3. Edit the plain text code in the right pane.

Click the insert buttons to add variable, image tags, or:

- Enter `%%` to show all the available variables.
- Hit `Ctrl + Space` to display the auto-completion pane.
- Use the preview pane to preview the changes in realtime.

From the options on the right, select:

- *Preview* ( ): Preview the subject.
- *Editor* (</>): Open the plain text code editor.
- *Horizontal Split* ( ): Editor and preview screens are horizontally split.
- *Vertical Split* ( ): Editor and preview screens are vertically split.

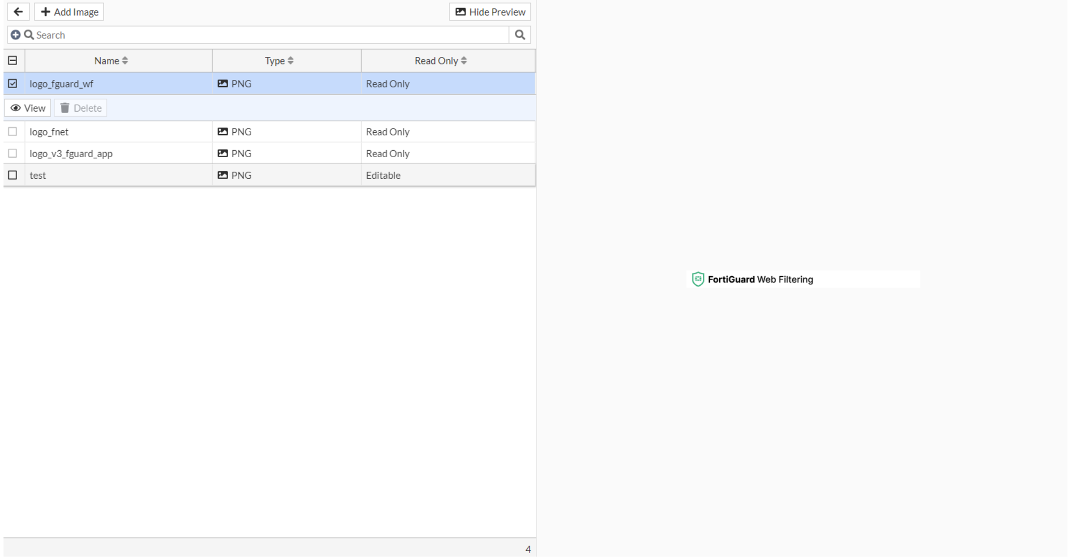
4. To insert a tag, see Inserting a tag.
5. To insert an image, see Inserting an image.
6. When you are finished editing the message, select *Save* to save your changes.
7. If you have made an error when editing the message, select *Load Default* to restore the message to its default value.
   See Adding an image on page 414.

Managing images

To manage the images used in replacement messages, go to *System* > *Replacement Messages* and select *Manage Images*.

By default, the following three images are available:

- `logo_fguard_wf`: FortiGuard Web Filtering logo.
- `logo_fnet`: Fortinet logo.
- `logo_v3_fguard_app`: Fortinet background.



⊟	Name	Type	Read Only
☑	logo_fguard_wf	PNG	Read Only
☐	logo_fnet	PNG	Read Only
☐	logo_v3_fguard_app	PNG	Read Only
☐	test	PNG	Editable

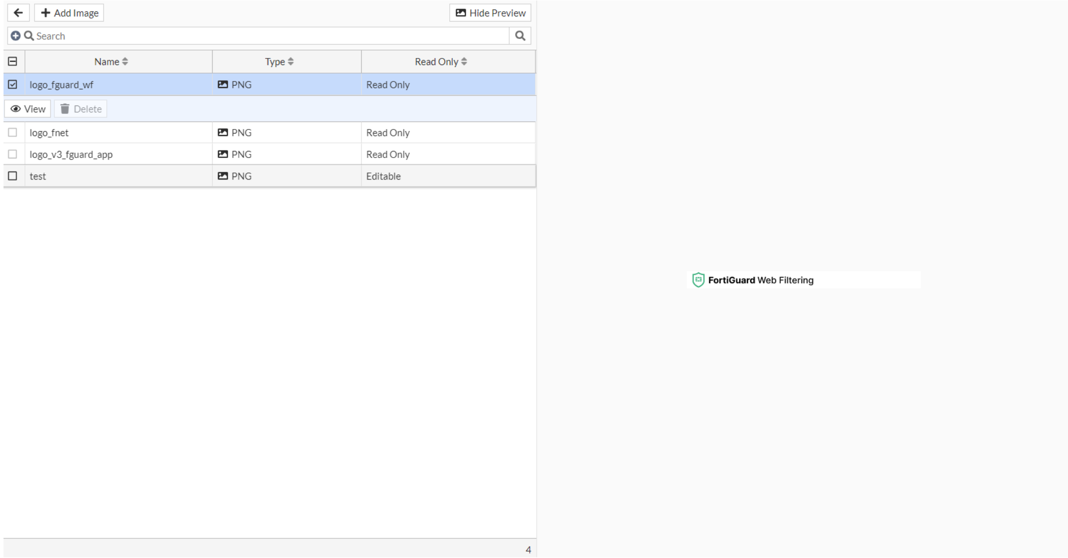
In the *Managing images* page, the following options are available:

Add Image	Select to add a new image file. See Adding an image on page 414.
Hide Preview	Select to hide the selected image preview.
Search	Enter a search term in the search field, then hit `Enter` to search the images list. To narrow down your search, see Column filter.
Edit	Select *Edit* to edit the selected image. The default images cannot be edited.
View	Select *View* to view the selected default image.
Delete	Select to delete the selected images. The default images cannot be deleted.

Adding an image

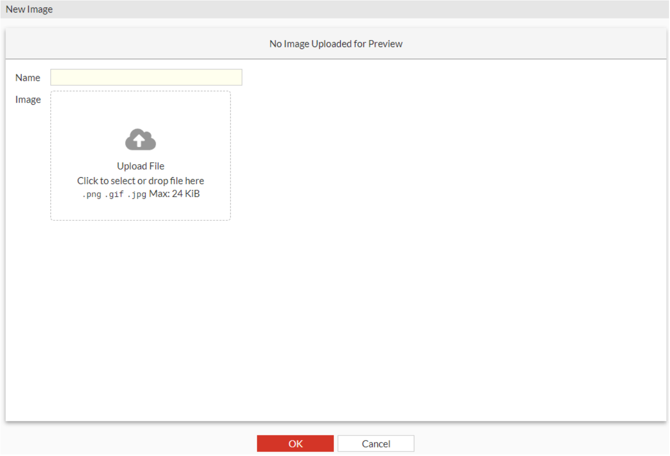
To add an image:

1. Go to *System* > *Replacement Messages* and select *Manage Images*.
   The *Manage Images* window opens.



⊟	Name	Type	Read Only
☑	logo_fguard_wf	PNG	Read Only
☐	logo_fnet	PNG	Read Only
☐	logo_v3_fguard_app	PNG	Read Only
☐	test	PNG	Editable

2. Select *Add Image*.
   The *New Image* window opens.


New Image
No Image Uploaded for Preview
Name
Image
Upload File
Click to select or drop file here
.png .gif .jpg Max: 24 KiB
OK
Cancel

3. Enter the following information:

Name	The name of the image.
Image	Click *Upload File*, locate the image from your computer, and click *Open*. Once the image is uploaded, you can preview it. The following image file types are supported: • `.png` • `.gif` • `.jpg` The maximum file size for the image is 24 KB

4. Click *OK*.

To insert an image to a replacement message:

1. Go to *System* > *Replacement Messages*.
2. In the *Replacement Messages* tab, select a message in the replacement message list and then select *Edit*.
   The *Edit Message* page opens.
3. In the plain text code where you intend to add an image, select *Insert Image*.
   The cursor goes to `%%IMAGE:`, a list of all the images with preview appears.
   Alternatively, enter `%%IMAGE:`, from the dropdown, select an image, and skip to step 5.
4. Select an image from the list.
5. Click *Save*.

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 418 for more information.

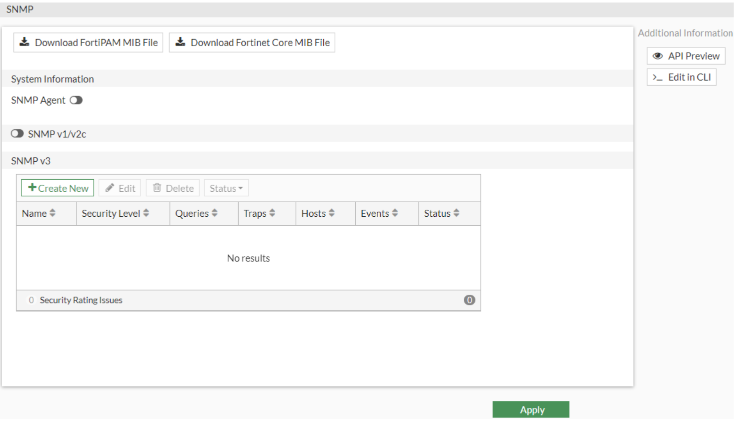
The FortiPAM SNMP implementation is read-only. SNMP v1, v2c, and v3 compliant SNMP managers have read-only access to FortiPAM system information through queries and can receive trap messages from the unit.

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*.



System Information

SNMP Agent ○

○ SNMP v1/v2c

SNMP v3

Name	Security Level	Queries	Traps	Hosts	Events	Status

No results

0 Security Rating Issues

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 418.
System Information	
SNMP Agent	Enable the FortiPAM SNMP agent. See SNMP agent on page 419.
SNMP v1/v2c Enable to see the list of the communities for SNMP v1/v2c (disabled by default). From within this section, you can create, edit or remove SNMP communities.	
Create New	Creates a new SNMP community. When you select *Create New*, the *New SNMP Community* page opens. See Creating or editing an SNMP community on page 420.
Edit	Modifies settings within an SNMP community. When you click *Edit*, the *Edit SNMP Community* page opens.
Delete	Removes an SNMP community from the list. To remove multiple SNMP communities, select multiple rows in the list by holding down the `Ctrl` or `Shift` keys and then select *Delete*.
Status	Enable or disable the SNMP community.
Name	The name of the community.
Queries	Indicates whether queries protocols (v1 and v2c) are enabled or disabled. A green check mark indicates that queries are enabled; a red x indicates that queries are disabled.
Traps	Indicates whether trap protocols (v1 and v2c) are enabled or disabled. A green check mark indicates that traps are enabled; a red x indicates that traps are disabled.
Hosts	List of hosts that are part of the SNMP community.
Events	Number of events that have occurred.
Status	Indicates whether the SNMP community is enabled or disabled.
SNMP v3 Lists the SNMP v3 users. From within this section, you can edit, create or remove an SNMP v3 user.	
Create New	Creates a new SNMP v3 user. When you select *Create New*, the *Create New SNMP User* page opens. See Creating or editing an SNMP user on page 422.
Edit	Modifies settings within the SNMP v3 user. When you click *Edit*, the *Edit SNMP User* page opens.

Delete	Removes an SNMP v3 user from the page. To remove multiple SNMP v3 users, select multiple rows in the list by holding down the `Ctrl` or `Shift` keys and then select *Delete*.
Status	Enable or disable the SNMP v3 user.
Name	The name of the SNMP v3 user.
Security Level	The security level of the user.
Queries	Indicates whether queries are enabled or disabled. A green check mark indicates that queries are enabled; a red x indicates that queries are disabled.
Traps	Indicates whether trap protocols (v1 and v2c) are enabled or disabled. A green check mark indicates that traps are enabled; a red x indicates that traps are disabled.
Hosts	List of hosts.
Events	Number of SNMP events associated with the SNMPv3 user.
Status	Indicates whether the SNMPv3 user is enabled or disabled.

Fortinet MIBs

The FortiPAM SNMP agent supports Fortinet proprietary MIBs, as well as standard RFC 1213 and RFC 2665 MIBs. RFC support includes support for the parts of RFC 2665 (Ethernet-like MIB) and the parts of RFC 1213 (MIB II) that apply to FortiPAM unit configuration.

There are two MIB files for FortiPAM units; both files are required for proper SNMP data collection:

- **Fortinet MIB**: contains traps, fields, and information that is common to all Fortinet products.
- **FortiPAM MIB**: contains traps, fields, and information that is specific to FortiPAM units.

The Fortinet MIB and FortiPAM MIB, along with the two RFC MIBs, are listed in the table in this section.

To download the MIB files, go to *System* > *SNMP* and select a MIB link in the SNMP section. See SNMP on page 416.

Your SNMP manager may already include standard and private MIBs in a compiled database that is ready to use. You must add the Fortinet proprietary MIB to this database to have access to the Fortinet-specific information.

MIB files are updated for each version of FortiPAM. When upgrading the firmware, ensure that you update the Fortinet FortiPAM MIB file compiled in your SNMP manager as well.

MIB file name	Description
FORTINET-CORE-MIB.mib	The Fortinet MIB includes all system configuration information and trap information that is common to all Fortinet products. Your SNMP manager requires this information to monitor FortiPAM unit configuration settings and receive traps from the FortiPAM SNMP agent.

MIB file name	Description
FORTINET-FortiPAM-MIB.mib	The FortiPAM MIB includes all system configuration information and trap information that is specific to FortiPAM units. Your SNMP manager requires this information to monitor FortiPAM configuration settings and receive traps from the FortiPAM SNMP agent. FortiManager systems require this MIB to monitor FortiPAM units.

SNMP get command syntax

Normally, to get configuration and status information for a FortiPAM unit, an SNMP manager would use an SNMP get command to get the information in a MIB field. The SNMP get command syntax would be similar to:

```
snmpget -v2c -c <community_name> <address_ipv4> {<OID> | <MIB_field>}
```

where:

- `<community_name>` refers to the SNMP community name added to the FortiPAM configuration. You can add more than one community name to a FortiPAM SNMP configuration. The most commonly used community name is public. For security reasons, Fortinet recommends that neither public nor private be used for SNMP community names.
- `<address_ipv4>` is the IP address of the FortiPAM interface that the SNMP manager connects to
- `{<OID> | <MIB_field>}` is the object identifier for the MIB field or the MIB field name itself.

For example, to retrieve the serial number of the FortiPAM device, the following command could be issued:

```
snmpget -v2c -c fortinet 192.168.1.110 1.3.6.1.4.1.12356.100.1.1.1.0
```

```
iso.3.6.1.4.1.12356.100.1.1.1.0 = STRING: "FPXVM2TM22000445"
```

In this example, the community name is fortinet, the IP address of the interface configured for SNMP management access is `192.168.1.110`. The serial number of the FortiPAM device is queried using the OID:

`1.3.6.1.4.1.12356.100.1.1.1.0.`

SNMP agent

The FortiPAM SNMP agent must be enabled before configuring other SNMP options. Enter information about the FortiPAM unit to identify it so that when your SNMP manager receives traps from the FortiPAM unit, you will know which unit sent the information.

To configure the SNMP agent in the GUI:

1. Go to *System* > *SNMP*.
2. Enable *SNMP Agent*.
3. Enter a description for the agent. The description can be up to 255 characters long.
4. Enter the physical location of the unit. The system location description can be up to 255 characters long.
5. Enter the contact information for the person responsible for this FortiPAM unit. The contact information can be up to 255 characters.
6. Click *Apply* to save your changes.

To configure the SNMP agent with the CLI:

Enter the following CLI commands:

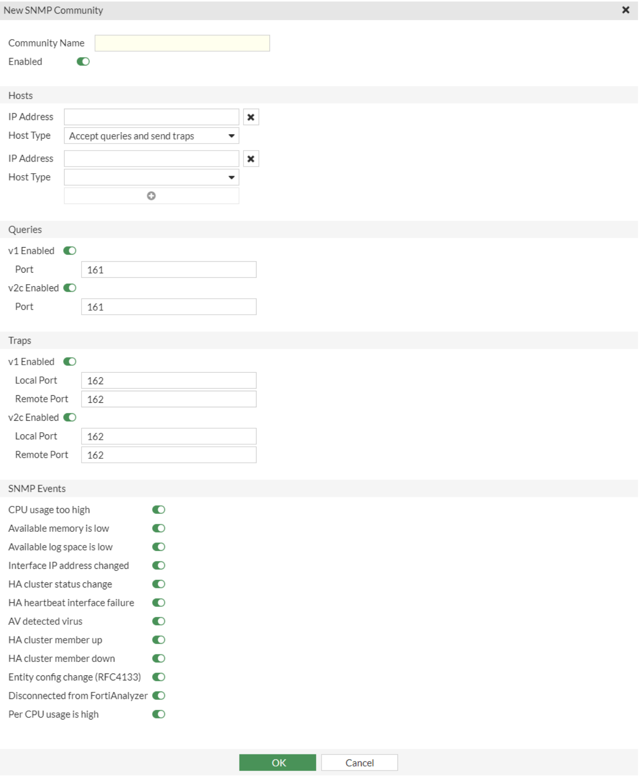
```
config system snmp sysinfo
   set status enable
   set contact-info <contact_information>
   set description <description_of_FortiPAM>
   set location <FortiPAM_location>
end
```

Creating or editing an SNMP community

An SNMP community is a grouping of devices for network administration purposes. Within that SNMP community, devices can communicate by sending and receiving traps and other information. One device can belong to multiple communities, such as one administrator terminal monitoring both a firewall SNMP and a printer SNMP community.

Add SNMP communities to your FortiPAM unit so that SNMP managers can view system information and receive SNMP traps. You can add up to three SNMP communities. Each community can have a different configuration for SNMP queries and traps and can be configured to monitor the FortiPAM unit for a different set of events. You can also add the IP addresses of up to sixteen SNMP managers to each community.

Enabling *SNMP v1/v2c* and selecting *Create New* in the *SNMP v1/v2c* pane opens the *New SNMP Community* page, which provides settings for configuring a new SNMP community. Double-clicking a community from the SNMP v1/v2c table opens the *Edit SNMP Community* page. Alternatively, select a community from the list and then select *Edit* to edit the SNMP community.


New SNMP Community

Community Name
Enabled

Hosts

IP Address
Host Type: Accept queries and send traps
IP Address
Host Type

Queries

v1 Enabled
Port: 161
v2c Enabled
Port: 161

Traps

v1 Enabled
Local Port: 162
Remote Port: 162
v2c Enabled
Local Port: 162
Remote Port: 162

SNMP Events

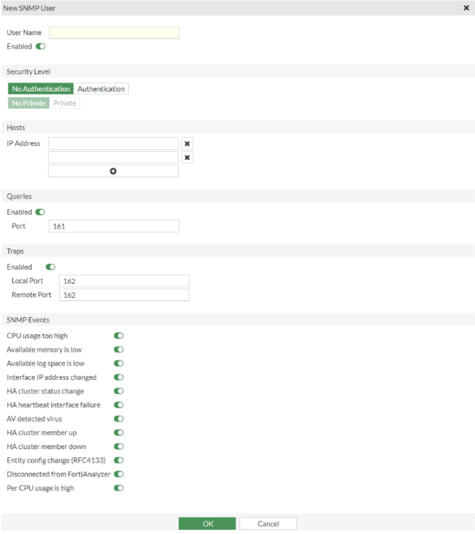
CPU usage too high
Available memory is low
Available log space is low
Interface IP address changed
HA cluster status change
HA heartbeat interface failure
AV detected virus
HA cluster member up
HA cluster member down
Entity config change (RFC4133)
Disconnected from FortiAnalyzer
Per CPU usage is high

Configure the following settings in the *New SNMP Community* page or *Edit SNMP Community page* and click *OK*:

Community Name	Enter a name to identify the SNMP community. After you create the SNMP community, you cannot edit the name.
Enabled	Enable or disable the SNMP community.
Hosts Settings for configuring the hosts of an SNMP community.	
IP Address	Enter the IP address/netmask of the SNMP managers that can use the settings in this SNMP community to monitor the unit. You can also set the IP address to 0.0.0.0 to so that any SNMP manager can use this SNMP community.
Host Type	Select one of the following: *Accept queries and send traps*, *Accept queries only*, or *Send traps only*.
X	Removes an SNMP manager from the list within the *Hosts* section.
+	Select to add a blank line to the Hosts list. You can add up to 16 SNMP managers to a single community.
Queries Settings for configuring queries for both SNMP v1 and v2c.	
v1 Enabled	Enable or disable SNMP v1 queries.
Port	Enter the port number (161 by default) that the SNMP managers in this community use for SNMP v1 and SNMP v2c queries to receive configuration information from the unit. The SNMP client software and the unit must use the same port for queries.
v2c Enabled	Enable or disable SNMP v2c queries.
Traps Settings for configuring local and remote ports for both v1 and v2c.	
v1 Enabled	Enable or disable SNMP v1 traps.
Local Port	Enter the local port numbers (162 by default) that the unit uses to send SNMP v1 or SNMP v2c traps to the SNMP managers in this community. The SNMP client software and the unit must use the same port for traps.
Remote Port	Enter the remote port number (162 by default) that the unit uses to send SNMP traps to the SNMP managers in this community. The SNMP client software and the unit must use the same port for traps.
v2C Enabled	Enable or disable SNMP v2c traps.
SNMP Events Enable each SNMP event for which the unit should send traps to the SNMP managers in this community. **Note**: The **CPU usage too high** trap’s sensitivity is slightly reduced by spreading values out over 8 polling cycles. This reduction prevents sharp spikes due to CPU intensive short-term events such as changing a policy.	

Creating or editing an SNMP user

Selecting *Create New* in the *SNMP v3* pane opens the *New SNMP User* page, which provides settings for configuring a new SNMP v3 user. Double-clicking a user from the SNMP v3 table opens the *Edit SNMP User* page. Alternatively, select an SNMP user and then select *Edit* to edit the SNMP user.



User Name
Enabled ●

No Authentication | Authentication
No Private | Private

IP Address

Enabled ●
Port 161

Enabled ●
Local Port 162
Remote Port 162

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 (RFC4133) ●
Disconnected from FortiAnalyzer ●
Per CPU usage is high ●

Configure the following settings in the *New SNMP User* page or *Edit SNMP User* page and click *OK*:

User Name	Enter the name of the user. After you create an SNMP user, you cannot change the user name.
Enabled	Enable or disable this SNMP user.
Security Level Select the type of security level the user will have: • *No Authentication* • *Authentication* and *No Private*—Select the authentication algorithm and enter password to use. • *Authentication* and *Private*—Select the authentication and encryption algorithm and enter the passwords to use.	
Authentication/Encryption Algorithm	If the security level is set to *Authentication* and *No Private*, you can select from the following authentication algorithms: • *MD5* • *SHA1* (default) • *SHA224* • *SHA256* • *SHA384* • *SHA512* If the security level is set to *Authentication* and *Private*, you can also select from the following encryption algorithms in addition to authentication algorithms: • *AES* (default) • *DES* • *AES256*

	• *AES256 Cisco*
Password	If the security level is set to *Authentication*, select *Change* and enter a password in the *Password* field.
Hosts Settings for configuring the hosts of an SNMP community.	
IP Address	Enter the IP address of the notification host. If you want to add more than one host, select + to add another host. Up to 16 hosts can be added. Select *X* to delete any hosts.
Queries Settings for configuring queries for both SNMP v1 and v2c.	
Enabled	Enable or disable the query. By default, the query is enabled.
Port	Enter the port number in the *Port* field (161 by default).
Traps Settings for configuring local and remote ports for both v1 and v2c.	
Enabled	Enable or disable the trap.
Local Port	Enter the local port number (162 by default).
Remote Port	Enter the remote port numbers (162 by default).
SNMP Events Select the SNMP events that will be associated with the user.	

Backup

FortiPAM configuration contains not only the system settings but also all user information and secret data. It is crucial to have a backup to avoid data loss. Whenever a hardware failure or system relocation is needed, a new FortiPAM can be easily set up by restoring the previous backup configuration. In the case of accidentally deleting data, you can retrieve the original configuration from the backup and paste the data back.

FortiPAM has two ways to back up its configuration:

- Manually trigger from the user menu. See *Backup and restore* in Admin on page 30.
- 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.

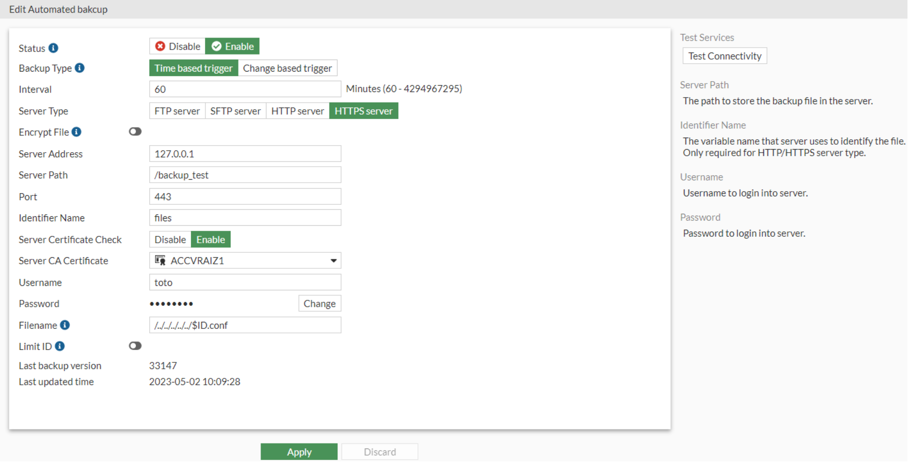
⚠ Whenever restoring a backup configuration, keep in mind that the secret password or key may not be the most recent one.

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 30.

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.



Edit Automated bakcup

Status	☒ Disable [✓ Enable]
Backup Type	[✓ Time based trigger] Change based trigger
Interval	60 Minutes (60 - 4294967295)
Server Type	FTP server SFTP server HTTP server [✓ HTTPS server]
Encrypt File	○
Server Address	127.0.0.1
Server Path	/backup_test
Port	443
Identifier Name	files
Server Certificate Check	Disable [✓ Enable]
Server CA Certificate	ACCVRAIZ1
Username	toto
Password	•••••••• Change
Filename	/../../../../$ID.conf
Limit ID	○
Last backup version	33147
Last updated time	2023-05-02 10:09:28

Test Services

Test Connectivity

Server Path

The path to store the backup file in the server.

Identifier Name

The variable name that server uses to identify the file. Only required for HTTP/HTTPS server type.

Username

Username to login into server.

Password

Password to login into server.

2. Enter the following information:

Status	Enable or disable automatic backup. **Note**: The option is enabled by default.
Backup Type	Select from the following two options: • *Time based trigger*: FortiPAM sends the backup configuration to the server every *Interval* minutes. • *Change based trigger*: FortiPAM checks the configuration every *Interval* minutes and if the configuration has changed, FortiPAM sends it to the server (default).
Interval	The time interval required in backup, in minutes (default = 60, 60 - 4294967295).
Server Type	Select from the following server types: • *FTP server* (default) • *SFTP server* • *HTTP server* • *HTTPS server*

	To successfully configure an HTTP/HTTPS server to backup with user authentication, ensure that you have filled in the username and password fields. The backup process will not function correctly if you leave either field empty. Alternatively, you can leave both fields empty if you want to avoid user authentication.
Encrypt File	Enable and enter cipher key to encrypt the backup file. The administrator must enter the same cipher key when restoring the configuration to FortiPAM. **Note**: The option is disabled by default.
Server Address	The IP address of the server.
Server Path	The path to store the backup file in the server.
Port	The port of the file server. Default values: • 21 (FTP server) (default) • 22 (SFTP server) • 80 (HTTP server) • 443 (HTTPS server) When upgrading, the port number is set according to the server type (ftp = 21, sftp = 22, http = 80, and https = 443).
Identifier Name	The variable name that server uses to identify the file. **Note**: Only required for *HTTP/HTTPS server* type.
Server Certificate Check	Enable/disable server identity check. This verifies the server domain name/IP address against the server certificate. **Note**: The option is disabled by default. **Note**: The option is only available for *HTTPS server*.
Server CA Certificate	From the dropdown, select a server CA certificate for server certificate check. **Note**: The option is only available when *Server Certificate Check* is enabled.
Username	Username to log in to the server.
Password	Password to log in to the server.
Filename	Filename pattern of the backup configuration. Valid variables are: `$SN $YYYY $MM $DD $hh $mm $ss $ID`. **Note**: The `$ID` variable is mandatory in the filename pattern

	Enter `$` to get the list of variables.
Limit ID	Enable to limit the value of `$ID` in the file name. The option allows administrators to set a maximum number of backup files (default = 1, 1 - 4294967295) to be stored on a backup server using specific filename patterns. For example, if the backup filename follows the format `PAM-$SN-$ID.conf`, where `$ID` represents the backup ID, when `$ID` reaches the maximum limit, it is reset to 0. The new backup file overwrites the old backup file using the same name.
Last backup version	The last backup version (noneditable).
Last updated time	The date and time when automatic backup was last done (noneditable).

3. Click *Apply*.
4. Click *Test Connectivity* to test the connection to the backup server.

Configuring automated backup settings on the CLI

```
config system backup
   set status {enable | disable}
   set cipher <passwd>
   set type {time-based | change-based}
   set server-type {ftp | sftp | http | https}
   set server-address <string>
   set server-path <path>
   set port <integer>
   set file-field-name <string>
   set server-user <string>
   set server-pass <passwd>
   set filename-pattern {$SN $YYYY $MM $DD $hh $mm $ss $ID}
   set ca-cert <string>
   set server-identity-check {enable | disable}
   set interval <integer>
   set max-id <integer>
   set backup-id <integer>
   set last-version <integer>
   set updated-time <integer>
end
```

Variables	Description
status {enable | disable}	Enable/disable automatic backup (default = enable).
cipher <passwd>	Enter the cipher key.
type {time-based | change-based}	Set the backup type: • `time-based`: Time based trigger. • `change-based`: Change based trigger (default).

Variables	Description
server-type {ftp | sftp | http | https}	Set the server type: • `ftp` (default) • `sftp` • `http` • `https`
server-address <string>	Enter the address of file server.
server-path <path>	Enter the path of file server (default = `/`).
port <integer>	Enter the port number of the file server (default = 21, 1 - 65535).
file-field-name <string>	Enter the field name for file upload (default = `files`).
server-user <string>	Enter the username of the server account.
server-pass <passwd>	Enter the password of the server account.
filename-pattern {$SN $YYYY $MM $DD $hh $mm $ss $ID}	Enter the file name pattern of the backup configuration (default = `$ID.conf`). **Note**: The `$ID` variable is mandatory in the filename pattern.
ca-cert <string>	Enter the CA certificate name.
server-identity-check {enable | disable}	Enable/disable server identity check (verify server domain name/IP address against the server certificate) (default = disable).
interval<integer>	Enter an interval for the backup, in minutes (60 - 4294967295, default = 60).
max-id <integer>	Enter the limit for `backup-id` (default = 0). **Note**: Use 0 to set no limit.
backup-id <integer>	The current backup id number. **Note**: The variable cannot be modified.
last-version <integer>	The last backup version. **Note**: The variable cannot be modified.
updated-time <integer>	The time when the last update was done. **Note**: The variable cannot be modified.

Example CLI configuration - Example

Backup to SFTP/FTP server

```
config system backup
   set status enable
   set server-type sftp
   set server-address "10.59.112.254"
   set server-path "backup/"
   set port 22
   set server-user "sftp_user"
   set server-pass <sftp_user_password>
   set filename-pattern "$SN-$YYYY-$MM-$DD-$hh-$mm-$ss-$ID.conf"
end
```

Backup to HTTPS/HTTP server

```
config system backup
   set status enable
   set server-type https
   set server-address "10.59.112.254"
   set server-path "/http_user/upload.php"
   set port 443
   set file-field-name "file"
   set server-user "http_user"
   set server-pass QA@fortinet
   set filename-pattern "$SN-$ID.conf"
   set ca-cert "ACCVRAIZ1"
   set server-identity-check enable
end
```

If user authentication is not required for HTTP and HTTPS servers, `server-user` and `server-pass` variables are not required.

Following is an example of php file to accept the submitted backup file.

```
fwd-svr@fwdsvr-virtual-machine:/var/www/html/http_user$ cat upload.php
<?php
   $name = $_FILES['file']['name'];
   $temp = $_FILES['file']['tmp_name'];
   if(move_uploaded_file($temp,"backup/".$name)){
   echo "Your file was uploaded";
   }
   else
   {
   echo "Your file couldn't upload";
   }
?>
```

Sending backup file to a server - Example

The example shows how an administrator can verify system backup configuration and the connection to the backup server.

To send a backup file to a server:

1. In the CLI console, enter the following commands:
   ```
      diagnose debug enable
      diagnose test application wad 1000
      ....
      ....
   Process [13]: type=secret-approval(14) index=0 pid=1080 state=running
    diagnosis=yes debug=enable valgrind=supported/disabled
   ```
2. Find the process with the `type` `secret-approval` and the index.
   In the example above, the process `type` is `14` and `index` is `0`.
3. Generate the diagnosis process using `2<process type><index>`.
   In the example above, the diagnosis process is `21400`.
4. Enter the following command:
   ```
   diagnose test application wad 21400
   ```

```
Set diagnosis process: type=secret-approval index=0 pid=1080
```

5. Enter the following command:

```
   diagnose test application wad
WAD process 1080 test usage:
```

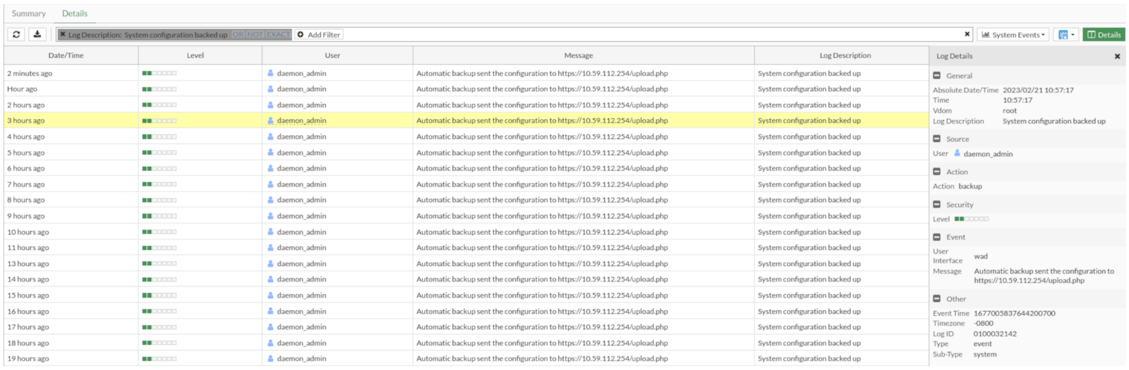
....

```
701: Test sending file using backup config
```

6. Enter the following command:

```
   diagnose test application wad 701
Sending backup to server using system.backup settings manually.
Finished sending backup to server. Check to see if backup file was successfully
uploaded.
```

Additionally, you can check *System Events* in *Log & Report* > *Events* to determine whether the system configuration backup process was successful.


Summary
Details
✖ Log Description: System configuration backed up OR NOT EXACT
Add Filter
System Events
Details

Date/Time	Level	User	Message	Log Description
2 minutes ago	■■□□□□□	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up
Hour ago	■■□□□□□	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up
2 hours ago	■■□□□□□	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up
3 hours ago	■■□□□□□	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up
4 hours ago	■■□□□□□	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up
5 hours ago	■■□□□□□	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up
6 hours ago	■■□□□□□	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up
7 hours ago	■■□□□□□	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up
8 hours ago	■■□□□□□	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up
9 hours ago	■■□□□□□	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up
10 hours ago	■■□□□□□	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up
11 hours ago	■■□□□□□	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up
13 hours ago	■■□□□□□	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up
14 hours ago	■■□□□□□	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up
15 hours ago	■■□□□□□	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up
16 hours ago	■■□□□□□	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up
17 hours ago	■■□□□□□	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up
18 hours ago	■■□□□□□	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up
19 hours ago	■■□□□□□	daemon_admin	Automatic backup sent the configuration to https://10.59.112.254/upload.php	System configuration backed up

Log Details

General

Absolute Date/Time 2023/02/21 10:57:17
Time 10:57:17
Vdom root
Log Description System configuration backed up

Source

User daemon_admin

Action

Action backup

Security

Level ■■□□□□□

Event

User Interface wad
Message Automatic backup sent the configuration to https://10.59.112.254/upload.php

Other

Event Time 1677005837644200700
Timezone -0800
Log ID 0100032142
Type event
Sub-Type system

Backing up/restoring log and video files using FTP - CLI

FortiPAM now supports backing up and restoring video and log files from a remote FTP server. This is mainly used during disk replacement.

Before you replace a disk, you can use the CLI to back up the video or the log file stored in the disk.

After the disk is replaced, the video and log files can be restored to the correct directories in the new disk using restoration CLI command.

See:

- Back up log files on page 430
- Back up video files on page 430
- Restore log files on page 431
- Restoring video files on page 431
- Breakpoint resume for video files on page 432

To run any of the following commands, you must be in the maintenance mode.
See Maintenance mode.

Back up log files

To back up log files:

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

```
 execute backup disk alllogs ftp <remote folder path> <ftp server>[:ftp port] <user>
<passwd>
```

Variable	Description
<remote folder path>	The absolute path of the target folder. You see the folder when you log in to the target server using FTP. Make sure that the folder exists before the backup is performed. **Note**: A new folder named using the user FortiPAM license number and file category (`all_logs` for logs) is created in the target folder to store the backed up log files.
<ftp server> [:ftp port]	The FTP server IPv4 or IPv6 address. You can also add the FQDN with the port.
<user>	The FTP server user name.
<passwd>	The FTP server password.

After running the backup command, the process used to generate the backup file and logs is stopped.

The process is restored automatically after the backup finishes.

The command used for log restoration is displayed on the terminal.

Back up video files

To back up video files:

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

```
 execute backup disk video ftp <remote folder path> <ftp server>[:ftp port] <user>
<passwd>
```

2.

Variable	Description
<remote folder path>	The absolute path of the target folder. You see the folder when you log in to the target server using FTP. Make sure that the folder exists before the backup is performed. **Note**: A new folder named using the user FortiPAM license number and file category (`video` for logs) is created in the target folder to store the backed up files.

Variable	Description
<ftp server>[:ftp port]	The FTP server IPv4 or IPv6 address. You can also add the FQDN with the port.
<user>	The FTP server user name.
<passwd>	The FTP server password.

Restore log files

To restore log files:

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

```
 execute restore disk alllogs ftp <remote folder path> <ftp server>[:ftp port] <user>
<passwd>
```

The parameters are the same as in Back up log files on page 430.

FortiPAM reminds the user if the target folder path is different from the default backup folder FortiPAM generates, i.e., `path_to_backup_target_folder/FPAMLicenseNumber_all_logs`.
You can continue restoration if the folder path is correct.

Similar to log back up, the process used to generate the backup file and logs is stopped. The process is restored automatically after the backup finishes.

Restoring video files

To restore video files:

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

```
execute restore disk video ftp <string> <ftp server>[:ftp port] <user> <passwd>
```

The parameters are the same as in Back up video files on page 430.

FortiPAM reminds the user if the target folder path is different from the default backup folder FortiPAM generates (`path_to_backup_target_folder/FPAMLicenseNumber_video`).
You can continue restoration if the folder path is correct.

Breakpoint resume for video files

If a backup/restore process is broken, the file already backed up and restored is not transferred again to the following backup/restore process.

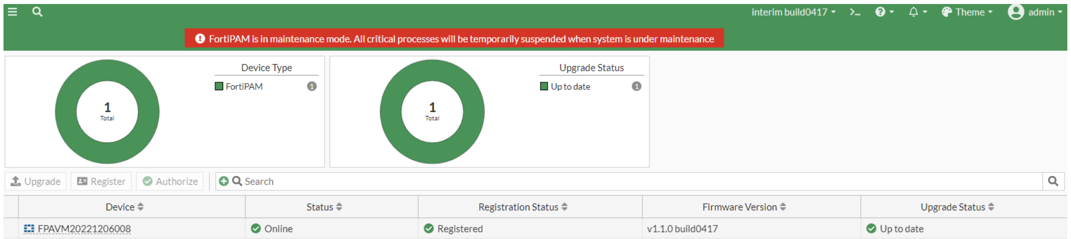
Firmware

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

The widgets at the top display:

- The total number of FortiPAM devices.
- The upgrade status of the FortiPAM devices.

The *Firmware* tab displays the device name, device status, registration status, firmware version, and the upgrade status.



FortiPAM is in maintenance mode. All critical processes will be temporarily suspended when system is under maintenance

Device	Status	Registration Status	Firmware Version	Upgrade Status
FPAVM20221206008	✓ Online	✓ Registered	v1.1.0 build0417	✓ Up to date

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

Upgrade	Upgrade the FortiPAM firmware. See Uploading a firmware on page 31.
Register	
Authorize	
Search	Enter a search term in the search field, then hit `Enter` to search. To narrow down your search, see Column filter.

Upgrading the firmware

Periodically, Fortinet issues firmware upgrades that fix known issues, add new features and functionality, and generally improve your FortiPAM experience.

Before proceeding to upgrade the system, Fortinet recommends that you back up the configuration. See Backup and restore on page 32.

To be able to upgrade the firmware, you must first register your FortiPAM with Fortinet. See Licensing on page 51.

To upgrade the firmware from FortiPAM GUI, see Uploading a firmware on page 31.

Always review all sections in *FortiPAM Release Notes* prior to upgrading your device.

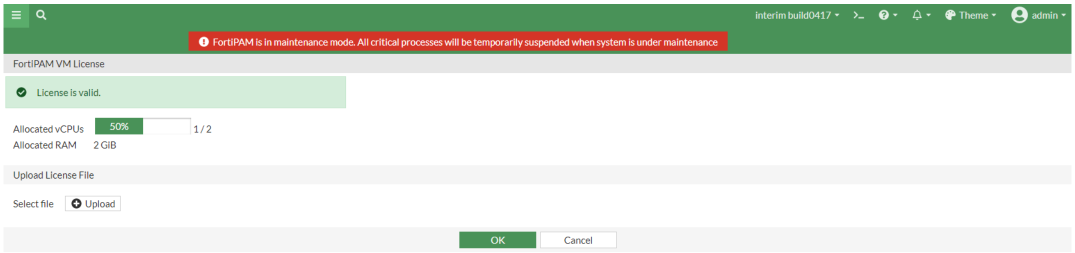
FortiPAM license

The FortiPAM-VM license can be uploaded from *System* > *FortiPAM License*.

You must be in maintenance mode to be able to upload a license. See Maintenance mode in Admin on page 30.

To upload a new license:

1. Go to *System* > *FortiPAM License*.
   The *FortiPAM VM License* window opens.



FortiPAM is in maintenance mode. All critical processes will be temporarily suspended when system is under maintenance

FortiPAM VM License

License is valid.

Allocated vCPUs 50% 1 / 2
Allocated RAM 2 GiB

Upload License File

Select file

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.

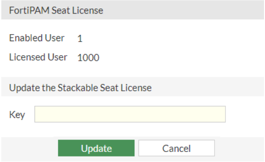
Use the CLI command `get system status` to verify the license status.

Stackable seat license for hardware models

For FortiPAM 1000G and 3000G hardware models, you can update the licensed seat using the provided key if you purchase a new stackable seat license with additional seats from FortiCare.

To update the license:

1. On a FortiPAM 1000G/3000G model, go to *System* > *FortiPAM License*.
   The *FortiPAM Seat License* window opens.



FortiPAM Seat License

Enabled User 1
Licensed User 1000

Update the Stackable Seat License

Key

2. Enter the key provided by FortiCare.
3. Click *Update* to save your changes.

> A warning appears if the number of seats in the new license is equal to or less than the existing license.
>
> Click *Yes* to force the update or *No* to abort the update.

To update the license using the CLI:

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

```
execute upd-seat-license <key-string>
```

FortiGuard license

Go to *System > FortiGuard License* to configure FortiGuard subscription services. See FortiGuard Distribution Network on page 62.

Concurrent user sessions

A concurrent session occurs when multiple users access FortiPAM using the same account.

By default, a user account may be used to log in concurrently from multiple locations. For enhanced security, this setting can be disabled by disabling *Concurrent Log-on* in the *Other General Setting* pane in *System > Settings*. When you disable the setting, only one session is allowed per user.

See Settings on page 373.

Alternatively, in the CLI console, enter the following commands to disable concurrent login.

```
config system global
 set admin-concurrent disable
end
```

When an admin concurrent session is disabled:

- Additional concurrent admin sessions are blocked while an admin session is active (default)

OR

- FortiPAM automatically terminates any previous sessions when the admin opens a new session.

This behavior can be changed when the `admin-concurrent` variable is disabled, allowing you to either block additional sessions or terminate (kick out) previous sessions when a new session is opened:

```
config system global
 set admin-concurrent disable
 set admin-new-login-action {block | kick-out} #admin-new-login-action is only displayed
when admin-concurrent is disabled, #default = block
end
```

Alternatively, use the *New Log-in Action* option when *Concurrent Log-on* is disabled in *System > Settings* to:

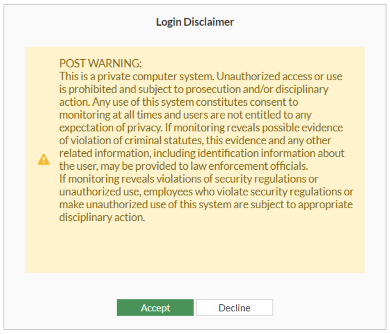
- Block additional concurrent admin sessions while an admin session is active (default).
- Terminate any previous sessions when the admin opens a new session.

See Settings on page 373.

Disclaimers via the CLI

FortiPAM allows you to set up login disclaimers.

Once you are successfully authenticated, a login disclaimer banner appears. You must click *Accept* to access FortiPAM. If you click *Decline*, you are logged out immediately.



Login Disclaimer

POST WARNING:
This is a private computer system. Unauthorized access or use is prohibited and subject to prosecution and/or disciplinary action. Any use of this system constitutes consent to monitoring at all times and users are not entitled to any expectation of privacy. If monitoring reveals possible evidence of violation of criminal statutes, this evidence and any other related information, including identification information about the user, may be provided to law enforcement officials.
If monitoring reveals violations of security regulations or unauthorized use, employees who violate security regulations or make unauthorized use of this system are subject to appropriate disciplinary action.

You can set up login disclaimers in the GUI using the *Login Disclaimer* toggle and the text box available in the *Other General Settings* pane in *System* > *Settings*.

Disclaimers via the CLI - Example

To configure a login disclaimer:

1. In the CLI console, enter the following command to enable the login disclaimer:

```
config system global
   set post-login-banner enable #display the administrator access disclaimer message
         after an administrator successfully logs in
end
```

2. In the CLI console, enter the following commands to set up the login disclaimer:

```
config system replacemsg admin post_admin-disclaimer-text
   set buffer "POST WARNING:
      This is a private computer system. Unauthorized access or use is prohibited and
            subject to prosecution and/or disciplinary action. Any use of this system
            constitutes consent to monitoring at all times and users are not entitled
            to any expectation of privacy. If monitoring reveals possible evidence of
            violation of criminal statutes, this evidence and any other related
            information, including identification information about the user, may be
            provided to law enforcement officials. If monitoring reveals violations of
            security regulations or unauthorized use, employees who violate security
            regulations or make unauthorized use of this system are subject to
            appropriate disciplinary action."
   set header none
   set format text
end
```

The disclaimer must begin and end with quotation marks.

Troubleshooting

FortiPAM operation requires multiple components to work together. Generally, a browser and FortiClient are necessary on the client side to connect to the FortiPAM GUI. Secrets on FortiPAM can then be used to connect to the target host.

If the FortiPAM system runs abnormally, pinpointing the failed component can be challenging. This chapter presents the usage of built-in debug tools to speed up finding errors.

You must have system administrator and CLI permissions to use the debug features including debug trace files. See Role on page 278.

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.

Troubleshooting network gateways

In the CLI console, enter the following commands:

```
 diagnose wad debug enable category gateway #dumps gateway config cache and the ongoing
gateway session
diagnose test application wad 426
diagnose test application wad 429
```

See troubleshooting Issue: WebRDP session recording fails and closes active session on page 441.

For FortiPAM related troubleshooting tips, see *Troubleshooting Tip: General Client-side Debugging Tips/Info* on the Fortinet Community.

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 437.

Related CLI commands:

Command	Description
diagnose wad debug file {enable | disable}	Enable/disable dump trace to files.
diagnose wad debug file max_size <size>	Set the maximum size for trace files.
diagnose wad debug file overwrite {enable | disable}	Allow overwriting when the file reaches maximum size.
diagnose wad debug file clear	Clear all the trace files.
diagnose wad debug file list	Show all trace related file stats.
diagnose wad debug file show {trace_file_name | all}	Show a specific or all trace file content.
diagnose wad debug file send tftp <addr> <save_zip_name.tar.gz>	Send trace files to TFTP server.
diagnose wad debug file send ftp <save_zip_name.tar.gz> <addr>:[port] [username] [password]	Send trace files to FTP server.

Example troubleshooting - example

1. In the CLI console, enter the following commands to set debug category and level:
   ```
   diagnose wad debug enable category secret
   diagnose wad debug enable level info
   ```
2. Enter the following command to set the maximum size for trace files:
   ```
   diagnose wad debug file max-size 2
   ```

3. Enter the following command to enable dump trace to files:
```
diagnose wad debug file enable
```
   Trace file is displayed now.
4. Enter the following command to disable dump trace to files:
```
diagnose wad debug file disable
```
5. Enter the following command to show all trace related file stats:
```
diagnose wad debug file list
size:0000000000, wad_worker-1.log
size:0000000000, wad_cert-inspection-0.log
size:0000000000, wad_debug-0.log
size:0000000000, wad_algo-0.log
size:0000000000, wad_user-info-0.log
size:0000000000, wad_dispatcher-0.log
size:0000000000, wad_secret-approval-0.log
size:0000000000, wad_config-notify-0.log
size:0000000000, wad_informer-0.log
size:0000000000, wad_YouTube-filter-cache-service-0.log
size:0000006869, wad_worker-0.log
size:0000000000, wad_pwd-changer-0.log
size:0000000000, wad_manager-0.log
```
6. Enter the following command to clear all the trace files:
```
diagnose wad debug clear
```
7. Enter the following command to show a specific file content:
```
diagnose wad debug file show wad_worker-0.log
```

```
[I][p:1066][s:369910368][r:2588] wad_gui_secret_handler :4123 Successfully fetched
     database list for admin
[I][p:1066][s:369910368][r:2588] wad_gui_secret_handler :4510 attach response body to
     response
[I][p:1066][s:369910368][r:2590] wad_gui_secret_handler :4060 METHOD OVERRIDE to GET,
     fetching list
[I][p:1066][s:369910368][r:2590] wad_gui_secret_folder_post_select :1669 Dev is NULL
[I][p:1066][s:369910368][r:2590] wad_gui_secret_folder_post_select :1715 filter gets
     all personal secret folders
[I][p:1066][s:369910368][r:2590] wad_gui_secret_handler :4088 Successfully fetched
     folder list for admin
[I][p:1066][s:369910368][r:2590] wad_gui_secret_handler :4510 attach response body to
     response
[I][p:1066][s:369910370][r:2592] wad_gui_secret_handler :4060 METHOD OVERRIDE to GET,
     fetching list
[I][p:1066][s:369910370][r:2592] wad_gui_secret_folder_post_select :1669 Dev is NULL
[I][p:1066][s:369910370][r:2592] wad_gui_secret_handler :4088 Successfully fetched
     folder list for admin
.
.
```

FortiPAM HTTP filter

When turning on the HTTP category debug, it can generate a lot of traces from the GUI. In the case where GUI traffic is not needed, using the FortiPAM HTTP filter helps clean out traffic that is not required.

You must have system administrator and CLI permissions to use the FortiPAM HTTP filter.

To use the FortiPAM trace filter feature:

1. In the CLI console, enter the following command to set the debug category to http:
   ```
   diagnose wad debug enable category http
   ```
2. Optionally, enter the following command to set the debug level:
   ```
   diagnose wad debug enable level <level>
   ```
3. Use the following CLI command to set up a filter for the FortiPAM traffic:
   ```
   diagnose wad filter pam
   ```

Variable	Description
none	Reset FortiPAM filter setting. All the HTTP traffic traces are displayed.
internal	Internal FortiPAM trace. HTTP traffic with `/pam api-gateway` is displayed, e.g., FortiClient and secret launcher traffic.
tcp-forward	TCP-forward trace. Traffic trace with `/tcp api-gateway` is displayed, e.g., TCP tunneling information when starting a launcher.
both	Internal FortiPAM and TCP-forward trace. HTTP traffic with `/tcp` and `/pam api-gateway` is displayed.

For most cases, the `both` option is recommended for the filter.

The FortiPAM filter can be used with `diagnose wad filter drop-unknown-session 1` to ignore more information during session initialization.

- Examples

1. Turning on `drop-unknown-session` with the `internal` option (`diagnose wad filter pam internal`) and launching a secret shows the following trace:
   ```
   PAM # [I][p:1070][s:930509823][r:2694] wad_http_req_proc_policy: 10453 ses_
         ctx:ct|Pvx|M|H|C|A1 fwd_srv=<nil>[I][p:1070][s:930509823][r:2694] wad_dump_fwd_
         http_resp: 2663 hreq=0x7f34b46a2e58 Forward response from Internal:
   HTTP/1.1 200 OK
   Content-Type: application/json
   Content-Length: 309
   [I][p:1070][s:930509826][r:2701] wad_dump_fwd_http_resp: 2663 hreq=0x7f34b46a2e58
         Forward response from Internal:
   HTTP/1.1 200 OK
   ```

```
Proxy-Agent: FortiPAM/1.0
X-Range: bytes=773458-
Content-Length: 0
```

2. Turning on `drop-unknown-session` with the `tcp-forward` option (`diagnose wad filter pam tcp-forward`) and launching a secret shows the following trace:

```
[I][p:1070][s:930509852][r:2799] wad_http_req_check_vs_tunnel_type :5182 Check redir
     PROXY port=22((null))
[I][p:1070][s:930509852][r:2799] wad_http_req_check_vs_tunnel_type :5190 TCP tunnel
     detected without type.
[I][p:1070][s:930509852][r:2799] wad_dump_fwd_http_resp :2663 hreq=0x7f34b46a41f8
     Forward response from Internal:
HTTP/1.1 101 Switching Protocols
Upgrade: tcp-forwarding/1.0
Connection: Upgrade
```

Issue: WebRDP session recording fails and closes active session

Applies to web based secret launching failures

To solve WebRDP session recording failure and closure of active session:

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

```
diagnose debug enable
diagnose wad debug enable level verbose
diagnose wad debug enable category http
diagnose wad debug enable category pam-video #If session recording is enabled
```

Alternatively, in the FortiPAM GUI:

a. Go to *Log & Report* > *Debug Settings*.
   The *Debug Settings* window opens.

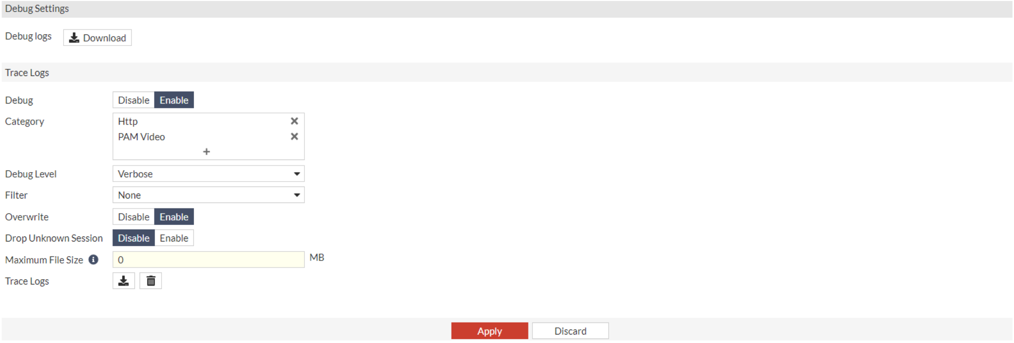
b. In the *Trace Logs* pane:

   i. Enable *Debug*.

   ii. In *Category*, select +, from the list, select *Http* and *PAM Video*.

   iii. In the *Debug Level* dropdown, select *Verbose*.

   iv. Enable *Overwrite*.



Debug Settings

Debug logs: Download

Trace Logs

Debug: Disable [✓ Enable]

Category: Http ✕
 PAM Video ✕
 +

Debug Level: Verbose

Filter: None

Overwrite: Disable [✓ Enable]

Drop Unknown Session: [✓ Disable] Enable

Maximum File Size: 0 MB

Trace Logs

c. Click *Apply*.

d. Reproduce the issue.

e. Return to *Log & Report* > *Debug Settings*.

f. In the *Trace Logs* pane, select the download icon (⭳) to download the trace log.
   A `.tar` trace file is downloaded on your computer.

Troubleshooting log and video disk encryption issues

Issue 1:

How to check disk encryption configuration and disk format?

The command `execute disk encryption status` shows both disk encryption configuration under `config secret setting` and also the format of log and video disks.

For example:

```
execute disk encryption status
In Configuration file, Disk encryption setting is Enable
Log Disk is /dev/sdb1 and it is in encrypted format.
Video Disk is /dev/sdc1 and it is in encrypted format.

[Good] Disk format matches the disk encryption setting in configuration file.

If there is problem regarding log or video,
Run command 'execute disk encryption log' for more information.
Run command 'execute disk encryption video' for more information.
```

Issue 2:

How to check the log or video disk status?

Use `execute disk encryption log` or `execute disk encryption video` command.

Where:

1. `Mount`: Indicates if the directory for log and video is correctly mounted to the disk device. An error usually means the log or video cannot be successfully saved into FortiPAM.
2. `Configuration`: Shows both the disk encryption configuration under `config secret setting` and the format of log and video disk. When configuration and disk format do not match, you need to check whether the correct configuration file is used or format the disk based on the setting in the configuration file.
3. `Open`: Disks can only be opened by using the correct `disk-encryption-password`. When the disk fails to open, it usually means the password in the configuration is incorrect.
4. `LUKS HEADER`: Dumps the encrypted disk header containing the disk label and other information.

For example:

```
execute disk encryption log
```

Log disk status:

1. `Mount`:

   device name: `/dev/mapper/dm_log`

   directory: `/var/log`

filesystem type: `ext4`

2. `Configuration`:

   In the configuration file, disk encryption is Enable.

   Disk is `/dev/sdb1` and it is in encrypted format.

   [Good] Disk format matches the disk encryption setting in configuration file.
3. `Open`:

   [Good] Disk is opened and active.
4. `Disk LUKS HEADER`:

   LUKS header information

   Version: 2

   Epoch:3

   Metadata area: 16384 [bytes]

   Keyslots area: 16744448 [bytes]

   UUID: 5633c25c-19e7-42e7-97f6-c62d2829bbba

   Label: LOGUSEDX8FAC98BD

   Subsystem: (no subsystem)

   Flags: (no flags)

Data segments:

0: crypt

offset: 16777216 [bytes]

length: (whole device)

cipher: aes-xts-plain64

sector: 512 [bytes]

Keyslots:

0: luks2

Key: 512 bits

Priority: normal

Cipher: aes-xts-plain64

Cipher key: 512 bits

PBKDF: argon2id

Time cost: 4

Memory: 774464

Threads: 2

Salt: d7 8c 1c f1 6d c0 f1 99 ed 00 3b 48 5f 6a 10 07

b4 17 f0 06 67 1b 51 f0 d9 53 80 df 0d 39 ff 74

AF stripes: 4000

AF hash: sha256

Area offset:32768 [bytes]

Area length:258048 [bytes]

Digest ID: 0

Tokens:

Digests:

0: pbkdf2

Hash: sha256

Iterations: 81715

Salt: 56 69 3c d0 f3 77 04 e5 e7 ec 2b 71 dd 66 28 33

0e 5c 07 8b 43 0c 27 47 48 ab 29 ee 95 ab 5d 58

Digest: 5e 8a dc b8

Issue 3:

What to do when there is `Open disk failed!` message after FortiPAM starts?

When there is `Open disk failed!` message when FortiPAM starts such as following:

```
System is starting...
we have 2 interfaces
Open disk failed! dev=/dev/vda1
Open dev /dev/vda1 in encryption format failed. ret=-4
```

Use `execute disk encryption` to get more help message.

```
execute disk encryption
```

`enable`: enable disk encryption on log and video disk.

`disable`: disable disk encryption on log and video disk.

`log`: check log disk encryption status.

`status`: check disk encryption status.

`video`: check video disk encryption status

Issue 4:

What to do when configuration does not match the disk format?

When disk-encryption setting in the configuration file and disk format does not match, use commands `execute disk encryption status` to get more help message.

```
FPAVUL2022103101 login:Disk Encryption is disabled in configuration file, but disk is in
     encrypted format! Device: /dev/vdb1
Run command 'execute disk encryption stat[ 35.678543] EXT4-fs (vdb1): VFS: Can't find
     ext4 filesystem us' for more information.
Storage HD2 mount failed. Giving up.
FPAVUL2022103101 login: admin
```

```
Password:
Welcome!
FPAVUL2022103101 # execute disk encryption status
In the configuration file, disk encryption setting is Disable
Log Disk is /dev/vda1 and it is in encrypted format.
Video Disk is /dev/vdb1 and it is in encrypted format.
[Error] Disk format does not match the disk encryption setting in configuration file.
```

Option 1:

Restore a previous backup configuration that contain `set disk-encryption enable` under `config secret setting`.

Contents in the disks could be kept if correct configuration is restored.

Option 2:

To enable disk encryption, run `execute disk encryption enable` command.

Option 3:

Run `execute disk format` command to format disk based on disk encryption setting.

Note that for option 2 and 3, disk will be encrypted/ formatted and all the content on the log and video disk is lost.

FortiClient troubleshooting tips

After you configure the required secrets, FortiClient uses the following three processes to launch the native application and start the video recording services:

- FortiVRS with session ID: 0
  - Save and drop ZTNA rules for each secret request.
  - Manage FortiVRS[X] daemons.
  - Upload video and metadata files to FortiPAM.
- FortiVRS with the user session
  - Start applications in the user session.
  - Record application videos.
  - Record the key and mouse metadata for the launched secret.
- FortiTCS
  - ZTNA daemon feature (responsible for TCP forwarding).
  - Create local proxy to forward TCP traffic.

Issue 1: Error contacting FortiClient

Ensure that FortiClient is running with the following three daemons:

- FortiTCS in session 0
- FortiVRS in session 0
- FortiVRS in user session [X]

Issue 2: Error starting the program

Ensure that the secret you are launching is installed on the client side machine with the environment variable set.

Issue 3: FortiPAM JSON error

This happens if you tamper the `ztna.config` file.

To recover, delete `ztna.config` and try again.

Issue 4: HTTP port mismatch between FortiPAM and FortiClient

Both FortiPAM and FortiVRS must use the same HTTP port.

To check for the port mismatch:

1. On FortiPAM, look for the value set in the *Client Port* field in the *Advanced* tab in *System* > *Settings*.
2. On the client machine, in the `fortivrs_session_0_1.log` file, ensure that the listeining port is same as the *Client Port* on FortiPAM.
3. If there is a mismatch between the port value in step 1 and 2, change the port value on FortiPAM to match the client machine port.

Issue 5: Secret not reaching the host

FortiClient can no longer reach the EMS server. Although ZTNA tunnels/rules can still be created, they fail to reach the host without an EMS connection.

Check the EMS server connection.

For fortitcs/fortivrs traces, go to `logs\trace\` in the FortiClient installation directory.

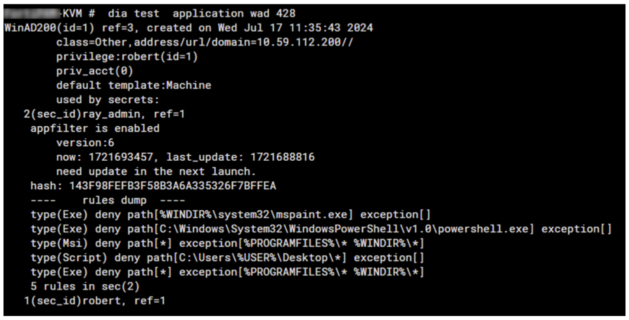
For the ZTNA configuration file, go to `C:\Users\Public\FortiClient\ztna\`.

For the secret session video recordings and metadata files, go to the Windows Temp directory `C:\Windows\Temp`.

Troubleshooting Windows application filter

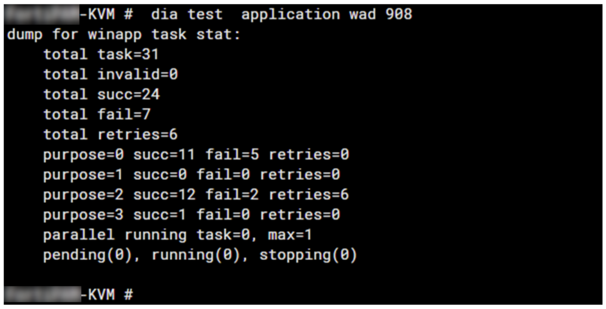
Use the following CLI commands to check the Windows application filter profile status:

```
 dignose debug enable
 diagnose test application wad 2300
 diagnose test application wad 428 #displays current rules per target and when they will be
updated
```



```
[redacted]KVM #  dia test  application wad 428
WinAD200(id=1) ref=3, created on Wed Jul 17 11:35:43 2024
        class=Other,address/url/domain=10.59.112.200//
        privilege:robert(id=1)
        priv_acct(0)
        default template:Machine
        used by secrets:
   2(sec_id)ray_admin, ref=1
    appfilter is enabled
        version:6
        now: 1721693457, last_update: 1721688816
        need update in the next launch.
    hash: 143F98FEFB3F58B3A6A335326F7BFFEA
    ----    rules dump  ----
    type(Exe) deny path[%WINDIR%\system32\mspaint.exe] exception[]
    type(Exe) deny path[C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe] exception[]
    type(Msi) deny path[*] exception[%PROGRAMFILES%\* %WINDIR%\*]
    type(Script) deny path[C:\Users\%USER%\Desktop\*] exception[]
    type(Exe) deny path[*] exception[%PROGRAMFILES%\* %WINDIR%\*]
    5 rules in sec(2)
   1(sec_id)robert, ref=1
```

```
 diagnose debug enable
 diagnose test application wad 2300
 diagnose test application wad 908 #displays the dump for the current status of the Windows
application filter tasks. This indicates the numbers of successful or failed tasks as well
as those that are pending, running, or stopped.
```



```
[redacted]-KVM #  dia test  application wad 908
dump for winapp task stat:
    total task=31
    total invalid=0
    total succ=24
    total fail=7
    total retries=6
    purpose=0 succ=11 fail=5 retries=0
    purpose=1 succ=0 fail=0 retries=0
    purpose=2 succ=12 fail=2 retries=6
    purpose=3 succ=1 fail=0 retries=0
    parallel running task=0, max=1
    pending(0), running(0), stopping(0)

[redacted]-KVM #
```

Hardening

System hardening reduces security risk by eliminating potential attack vectors and shrinking the system's attack surface.

This chapter describes some best practices that contribute to the hardening of the FortiPAM device.

The following topics are included in this section:

- Secure password storage on page 448
- Verify the private-data-encryption feature Example on page 449
- How to restore a backup configuration file with private-data-encryption enabled Example on page 449
- Enabling private-data-encryption on an HA cluster Example on page 450

Secure password storage

The passwords, and private keys used in certificates, that are stored on the FortiPAM are encrypted using a predefined private key, and encoded when displayed in the CLI and configuration file.

Passwords cannot be decrypted without the private key and are not shown anywhere in clear text. The private key is required on other FortiPAM to restore the system from a configuration file. In an HA cluster, the same key should be used on all of the units.

To enhance password security, specify a custom private key for the encryption process. This ensures that the key is only known by you.

FortiPAM models with a Trusted Platform Module (TPM) can store the primary encryption password, which is used to generate the primary encryption key, on the TPM. For more information, see FortiPAM with TPM on page 47.

To configure the private encryption key:

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

   ```
   config system global
     set private-data-encryption enable
   end
   Please type your private data encryption key (32 hexadecimal numbers):
   ********************************
   Please re-enter your private data encryption key (32 hexadecimal numbers) again:
   ********************************
   Your private data encryption key is accepted.
   ```

   See Verify the private-data-encryption feature Example on page 449.

Verify the `private-data-encryption` feature - Example

In this topic, we demonstrate how to verify the `private-data-encryption` feature, also known as Secure password storage. See Secure password storage on page 448.

To verify the `private-data-encryption` feature:

1. After configuring the custom 32 characters hexadecimal private data encryption key as shown in Secure password storage on page 448, in the CLI console, enter the following commands and note down the `B64TEXT` and `B64HMAC` sample keys that appear:

```
execute private-encryption-key sample
```

The following shows an example of successful activation:

```
execute private-encryption-key sample
B64TEXT: oR3J+DhKPF4xSFDZv43o/pkRBCTop+4w1IU8OEaLh5I=
B64HMAC: /4e77yCRzi6hunROBDm+/97bthc=
```

The following shows an example where the `private-data-encryption` feature is not enabled:

```
 execute private-encryption-key sample
 Private encryption is not enabled.
 Command fail. Return code 7.
```

2. In the CLI console, enter the following commands to verify the `private-data-encryption` feature:

```
  execute private-encryption-key verify  <B64TEXT> <B64HMAC>
  execute private-encryption-key verify oR3J+DhKPF4xSFDZv43o/pkRBCTop+4w1IU8OEaLh5I=
/4e77yCRzi6hunROBDm+/97bthc=
 Verification passed.
```

Or

```
 get system status | grep "Private Encryption"
 Private Encryption: Enable
```

How to restore a backup configuration file with `private-data-encryption` enabled - Example

In this topic, we demonstrate how to restore a backup configuration file with `private-data-encryption` enabled when the FortiPAM device is factory reset or replaced due to hardware failure.

Here, `private-data-encryption` is enabled with `0123456789abcdef0123456789abcdef` as the private key.

To restore a backup configuration file:

1. In the CLI console, enter the following commands to enable `private-data-encryption`:

```
config system global
 set private-data-encryption enable
```

```
end
Please type your private data encryption key (32 hexadecimal numbers):
 0123456789abcdef0123456789abcdef
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
 0123456789abcdef0123456789abcdef
Private data encryption key is accepted.
```

2. To back up and restore configuration files, see Backup and restore.

In case the FortiPAM device accidentally factory resets or there is a hardware failure, restoring the backed up configuration file does not retrieve all the previously encrypted passwords.

The following shows the configuration file error when booting up:

```
Initializing firewall...
System is starting...
The config file may contain errors,
Please see details by the command 'diagnose debug config-error-log
read'
```

3. To restore the configuration on factory reset or on a new FortiPAM device, you must set the private key prior to restoring the configuration file:

```
config system global
 set private-data-encryption enable
end
Please type your private data encryption key (32 hexadecimal numbers):
0123456789abcdef0123456789abcdef
Please re-enter your private data encryption key (32 hexadecimal numbers) again:
0123456789abcdef0123456789abcdef
```

4. The private data encryption key is accepted.
   When this private data encryption key is entered, the configuration file is restored.

Enabling `private-data-encryption` on an HA cluster - Example

When using an HA cluster, the keys used for `private-data-encryption` are synchronized among all the cluster members.

In a redundant setup (HA), the units must have the same key so that the encrypted elements are properly synchronized.

To enable `private-data-encryption` before the HA cluster is formed:

1. In the CLI console, on each member of the HA cluster to be formed, enter the following commands:

```
config system global
   set private-data-encryption enable
 end
 Please type the private data encryption key (32 hexadecimal numbers):
 0123456789abcdef0123456789abcdef
```

```
  Please re-enter the private data encryption key (32 hexadecimal numbers) again:
0123456789abcdef0123456789abcdef
  The private data encryption key is accepted.
```

To enable `private-data-encryption` on the HA cluster:

1. In the CLI console, on any member of the HA cluster, enter the following commands:

   ```
    config system global
     set private-data-encryption enable
    end
    Please type the private data encryption key (32 hexadecimal numbers):
    0123456789abcdef0123456789abcdef
    Please re-enter the private data encryption key (32 hexadecimal numbers) again:
   0123456789abcdef0123456789abcdef
    The private data encryption key is accepted.
   ```

   The setting and the key is pushed to all the members in the HA cluster.

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*.

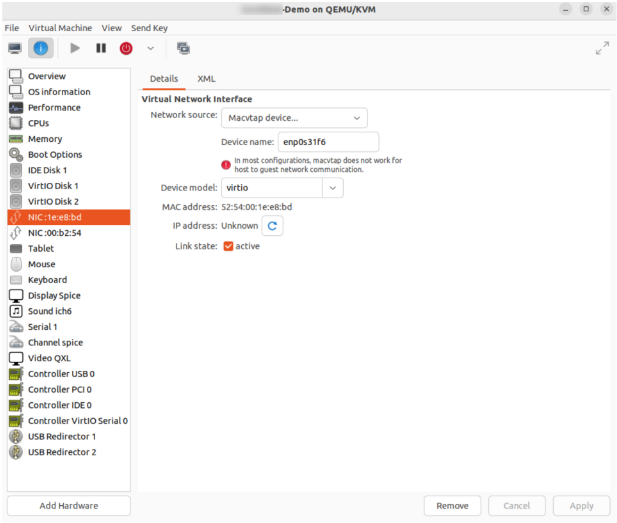
To add ethernet interfaces:

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`.

If no host device information shows up, i.e., the *Network source* dropdown only shows *Macvtap* with no *enxxx* information, you must enter the ethernet interface name in *Device name*.



Virtual Network Interface

Network source: Macvtap device...

Device name: enp0s31f6

In most configurations, macvtap does not work for host to guest network communication.

Device model: virtio

MAC address: 52:54:00:1e:e8:bd

IP address: Unknown

Link state: ☑ active

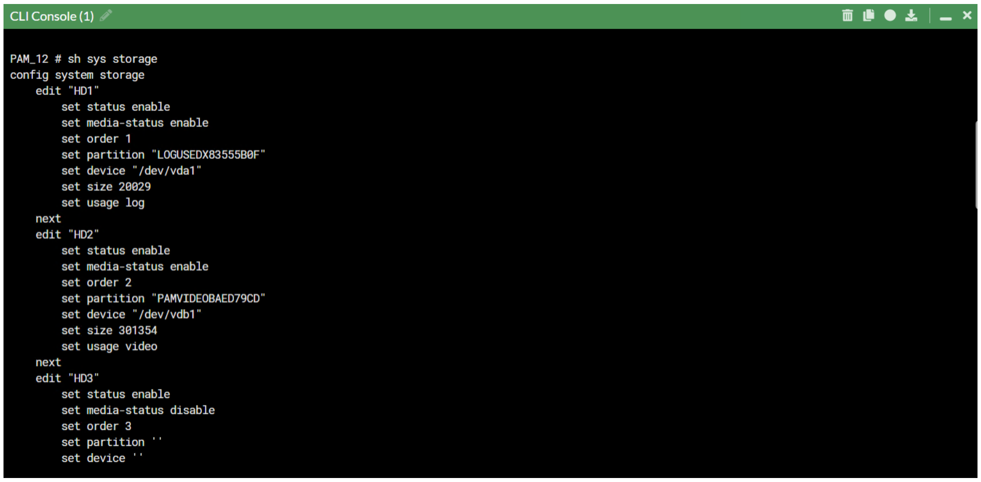
4. In the *Device model* dropdown, select *virtio*.
5. Click *Apply*.
6. Click *Add Hardware*, and select the option to add an additional interface.
7. In the *Device model* dropdown, select *virtio*.
8. Select *Finish*.
9. Click *Begin Installation* to start installing the new VM.

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 ''
```



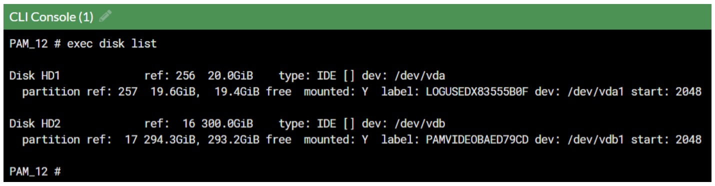
CLI Console (1)

```
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  20.0GiB    type: IDE [] dev: /dev/vda
  partition ref: 257  19.6GiB,  19.4GiB free  mounted: Y  label: LOGUSEDX83555B0F dev: /dev/vda1 start: 2048

Disk HD2            ref:  16 300.0GiB    type: IDE [] dev: /dev/vdb
  partition ref:  17 294.3GiB, 293.2GiB 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
```

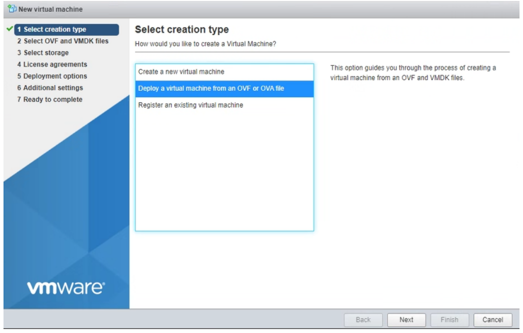
Disk formatting results in the loss of all existing logs and videos.

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*.



Select creation type

How would you like to create a Virtual Machine?

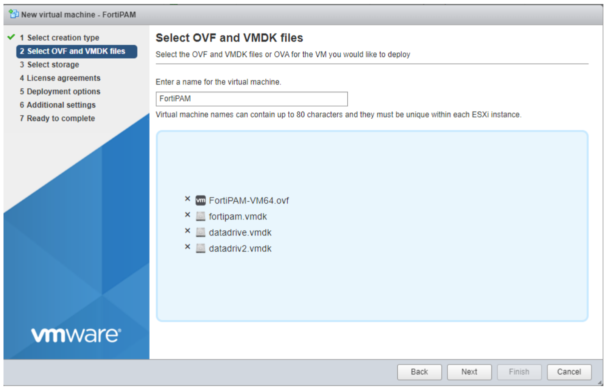
Create a new virtual machine

Deploy a virtual machine from an OVF or OVA file

Register an existing virtual machine

This option guides you through the process of creating a virtual machine from an OVF and VMDK files.

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*.



Select OVF and VMDK files

Select the OVF and VMDK files or OVA for the VM you would like to deploy

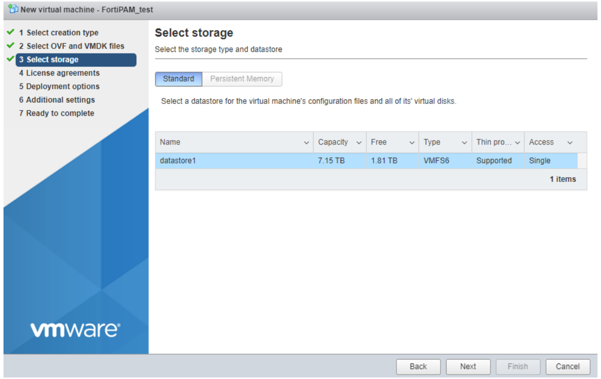
Enter a name for the virtual machine.

FortiPAM

Virtual machine names can contain up to 80 characters and they must be unique within each ESXi instance.

× FortiPAM-VM64.ovf
× fortipam.vmdk
× datadrive.vmdk
× datadriv2.vmdk

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



Select storage

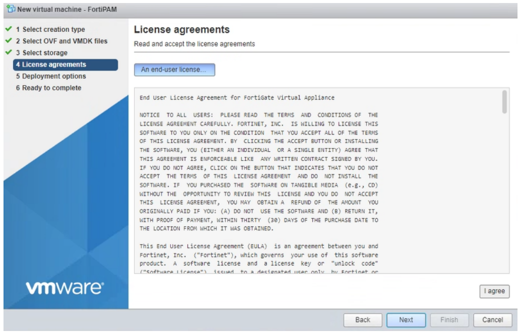
Select the storage type and datastore

Select a datastore for the virtual machine's configuration files and all of its' virtual disks.

Name	Capacity	Free	Type	Thin pro...	Access
datastore1	7.15 TB	1.81 TB	VMFS6	Supported	Single

1 items

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



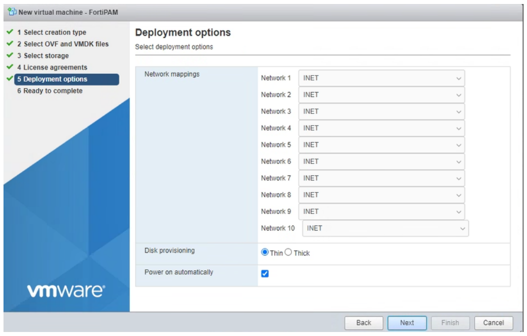
License agreements

Read and accept the license agreements

```
End User License Agreement for FortiGate Virtual Appliance

NOTICE  TO ALL  USERS:  PLEASE READ  THE TERMS  AND  CONDITIONS OF  THE
LICENSE AGREEMENT CAREFULLY. FORTINET, INC.  IS WILLING TO LICENSE THIS
SOFTWARE TO YOU ONLY ON THE CONDITION  THAT YOU ACCEPT ALL OF THE TERMS
OF THIS LICENSE AGREEMENT. BY  CLICKING THE ACCEPT BUTTON OR INSTALLING
THE SOFTWARE, YOU (EITHER AN INDIVIDUAL  OR A SINGLE ENTITY) AGREE THAT
THIS AGREEMENT IS ENFORCEABLE LIKE  ANY WRITTEN CONTRACT SIGNED BY YOU.
IF YOU DO NOT AGREE, CLICK ON THE BUTTON THAT INDICATES THAT YOU DO NOT
ACCEPT  THE TERMS  OF THIS  LICENSE AGREEMENT  AND DO  NOT INSTALL  THE
SOFTWARE. IF  YOU PURCHASED THE  SOFTWARE ON TANGIBLE MEDIA  (e.g., CD)
WITHOUT THE  OPPORTUNITY TO REVIEW THIS  LICENSE AND YOU DO  NOT ACCEPT
THIS  LICENSE AGREEMENT,  YOU MAY  OBTAIN A  REFUND OF  THE AMOUNT  YOU
ORIGINALLY PAID IF YOU: (A) DO NOT  USE THE SOFTWARE AND (B) RETURN IT,
WITH PROOF OF PAYMENT, WITHIN THIRTY  (30) DAYS OF THE PURCHASE DATE TO
THE LOCATION FROM WHICH IT WAS OBTAINED.

This End User License Agreement (EULA)  is an agreement between you and
Fortinet, Inc.  ("Fortinet"), which governs  your use of  this software
product.  A  software  license  and  a license  key  or  "unlock  code"
("Software License")  issued  to a designated user only  by Fortinet or
```

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.



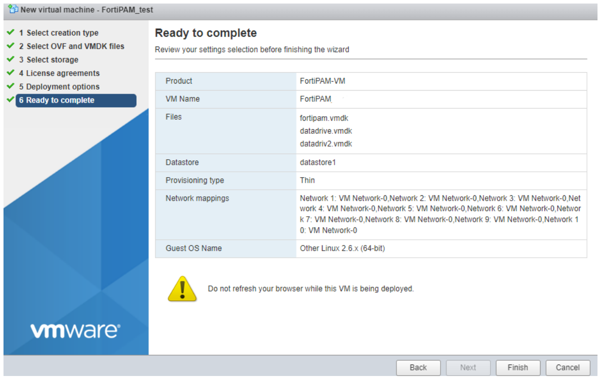
Deployment options

Select deployment options

Network mappings	Network 1	INET
	Network 2	INET
	Network 3	INET
	Network 4	INET
	Network 5	INET
	Network 6	INET
	Network 7	INET
	Network 8	INET
	Network 9	INET
	Network 10	INET
Disk provisioning	● Thin ○ Thick	
Power on automatically	☑	

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*.



New virtual machine - FortiPAM_test

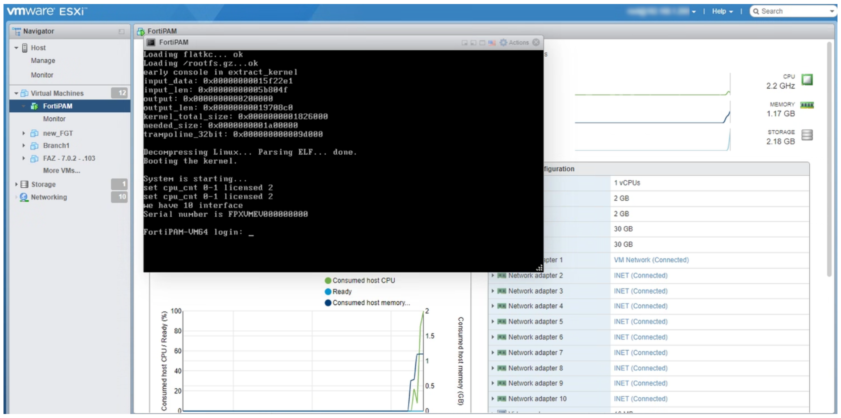
Ready to complete

Review your settings selection before finishing the wizard

Product	FortiPAM-VM
VM Name	FortiPAM
Files	fortipam.vmdk datadrive.vmdk datadriv2.vmdk
Datastore	datastore1
Provisioning type	Thin
Network mappings	Network 1: VM Network-0,Network 2: VM Network-0,Network 3: VM Network-0,Network 4: VM Network-0,Network 5: VM Network-0,Network 6: VM Network-0,Network 7: VM Network-0,Network 8: VM Network-0,Network 9: VM Network-0,Network 10: VM Network-0
Guest OS Name	Other Linux 2.6.x (64-bit)

Do not refresh your browser while this VM is being deployed.

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.



```
Loading flatkc... ok
Loading /rootfs.gz...ok
early console in extract_kernel
input_data: 0x00000000015f22e1
input_len: 0x00000000005b804f
output: 0x0000000000200000
output_len: 0x00000000019708c0
kernel_total_size: 0x0000000001826000
needed_size: 0x0000000001a00000
trampoline_32bit: 0x000000000009d000

Decompressing Linux... Parsing ELF... done.
Booting the kernel.

System is starting...
set cpu_cnt 0-1 licensed 2
set cpu_cnt 0-1 licensed 2
we have 10 interface
Serial number is FPXVMEV000000000

FortiPAM-VM64 login: _
```

figuration	
	1 vCPUs
	2 GB
	2 GB
	30 GB
	30 GB
apter 1	VM Network (Connected)
Network adapter 2	INET (Connected)
Network adapter 3	INET (Connected)
Network adapter 4	INET (Connected)
Network adapter 5	INET (Connected)
Network adapter 6	INET (Connected)
Network adapter 7	INET (Connected)
Network adapter 8	INET (Connected)
Network adapter 9	INET (Connected)
Network adapter 10	INET (Connected)

See FortiPAM appliance setup on page 45 for CLI related settings to verify the disk usage type and set up FortiPAM.

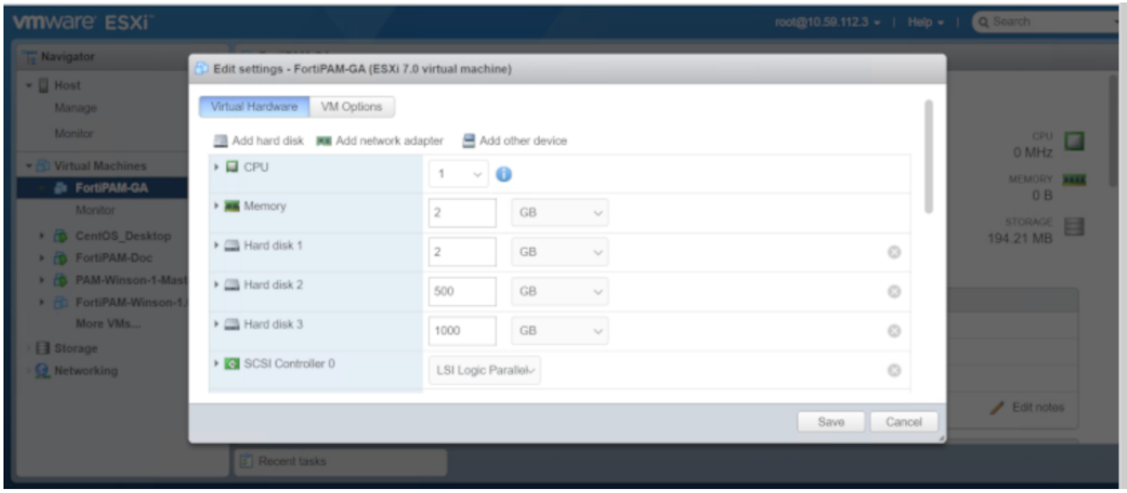
10. The default size for the log and the video disk is 30 GB. If the size does not meet your requirement, see *Log and video disk size guidelines* in *System requirements* in the *VMware ESXi Admin Guide*.

To adjust the log or video disk size:

Disk size tuning results in the loss of existing logs and videos.

a. Shutdown your VM.
b. In the VMware vSphere Client, right-click the name of the virtual appliance, and select *Edit settings*.
The *Edit settings* page is displayed.
c. Ensure that you are in the *Virtual Hardware* tab.
d. Keep *Hard disk 1* as 2 GB. *Hard disk 1* is used for FortiPAM bootup.

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



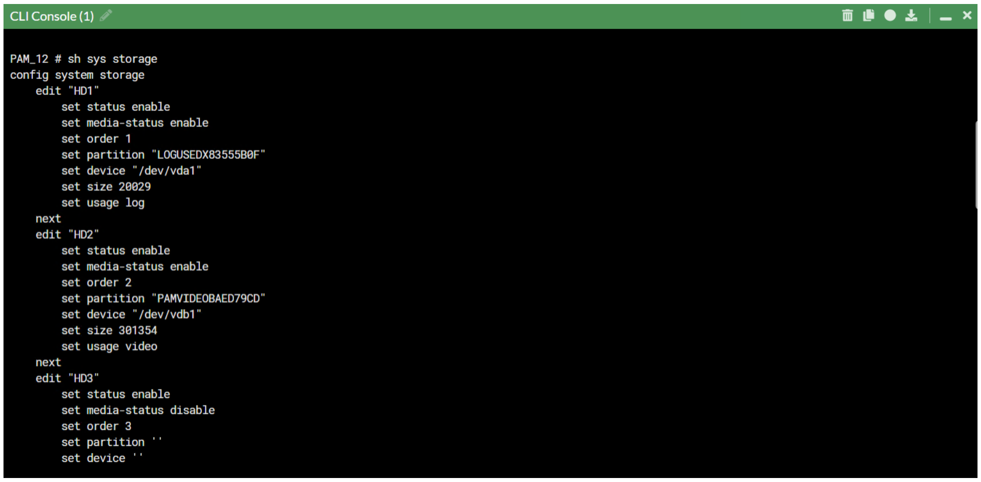
Edit settings - FortiPAM-GA (ESXi 7.0 virtual machine)

CPU 1
Memory 2 GB
Hard disk 1 2 GB
Hard disk 2 500 GB
Hard disk 3 1000 GB
SCSI Controller 0 LSI Logic Parallel

f. Click *Save* to save the changes.
You can now power on the VM.

11. If *Power on automatically* is unselected in step 7 and the VM has never been powered on, any disk size change automatically takes effect after the VM is powered on the first time.
If the disk sizes are tuned after powering on the VM for the first time, enter `sh sys storage` CLI command to verify that the disk size change was successful:

```
config system storage
   edit "HD1"
      set status enable
      set media-status enable
      set order 1
      set partition "LOGUSEDX83555B0F"
      set device "/dev/vda1"
      set size 20029
      set usage log
   next
   edit "HD2"
      set status enable
      set media-status enable
      set order 2
      set partition "PAMVIDEOBAED79CD"
      set device "/dev/vdb1"
      set size 301354
      set usage video
   next
   edit "HD3"
      set status enable
      set media-status disable
      set order 3
      set partition ''
      set device ''
```

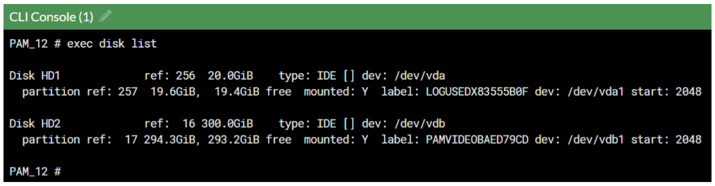


```
PAM_12 # sh sys storage
config system storage
    edit "HD1"
        set status enable
        set media-status enable
        set order 1
        set partition "LOGUSEDX83555B0F"
        set device "/dev/vda1"
        set size 20029
        set usage log
    next
    edit "HD2"
        set status 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.



```
PAM_12 # exec disk list

Disk HD1            ref: 256  20.0GiB    type: IDE [] dev: /dev/vda
  partition ref: 257  19.6GiB,  19.4GiB free  mounted: Y  label: LOGUSEDX83555B0F dev: /dev/vda1 start: 2048

Disk HD2            ref:  16 300.0GiB    type: IDE [] dev: /dev/vdb
  partition ref:  17 294.3GiB, 293.2GiB 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):

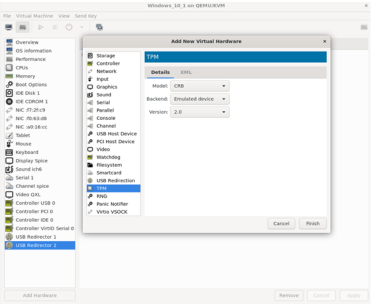
1. In the command line, enter the following commands:

```
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 452.
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*.



Model: CRB

Backend: Emulated device

Version: 2.0

This adds *TPM v2.0* to the list of hardware devices on the left.

Appendix D: vTPM for FortiPAM on VMware

To successfully enable vTPM, you must configure a key provider on the VMware vSphere client.

Ensure that TPM is set up as part of the initial configuration, i.e., before powering on the FortiPAM-VM for the first time.

To configure a key provider:

1. Select the virtual appliance in the VMware vSphere client and go to *Configure* > *Security* > *Key Providers*.
2. In *Key Providers*, from the *Add* dropdown, select *Add Native Key Provider*.
3. In the *Add Native Key Provider* window:
   a. Enter a name for the native key provider.
   b. Deselect *Use key provider only with TPM protected ESXi hosts*.
   c. Select *ADD KEY PROVIDER*.
4. Select the new key provider from the key providers list and then select *BACK UP*.
   The *Back up Native Key Provider* window opens.
5. Select *BACK UP KEY PROVIDER*.
   The key provider is saved on your computer.

To enable vTPM for FortiPAM:

1. Right-click the virtual appliance in the VMware vSphere client and select *Edit Settings*.

   Ensure that the *Guest OS Version* in *VM Options* tab is set to *Other 4.x or later Linux (64-bit)* or higher.

2. In *Edit Settings*, click *Add New Device* and select *Trusted Platform Module*.
3. Click *OK*.

Appendix E: Enabling soft RAID on KVM or VMware

To expand hard disk capacity, you can enable RAID on the FortiPAM-VM. After RAID is enabled, hard disk capacity can be expanded from 2 TB to 16 TB.

Individual disks of sizes up to 2 TB are supported.

Starting FortiPAM 1.1.0, the disk size is limited by the GPT partition size.

Soft RAID is supported on KVM and VMware platforms. Hyper-V and other platforms are not supported yet.

Note: Soft RAID for VMware requires disks of the same size.

RAID can only be configured using the CLI commands.

Enabling, disabling, and changing the RAID level, erases all the data on the log and video disk. Also, the FortiPAM device reboots every time RAID is enabled, disabled, or the RAID level is changed.

To configure RAID via CLI:

1. Before enabling RAID, enter the following command in the CLI console to verify that the FortiPAM has multiple disks:
   ```
   execute disk list
   ```
   or
   ```
   diagnose hardware deviceinfo disk
   ```
   Use `diagnose system disk info` to check the disk-related information.

2. In the CLI console, enter the following command to enable RAID:
   ```
   execute disk raid enable <RAID level> #The default value is Raid-0
   ```
   Two partitions will be created after RAID is enabled. One partition for log and one for video.

   To disable RAID, enter `execute disk raid disable`.

When there are two disks, RAID `level 0` and `1` are available. Only when there are four disks, RAID `level 5` and `10` are available.

3. From the *Admin* dropdown in the banner, go to *System* > *Reboot* to reboot FortiPAM.

Reboot is only available when FortiPAM is in maintenance mode.

To enable the maintenance mode, see Enabling maintenance mode.

4. In the *Reboot* window, click *OK* to confirm.
   Optionally, enter an event log message.
5. For the FortiPAM-VM, in the CLI console, check the RAID status by entering the following command:

```
execute disk raid status #Raid is now available
```

If the above steps do not enable RAID on FortiPAM-VM, use the following workaround:

1. Factory reset your FortiPAM-VM.
2. Remove disk from your FortiPAM-VM, then add the disk again.
3. Now follow the steps in Configuring RAID via CLI.

Rebuilding a RAID with a different RAID level

Admin can only rebuild RAID at the same RAID level if a RAID error has been detected. Also, changing the RAID level takes a while and deletes all data on the disk.

Use the following CLI command to rebuild RAID:

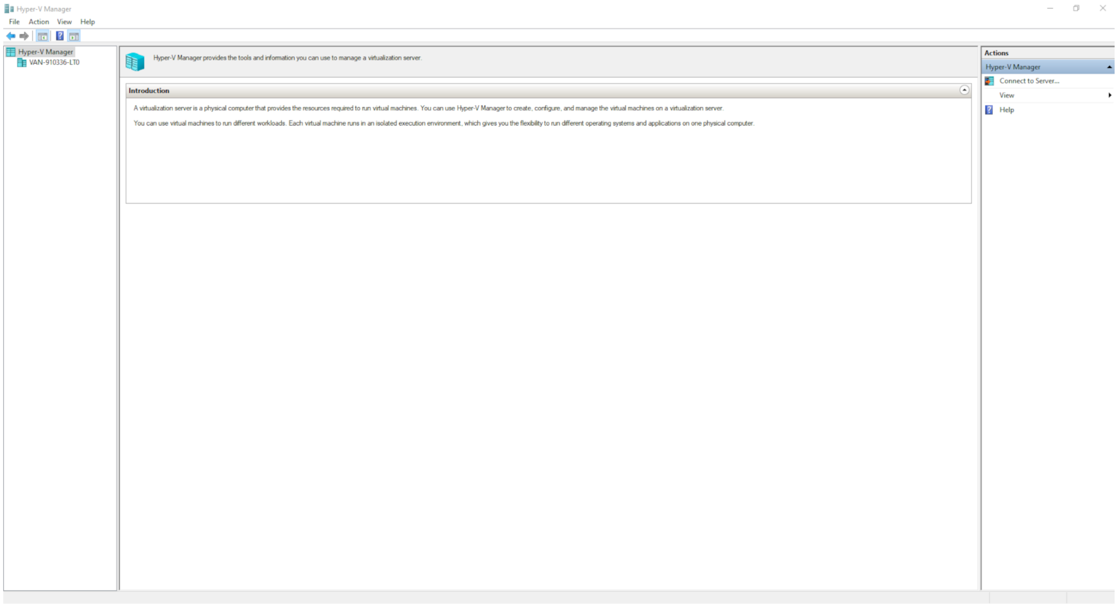
```
execute disk raid rebuild-level <RAID level>
```

Appendix F: Installation on Hyper-V

Once you have downloaded the `out.hyperv.zip` file and extracted the package contents to a folder on your management computer/Microsoft server, you can deploy the VHD package to your MS Hyper-V environment.

To deploy FortiPAM-VM on MS Hyper-V without TPM support:

1. Launch the Hyper-V Manager on your management computer.
   The *Hyper-V Manager* homepage opens.



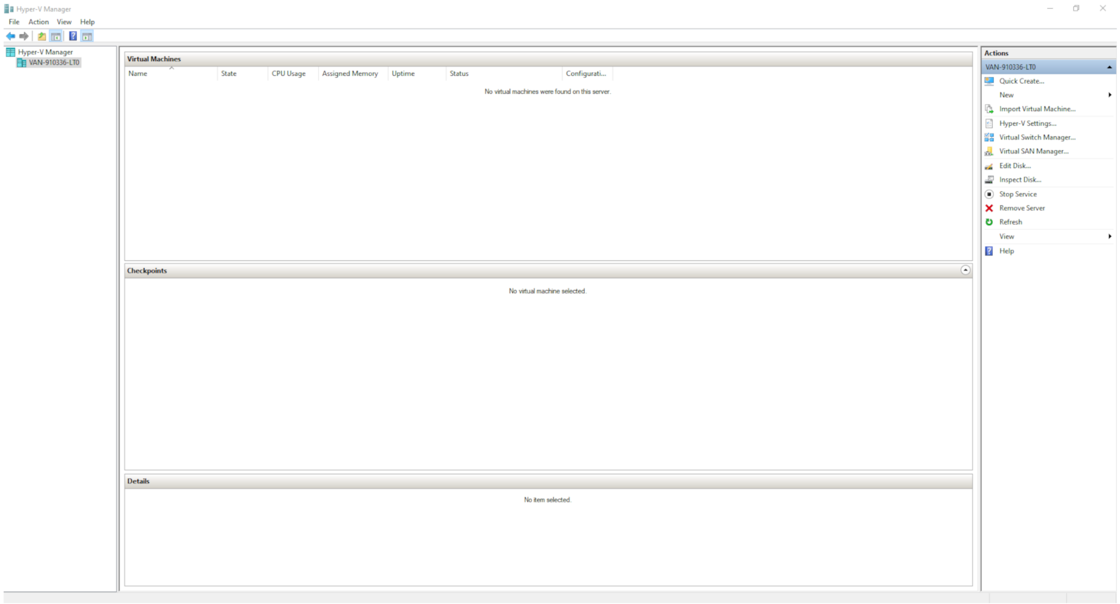
Hyper-V Manager provides the tools and information you can use to manage a virtualization server.

Introduction

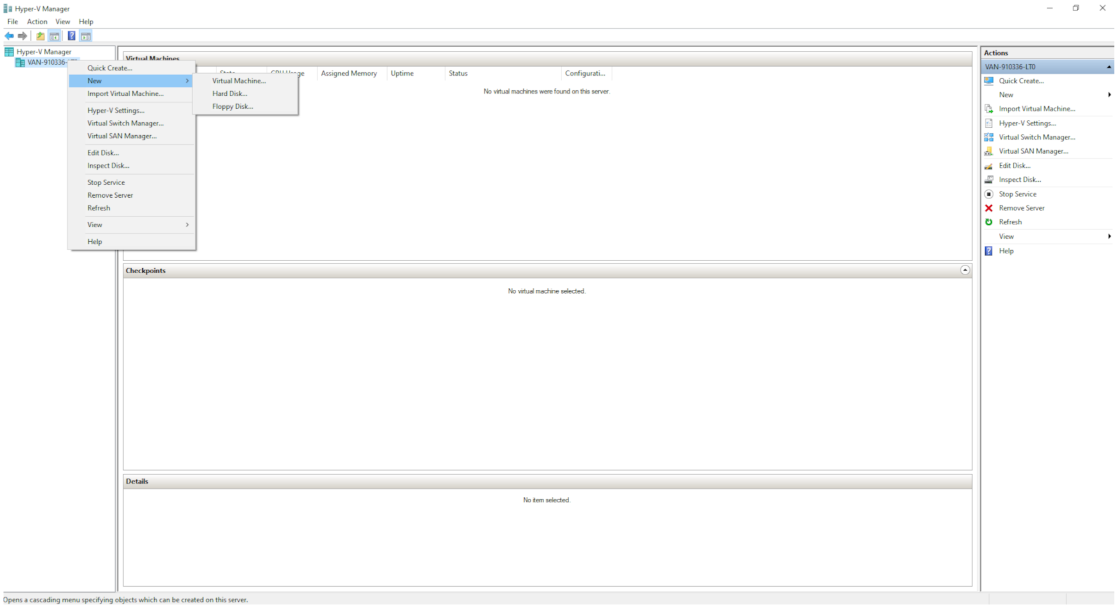
A virtualization server is a physical computer that provides the resources required to run virtual machines. You can use Hyper-V Manager to create, configure, and manage the virtual machines on a virtualization server.

You can use virtual machines to run different workloads. Each virtual machine runs in an isolated execution environment, which gives you the flexibility to run different operating systems and applications on one physical computer.

2. In the left tree menu, select your management computer.
   The server details page is displayed.

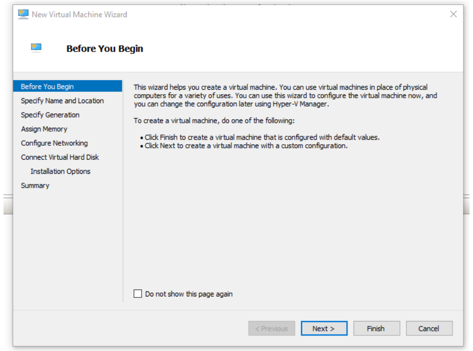


3. Right-click the server/management computer and select *New* > *Virtual Machine*. Optionally, in the *Action* menu, select *New* and select *Virtual Machine*.



Opens a cascading menu specifying objects which can be created on this server.

The *New Virtual Machine Wizard* opens.



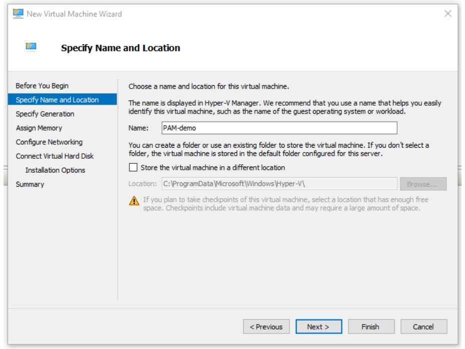
This wizard helps you create a virtual machine. You can use virtual machines in place of physical computers for a variety of uses. You can use this wizard to configure the virtual machine now, and you can change the configuration later using Hyper-V Manager.

To create a virtual machine, do one of the following:

- Click Finish to create a virtual machine that is configured with default values.
- Click Next to create a virtual machine with a custom configuration.

☐ Do not show this page again

4. In *New Virtual Machine Wizard*, click *Next* to create a VM with a custom configuration.
   The *Specify Name and Location* tab is displayed.
5. In *Specify Name and Location*, enter a name for this VM, and click *Next*.
   The *Hyper-V Manager* displays the name you enter for the VM.



Specify Name and Location

Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: PAM-demo

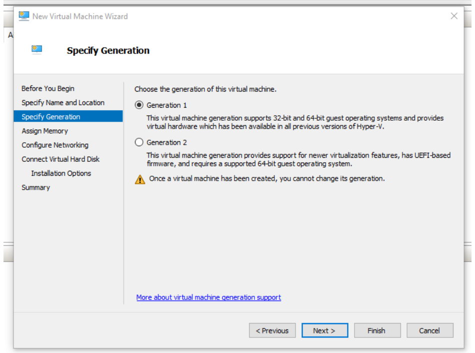
You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☐ Store the virtual machine in a different location

Location: C:\ProgramData\Microsoft\Windows\Hyper-V\

If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.

6. In *Specify Generation*, select *Generation 1*, and click *Next*.



Specify Generation

Choose the generation of this virtual machine.

● Generation 1

This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.

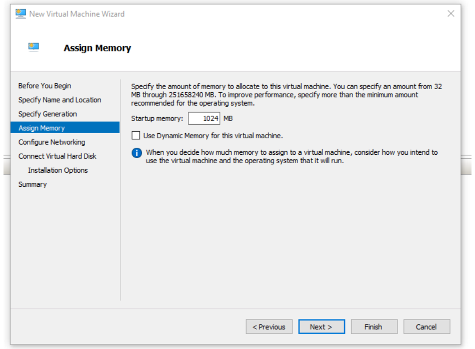
○ Generation 2

This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.

Once a virtual machine has been created, you cannot change its generation.

Generation 1 does not support TPM. To install FortiPAM-VM on Hyper-V with TPM, see Deploying FortiPAM on Hyper-V with TPM.

7. In *Assign Memory*, specify the amount of memory to allocate to this VM in *Startup memory*, and click *Next*.
   Ensure that *Use Dynamic Memory for this virtual machine* is unchecked.



Assign Memory

Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 251658240 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

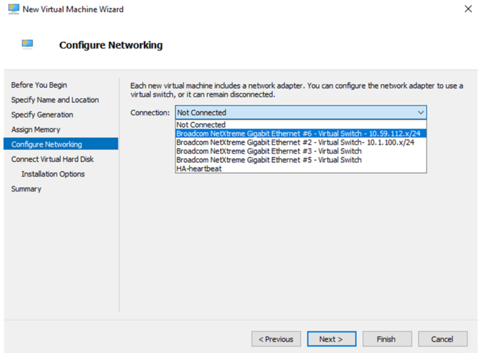
Startup memory: 1024 MB

☐ Use Dynamic Memory for this virtual machine.

When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

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

8. In *Configure Networking*, from the *Connection* dropdown, select a network adapter, and click *Next*.
   Each new VM includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected. You can configure more network adapters in the *Settings* window later.

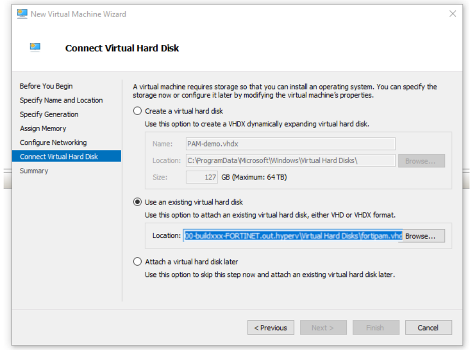


Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection: Not Connected

Not Connected
Broadcom NetXtreme Gigabit Ethernet #6 - Virtual Switch - 10.59.112.x/24
Broadcom NetXtreme Gigabit Ethernet #2 - Virtual Switch- 10.1.100.x/24
Broadcom NetXtreme Gigabit Ethernet #3 - Virtual Switch
Broadcom NetXtreme Gigabit Ethernet #5 - Virtual Switch
HA-heartbeat

9. In *Connect Virtual Hard Disk*, select *Use an existing virtual hard disk*, click *Browse* and locate the `fortipam.vhd` file that you downloaded from FortiCloud, and click *Next*.



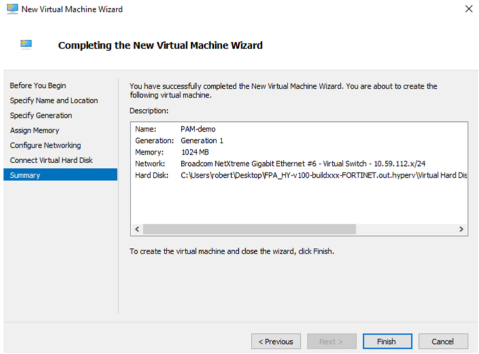
A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

○ Create a virtual hard disk
Use this option to create a VHDX dynamically expanding virtual hard disk.
Name: PAM-demo.vhdx
Location: C:\ProgramData\Microsoft\Windows\Virtual Hard Disks\
Size: 127 GB (Maximum: 64 TB)

● Use an existing virtual hard disk
Use this option to attach an existing virtual hard disk, either VHD or VHDX format.
Location: 00-buildxxx-FORTINET.out.hyperv\Virtual Hard Disks\fortipam.vhd

○ Attach a virtual hard disk later
Use this option to skip this step now and attach an existing virtual hard disk later.

10. In *Completing the New Virtual Machine Wizard*, the installation summary is displayed.


New Virtual Machine Wizard
Completing the New Virtual Machine Wizard
Before You Begin
Specify Name and Location
Specify Generation
Assign Memory
Configure Networking
Connect Virtual Hard Disk
Summary
< Previous
Next >
Finish
Cancel

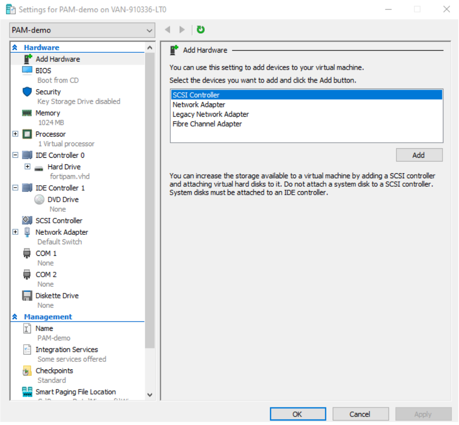
You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.

Description:

Name: PAM-demo
Generation: Generation 1
Memory: 1024 MB
Network: Broadcom NetXtreme Gigabit Ethernet #6 - Virtual Switch - 10.59.112.x/24
Hard Disk: C:\Users\robert\Desktop\FPA_HY-v100-buildxxx-FORTINET.out.hyperv\Virtual Hard Dis

To create the virtual machine and close the wizard, click Finish.

11. To create the VM and close the wizard, click *Finish*.
12. Right-click the VM and select *Settings* from the menu. Optionally, having selected the VM, in the *Action* menu, click *Settings*.



You can use this setting to add devices to your virtual machine.

Select the devices you want to add and click the Add button.

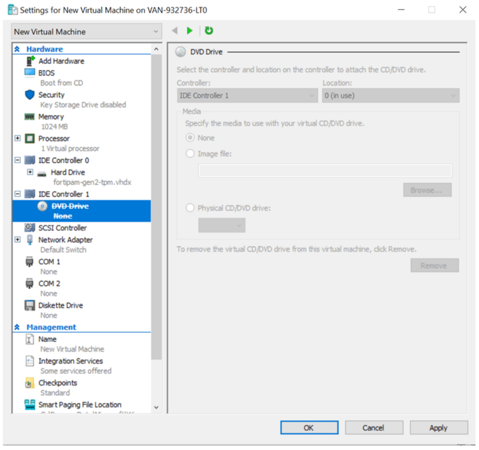
You can increase the storage available to a virtual machine by adding a SCSI controller and attaching virtual hard disks to it. Do not attach a system disk to a SCSI controller. System disks must be attached to an IDE controller.

13. In *Hardware*, to remove a DVD drive:

    a. Select a DVD drive in *IDE Controller 1*.

    b. Click *Remove*.

    c. Click *Apply*.



Select the controller and location on the controller to attach the CD/DVD drive.

Controller: IDE Controller 1

Location: 0 (in use)

Media

Specify the media to use with your virtual CD/DVD drive.

● None

○ Image file:

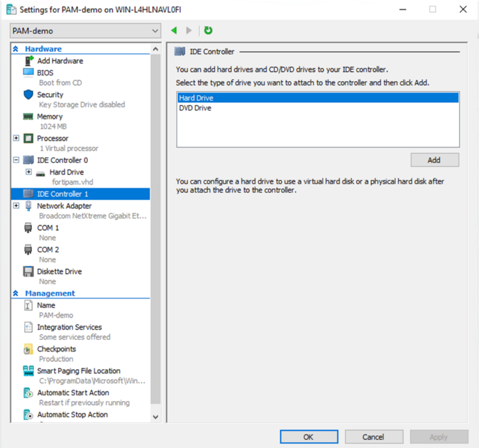
○ Physical CD/DVD drive:

To remove the virtual CD/DVD drive from this virtual machine, click Remove.

14. In *Hardware*, to add a hard drive:

    a. Click *IDE Controller 1*.

    b. Select *Hard Drive*.



You can add hard drives and CD/DVD drives to your IDE controller.

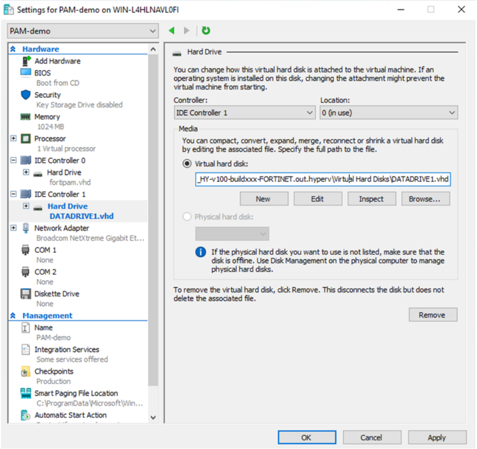
Select the type of drive you want to attach to the controller and then click Add.

You can configure a hard drive to use a virtual hard disk or a physical hard disk after you attach the drive to the controller.

    c. Click *Add*.

d. In *Hard Drive*, click *Browse* and locate the `DATADRIVE1.vhd` file that is in the same folder as `fortipam.vhd` file.

e. Click *Apply*.



Settings for PAM-demo on WIN-L4HLNAVL0FI

Hard Drive

You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.

Controller: IDE Controller 1

Location: 0 (in use)

Media

You can compact, convert, expand, merge, reconnect or shrink a virtual hard disk by editing the associated file. Specify the full path to the file.

● Virtual hard disk: `_HY-v100-buildxxx-FORTINET.out.hyperv\Virtual Hard Disks\DATADRIVE1.vhd`

○ Physical hard disk:

If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.

To remove the virtual hard disk, click Remove. This disconnects the disk but does not delete the associated file.

f. Click *OK*.

15. Repeat step 14 to add a second disk, `DATADRIVE2.vhd`.

16. From the virtual machines list, right-click the FortiPAM-VM and select *Start* to power on the VM.

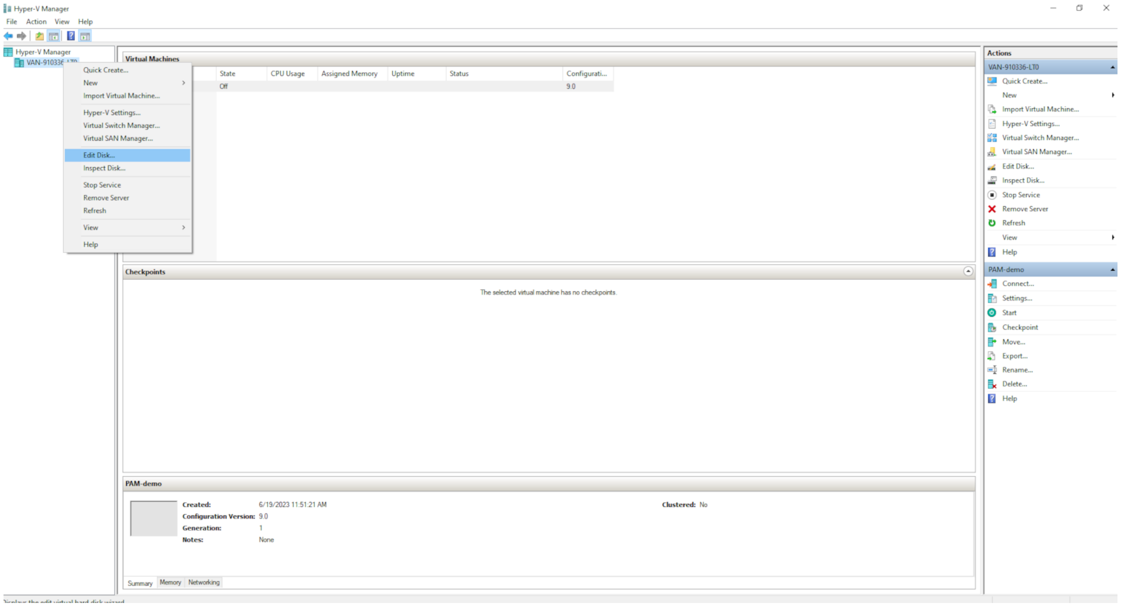
17. Select your newly created VM and launch it.
    See FortiPAM appliance setup on page 45 for CLI related settings to verify the disk usage type and set up FortiPAM.

To deploy FortiPAM-VM on MS Hyper-V with TPM support:

To use FortiPAM with TPM on a Hyper-V platform, first, you must convert the virtual hard disk from `*.vhd` to `*.vhdx` format (step 1) and then specify *Generation 2* when creating a new VM (step 2). Finally, you must enable TPM on Hyper-V before powering on the VM (step 3).

1. **Converting hard disk to `*.vhdx`:**

   a. In the left tree menu, right-click the server/management computer and select *Edit Disk*. Optionally, having selected the server, select *Action* and then select *Edit Disk*.



PAM-demo

Created: 6/19/2023 11:51:21 AM

Configuration Version: 9.0

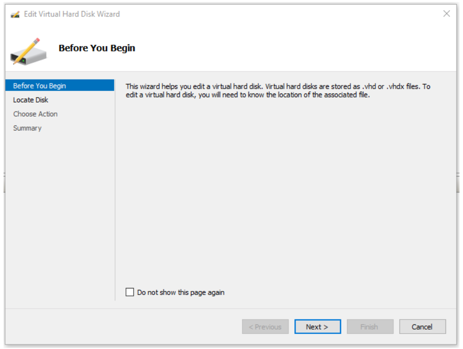
Generation: 1

Notes: None

Clustered: No

The selected virtual machine has no checkpoints.

The *Edit Virtual Hard Disk Wizard* opens.

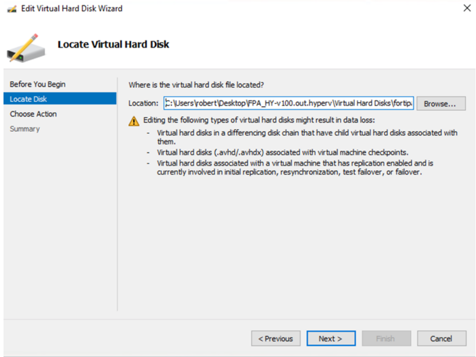


This wizard helps you edit a virtual hard disk. Virtual hard disks are stored as .vhd or .vhdx files. To edit a virtual hard disk, you will need to know the location of the associated file.

□ Do not show this page again

b. In the *Edit Virtual Hard Disk Wizard*, click *Next*.

c. In *Locate Virtual Hard Disk*, click *Browse* and locate the `fortipam.vhd` file that you downloaded from FortiCloud, and click *Next*.



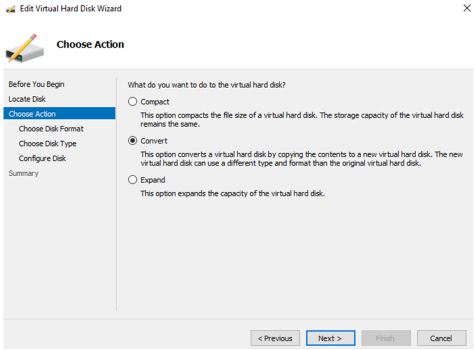
Where is the virtual hard disk file located?

Location: C:\Users\robert\Desktop\FPA_HY-v100.out.hyperv\Virtual Hard Disks\fortip

⚠ Editing the following types of virtual hard disks might result in data loss:

- Virtual hard disks in a differencing disk chain that have child virtual hard disks associated with them.
- Virtual hard disks (.avhd/.avhdx) associated with virtual machine checkpoints.
- Virtual hard disks associated with a virtual machine that has replication enabled and is currently involved in initial replication, resynchronization, test failover, or failover.

d. In *Choose Action*, select *Convert*, and click *Next*.



What do you want to do to the virtual hard disk?

○ Compact

This option compacts the file size of a virtual hard disk. The storage capacity of the virtual hard disk remains the same.

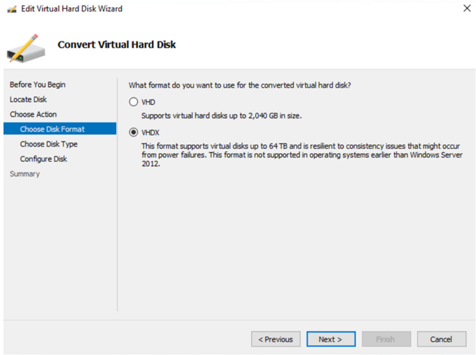
● Convert

This option converts a virtual hard disk by copying the contents to a new virtual hard disk. The new virtual hard disk can use a different type and format than the original virtual hard disk.

○ Expand

This option expands the capacity of the virtual hard disk.

e. In *Choose Action* > *Choose Disk Format*, select *VHDX*, and click *Next*.



What format do you want to use for the converted virtual hard disk?

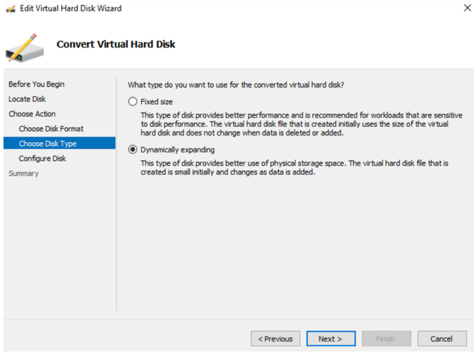
○ VHD

Supports virtual hard disks up to 2,040 GB in size.

● VHDX

This format supports virtual disks up to 64 TB and is resilient to consistency issues that might occur from power failures. This format is not supported in operating systems earlier than Windows Server 2012.

f. In *Choose Action* > *Choose Disk Type*, select *Dynamically expanding*, and click *Next*.



What type do you want to use for the converted virtual hard disk?

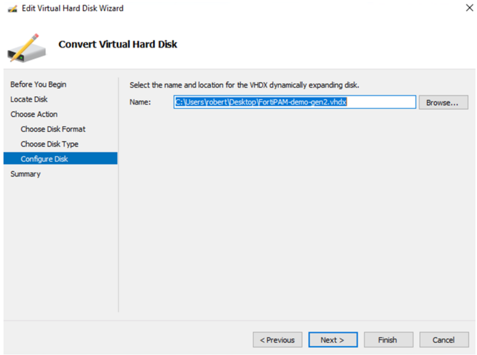
○ Fixed size

This type of disk provides better performance and is recommended for workloads that are sensitive to disk performance. The virtual hard disk file that is created initially uses the size of the virtual hard disk and does not change when data is deleted or added.

● Dynamically expanding

This type of disk provides better use of physical storage space. The virtual hard disk file that is created is small initially and changes as data is added.

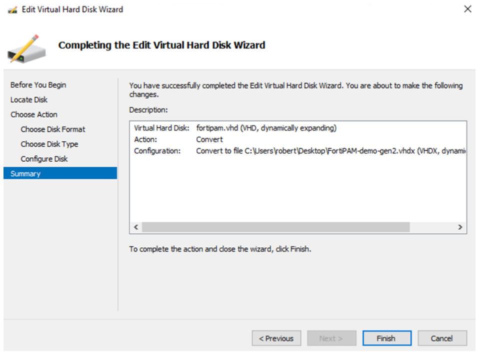
g. In *Choose Action* > *Configure Disk*, enter a name for the VHDX disk, click *Browse* to configure a location for this disk, and click *Next*.



Select the name and location for the VHDX dynamically expanding disk.

Name: C:\Users\robert\Desktop\FortiPAM-demo-gen2.vhdx

h. In *Completing the Edit Virtual Hard Disk Wizard*, the summary is displayed.



You have successfully completed the Edit Virtual Hard Disk Wizard. You are about to make the following changes.

Description:

```
Virtual Hard Disk:  fortipam.vhd (VHD, dynamically expanding)
Action:             Convert
Configuration:      Convert to file C:\Users\robert\Desktop\FortiPAM-demo-gen2.vhdx (VHDX, dynami
```

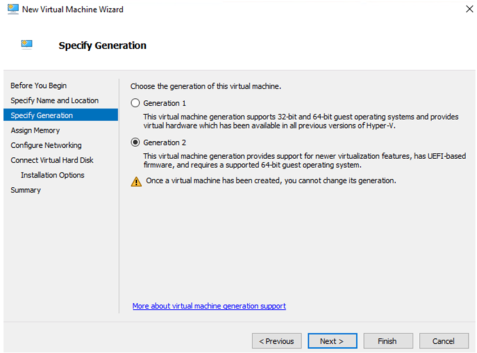
To complete the action and close the wizard, click Finish.

i. Click *Finish*.

j. Repeat steps *a* to *i* to convert `DATADRIVE1.vhd` and `DATADRIVE2.vhd`.

2. **Creating a 2nd generation Hyper-V VM**:
   Follow the same procedure as detailed in Deploying FortiPAM-VM on Hyper-V without TPM, except:

a. In Step 6, select *Generation 2*.



Specify Generation

Choose the generation of this virtual machine.

○ Generation 1

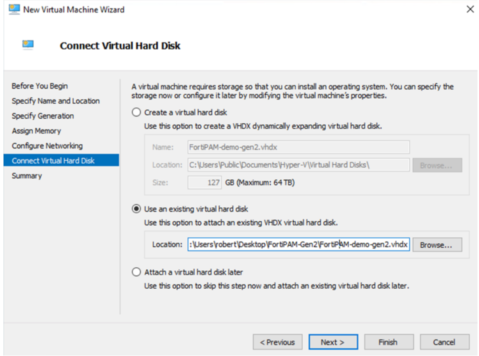
This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.

● Generation 2

This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.

⚠ Once a virtual machine has been created, you cannot change its generation.

b. In Step 9, click *Browse* and locate the `*.vhdx` file that you converted from `fortipam.vhd`.



Connect Virtual Hard Disk

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

○ Create a virtual hard disk

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name: FortiPAM-demo-gen2.vhdx

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

Size: 127 GB (Maximum: 64 TB)

● Use an existing virtual hard disk

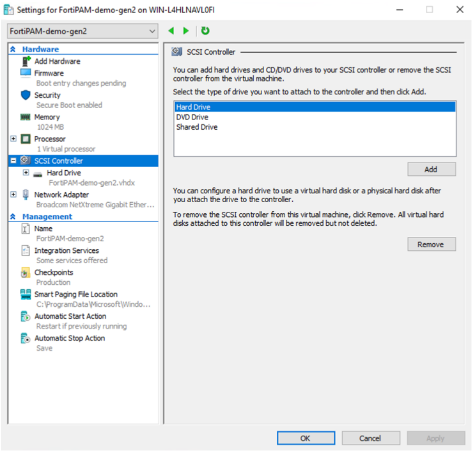
Use this option to attach an existing VHDX virtual hard disk.

Location: :\Users\robert\Desktop\FortiPAM-Gen2\FortiPAM-demo-gen2.vhdx

○ Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

c. In step 14 (a, b, and c), click *SCSI Controller*, select *Hard Drive*, and click *Add*.



SCSI Controller

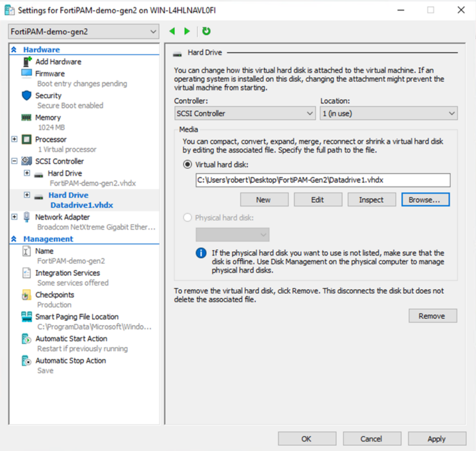
You can add hard drives and CD/DVD drives to your SCSI controller or remove the SCSI controller from the virtual machine.

Select the type of drive you want to attach to the controller and then click Add.

You can configure a hard drive to use a virtual hard disk or a physical hard disk after you attach the drive to the controller.

To remove the SCSI controller from this virtual machine, click Remove. All virtual hard disks attached to this controller will be removed but not deleted.

d. In step 14 d, in *Hard Drive*, click *Browse* and locate the `*.vhdx` file for `DATADRIVE1.vhd` that you earlier converted in Converting hard disk to *.vhdx.



Settings for FortiPAM-demo-gen2 on WIN-L4HLNAVL0FI

FortiPAM-demo-gen2

Hardware
- Add Hardware
- Firmware: Boot entry changes pending
- Security: Secure Boot enabled
- Memory: 1024 MB
- Processor: 1 Virtual processor
- SCSI Controller
  - Hard Drive: FortiPAM-demo-gen2.vhdx
  - Hard Drive: Datadrive1.vhdx
- Network Adapter: Broadcom NetXtreme Gigabit Ether...

Management
- Name: FortiPAM-demo-gen2
- Integration Services: Some services offered
- Checkpoints: Production
- Smart Paging File Location: C:\ProgramData\Microsoft\Windo...
- Automatic Start Action: Restart if previously running
- Automatic Stop Action: Save

Hard Drive

You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.

Controller: SCSI Controller

Location: 1 (in use)

Media

You can compact, convert, expand, merge, reconnect or shrink a virtual hard disk by editing the associated file. Specify the full path to the file.

● Virtual hard disk:

C:\Users\robert\Desktop\FortiPAM-Gen2\Datadrive1.vhdx

New | Edit | Inspect | Browse...

○ Physical hard disk:

If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.

To remove the virtual hard disk, click Remove. This disconnects the disk but does not delete the associated file.

Remove

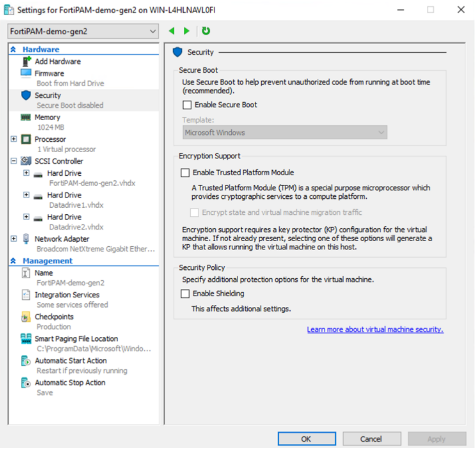
OK | Cancel | Apply

e. Repeat steps *c* and *d* to add `*.vhdx` file for `DATADRIVE2.vhd`.

Secure boot must be disabled before starting the VM.

To disable secure boot:

1. From the virtual machines list, right-click the VM and select *Settings*. Optionally, having select the VM, select *Action* and then select *Settings*.
2. Go to *Security* and uncheck *Enable Secure Boot*.
3. Click *Apply*.



Settings for FortiPAM-demo-gen2 on WIN-L4HLNAVL0FI

FortiPAM-demo-gen2

Hardware
- Add Hardware
- Firmware: Boot from Hard Drive
- Security: Secure Boot disabled
- Memory: 1024 MB
- Processor: 1 Virtual processor
- SCSI Controller
  - Hard Drive: FortiPAM-demo-gen2.vhdx
  - Hard Drive: Datadrive1.vhdx
  - Hard Drive: Datadrive2.vhdx
- Network Adapter: Broadcom NetXtreme Gigabit Ether...

Management
- Name: FortiPAM-demo-gen2
- Integration Services: Some services offered
- Checkpoints: Production
- Smart Paging File Location: C:\ProgramData\Microsoft\Windo...
- Automatic Start Action: Restart if previously running
- Automatic Stop Action: Save

Security

Secure Boot

Use Secure Boot to help prevent unauthorized code from running at boot time (recommended).

□ Enable Secure Boot

Template: Microsoft Windows

Encryption Support

□ Enable Trusted Platform Module

A Trusted Platform Module (TPM) is a special purpose microprocessor which provides cryptographic services to a compute platform.

□ Encrypt state and virtual machine migration traffic

Encryption support requires a key protector (KP) configuration for the virtual machine. If not already present, selecting one of these options will generate a KP that allows running the virtual machine on this host.

Security Policy

Specify additional protection options for the virtual machine.

□ Enable Shielding

This affects additional settings.

Learn more about virtual machine security.

OK | Cancel | Apply

4. Click *OK*.

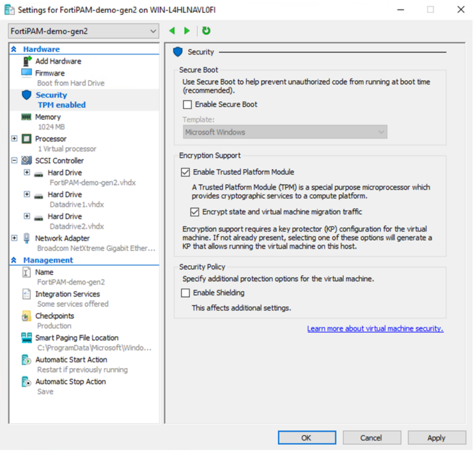
3. **Enabling TPM on Hyper-V**:

Ensure that TPM is set up as part of the initial configuration, i.e., before powering on the FortiPAM-VM for the first time.

a. From the virtual machines list, right-click the VM and select *Settings*. Optionally, having select the VM, select *Action* and then select *Settings*.

b. Go to Security and check *Enable Trusted Platform Module*. Optionally, enable *Encrypt state and virtual machine migration traffic*.

c. Click *Apply*.



Security

Secure Boot

Use Secure Boot to help prevent unauthorized code from running at boot time (recommended).

□ Enable Secure Boot

Template: Microsoft Windows

Encryption Support

☑ Enable Trusted Platform Module

A Trusted Platform Module (TPM) is a special purpose microprocessor which provides cryptographic services to a compute platform.

☑ Encrypt state and virtual machine migration traffic

Encryption support requires a key protector (KP) configuration for the virtual machine. If not already present, selecting one of these options will generate a KP that allows running the virtual machine on this host.

Security Policy

Specify additional protection options for the virtual machine.

□ Enable Shielding

This affects additional settings.

Learn more about virtual machine security.

d. Click *OK*.

You can now power on your VM.

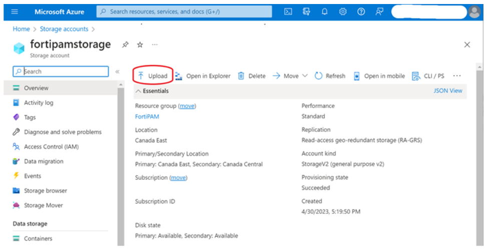
Appendix G: Installation on Azure

If deploying FortiPAM from the Marketplace, skip to Creating the FortiPAM-VM on page 477.

Uploading the VHD file to an Azure storage account

To upload the VHD file to an Azure storage account:

1. Unzip the `FPA_AZURE-v100-buildXXXX-FORTINET.out.hyperv.zip` file and store the `fortipam.vhd` file on your management computer.
2. Go to your storage account on the Microsoft Azure Portal and click *Upload*.



Resource group (move)
FortiPAM

Location
Canada East

Primary/Secondary Location
Primary: Canada East, Secondary: Canada Central

Subscription (move)

Subscription ID

Disk state
Primary: Available, Secondary: Available

Performance
Standard

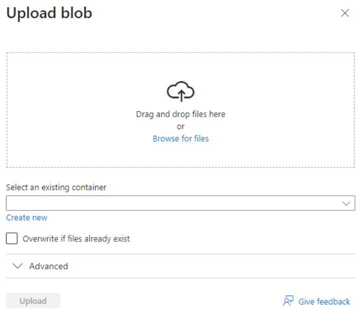
Replication
Read-access geo-redundant storage (RA-GRS)

Account kind
StorageV2 (general purpose v2)

Provisioning state
Succeeded

Created
4/30/2023, 5:19:50 PM

The *Upload blob* window opens.

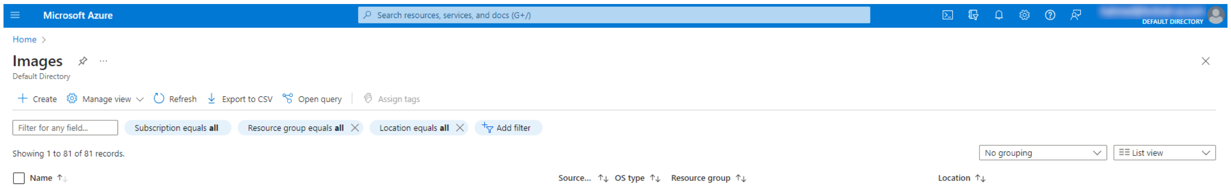


3. Select *Browse for files* and locate the `fortipam.vhd` file that you downloaded and unzipped in step 1.
4. Click *Upload*.

Creating an image on Azure Images

To create an image:

1. Go to *Images* on the Azure Portal and select *Create*.

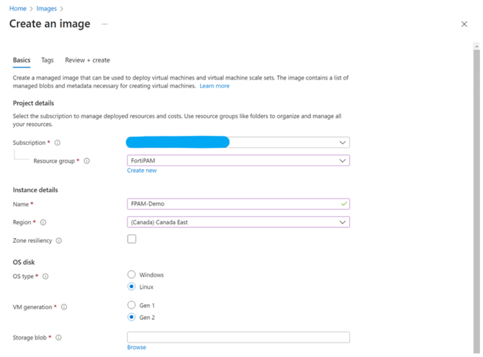


Showing 1 to 81 of 81 records.

The *Create an image* wizard opens.

2. From the *Resource group* dropdown, select a resource group.
3. In *Name*, enter the name for the image.
4. In the *Region* dropdown, select a region.
5. In *OS type*, select *Linux*.
6. In *VM generation*, you can select *Gen 1* or *Gen 2*.

> *Gen 1* VMs use BIOS-based architecture, whereas *Gen 2* VMs use the new UEFI-based boot architecture.



Create a managed image that can be used to deploy virtual machines and virtual machine scale sets. The image contains a list of managed blobs and metadata necessary for creating virtual machines. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ [redacted]

Resource group * ⓘ FortiPAM

Create new

Instance details

Name * FPAM-Demo ✓

Region * ⓘ (Canada) Canada East

Zone resiliency ⓘ □

OS disk

OS type * ⓘ ○ Windows ● Linux

VM generation * ⓘ ○ Gen 1 ● Gen 2

Storage blob * ⓘ

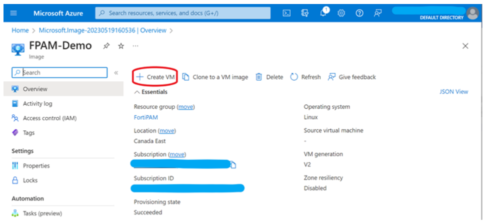
Browse

7. In the *Storage blob*, click *Browse*, locate the `fortipam.vhd` file that you uploaded to your storage account in Uploading the VHD file to an Azure storage account on page 476, and click *Next : Tags*.
8. Optionally, in *Tags*, enter tags, and click *Next : Review + Create*.
9. Review your settings and then click *Create*.
   Note: The deployment may take several minutes to finish.

Creating the FortiPAM-VM

To create the FortiPAM-VM:

1. On the Azure Portal, open the image you created in Creating an image on Azure Images on page 476, and click *Create VM*.



Resource group (move) FortiPAM

Location (move) Canada East

Subscription (move) [redacted]

Subscription ID [redacted]

Provisioning state Succeeded

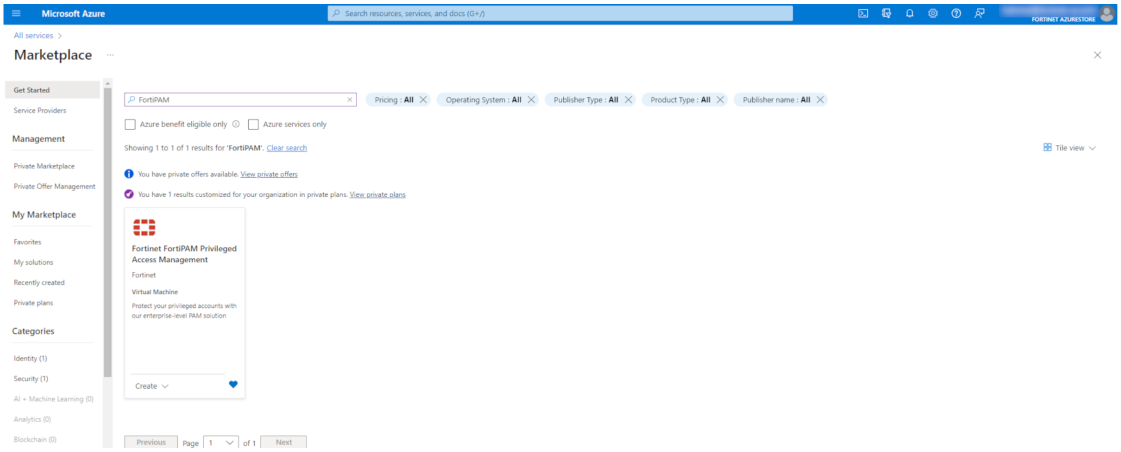
Operating system Linux

Source virtual machine -

VM generation V2

Zone resiliency Disabled

Alternatively, go to the *Marketplace* on the Azure Portal and look for FortiPAM.



Microsoft Azure

Search resources, services, and docs (G+/)

[redacted] FORTINET AZURESTORE

All services >

Marketplace ···

Get Started

Service Providers

Management

Private Marketplace

Private Offer Management

My Marketplace

Favorites

My solutions

Recently created

Private plans

Categories

Identity (1)

Security (1)

AI + Machine Learning (0)

Analytics (0)

Blockchain (0)

FortiPAM

Pricing : **All** | Operating System : **All** | Publisher Type : **All** | Product Type : **All** | Publisher name : **All**

□ Azure benefit eligible only □ Azure services only

Showing 1 to 1 of 1 results for '**FortiPAM**'. Clear search

Tile view

You have private offers available. View private offers

You have 1 results customized for your organization in private plans. View private plans

Fortinet FortiPAM Privileged Access Management

Fortinet

Virtual Machine

Protect your privileged accounts with our enterprise-level PAM solution

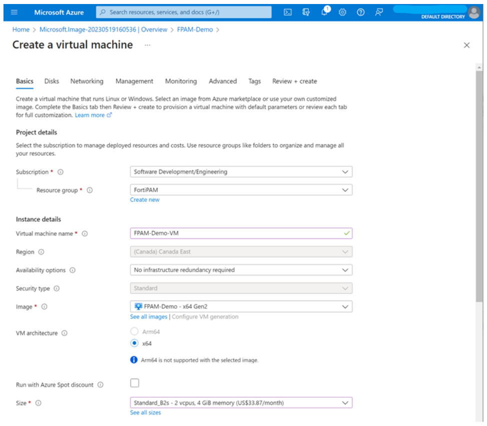
Create

Previous Page 1 of 1 Next

Click on the *Fortinet FortiPAM Privileged Access Management* card and select *Create*.

The *Create a virtual machine* wizard opens.

2. In *Virtual machine name*, enter a name for the VM being created.
3. In the *Region* dropdown, select a region if the region is not automatically selected.
4. In the *Image* dropdown, select the image created in Creating an image on Azure Images on page 476 if the image is not automatically selected.
5. In the *Size* dropdown, select a size that supports the workload you intend to perform.
   The following shows a screenshot when FortiPAM is deployed using the image you created in Creating an image on Azure Images on page 476.



Microsoft Azure

Search resources, services, and docs (G+/)

[redacted] DEFAULT DIRECTORY

Home > Microsoft.Image-20230519160536 | Overview > FPAM-Demo >

Create a virtual machine ···

Basics | Disks | Networking | Management | Monitoring | Advanced | Tags | Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Software Development/Engineering

Resource group * : FortiPAM

Create new

Instance details

Virtual machine name * : FPAM-Demo-VM

Region : (Canada) Canada East

Availability options : No infrastructure redundancy required

Security type : Standard

Image * : FPAM-Demo - x64 Gen2

See all images | Configure VM generation

VM architecture : ○ Arm64 ● x64

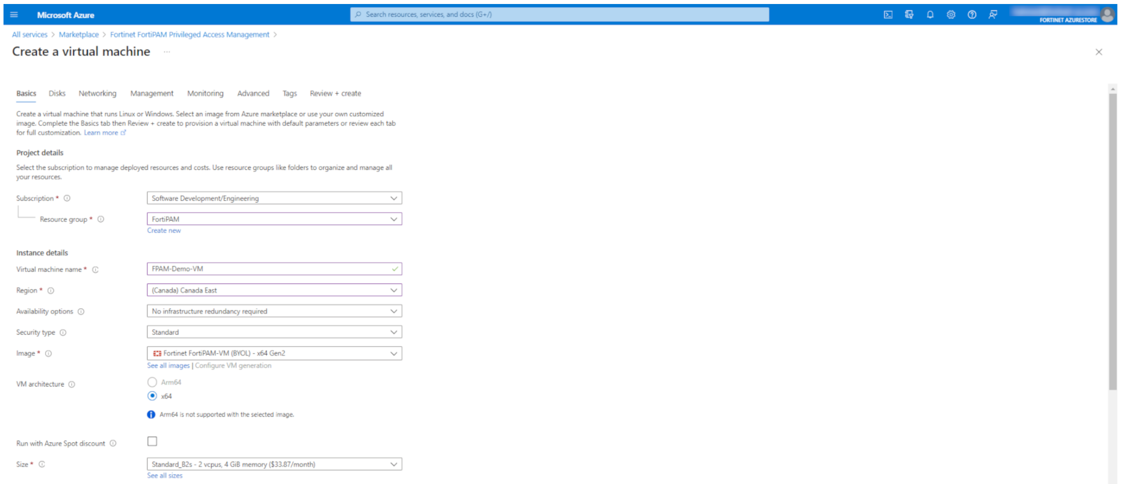
Arm64 is not supported with the selected image.

Run with Azure Spot discount : □

Size * : Standard_B2s - 2 vcpus, 4 GiB memory (US$33.87/month)

See all sizes

The following shows a screenshot when FortiPAM is deployed from the *Marketplace*.


Microsoft Azure
Search resources, services, and docs (G+/)
FORTINET AZURESTORE
All services > Marketplace > Fortinet FortiPAM Privileged Access Management >
Basics
Disks
Networking
Management
Monitoring
Advanced
Tags
Review + create

Create a virtual machine

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. Learn more

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Software Development/Engineering

Resource group * : FortiPAM

Create new

Instance details

Virtual machine name * : FPAM-Demo-VM ✓

Region * : (Canada) Canada East

Availability options : No infrastructure redundancy required

Security type : Standard

Image * : Fortinet FortiPAM-VM (BYOL) - x64 Gen2

See all images | Configure VM generation

VM architecture : ○ Arm64 ● x64

Arm64 is not supported with the selected image.

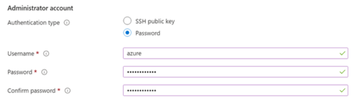
Run with Azure Spot discount : □

Size * : Standard_B2s - 2 vcpus, 4 GiB memory ($33.87/month)

See all sizes

6. In the *Administrator account* pane:
   a. In *Authentication type*, select *Password*.
   b. In *Username*, enter a username.
   c. In *Password*, enter the password.
   d. In *Confirm password*, enter the password again to confirm.

The account is created with the *Super Administrator* role on FortiPAM.



Administrator account

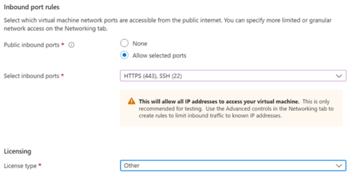
Authentication type : ○ SSH public key ● Password

Username * : azure ✓

Password * : ••••••••••••• ✓

Confirm password * : ••••••••••••• ✓

7. In the *Inbound port rules* pane:
   a. In *Public inbound ports*, select *Allow selected ports*.
   b. In the *Select inbound ports* dropdown, select *HTTPS (443), SSH (22)*.
8. In the *License Type* dropdown, select *Other*, and click *Next*.



Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * : ○ None ● Allow selected ports

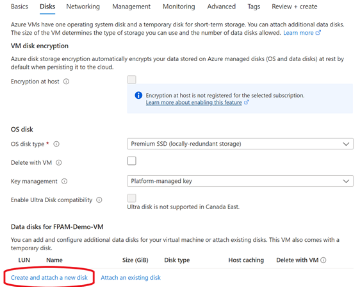
Select inbound ports * : HTTPS (443), SSH (22)

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Licensing

License type * : Other

9. In *Data disks for FPAM-demo-VM*, select *Create and attach a new disk*.



Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. Learn more

VM disk encryption

Azure disk storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud.

Encryption at host : □

Encryption at host is not registered for the selected subscription.
Learn more about enabling this feature

OS disk

OS disk type * : Premium SSD (locally-redundant storage)

Delete with VM : □

Key management : Platform-managed key

Enable Ultra Disk compatibility : □

Ultra disk is not supported in Canada East.

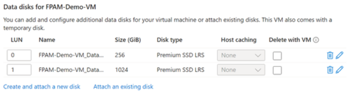
Data disks for FPAM-Demo-VM

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM

Create and attach a new disk   Attach an existing disk

10. Create a disk for the log and another for the video, and click *Next*.

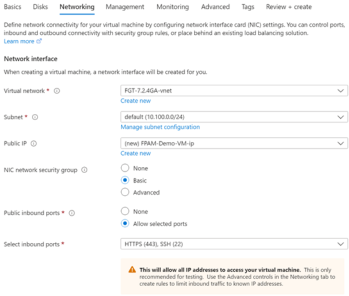


Data disks for FPAM-Demo-VM

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching	Delete with VM
0	FPAM-Demo-VM_Data...	256	Premium SSD LRS	None	□
1	FPAM-Demo-VM_Data...	1024	Premium SSD LRS	None	□

11. In the *Networking* tab:
    a. In the *Virtual network* dropdown, select a virtual network.
    b. In the *Subnet* dropdown, select a subnet.
    c. In the *Public IP* dropdown, select a public IP address or create a new public IP address.
    d. In *NIC network security group*, select *Basic*.
    e. In *Public inbound ports*, select *Allow selected ports*.
    f. In the *Select inbound ports* dropdown, select *HTTPS (443), SSH (22)*, and click *Next*.



Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution.
Learn more

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network * : FGT-7.2.4GA-vnet
Create new

Subnet * : default (10.100.0.0/24)
Manage subnet configuration

Public IP : (new) FPAM-Demo-VM-ip
Create new

NIC network security group: ○ None ● Basic ○ Advanced

Public inbound ports * : ○ None ● Allow selected ports

Select inbound ports * : HTTPS (443), SSH (22)

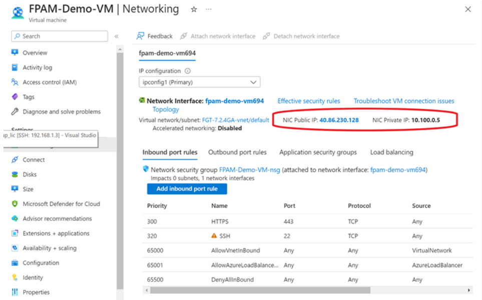
This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

12. Click *Next* and navigate through the remaining tabs.
13. Finally, review your settings and then click *Create*.

    Note: The VM deployment may take several minutes to finish.

Initial configuration

1. On the FortiPAM-VM *Networking* page, copy and save the network interface's private and public IP addresses.



IP configuration: ipconfig1 (Primary)

Network Interface: fpam-demo-vm694 Effective security rules Troubleshoot VM connection issues Topology
Virtual network/subnet: FGT-7.2.4GA-vnet/default NIC Public IP: 40.86.230.128 NIC Private IP: 10.100.0.5
Accelerated networking: Disabled

Network security group FPAM-Demo-VM-nsg (attached to network interface: fpam-demo-vm694)
Impacts 0 subnets, 1 network interfaces

Priority	Name	Port	Protocol	Source
300	HTTPS	443	TCP	Any
320	SSH	22	TCP	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork
65001	AllowAzureLoadBalance...	Any	Any	AzureLoadBalancer
65500	DenyAllInBound	Any	Any	Any

2. In the VM serial console, log in as the default super admin set up in step 6 of Creating the FortiPAM-VM on page 477.
3. Using the following CLI commands, configure `port1`:

   You can skip this step if FortiPAM is in standalone mode.

```
config system interface
   edit port1
      set mode static #by default, set as dhcp
```

```
        set ip 10.100.0.5/24 #set to the private IP address assigned by Azure in step 1
    next
end
Enable PAM Service on port1 with IP 10.100.0.5
```

When upgrading a FortiPAM instance, use the following CLI command to enable synchronizing the virtual IP address to the IP address of the external interface:

```
Example

 config firewall vip
  set intf-ip-sync enable
  set extintf "port1" #The interface connected to the source network
that receives the packets forwarded to the destination network.
 end
```

When installing a new FortiPAM instance, the synchronization happens automatically.

4. Using the following CLI commands, configure a static route if the interface is configured as static mode:

```
config router static
    edit 1
        set gateway 10.100.0.1
        set device port1
    next
end
```

5. Optionally, to encrypt disk to protect logs and videos, see Configuring log and video disk encryption on page 347.
6. On a web browser, go to `https://<Public IP>` to access the FortiPAM-VM GUI.
   Note: The public IP address was saved in step 1.
7. Log in with the super admin username and password as set up in step 6 of Creating the FortiPAM-VM on page 477.
   The *FortiPAM VM license* window appears immediately after you log in.
8. In the *Upload License File* pane, select *Upload* and browse to the license file on your management computer.
9. Click *OK*.
   After the boot up, the license status changes to valid.

   You can now use your FortiPAM-VM deployed on Azure.

Evaluation license is not available on Azure.

Appendix H: FortiPAM hardware RAID CLI commands

The FortiPAM hardware devices 1000G and 3000G are equipped with a hardware RAID card. All the hard disks are configured in the RAID-10 group.

For the FortiPAM hardware devices, in the CLI console, check the RAID status by entering the following command:

```
diagnose system raid status
   Storcli RAID:
   RAID Level: Raid-10
   RAID Status: OK
   RAID Size: 5587GB
   Groups: 3
   Disk 0: OK 1862GB Group-1
   Disk 1: OK 1862GB Group-1
   Disk 2: OK 1862GB Group-2
   Disk 3: OK 1862GB Group-2
   Disk 4: OK 1862GB Group-3
   Disk 5: OK 1862GB Group-3
   Disk 6: Unavailable 0GB
   Disk 7: Unavailable 0GB
   Disk 8: Unavailable 0GB
   Disk 9: Unavailable 0GB
   Disk 10: Unavailable 0GB
   Disk 11: Unavailable 0GB
   Disk 12: Unavailable 0GB
   Disk 13: Unavailable 0GB
   Disk 14: Unavailable 0GB
   Disk 15: Unavailable 0GB
   .
   .
   .
```

For the FortiPAM hardware devices, in the CLI console, check the disk status by entering the following command:

```
diagnose system disk health
   Disk 0: SMART Health Status: OK
   Disk 1: SMART Health Status: OK
   Disk 2: SMART Health Status: OK
   Disk 3: SMART Health Status: OK
   Disk 4: SMART Health Status: OK
   Disk 5: SMART Health Status: OK
   Disk 6: Unavailable
   Disk 7: Unavailable
   Disk 8: Unavailable
   Disk 9: Unavailable
   Disk 10: Unavailable
   Disk 11: Unavailable
   Disk 12: Unavailable
   Disk 13: Unavailable
   Disk 14: Unavailable
   Disk 15: Unavailable
   .
   .
```

```
      .
```

For the FortiPAM hardware devices, in the CLI console, check the disk information by entering the following command:

```
diagnose system disk info
   Disk 0:
   Vendor: SEAGATE
   Product: ST2000NM001B
   Revision: N001
   Compliance: SPC-5
   User Capacity: 2,000,398,934,016 bytes [2.00 TB]
   Logical block size: 512 bytes
   LU is fully provisioned
   Rotation Rate: 7200 rpm
   Form Factor: 3.5 inches
   Logical Unit id: 0x5000c500d9c75b8b
   Serial number: WRE06YSQ0000C246A3JM
   Device type: disk
   Transport protocol: SAS (SPL-3)
   Local Time is: Thu Apr 13 12:12:44 2023 GMT
   SMART support is: Available - device has SMART capability.
   SMART support is: Enabled
   Temperature Warning: Enabled
   .
   .
   .
```

Creating a RAID-10 disk group on hardware FortiPAM

By default, FortiPAM 1000G and 3000G are configured in RAID-10.

You can recreate RAID-10 using the CLI.

Since all the data on the disks are wiped off. You must perform a backup before using this CLI command.

Use the following CLI command to create a RAID-10 disk group:

```
execute raid create-and-format
   This operation will create RAID disk and format it to ext4 file system.
   All existing data will be lost!
   Do you want to continue? (y/n)
```

Hot swapping failed disks on FortiPAM 1000G/3000G

The following procedure was drawn from a simulated case of a failed disk. The procedure that applies to your use case may be different.

1. Unplug the disk.
2. Run the `diagnose system raid status` CLI command.
   The disk status turns *Unavailable*.
3. Plug the disk back.
   The disk status turns *Failed*.
4. Run the `execute raid delete \[disk-index\]` CLI command.
   After a while, the disk status turns *Unused*.
5. Unplug the disk.
6. After a while, plug the disk again.
7. The disk status turns *Rebuilding*.
8. Keep FortiPAM 1000G/3000G running.
   After 10 hours, the disk status turns *OK*.

   RAID is recovered.

Appendix I: Default launchers parameters

The following tables list the default secret launcher executables, parameters, and initial and clean commands.

PuTTY

Executable	Parameter	Initial Commands	Clean Commands
`putty.exe`	`$USER@$HOST -pw $PASSWORD -P $PORT`		

SecureCRT

Executable	Parameter	Initial Commands	Clean Commands
`secureCRT.exe`	`/ssh2 $USER@$HOST /PASSWORD $PASSWORD /P $PORT /AUTH password,keyboard-interactive,publickey` (username and password parameter)		

Remote Desktop-Windows

Executable	Parameter	Initial Commands	Clean Commands

`mstsc.exe`	`/V:$TARGET:$PORT /noConsentPrompt`	When the domain is used:
		`cmdkey /generic:$TARGET /user:$DOMAIN\$USER /pass:"$PASSWORD"`
		When the domain is not used:
		`cmdkey /generic:$TARGET /user:$USER /pass:"$PASSWORD"`
			`cmdkey /del:$TARGET`

WinSCP

Executable	Parameter	Initial Commands	Clean Commands
`winscp.exe`	`scp://$USER:$PASSWORD@$HOST:$PORT /newinstance`		

TightVNC

Executable	Parameter	Initial Commands	Clean Commands
`tvnviewer.exe`	`$HOST::$PORT -PASSWORD=$PASSWORD`		

VNC Viewer

Executable	Parameter	Initial Commands	Clean Commands
`vncviewer.exe`	Proxy mode: `$HOST::$PORT` Non-proxy mode: `–config $TMPFILE`	Non-proxy init-commands: **1.** `echo [connection] > $TMPFILE` **2.** `echo host=$HOST >> $TMPFILE` **3.** `echo port=$PORT >> $TMPFILE` **4.** `echo password=$VNCPASSWORD >> $TMPFILE` **5.** `echo username=$USER >> $TMPFILE`	Non-proxy clean commands: `cmdkey /del:$TARGET`

SSH CLI

Executable	Parameter	Initial Commands	Clean Commands
`ssh.exe`	`$USER@$HOST -p $PORT`		

Microsoft SQL CLI

Executable	Parameter	Initial Commands	Clean Commands
`sqlcmd.exe`	`-S $HOST,$PORT -U $USER -P $PASSWORD -y 30 -Y 30`		

MySQL CLI

Executable	Parameter	Initial Commands	Clean Commands
`mysql.exe`	`-u $USER -h $HOST -P $PORT -p$PASSWORD`		

MySQL Shell

Executable	Parameter	Initial Commands	Clean Commands
`mysqlsh.exe`	`--mysql --sql --result-format=json/pretty -u $USER -h $HOST -P $PORT -p$PASSWORD`		

PostgreSQL CLI

Executable	Parameter	Initial Commands	Clean Commands
`psql.exe`	`"host=$HOST port=$PORT dbname=postgres user=$USER password=$PASSWORD"`		

SSMS

Executable	Parameter	Initial Commands	Clean Commands
`ssms.exe`	`-S $HOST, $PORT -U $USER`	`cmdkey /generic:Microsoft:SSMS:19:$HOST, $PORT:$USER:8c91a03d-f9b4-46c0-a305-b5dcc79ff907:1 /user:$USER /pass:"$PASSWORD"` See Powershell script on page 488	`cmdkey /delete:Microsoft:SSMS:19:$HOST, $PORT:$USER:8c91a03d-f9b4-46c0-a305-b5dcc79ff907:1`

HeidiSQL

Executable	Parameter	Initial Commands	Clean Commands
`heidisql.exe`	1. `mssql: --nettype 4 -u "$USER" -p "$PASSWORD" -h $HOST --library MSOLEDBSQL -P`		

Executable	Parameter	Initial Commands	Clean Commands
	`$PORT` **2.** `nettype 0 -u "$USER" -p "$PASSWORD" -h $HOST --library libmariadb.dll -P $PORT` **3.** `--nettype 8 -u "$USER" -p "$PASSWORD" -h $HOST --library libpq-12.dll -P $PORT`		

MobaXterm

Executable	Parameter	Initial Commands	Clean Commands
`mobaxterm.exe`	`-newtab \"ssh $USER@$HOST -p $PORT\"`		

Xshell

Executable	Parameter	Initial Commands	Clean Commands
`Xshell.exe`	`-newwin ssh://$USER@$HOST:$PORT`		

Powershell script

```
powershell
$xmlChildName = @"
<?xml version="1.0"?>
<SqlStudio>
<ServerTypes>
<Element>
<Key>
<guid>8c91a03d-f9b4-46c0-a305-b5dcc79ff907</guid>
</Key>
<Value>
<ServerTypeItem>
<Servers>
<Element>
<Time>
<long>-638197664443740231</long>
</Time>
<Item>
<ServerConnectionItem>
<Instance>$HOST,$PORT</Instance>
```

```
<AuthenticationMethod>1</AuthenticationMethod>
<Connections>
<Element>
<Time>
<long>-638197664443691066</long>
</Time>
<Item>
<ServerConnectionSettings>
<Password/>
<Instance>$HOST,$PORT</Instance>
<UserName>$USER</UserName>
<ServerType>8c91a03d-f9b4-46c0-a305-b5dcc79ff907</ServerType>
<AuthenticationMethod>1</AuthenticationMethod>
<Database/>
<Advanced>
<Element>
<Key>
<string>IniDb</string>
</Key>
<Value/>
</Element>
<Element>
<Key>
<string>CT</string>
</Key>
<Value>
<string>30</string>
</Value>
</Element>
<Element>
<Key>
<string>ET</string>
</Key>
<Value>
<string>0</string>
</Value>
</Element>
<Element>
<Key>
<string>PSize</string>
</Key>
<Value>
<string>4096</string>
</Value>
</Element>
<Element>
<Key>
<string>EC</string>
</Key>
<Value>
<string>False</string>
</Value>
</Element>
<Element>
<Key>
<string>UCCC</string>
</Key>
```

```
<Value>
<string>False</string>
</Value>
</Element>
<Element>
<Key>
<string>CCC</string>
</Key>
<Value>
<string>-986896</string>
</Value>
</Element>
<Element>
<Key>
<string>TSC</string>
</Key>
<Value>
<string>False</string>
</Value>
</Element>
<Element>
<Key>
<string>UCTI</string>
</Key>
<Value>
<string>False</string>
</Value>
</Element>
<Element>
<Key>
<string>CTI</string>
</Key>
<Value>
<string/>
</Value>
</Element>
<Element>
<Key>
<string>CES</string>
</Key>
<Value/>
</Element>
<Element>
<Key>
<string>CESEnclave</string>
</Key>
<Value/>
</Element>
<Element>
<Key>
<string>CESProtocol</string>
</Key>
<Value/>
</Element>
<Element>
<Key>
<string>CESUrl</string>
```

```
</Key>
<Value/>
</Element>
<Element>
<Key>
<string>Prot</string>
</Key>
<Value/>
</Element>
</Advanced>
<OtherParams/>
</ServerConnectionSettings>
</Item>
</Element>
</Connections>
</ServerConnectionItem>
</Item>
</Element>
</Servers>
</ServerTypeItem>
</Value>
</Element>
</ServerTypes>
</SqlStudio>
"@
$xmlFileName =
     "C:\\Windows\\SysWOW64\\config\\systemprofile\\AppData\\Roaming\\Microsoft\\SQL
     Server Management Studio\\19.0\\UserSettings.xml"
if (-Not (Test-Path $xmlFileName)) {Copy "C:\\Users\\$LOCAL_
     USER\\AppData\\Roaming\\Microsoft\\SQL Server Management
     Studio\\19.0\\UserSettings.xml" $xmlFileName}
[xml]$xmlDoc = New-Object system.Xml.XmlDocument
[xml]$xmlDoc = Get-Content $xmlFileName
[xml]$child = $xmlChildName
$exist = $xmlDoc.SelectNodes("//Connections[Element[Item[ServerConnectionSettings
     [Instance= '$HOST,$PORT']]]]")
if ([String]::IsNullOrEmpty($exist)) {
$node = $xmlDoc.SelectSingleNode("//Element[Key[guid= '8c91a03d-f9b4-46c0-a305-
     b5dcc79ff907']]")
$copy = $xmlDoc.ImportNode($child.get_DocumentElement(), $true)
if ([String]::IsNullOrEmpty($node)) {
$node = $xmlDoc.SelectSingleNode('//ServerTypes')
$node.ParentNode.RemoveChild($node)
$xmlDoc.SqlStudio.SSMS.ConnectionOptions.AppendChild($copy.ServerTypes)
} else {
$inner = $node.Value.ServerTypeItem.Servers
$inner.AppendChild($copy.ServerTypes.Element.Value.ServerTypeItem.Servers.Element)
}
$xmlDoc.Save($xmlFileName)}
```

Appendix J: Installation on AWS

FortiPAM installation on AWS and initial setup:

1. Converting qcow2 to a RAW format for AWS import-image tool on page 492
2. Creating an S3 bucket on AWS on page 493
3. Uploading RAW file to the AWS S3 bucket on page 494
4. Creating a snapshot from the RAW file in the AWS S3 bucket on page 494
5. Creating AMI from the snapshot on page 497
6. Configuring a security group on page 498
7. Launching the FortiPAM instance from AMI on page 500
8. Initial configuration on page 501
9. Licensing on page 503

Converting qcow2 to a RAW format for AWS import-image tool

To convert qcow2 to a RAW format for AWS import-image tool:

1. Unzip the `FPA_KVM_AWS-v100-buildxxxx-FORTINET.out.kvm.zip` file and locate the `fortipam.qcow2` file.
2. On a Linux machine, install `qemu-utils` package to get the `qemu-img` tool:

   ```
   $ sudo apt-get install qemu-utils
   ```

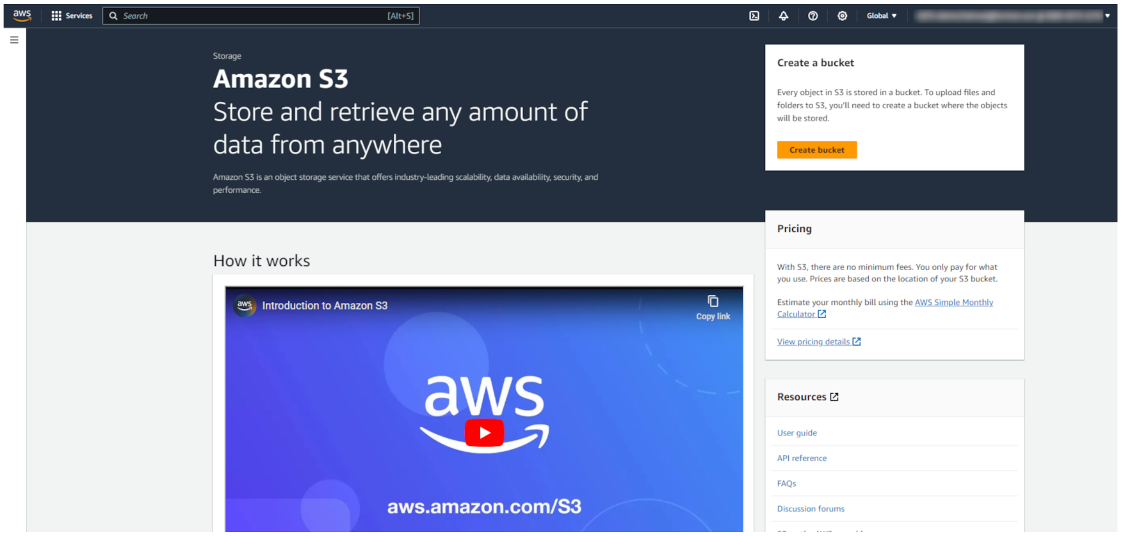
3. Use `qemu-img` to convert the image into RAW format:

   ```
   $ qemu-img convert fortipam.qcow2 fortipam.raw
   ```

Creating an S3 bucket on AWS

To create an S3 bucket on AWS:

1. Select *Services* and from the list on the left, go to *Storage* > *S3*.
2. Select *Create bucket*.



Amazon S3

Store and retrieve any amount of data from anywhere

Amazon S3 is an object storage service that offers industry-leading scalability, data availability, security, and performance.

Create a bucket

Every object in S3 is stored in a bucket. To upload files and folders to S3, you'll need to create a bucket where the objects will be stored.

Create bucket

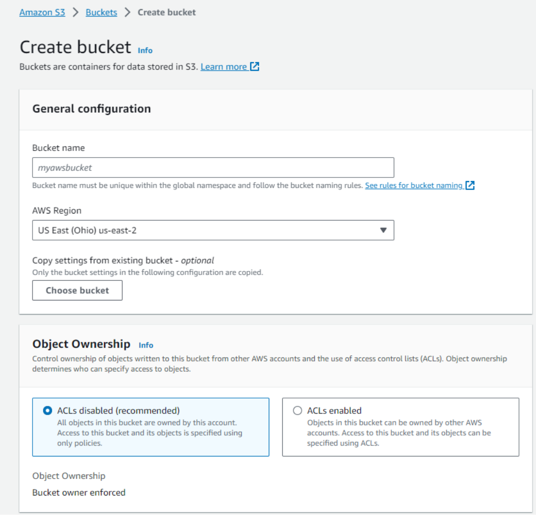
Pricing

With S3, there are no minimum fees. You only pay for what you use. Prices are based on the location of your S3 bucket.

Estimate your monthly bill using the AWS Simple Monthly Calculator

View pricing details

The *Create bucket* page opens.



Create bucket

Buckets are containers for data stored in S3. Learn more

General configuration

Bucket name: *myawsbucket*

Bucket name must be unique within the global namespace and follow the bucket naming rules. See rules for bucket naming

AWS Region: US East (Ohio) us-east-2 ▾

Copy settings from existing bucket - *optional*

Only the bucket settings in the following configuration are copied.

Object Ownership

Control ownership of objects written to this bucket from other AWS accounts and the use of access control lists (ACLs). Object ownership determines who can specify access to objects.

● ACLs disabled (recommended)
All objects in this bucket are owned by this account. Access to this bucket and its objects is specified using only policies.

○ ACLs enabled
Objects in this bucket can be owned by other AWS accounts. Access to this bucket and its objects can be specified using ACLs.

Object Ownership

Bucket owner enforced

3. In the *General* configurations pane, enter the following information:

Bucket name	The name of the bucket.
AWS Region	From the dropdown, select a region where the bucket is stored.

4. Leave all other settings on default.
5. Click *Create bucket*.

Uploading RAW file to the AWS S3 bucket

To upload RAW file to the AWS S3 bucket:

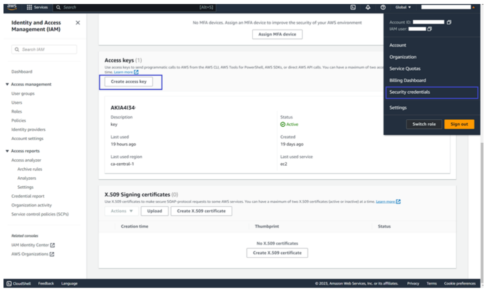
1. Using the following command, install the AWS CLI :

   ```
   $ sudo pip install awscli --ignore-installed six
   ```

2. Using the following command, add your AWS credential to `~/.aws/config`:

   ```
   [default]
   aws_access_key_id=AKIA4I34XXXXXXXX
   aws_secret_access_key=ACR8XXXXXXXXXXXXXXXXXXXXX
   region = us-west-1
   ```

   Note: Access key can be created from *Security credentials* in your IAM Account.



No MFA devices. Assign an MFA device to improve the security of your AWS environment

Use access keys to send programmatic calls to AWS from the AWS CLI, AWS Tools for PowerShell, AWS SDKs, or direct AWS API calls. You can have a maximum of two acc... time.

AKIA4I34

Description key	Status Active
Last used 19 hours ago	Created 19 days ago
Last used region ca-central-1	Last used service ec2

Use X.509 certificates to make secure SOAP-protocol requests to some AWS services. You can have a maximum of two X.509 certificates (active or inactive) at a time.

Creation time	Thumbprint	Status

No X.509 certificates

3. Using the following command, copy the RAW image to the S3 bucket:

   ```
    $ aws s3 cp fortipam.raw s3://fortipam-doc #fortipam-doc is the S3 bucket created
   earlier
   ```

Creating a snapshot from the RAW file in the AWS S3 bucket

To create a snapshot from the RAW file in the AWS S3 bucket:

1. Create the `vmimport` role:
   1. Create a JSON file `trust-policy.json` with the following content:

      ```
      $ vim trust-policy.json
      {
       "Version": "2012-10-17",
       "Statement": [
        {
         "Effect": "Allow",
         "Principal":{"Service":"vmie.amazonaws.com" },
         "Action": "sts:AssumeRole",
         "Condition": {
          "StringEquals":{
            "sts:Externalid": "vmimport"
          }
         }
        }
       ]
      }
      ```

b. Using the following AWS CLI command, create the `vmimport` role:

```
$ aws iam create-role --role-name vmimport --assume-role-policy-document
file://trust-policy.json
```

2. Assign a policy for the S3 bucket:

a. Create a JSON file `role-policy.json` with the following content:

```
$ vim role-policy.json
{
  "Version":"2012-10-17",
  "Statement":[
    {
     "Effect": "Allow",
     "Action": [
       "s3:GetBucketLocation",
       "s3:GetObject",
       "s3:ListBucket"
     ],
     "Resource": [
       "arn:aws:s3:::disk-image-file-bucket",
       "arn:aws:s3:::disk-image-file-bucket/*"
     ]
    },
    {
     "Effect": "Allow",
     "Action": [
       "s3:GetBucketLocation",
       "s3:GetObject",
       "s3:ListBucket",
       "s3:PutObject",
       "s3:GetBucketAcl"
      ],
      "Resource": [
        "arn:aws:s3:::fortipam-doc",
        "arn:aws:s3:::fortipam-doc/*"
      ]
     },
     {
      "Effect": "Allow",
      "Action": [
        "ec2:ModifySnapshotAttribute",
        "ec2:CopySnapshot",
        "ec2:RegisterImage",
        "ec2:Describe*"
        ],
        "Resource": "*"
      }
     ]
    }
```

b. Using the following AWS CLI command, assign a policy for the S3 bucket:

```
$ aws iam put-role-policy --role-name vmimport --policy-name vmimport --policy-
document file://role-policy.json
```

3. Create a JSON file `container.json` with the following content:

```
$ vim container.json
{
  "Description": "fortipam image",
  "Format": "raw",
  "UserBucket": {
    "S3Bucket": "fortipam-doc",
    "S3Key": "fortipam.raw"
   }
 }
```

4. Using the following AWS CLI command, import the FortiPAM image:

```
 $ aws ec2 import-snapshot --description "fortipam" --disk-container
file://container.json
 {
  "Description": "fortipam",
  "ImportTaskId": "import-snap-0b087779796478a51",
  "SnapshotTaskDetail": {
    "Description": "fortipam",
    "DiskImageSize": 0.0,
    "Progress": "0",
    "Status": "active",
    "StatusMessage": "pending",
    "UserBucket": {
      "S3Bucket": "fortipam-doc",
      "S3Key": "fortipam.raw"
    }
   },
   "Tags": []
  }
```

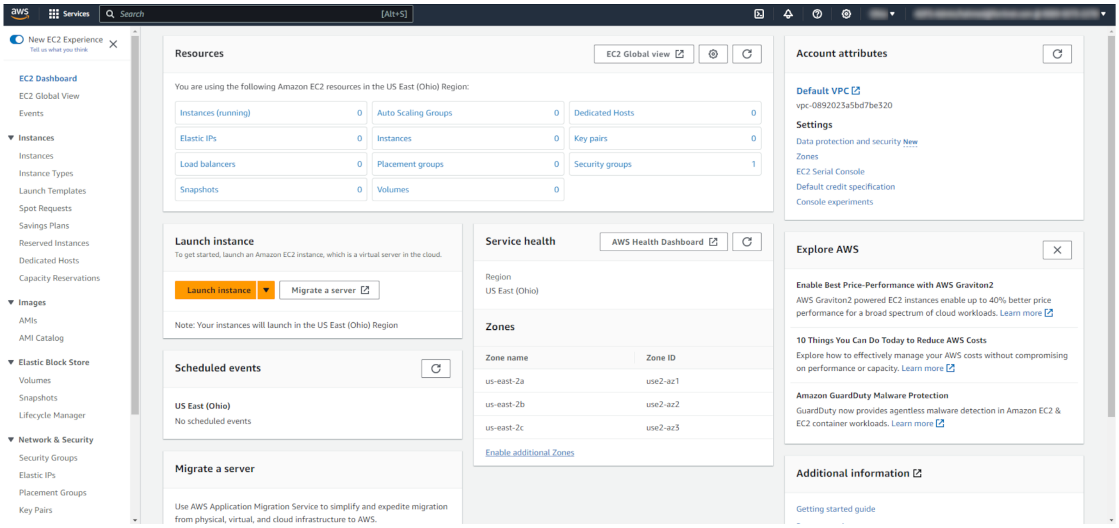
Importing the image may take some time. You can use the following AWS CLI command to monitor the progress of import:

```
$ aws ec2 describe-import-snapshot-tasks --import-task-ids import-snap-0b087779796478a51
{
 "ImportSnapshotTasks": [
   {
    "Description": "fortipam",
    "ImportTaskId": "import-snap-0b087779796478a51",
    "SnapshotTaskDetail": {
      "Description": "fortipam",
      "DiskImageSize": 2147483648.0,
      "Format": "RAW",
      "SnapshotId": "snap-0bda3d6b6d21f122c",
      "Status": "completed",
      "UserBucket": {
        "S3Bucket": "fortipam-doc",
        "S3Key": "fortipam.raw"
      }
    },
     "Tags": []
    }
   ]
  }
```

Creating AMI from the snapshot

To create AMI from snapshot:

1. In the AWS console, from the *Services* menu, go to *Compute* > *EC2*.



You are using the following Amazon EC2 resources in the US East (Ohio) Region:

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Note: Your instances will launch in the US East (Ohio) Region

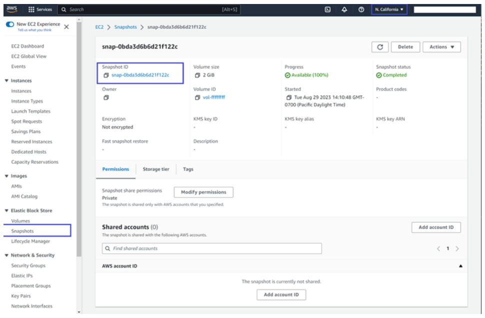
Use AWS Application Migration Service to simplify and expedite migration from physical, virtual, and cloud infrastructure to AWS.

AWS Graviton2 powered EC2 instances enable up to 40% better price performance for a broad spectrum of cloud workloads. Learn more

Explore how to effectively manage your AWS costs without compromising on performance or capacity. Learn more

GuardDuty now provides agentless malware detection in Amazon EC2 & EC2 container workloads. Learn more

2. From the menu, go to *Elastic Block Store* > *Snapshots* and look for the snapshot ID.



snap-0bda3d6b6d21f122c

Snapshot ID: snap-0bda3d6b6d21f122c

Volume size: 2 GiB

Progress: Available (100%)

Snapshot status: Completed

Owner:

Volume ID: vol-ffffffff

Started: Tue Aug 29 2023 14:10:48 GMT-0700 (Pacific Daylight Time)

Product codes: -

Encryption: Not encrypted

KMS key ID: -

KMS key alias: -

KMS key ARN: -

Fast snapshot restore: -

Description: -

Snapshot share permissions: Private

The snapshot is shared only with AWS accounts that you specified.

Shared accounts (0)

The snapshot is shared with the following AWS accounts.

The snapshot is currently not shared.

Alternatively, the `describe-import-snapshot-tasks` command used to Monitor the progress of FortiPAM image import can be used find the snapshot ID.

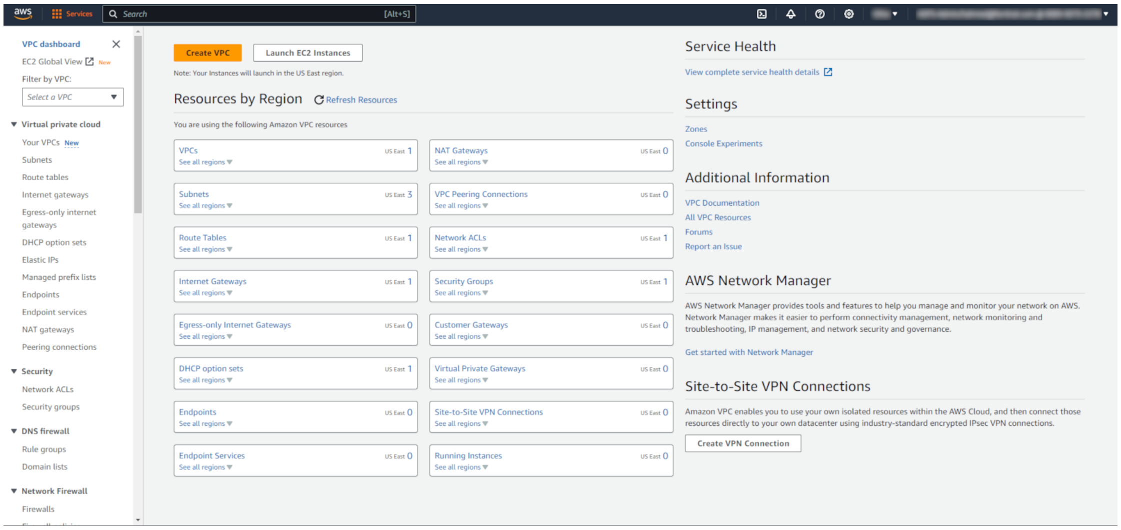
3. Using the following AWS CLI command, create a FortiPAM image:

```
$ aws ec2 register-image \
  --region us-west-1 \
  --name fortipam-uefi-tpm \
  --boot-mode uefi \
  --architecture x86_64 \
  --root-device-name /dev/sda1 \
  --block-device-mappings DeviceName=/dev/sda1,Ebs={SnapshotId= snap-0bda3d6b6d21f122c}
\
  --tpm-support v2.0 \
  --ena-support
```

Configuring a security group

To configure a security group

1. In the AWS console, search *VPC* and select VPC from the search result.
   The *VPC dashboard* opens.


Services
Search [Alt+S]
[redacted]
VPC dashboard
EC2 Global View New
Filter by VPC:
Select a VPC
Virtual private cloud
Your VPCs New
Subnets
Route tables
Internet gateways
Egress-only internet gateways
DHCP option sets
Elastic IPs
Managed prefix lists
Endpoints
Endpoint services
NAT gateways
Peering connections
Security
Network ACLs
Security groups
DNS firewall
Rule groups
Domain lists
Network Firewall
Firewalls
Create VPC
Launch EC2 Instances
Resources by Region
Refresh Resources
VPCs US East 1 See all regions
NAT Gateways US East 0 See all regions
Subnets US East 3 See all regions
VPC Peering Connections US East 0 See all regions
Route Tables US East 1 See all regions
Network ACLs US East 1 See all regions
Internet Gateways US East 1 See all regions
Security Groups US East 1 See all regions
Egress-only Internet Gateways US East 0 See all regions
Customer Gateways US East 0 See all regions
DHCP option sets US East 1 See all regions
Virtual Private Gateways US East 0 See all regions
Endpoints US East 0 See all regions
Site-to-Site VPN Connections US East 0 See all regions
Endpoint Services US East 0 See all regions
Running Instances US East 0 See all regions
Service Health
View complete service health details
Settings
Zones
Console Experiments
Additional Information
VPC Documentation
All VPC Resources
Forums
Report an Issue
AWS Network Manager
Get started with Network Manager
Site-to-Site VPN Connections
Create VPN Connection

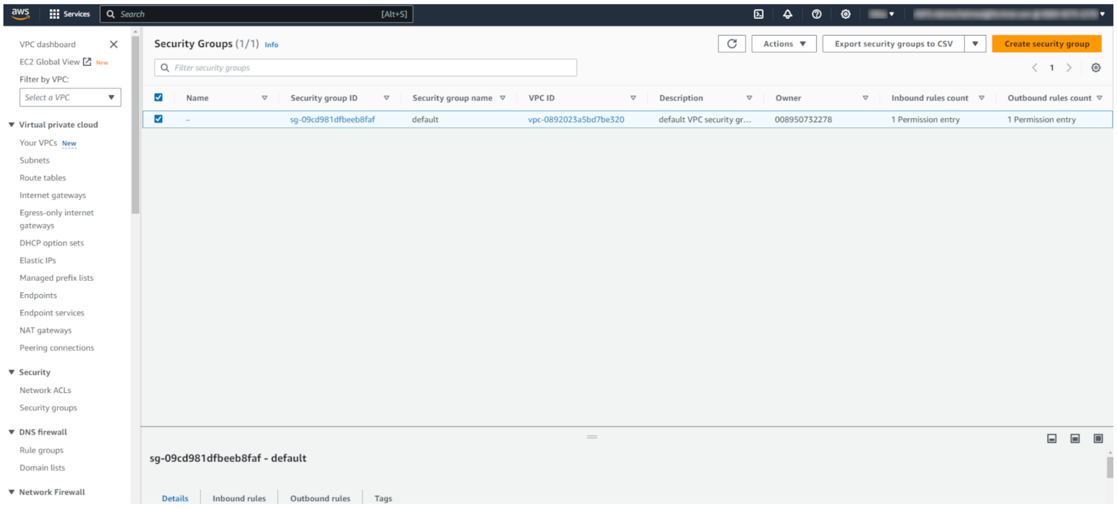
Note: Your Instances will launch in the US East region.

You are using the following Amazon VPC resources

AWS Network Manager provides tools and features to help you manage and monitor your network on AWS. Network Manager makes it easier to perform connectivity management, network monitoring and troubleshooting, IP management, and network security and governance.

Amazon VPC enables you to use your own isolated resources within the AWS Cloud, and then connect those resources directly to your own datacenter using industry-standard encrypted IPsec VPN connections.

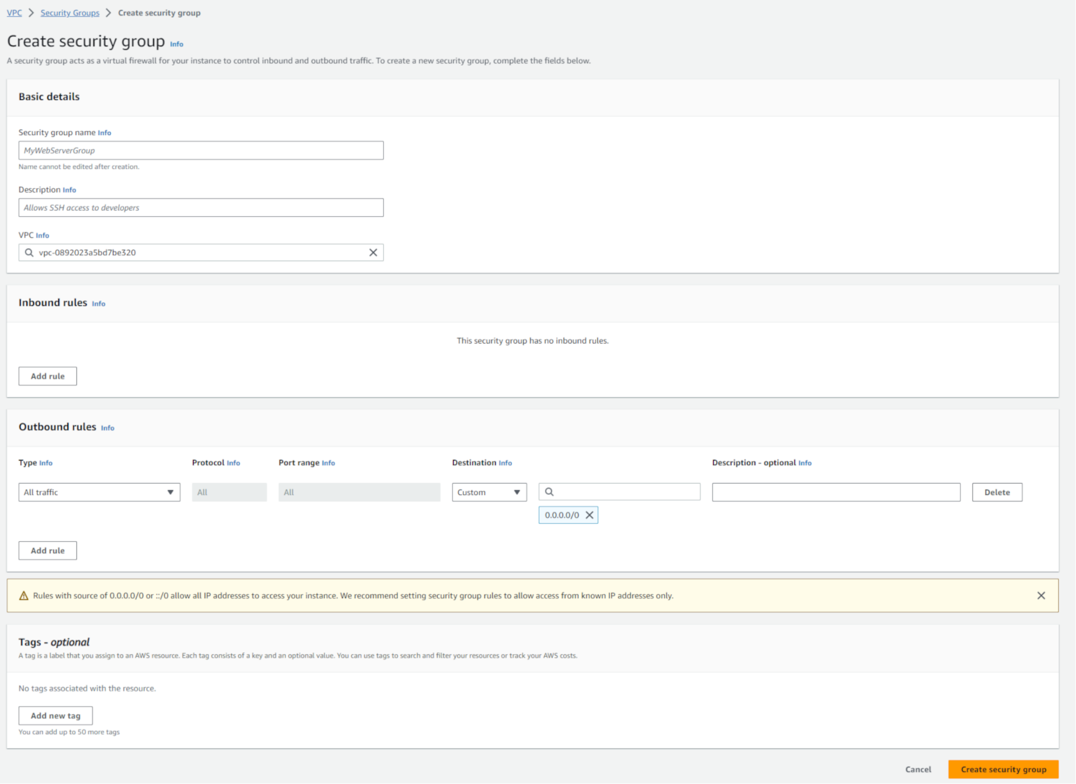
2. In the *VPC dashboard*, select *Security Groups*.
   The *Security Groups* window opens.



☑	Name	Security group ID	Security group name	VPC ID	Description	Owner	Inbound rules count	Outbound rules count
☑	–	sg-09cd981dfbeeb8faf	default	vpc-0892023a5bd7be320	default VPC security gr...	008950732278	1 Permission entry	1 Permission entry

sg-09cd981dfbeeb8faf - default

3. In the *Security Groups* window, select *Create security group*.
   The *Create security group* page opens.



VPC > Security Groups > Create security group

Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info

MyWebServerGroup

Name cannot be edited after creation.

Description Info

Allows SSH access to developers

VPC Info

vpc-0892023a5bd7be320

Inbound rules Info

This security group has no inbound rules.

Outbound rules Info

Type	Protocol	Port range	Destination		Description - optional	
All traffic	All	All	Custom	0.0.0.0/0		Delete

⚠ Rules with source of 0.0.0.0/0 or ::/0 allow all IP addresses to access your instance. We recommend setting security group rules to allow access from known IP addresses only.

Tags - *optional*

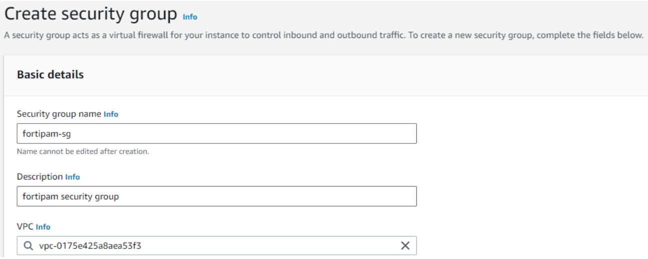
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

You can add up to 50 more tags

4. In the *Basic details* pane, enter the following information:

Security group name	The name of the security group. **Note**: The name of the group cannot be changed after creation.
Description	The description for the security group.
VPC	Search and select the VPC in which to create the security group.



Create security group Info

A security group acts as a virtual firewall for your instance to control inbound and outbound traffic. To create a new security group, complete the fields below.

Basic details

Security group name Info

fortipam-sg

Name cannot be edited after creation.

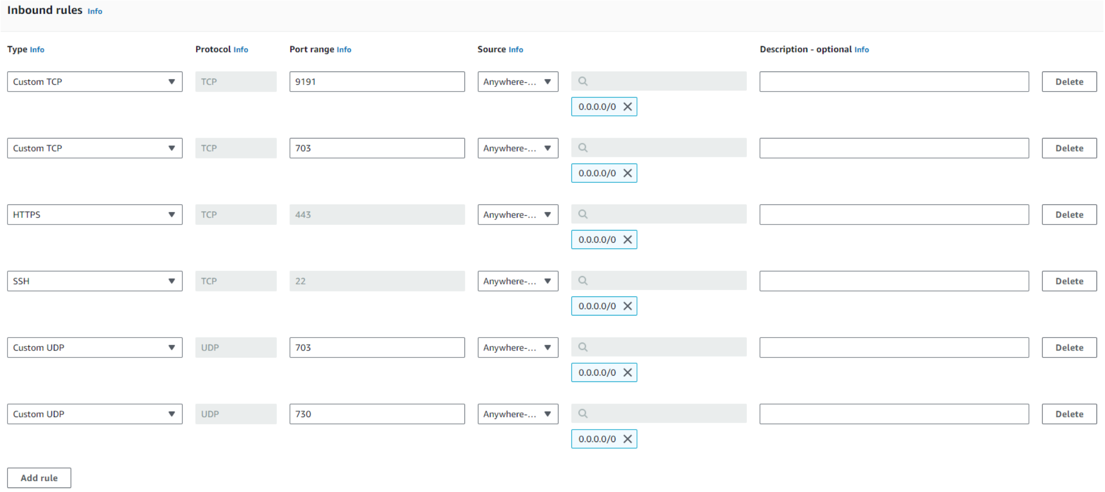
Description Info

fortipam security group

VPC Info

vpc-0175e425a8aea53f3

5. In the *Inbound rules* pane, add the following inbound rules:



Inbound rules Info

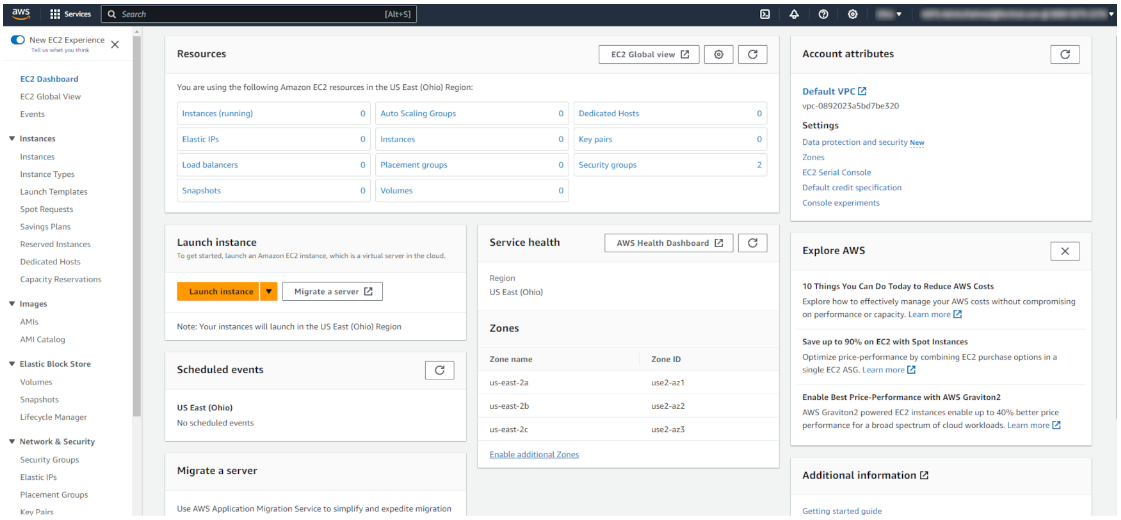
Type Info	Protocol Info	Port range Info	Source Info		Description - optional Info	
Custom TCP	TCP	9191	Anywhere-...	0.0.0.0/0 ✕		Delete
Custom TCP	TCP	703	Anywhere-...	0.0.0.0/0 ✕		Delete
HTTPS	TCP	443	Anywhere-...	0.0.0.0/0 ✕		Delete
SSH	TCP	22	Anywhere-...	0.0.0.0/0 ✕		Delete
Custom UDP	UDP	703	Anywhere-...	0.0.0.0/0 ✕		Delete
Custom UDP	UDP	730	Anywhere-...	0.0.0.0/0 ✕		Delete

6. Use the default outbound rule that allows all the traffic.
7. Click *Create security group*.

Launching the FortiPAM instance from AMI

To launch the FortiPAM instance:

1. In the AWS console, from the *Services* menu, go to *Compute* > *EC2*.
   The *EC2 Dashboard* opens.



Resources

You are using the following Amazon EC2 resources in the US East (Ohio) Region:

Instances (running)	0	Auto Scaling Groups	0	Dedicated Hosts	0
Elastic IPs	0	Instances	0	Key pairs	0
Load balancers	0	Placement groups	0	Security groups	2
Snapshots	0	Volumes	0		

Account attributes

Default VPC
vpc-0892023a5bd7be320

Settings
Data protection and security New
Zones
EC2 Serial Console
Default credit specification
Console experiments

Launch instance

To get started, launch an Amazon EC2 instance, which is a virtual server in the cloud.

Note: Your instances will launch in the US East (Ohio) Region

Service health

Region
US East (Ohio)

Zones

Zone name	Zone ID
us-east-2a	use2-az1
us-east-2b	use2-az2
us-east-2c	use2-az3

Enable additional Zones

Explore AWS

10 Things You Can Do Today to Reduce AWS Costs
Explore how to effectively manage your AWS costs without compromising on performance or capacity. Learn more

Save up to 90% on EC2 with Spot Instances
Optimize price-performance by combining EC2 purchase options in a single EC2 ASG. Learn more

Enable Best Price-Performance with AWS Graviton2
AWS Graviton2 powered EC2 instances enable up to 40% better price performance for a broad spectrum of cloud workloads. Learn more

Scheduled events

US East (Ohio)
No scheduled events

Migrate a server

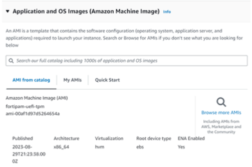
Use AWS Application Migration Service to simplify and expedite migration

Additional information

Getting started guide

2. Go to *Images* > *AMIs* and select *Launch instance from AMI*.
   The *Launch an instance* page opens.
3. In the *Name and tags* pane, enter the name for the instance.

4. Ensure that the correct AMI is selected in the *Application and OS Images (Amazon Machine Image)* pane.



▾ Application and OS Images (Amazon Machine Image) Info

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. Search or Browse for AMIs if you don't see what you are looking for below

Search our full catalog including 1000s of application and OS images

Amazon Machine Image (AMI)
fortipam-uefi-tpm
ami-00af1d97d5264654a

Published	Architecture	Virtualization	Root device type	ENA Enabled
2023-08-29T21:23:38.000Z	x86_64	hvm	ebs	Yes

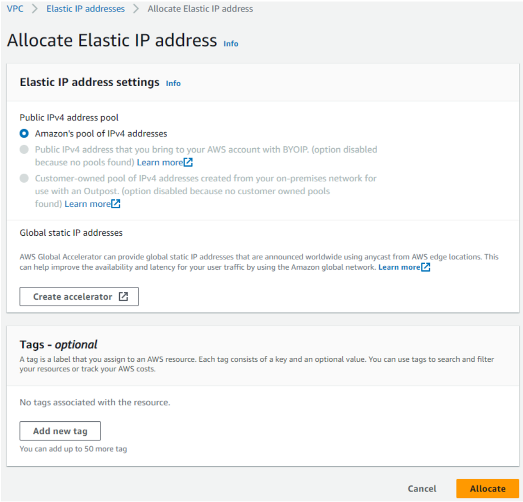
5. In the *Instance type* pane, select *m5.xlarge*.

> You must choose an instance type that supports EC2 Serial Console.

6. In the *Key pair (login)* pane, from the dropdown, select *Proceed without a key pair (Not recommended)*.
7. In the *Network settings* pane:
   a. In *Firewall (security groups)*, select *Select existing security group*.
   b. From the *Common security groups* dropdown, select the security group created in Configuring a security group on page 498.
   c. Optionally, click *Edit* in *Network settings* to add more interfaces and choose a subnet.
8. In *Configure storage* pane:
   a. In the field for root volume, enter `2` (in GB).
   b. Select *Add new volume*, and in the field, enter `300` (in GB) to add a new volume for the log.
   c. Select *Add new volume* and in the field enter `1024` (in GB) to add a new volume for video.
9. Click *Launch instance*.

Initial configuration

1. In the AWS console, search *VPC* and select VPC from the search result.
   The *VPC dashboard* opens.
2. In *Virtual private cloud* on the left, select *Elastic IPs*.
   The *Elastic IP addresses* window opens.



Allocate Elastic IP address Info

Elastic IP address settings Info

Public IPv4 address pool

● Amazon's pool of IPv4 addresses

○ Public IPv4 address that you bring to your AWS account with BYOIP. (option disabled because no pools found) Learn more

○ Customer-owned pool of IPv4 addresses created from your on-premises network for use with an Outpost. (option disabled because no customer owned pools found) Learn more

Global static IP addresses

AWS Global Accelerator can provide global static IP addresses that are announced worldwide using anycast from AWS edge locations. This can help improve the availability and latency for your user traffic by using the Amazon global network. Learn more

Tags - *optional*

A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

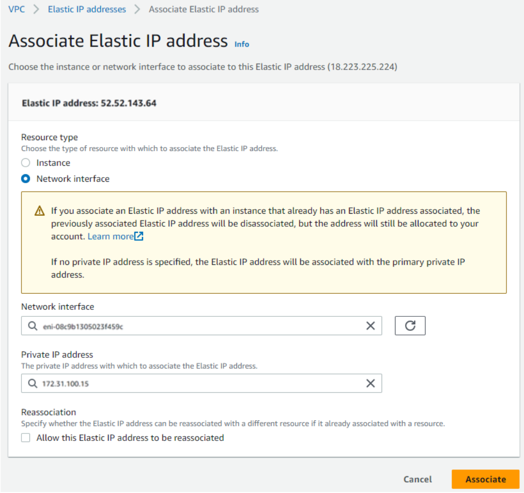
No tags associated with the resource.

You can add up to 50 more tag

3. In the *Elastic IP addresses* window, click *Allocate* to create a new public IP address.
4. Select an IP address from the elastic IP addresses list, and from the *Actions* dropdown, select *Associate Elastic IP address*.

The *Associate Elastic IP address* page opens.

5. In *Resource type*, select *Network* interface.
6. In the *Network interface* dropdown, select a network interface.
7. In the *Private IP address* dropdown, select a private IP address.



Associate Elastic IP address Info

Choose the instance or network interface to associate to this Elastic IP address (18.223.225.224)

Elastic IP address: 52.52.143.64

Resource type
Choose the type of resource with which to associate the Elastic IP address.

○ Instance
● Network interface

⚠ If you associate an Elastic IP address with an instance that already has an Elastic IP address associated, the previously associated Elastic IP address will be disassociated, but the address will still be allocated to your account. Learn more

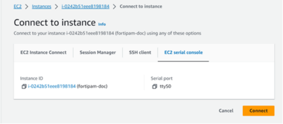
If no private IP address is specified, the Elastic IP address will be associated with the primary private IP address.

Network interface
eni-08c9b1305023f459c

Private IP address
The private IP address with which to associate the Elastic IP address.
172.31.100.15

Reassociation
Specify whether the Elastic IP address can be reassociated with a different resource if it already associated with a resource.
□ Allow this Elastic IP address to be reassociated

8. Click *Associate*.
9. In the AWS console, from the *Services* menu, go to *Compute* > *EC2*.
10. In the *EC2 Dashboard*, go to *Instances* > *Instances*, select the FortiPAM instance from the list, and then select *Connect*.
11. From the *EC2 serial console* tab, click *Connect*.



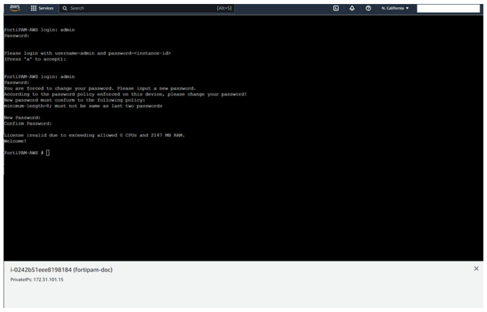
Connect to instance Info

Connect to your instance i-0242b51eee8198184 (fortipam-doc) using any of these options

Instance ID
i-0242b51eee8198184 (fortipam-doc)

Serial port
ttyS0

12. Log in as the administrator with the AWS instance ID password.
13. FortiPAM asks you to change your password. Enter a new password. Enter the password again to confirm.



```
FortiPAM-AWS login: admin
Password:


Please login with username=admin and password=<instance-id>
(Press 'a' to accept):


FortiPAM-AWS login: admin
Password:
You are forced to change your password. Please input a new password.
According to the password policy enforced on this device, please change your password!
New password must conform to the following policy:
minimum-length=8; must not be same as last two passwords

New Password:
Confirm Password:

License invalid due to exceeding allowed 0 CPUs and 2147 MB RAM.
Welcome!

FortiPAM-AWS # 
```

i-0242b51eee8198184 (fortipam-doc)
PrivateIPs: 172.31.101.15

14. Use the following FortiPAM CLI commands to configure the port1, change mode from DHCP to static and set the IP address to the same as the private IP address in steps 4 to 8:

You can skip this step if FortiPAM is in standalone mode.

```
config system interface
 edit "port1"
```

```
    set mode static #by default, set as dhcp
    set ip 172.31.100.15/24 #set to the private IP address assigned by AWS in step 7
  next
end
```

When upgrading a FortiPAM instance, use the following CLI command to enable synchronizing the virtual IP address to the IP address of the external interface:

```
Example

 config firewall vip
  set intf-ip-sync enable
  set extintf "port1" #The interface connected to the source network
that receives the packets forwarded to the destination network.
 end
```

When installing a new FortiPAM instance, the synchronization happens automatically.

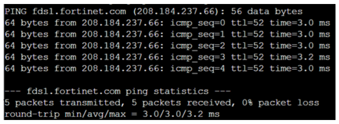
15. Use the following FortiPAM CLI commands to configure a static route if the interface is configured as static mode:

```
config router static
 edit 1
  set gateway 172.31.100.1
  set device port1
 next
end
```

16. Optionally, use the following command to verify that you can access the public network:

```
 execute ping update.fortiguard.net
```

You should receive an echo reply packet similar to the following:



```
PING fds1.fortinet.com (208.184.237.66): 56 data bytes
64 bytes from 208.184.237.66: icmp_seq=0 ttl=52 time=3.0 ms
64 bytes from 208.184.237.66: icmp_seq=1 ttl=52 time=3.0 ms
64 bytes from 208.184.237.66: icmp_seq=2 ttl=52 time=3.0 ms
64 bytes from 208.184.237.66: icmp_seq=3 ttl=52 time=3.2 ms
64 bytes from 208.184.237.66: icmp_seq=4 ttl=52 time=3.0 ms

--- fds1.fortinet.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 3.0/3.0/3.2 ms
```

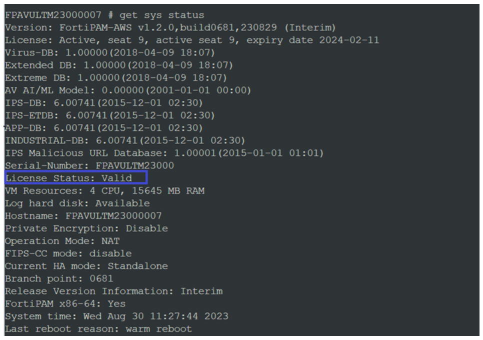
17. Optionally, to encrypt disk to protect logs and videos, see Configuring log and video disk encryption on page 347.

Licensing

To successfully license FortiPAM:

1. Download the license file (`.lic`), see Registering and downloading your license.
2. Upload the license file from the public IP address using SCP, see Uploading the license file using SCP.
3. After the boot up, the license status changes to valid.
   You can check the license status using the following CLI command:

```
 get system status
```



```
FPAVULTM23000007 # get sys status
Version: FortiPAM-AWS v1.2.0,build0681,230829 (Interim)
License: Active, seat 9, active seat 9, expiry date 2024-02-11
Virus-DB: 1.00000(2018-04-09 18:07)
Extended DB: 1.00000(2018-04-09 18:07)
Extreme DB: 1.00000(2018-04-09 18:07)
AV AI/ML Model: 0.00000(2001-01-01 00:00)
IPS-DB: 6.00741(2015-12-01 02:30)
IPS-ETDB: 6.00741(2015-12-01 02:30)
APP-DB: 6.00741(2015-12-01 02:30)
INDUSTRIAL-DB: 6.00741(2015-12-01 02:30)
IPS Malicious URL Database: 1.00001(2015-01-01 01:01)
Serial-Number: FPAVULTM23000
License Status: Valid
VM Resources: 4 CPU, 15645 MB RAM
Log hard disk: Available
Hostname: FPAVULTM23000007
Private Encryption: Disable
Operation Mode: NAT
FIPS-CC mode: disable
Current HA mode: Standalone
Branch point: 0681
Release Version Information: Interim
FortiPAM x86-64: Yes
System time: Wed Aug 30 11:27:44 2023
Last reboot reason: warm reboot
```

4. Optional- Customize VIP if default VIP is not preferred:

   ```
   config firewall vip
    edit "fortipam_vip"
     set extip 172.31.100.15 #external visible virtual IP address
    next
   end
   ```

5. You can now use your FortiPAM-VM deployed on AWS.
   On a web browser, go to `https://<Public IP>` to access the FortiPAM-VM GUI. This is the same IP address set up in step 4 above.

Appendix K: Installation on GCP

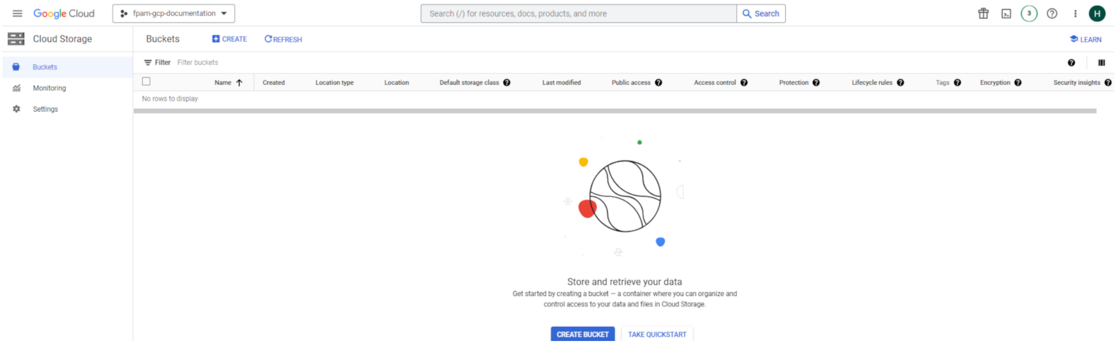
FortiPAM installation on GCP and initial setup:

1. Creating a cloud storage bucket on GCP on page 505
2. Adding the FortiPAM image file to the storage bucket on page 506
3. Creating a FortiPAM image on GCP on page 507
4. Creating VM instance from the image on page 509
5. Licensing on page 513
6. Static interface IP address on page 514
7. Setting up HA on page 515
8. Enabling vTPM on page 517

Creating a cloud storage bucket on GCP

To create a cloud storage bucket on GCP:

1. From the navigation pane, go to *Cloud Storage* > *Bucket*.
   The *Buckets* window opens.



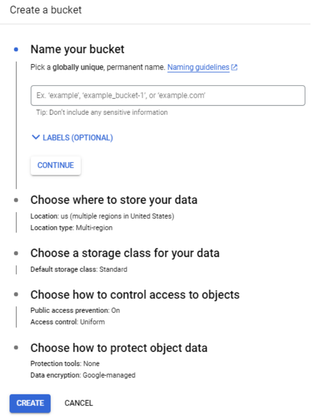
□	Name ↑	Created	Location type	Location	Default storage class	Last modified	Public access	Access control	Protection	Lifecycle rules	Tags	Encryption	Security insights

No rows to display

Store and retrieve your data

Get started by creating a bucket — a container where you can organize and control access to your data and files in Cloud Storage.

2. Select +*CREATE/CREATE BUCKET* to create a new storage bucket.


Create a bucket

- Name your bucket

  Pick a **globally unique**, permanent name. Naming guidelines

  Ex. 'example', 'example_bucket-1', or 'example.com'

  Tip: Don't include any sensitive information

  LABELS (OPTIONAL)

  CONTINUE

- Choose where to store your data

  Location: us (multiple regions in United States)
  Location type: Multi-region

- Choose a storage class for your data

  Default storage class: Standard

- Choose how to control access to objects

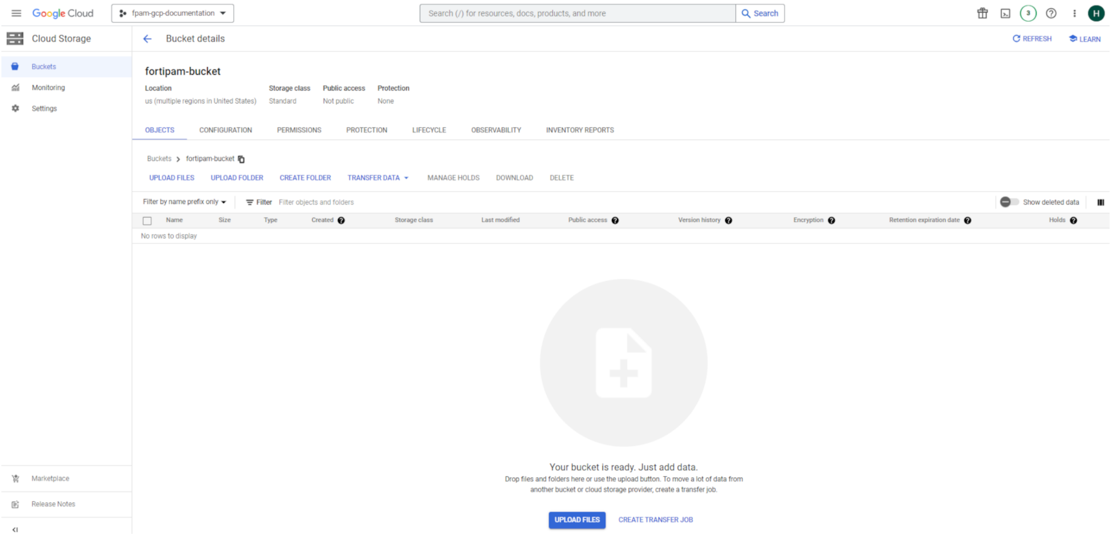
  Public access prevention: On
  Access control: Uniform

- Choose how to protect object data

  Protection tools: None
  Data encryption: Google-managed

3. In *Name*, enter a name for the storage bucket, and click *CONTINUE*.

4. In *Choose where to store your data*, select *Multi-region*, from the dropdown select a location, and click *CONTINUE*.
5. In *Choose a storage class for your data*, keep the default settings, and click *CONTINUE*.
6. In *Choose how to control access to objects*, keep the default settings, and click *CONTINUE*.
7. In *Choose how to protect object data*, keep the default settings, and click *CONTINUE*.
8. Select *Create*.
   The storage bucket is created.



fortipam-bucket

Location	Storage class	Public access	Protection
us (multiple regions in United States)	Standard	Not public	None

Buckets > fortipam-bucket

No rows to display

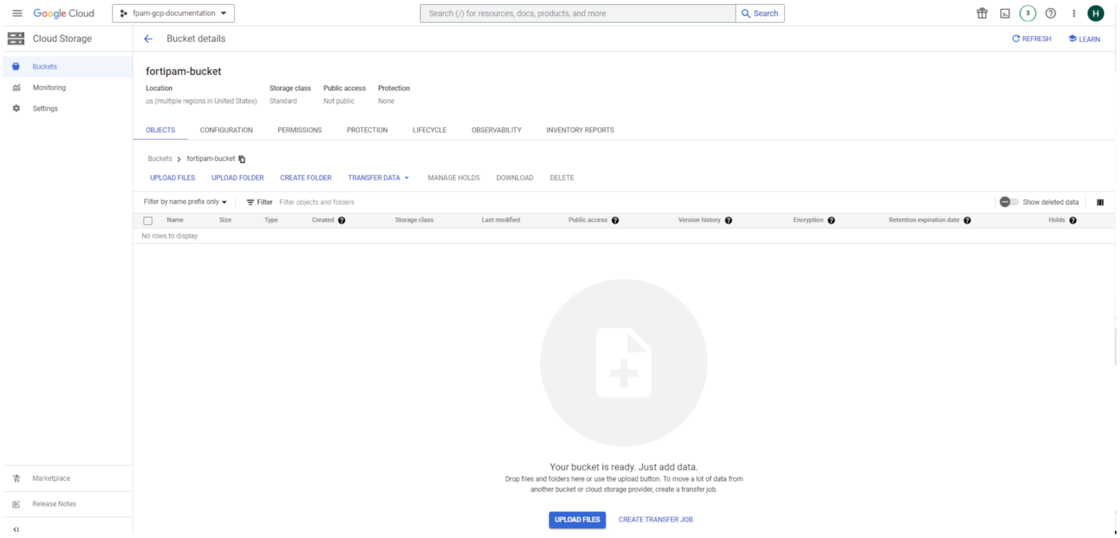
Your bucket is ready. Just add data.

Drop files and folders here or use the upload button. To move a lot of data from another bucket or cloud storage provider, create a transfer job.

Adding the FortiPAM image file to the storage bucket

To add the FortiPAM image file to the storage bucket:

1. From the navigation pane, go to *Cloud Storage* > *Bucket*.
2. In the *Buckets* window, click the name of the storage bucket created in Creating a cloud storage bucket on GCP on page 505 to open it.



fortipam-bucket

Location	Storage class	Public access	Protection
us (multiple regions in United States)	Standard	Not public	None

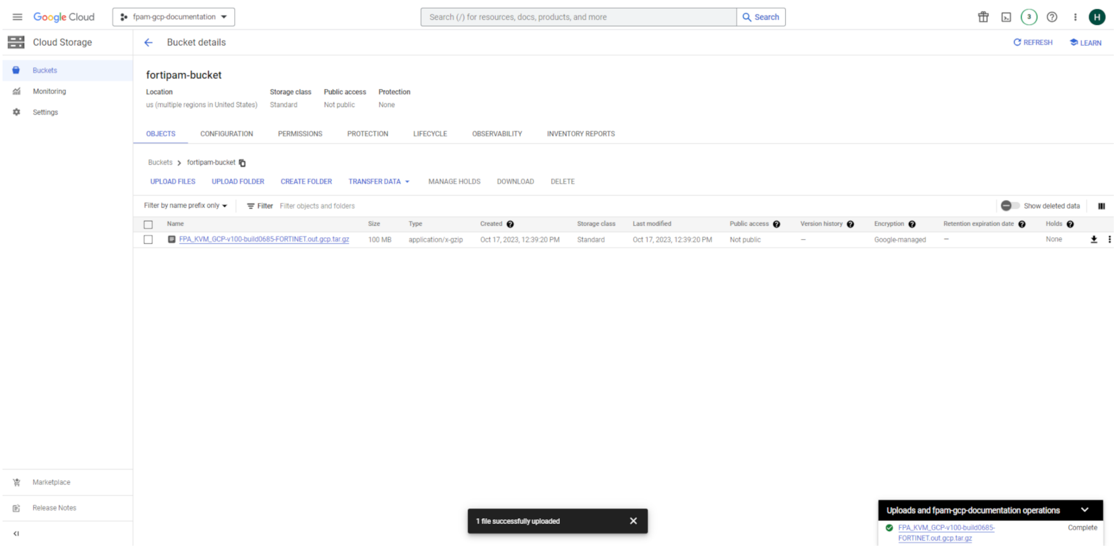
Buckets > fortipam-bucket

No rows to display

Your bucket is ready. Just add data.

Drop files and folders here or use the upload button. To move a lot of data from another bucket or cloud storage provider, create a transfer job.

3. Select *UPLOAD FILES*, locate the FortiPAM image file from your management computer, and click *Open*.
   The FortiPAM image file is successfully uploaded to the storage bucket.



fortipam-bucket

Location	Storage class	Public access	Protection
us (multiple regions in United States)	Standard	Not public	None

□	Name	Size	Type	Created	Storage class	Last modified	Public access	Version history	Encryption	Retention expiration date	Holds
□	FPA_KVM_GCP-v100-build0685-FORTINET.out.gcp.tar.gz	100 MB	application/x-gzip	Oct 17, 2023, 12:39:20 PM	Standard	Oct 17, 2023, 12:39:20 PM	Not public	–	Google-managed	–	None

1 file successfully uploaded

Uploads and fpam-gcp-documentation operations

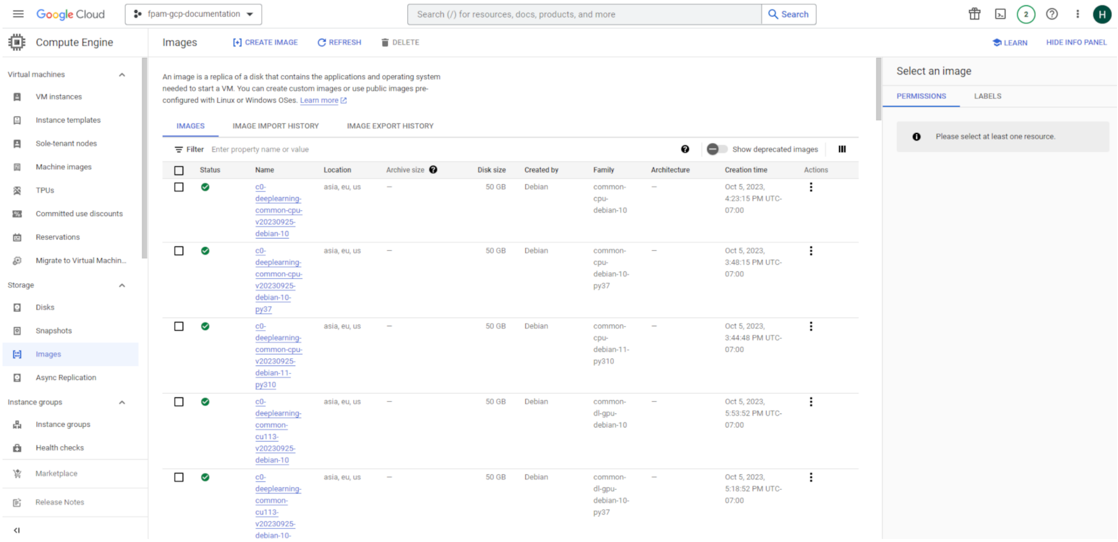
FPA_KVM_GCP-v100-build0685-FORTINET.out.gcp.tar.gz Complete

Creating a FortiPAM image on GCP

If you want to use vTPM, see Enabling vTPM on page 517 to create an image.

To create a FortiPAM image on GCP:

1. From the navigation pane, go to *Compute Engine* > *Storage* > *Images*.
   The *Images* window opens.

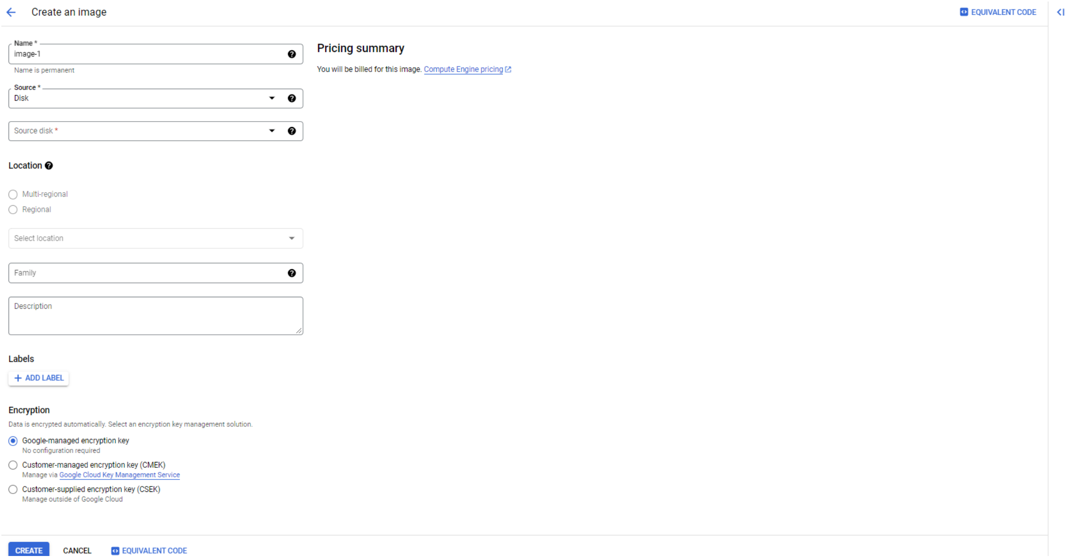


An image is a replica of a disk that contains the applications and operating system needed to start a VM. You can create custom images or use public images pre-configured with Linux or Windows OSes. Learn more

□	Status	Name	Location	Archive size	Disk size	Created by	Family	Architecture	Creation time	Actions
□	✓	c0-deeplearning-common-cpu-v20230925-debian-10	asia, eu, us	–	50 GB	Debian	common-cpu-debian-10	–	Oct 5, 2023, 4:23:15 PM UTC-07:00	⋮
□	✓	c0-deeplearning-common-cpu-v20230925-debian-10-py37	asia, eu, us	–	50 GB	Debian	common-cpu-debian-10-py37	–	Oct 5, 2023, 3:48:15 PM UTC-07:00	⋮
□	✓	c0-deeplearning-common-cpu-v20230925-debian-11-py310	asia, eu, us	–	50 GB	Debian	common-cpu-debian-11-py310	–	Oct 5, 2023, 3:44:48 PM UTC-07:00	⋮
□	✓	c0-deeplearning-common-cu113-v20230925-debian-10	asia, eu, us	–	50 GB	Debian	common-dl-gpu-debian-10	–	Oct 5, 2023, 5:53:52 PM UTC-07:00	⋮
□	✓	c0-deeplearning-common-cu113-v20230925-debian-10-	asia, eu, us	–	50 GB	Debian	common-dl-gpu-debian-10-py37	–	Oct 5, 2023, 5:18:52 PM UTC-07:00	⋮

Please select at least one resource.

2. In the *Images* window, select *Create Image*, and click *CONTINUE*.
   The *Create an image* window opens.

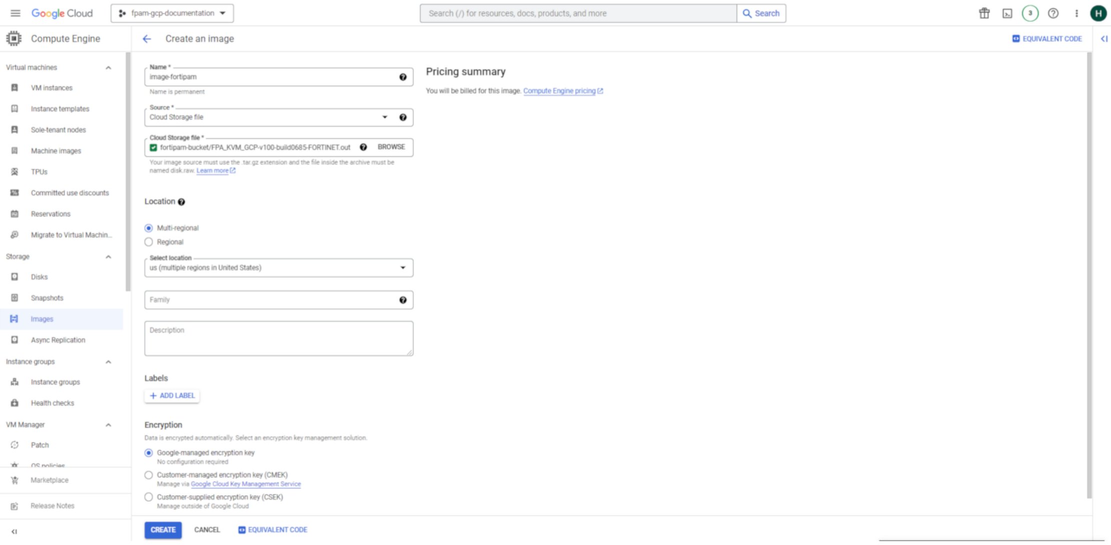


Name *: image-1
Name is permanent
Source *: Disk
Source disk *
Location:
○ Multi-regional
○ Regional
Select location
Family
Description
Data is encrypted automatically. Select an encryption key management solution.
● Google-managed encryption key
No configuration required
○ Customer-managed encryption key (CMEK)
Manage via Google Cloud Key Management Service
○ Customer-supplied encryption key (CSEK)
Manage outside of Google Cloud

3. In *Name*, enter a name for the image.
4. In the *Source* dropdown, select *Cloud Storage file*.
5. Select *BROWSE*, from the *Select object* pane that opens, go to the FortiPAM image file, and click *SELECT*.

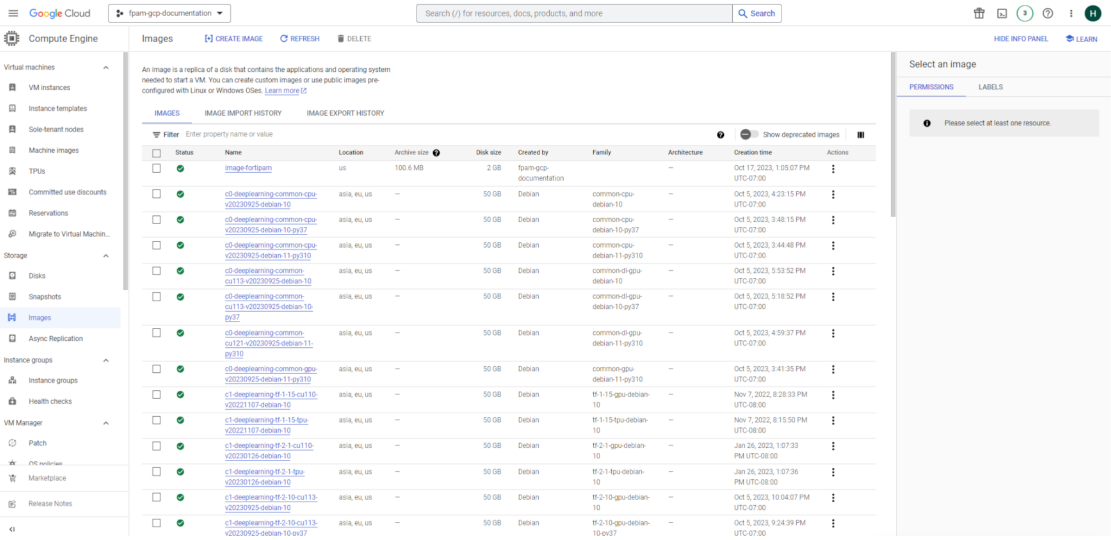
> The image source must have `.tar.gz` as its extension and the file in it must be named `disk.raw`.

6. Ensure that the *Location* is set to *Multi-regional*.
7. Leave the rest of the settings in the default state.



Name *: image-fortipam
Name is permanent
Source *: Cloud Storage file
Cloud Storage file *: fortipam-bucket/FPA_KVM_GCP-v100-build0685-FORTINET.out BROWSE
Your image source must use the .tar.gz extension and the file inside the archive must be named disk.raw. Learn more
Location:
● Multi-regional
○ Regional
Select location: us (multiple regions in United States)
Family
Description
Data is encrypted automatically. Select an encryption key management solution.
● Google-managed encryption key
No configuration required
○ Customer-managed encryption key (CMEK)
Manage via Google Cloud Key Management Service
○ Customer-supplied encryption key (CSEK)
Manage outside of Google Cloud

8. Click *CREATE*.
The new FortiPAM image is now listed at the top in the *Images* window.



An image is a replica of a disk that contains the applications and operating system needed to start a VM. You can create custom images or use public images pre-configured with Linux or Windows OSes. Learn more

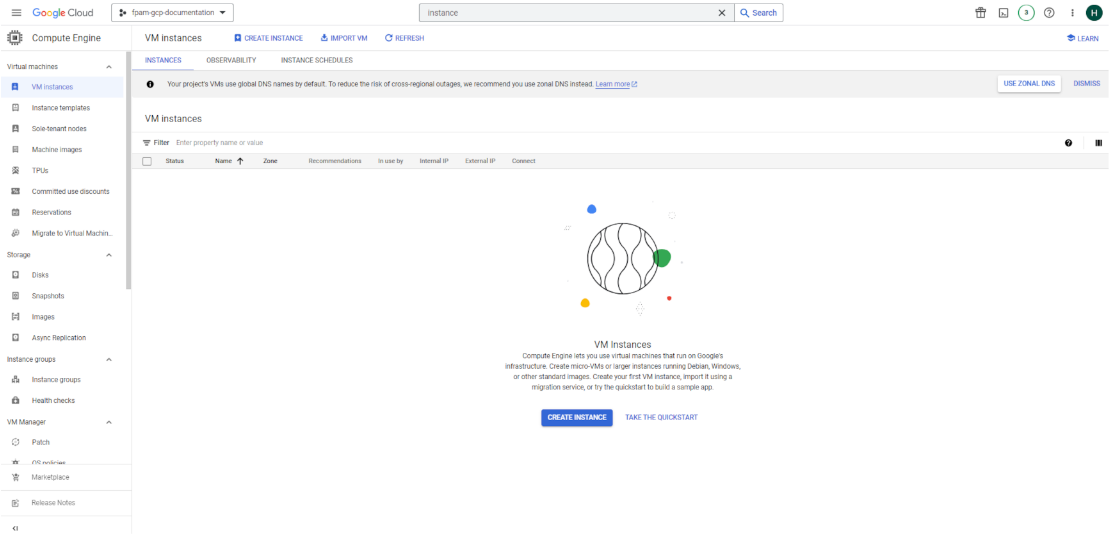
Status	Name	Location	Archive size	Disk size	Created by	Family	Architecture	Creation time	Actions
✓	image-fortipam	us	100.6 MB	2 GB	fpam-gcp-documentation		–	Oct 17, 2023, 1:05:07 PM UTC-07:00	⋮
✓	c0-deeplearning-common-cpu-v20230925-debian-10	asia, eu, us	–	50 GB	Debian	common-cpu-debian-10	–	Oct 5, 2023, 4:23:15 PM UTC-07:00	⋮
✓	c0-deeplearning-common-cpu-v20230925-debian-10-py37	asia, eu, us	–	50 GB	Debian	common-cpu-debian-10-py37	–	Oct 5, 2023, 3:48:15 PM UTC-07:00	⋮
✓	c0-deeplearning-common-cpu-v20230925-debian-11-py310	asia, eu, us	–	50 GB	Debian	common-cpu-debian-11-py310	–	Oct 5, 2023, 3:44:48 PM UTC-07:00	⋮
✓	c0-deeplearning-common-cu113-v20230925-debian-10	asia, eu, us	–	50 GB	Debian	common-dl-gpu-debian-10	–	Oct 5, 2023, 5:53:52 PM UTC-07:00	⋮
✓	c0-deeplearning-common-cu113-v20230925-debian-10-py37	asia, eu, us	–	50 GB	Debian	common-dl-gpu-debian-10-py37	–	Oct 5, 2023, 5:18:52 PM UTC-07:00	⋮
✓	c0-deeplearning-common-cu121-v20230925-debian-11-py310	asia, eu, us	–	50 GB	Debian	common-dl-gpu-debian-11-py310	–	Oct 5, 2023, 4:59:37 PM UTC-07:00	⋮
✓	c0-deeplearning-common-gpu-v20230925-debian-11-py310	asia, eu, us	–	50 GB	Debian	common-gpu-debian-11-py310	–	Oct 5, 2023, 3:41:35 PM UTC-07:00	⋮
✓	c1-deeplearning-tf-1-15-cu110-v20221107-debian-10	asia, eu, us	–	50 GB	Debian	tf-1-15-gpu-debian-10	–	Nov 7, 2022, 8:28:33 PM UTC-08:00	⋮
✓	c1-deeplearning-tf-1-15-tpu-v20221107-debian-10	asia, eu, us	–	50 GB	Debian	tf-1-15-tpu-debian-10	–	Nov 7, 2022, 8:15:50 PM UTC-08:00	⋮
✓	c1-deeplearning-tf-2-1-cu110-v20230126-debian-10	asia, eu, us	–	50 GB	Debian	tf-2-1-gpu-debian-10	–	Jan 26, 2023, 1:07:33 PM UTC-08:00	⋮
✓	c1-deeplearning-tf-2-1-tpu-v20230126-debian-10	asia, eu, us	–	50 GB	Debian	tf-2-1-tpu-debian-10	–	Jan 26, 2023, 1:07:36 PM UTC-08:00	⋮
✓	c1-deeplearning-tf-2-10-cu113-v20230925-debian-10	asia, eu, us	–	50 GB	Debian	tf-2-10-gpu-debian-10	–	Oct 5, 2023, 10:04:07 PM UTC-07:00	⋮
✓	c1-deeplearning-tf-2-10-cu113-v20230925-debian-10-py37	asia, eu, us	–	50 GB	Debian	tf-2-10-gpu-debian-10-py37	–	Oct 5, 2023, 9:24:39 PM UTC-07:00	⋮

Please select at least one resource.

Creating VM instance from the image

To create VM instance from the image:

1. From the navigation pane, go to *Compute Engine* > *VM instances*.
   The *VM instances* window opens.



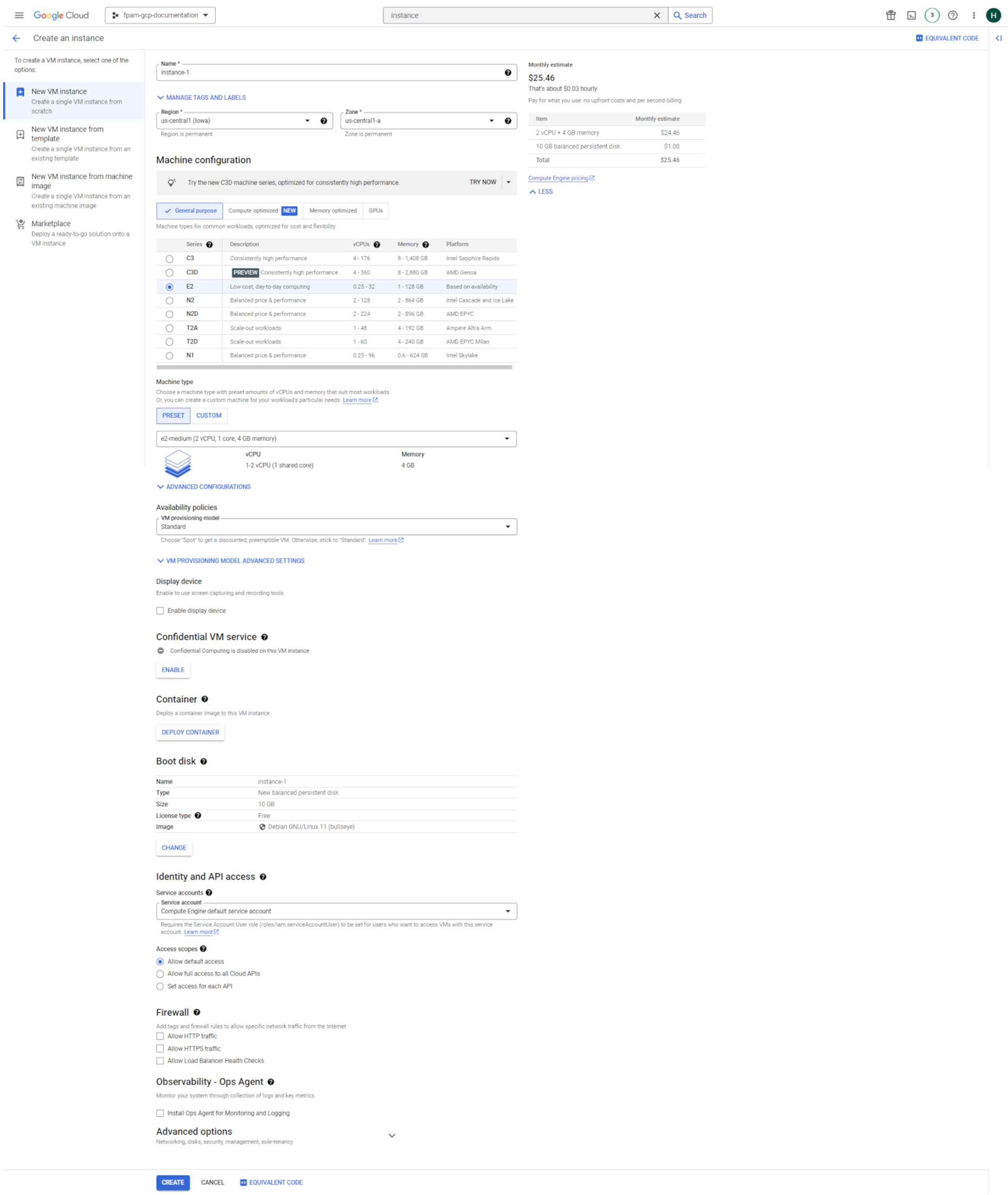
Your project's VMs use global DNS names by default. To reduce the risk of cross-regional outages, we recommend you use zonal DNS instead. Learn more

VM instances

VM Instances

Compute Engine lets you use virtual machines that run on Google's infrastructure. Create micro-VMs or larger instances running Debian, Windows, or other standard images. Create your first VM instance, import it using a migration service, or try the quickstart to build a sample app.

2. Select CREATE INSTANCE.
   The *Create an instance* window opens.



Create an instance

To create a VM instance, select one of the options:

- New VM instance
  Create a single VM instance from scratch
- New VM instance from template
  Create a single VM instance from an existing template
- New VM instance from machine image
  Create a single VM instance from an existing machine image
- Marketplace
  Deploy a ready-to-go solution onto a VM instance

Name * instance-1

MANAGE TAGS AND LABELS

Region * us-central1 (Iowa) — Region is permanent

Zone * us-central1-a — Zone is permanent

Machine configuration

Try the new C3D machine series, optimized for consistently high performance. TRY NOW

General purpose | Compute optimized NEW | Memory optimized | GPUs

Machine types for common workloads, optimized for cost and flexibility

	Series	Description	vCPUs	Memory	Platform
○	C3	Consistently high performance	4 - 176	8 - 1,408 GB	Intel Sapphire Rapids
○	C3D	PREVIEW Consistently high performance	4 - 360	8 - 2,880 GB	AMD Genoa
●	E2	Low cost, day-to-day computing	0.25 - 32	1 - 128 GB	Based on availability
○	N2	Balanced price & performance	2 - 128	2 - 864 GB	Intel Cascade and Ice Lake
○	N2D	Balanced price & performance	2 - 224	2 - 896 GB	AMD EPYC
○	T2A	Scale-out workloads	1 - 48	4 - 192 GB	Ampere Altra Arm
○	T2D	Scale-out workloads	1 - 60	4 - 240 GB	AMD EPYC Milan
○	N1	Balanced price & performance	0.25 - 96	0.6 - 624 GB	Intel Skylake

Machine type

Choose a machine type with preset amounts of vCPUs and memory that suit most workloads.
Or, you can create a custom machine for your workload's particular needs. Learn more

PRESET | CUSTOM

e2-medium (2 vCPU, 1 core, 4 GB memory)

vCPU	Memory
1-2 vCPU (1 shared core)	4 GB

ADVANCED CONFIGURATIONS

Availability policies

VM provisioning model: Standard

Choose "Spot" to get a discounted, preemptible VM. Otherwise, stick to "Standard". Learn more

VM PROVISIONING MODEL ADVANCED SETTINGS

Display device

Enable to use screen capturing and recording tools.

□ Enable display device

Confidential VM service

Confidential Computing is disabled on this VM instance

ENABLE

Container

Deploy a container image to this VM instance

DEPLOY CONTAINER

Boot disk

Name	instance-1
Type	New balanced persistent disk
Size	10 GB
License type	Free
Image	Debian GNU/Linux 11 (bullseye)

CHANGE

Identity and API access

Service accounts

Service account: Compute Engine default service account

Requires the Service Account User role (roles/iam.serviceAccountUser) to be set for users who want to access VMs with this service account. Learn more

Access scopes

● Allow default access
○ Allow full access to all Cloud APIs
○ Set access for each API

Firewall

Add tags and firewall rules to allow specific network traffic from the Internet

□ Allow HTTP traffic
□ Allow HTTPS traffic
□ Allow Load Balancer Health Checks

Observability - Ops Agent

Monitor your system through collection of logs and key metrics.

□ Install Ops Agent for Monitoring and Logging

Advanced options

Networking, disks, security, management, sole-tenancy

CREATE CANCEL EQUIVALENT CODE

Monthly estimate

$25.46

That's about $0.03 hourly

Pay for what you use: no upfront costs and per second billing

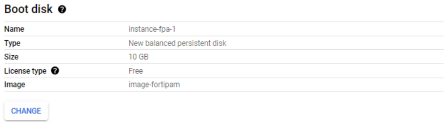
Item	Monthly estimate
2 vCPU + 4 GB memory	$24.46
10 GB balanced persistent disk	$1.00
Total	$25.46

Compute Engine pricing

LESS

3. In *Name*, enter a name for the VM instance.
4. From the *Region* dropdown, select a region where the resource is located.
5. From the *Zone* dropdown, select a zone within the region where the resource is located.
6. In *Machine configuration*, select a machine type for deployment.
7. In *Boot disk*, select *CHANGE*:
   a. Switch to the *CUSTOM IMAGES* tab.
   b. From the *Image* dropdown, select the image created in Creating a FortiPAM image on GCP on page 507.

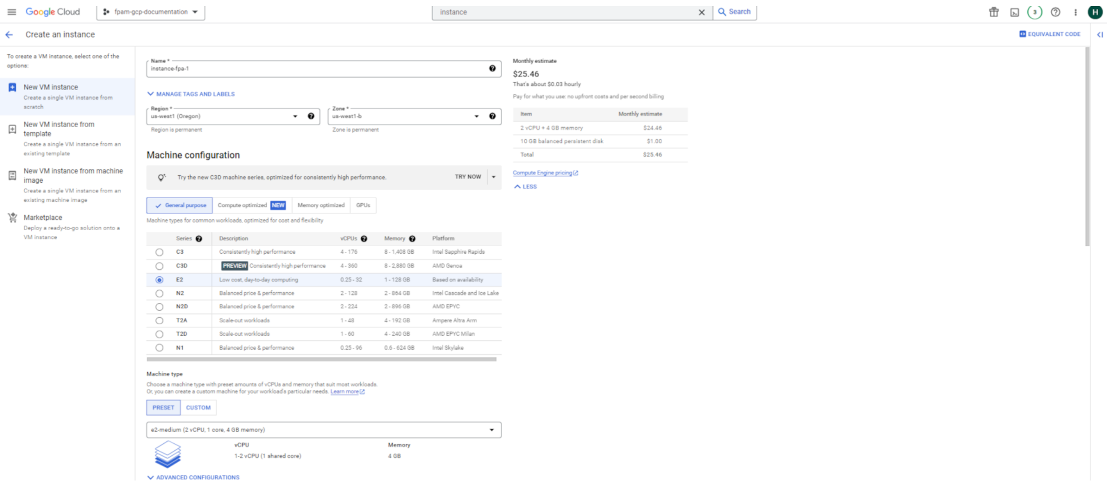
c. Click *SELECT*.



Boot disk

Name	instance-fpa-1
Type	New balanced persistent disk
Size	10 GB
License type	Free
Image	image-fortipam

8. Leave the following settings in the default state:
   - *ADVANCED CONFIGURATIONS*
   - *Display device*
   - *Confidential VM service*
   - *Container*
   - *Identity and API access*
   - *Firewall*
   - *Observability - Ops Agent*



To create a VM instance, select one of the options:

New VM instance
Create a single VM instance from scratch

New VM instance from template
Create a single VM instance from an existing template

New VM instance from machine image
Create a single VM instance from an existing machine image

Marketplace
Deploy a ready-to-go solution onto a VM instance

Name *: instance-fpa-1

Region *: us-west1 (Oregon)
Region is permanent

Zone *: us-west1-b
Zone is permanent

Machine configuration

Try the new C3D machine series, optimized for consistently high performance.

Machine types for common workloads, optimized for cost and flexibility

	Series	Description	vCPUs	Memory	Platform
○	C3	Consistently high performance	4 - 176	8 - 1,408 GB	Intel Sapphire Rapids
○	C3D	PREVIEW Consistently high performance	4 - 360	8 - 2,880 GB	AMD Genoa
●	E2	Low cost, day-to-day computing	0.25 - 32	1 - 128 GB	Based on availability
○	N2	Balanced price & performance	2 - 128	2 - 864 GB	Intel Cascade and Ice Lake
○	N2D	Balanced price & performance	2 - 224	2 - 896 GB	AMD EPYC
○	T2A	Scale-out workloads	1 - 48	4 - 192 GB	Ampere Altra Arm
○	T2D	Scale-out workloads	1 - 60	4 - 240 GB	AMD EPYC Milan
○	N1	Balanced price & performance	0.25 - 96	0.6 - 624 GB	Intel Skylake

Machine type

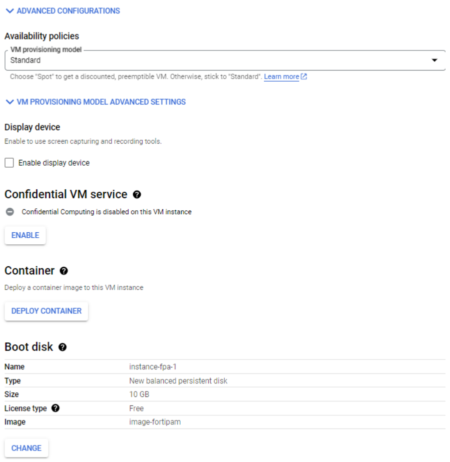
Choose a machine type with preset amounts of vCPUs and memory that suit most workloads.
Or, you can create a custom machine for your workload's particular needs. Learn more

e2-medium (2 vCPU, 1 core, 4 GB memory)

vCPU: 1-2 vCPU (1 shared core)
Memory: 4 GB

Monthly estimate
$25.46
That's about $0.03 hourly
Pay for what you use: no upfront costs and per second billing

Item	Monthly estimate
2 vCPU + 4 GB memory	$24.46
10 GB balanced persistent disk	$1.00
Total	$25.46



Availability policies

VM provisioning model: Standard

Choose "Spot" to get a discounted, preemptible VM. Otherwise, stick to "Standard". Learn more

Display device

Enable to use screen capturing and recording tools.

□ Enable display device

Confidential VM service

Confidential Computing is disabled on this VM instance

Container

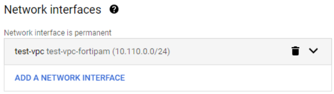
Deploy a container image to this VM instance

Boot disk

Name	instance-fpa-1
Type	New balanced persistent disk
Size	10 GB
License type	Free
Image	image-fortipam

9. Expand *Advanced options* > *Networking*:

   a. In *Network interfaces*, ensure that a network interface with a subnetwork is selected.

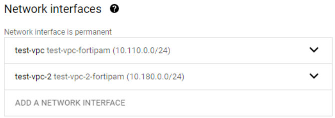


Network interfaces

Network interface is permanent

test-vpc test-vpc-fortipam (10.110.0.0/24)

b. In *Network interfaces*, add another network if the FortiPAM will be used in an HA cluster.



Network interfaces

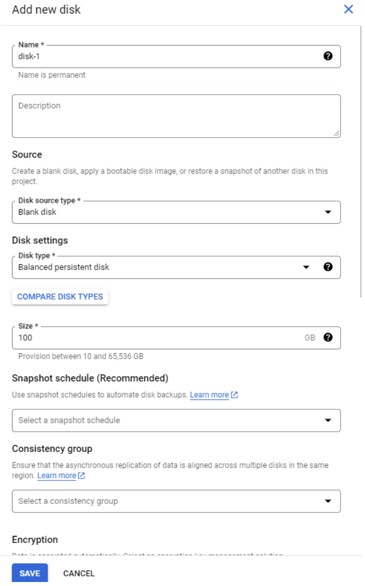
Network interface is permanent

test-vpc test-vpc-fortipam (10.110.0.0/24)

test-vpc-2 test-vpc-2-fortipam (10.180.0.0/24)

10. Expand *Advanced options* > *Disks*:
We create two disks; one for storing logs and the other for storing videos.

a. Select +*ADD NEW DISK*.
The *Add new disk* pane opens.



Add new disk

Name *: disk-1

Name is permanent

Description

Source

Create a blank disk, apply a bootable disk image, or restore a snapshot of another disk in this project.

Disk source type *: Blank disk

Disk settings

Disk type *: Balanced persistent disk

Size *: 100 GB

Provision between 10 and 65,536 GB

Snapshot schedule (Recommended)

Use snapshot schedules to automate disk backups. Learn more

Select a snapshot schedule

Consistency group

Ensure that the asynchronous replication of data is aligned across multiple disks in the same region. Learn more

Select a consistency group

Encryption

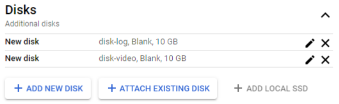
b. In *Name*, enter a name for the disk.

c. In *Size*, enter `10` (in GB) to add a new volume for the log.

d. Leave the remaining settings in the default state.

e. Click *Save*.

f. Repeat steps `a` to `e` to add a new volume for storing videos.



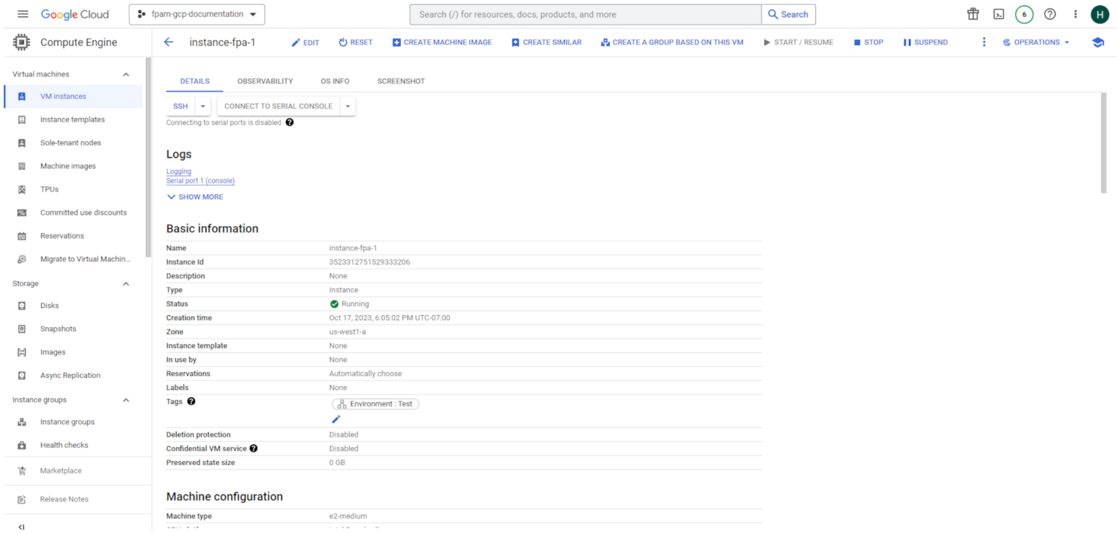
Disks

Additional disks

New disk	disk-log, Blank, 10 GB
New disk	disk-video, Blank, 10 GB

11. Click *CREATE*.

12. From the VM instance list, click the name of the VM instance you created.
The instance page opens.



Connecting to serial ports is disabled

Logs

Logging
Serial port 1 (console)
SHOW MORE

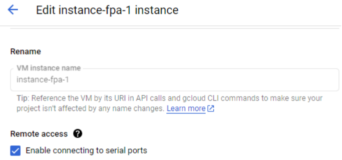
Basic information

Name	instance-fpa-1
Instance Id	3523312751529333206
Description	None
Type	Instance
Status	Running
Creation time	Oct 17, 2023, 6:05:02 PM UTC-07:00
Zone	us-west1-a
Instance template	None
In use by	None
Reservations	Automatically choose
Labels	None
Tags	Environment : Test
Deletion protection	Disabled
Confidential VM service	Disabled
Preserved state size	0 GB

Machine configuration

Machine type	e2-medium

13. Select *EDIT* and in *Remote access*, select *Enable connecting to serial ports*.



Edit instance-fpa-1 instance

Rename

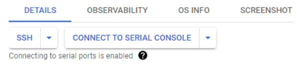
VM instance name: instance-fpa-1

Tip: Reference the VM by its URI in API calls and gcloud CLI commands to make sure your project isn't affected by any name changes. Learn more

Remote access

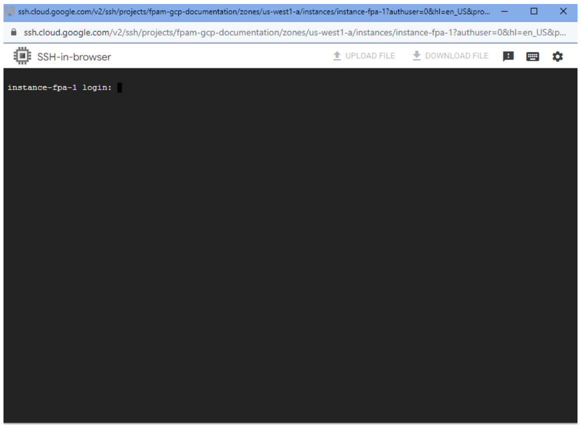
☑ Enable connecting to serial ports

14. Click *SAVE*.
15. In the instance page, select *CONNECT TO SERIAL CONSOLE*.



Connecting to serial ports is enabled

The SSH serial console opens.



ssh.cloud.google.com/v2/ssh/projects/fpam-gcp-documentation/zones/us-west1-a/instances/instance-fpa-1?authuser=0&hl=en_US&pro...

ssh.cloud.google.com/v2/ssh/projects/fpam-gcp-documentation/zones/us-west1-a/instances/instance-fpa-1?authuser=0&hl=en_US&p...

```
instance-fpa-1 login:
```

16. Use `admin` as the username and the *Instance Id* to log in for the first time.

Licensing

To successfully license FortiPAM:

1. Download the license file (`.lic`), see Registering and downloading your license.
2. Upload the license file from the public IP address using SCP, see Uploading the license file using SCP.

3. FortiPAM reboots. After a few minutes, the license status changes to valid.
   You can check the license status using the following CLI command:

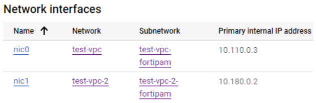
   ```
   get system status
   ```

Static interface IP address

You must use a static IP address if you intend to form an HA cluster.

To find out the static IP addresses that GCP has assigned to the interfaces:

1. From the navigation pane, go to *Compute Engine* > *VM instances*.
2. From the VM instances list, click the name of the VM instance you created.
3. In the *Network interfaces* pane, you see the static IP addresses assigned to the interfaces used in Creating VM instance from the image on page 509.
   Note down the IP addresses.



Network interfaces

Name ↑	Network	Subnetwork	Primary internal IP address
nic0	test-vpc	test-vpc-fortipam	10.110.0.3
nic1	test-vpc-2	test-vpc-2-fortipam	10.180.0.2

To configure port1, change mode from DHCP to static and set the IP address:

You can skip this step if FortiPAM is in standalone mode.

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

   ```
   config system interface
    edit port1
     set mode static #by default set as dhcp
     set ip 10.110.0.3/32 #set to the IP address assigned by GCP
    next
   end
   ```

When upgrading a FortiPAM instance, use the following CLI command to enable synchronizing the virtual IP address to the IP address of the external interface:

```
Example
```

```
 config firewall vip
  set intf-ip-sync enable
  set extintf "port1" #The interface connected to the source network
that receives the packets forwarded to the destination network.
 end
```

When installing a new FortiPAM instance, the synchronization happens automatically.

To configure a static route if the interface is configured as static mode:

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

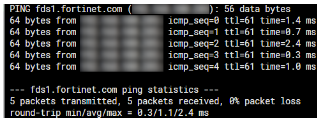
```
config router static
 edit 1
  set device port1
  set gateway 10.110.0.1
 next
end
```

To verify access to the public network:

1. Optionally, in the FortiPAM CLI console, enter the following command:

   ```
   execute ping update.fortiguard.net
   ```

   You should receive an echo reply packet similar to the following:



```
PING fds1.fortinet.com ([redacted]): 56 data bytes
64 bytes from [redacted] icmp_seq=0 ttl=61 time=1.4 ms
64 bytes from [redacted] icmp_seq=1 ttl=61 time=0.7 ms
64 bytes from [redacted] icmp_seq=2 ttl=61 time=2.4 ms
64 bytes from [redacted] icmp_seq=3 ttl=61 time=0.3 ms
64 bytes from [redacted] icmp_seq=4 ttl=61 time=1.0 ms

--- fds1.fortinet.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 0.3/1.1/2.4 ms
```

Optionally, to encrypt disk to protect logs and videos, see Configuring log and video disk encryption on page 347.

Optional- To customize VIP if default VIP is not preferred:

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

```
config firewall vip
 edit "fortipam_vip"
  set extip 10.110.0.3 #external visible virtual IP address
 next
end
```

You can now use your FortiPAM-VM deployed on GCP.

On a web browser, go to `https://<Public IP>` to access the FortiPAM-VM GUI. This is the same IP address set up above.

Setting up HA

Prerequisites

To deploy and configure FortiPAM as an Active-Passive HA solution, you need the following:

- Availability to accommodate the required GCP resources:
  - Four network/subnets
    - Ensure that the two FortiPAM devices have connectivity to each other on each network.
    - Appropriate ingress/egress firewall rules for relevant networks (same as a single FortiPAM-VM deployment).
  - Three public (external) IP addresses:

  - One for traffic to/through the active (primary) FortiPAM. At the event of failover, this IP address will move from the primary FortiPAM to the secondary. This must be a static external IP address. It should be reserved/created before creating FortiPAM instances, or promote an ephemeral IP to a static one after deployment. See Reserving a Static External IP Address.
  - Two for management access to each FortiPAM. They can be ephemeral IP address, but static ones are highly recommended. See IP Addresses.
- All internal IP addresses must be static, not DHCP. You should change ephemeral IP addresses to static ones after deployment. See Reserving a Static Internal IP Address.
- Two FortiPAM-VM instances:
  - The two nodes must be deployed in the same region/zone.
  - Each FortiPAM-VM must have at least four network interfaces.
  - Each FortiPAM-VM should have a log disk attached. Log disks should be created before deploying FortiPAM instances. This is the same requirement as when deploying a single FortiPAM-VM.
  - Machine types that support at least four network interfaces. Creating Instances with Multiple Network Interfaces.
  - Two valid FortiPAM-VM BYOL licenses. See Licensing on page 51.
- You must configure an SDN connector with GCP on the primary FortiPAM:

```
config system sdn-connector
 edit "gcp_conn"
 set type gcp
 set ha-status enable
 config external-ip
  edit "reserve-fpamhapublic"
  next
 end
 config route
  edit "route-internal"
  next
 end
 next
end
```

To set up a FortiPAM HA cluster:

1. To form an HA cluster, deploy two FortiPAM-VMs separately by following 1 - 6 in FortiPAM installation on GCP and initial setup.
2. As shown in Static interface IP address on page 514, note down the external IP addresses assigned to `nic0` for each FortiPAM. These are then used in step 3.
3. Connect to the primary FortiPAM external IP address using SSH, then enter the following CLI commands:

```
config system ha
 set group-name <choose a group name for the cluster>
 set mode active-passive
 set password <your-ha-password>
 set hbdev "port3" 100
 set ha-mgmt-status enable
 config ha-mgmt-interfaces
  edit 1
   set interface "port4"
   set gateway <ip address of MGMT network intrinsic router>
  next
  end
  set override enable
  set priority 255
  set unicast-status enable
  set unicast-gateway 10.4.100.254
  config unicast-peers
   edit 1
    set peer-ip 10.4.100.12
   next
  end
end
config system sdn-connector
 edit "gcp_conn"
 set type gcp
 set ha-status enable
 config external-ip
  edit "reserve-fpamhapublic"
  next
 end
 config route
  edit "route-internal"
  next
 end
 next
end
```

4. On the primary FortiPAM, enter the following CLI commands so that the interface IP address or the firewall VIP is not synchronized:

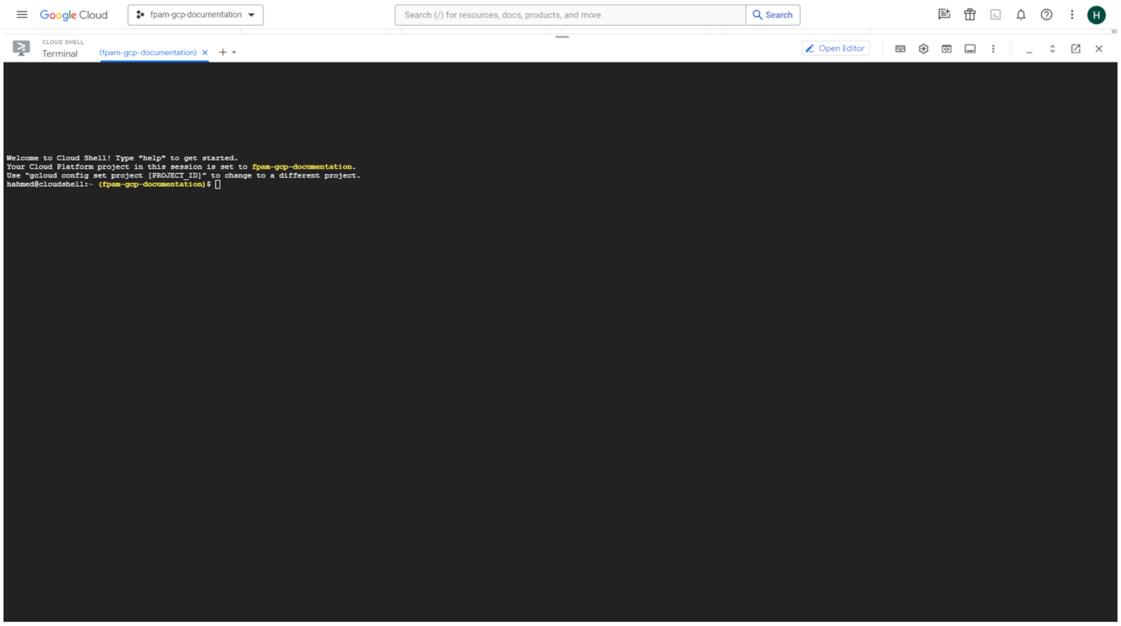
```
config system vdom-exception
 edit 1
  set object system.interface
 next
 edit 2
  set object firewall.vip
 next
end
```

This configuration is automatically synchronized once the secondary has been configured.

Enabling vTPM

To enable vTPM:

1. Add the FortiPAM image file to the storage bucket. See Adding the FortiPAM image file to the storage bucket on page 506.
2. From the top-right, select *Activate Cloud Shell*.
   The *CLOUD SHELL Terminal* opens.



```
Welcome to Cloud Shell! Type "help" to get started.
Your Cloud Platform project in this session is set to fpam-gcp-documentation.
Use "gcloud config set project [PROJECT_ID]" to change to a different project.
hahmed@cloudshell:~ (fpam-gcp-documentation)$ 
```

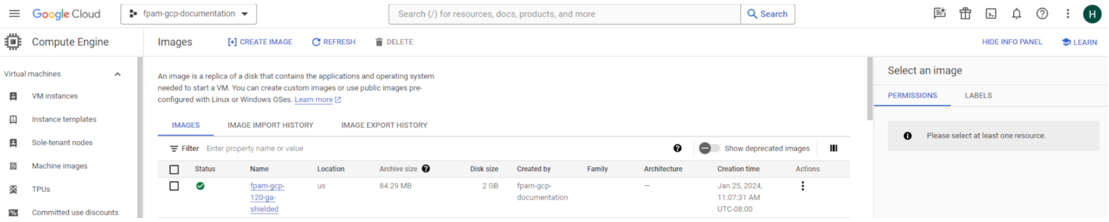
3. In the terminal, use the following commands to create a FortiPAM image:

   ```
    gcloud compute --project={project-name} images create gcp-fpa-{buildnum}-shielded --source-uri=https://storage.googleapis.com/{Bucket-name}/image.out.gcp.tar.gz --guest-os-features=UEFI_COMPATIBLE,GVNIC
   ```

   For example:

   ```
    gcloud compute --project=fpam-gcp-documentation images create fpam-gcp-120-ga-shielded --source-uri=https://storage.googleapis.com/fortipam-bucket/FPA_KVM_GCP-v100-build0697-FORTINET.out.gcp.tar.gz --guest-os-features=UEFI_COMPATIBLE,GVNIC
   ```

   A new image is created in *Compute Engine* > *Storage* > *Images*.

   An image is a replica of a disk that contains the applications and operating system needed to start a VM. You can create custom images or use public images pre-configured with Linux or Windows OSes. Learn more

☐	Status	Name	Location	Archive size	Disk size	Created by	Family	Architecture	Creation time	Actions
☐	✓	fpam-gcp-120-ga-shielded	us	84.29 MB	2 GB	fpam-gcp-documentation		–	Jan 25, 2024, 11:07:31 AM UTC-08:00	⋮

   Please select at least one resource.

4. Create the FortiPAM VM using the image created in step 3. See Creating VM instance from the image on page 509. When creating the VM, in *Advanced options* > *Security*, ensure that *Turn on vTPM* and *Turn on Integrity Monitoring* is enabled.
5. Once the VM is ready, in the SSH serial console, enter the following commands to verify that vTPM is enabled:

   ```
    diagnose tpm selftest
   ```

   The following message appears if vTPM was successfully set up:

   ```
   Successfully tested. Works as expected.
   ```

Appendix L: WinRM configuration for Windows server

WinRM is needed for agentless RDP session log retrieving.

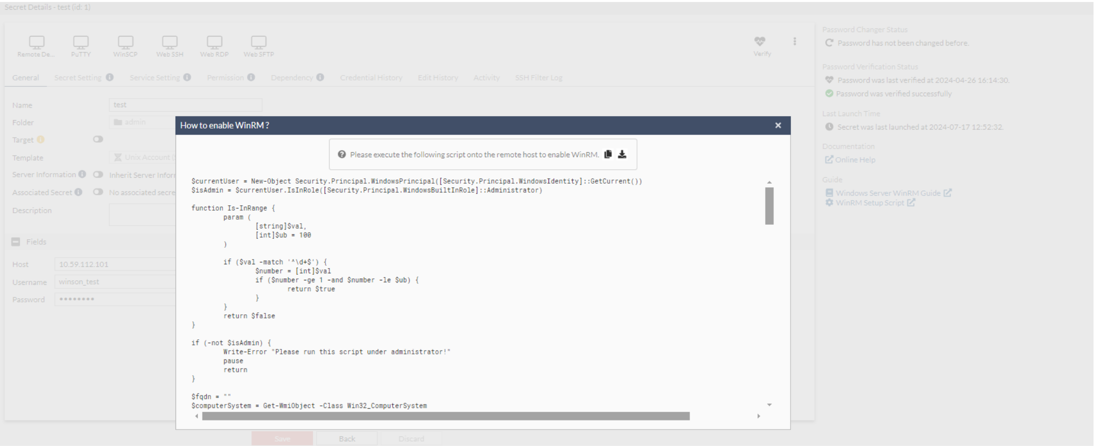
Use the commands as shown below to enable WinRM and set authentication on the target Windows servers.

1. Quick setup with script from FortiPAM on page 519
2. Executing the script on the sever with administrative privileges on page 519
3. Configuring WinRM on the server manually on page 520
4. Creating a privileged account on page 523

To setup WinRM on a Windows server, you can copy the WinRM setup script (recommended) from FortiPAM and execute the script on the Windows server or do it manually.

Quick setup with script from FortiPAM

1. Go to *Secrets* > *Secrets*.
2. From the list, double-click to open the secret.
3. Click *WinRM Setup Script*on the right to open the script.



Name: test
Folder: admin
Template: Unix Account (
Server Information: Inherit Server Infor
Associated Secret: No associated secre
Host: 10.59.112.101
Username: winson_test
Password: ••••••••

Password has not been changed before.

Password was last verified at 2024-04-26 16:14:30.

Password was verified successfully

Secret was last launched at 2024-07-17 12:52:32.

How to enable WinRM ?

Please execute the following script onto the remote host to enable WinRM.

```
$currentUser = New-Object Security.Principal.WindowsPrincipal([Security.Principal.WindowsIdentity]::GetCurrent())
$isAdmin = $currentUser.IsInRole([Security.Principal.WindowsBuiltInRole]::Administrator)

function Is-InRange {
        param (
                [string]$val,
                [int]$ub = 100
        )

        if ($val -match '^\d+$') {
                $number = [int]$val
                if ($number -ge 1 -and $number -le $ub) {
                        return $true
                }
        }
        return $false
}

if (-not $isAdmin) {
        Write-Error "Please run this script under administrator!"
        pause
        return
}

$fqdn = ""
$computerSystem = Get-WmiObject -Class Win32_ComputerSystem
```

4. Click *Download script* to download the script to your management computer. Alternatively, click *Copy script* to copy the script.

Executing the script on the sever with administrative privileges

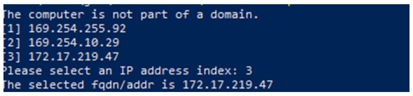
To execute the script on the server with administrative privileges:

1. Before executing the scripts on a newly installed machine or one that has never been configured for WinRM, please initiate *winrm qc* first in PowerShell.
2. Run the scripts in PowerShell with administrative privileges using the following command:

   ```
   powershell.exe -ExecutionPolicy Bypass -File auto_winrm.ps1
   ```

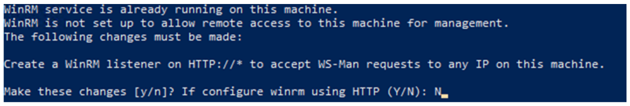
   Alternatively, use the following command:

```
powershell.exe auto_winrm.ps1
```



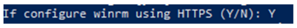
```
The computer is not part of a domain.
[1] 169.254.255.92
[2] 169.254.10.29
[3] 172.17.219.47
Please select an IP address index: 3
The selected fqdn/addr is 172.17.219.47
```

3. Choose the correct IP address as the hostname if the computer is not part of a domain. Otherwise, it uses the FQDN as the hostname.
4. Choose if you want to configure HTTP listening for WinRM.



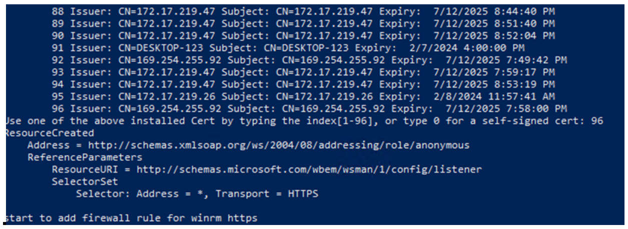
```
WinRM service is already running on this machine.
WinRM is not set up to allow remote access to this machine for management.
The following changes must be made:

Create a WinRM listener on HTTP://* to accept WS-Man requests to any IP on this machine.

Make these changes [y/n]? If configure winrm using HTTP (Y/N): N
```

5. Choose if you want to configure HTTPS listener for WinRM.



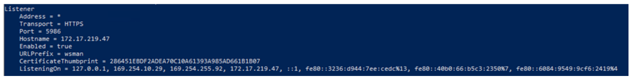
```
If configure winrm using HTTPS (Y/N): Y
```

6. If HTTPS is selected and there are already certificates installed, choose the one by index or enter `0` to create a self-signed certificate.



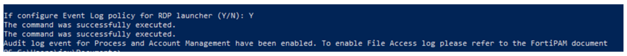
```
        88 Issuer: CN=172.17.219.47 Subject: CN=172.17.219.47 Expiry:  7/12/2025 8:44:40 PM
        89 Issuer: CN=172.17.219.47 Subject: CN=172.17.219.47 Expiry:  7/12/2025 8:51:40 PM
        90 Issuer: CN=172.17.219.47 Subject: CN=172.17.219.47 Expiry:  7/12/2025 8:52:04 PM
        91 Issuer: CN=DESKTOP-123 Subject: CN=DESKTOP-123 Expiry:  2/7/2024 4:00:00 PM
        92 Issuer: CN=169.254.255.92 Subject: CN=169.254.255.92 Expiry:  7/12/2025 7:49:42 PM
        93 Issuer: CN=172.17.219.47 Subject: CN=172.17.219.47 Expiry:  7/12/2025 7:59:17 PM
        94 Issuer: CN=172.17.219.47 Subject: CN=172.17.219.47 Expiry:  7/12/2025 8:53:19 PM
        95 Issuer: CN=172.17.219.26 Subject: CN=172.17.219.26 Expiry:  2/8/2024 11:57:41 AM
        96 Issuer: CN=169.254.255.92 Subject: CN=169.254.255.92 Expiry:  7/12/2025 7:58:00 PM
Use one of the above installed Cert by typing the index[1-96], or type 0 for a self-signed cert: 96
ResourceCreated
    Address = http://schemas.xmlsoap.org/ws/2004/08/addressing/role/anonymous
    ReferenceParameters
        ResourceURI = http://schemas.microsoft.com/wbem/wsman/1/config/listener
        SelectorSet
            Selector: Address = *, Transport = HTTPS

start to add firewall rule for winrm https
```

The firewall rules for listeners is enabled and the list of all the listeners is displayed.



```
Listener
    Address = *
    Transport = HTTPS
    Port = 5986
    Hostname = 172.17.219.47
    Enabled = true
    URLPrefix = wsman
    CertificateThumbprint = 286451EBDF2ADEA70C10A61393A985AD661B1B07
    ListeningOn = 127.0.0.1, 169.254.10.29, 169.254.255.92, 172.17.219.47, ::1, fe80::3236:d944:7ee:cedc%13, fe80::40b0:66:b5c3:2350%7, fe80::6084:9549:9cf6:2419%4
```

7. Finally, choose if you want to enable Event log policy for RDP log retrieval feature.



```
If configure Event Log policy for RDP launcher (Y/N): Y
The command was successfully executed.
The command was successfully executed.
Audit log event for Process and Account Management have been enabled. To enable File Access log please refer to the FortiPAM document
```

Configuring WinRM on the server manually

Alternatively, you can configure WinRM manually.

To configure WinRM on the server manually:

1. Open the Windows PowerShell console as an administrator and enter the following command:

   ```
   winrm quickconfig
   ```

   The command enables WinRM service with default setting.
2. If WinRM over HTTPS is required for enhanced security, add an HTTPS listener:
   a. If the server has already been issued a certificate in the local certificate store, use the following command:

      ```
      Get-ChildItem -Path Cert:\LocalMachine\My
      ```

      This lists all the certificates in `Cert:\LocalMachine\My`.

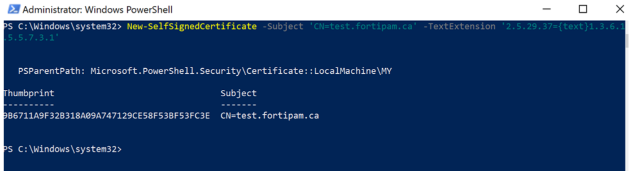
      Choose one and copy the thumbprint for later use.

   b. If the server needs a self-signed certificate, use the following command:

      ```
      New-SelfSignedCertificate -Subject 'CN=<windows host name>' -TextExtension
      '2.5.29.37={text}1.3.6.1.5.5.7.3.1'
      ```

Replace `<windows host name>` with the actual hostname (FQDN or an IP address of the server).

After running the above command, the result is displayed with the thumbprint.



```
PS C:\Windows\system32> New-SelfSignedCertificate -Subject 'CN=test.fortipam.ca' -TextExtension '2.5.29.37={text}1.3.6.1
.5.5.7.3.1'


   PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\MY

Thumbprint                                Subject
----------                                -------
9B6711A9F32B318A09A747129CE58F53BF53FC3E  CN=test.fortipam.ca


PS C:\Windows\system32>
```

c. Add an HTTPS listener using the following command:

```
 winrm create winrm/config/Listener?Address=*+Transport=HTTPS '@{Hostname="<windows
host name>"; CertificateThumbprint="<thumbprint received by New-Self Signed
Certificate>"}'
```

Replace `<windows host name>` with the one used in step b.

Replace the `<thumbprint received by New-Self Signed Certificate>` with the thumbprint from step a or b.

3. Use the following command to see if everything works correctly:

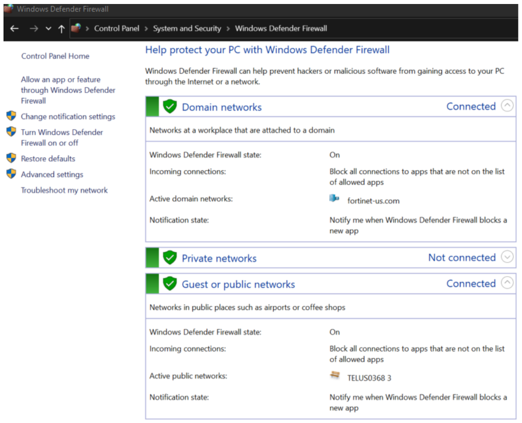
```
winrm enumerate winrm/config/listener
```

The above command should display the corresponding listener in the console.

4. Configure the firewall rules for WinRM:
WinRM traffic (5985 for HTTP, 5986 for HTTPs) can be blocked by default on some Windows servers or cloud platforms. Ensure that the WinRM traffic is allowed for RDP log retrieving.

Enabling Windows Remote Management

a. On the target Windows server, go to *Control Panel* > *System and Security* > *Windows Defender Firewall*.


Windows Defender Firewall
Control Panel > System and Security > Windows Defender Firewall
Control Panel Home
Allow an app or feature through Windows Defender Firewall
Change notification settings
Turn Windows Defender Firewall on or off
Restore defaults
Advanced settings
Troubleshoot my network

Help protect your PC with Windows Defender Firewall

Windows Defender Firewall can help prevent hackers or malicious software from gaining access to your PC through the Internet or a network.

Domain networks — Connected

Networks at a workplace that are attached to a domain

Windows Defender Firewall state: On
Incoming connections: Block all connections to apps that are not on the list of allowed apps
Active domain networks: fortinet-us.com
Notification state: Notify me when Windows Defender Firewall blocks a new app

Private networks — Not connected

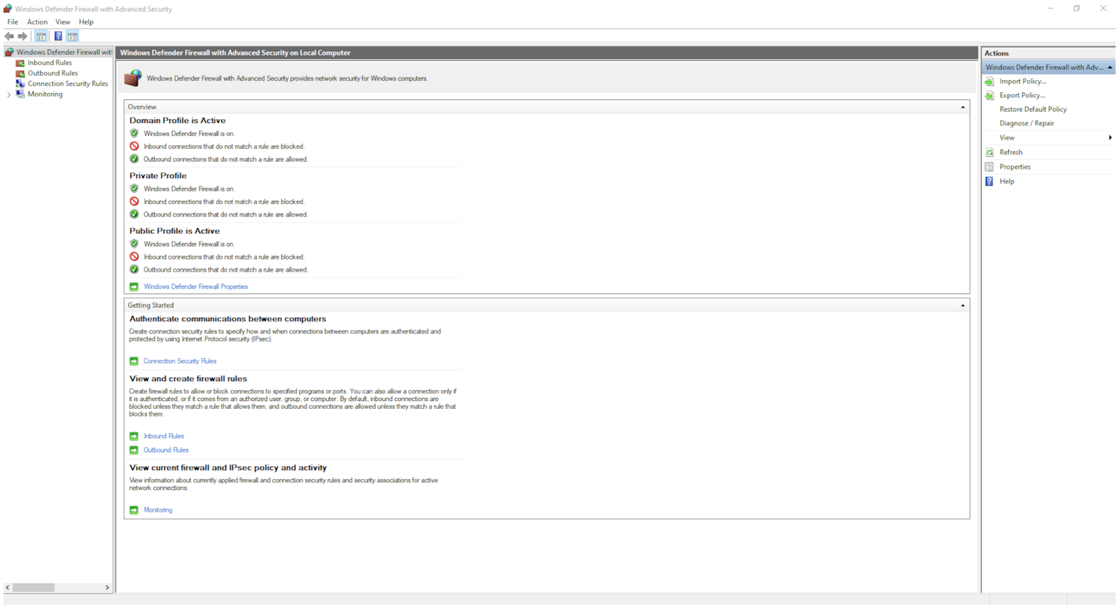
Guest or public networks — Connected

Networks in public places such as airports or coffee shops

Windows Defender Firewall state: On
Incoming connections: Block all connections to apps that are not on the list of allowed apps
Active public networks: TELUS0368 3
Notification state: Notify me when Windows Defender Firewall blocks a new app

b. From the menu on the left, select *Advanced settings*.

c. In the *User Account Control* dialog that opens, click *Yes*.
A new window opens.



Windows Defender Firewall with Advanced Security on Local Computer

Windows Defender Firewall with Advanced Security provides network security for Windows computers.

Overview

Domain Profile is Active

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Private Profile

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Public Profile is Active

- Windows Defender Firewall is on.
- Inbound connections that do not match a rule are blocked.
- Outbound connections that do not match a rule are allowed.

Windows Defender Firewall Properties

Getting Started

Authenticate communications between computers

Create connection security rules to specify how and when connections between computers are authenticated and protected by using Internet Protocol security (IPsec).

Connection Security Rules

View and create firewall rules

Create firewall rules to allow or block connections to specified programs or ports. You can also allow a connection only if it is authenticated, or if it comes from an authorized user, group, or computer. By default, inbound connections are blocked unless they match a rule that allows them, and outbound connections are allowed unless they match a rule that blocks them.

Inbound Rules

Outbound Rules

View current firewall and IPsec policy and activity

View information about currently applied firewall and connection security rules and security associations for active network connections.

Monitoring

d. From the menu on the left, select *Inbound Rules*.

e. In the *Inbound Rules* window, according to your network topology, right-click *Windows Remote Management* and select *Enable Rule*.

5. **Audit policy setting for RDP log retrieving**:

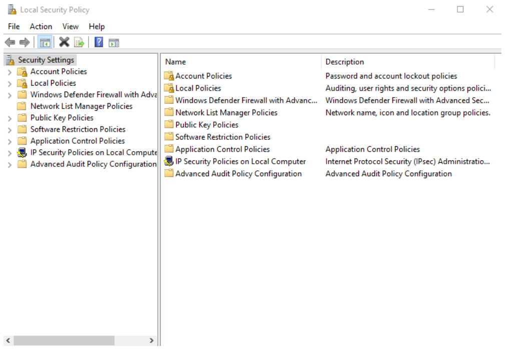
a. Log in to the Windows machine to configure the policy as an administrator.

b. Go to *Control Panel > System and Security*.

c. Click *Administrative Tools* and in the new window that opens, double-click *Local Security Policy*.

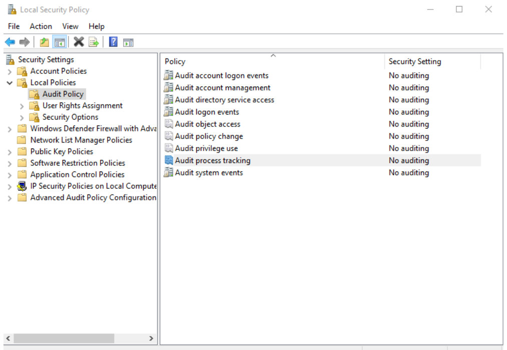
d. In the the *User Account Control* dialog that opens, click *Yes*.

The *Local Security Policy* window opens.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Name	Description
Account Policies	Password and account lockout policies
Local Policies	Auditing, user rights and security options polici...
Windows Defender Firewall with Advanc...	Windows Defender Firewall with Advanced Sec...
Network List Manager Policies	Network name, icon and location group policies.
Public Key Policies	
Software Restriction Policies	
Application Control Policies	Application Control Policies
IP Security Policies on Local Computer	Internet Protocol Security (IPsec) Administratio...
Advanced Audit Policy Configuration	Advanced Audit Policy Configuration

e. From the navigation pane on the left, expand *Local Policies > Audit Policy*.


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Defender Firewall with Adva
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration

Policy	Security Setting
Audit account logon events	No auditing
Audit account management	No auditing
Audit directory service access	No auditing
Audit logon events	No auditing
Audit object access	No auditing
Audit policy change	No auditing
Audit privilege use	No auditing
Audit process tracking	No auditing
Audit system events	No auditing

f. For the event filter profile that applies to the privileged account secret on FortiPAM:
   i. If *Process Log* is set to *Monitor*, set *Audit process tracking* as success and failure by right-clicking *Audit process tracking*, selecting *Properties*, selecting *Success* and *Failure*, and clicking *OK*.
   ii. If *Filesystem Log* is set to *Monitor*, set *Audit object access* as success and failure by right-clicking *Audit object access*, selecting *Properties*, selecting *Success* and *Failure*, and clicking *OK*.

> When you enable the policy to audit object access events, you must specify which files, folders, and user actions are logged.
>
> You must be specific with the setting to avoid excessive logging.

   iii. If *User Management Log* is set to *Monitor*, set *Audit account management* as success and failure by right-clicking *Audit account management*, selecting *Properties*, selecting *Success* and *Failure*, and clicking *OK*.

g. Log in to the Windows machine to configure policy and administrator privileges.

h. On the Windows machine, open *File Explorer*, right-click the file you intend to set the auditing policy for, and select *Properties*:
   i. Go to the *Security* tab, click *Advanced*.
   ii. Go to the *Auditing* tab, click *Continue*.
   iii. In the *User Account Control* dialog, click *Yes*.
   iv. Click *Add*.

> The *Add* button is labelled *Edit* on Windows 8.

   v. In the new window that opens, click *Select a principal*.
   vi. In *Select User, Computer, Service Account, or Group*, click *Advanced*.
   vii. Select users whose access to the file you want to monitor.
   viii. Click *OK*.
   ix. In the *Permissions* tab, set the permission for each of the user you have added.
   x. Click *OK*.

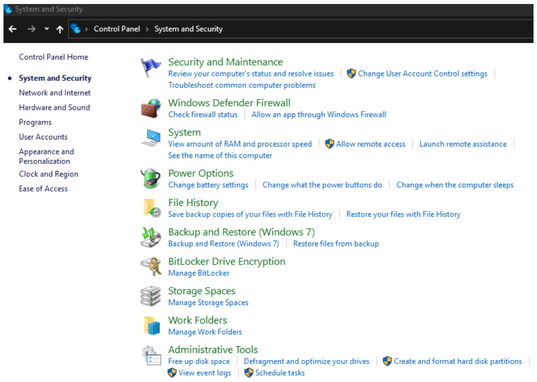
i. Click *OK*.
   The configuration is now complete. Windows will generate audit events when the users you have specified takes actions on the files or folders for which you have set up audit policies.

Creating a privileged account

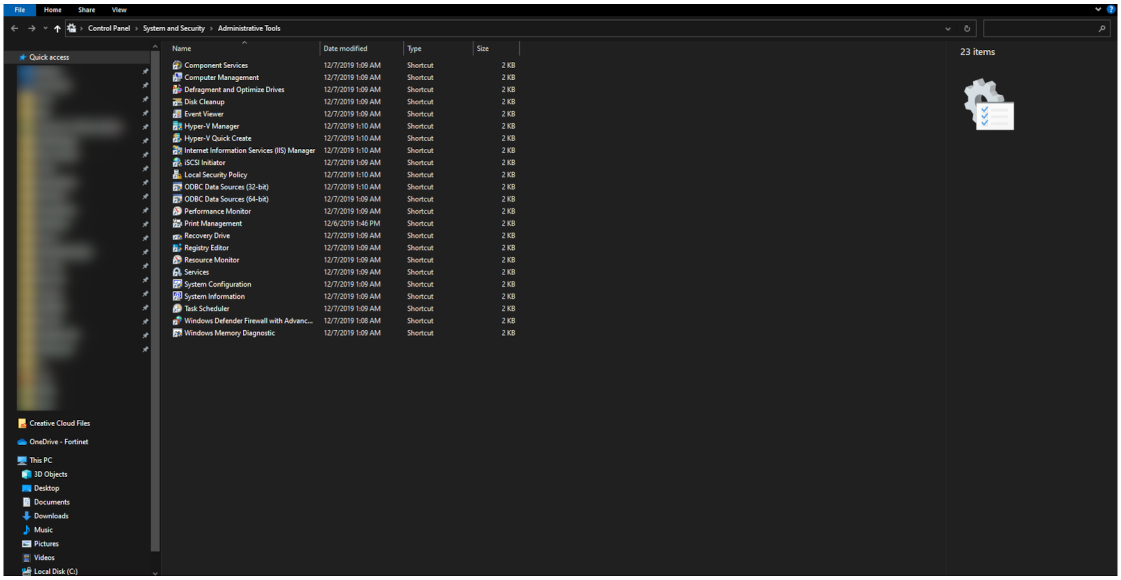
We create a new user belonging to the administrators groups.

To create a privileged account:

1. Go to *Control Panel > System and Security*.

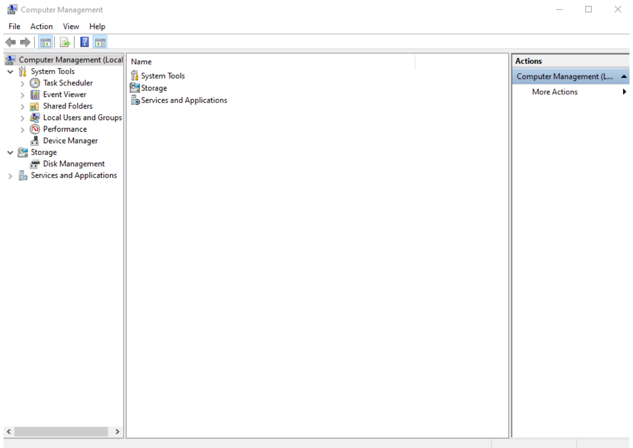

System and Security
Control Panel › System and Security
Control Panel Home
System and Security
Network and Internet
Hardware and Sound
Programs
User Accounts
Appearance and Personalization
Clock and Region
Ease of Access
Security and Maintenance
Review your computer's status and resolve issues | Change User Account Control settings | Troubleshoot common computer problems
Windows Defender Firewall
Check firewall status | Allow an app through Windows Firewall
System
View amount of RAM and processor speed | Allow remote access | Launch remote assistance | See the name of this computer
Power Options
Change battery settings | Change what the power buttons do | Change when the computer sleeps
File History
Save backup copies of your files with File History | Restore your files with File History
Backup and Restore (Windows 7)
Backup and Restore (Windows 7) | Restore files from backup
BitLocker Drive Encryption
Manage BitLocker
Storage Spaces
Manage Storage Spaces
Work Folders
Manage Work Folders
Administrative Tools
Free up disk space | Defragment and optimize your drives | Create and format hard disk partitions | View event logs | Schedule tasks

2. Click *Administrative Tools*.
3. In the *User Account Control* dialog that opens, click *Yes*.
   A new window opens.

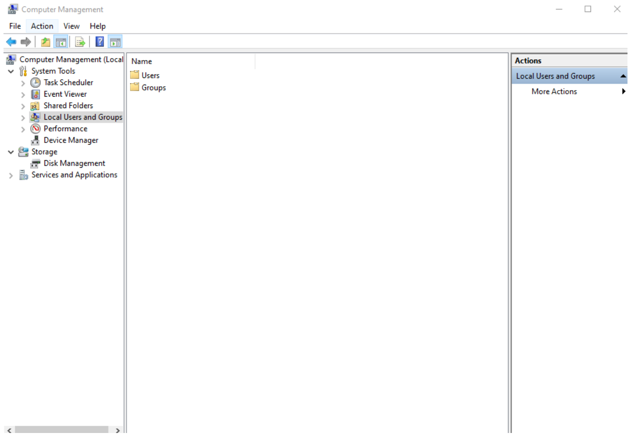


Name	Date modified	Type	Size
Component Services	12/7/2019 1:09 AM	Shortcut	2 KB
Computer Management	12/7/2019 1:09 AM	Shortcut	2 KB
Defragment and Optimize Drives	12/7/2019 1:09 AM	Shortcut	2 KB
Disk Cleanup	12/7/2019 1:09 AM	Shortcut	2 KB
Event Viewer	12/7/2019 1:09 AM	Shortcut	2 KB
Hyper-V Manager	12/7/2019 1:10 AM	Shortcut	2 KB
Hyper-V Quick Create	12/7/2019 1:10 AM	Shortcut	2 KB
Internet Information Services (IIS) Manager	12/7/2019 1:10 AM	Shortcut	2 KB
iSCSI Initiator	12/7/2019 1:09 AM	Shortcut	2 KB
Local Security Policy	12/7/2019 1:10 AM	Shortcut	2 KB
ODBC Data Sources (32-bit)	12/7/2019 1:10 AM	Shortcut	2 KB
ODBC Data Sources (64-bit)	12/7/2019 1:09 AM	Shortcut	2 KB
Performance Monitor	12/7/2019 1:09 AM	Shortcut	2 KB
Print Management	12/6/2019 1:46 PM	Shortcut	2 KB
Recovery Drive	12/7/2019 1:09 AM	Shortcut	2 KB
Registry Editor	12/7/2019 1:09 AM	Shortcut	2 KB
Resource Monitor	12/7/2019 1:09 AM	Shortcut	2 KB
Services	12/7/2019 1:09 AM	Shortcut	2 KB
System Configuration	12/7/2019 1:09 AM	Shortcut	2 KB
System Information	12/7/2019 1:09 AM	Shortcut	2 KB
Task Scheduler	12/7/2019 1:09 AM	Shortcut	2 KB
Windows Defender Firewall with Advanc...	12/7/2019 1:08 AM	Shortcut	2 KB
Windows Memory Diagnostic	12/7/2019 1:09 AM	Shortcut	2 KB

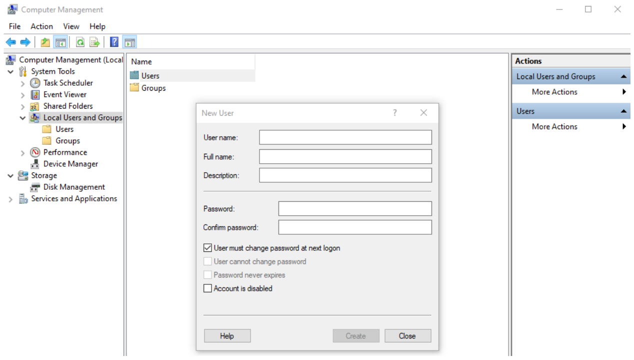
4. Double-click *Computer Management* to open it.
5. In the *User Account Control* dialog that opens, click *Yes*.
   The *Computer Management* window opens.



6. From the navigation pane on the left, select *Local Users and Groups*.



7. Right-click the *Users* folder and select *New User...*.
   The *New User* dialog opens.



☑ User must change password at next logon
□ User cannot change password
□ Password never expires
□ Account is disabled

8. In the *New User* dialog:
   a. In *User name*, enter a username.
   b. In *Full name*, enter the full name of the user.
   c. In *Description*, enter a description for the user.
   d. In *Password*, enter a password.
   e. In *Confirm password*, enter the password again to confirm.
   f. Click *Create* to create the user.
9. Double-click the *Users* folder, right-click the user that was created in step 8, and select *Properties*.

10. In the new dialog that opens, go to the *Member Of tab*, select *Administrators*, and click *Add...*.
11. Click *OK* to save changes.

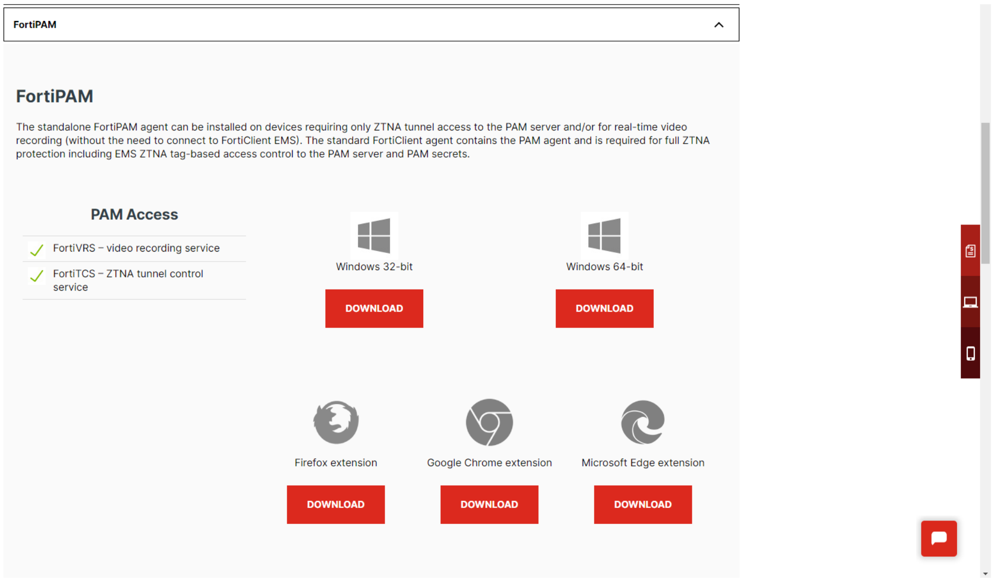
> If you intend to retrieve RDP logs for the privileged account, you must create a secret for the privileged account with a Windows target. See Creating a secret on page 72.

Appendix M: FortiPAM browser extension and standalone FortiClient air-gapped installation

To install FortiPAM browser extension:

The FortiPAM Firefox extension is installed automatically when you install the standalone FortiClient.

1. Go to Fortinet Product Downloads center.
2. From the list, click *FortiPAM* to expand it.



FortiPAM

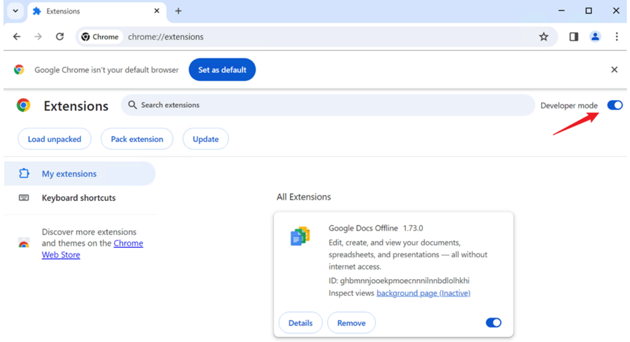
The standalone FortiPAM agent can be installed on devices requiring only ZTNA tunnel access to the PAM server and/or for real-time video recording (without the need to connect to FortiClient EMS). The standard FortiClient agent contains the PAM agent and is required for full ZTNA protection including EMS ZTNA tag-based access control to the PAM server and PAM secrets.

PAM Access

- ✓ FortiVRS – video recording service
- ✓ FortiTCS – ZTNA tunnel control service

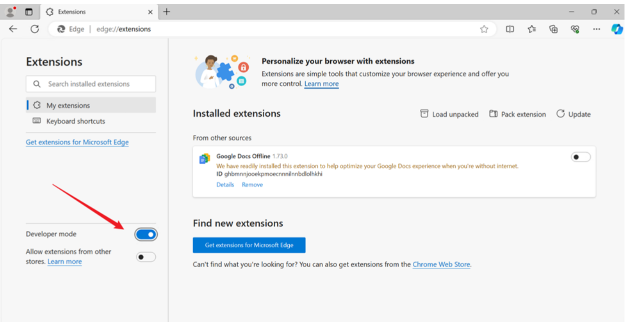
3. Click the *DOWNLOAD* button below the browser icon to download the required FortiPAM browser extension:
   a. *Google Chrome*: `fortipam-chrome-extension.crx`
   b. *Microsoft Edge*: `fortipam-edge-extension.crx`
   c. *Mozilla Firefox*: `fortipam-firefox-extension.xpi`
4. Copy the downloaded FortiPAM browser extension file to the air-gapped computer.
5. On the air-gappend computer, in a web browser window, open the web extensions page using the following URL:
   a. *Google Chrome*: chrome://extensions
   b. *Microsoft Edge*: edge://extensions
   c. *Mozilla Firefox*: about:addons
6. Enable *Developer mode* on the web browser and refresh the web page:
   Note: On Mozilla Firefox, you do not need to explicitly enable the developer mode.

a. On Google Chrome:



Google Docs Offline 1.73.0
Edit, create, and view your documents, spreadsheets, and presentations — all without internet access.
ID: ghbmnnjooekpmoecnnnilnnbdlolhkhi
Inspect views background page (Inactive)

b. On Microsoft Edge:



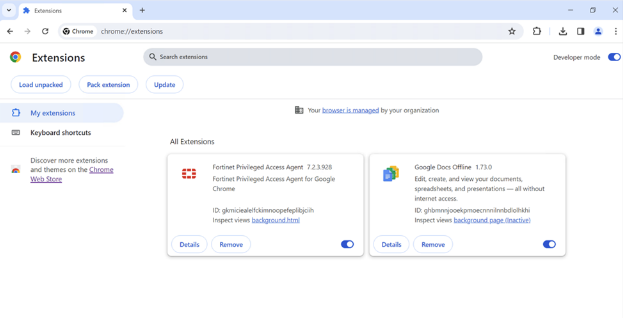
Extensions are simple tools that customize your browser experience and offer you more control. Learn more

Google Docs Offline 1.73.0
We have readily installed this extension to help optimize your Google Docs experience when you're without internet.
ID ghbmnnjooekpmoecnnnilnnbdlolhkhi

Can't find what you're looking for? You can also get extensions from the Chrome Web Store.

7. Drag and drop the FortiPAM browser extension file to the extension page, and install the browser extension by clicking *Add Extension*.

a. On Google Chrome:

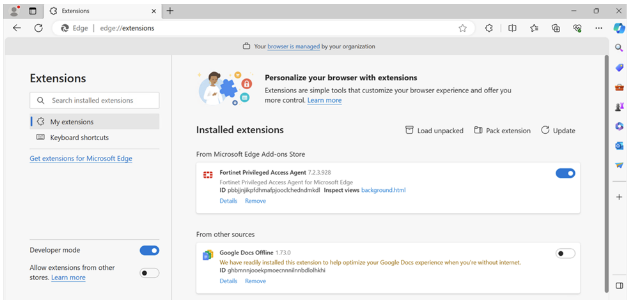


Your browser is managed by your organization

Fortinet Privileged Access Agent 7.2.3.928
Fortinet Privileged Access Agent for Google Chrome
ID: gkmiciealelfckimnoopefeplibjciih
Inspect views background.html

Google Docs Offline 1.73.0
Edit, create, and view your documents, spreadsheets, and presentations — all without internet access.
ID: ghbmnnjooekpmoecnnnilnnbdlolhkhi
Inspect views background page (Inactive)

b. On Microsoft Edge:


Extensions
edge://extensions
Extensions
Search installed extensions
My extensions
Keyboard shortcuts
Get extensions for Microsoft Edge
Developer mode
Allow extensions from other stores. Learn more
Personalize your browser with extensions
Installed extensions
Load unpacked
Pack extension
Update
From Microsoft Edge Add-ons Store
From other sources
Details
Remove
Details
Remove

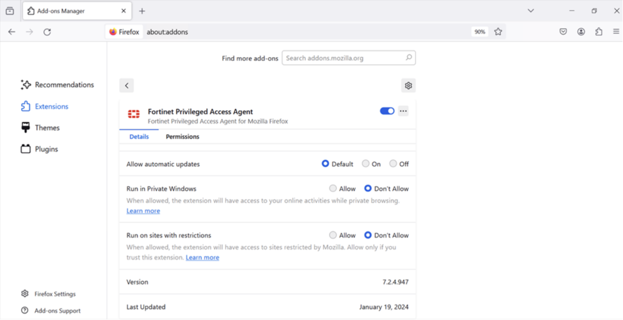
Your browser is managed by your organization

Extensions are simple tools that customize your browser experience and offer you more control. Learn more

Fortinet Privileged Access Agent 7.2.3.928
Fortinet Privileged Access Agent for Microsoft Edge
ID pbbjjnjikpfdhmafpjooclchedndmkdl Inspect views background.html

Google Docs Offline 1.73.0
We have readily installed this extension to help optimize your Google Docs experience when you're without internet.
ID ghbmnnjooekpmoecnnnilnnbdlolhkhi

c. On Mozilla Firefox:



Fortinet Privileged Access Agent
Fortinet Privileged Access Agent for Mozilla Firefox

Allow automatic updates ● Default ○ On ○ Off

Run in Private Windows ○ Allow ● Don't Allow
When allowed, the extension will have access to your online activities while private browsing. Learn more

Run on sites with restrictions ○ Allow ● Don't Allow
When allowed, the extension will have access to sites restricted by Mozilla. Allow only if you trust this extension. Learn more

Version 7.2.4.947

Last Updated January 19, 2024

To install standalone FortiClient:

The standalone FortiClient requires FortiPAM browser extension to offer PAM related functionalities.

You must install FortiPAM browser extension.

The standalone FortiClient and the FortiPAM browser extension can be installed in any order.

1. Go to Fortinet Product Downloads center.
2. From the list, click *FortiPAM* to expand it.
3. Click the *DOWNLOAD* button below *Windows 64-bit* or *Windows 32-bit* icon to download standalone FortiClient.
4. Copy the downloaded FortiClient installation file to the air-gapped computer.
5. On the air-gapped computer, double-click the FortiClient installation file to install it.

Appendix N: Performance test results

FortiPAM is a cutting edge platform that inherits the high performance design of the FortiOS platform.

The FortiPAM platform is capable of:

- Dynamically distributing tasks across multiple CPUs to load balance workload.
- Improves CPU performance by caching the frequently accessed data.
- Using asynchronous I/O techniques elevates hard disk and network performance.

FortiPAM-VM minimum requirements based on different user seats

SKU	Seats	vCPUs	Memory (GB)	Log disk (GB)	Video disk (GB)
FC1-10-PAVUL-591-02-12	<10	2	8	20	150
FC2-10-PAVUL-591-02-12	<25	4	8	40	300
FC3-10-PAVUL-591-02-12	<50	4	8	100	500
FC4-10-PAVUL-591-02-12	<100	8	16	200	1 TB
FC5-10-PAVUL-591-02-12	<250	16	16	400	1 TB

Larger log and video disks are preferred.

FortiPAM-VM performance as tested in the lab

VM configuration

Dell server

- PowerEdge R450 Server
- Intel Xeon Silver 4310 2.1G, 12C/24T, 10.4GT/s, 18M Cache, Turbo

CPU cores

- 16

Memory

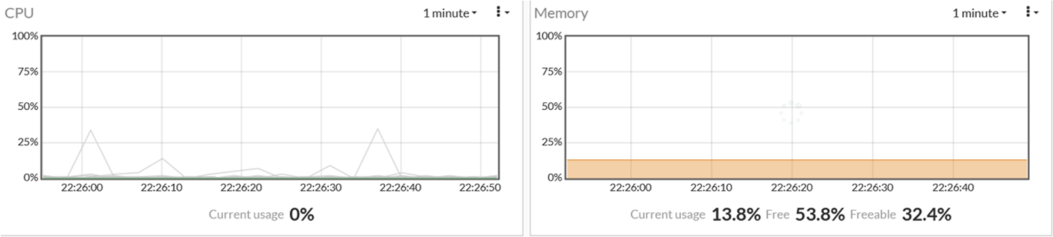
- 16 GB

Results

Keep 1000 launching sessions of SSH and Web SSH

- SSH traffic speed: 1 ssh command/per session/per second
- Video recording: 60K bytes/per session/per second

CPU and *Memory* widget in the *Dashboard* page

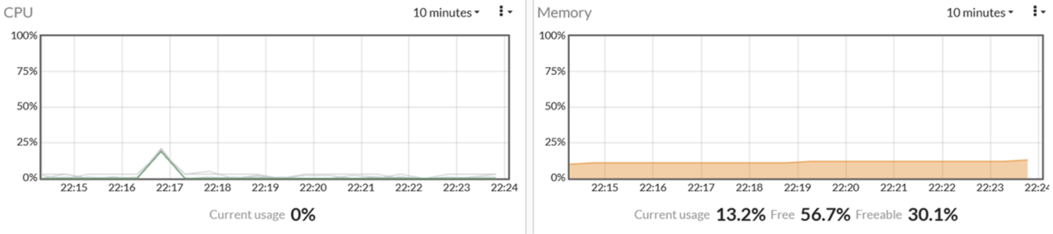


Note: The data was collected from the test performed in the FortiPAM lab.

Keep 90 launching session of Web RDP

- Video recording enabled
- Windows desktop page keeps refreshing the Task Manager window

CPU and *Memory* widget in the *Dashboard* page



Note: The data was collected from the test performed in the FortiPAM lab.

Appendix O: How to find a selector - Example

Selectors help you precisely locate elements on a web page.

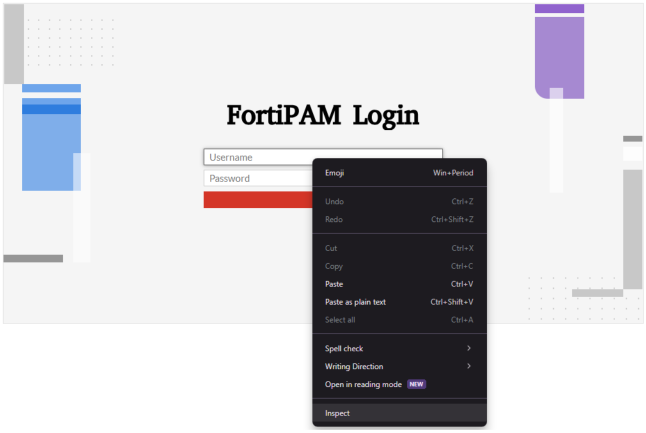
To find the appropriate selector for an input field, you can use the web browser inspection tool.

Example 1

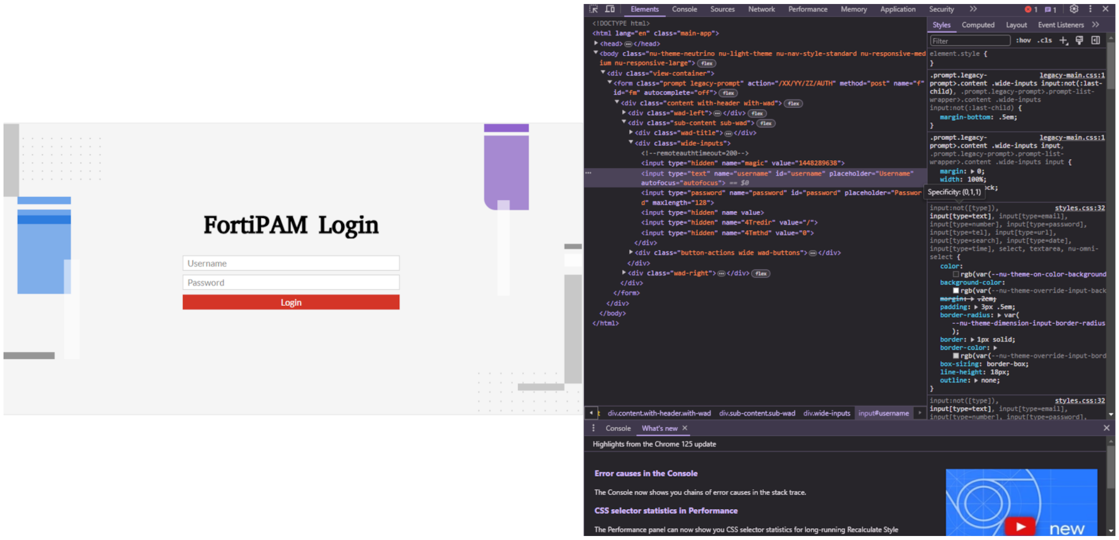
Finding selector for the *Username* field on the FortiPAM login page using the Google Chrome web browser

To find the selector for the *Username* field:

1. On the FortiPAM login page, right-click the *Username* field and select *Inspect*.



The HTML code for the *Username* field is highlighted in the Chrome developer tool.



```
<!DOCTYPE html>
<html lang="en" class="main-app">
 ▶<head>⋯</head>
 ▼<body class="nu-theme-neutrino nu-light-theme nu-nav-style-standard nu-responsive-medium nu-responsive-large"> flex
   ▼<div class="view-container">
     ▼<form class="prompt legacy-prompt" action="/XX/YY/ZZ/AUTH" method="post" name="f" id="fm" autocomplete="off"> flex
       ▼<div class="content with-header with-wad"> flex
         ▶<div class="wad-left">⋯</div> flex
         ▼<div class="sub-content sub-wad"> flex
           ▶<div class="wad-title">⋯</div>
           ▼<div class="wide-inputs">
              <!--remoteauthtimeout=200-->
              <input type="hidden" name="magic" value="1448289638">
              <input type="text" name="username" id="username" placeholder="Username" autofocus="autofocus"> == $0
              <input type="password" name="password" id="password" placeholder="Password" maxlength="128">
              <input type="hidden" name value>
              <input type="hidden" name="4Tredir" value="/">
              <input type="hidden" name="4Tmthd" value="0">
            </div>
           ▶<div class="button-actions wide wad-buttons">⋯</div>
          </div>
         ▶<div class="wad-right">⋯</div> flex
        </div>
      </form>
    </div>
  </body>
</html>
```

```
element.style {
}
.prompt.legacy-prompt>.content .wide-inputs input:not(:last-child), .prompt.legacy-prompt>.prompt-list-wrapper>.content .wide-inputs input:not(:last-child) {      legacy-main.css:1
    margin-bottom: .5em;
}
.prompt.legacy-prompt>.content .wide-inputs input, .prompt.legacy-prompt>.prompt-list-wrapper>.content .wide-inputs input {      legacy-main.css:1
    margin: ▶ 0;
    width: 100%;
    ck;
}
input:not([type]), input[type=text], input[type=email], input[type=number], input[type=password], input[type=tel], input[type=url], input[type=search], input[type=date], input[type=time], select, textarea, nu-omni-select {      styles.css:32
    color:
        rgb(var(--nu-theme-on-color-background
    background-color:
        rgb(var(--nu-theme-override-input-back
    ~~margin: ▶ .2em;~~
    padding: ▶ 3px .5em;
    border-radius: ▶ var(
        --nu-theme-dimension-input-border-radius
        );
    border: ▶ 1px solid;
    border-color: ▶
        rgb(var(--nu-theme-override-input-bord
    box-sizing: border-box;
    line-height: 18px;
    outline: ▶ none;
}
input:not([type]),      styles.css:32
input[type=text], input[type=email],
input[type=number], input[type=password],
```

Highlights from the Chrome 125 update

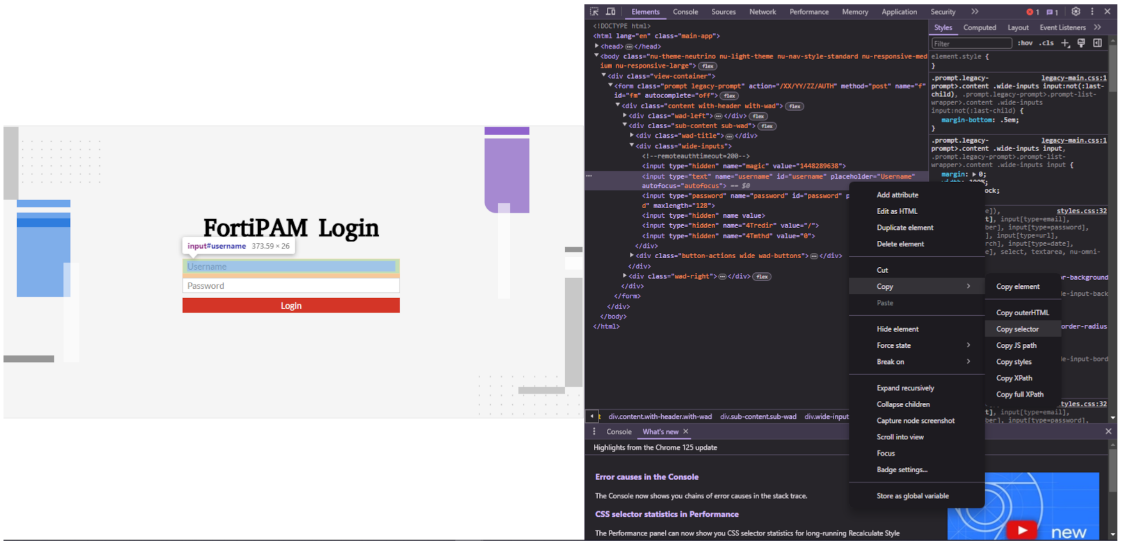
Error causes in the Console

The Console now shows you chains of error causes in the stack trace.

CSS selector statistics in Performance

The Performance panel can now show you CSS selector statistics for long-running Recalculate Style

2. Right-click the highlighted area and select *Copy* > *Copy selector*.



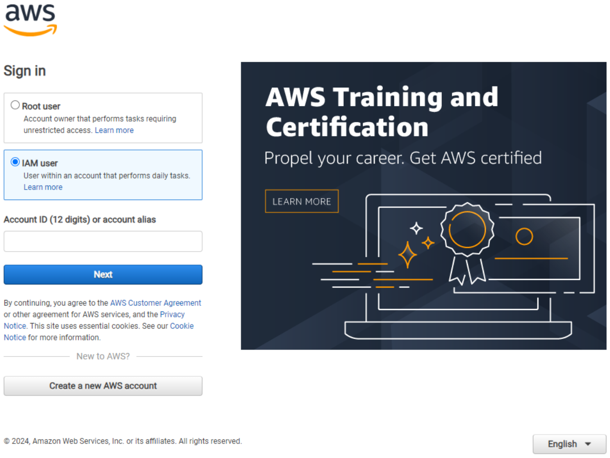
3. Paste the selector `#username` to the web filler configuration in secret template.

Example 2

Finding selector for the *Account ID* field on AWS IAM user login page using the Microsoft Edge web browser

To find the selector for the *Account ID* field:

1. On the AWS *Sign in* page, select *IAM user*.



Sign in

○ Root user
Account owner that performs tasks requiring unrestricted access. Learn more

● IAM user
User within an account that performs daily tasks. Learn more

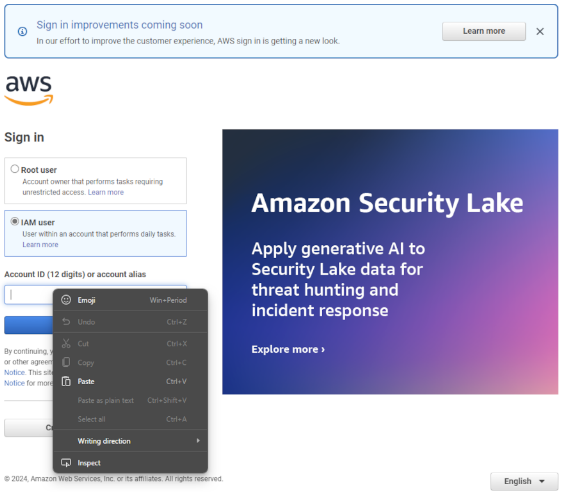
Account ID (12 digits) or account alias

By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

aws
Next
New to AWS?
Create a new AWS account
English
AWS Training and Certification
Propel your career. Get AWS certified
LEARN MORE

2. Right-click the *Account ID (12 digits) or account alias* field and select *Inspect*.



Sign in improvements coming soon
In our effort to improve the customer experience, AWS sign in is getting a new look.

Sign in

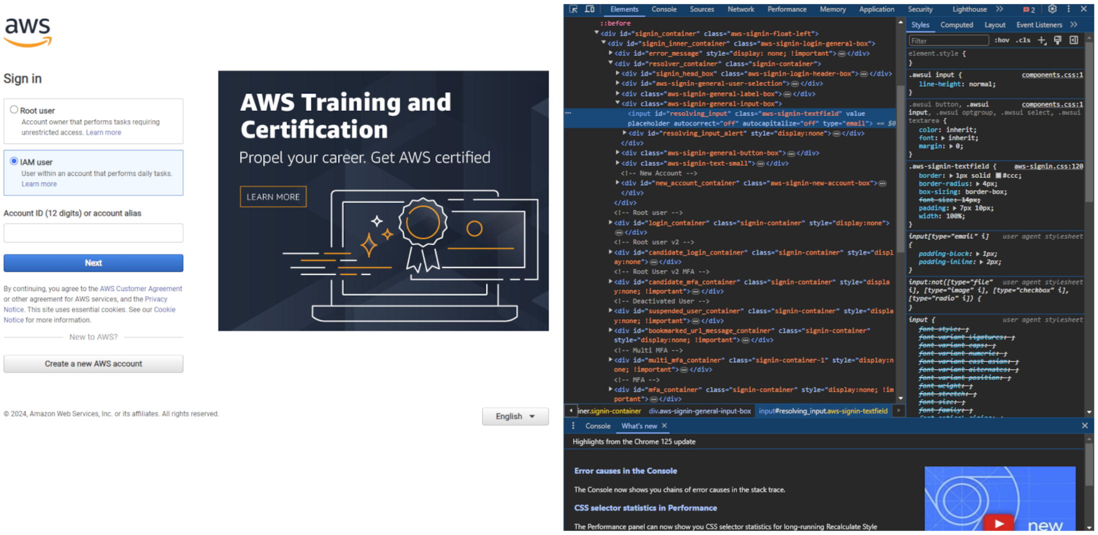
○ Root user
Account owner that performs tasks requiring unrestricted access. Learn more

● IAM user
User within an account that performs daily tasks. Learn more

Account ID (12 digits) or account alias

© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.

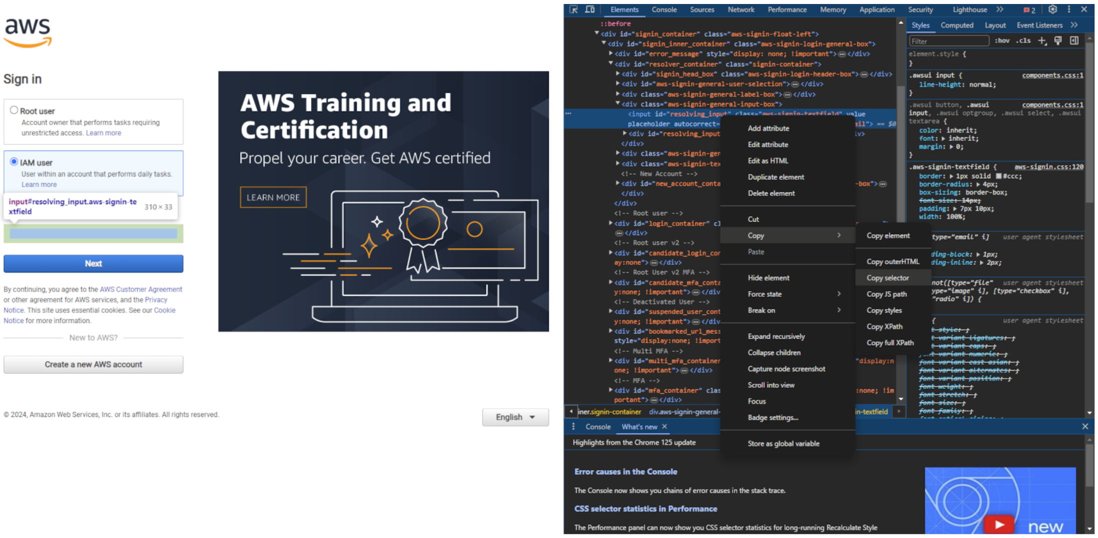
The HTML code for the *Account ID (12 digits) or account alias* field is highlighted in the Edge developer tool.


aws
Sign in
○ Root user
Account owner that performs tasks requiring unrestricted access. Learn more
● IAM user
User within an account that performs daily tasks. Learn more
Account ID (12 digits) or account alias
Next
By continuing, you agree to the AWS Customer Agreement or other agreement for AWS services, and the Privacy Notice. This site uses essential cookies. See our Cookie Notice for more information.
New to AWS?
Create a new AWS account
© 2024, Amazon Web Services, Inc. or its affiliates. All rights reserved.
English
AWS Training and Certification
Propel your career. Get AWS certified
LEARN MORE
Elements
Console
Sources
Network
Performance
Memory
Application
Security
Lighthouse
Styles
Computed
Layout
Event Listeners
Console
What's new
Highlights from the Chrome 125 update
Error causes in the Console
The Console now shows you chains of error causes in the stack trace.
CSS selector statistics in Performance
The Performance panel can now show you CSS selector statistics for long-running Recalculate Style
new

```
::before
▼<div id="signin_container" class="aws-signin-float-left">
  ▼<div id="signin_inner_container" class="aws-signin-login-general-box">
    ▶<div id="error_message" style="display: none; !important">⋯</div>
    ▼<div id="resolver_container" class="signin-container">
      ▶<div id="signin_head_box" class="aws-signin-login-header-box">⋯</div>
      ▶<div id="aws-signin-general-user-selection">⋯</div>
      ▶<div class="aws-signin-general-label-box">⋯</div>
      ▼<div class="aws-signin-general-input-box">
          <input id="resolving_input" class="aws-signin-textfield" value
          placeholder autocorrect="off" autocapitalize="off" type="email"> == $0
        ▶<div id="resolving_input_alert" style="display:none">⋯</div>
        </div>
      ▶<div class="aws-signin-general-button-box">⋯</div>
      ▶<div class="aws-signin-text-small">⋯</div>
        <!-- New Account -->
      ▶<div id="new_account_container" class="aws-signin-new-account-box">⋯
        </div>
      </div>
      <!-- Root user -->
    ▶<div id="login_container" class="signin-container" style="display:none">
      ⋯</div>
      <!-- Root user v2 -->
    ▶<div id="candidate_login_container" class="signin-container" style="displ
      ay:none">⋯</div>
      <!-- Root User v2 MFA -->
    ▶<div id="candidate_mfa_container" class="signin-container" style="displa
      y:none; !important">⋯</div>
      <!-- Deactivated User -->
    ▶<div id="suspended_user_container" class="signin-container" style="displa
      y:none; !important">⋯</div>
    ▶<div id="bookmarked_url_message_container" class="signin-container"
      style="display:none; !important">⋯</div>
      <!-- Multi MFA -->
    ▶<div id="multi_mfa_container" class="signin-container-1" style="display:n
      one; !important">⋯</div>
      <!-- MFA -->
    ▶<div id="mfa_container" class="signin-container" style="display:none; !im
      portant">⋯</div>
```

```
iner.signin-container  div.aws-signin-general-input-box  input#resolving_input.aws-signin-textfield
```

3. Right-click the highlighted area and select *Copy* > *Copy selector*.


aws
Sign in
○ Root user
Account owner that performs tasks requiring unrestricted access. Learn more
● IAM user
User within an account that performs daily tasks. Learn more
input#resolving_input.aws-signin-textfield
310 × 33
Next
Create a new AWS account
English
AWS Training and Certification
Propel your career. Get AWS certified
LEARN MORE
Add attribute
Edit attribute
Edit as HTML
Duplicate element
Delete element
Cut
Copy
Paste
Hide element
Force state
Break on
Expand recursively
Collapse children
Capture node screenshot
Scroll into view
Focus
Badge settings...
Store as global variable
Copy element
Copy outerHTML
Copy selector
Copy JS path
Copy styles
Copy XPath
Copy full XPath
Console
What's new
Highlights from the Chrome 125 update
Error causes in the Console
The Console now shows you chains of error causes in the stack trace.
CSS selector statistics in Performance
The Performance panel can now show you CSS selector statistics for long-running Recalculate Style
new

4. Paste the `#resolving_input` selector to the web filler configuration in secret template.

Appendix P: How to input the authentication path - Example

A login URL can be long. Usually, the URL is composed of:

- *Scheme*: The protocol used to access the resource, e.g., `https://` or `http://`.
- *Host*: The IP address or the domain name of the server.
- *Path*: The location of the resource on the server.
- *Other parameters*: Additional information such as query parameters to the server about the request.

  They are separated from the path by `?`.

Example 1

When accessing the FortiPAM GUI by entering the login IP address, e.g., `https://192.168.1.99` in the web browser address bar and hitting enter, the full URL shown in the browser is `https://192.168.1.99/remote/login?lang=en`.

You can specify `/remote/login` as the `auth-path`.

Example 2

For the Microsoft Azure portal, you can configure the `auth-path` as `/organizations/oauth2/v2.0/authorize` while the full authentication URL is `https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize?redirect_uri=https%3A%2F%2Fportal.azure.com%2Fsignin%2Findex%2F&response_type=code%20id_token&scope=https%3A%2F%2Fmanagement.core.windows.net%2F%2Fuser_impersonation%20openid%20email%20profile&state=OpenIdConnect....`

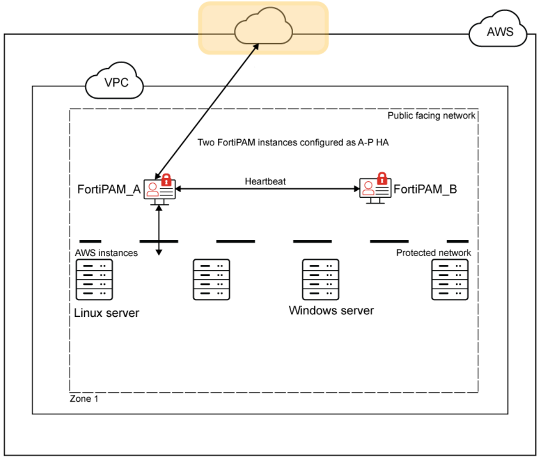
Appendix Q: FortiPAM HA on AWS

This chapter provides a sample configuration of active-passive (A-P) FortiPAM high availability (HA).

You can configure FortiPAM's native HA feature on AWS with two FortiPAM instances: one acting as the primary node and the other as the secondary node, both located in a single VPC.

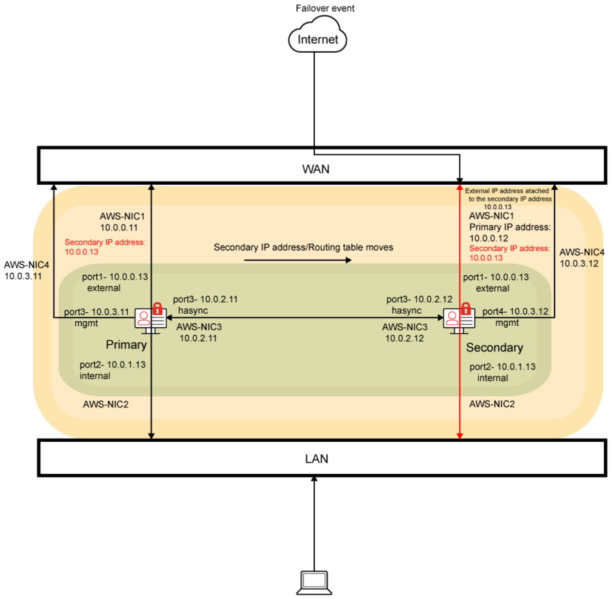
When HA primary and secondary nodes are deployed in different AZs, they must be placed within the same VPC and share the same subnets. Configuring the primary and secondary nodes to use the same VIP allows users to connect to the same IP address after a failover.

You can configure a pair of FortiPAM devices as HA with unicast mode. The pair of FortiPAM devices run heartbeats between dedicated ports and synchronize OS configurations. When the primary node fails, the secondary node takes over as the primary node so that endpoints continue to communicate with external resources over FortiPAM.



How to configure FortiPAM HA on the AWS platform

HA deployment topology



FortiPAM-A [Primary] IP addresses

Port	PAM interface IP address	AWS primary IP address	AWS secondary IP address	Public IP address
Port 1	10.0.0.13 (WAN)	10.0.0.11	10.0.0.13	FortiPAM GUI VIP
Port 2	10.0.1.11 (LAN)	10.0.1.11	N/A	
Port 3	10.0.2.11(HA)	10.0.2.11	N/A	
Port 4	10.0.3.11 (MGMT)	10.0.3.11	N/A	MGMT VIP

FortiPAM-B [Secondary] IP addresses

Port	PAM interface IP address	AWS primary IP address	AWS secondary IP address	Public IP address
Port 1	10.0.0.13 (WAN)	10.0.0.12	10.0.0.13	FortiPAM GUI VIP
Port 2	10.0.1.12 (LAN)	10.0.1.12	N/A	
Port 3	10.0.2.12 (HA)	10.0.2.12	N/A	
Port 4	10.0.3.12 (MGMT)	10.0.3.12	N/A	MGMT VIP

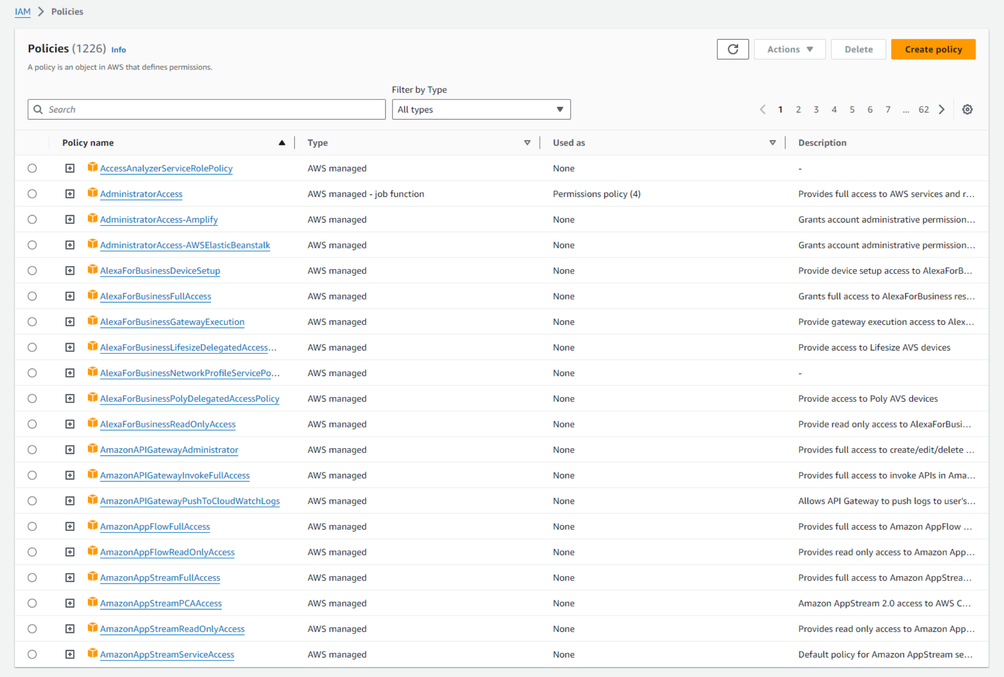
Prerequisites

- Creating a custom permission policy on page 539
- Creating an IAM role on page 540
- Creating a VPC on page 543
- Creating subnets on page 544
- Creating an internet gateway on page 545
- Configuring routing tables on page 546
- Creating network interfaces on page 548
- Creating elastic IP addresses on page 549

Creating a custom permission policy

To create a custom permission policy:

1. In the AWS console, open *IAM*.
2. From the *Dashboard*, go to *Access management* > *Policies*.
   The *Policies* window opens.



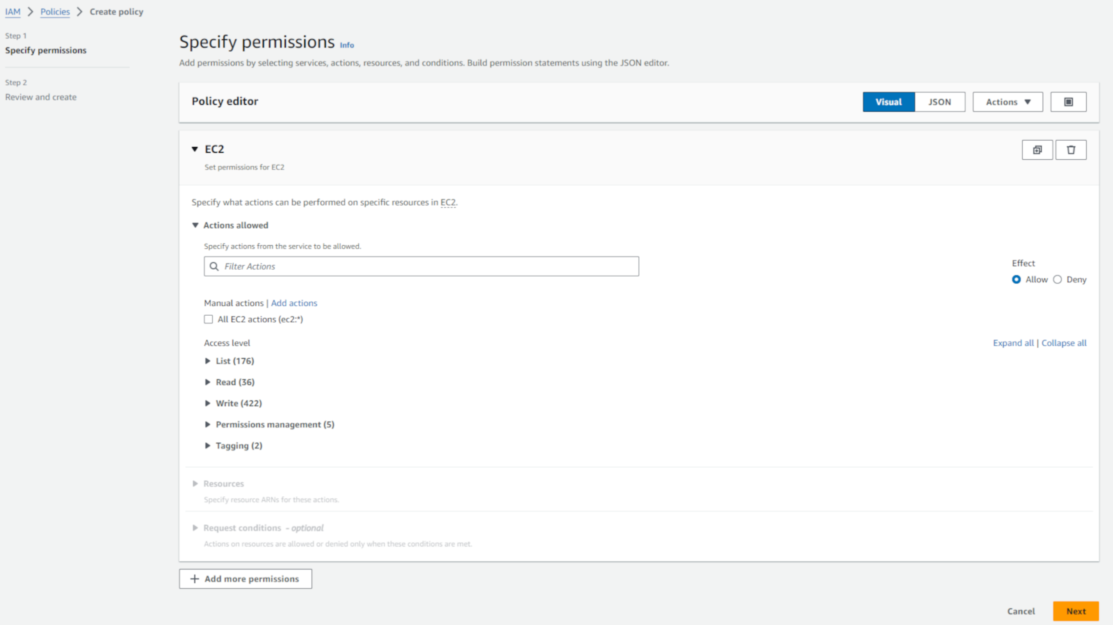
Policies (1226)

A policy is an object in AWS that defines permissions.

		Policy name ▲	Type ▽	Used as ▽	Description
○	⊞	AccessAnalyzerServiceRolePolicy	AWS managed	None	-
○	⊞	AdministratorAccess	AWS managed - job function	Permissions policy (4)	Provides full access to AWS services and r...
○	⊞	AdministratorAccess-Amplify	AWS managed	None	Grants account administrative permission...
○	⊞	AdministratorAccess-AWSElasticBeanstalk	AWS managed	None	Grants account administrative permission...
○	⊞	AlexaForBusinessDeviceSetup	AWS managed	None	Provide device setup access to AlexaForB...
○	⊞	AlexaForBusinessFullAccess	AWS managed	None	Grants full access to AlexaForBusiness res...
○	⊞	AlexaForBusinessGatewayExecution	AWS managed	None	Provide gateway execution access to Alex...
○	⊞	AlexaForBusinessLifesizeDelegatedAccess...	AWS managed	None	Provide access to Lifesize AVS devices
○	⊞	AlexaForBusinessNetworkProfileServicePo...	AWS managed	None	-
○	⊞	AlexaForBusinessPolyDelegatedAccessPolicy	AWS managed	None	Provide access to Poly AVS devices
○	⊞	AlexaForBusinessReadOnlyAccess	AWS managed	None	Provide read only access to AlexaForBusi...
○	⊞	AmazonAPIGatewayAdministrator	AWS managed	None	Provides full access to create/edit/delete ...
○	⊞	AmazonAPIGatewayInvokeFullAccess	AWS managed	None	Provides full access to invoke APIs in Ama...
○	⊞	AmazonAPIGatewayPushToCloudWatchLogs	AWS managed	None	Allows API Gateway to push logs to user's...
○	⊞	AmazonAppFlowFullAccess	AWS managed	None	Provides full access to Amazon AppFlow ...
○	⊞	AmazonAppFlowReadOnlyAccess	AWS managed	None	Provides read only access to Amazon App...
○	⊞	AmazonAppStreamFullAccess	AWS managed	None	Provides full access to Amazon AppStrea...
○	⊞	AmazonAppStreamPCAAccess	AWS managed	None	Amazon AppStream 2.0 access to AWS C...
○	⊞	AmazonAppStreamReadOnlyAccess	AWS managed	None	Provides read only access to Amazon App...
○	⊞	AmazonAppStreamServiceAccess	AWS managed	None	Default policy for Amazon AppStream se...

3. From the list, select *Create policy*.

4. In the *Service* dropdown, select *EC2*.



IAM > Policies > Create policy

Step 1
Specify permissions

Step 2
Review and create

Specify permissions Info

Add permissions by selecting services, actions, resources, and conditions. Build permission statements using the JSON editor.

Policy editor — Visual | JSON | Actions ▼

▼ EC2
Set permissions for EC2

Specify what actions can be performed on specific resources in EC2.

▼ Actions allowed
Specify actions from the service to be allowed.

Filter Actions

Effect
● Allow ○ Deny

Manual actions | Add actions
□ All EC2 actions (ec2:*)

Access level — Expand all | Collapse all
- ▶ List (176)
- ▶ Read (36)
- ▶ Write (422)
- ▶ Permissions management (5)
- ▶ Tagging (2)

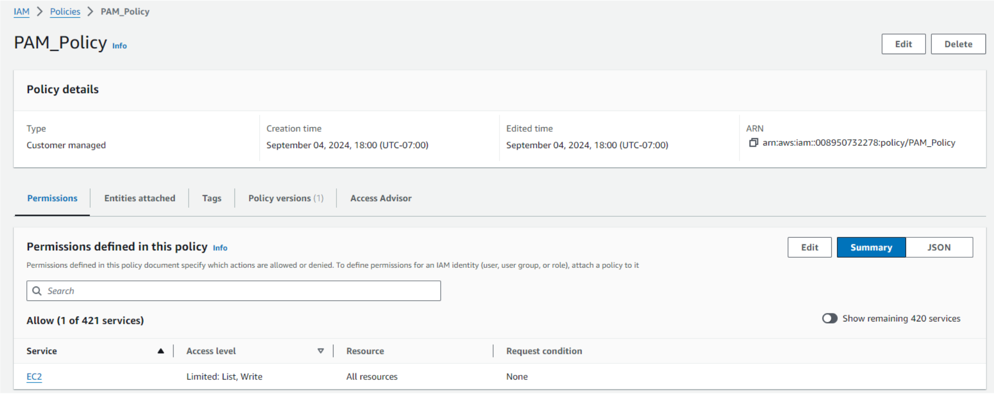
▶ Resources
Specify resource ARNs for these actions.

▶ Request conditions - *optional*
Actions on resources are allowed or denied only when these conditions are met.

+ Add more permissions

Cancel | Next

5. In *Actions Allowed*, select options from *List* and *Write*.
6. In *Resources*, select *All*.
7. Click *Next*.
8. In *Policy* details:
   a. In *Policy name*, enter a name for the policy name.
   b. Optionally, enter a description for the policy.
9. Click *Create policy*.



IAM > Policies > PAM_Policy

PAM_Policy Info — Edit | Delete

Policy details

Type	Creation time	Edited time	ARN
Customer managed	September 04, 2024, 18:00 (UTC-07:00)	September 04, 2024, 18:00 (UTC-07:00)	arn:aws:iam::008950732278:policy/PAM_Policy

Permissions | Entities attached | Tags | Policy versions (1) | Access Advisor

Permissions defined in this policy Info — Edit | Summary | JSON

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Search

Allow (1 of 421 services) — Show remaining 420 services

Service	Access level	Resource	Request condition
EC2	Limited: List, Write	All resources	None

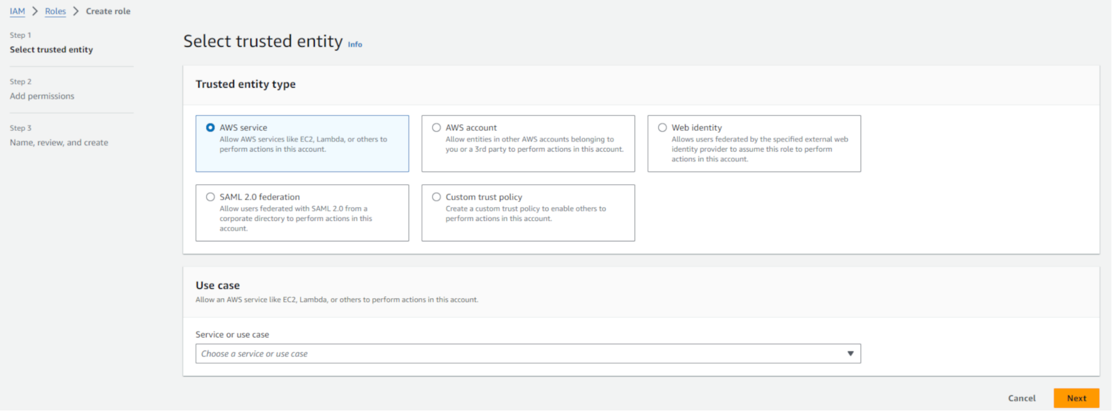
Creating an IAM role

The IAM role is necessary for HA failover.

Ensure that the IAM role can read and write EC2 information to read, detach, and reattach network interfaces and edit routing tables.

To create an IAM role:

1. In the AWS console, open *IAM*.
2. From the *Dashboard*, go to *Access management* > *Roles*.
3. Select *Create role*, to create a new role.
   The *Select trusted entity wizard* opens.



IAM > Roles > Create role

Step 1
Select trusted entity

Step 2
Add permissions

Step 3
Name, review, and create

Select trusted entity Info

Trusted entity type

● AWS service
Allow AWS services like EC2, Lambda, or others to perform actions in this account.

○ AWS account
Allow entities in other AWS accounts belonging to you or a 3rd party to perform actions in this account.

○ Web identity
Allows users federated by the specified external web identity provider to assume this role to perform actions in this account.

○ SAML 2.0 federation
Allow users federated with SAML 2.0 from a corporate directory to perform actions in this account.

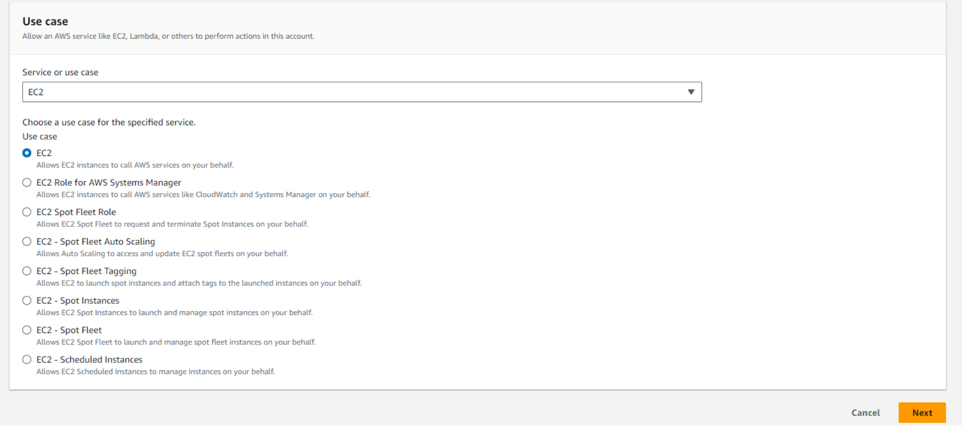
○ Custom trust policy
Create a custom trust policy to enable others to perform actions in this account.

Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case
Choose a service or use case ▼

Cancel Next

4. From *Trusted entity type*, select *AWS service*.
5. In the *Use case* dropdown, select *EC2*.



Use case
Allow an AWS service like EC2, Lambda, or others to perform actions in this account.

Service or use case
EC2 ▼

Choose a use case for the specified service.
Use case

● EC2
Allows EC2 instances to call AWS services on your behalf.

○ EC2 Role for AWS Systems Manager
Allows EC2 instances to call AWS services like CloudWatch and Systems Manager on your behalf.

○ EC2 Spot Fleet Role
Allows EC2 Spot Fleet to request and terminate Spot Instances on your behalf.

○ EC2 - Spot Fleet Auto Scaling
Allows Auto Scaling to access and update EC2 spot fleets on your behalf.

○ EC2 - Spot Fleet Tagging
Allows EC2 to launch spot instances and attach tags to the launched instances on your behalf.

○ EC2 - Spot Instances
Allows EC2 Spot Instances to launch and manage spot instances on your behalf.

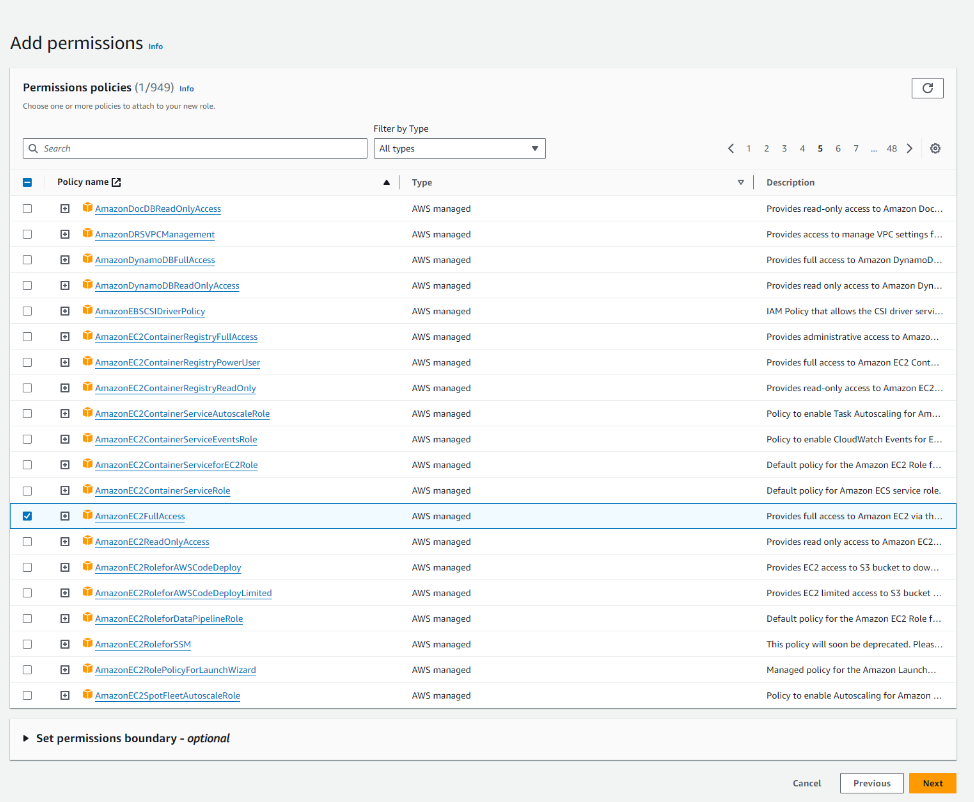
○ EC2 - Spot Fleet
Allows EC2 Spot Fleet to launch and manage spot fleet instances on your behalf.

○ EC2 - Scheduled Instances
Allows EC2 Scheduled Instances to manage instances on your behalf.

Cancel Next

6. Click *Next*.
   The *Add permissions* window opens.

7. From the permission policies list, select *AmazonEC2FullAccess*.



Add permissions

Permissions policies (1/949) Info

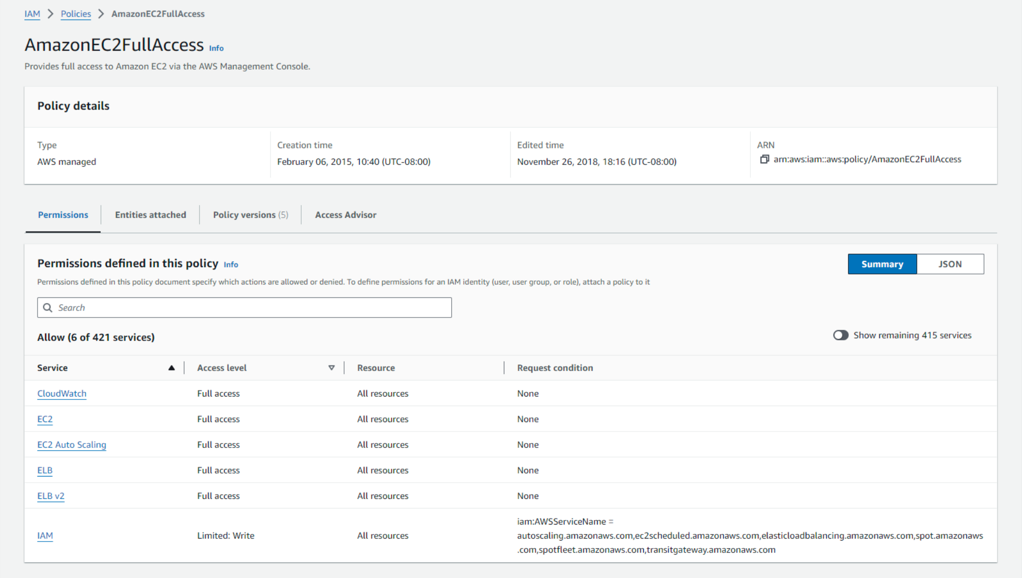
Choose one or more policies to attach to your new role.

Filter by Type: All types

■	Policy name	Type	Description
□	AmazonDocDBReadOnlyAccess	AWS managed	Provides read-only access to Amazon Doc…
□	AmazonDRSVPCManagement	AWS managed	Provides access to manage VPC settings f…
□	AmazonDynamoDBFullAccess	AWS managed	Provides full access to Amazon DynamoD…
□	AmazonDynamoDBReadOnlyAccess	AWS managed	Provides read only access to Amazon Dyn…
□	AmazonEBSCSIDriverPolicy	AWS managed	IAM Policy that allows the CSI driver servi…
□	AmazonEC2ContainerRegistryFullAccess	AWS managed	Provides administrative access to Amazo…
□	AmazonEC2ContainerRegistryPowerUser	AWS managed	Provides full access to Amazon EC2 Cont…
□	AmazonEC2ContainerRegistryReadOnly	AWS managed	Provides read-only access to Amazon EC2…
□	AmazonEC2ContainerServiceAutoscaleRole	AWS managed	Policy to enable Task Autoscaling for Am…
□	AmazonEC2ContainerServiceEventsRole	AWS managed	Policy to enable CloudWatch Events for E…
□	AmazonEC2ContainerServiceforEC2Role	AWS managed	Default policy for the Amazon EC2 Role f…
□	AmazonEC2ContainerServiceRole	AWS managed	Default policy for Amazon ECS service role.
☑	AmazonEC2FullAccess	AWS managed	Provides full access to Amazon EC2 via th…
□	AmazonEC2ReadOnlyAccess	AWS managed	Provides read only access to Amazon EC2…
□	AmazonEC2RoleforAWSCodeDeploy	AWS managed	Provides EC2 access to S3 bucket to dow…
□	AmazonEC2RoleforAWSCodeDeployLimited	AWS managed	Provides EC2 limited access to S3 bucket …
□	AmazonEC2RoleforDataPipelineRole	AWS managed	Default policy for the Amazon EC2 Role f…
□	AmazonEC2RoleforSSM	AWS managed	This policy will soon be deprecated. Pleas…
□	AmazonEC2RolePolicyForLaunchWizard	AWS managed	Managed policy for the Amazon Launch…
□	AmazonEC2SpotFleetAutoscaleRole	AWS managed	Policy to enable Autoscaling for Amazon …

▸ **Set permissions boundary - *optional***

Click the *AmazonEC2FullAccess* role to see it in a new window.



IAM > Policies > AmazonEC2FullAccess

AmazonEC2FullAccess Info

Provides full access to Amazon EC2 via the AWS Management Console.

Policy details

Type	Creation time	Edited time	ARN
AWS managed	February 06, 2015, 10:40 (UTC-08:00)	November 26, 2018, 18:16 (UTC-08:00)	arn:aws:iam::aws:policy/AmazonEC2FullAccess

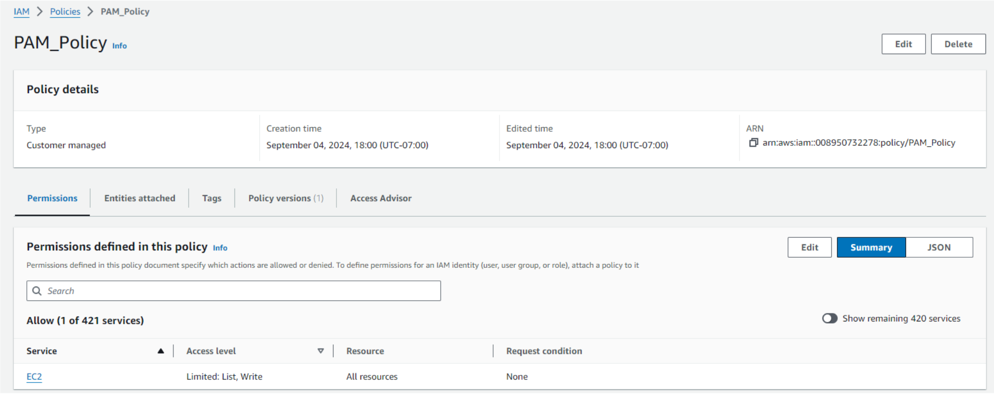
Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Allow (6 of 421 services)

Service	Access level	Resource	Request condition
CloudWatch	Full access	All resources	None
EC2	Full access	All resources	None
EC2 Auto Scaling	Full access	All resources	None
ELB	Full access	All resources	None
ELB v2	Full access	All resources	None
IAM	Limited: Write	All resources	iam:AWSServiceName = autoscaling.amazonaws.com,ec2scheduled.amazonaws.com,elasticloadbalancing.amazonaws.com,spot.amazonaws.com,spotfleet.amazonaws.com,transitgateway.amazonaws.com

8. From the permissions policies list, look for the policy created in Creating a custom permission policy on page 539, and select it.
   Click the *PAM_Policy* role to see it in a new window.



IAM > Policies > PAM_Policy

PAM_Policy Info

Policy details

Type	Creation time	Edited time	ARN
Customer managed	September 04, 2024, 18:00 (UTC-07:00)	September 04, 2024, 18:00 (UTC-07:00)	arn:aws:iam::008950732278:policy/PAM_Policy

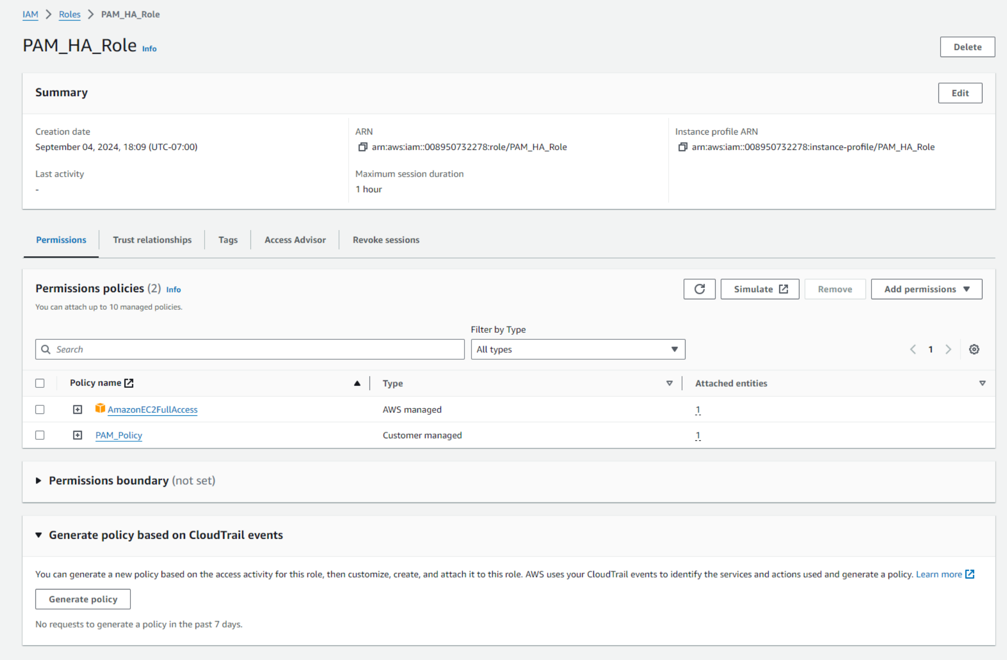
Permissions defined in this policy Info

Permissions defined in this policy document specify which actions are allowed or denied. To define permissions for an IAM identity (user, user group, or role), attach a policy to it

Allow (1 of 421 services)

Service	Access level	Resource	Request condition
EC2	Limited: List, Write	All resources	None

9. Click *Next*.
10. In *Role* details, enter a role name.
11. Optionally, enter a description.
12. Click *Create role*.



IAM > Roles > PAM_HA_Role

PAM_HA_Role Info

Summary

Creation date	ARN	Instance profile ARN
September 04, 2024, 18:09 (UTC-07:00)	arn:aws:iam::008950732278:role/PAM_HA_Role	arn:aws:iam::008950732278:instance-profile/PAM_HA_Role
Last activity	Maximum session duration	
-	1 hour	

Permissions policies (2) Info

You can attach up to 10 managed policies.

Filter by Type: All types

□	Policy name	Type	Attached entities
□	AmazonEC2FullAccess	AWS managed	1
□	PAM_Policy	Customer managed	1

▸ **Permissions boundary** (not set)

▾ **Generate policy based on CloudTrail events**

You can generate a new policy based on the access activity for this role, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more

No requests to generate a policy in the past 7 days.

Creating a VPC

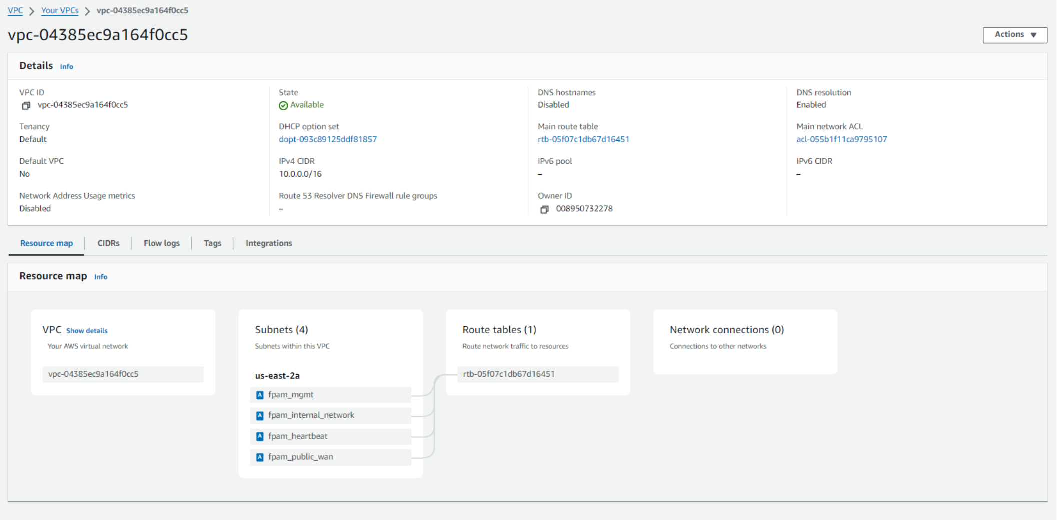
We create a VPC with four subnets.

The VPC is created with `10.0.0.0/16` CIDR.

To create a VPC:

1. In the AWS console, open *VPC*.
2. In the *VPC dashboard*, select *Create VPC*.
   The *Create VPC* wizard opens.
3. Keep the default settings.

4. Select *Create VPC*.
   The VPC is created.
5. Click *View VPC* to see the newly created VPC.



VPC > Your VPCs > vpc-04385ec9a164f0cc5

vpc-04385ec9a164f0cc5

Details Info

VPC ID vpc-04385ec9a164f0cc5	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-093c89125ddf81857	Main route table rtb-05f07c1db67d16451	Main network ACL acl-055b1f11ca9795107
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool –	IPv6 CIDR –
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups –	Owner ID 008950732278	

Resource map Info

VPC Show details
Your AWS virtual network
vpc-04385ec9a164f0cc5

Subnets (4)
Subnets within this VPC
us-east-2a
fpam_mgmt
fpam_internal_network
fpam_heartbeat
fpam_public_wan

Route tables (1)
Route network traffic to resources
rtb-05f07c1db67d16451

Network connections (0)
Connections to other networks

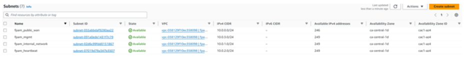
Creating subnets

We create four subnets.

The four subnets are the following:

- Public WAN
  `10.0.0.0/24`
- Internal network
  `10.0.1.0/24`
- Heartbeat network
  `10.0.2.0/24`
- Management network
  `10.0.3.0/24`

The VPC created in Creating a VPC on page 543 is used in both the primary and the secondary FortiPAM.



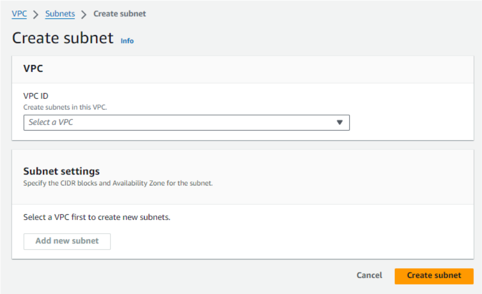
Subnets (7) Info

Last updated less than a minute ago
Actions ▼
Create subnet
Find resources by attribute or tag
< 1 >

□	Name	Subnet ID	State	VPC	IPv4 CIDR	IPv6 CIDR	Available IPv4 addresses	Availability Zone	Availability Zone ID
□	fpam_public_wan	subnet-055abbdaf9280aa22	Available	vpc-038129f10ec358098 | fpa...	10.0.0.0/24	–	246	ca-central-1d	cac1-az4
□	fpam_mgmt	subnet-091a0ede1431f7c79	Available	vpc-038129f10ec358098 | fpa...	10.0.3.0/24	–	249	ca-central-1d	cac1-az4
□	fpam_internal_network	subnet-02d6c99fdd0151867	Available	vpc-038129f10ec358098 | fpa...	10.0.1.0/24	–	249	ca-central-1d	cac1-az4
□	fpam_heartbeat	subnet-07019d79a547b3507	Available	vpc-038129f10ec358098 | fpa...	10.0.2.0/24	–	249	ca-central-1d	cac1-az4

To create a subnet:

1. In the VPC created in Creating a VPC on page 543, go to *Virtual private cloud* > *Subnets*.
2. Select *Create subnet*.
   The *Create subnet* wizard opens.



Create subnet

VPC

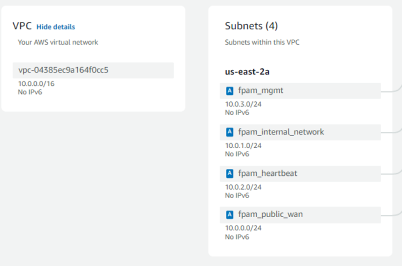
VPC ID
Create subnets in this VPC.
Select a VPC

Subnet settings
Specify the CIDR blocks and Availability Zone for the subnet.

Select a VPC first to create new subnets.

Add new subnet

3. From the *VPC ID* dropdown, select the VPC created in Creating a VPC on page 543.
4. In the *Subnet settings* pane:
   a. Enter a name in *Subnet name*.
   b. In *IPv4 subnet CIDR block*, enter the IPv4 subnet.
   c. Select *Add new subnet* and add three more subnets.
   d. Select *Create subnet* to create the subnets.



VPC
Your AWS virtual network
vpc-04385ec9a164f0cc5
10.0.0.0/16
No IPv6

Subnets (4)
Subnets within this VPC
us-east-2a
fpam_mgmt
10.0.3.0/24
No IPv6
fpam_internal_network
10.0.1.0/24
No IPv6
fpam_heartbeat
10.0.2.0/24
No IPv6
fpam_public_wan
10.0.0.0/24
No IPv6

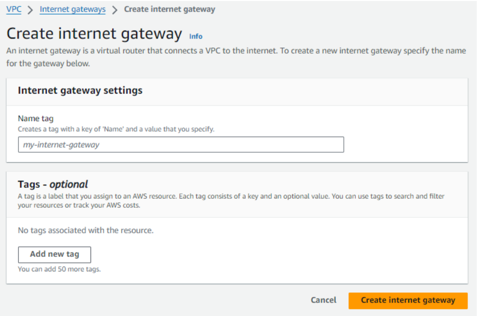
Creating an internet gateway

We create a new gateway and attach it to the newly created VPC in Creating a VPC on page 543.

The internet gateway takes charge of the VPC to communicate to the public internet.

To create an internet gateway:

1. In VPC, go to *Virtual private cloud* > *Internet gateways*.
2. From the internet gateways list, select *Create internet gateway*.
   The *Create internet gateway* wizard opens.



Create internet gateway

An internet gateway is a virtual router that connects a VPC to the internet. To create a new internet gateway specify the name for the gateway below.

Internet gateway settings

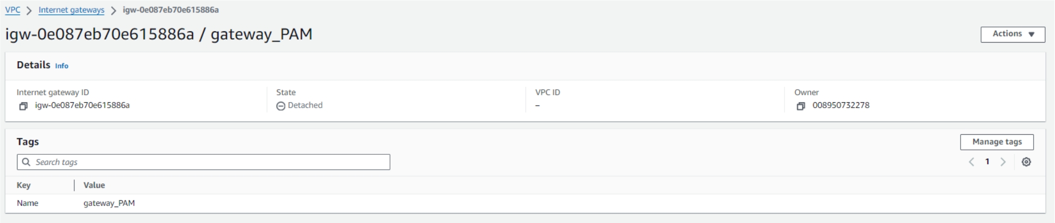
Name tag
Creates a tag with a key of 'Name' and a value that you specify.
my-internet-gateway

Tags - *optional*
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

Add new tag
You can add 50 more tags.

3. Enter a name for the tag.
4. Click *Create internet gateway*.
   The internet gateway is created.



igw-0e087eb70e615886a / gateway_PAM

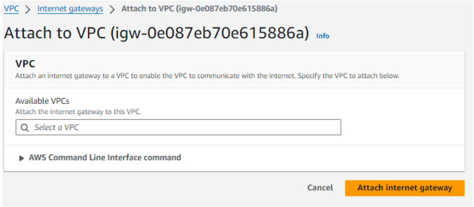
Details Info

Internet gateway ID	State	VPC ID	Owner
igw-0e087eb70e615886a	Detached	–	008950732278

Tags

Key	Value
Name	gateway_PAM

5. From the *Actions* dropdown on the right, select *Attach to VPC*.
   The *Attach to VPC* window opens.



VPC > Internet gateways > Attach to VPC (igw-0e087eb70e615886a)

Attach to VPC (igw-0e087eb70e615886a) Info

VPC

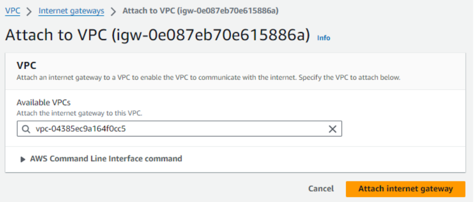
Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

Available VPCs

Attach the internet gateway to this VPC.

Select a VPC
▶ AWS Command Line Interface command
Cancel
Attach internet gateway

6. From *Available VPCs*, select the VPC created in Creating a VPC on page 543.



VPC > Internet gateways > Attach to VPC (igw-0e087eb70e615886a)

Attach to VPC (igw-0e087eb70e615886a) Info

VPC

Attach an internet gateway to a VPC to enable the VPC to communicate with the internet. Specify the VPC to attach below.

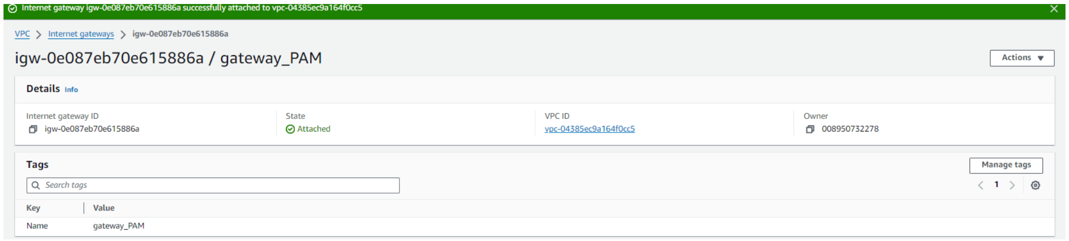
Available VPCs

Attach the internet gateway to this VPC.

vpc-04385ec9a164f0cc5

▶ AWS Command Line Interface command
Cancel
Attach internet gateway

7. Click *Attach internet gateway*.
   The internet gateway is attached to the VPC.



Internet gateway igw-0e087eb70e615886a successfully attached to vpc-04385ec9a164f0cc5

igw-0e087eb70e615886a / gateway_PAM

Details Info

Internet gateway ID	State	VPC ID	Owner
igw-0e087eb70e615886a	Attached	vpc-04385ec9a164f0cc5	008950732278

Tags

Key	Value
Name	gateway_PAM

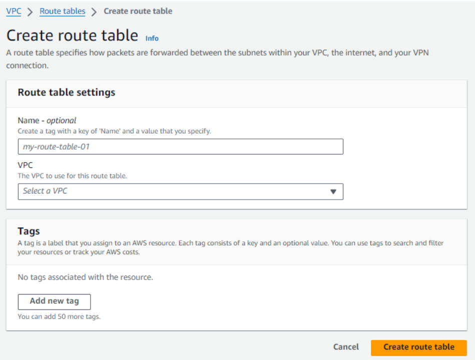
Configuring routing tables

We configure two routing tables under the recently created VPC and gateway.

The following shows the public WAN, internal network, heartbeat routing table, and subnets association information.

To configure routing table:

1. In *VPC*, go to *Virtual private cloud* > *Route tables*.
   a. From the right, select *Create route table*.
      The *Create route table* wizard opens.



VPC > Route tables > Create route table

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
my-route-table-01

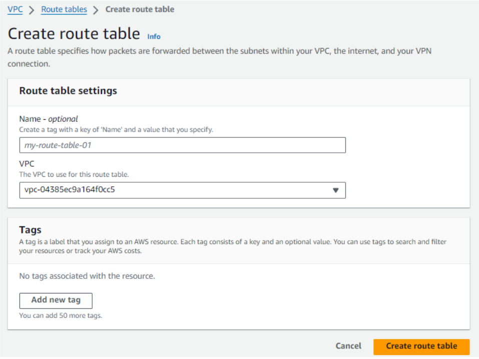
VPC
The VPC to use for this route table.
Select a VPC

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

You can add 50 more tags.

2. From the *VPC* dropdown, select the VPC created in Creating a VPC on page 543.



VPC > Route tables > Create route table

Create route table Info

A route table specifies how packets are forwarded between the subnets within your VPC, the internet, and your VPN connection.

Route table settings

Name - *optional*
Create a tag with a key of 'Name' and a value that you specify.
my-route-table-01

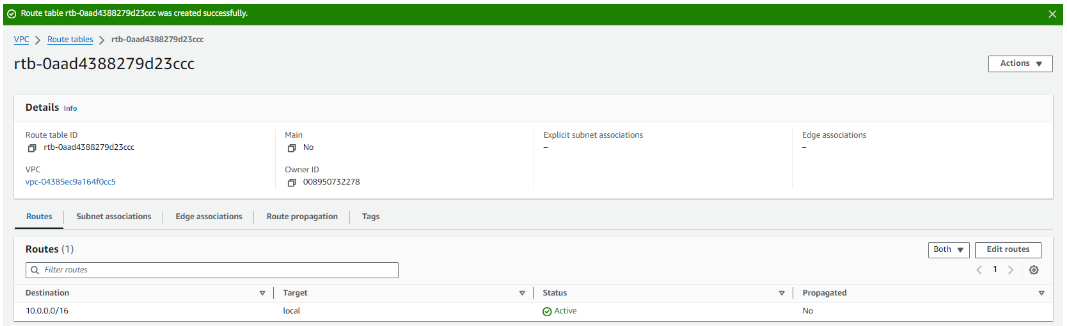
VPC
The VPC to use for this route table.
vpc-04385ec9a164f0cc5

Tags
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

You can add 50 more tags.

3. Select *Create route table*.
   The routing table is created.



Route table rtb-0aad4388279d23ccc was created successfully.

VPC > Route tables > rtb-0aad4388279d23ccc

rtb-0aad4388279d23ccc

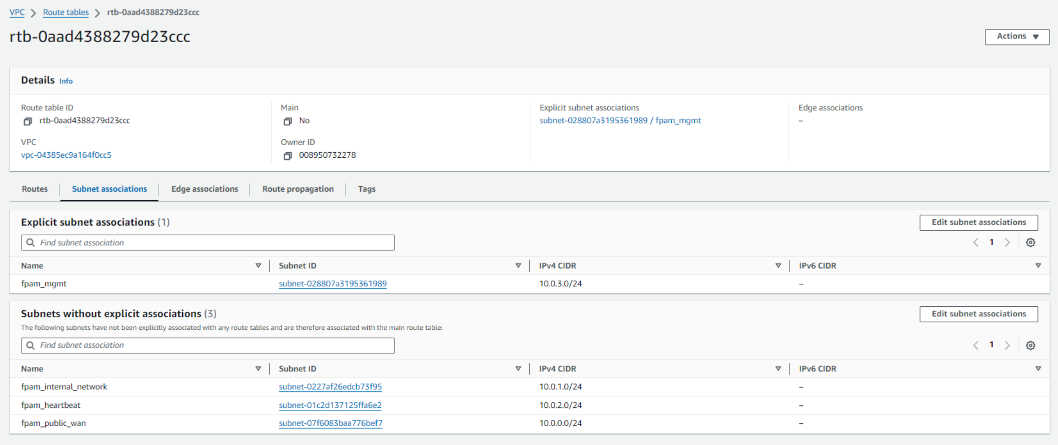
Details Info

Route table ID: rtb-0aad4388279d23ccc
Main: No
Explicit subnet associations: –
Edge associations: –
VPC: vpc-04385ec9a164f0cc5
Owner ID: 008950732278

Routes (1)

Destination	Target	Status	Propagated
10.0.0.0/16	local	Active	No

4. In the *Subnet associations* tab, from the right, select *Edit subnet associations*.
5. Select the subnet with *IPv4 CIDR* as `10.0.3.0/24` and click *Save association*.
   The subnet associations are updated for the routing table.



VPC > Route tables > rtb-0aad4388279d23ccc

rtb-0aad4388279d23ccc

Details Info

Route table ID rtb-0aad4388279d23ccc	Main No	Explicit subnet associations subnet-028807a3195361989 / fpam_mgmt	Edge associations –
VPC vpc-04385ec9a164f0cc5	Owner ID 008950732278		

Routes | Subnet associations | Edge associations | Route propagation | Tags

Explicit subnet associations (1)

Edit subnet associations
Find subnet association

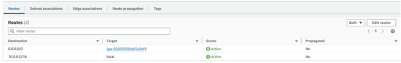
Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
fpam_mgmt	subnet-028807a3195361989	10.0.3.0/24	–

Subnets without explicit associations (3)

The following subnets have not been explicitly associated with any route tables and are therefore associated with the main route table:

Name	Subnet ID	IPv4 CIDR	IPv6 CIDR
fpam_internal_network	subnet-0227af26edcb73f95	10.0.1.0/24	–
fpam_heartbeat	subnet-01c2d137125ffa6e2	10.0.2.0/24	–
fpam_public_wan	subnet-07f6083baa776bef7	10.0.0.0/24	–

6. Create another routing table with a target.

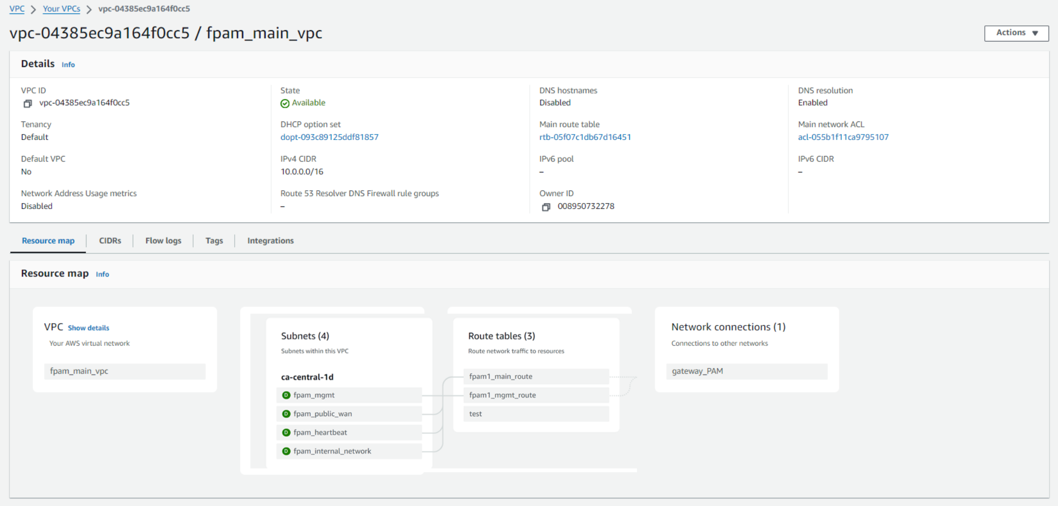


Routes | Subnet associations | Edge associations | Route propagation | Tags
Both ▼
Edit routes
Filter routes

Routes (2)

Destination	Target	Status	Propagated
0.0.0.0/0	igw-0583f2096e05a5bf4	Active	No
10.0.0.0/16	local	Active	No

After VPC, subnets, gateways, and routing tables have been set up, the VPC configuration looks like the following:



VPC > Your VPCs > vpc-04385ec9a164f0cc5

vpc-04385ec9a164f0cc5 / fpam_main_vpc

Details Info

VPC ID vpc-04385ec9a164f0cc5	State Available	DNS hostnames Disabled	DNS resolution Enabled
Tenancy Default	DHCP option set dopt-093c89125ddf81857	Main route table rtb-05f07c1db67d16451	Main network ACL acl-055b1f11ca9795107
Default VPC No	IPv4 CIDR 10.0.0.0/16	IPv6 pool –	IPv6 CIDR –
Network Address Usage metrics Disabled	Route 53 Resolver DNS Firewall rule groups –	Owner ID 008950732278	

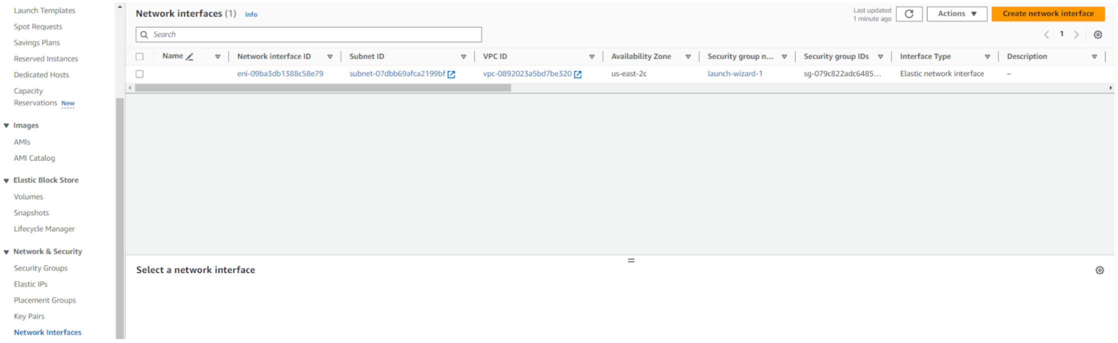
Resource map Info

Creating network interfaces

We create a network interface in every VPC subnet.

To create network interface:

1. Go to *EC2* > *Network & Security* > *Network Interfaces*.
The *Network interfaces* window opens.

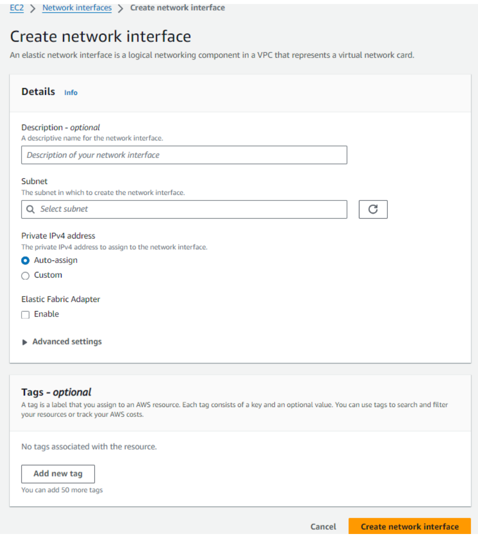


Network interfaces (1)

□	Name	Network interface ID	Subnet ID	VPC ID	Availability Zone	Security group n...	Security group IDs	Interface Type	Description
□		eni-09ba3db1388c58e79	subnet-07dbb69afca2199bf	vpc-0892023a5bd7be320	us-east-2c	launch-wizard-1	sg-079c822adc6485...	Elastic network interface	–

Select a network interface

2. From the right, select *Create network interface*.
   The *Create network interface wizard* opens.



Create network interface

An elastic network interface is a logical networking component in a VPC that represents a virtual network card.

Details

Description - *optional*
A descriptive name for the network interface.
Description of your network interface

Subnet
The subnet in which to create the network interface.
Select subnet

Private IPv4 address
The private IPv4 address to assign to the network interface.
● Auto-assign
○ Custom

Elastic Fabric Adapter
□ Enable

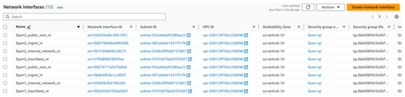
▶ Advanced settings

Tags - *optional*
A tag is a label that you assign to an AWS resource. Each tag consists of a key and an optional value. You can use tags to search and filter your resources or track your AWS costs.

No tags associated with the resource.

You can add 50 more tags

3. From the *Subnet* dropdown, select one of the subnets created in Creating subnets on page 544.
4. In the *Security groups* pane, select a security group.
5. Click *Create network interface* to create the network interface.
   We create a total of eight network interfaces where four are used for each FortiPAM unit.



Network interfaces (10)

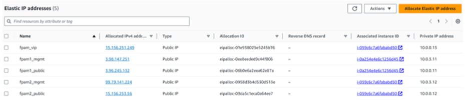
□	Name	Network interface ID	Subnet ID	VPC ID	Availability Zone	Security group n...	Security group IDs	In
□	fpam2_public_wan_ni	eni-0542f4e6bc3961491	subnet-055abbdaf9280aa22	vpc-038129f10ec358098	ca-central-1d	fpam-sp	sg-0de506f453a587...	El
□	fpam2_mgmt_ni	eni-008176948a4994386	subnet-091a0ede1431f7c79	vpc-038129f10ec358098	ca-central-1d	fpam-sp	sg-0de506f453a587...	El
□	fpam2_internal_network_ni	eni-0b753fe6b8cc5821f	subnet-02d6c99fdd0151867	vpc-038129f10ec358098	ca-central-1d	fpam-sp	sg-0de506f453a587...	El
□	fpam2_heartbeat_ni	eni-01ffd8fb878f4f3ec	subnet-07019d79a347b3507	vpc-038129f10ec358098	ca-central-1d	fpam-sp	sg-0de506f453a587...	El
□	fpam1_public_wan_ni	eni-00674771afe7f28b8	subnet-055abbdaf9280aa22	vpc-038129f10ec358098	ca-central-1d	fpam-sp	sg-0de506f453a587...	El
□	fpam1_mgmt_ni	eni-08ab4dfc6e1cc9027	subnet-091a0ede1431f7c79	vpc-038129f10ec358098	ca-central-1d	fpam-sp	sg-0de506f453a587...	El
□	fpam1_internal_network_ni	eni-058ef8cfb618fea95	subnet-02d6c99fdd0151867	vpc-038129f10ec358098	ca-central-1d	fpam-sp	sg-0de506f453a587...	El
□	fpam1_heartbeat_ni	eni-005e3356705ab9ab7	subnet-07019d79a347b3507	vpc-038129f10ec358098	ca-central-1d	fpam-sp	sg-0de506f453a587...	El

Creating elastic IP addresses

To create elastic IP address:

1. Go to *EC2 > Network & Security > Elastic IPs*.
   You should have five elastic IP addresses.
   Setting up the environment requires five elastic IP addresses:
   - One public WAN IP address. This is the FortiPAM GUI VIP.
   - One FortiPAM primary management IP address.
   - One FortiPAM secondary IP address.
   - Two temporary IP addresses.

2. From the right, select *Allocate Elastic IP address*.
   The *Allocate Elastic IP address* window opens.
3. Manually associate the elastic IP addresses to the network interface private IP address.



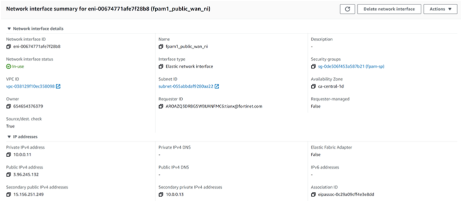
Elastic IP addresses (5)

Actions
Allocate Elastic IP address
Find resources by attribute or tag

	Name	Allocated IPv4 addr...	Type	Allocation ID	Reverse DNS record	Associated instance ID	Private IP address
□	fpam_vip	15.156.251.249	Public IP	eipalloc-01e938025e5245b76	-	i-059c6c7a6fababd50	10.0.0.13
□	fpam1_mgmt	3.98.147.251	Public IP	eipalloc-0ee8eeded9c44f006	-	i-0a254e4e6c1256d45	10.0.3.11
□	fpam1_public	3.96.245.132	Public IP	eipalloc-06b0e6a2eea62e87a	-	i-0a254e4e6c1256d45	10.0.0.11
□	fpam2_mgmt	99.79.141.224	Public IP	eipalloc-0958d3b4d530d513e	-	i-059c6c7a6fababd50	10.0.3.12
□	fpam2_public	15.156.253.56	Public IP	eipalloc-09da5c1eca0a64ee7	-	i-059c6c7a6fababd50	10.0.0.12

We take a look at the current FortiPAM primary and secondary WAN interface configuration by going to *Network & Security* > *Network Interfaces* and opening the network interface.

From the first screenshot below, the secondary public IPv4 address and the private IPv4 address is the FortiPAM public VIP and `port1` IP address respectively.



Network interface summary for eni-00674771afe7f28b8 (fpam1_public_wan_ni)

▼ Network interface details

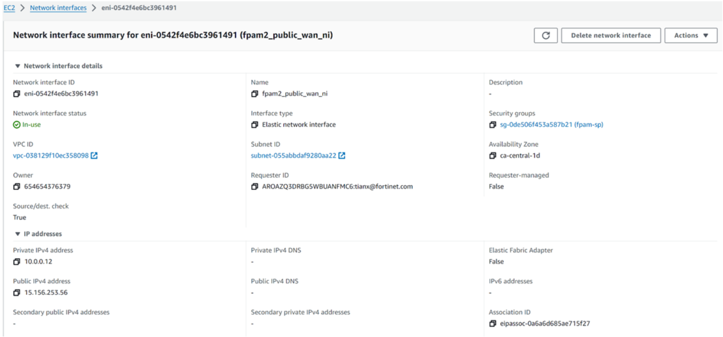
Network interface ID: eni-00674771afe7f28b8
Name: fpam1_public_wan_ni
Description: -
Network interface status: In-use
Interface type: Elastic network interface
Security groups: sg-0de506f453a587b21 (fpam-sp)
VPC ID: vpc-038129f10ec358098
Subnet ID: subnet-055abbdaf9280aa22
Availability Zone: ca-central-1d
Owner: 654654376379
Requester ID: AROAZQ3DRBG5WBUANFMC6:tianx@fortinet.com
Requester-managed: False
Source/dest. check: True

▼ IP addresses

Private IPv4 address: 10.0.0.11
Private IPv4 DNS: -
Elastic Fabric Adapter: False
Public IPv4 address: 3.96.245.132
Public IPv4 DNS: -
IPv6 addresses: -
Secondary public IPv4 addresses: 15.156.251.249
Secondary private IPv4 addresses: 10.0.0.13
Association ID: eipassoc-0c29a09cff4e3e8dd

From the second screenshot, the secondary public and private IP addresses are empty since it is the secondary backup FortiPAM for now.

When the primary FortiPAM is down, the secondary public and private IP addresses are displayed.



EC2 > Network interfaces > eni-0542f4e6bc3961491

Network interface summary for eni-0542f4e6bc3961491 (fpam2_public_wan_ni)

▼ Network interface details

Network interface ID: eni-0542f4e6bc3961491
Name: fpam2_public_wan_ni
Description: -
Network interface status: In-use
Interface type: Elastic network interface
Security groups: sg-0de506f453a587b21 (fpam-sp)
VPC ID: vpc-038129f10ec358098
Subnet ID: subnet-055abbdaf9280aa22
Availability Zone: ca-central-1d
Owner: 654654376379
Requester ID: AROAZQ3DRBG5WBUANFMC6:tianx@fortinet.com
Requester-managed: False
Source/dest. check: True

▼ IP addresses

Private IPv4 address: 10.0.0.12
Private IPv4 DNS: -
Elastic Fabric Adapter: False
Public IPv4 address: 15.156.253.56
Public IPv4 DNS: -
IPv6 addresses: -
Secondary public IPv4 addresses: -
Secondary private IPv4 addresses: -
Association ID: eipassoc-0a6a6d685ae715f27

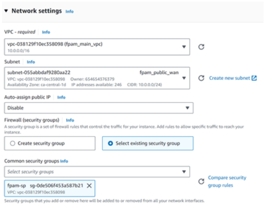
Configuring the FortiPAM instances on AWS

To configure FortiPAM instance:

1. Upload FortiPAM image and create the FortiPAM AMI.
   See Appendix J: Installation on AWS on page 492.

   Before launching the FortiPAM instance from AMI, you must create a FortiPAM security group.

   The following shows the FortiPAM instance network settings with VPC, public WAN subnet, and the security group created beforehand.



▼ Network settings

VPC - *required*
vpc-038129f10ec358098 (fpam_main_vpc)
10.0.0.0/16

Subnet
subnet-055abbdaf9280aa22 fpam_public_wan
VPC: vpc-038129f10ec358098 Owner: 654654376379
Availability Zone: ca-central-1d IP addresses available: 246 CIDR: 10.0.0.0/24)

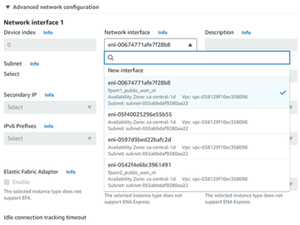
Auto-assign public IP
Disable

Firewall (security groups)
A security group is a set of firewall rules that control the traffic for your instance. Add rules to allow specific traffic to reach your instance.

○ Create security group ● Select existing security group

Common security groups
Select security groups
fpam-sp sg-0de506f453a587b21
VPC: vpc-038129f10ec358098
Security groups that you add or remove here will be added to or removed from all your network interfaces.

2. In *Advanced network configuration*, attach the four network interfaces created in Creating network interfaces on page 548 to the FortiPAM instance.



▼ Advanced network configuration

Network interface 1

Device index: 0

Network interface: eni-00674771afe7f28b8

Description

Subnet: Select

Secondary IP: Select

IPv6 Prefixes: Select

New interface

eni-00674771afe7f28b8 ✓
fpam1_public_wan_ni
Availability Zone: ca-central-1d Vpc: vpc-038129f10ec358098
Subnet: subnet-055abbdaf9280aa22

eni-05f40025296e55b55
Availability Zone: ca-central-1d Vpc: vpc-038129f10ec358098
Subnet: subnet-055abbdaf9280aa22

eni-0597d3bed22bafc2d
Availability Zone: ca-central-1d Vpc: vpc-038129f10ec358098
Subnet: subnet-055abbdaf9280aa22

eni-0542f4e6bc3961491
fpam2_public_wan_ni
Availability Zone: ca-central-1d Vpc: vpc-038129f10ec358098
Subnet: subnet-055abbdaf9280aa22

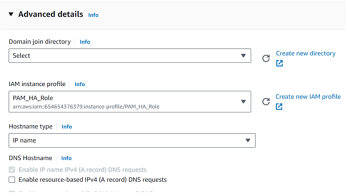
Elastic Fabric Adapter
□ Enable
The selected instance type does not support EFA.

The selected instance type does not support ENA Express.

The selected instance type does not support ENA Express.

Idle connection tracking timeout

3. In *Advanced details*, attach HA role to the FortiPAM instance.



▼ Advanced details

Domain join directory
Select

IAM instance profile
PAM_HA_Role
arn:aws:iam::654654376379:instance-profile/PAM_HA_Role

Hostname type
IP name

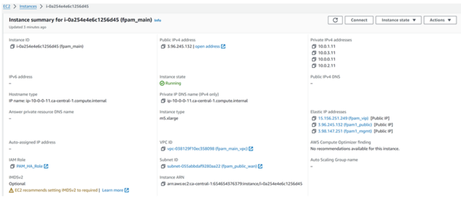
DNS Hostname
☑ Enable IP name IPv4 (A record) DNS requests
□ Enable resource-based IPv4 (A record) DNS requests

Launching the FortiPAM instance

The following shows the main configurations and network settings for the primary and the secondary FortiPAM instances.

Currently, both the FortiPAM GUI VIP and the `port1` IP address are attached to the main FortiPAM instance.

FPAM_MAIN



EC2 > Instances > i-0a254e4e6c1256d45

Instance summary for i-0a254e4e6c1256d45 (fpam_main)
Updated 3 minutes ago

Instance ID: i-0a254e4e6c1256d45 (fpam_main)

Public IPv4 address: 3.96.245.132 | open address

Private IPv4 addresses:
10.0.1.11
10.0.3.11
10.0.0.11
10.0.2.11

IPv6 address: –

Instance state: Running

Public IPv4 DNS: –

Hostname type: IP name: ip-10-0-0-11.ca-central-1.compute.internal

Private IP DNS name (IPv4 only): ip-10-0-0-11.ca-central-1.compute.internal

Answer private resource DNS name: –

Instance type: m5.xlarge

Elastic IP addresses:
15.156.251.249 (fpam_vip) [Public IP]
3.96.245.132 (fpam1_public) [Public IP]
3.98.147.251 (fpam1_mgmt) [Public IP]

Auto-assigned IP address: –

VPC ID: vpc-038129f10ec358098 (fpam_main_vpc)

AWS Compute Optimizer finding: No recommendations available for this instance.

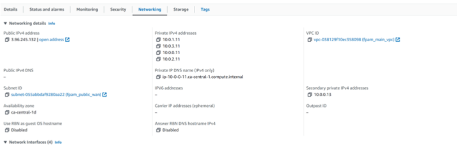
IAM Role: PAM_HA_Role

Subnet ID: subnet-055abbdaf9280aa22 (fpam_public_wan)

Auto Scaling Group name: –

IMDSv2: Optional
EC2 recommends setting IMDSv2 to required | Learn more

Instance ARN: arn:aws:ec2:ca-central-1:654654376379:instance/i-0a254e4e6c1256d45



Details | Status and alarms | Monitoring | Security | Networking | Storage | Tags

▼ Networking details

Public IPv4 address: 3.96.245.132 | open address

Private IPv4 addresses:
10.0.1.11
10.0.3.11
10.0.0.11
10.0.2.11

VPC ID: vpc-038129f10ec358098 (fpam_main_vpc)

Public IPv4 DNS: –

Private IP DNS name (IPv4 only): ip-10-0-0-11.ca-central-1.compute.internal

Subnet ID: subnet-055abbdaf9280aa22 (fpam_public_wan)

IPV6 addresses: –

Secondary private IPv4 addresses: 10.0.0.13

Availability zone: ca-central-1d

Carrier IP addresses (ephemeral): –

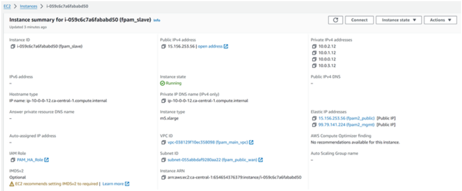
Outpost ID: –

Use RBN as guest OS hostname: Disabled

Answer RBN DNS hostname IPv4: Disabled

▼ Network Interfaces (4)

FPAM_SECONDARY



EC2 > Instances > i-059c6c7a6fababd50

Instance summary for i-059c6c7a6fababd50 (fpam_slave) Info

Updated 3 minutes ago

Instance ID
i-059c6c7a6fababd50 (fpam_slave)

Public IPv4 address
15.156.253.56 | open address

Private IPv4 addresses
10.0.2.12
10.0.1.12
10.0.0.12
10.0.3.12

IPv6 address
–

Instance state
Running

Public IPv4 DNS
–

Hostname type
IP name: ip-10-0-0-12.ca-central-1.compute.internal

Private IP DNS name (IPv4 only)
ip-10-0-0-12.ca-central-1.compute.internal

Answer private resource DNS name
–

Instance type
m5.xlarge

Elastic IP addresses
15.156.253.56 (fpam2_public) [Public IP]
99.79.141.224 (fpam2_mgmt) [Public IP]

Auto-assigned IP address
–

VPC ID
vpc-038129f10ec358098 (fpam_main_vpc)

AWS Compute Optimizer finding
No recommendations available for this instance.

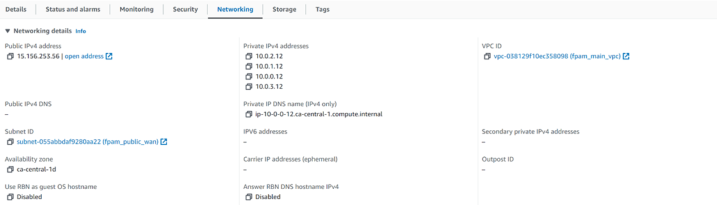
IAM Role
PAM_HA_Role

Subnet ID
subnet-055abbdaf9280aa22 (fpam_public_wan)

Auto Scaling Group name
–

IMDSv2
Optional
⚠ EC2 recommends setting IMDSv2 to required | Learn more

Instance ARN
arn:aws:ec2:ca-central-1:654654376379:instance/i-059c6c7a6fababd50



▼ Networking details Info

Public IPv4 address
15.156.253.56 | open address

Private IPv4 addresses
10.0.2.12
10.0.1.12
10.0.0.12
10.0.3.12

VPC ID
vpc-038129f10ec358098 (fpam_main_vpc)

Public IPv4 DNS
–

Private IP DNS name (IPv4 only)
ip-10-0-0-12.ca-central-1.compute.internal

Subnet ID
subnet-055abbdaf9280aa22 (fpam_public_wan)

IPV6 addresses
–

Secondary private IPv4 addresses
–

Availability zone
ca-central-1d

Carrier IP addresses (ephemeral)
–

Outpost ID
–

Use RBN as guest OS hostname
Disabled

Answer RBN DNS hostname IPv4
Disabled

Configuring FortiPAM HA

After the FortiPAM instance boots up, configure `FortiPAM_A` interfaces and the static route as below:

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

```
 config system interface
  edit "port1"
   set ip 10.0.0.13 255.255.255.0
   set allowaccess ping ssh ftm
  next
  edit "port2"
   set ip 10.0.1.11 255.255.255.0
   set allowaccess ping ssh
  end
  edit "port4"
   set ip 10.0.3.11 255.255.255.0
   set allowaccess ping ssh
  next
 end
 config router static
  edit
   set gateway 10.0.0.1
   set device "port1"
  next
 end
config system ha
 set group-name "test"
 set mode active-passive
 set password 123 #change into a personal password. FortiPAM primary and secondary share
the same password.
 set hbdev "port3" 0
 set ha-mgmt-status enable
 config ha-mgmt-interface
  edit 1
   set interface "port4"
   set gateway 10.0.3.1
  next
 end
 set override enable
 set priority 250
 set unicaset-status enable
 set unicast-gateway 10.0.2.1
 config unicast-peers
  edit 1
   set peer-ip 10.0.2.12
  next
 end
end
config system vdom-exeption
 edit 1
  set object router static
 next
 edit 2
  set object system.interface
  next
  edit 3
   set object firewall.vip
  next
 end
```

2. Login to `FortiPAM_A` with the VIP and add a valid FortiPAM license.
   To add a license to the FortiPAM instance on AWS, see Licensing.
3. After the license has been validated, power off `FortiPAM_A` instance.
4. Configure `FortiPAM_B` as `FortiPAM_A`:

```
  config system interface
   edit "port1"
    set ip 10.0.0.13 255.255.255.0
    set allowaccess ping ssh ftm
   next
   edit "port2"
    set ip 10.0.1.12 255.255.255.0
   set allowaccess ping ssh
   next
   edit "port3"
    set ip 10.0.2.12 255.255.255.0
    set allowaccess ping ssh
   next
   edit "port4"
    set ip 10.0.3.12 255.255.255.0
    set allowaccess ping ssh
   next
  end
  config router static
   edit 1
    set gateway 10.0.0.1
    set device "port1"
   next
  end
  config system ha
   set group-name "test"
   set password 123 #change into a personal password. FortiPAM primary and secondary
share the same password.
   set mode active-passive
   set hbdev "port3" 0
```

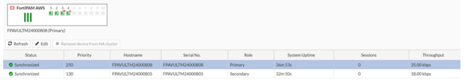
```
        set ha-mgmt-status enable
         edit 1
          set interface "port4"
          set gateway 10.0.3.1
         next
        end
        set override enable
        set priority 130
        set unicast-status enable
        set unicaset-gateway 10.0.2.1
        config unicast-peers
         edit 1
          set peer-ip 10.0.2.11
         next
        end
       end
       config system vdom-exception
        edit 1
         set object router.static
        next
        edit 2
         set object system.interface
        next
        edit 3
         set object firewall.vip
        next
       end
```

After FortiPAM_B license has been validated, you can power on the FortiPAM_A.

Testing and debugging HA failover

1. In the CLI console, enter the following command to verify that FortiPAM units are in sync:

   ```
   get system ha
   ```

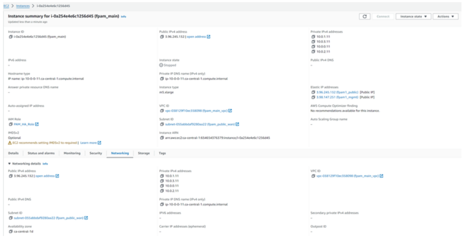
   FPAVULTM24000808 (Primary)

Status	Priority	Hostname	Serial No.	Role	System Uptime	Sessions	Throughput
Synchronized	250	FPAVULTM24000808	FPAVULTM24000808	Primary	36m 53s	0	35.00 kbps
Synchronized	130	FPAVULTM24000805	FPAVULTM24000805	Secondary	32m 50s	0	18.00 kbps

2. In the FortiPAM GUI, create a secret.
   To create a secret, see Creating a secret on page 72.

   Verify that you can launch the secret.

   See Launching a secret on page 97.
3. Before you power off PAM_MAIN, you can see that the second IP address (10.0.0.0.13) and the VIP (15.156.251.249) are attached to PAM_MAIN.
   The second IP address and the VIP are not attached to PAM_SECONDARY.
4. Power off PAM_MAIN.
5. Wait for five seconds and you can relogin to FortiPAM GUI successfully.
6. Launch the secret that was set up in step 2.
   You should be able to successfully launch the secret.
7. Check the PAM_SECONDARY status on AWS, you can see that both the second IP address (10.0.0.13) and the VIP (52.40.235.215) attached to the PAM_MAIN move to FortiPAM_B leaving FortiPAM_A.
   PAM_MAIN status



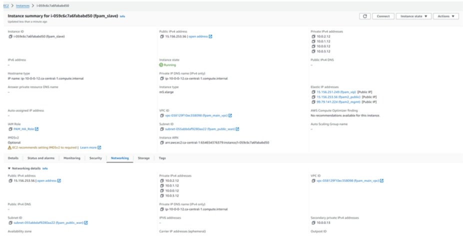
Instance summary for i-0a254e4e6c1256d45 (fpam_main)
Updated less than a minute ago

Instance ID: i-0a254e4e6c1256d45 (fpam_main)
Public IPv4 address: 3.96.245.132 | open address
Private IPv4 addresses: 10.0.1.11, 10.0.3.11, 10.0.0.11, 10.0.2.11
IPv6 address: –
Instance state: Stopped
Public IPv4 DNS: –
Hostname type: IP name: ip-10-0-0-11.ca-central-1.compute.internal
Private IP DNS name (IPv4 only): ip-10-0-0-11.ca-central-1.compute.internal
Answer private resource DNS name: –
Instance type: m5.xlarge
Elastic IP addresses: 3.96.245.132 (fpam1_public) [Public IP], 3.98.147.251 (fpam1_mgmt) [Public IP]
Auto-assigned IP address: –
VPC ID: vpc-038129f10ec358098 (fpam_main_vpc)
AWS Compute Optimizer finding: No recommendations available for this instance.
IAM Role: PAM_HA_Role
Subnet ID: subnet-055abbdaf9280aa22 (fpam_public_wan)
Auto Scaling Group name: –
IMDSv2: Optional
⚠ EC2 recommends setting IMDSv2 to required | Learn more
Instance ARN: arn:aws:ec2:ca-central-1:654654376379:instance/i-0a254e4e6c1256d45

▼ Networking details Info

Public IPv4 address: 3.96.245.132 | open address
Private IPv4 addresses: 10.0.1.11, 10.0.3.11, 10.0.0.11, 10.0.2.11
VPC ID: vpc-038129f10ec358098 (fpam_main_vpc)
Public IPv4 DNS: –
Private IP DNS name (IPv4 only): ip-10-0-0-11.ca-central-1.compute.internal
Subnet ID: subnet-055abbdaf9280aa22 (fpam_public_wan)
IPV6 addresses: –
Secondary private IPv4 addresses: –
Availability zone: ca-central-1d
Carrier IP addresses (ephemeral): –
Outpost ID: –

The PAM_SECONDARY automatically attaches with the FortiPAM GUI VIP and the port1 IP address as the secondary private IP address (10.0.0.13).



Instance summary for i-059c6c7a6fababd50 (fpam_slave)
Updated less than a minute ago

Instance ID: i-059c6c7a6fababd50 (fpam_slave)
Public IPv4 address: 15.156.253.56 | open address
Private IPv4 addresses: 10.0.2.12, 10.0.1.12, 10.0.0.12, 10.0.3.12
IPv6 address: –
Instance state: Running
Public IPv4 DNS: –
Hostname type: IP name: ip-10-0-0-12.ca-central-1.compute.internal
Private IP DNS name (IPv4 only): ip-10-0-0-12.ca-central-1.compute.internal
Answer private resource DNS name: –
Instance type: m5.xlarge
Elastic IP addresses: 15.156.251.249 (fpam_vip) [Public IP], 15.156.253.56 (fpam2_public) [Public IP], 99.79.141.224 (fpam2_mgmt) [Public IP]
Auto-assigned IP address: –
VPC ID: vpc-038129f10ec358098 (fpam_main_vpc)
AWS Compute Optimizer finding: No recommendations available for this instance.
IAM Role: PAM_HA_Role
Subnet ID: subnet-055abbdaf9280aa22 (fpam_public_wan)
Auto Scaling Group name: –
IMDSv2: Optional
⚠ EC2 recommends setting IMDSv2 to required | Learn more
Instance ARN: arn:aws:ec2:ca-central-1:654654376379:instance/i-059c6c7a6fababd50

▼ Networking details Info

Public IPv4 address: 15.156.253.56 | open address
Private IPv4 addresses: 10.0.2.12, 10.0.1.12, 10.0.0.12, 10.0.3.12
VPC ID: vpc-038129f10ec358098 (fpam_main_vpc)
Public IPv4 DNS: –
Private IP DNS name (IPv4 only): ip-10-0-0-12.ca-central-1.compute.internal
Subnet ID: subnet-055abbdaf9280aa22 (fpam_public_wan)
IPV6 addresses: –
Secondary private IPv4 addresses: 10.0.0.13
Availability zone
Carrier IP addresses (ephemeral)
Outpost ID

When you SSH to the PAM_SECONDARY and enable the debug command, you can power off PAM_MAIN to trigger a failover.

```
diagnose debug en
diag nose debug application awsd-1
```

You can now see some HA failover debug information.

Appendix R: FortiPAM HA on Azure

To deploy and configure FortiPAM as an Active-Passive HA solution:

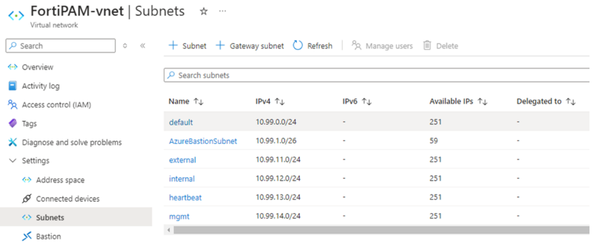
1. Configuring Azure virtual network and subnets on page 556
2. Creating public IP addresses on page 557
3. Creating the FortiPAM-VM on Azure on page 558
4. Enabling HA on FortiPAM on page 559
5. Accessing the FortiPAM GUI portal on page 563
6. Accessing HA management interface on page 563
7. Setting up SDN connector on page 564
8. Configuring SDN connector on FortiPAM on page 567
9. Accessing the GUI portal after the HA failover on page 569
10. Adding a DR node on page 569
11. Verification on page 574

Configuring Azure virtual network and subnets

We configure a virtual network with four subnets:

- One to access to the FortiPAM GUI portal
- (Optional) One to connect to the internal target servers
- One for HA heartbeat
- One for dedicated HA management

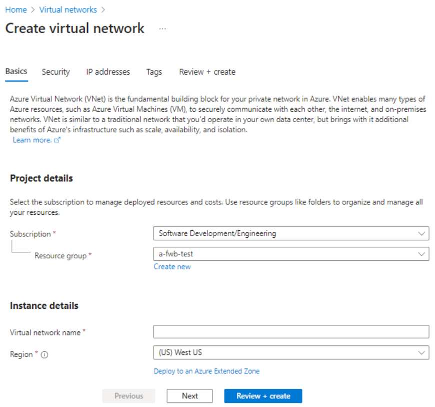
The following shows a virtual network with four subnets: *external*, *internal*, *heartbeat*, and *mgmt*.



Name	IPv4	IPv6	Available IPs	Delegated to
default	10.99.0.0/24	-	251	-
AzureBastionSubnet	10.99.1.0/26	-	59	-
external	10.99.11.0/24	-	251	-
internal	10.99.12.0/24	-	251	-
heartbeat	10.99.13.0/24	-	251	-
mgmt	10.99.14.0/24	-	251	-

To configure Azure virtual network and subnets:

1. In the Azure portal, using the search bar, open *Virtual networks*.
2. From the list, select +*Create*.
   The *Create virtual network* wizard opens.



Create virtual network

Azure Virtual Network (VNet) is the fundamental building block for your private network in Azure. VNet enables many types of Azure resources, such as Azure Virtual Machines (VM), to securely communicate with each other, the internet, and on-premises networks. VNet is similar to a traditional network that you'd operate in your own data center, but brings with it additional benefits of Azure's infrastructure such as scale, availability, and isolation.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * Software Development/Engineering

Resource group * a-fwb-test

Instance details

Virtual network name *

Region * (US) West US

3. From the *Subscription* dropdown, select a subscription.
4. From the *Resource group* dropdown, select a resource group.
5. In *Virtual network name*, enter a name for the virtual network.
6. In *Region*, select a region where the virtual network is created.
7. Click *Next*.
8. Click *Next*.
9. In *Add IPv4 address space*, define the address space.
   For example, an address space `10.0.0.0/16` defines the IP range for the virtual network.
10. Select *Add a subnet* to add subnets to the virtual network.
    The *Add a subnet* window opens.
    a. Enter a name for the subnet.
    b. Define an IP range for the subnet.
    c. Click *Add*.
11. Repeat step 10 to add three more subnets.
12. Click *Review + create*.
13. Review the configuration.
14. Click *Create*.

Creating public IP addresses

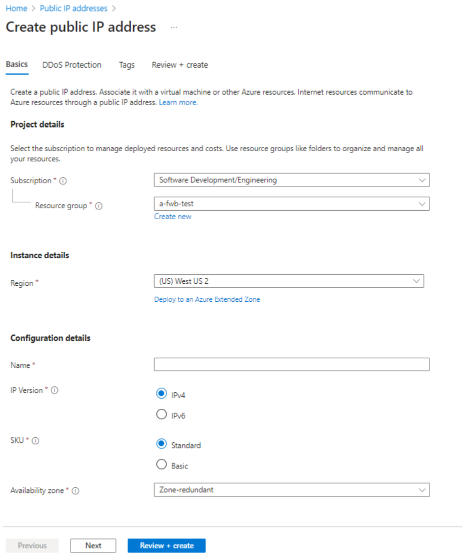
We create three public IP addresses:

- One for traffic to the active (primary) FortiPAM. In case of failover, the IP address moves from the primary FortiPAM to the secondary.
- Two for management access to each FortiPAM.

All the internal IP addresses for the FortiPAM-VM must be static on the Azure portal.

To create a public IP address:

1. In the Azure portal, using the search bar, open *Public IP addresses*.
2. From the list, select *Create*.
   The *Create public IP address* wizard opens.



Create a public IP address. Associate it with a virtual machine or other Azure resources. Internet resources communicate to Azure resources through a public IP address. Learn more.

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * : Software Development/Engineering

Resource group * : a-fwb-test (Create new)

Instance details

Region * : (US) West US 2 (Deploy to an Azure Extended Zone)

Configuration details

Name * :

IP Version * : ● IPv4 ○ IPv6

SKU * : ● Standard ○ Basic

Availability zone * : Zone-redundant

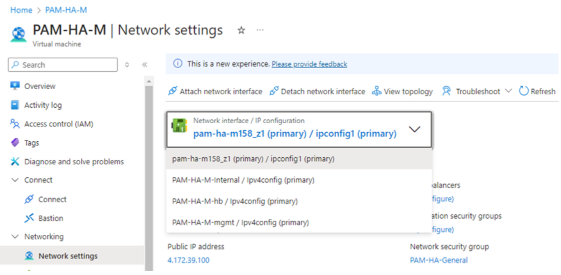
3. From the *Subscription* dropdown, select a subscription.
4. From the *Resource group* dropdown, select a resource group.
5. In *Region*, select a region where the public IP address is created.
6. In *Name*, enter the name for the public IP address.
7. In *IP Version*, select *IPv4*.
8. Click *Next*.
9. Click *Review+create* to create the public IP address.
10. Repeat steps 1 - 9 to create two additional public IP addresses.

Creating the FortiPAM-VM on Azure

To create the FortiPAM-VM on Azure:

1. Create two FortiPAM VMs on Azure.
   See Appendix G: Installation on Azure on page 476.
   Ensure that the following are correctly configured:
   a. Each FortiPAM-VM should be in the same region and they must have the same VM and disk size.
   b. Add four network interfaces to the FortiPAM-VM.
      One interface for every subnet in the same order.

      Following is the network settings for the primary FortiPAM node:



This is a new experience. Please provide feedback

Network interface / IP configuration: pam-ha-m158_z1 (primary) / ipconfig1 (primary)

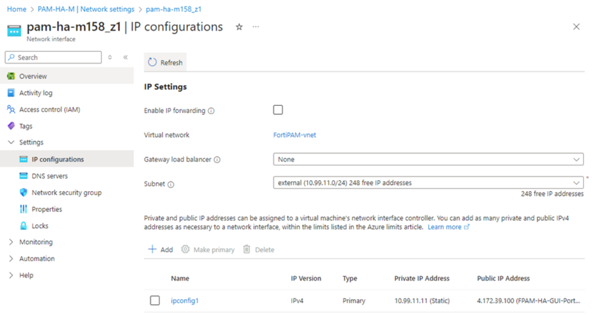
pam-ha-m158_z1 (primary) / ipconfig1 (primary)
PAM-HA-M-Internal / Ipv4config (primary)
PAM-HA-M-hb / Ipv4config (primary)
PAM-HA-M-mgmt / Ipv4config (primary)

Public IP address: 4.172.39.100

Network security group: PAM-HA-General

   c. Assign the public IP address to the external interface of the primary FortiPAM.
      Go to *Settings* > *IP configurations* in the network interface for the primary FortiPAM node.

      Following is the IP configuration for the FortiPAM primary node external interface:



pam-ha-m158_z1 | IP configurations

IP Settings

Enable IP forwarding ☐

Virtual network: FortiPAM-vnet

Gateway load balancer: None

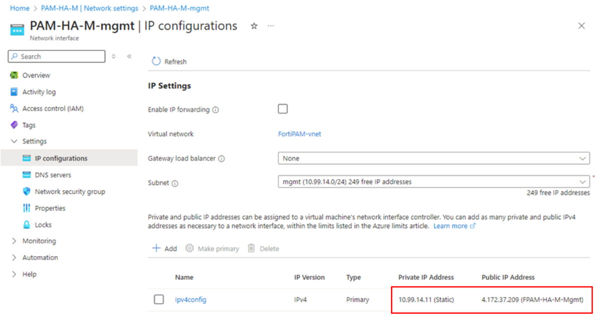
Subnet: external (10.99.11.0/24) 248 free IP addresses

248 free IP addresses

Private and public IP addresses can be assigned to a virtual machine's network interface controller. You can add as many private and public IPv4 addresses as necessary to a network interface, within the limits listed in the Azure limits article. Learn more

	Name	IP Version	Type	Private IP Address	Public IP Address
☐	ipconfig1	IPv4	Primary	10.99.11.11 (Static)	4.172.39.100 (FPAM-HA-GUI-Port...

d. Assign the public IP addresses to the *mgmt* interface of the primary FortiPAM.
Following is the FortiPAM primary node management interface IP configuration:



PAM-HA-M-mgmt | IP configurations

IP Settings

Enable IP forwarding ☐

Virtual network: FortiPAM-vnet

Gateway load balancer: None

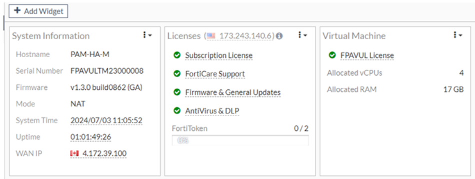
Subnet: mgmt (10.99.14.0/24) 249 free IP addresses

249 free IP addresses

Private and public IP addresses can be assigned to a virtual machine's network interface controller. You can add as many private and public IPv4 addresses as necessary to a network interface, within the limits listed in the Azure limits article. Learn more

	Name	IP Version	Type	Private IP Address	Public IP Address
☐	Ipv4config	IPv4	Primary	10.99.14.11 (Static)	4.172.37.209 (FPAM-HA-M-Mgmt)

e. Each FortiPAM instance must have its own valid license.



System Information

Hostname	PAM-HA-M
Serial Number	FPAVULTM23000008
Firmware	v1.3.0 build0862 (GA)
Mode	NAT
System Time	2024/07/03 11:05:52
Uptime	01:01:49:26
WAN IP	4.172.39.100

Licenses (173.243.140.6)

- ✓ Subscription License
- ✓ FortiCare Support
- ✓ Firmware & General Updates
- ✓ AntiVirus & DLP

FortiToken 0 / 2 (0%)

Virtual Machine

✓ FPAVUL License

Allocated vCPUs	4
Allocated RAM	17 GB

Enabling HA on FortiPAM

To enable HA on FortiPAM:

1. Configure the network interfaces on FortiPAM to match the IP addresses configured on Azure network interfaces.
   To configure a network interface, see Editing an interface on page 358.

   The following IP addresses are configured on Azure:

	port1 (external)	port2 (internal)	port3 (heartbeat)	port4 (mgmt)
Primary	10.99.11.11/24 Public IP address: 4.172.39.100	10.99.12.11/24	10.99.13.11/24	10.99.14.11/24 Public IP address: 4.172.37.209
Secondary	10.99.11.12/24	10.99.12.12/24	10.99.13.12/24	10.99.14.12/24 Public IP address: 4.172.38.127

2. To enable HA, all the interfaces on FortiPAM must be in the static mode. After changing the `port1` interface from dynamic (DHCP) mode to static, a static router must be added. SSH should also be enabled on `port4` (*mgmt* interface) using `set allowaccess ssh`.

The following shows the system interface configuration for the primary HA node:

```
config system interface
 edit "port1" #private IP address for the external subnet
  set ip 10.99.11.11 255.255.255.0
  set type physical
  set snmp-index 1
  next
  edit "port2" #private IP address for the internal subnet
   set ip 10.99.12.11 255.255.255.255.0
   set type physical
   set snmp-index 3
  next
  edit "port3" #private IP address for the heartbeat subnet
   set ip 10.99.13.11 255.255.255.0
   set type physical
   set snmp-index 4
  next
  edit "port4" #private IP address for the mgmt subnet
   set ip 10.99.14.11 255.255.255.0
   set allowaccess ssh
   set type physical
   set snmp-index 5
  next
  edit "ssl.root"
   set type tunnel
   set alias "SSL VPN interface"
   set snmp-index 2
  next
 end
 show router static
 config router static
  edit 1 #gateway for the private IP address for the external interface
   set gateway 10.99.11.1
   set device "port1"
  next
 end
```

The following shows the system interface configuration for the HA secondary node:

```
config system interface
 edit "port1" #private IP address for the external subnet
  set ip 10.99.11.11 255.255.255.0
  set type physical
  set snmp-index 1
 next
 edit "port2" #private IP address for the internal subnet
  set ip 10.99.12.11 255.255.255.0
  set type physical
  set snmp-index 3
 next
 edit "port3" #private IP address for the heartbeat subnet
  set ip 10.99.13.12 255.255.255.0
  set type physical
  set snmp-index 4
 next
 edit "port4" #private IP address for the mgmt subnet
  set ip 10.99.14.12 255.255.255.0
```

```
      set allowaccess ssh
      set type physical
      set snmp-index 5
    next
    edit "ssl.root"
      set type tunnel
      set alias "SSL VPN interface"
      set snmp-index 2
    next
  end
  show router static
  config router static
    edit 1 #gateway for the private IP address for the external interface
      set gateway 10.99.11.1
      set device "port1"
    next
  end
```

3. **Configuring `vdom-exception`**.
   Add objects that can be configured independently across different HA members.

   In the CLI console, enter the following commands:

   ```
   config system vdom-exception
    edit 1
     set object system.interface
    next
    edit 2
     set object firewall.vip
    next
   end
   ```

4. **Configuring HA in System**.
   Enable HA on the primary and the secondary FortiPAM.
   a. On the primary FortiPAM, go to *System* > *HA* and enter a higher priority value in *Device priority*.
   b. Configure the same *Group name* and *Password* on the primary and the secondary FortiPAM units.
   c. In *Heartbeat interfaces*, select +, from *Select Entries*, select `port3`, and click *Close.*
   d. In *Management Interface Reservation*, in *Interface*, select `port4`.
   e. In *Gateway*, enter the remote gateway IPv4 address.
   f. In *Destination subnet*, enter the destination subnet.
   g. Enable *Unicast Status*.
   h. Enter the gateway IPv4 address.
   i. In *Peer IP*, select +, enter the IP address of the HA heartbeat interface of the other FortiPAM-VM in the HA cluster.

      On the primary FortiPAM, set *Peer IP* as the `port3` (heartbeat) private IP address of the secondary FortiPAM.

      On the secondary FortiPAM, set *Peer IP* as the `port3` (heartbeat) private IP address of the primary FortiPAM.

      The following shows the HA configuration on the primary and the secondary FortiPAM nodes in the HA cluster:

      Primary

      ```
      config system ha
       set group-name "Azure_PAM_HA"
       set mode active-passive
       set password ENC XghDJZtZmoAMNt2RcCq
      ```

```
   set hbdev "port3" 0
   set ha-mgmt-status enable
   config ha-mgmt-interfaces
    edit 1 #gateway for the private IP address of the mgmt interface
     set interface "port4"
     set gateway 10.99.14.1
    next
   end
   set override enable
   set priority 200
   set unicast-status enable
   set unicast-gateway 10.99.13.1 #gateway for the private IP address of the HB
interface
   config unicast-peers
    edit 1
     set peer-ip 10.99.13.12 #private IP address of the secondary FortiPAM HB
interface
    next
   end
  end
```

Secondary

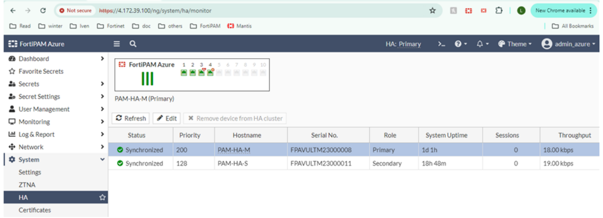
```
  config system ha
   set group-name "Azure_PAM_HA"
   set mode active-passive
   set password ENC XghDJZtZmoAMNt2RcCq
   set hbdev "port3" 0
   set ha-mgmt-status enable
   config ha-mgmt-interface
    edit 1 #gateway for the private IP address of the mgmt interface
     set interface "port4"
     set gateway 10.99.14.1
    next
   end
   set override enable
   set unicast-status enable
   set unicast-gateway 10.99.13.1 #gateway for the private IP address of the HB
interface
   config unicast-peers
    edit 1
     set peer-ip 10.99.13.11 #private IP address of the primary FortiPAM HB interface
    next
   end
  end
```

j. Click *OK*.

Accessing the FortiPAM GUI portal

To access the FortiPAM GUI portal:

1. Use the `port1` public IP address and verify that the HA cluster is in sync.



PAM-HA-M (Primary)

Status	Priority	Hostname	Serial No.	Role	System Uptime	Sessions	Throughput
Synchronized	200	PAM-HA-M	FPAVULTM23000008	Primary	1d 1h	0	18.00 kbps
Synchronized	128	PAM-HA-S	FPAVULTM23000011	Secondary	18h 48m	0	19.00 kbps

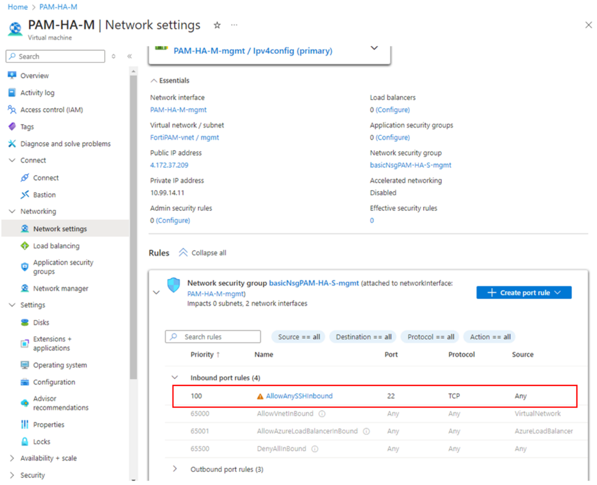
Accessing HA management interface

To access the HA management interface:

To access the management interface of the FortiPAM HA member, SSH to the public IP address associated to the `port4`.

Note:

1. On the Azure portal, `port22` must be allowed in the Network security group of the management interface.



Network interface
PAM-HA-M-mgmt

Virtual network / subnet
FortiPAM-vnet / mgmt

Public IP address
4.172.37.209

Private IP address
10.99.14.11

Admin security rules
0 (Configure)

Load balancers
0 (Configure)

Application security groups
0 (Configure)

Network security group
basicNsgPAM-HA-S-mgmt

Accelerated networking
Disabled

Effective security rules
0

Network security group basicNsgPAM-HA-S-mgmt (attached to networkInterface: PAM-HA-M-mgmt)
Impacts 0 subnets, 2 network interfaces

Priority ↑	Name	Port	Protocol	Source
Inbound port rules (4)				
100	AllowAnySSHInbound	22	TCP	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer
65500	DenyAllInBound	Any	Any	Any
Outbound port rules (3)				

2. On FortiPAM, SSH must be enabled on `port4`.

```
show system interface
config system interface
 edit "port1"
  set ip 10.99.11.11 255.255.255.0
  set type physical
  set snmp-index 1
 next
 edit "port2"
  set ip 10.99.12.11 255.255.255.0
  set type physical
  set snmp-index 3
  next
  edit "port4"
```

```
   set ip 10.99.14.12 255.255.255.0
   set allowaccess ping ssh #ssh enabled on port4
   set type physical
   set snmp-index 5
  next
  edit "ssl.root"
   set type tunnel
   set alias "SSL VPN interface"
   set snmp-index 2
  next
end
```

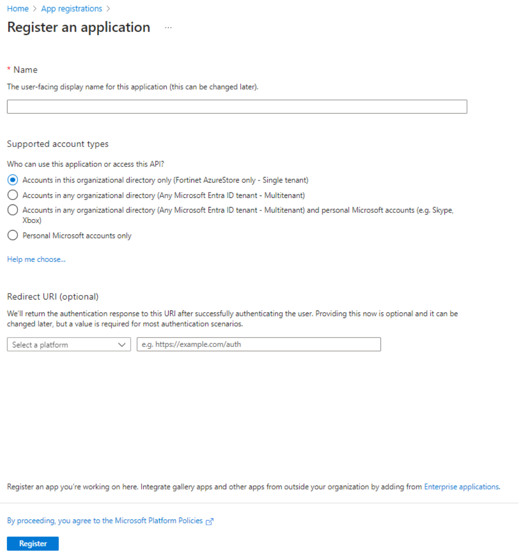
Setting up SDN connector

Adding Azure application registration

We add the Azure application registration to allow FortiPAM to make the API call.

To add Azure application registration:

1. In the Azure portal, using the search bar, open *App registrations*.
2. Select *New registration*.
   The *Register an application* wizard opens.



Home > App registrations >

Register an application ···

* Name

The user-facing display name for this application (this can be changed later).

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Fortinet AzureStore only - Single tenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant)

○ Accounts in any organizational directory (Any Microsoft Entra ID tenant - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

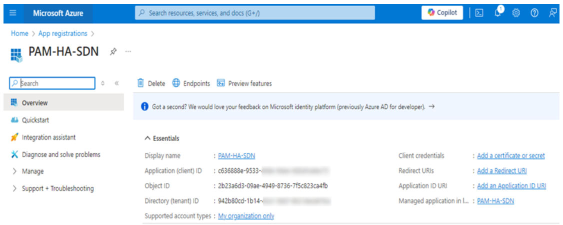
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Select a platform | e.g. https://example.com/auth

Register an app you're working on here. Integrate gallery apps and other apps from outside your organization by adding from Enterprise applications.

By proceeding, you agree to the Microsoft Platform Policies

3. In *Name*, enter a name for the application.
4. Keep the default setting for *Supported account types*.
5. Click *Register*.
   The application is created.


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home > App registrations >
Delete
Endpoints
Preview features
Overview
Quickstart
Integration assistant
Diagnose and solve problems
Manage
Support + Troubleshooting

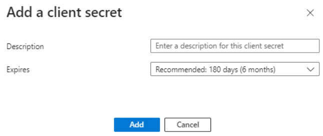
PAM-HA-SDN

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name : PAM-HA-SDN
Application (client) ID : c636888e-9533-[redacted]
Object ID : 2b23a6d3-09ae-4949-8736-7f5c823ca4fb
Directory (tenant) ID : 942b80cd-1b14-[redacted]
Supported account types : My organization only
Client credentials : Add a certificate or secret
Redirect URIs : Add a Redirect URI
Application ID URI : Add an Application ID URI
Managed application in l... : PAM-HA-SDN

6. Creating a client secret for the new application:
   a. In the new application, go to *Manage* > *Certificates & secrets*.
   b. Go to the *Client secrets* tab.
   c. Select *New client secret*.
      The *Add a client secret* window opens.



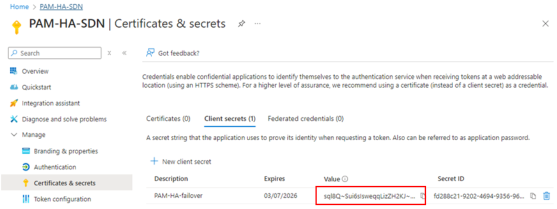
Add a client secret

Description: Enter a description for this client secret
Expires: Recommended: 180 days (6 months)

   d. From the *Expires* dropdown, choose an expiration time for the client secret.

You must renew the client secret on time for HA to failover properly.

   e. Click *Add*.
   f. Copy and save the client secret value on your management computer.
      The secret value is used in the FortiPAM SDN connection configuration.



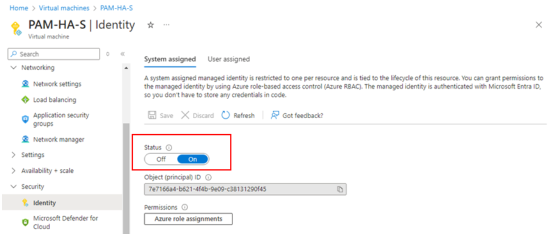
PAM-HA-SDN | Certificates & secrets

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
PAM-HA-failover	03/07/2026	sql8Q~Sui6sIsweqqLizZH2KJ~...	fd288c21-9202-4694-9356-96...

7. Adding an Azure IAM role:
   Add IAM role for the FortiPAM-VM and the SDN application.
   a. In the Azure portal, using the search bar, open *Virtual machines*.
   b. From the list, click to open the secondary FortiPAM-VM.
   c. Go to *Security* > *Identity* and ensure that the FortiPAM-VM has the system assigned managed identity status enabled.



PAM-HA-S | Identity
Virtual machine

A system assigned managed identity is restricted to one per resource and is tied to the lifecycle of this resource. You can grant permissions to the managed identity by using Azure role-based access control (Azure RBAC). The managed identity is authenticated with Microsoft Entra ID, so you don't have to store any credentials in code.

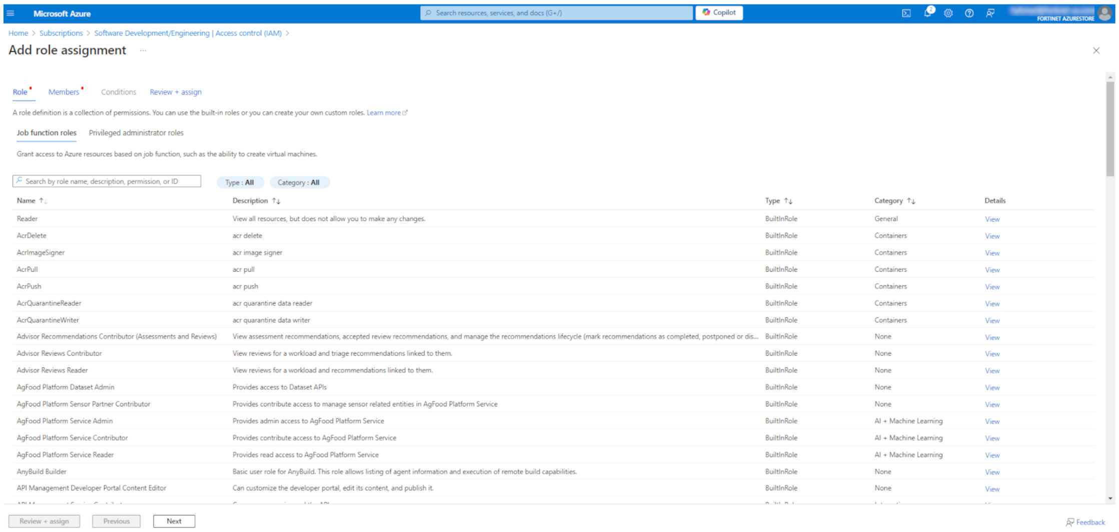
Status: Off [✓ On]

Object (principal) ID: 7e7166a4-b621-4f4b-9e09-c38131290f45

Permissions

   d. Adding role assignment:
      i. In the Azure portal, using the search bar, open *Subscriptions*.
      ii. Click to open the subscription and go to *Access Control (IAM)*.

iii. Select *Add* > *Add role assignment* to add a role assignment.



Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
FORTINET AZURESTORE
Home > Subscriptions > Software Development/Engineering | Access control (IAM) >
Role
Members
Conditions
Review + assign
Job function roles
Privileged administrator roles
Search by role name, description, permission, or ID
Type : All
Category : All
Review + assign
Previous
Next
Feedback

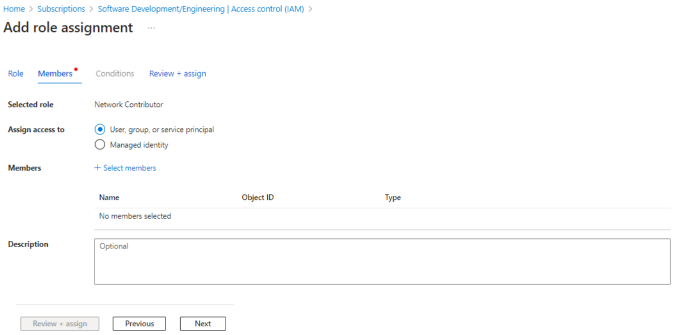
Add role assignment

A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more

Grant access to Azure resources based on job function, such as the ability to create virtual machines.

Name ↑↓	Description ↑↓	Type ↑↓	Category ↑↓	Details
Reader	View all resources, but does not allow you to make any changes.	BuiltInRole	General	View
AcrDelete	acr delete	BuiltInRole	Containers	View
AcrImageSigner	acr image signer	BuiltInRole	Containers	View
AcrPull	acr pull	BuiltInRole	Containers	View
AcrPush	acr push	BuiltInRole	Containers	View
AcrQuarantineReader	acr quarantine data reader	BuiltInRole	Containers	View
AcrQuarantineWriter	acr quarantine data writer	BuiltInRole	Containers	View
Advisor Recommendations Contributor (Assessments and Reviews)	View assessment recommendations, accepted review recommendations, and manage the recommendations lifecycle (mark recommendations as completed, postponed or dis...	BuiltInRole	None	View
Advisor Reviews Contributor	View reviews for a workload and triage recommendations linked to them.	BuiltInRole	None	View
Advisor Reviews Reader	View reviews for a workload and recommendations linked to them.	BuiltInRole	None	View
AgFood Platform Dataset Admin	Provides access to Dataset APIs	BuiltInRole	None	View
AgFood Platform Sensor Partner Contributor	Provides contribute access to manage sensor related entities in AgFood Platform Service	BuiltInRole	None	View
AgFood Platform Service Admin	Provides admin access to AgFood Platform Service	BuiltInRole	AI + Machine Learning	View
AgFood Platform Service Contributor	Provides contribute access to AgFood Platform Service	BuiltInRole	AI + Machine Learning	View
AgFood Platform Service Reader	Provides read access to AgFood Platform Service	BuiltInRole	AI + Machine Learning	View
AnyBuild Builder	Basic user role for AnyBuild. This role allows listing of agent information and execution of remote build capabilities.	BuiltInRole	None	View
API Management Developer Portal Content Editor	Can customize the developer portal, edit its content, and publish it.	BuiltInRole	None	View

iv. From the list, select *Network Contributor*, and click *Next*.
The *Add role assignment* wizard opens.



Home > Subscriptions > Software Development/Engineering | Access control (IAM) >
Role
Members
Conditions
Review + assign
Review + assign
Previous
Next

Add role assignment

Selected role: Network Contributor

Assign access to: ● User, group, or service principal ○ Managed identity

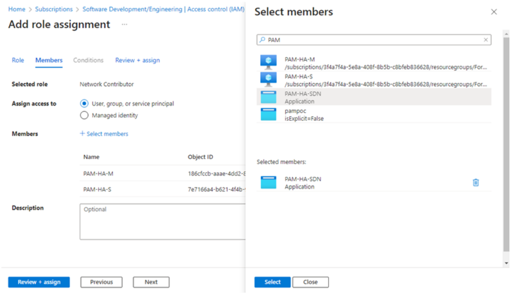
Members: + Select members

Name	Object ID	Type
No members selected		

Description: Optional

v. In *Assign access to*, for *User, group, or service principal*:

i. In *Members*, select +*Select members*, from *Select members*, select the SDN application.



Home > Subscriptions > Software Development/Engineering | Access control (IAM)
Role
Members
Conditions
Review + assign
Review + assign
Previous
Next
Select
Close

Add role assignment

Selected role: Network Contributor

Assign access to: ● User, group, or service principal ○ Managed identity

Members: + Select members

Name	Object ID
PAM-HA-M	186cfccb-aaae-4dd2-8
PAM-HA-S	7e7166a4-b621-4f4b-

Description: Optional

Select members

PAM

PAM-HA-M
/subscriptions/3f4a7f4a-5e8a-408f-8b5b-c8bfeb836628/resourcegroups/For...

PAM-HA-S
/subscriptions/3f4a7f4a-5e8a-408f-8b5b-c8bfeb836628/resourcegroups/For...

PAM-HA-SDN
Application

pampoc
isExplicit=False

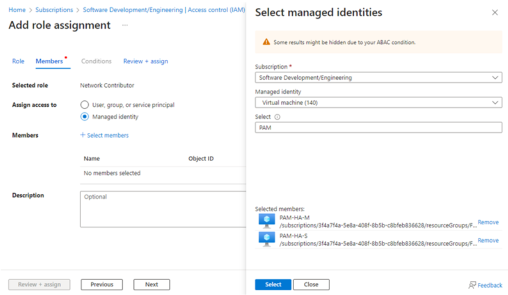
Selected members:

PAM-HA-SDN
Application

ii. Click *Select*.

vi. In *Assign access to*, for *Managed identity*:

i. In *Members*, select +*Select members*, from *Select managed identities*, select the primary and the secondary FortiPAM units.



Home > Subscriptions > Software Development/Engineering | Access control (IAM)

Add role assignment ...

Selected role: Network Contributor

Assign access to: ○ User, group, or service principal ● Managed identity

Members: + Select members

Name	Object ID
No members selected	

Description: Optional

Select managed identities

Some results might be hidden due to your ABAC condition.

Subscription *: Software Development/Engineering

Managed identity: Virtual machine (140)

Select: PAM

Selected members:

PAM-HA-M /subscriptions/3f4a7f4a-5e8a-408f-8b5b-c8bfeb836628/resourceGroups/F... Remove

PAM-HA-S /subscriptions/3f4a7f4a-5e8a-408f-8b5b-c8bfeb836628/resourceGroups/F... Remove

ii. Click *Select*.

vii. Click *Review+assign*.

Configuring SDN connector on FortiPAM

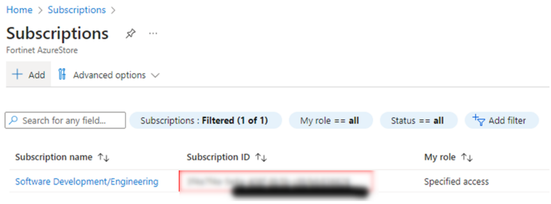
To configure an SDN connector on FortiPAM:

1. On the primary FortiPAM, enter the following commands:

```
config system sdn-connector
 edit "azure-ha"
  set type azure
  set use-metadata-iam disable
  set ha-status enable
  set tenant-id ""
  set client-secret ""
  set subscription-id ""
  set resource-group "FortiPAM"
  config nic
   edit "pam-ha-m158_z1"
    config ip
     edit "ipconfig1"
      set public-ip "FPAM-HA-GUI-Portal"
     next
    end
   next
  end
 next
end
```

Notes:

- `tenant-id` and `client-id` can be found from the PAM-HA-SDN application created in Adding Azure application registration on page 564.
- `client-secret` is the secret value created in Creating a client secret.
- `subscription-id` is in *Subscriptions* in the Azure portal.



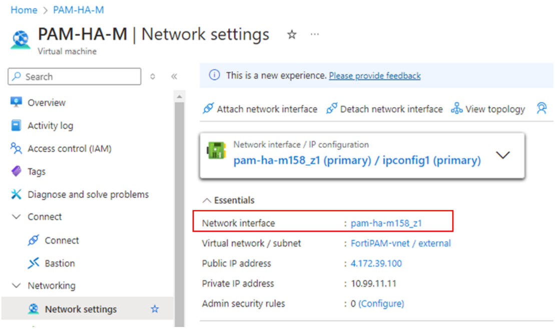
Home > Subscriptions >

Subscriptions

Fortinet AzureStore

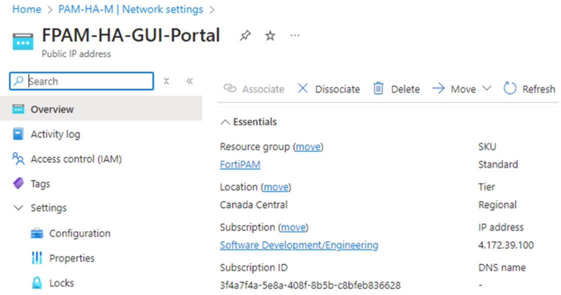
Subscription name ↑↓	Subscription ID ↑↓	My role ↑↓
Software Development/Engineering	[redacted]	Specified access

- In `config nic`, add the network interface used to access the GUI portal and the public IP address name.



Network interface / IP configuration
pam-ha-m158_z1 (primary) / ipconfig1 (primary)

Network interface : pam-ha-m158_z1
Virtual network / subnet : FortiPAM-vnet / external
Public IP address : 4.172.39.100
Private IP address : 10.99.11.11
Admin security rules : 0 (Configure)



Resource group (move)
FortiPAM
Location (move)
Canada Central
Subscription (move)
Software Development/Engineering
Subscription ID
3f4a7f4a-5e8a-408f-8b5b-c8bfeb836628

SKU
Standard
Tier
Regional
IP address
4.172.39.100
DNS name
-

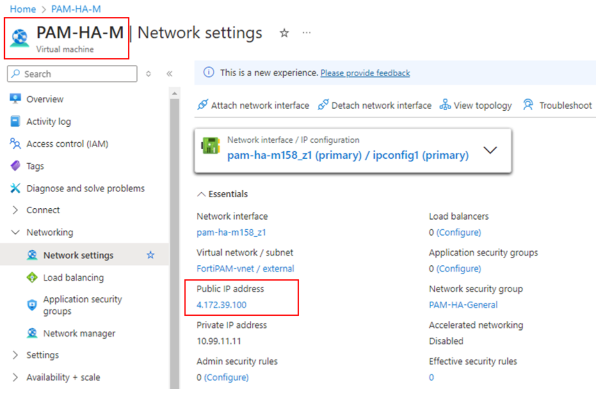
2. On the secondary FortiPAM, enter the following commands to configure the SDN connector on the HA secondary node. The settings are similar to those on the primary node. The only difference is in `config nic`. You must change the interface name to that of the secondary node.

```
config system sdn-connector
 edit "azure-ha"
  set type azure
  set use-metadata-iam disable
  set ha-status enable
  set tenant-id ""
  set client-id ""
  set client-secret ENC MJgnqCoyzYiCKoN21Ig8GNWChnAKWYDMpZ5g7gq0OGaHyUr
  set subscription-id ""
  set resource-group "FortiPAM"
  config nic
   edit "pam-ha-s194_z1"
    config ip
     edit "ipconfig1"
      set public-ip "FPAM-HA-GUI-Portal"
     next
    end
   next
  end
 next
end
```

Accessing the GUI portal after the HA failover

To access the GUI portal after the HA failover:

1. Before HA failover, ensure that the public IP address is associated to the primary FortiPAM node.

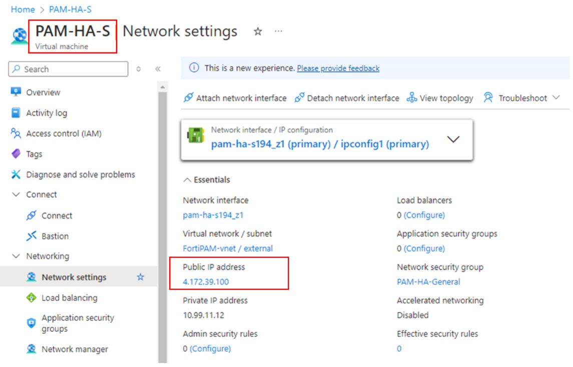


Network interface / IP configuration: pam-ha-m158_z1 (primary) / ipconfig1 (primary)

Essentials

Network interface pam-ha-m158_z1	Load balancers 0 (Configure)
Virtual network / subnet FortiPAM-vnet / external	Application security groups 0 (Configure)
Public IP address 4.172.39.100	Network security group PAM-HA-General
Private IP address 10.99.11.11	Accelerated networking Disabled
Admin security rules 0 (Configure)	Effective security rules 0

2. When the primary node is shut, the public IP address is associated with the secondary node. The FortiPAM service is available on the same IP address.



Network interface / IP configuration: pam-ha-s194_z1 (primary) / ipconfig1 (primary)

Essentials

Network interface pam-ha-s194_z1	Load balancers 0 (Configure)
Virtual network / subnet FortiPAM-vnet / external	Application security groups 0 (Configure)
Public IP address 4.172.39.100	Network security group PAM-HA-General
Private IP address 10.99.11.12	Accelerated networking Disabled
Admin security rules 0 (Configure)	Effective security rules 0

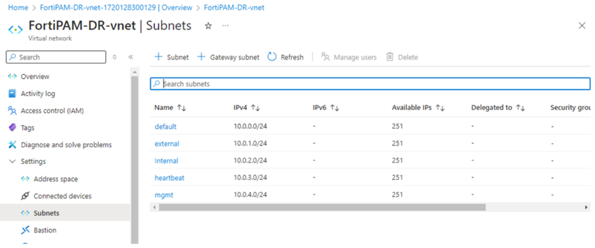
Adding a DR node

The disaster recovery node is usually in a different region. Here, the HA primary and secondary nodes are located in Central Canada, and the DR node is in Western US.

Prerequisites

- Virtual network with four subnets

  Similar to *FortiPAM-vnet* virtual network for the primary and the secondary FortiPAM nodes, create another *FortiPAM-DR-vnet* virtual network with four subnets for the DR node- *external*, *internal*, *heartbeat*, and *mgmt*.



Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs ↑↓	Delegated to ↑↓	Security grou
default	10.0.0.0/24	-	251	-	-
external	10.0.1.0/24	-	251	-	-
Internal	10.0.2.0/24	-	251	-	-
heartbeat	10.0.3.0/24	-	251	-	-
mgmt	10.0.4.0/24	-	251	-	-

- Three public IP addresses for DR:
  - One for the GUI portal

    If both the primary and secondary fail, the DR node takes over. The public IP address *FPAM-HA-GUI-Portal* used for the GUI cannot switch to associate with the DR external interface. Therefore, the DR external interface should associate with its own public IP address *FPAM-DR-GUI-Portal*. The DR GUI portal does not respond to any request unless it becomes the primary node.
  - One for the HA heartbeat interface

    The hearbeat interface on the primary, secondary, and the DR nodes must be able to reach each other.

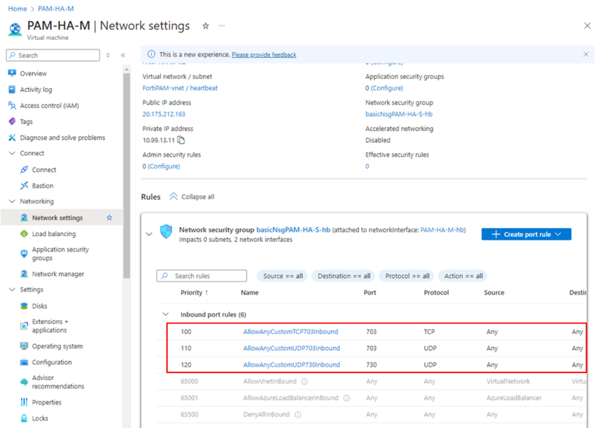
    The example uses public IP addresses.
  - One for the management interface
- Two public IP addresses for the HA primary and the secondary heartbeat interface.

  The IP assignment for the HA nodes is shown below.

	port1(external)	port2(internal)	port3(heartbeat)	port4(mgmt)
Primary (Canada Central)	10.99.11.11/24 Public IP address: 4.172.39.100	10.99.12.11/24	10.99.13.11/24 Public IP address: 20.175.212.163	10.99.14.11/24 Public IP address: 4.172.37.209
Secondary (Canada Central)	10.99.11.12/24	10.99.12.12/24	10.99.13.12/24 Public IP address: 20.175.211.121	10.99.14.12/24 Public IP address: 4.172.38.127
DR (US West 3)	10.0.1.13/24 Public IP address: 4.227.50.87	10.0.2.13/24	10.0.3.13/24 Public IP address: 4.227.49.239	10.0.4.13/24 Public IP address: 4.236.21.150

To add a DR node:

1. Create a FortiPAM VM on Azure.
   See Appendix G: Installation on Azure on page 476.
2. Ensure that the following are correctly configured:
   a. The FortiPAM DR node must have the same VM and disk size as the primary/secondary nodes.
   b. Add four network interfaces to the FortiPAM DR node. One interface for the one subnet in the same order as the other two HA nodes.
   c. Attach public IP addresses to the *external*, *heartbeat*, and the *mgmt* interface.
   d. The FortiPAM DR node must have its own valid license.
3. Adding inbound rule for HA hearbeat:
   The following ports are used for HA sync and hearbeat. Create inbound rules on the heartbeat interfaces of all HA nodes to allow related traffic.
   a. **TCP**: `port703`
   b. **UDP**: `port703`
   c. **UDP**: `port730`
   The following are the inbound port rules for the network security group used by the heartbeat interface of the primary HA node:



Virtual network / subnet: FortiPAM-vnet / heartbeat

Application security groups: 0 (Configure)

Public IP address: 20.175.212.163

Network security group: basicNsgPAM-HA-S-hb

Private IP address: 10.99.13.11

Accelerated networking: Disabled

Admin security rules: 0 (Configure)

Effective security rules: 0

Network security group basicNsgPAM-HA-S-hb (attached to networkInterface: PAM-HA-M-hb)
Impacts 0 subnets, 2 network interfaces

Priority ↑	Name	Port	Protocol	Source	Desti
Inbound port rules (6)					
100	AllowAnyCustomTCP703Inbound	703	TCP	Any	Any
110	AllowAnyCustomUDP703Inbound	703	UDP	Any	Any
120	AllowAnyCustomUDP730Inbound	730	UDP	Any	Any
65000	AllowVnetInBound	Any	Any	VirtualNetwork	Virtu
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any
65500	DenyAllInBound	Any	Any	Any	Any

4. Adding DR settings to both the primary and the secondary FortiPAM node.
   Enter the following CLI commands n the HA primary and secondary node
   a. On the primary node, add `router.static` to `vdom-exception` so that DR has its own routing table.

```
config system vdom-exception
 edit 1
  set object system.interface
 next
 edit 2
  set object firewall.vip
 next
 edit 3
  set object router.static
 next
end
```

   b. On the primary and the secondary nodes, add the DR heartbeat public IP address to the HA configuration.
      Primary

```
config system ha
 set group-name "Azure_PAM_HA"
 set mode active-passive
 set password M0NNJmJSOx1zQiFkNIZGP4
 set hbdev "port3" 0
 set ha-mgmt-status enable
 config ha-mgmt-interfaces
  edit 1
   set interface "port4"
   set gateway 10.99.14.1
  next
 end
 set override enable
 set priority 200
 set unicast-status enable
 set unicast-gateway 10.99.13.1
 config unicast-peers
  edit 1
   set peer-ip 10.99.13.12
  next
  edit 2
   set peer-ip 4.227.49.239 #DR heartbeat public IP address
  next
 end
end
```

Secondary

```
config system ha
 set group-name "Azure_PAM_HA"
 set mode active-passive
 set password ENC PVZn2zzYwbS0QA/cn1M25x8nbw5
 set hbdev "port3" 0
 set ha-mgmt-status enable
 config ha-mgmt-interface
  edit 1
   set interface "port4"
   set gateway 10.99.14.1
  next
 end
 set override enable
 set unicast-status enable
 set unicast-gateway 10.99.13.1
 config unicast-peers
  edit 1
   set peer-ip 10.99.13.11
  next
  edit 2
   set peer-ip 4.227.49.239 #DR heartbeat public IP address
  next
 end
end
```

c. On the primary and the secondary nodes, add a static route to the DR hearbeat public IP through their own heartbeat interface.

Primary

```
config router static
 edit 1
  set gateway 10.99.11.1
  set device "port1"
 next
 edit 2
  set dst 4.227.49.239 255.255.255.255.255
  set gateway 10.99.13.1
  set distance 5
  set device "port3"
  set comment "HA DR heartbeat interface"
 next
end
```

Secondary

```
config router static
 edit 1
  set gateway 10.99.11.1
  set device "port1"
 next
 edit 2
  set dst 4.227.49.239 255.255.255.255
  set gateway 10.99.13.1
  set distance 5
  set device "port3"
 next
end
```

5. Enabling HA on DR.
   a. We configure a static route to the primary and the secondary heartbeat interfaces using the public IP address.

```
config router static
 edit 1 #External interface private IP gateway
  set gateway 10.0.1.1
  set device "port1"
 next
 edit 2 #Secondary node heartbeat interface public IP address
  set dst 20.175.211.121 255.255.255.255.255
  set gateway 10.0.3.1 #Heartbeat interface gateway
  set distance 5
  set device "port3"
  set comment "To HA secondary heartbeat interface"
 next
 edit 3 #primary node heartbeat interface public IP address
  set dst 20.175.212.163 255.255.255.255
  set gateway 10.0.3.1
  set distance 5
  set device "port3"
  set comment "To HA primary hearbeat interface"
 next
end
```

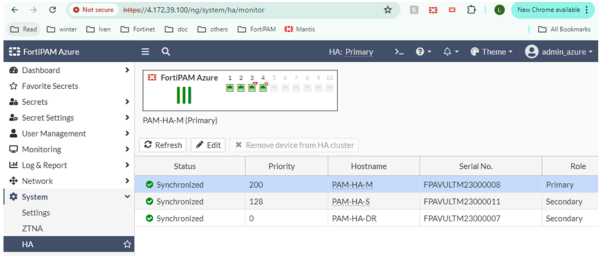
   b. Enabling HA.
      i. Go to *System* > *HA*.
      ii. Configure the same *Group name* and *Password* as on the primary node.
      iii. In *Heartbeat interfaces*, select +, from *Select Entries*, select `port3`, and click *Close*.
      iv. In *Management Interface Reservation*, in *Interface*, select `port4`.
      v. In *Gateway*, enter the remote gateway IPv4 address.
      vi. Enable *Unicast Status*.
      vii. Enter the gateway IPv4 address.
      viii. In *Peer IP*, select +, enter the IP address of the HA heartbeat interface of the other FortiPAM-VM in the HA cluster.
      The following shows the HA configuration:

```
config system ha
 set group-name "Azure_PAM_HA"
 set mode active-passive
 set password ENC
 set hbdev "PORT3" 0
 set ha-mgmt-interfaces
 config ha-mgmt-interfaces
  edit 1
   set interface "port4"
   set gateway 10.0.4.1
  next
 end
 set override enable
 set priority 0
 set unicast-status enable
 set unicast-gateway 10.0.3.1
 config unicast-peers
  edit 1
   set peer-ip 20.175.212.163
  next
  edit 2
   set peer-ip 20.175.211.121
  next
 end
end
```

ix. Click *OK*.

Verification

1. Access the GUI using the public IP address of port1 (`FPAM-HA-GUI-Portal`: `4.172.39.100`) and verify that all the HA nodes are in sync by going to *System* > *HA*.
   Note: Syncing the HA cluster nodes can take up to 30 minutes.



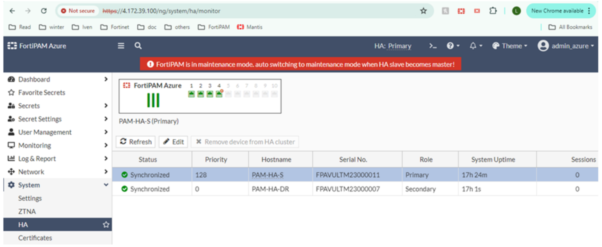
https://4.172.39.100/ng/system/ha/monitor

FortiPAM Azure — HA: Primary

PAM-HA-M (Primary)

Status	Priority	Hostname	Serial No.	Role
✓ Synchronized	200	PAM-HA-M	FPAVULTM23000008	Primary
✓ Synchronized	128	PAM-HA-S	FPAVULTM23000011	Secondary
✓ Synchronized	0	PAM-HA-DR	FPAVULTM23000007	Secondary

2. Shutdown the primary node.
   The secondary node becomes the active node.
3. Access the GUI portal using the same public IP address (`FPAM-HA-GUI-Portal`: `4.172.39.100`) and verify that the original secondary node and the DR node are in sync.



https://4.172.39.100/ng/system/ha/monitor

FortiPAM Azure — HA: Primary

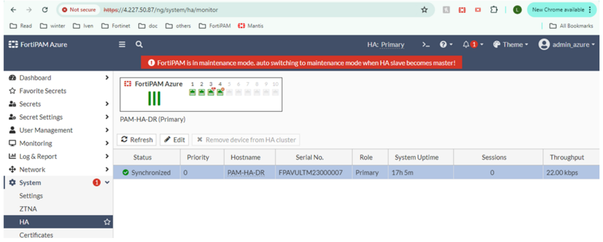
FortiPAM is in maintenance mode. auto switching to maintenance mode when HA slave becomes master!

PAM-HA-S (Primary)

Status	Priority	Hostname	Serial No.	Role	System Uptime	Sessions
✓ Synchronized	128	PAM-HA-S	FPAVULTM23000011	Primary	17h 24m	0
✓ Synchronized	0	PAM-HA-DR	FPAVULTM23000007	Secondary	17h 1s	0

4. Shutdown the secondary node.
   The DR node becomes the active node.

5. Access the GUI portal using the DR node public IP address (`FPAM-DR-GUI-Portal: 4.227.50.87`).



FortiPAM is in maintenance mode. auto switching to maintenance mode when HA slave becomes master!

PAM-HA-DR (Primary)

Status	Priority	Hostname	Serial No.	Role	System Uptime	Sessions	Throughput
Synchronized	0	PAM-HA-DR	FPAVULTM23000007	Primary	17h 5m	0	22.00 kbps

6. Power on the primary and the secondary nodes.
7. Verify that the FortiPAM service is available again by accessing the GUI portal of the primary node (`PAM-HA-GUI-Portal: 4.172.39.100`).
   All the three nodes in the HA cluster are now in sync.

www.fortinet.com

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. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. 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.