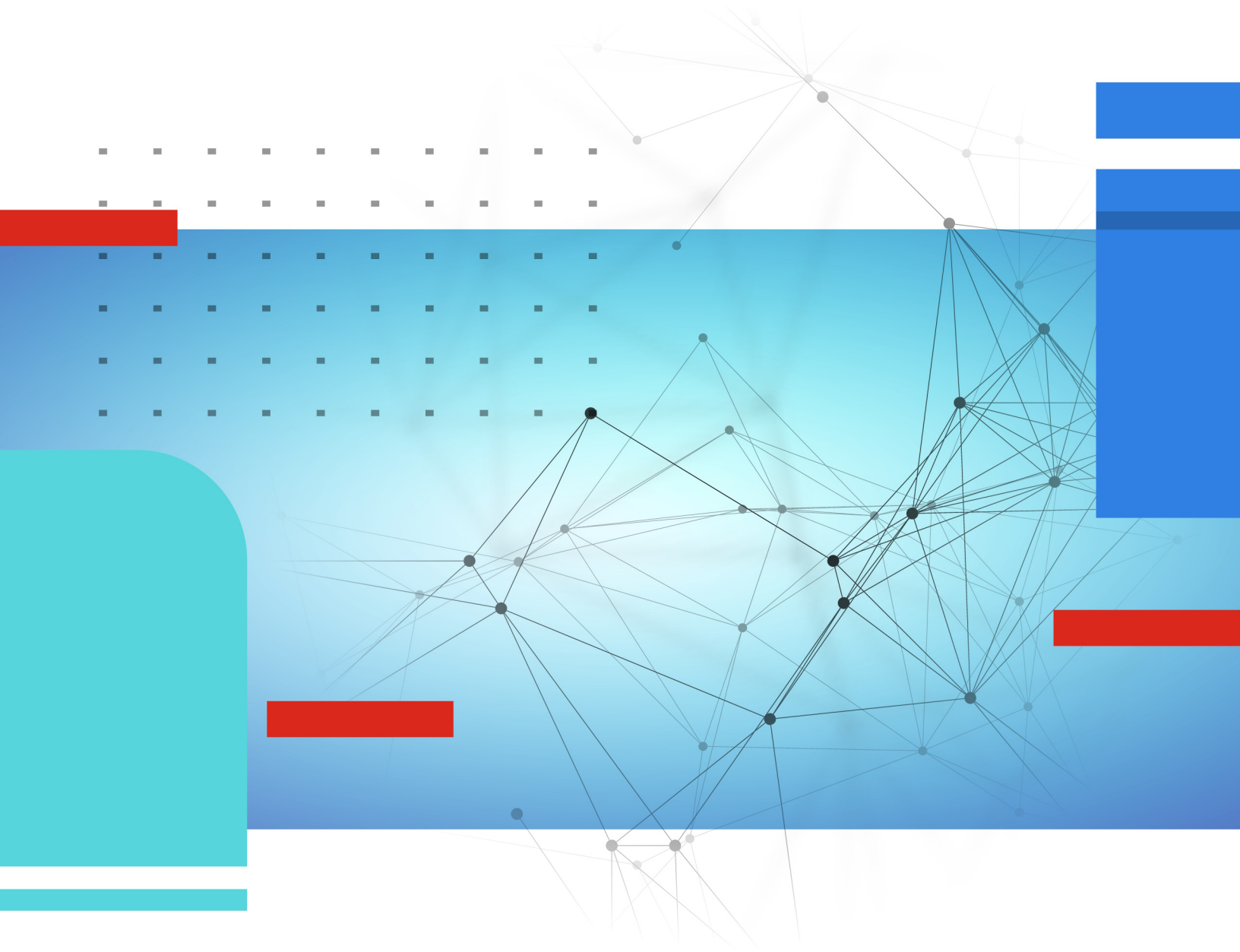
Administration Guide

FortiPAM 1.5.1



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

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

FORTINET BLOG
https://blog.fortinet.com

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

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

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

FORTIGUARD LABS
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com



November 18, 2025
FortiPAM 1.5.1 Administration Guide
74-151-1084296-20251118

TABLE OF CONTENTS

Change Log **10**
What's new in FortiPAM **11**
FortiPAM 1.5.1 11
FortiPAM 1.5.0 11
Secret/Launch 11
User/Group 16
System/Log 17
Others 18
Introduction **20**
FortiPAM concepts 21
Organization of the guide 21
Using the GUI 22
Banner 22
GUI based global search 23
CLI commands 24
Admin 24
Tables 29
Modes of operation 34
FortiPAM deployment options 35
Feature availability 38
Agentless mode 39
FortiPAM installation **42**
Installing FortiClient with the FortiPAM feature 43
FortiPAM appliance setup 43
FortiPAM with TPM 46
Connecting to target remote systems 48
Licensing **49**
License expiry and renewal 51
Renewing FortiPAM-VM license 54
Dashboard **56**
Adding a custom dashboard 59
System information widget 59
Licenses widget 61
FortiGuard Distribution Network 61
VM license 65
Secrets **67**
Secrets 68
Creating a secret 71
Launching a secret 99
Check out and check in a secret 101
Uploading secrets using the secret upload template 101
Change password 103

Verify password 106
Example secret configurations example 107
Configuring a web FortiProduct secret Example 110
Configuring an ESXi web secret Example 112
Configuring and accessing a secret that uses an approval profile with custom fields Example 113
Targets 116
Creating a target 117
Personal/public folder 127
Creating a folder 131
My requests list 136
Make a request 137
Approval list 140
Approving a request 141
Reviewing multiple requests 143
Job list 144
Creating a job 144
Discovery 147
Creating discovery entry 148
Secret settings 153
Templates 153
Creating secret templates 157
Launchers 167
Creating a launcher 172
Launch session monitor 178
Policies 179
Creating a policy 180
Classification tags 185
Creating a classification tag 186
Addresses 186
Creating an address 187
Creating an address group 188
Dependency updater 189
Service accounts 189
Updating service accounts 190
Creating a dependency updater 190
Updating a service account credential Example 192
Approval flow 194
Approval profile 194
Approval email template 198
Creating an approval email template 200
Creating an approval email template using the CLI 204
Approving secrets by Email 204
Password changers 211
Creating a password changer 213
Password policies 225
Creating a password policy 226

Character sets 228
Creating a character set 228
AntiVirus 229
Creating an antivirus profile 230
Data loss prevention (DLP) protection for secrets 232
Supported file types 237
DLP file pattern 239
SSH filter profiles 241
Creating an SSH filter 241
Event filter profile 247
Creating an event filter profile 248
Window app filter 250
Key features 250
Benefits of using Windows App Filter 250
Limitations 251
Creating a Windows app filter profile 252
Integrity check 254
Creating a client software entry for integrity check 255
User management 258
User list 258
Creating a user 263
Importing LDAP users 277
User groups 280
Auto provision rules 285
Sponsored groups 286
Role 289
Access control options 297
Log permissions 300
LDAP servers 301
SAML Single Sign-On (SSO) 304
Auto provision rules 308
RADIUS servers 312
Schedule 314
FortiTokens 316
Monitoring 319
User monitor 319
Active sessions 319
Over-the-shoulder monitoring (Live recording) 321
Log & report 323
Secret event & video 323
System event 328
Security event 330
ZTNA traffic 333
Disk usage 334
Automation 336

Stitch 336
Trigger 343
Action 345
Reports 346
General 346
Secret audit 353
Log settings 354
Configuring log and video disk encryption 357
Email alert settings 361
Email alert when the glass breaking mode is activated example 363
Debug settings 363
Automation trigger settings 366
Network 367
Interfaces 367
Editing an interface 368
Static routes 371
Creating an IPv4 static route 372
DNS settings 374
Security fabric 376
Fabric Connectors 376
Packet capture 381
Creating a packet capture filter 381
FortiPAM server 383
Secret gateway 384
Introduction 384
Creating a gateway on the FortiPAM GUI 387
Reverse service 391
Configuring traffic proxy on gateway CLI 392
System 397
Settings 397
Testing the email service connection example 405
How FortiPAM chooses the sender email address 406
ZTNA tags 407
Creating a ZTNA tag group 407
ZTNA user control 408
ZTNA tag control example 410
ZTNA-based FortiPAM access control 411
High availability 414
HA active-passive cluster setup 418
Upgrading FortiPAM devices in an HA cluster 420
Disaster recovery 421
Certificates 423
Creating a certificate 425
Generating a CSR (Certificate Signing Request) 428
Importing CA certificate 430
Uploading a remote certificate 431
Importing a CRL (Certificate revocation list) 431

Replacement messages 433
Replacement messages descriptions 435
Editing a replacement message 436
Managing images 438
SNMP 441
Fortinet MIBs 443
SNMP agent 444
Creating or editing an SNMP community 445
Creating or editing an SNMP user 447
Configuration backup 448
Sending backup file to a server Example 453
Backing up/restoring log and video files using FTP CLI 454
Remote video storage 457
Firmware 460
FortiPAM license 460
Stackable seat license for hardware models 461
FortiGuard license 462
Setup wizard 462
Concurrent user sessions 466
Disclaimers via the CLI 467
Troubleshooting 469
Troubleshoot using trace files 470
Example troubleshooting example 470
FortiPAM HTTP filter 471
Issue: WebRDP session recording fails and closes active session 473
Troubleshooting log and video disk encryption issues 474
Issue 1: 474
Issue 2: 474
Issue 3: 476
Issue 4: 476
FortiClient troubleshooting tips 477
Issue 1: Error contacting FortiClient 477
Issue 2: Error starting the program 478
Issue 3: FortiPAM JSON error 478
Issue 4: HTTP port mismatch between FortiPAM and FortiClient 478
Issue 5: Secret not reaching the host 478
Troubleshooting Windows application filter 479
Issue: Some configurations are removed after last reboot 479
Troubleshooting a secret that uses Windows Machine template with the default SAMBA password changer 482
Verifying password 482
Change password 484
Abnormal traffic detection and resolution 487
Hardening 489
Secure password storage 489
Verify the private-data-encryption feature Example 490

How to restore a backup configuration file with private-data-encryption enabled Example ... 490
Enabling private-data-encryption on an HA cluster Example ... 491
Appendix A: Installation on KVM ... 493
Appendix B: Installation on VMware ... 496
Appendix C: Installing vTPM package on KVM and adding vTPM to FortiPAM-VM ... 501
Appendix D: vTPM for FortiPAM on VMware ... 503
Appendix E: Enabling soft RAID on KVM or VMware ... 504
Appendix F: Installation on Hyper-V ... 506
Appendix G: Installation on Azure ... 518
Appendix H: FortiPAM hardware RAID CLI commands ... 524
Appendix I: Default launchers parameters ... 527
Appendix J: Installation on AWS ... 534
FortiPAM installation on AWS and initial setup: ... 534
Appendix K: Installation on GCP ... 547
FortiPAM installation on GCP and initial setup: ... 547
Appendix L: WinRM configuration for Windows server ... 561
Appendix M: FortiPAM browser extension and standalone FortiClient air-gapped installation ... 569
Appendix N: Performance test results ... 572
FortiPAM-VM minimum requirements based on different user seats ... 572
FortiPAM-VM performance as tested in the lab ... 572
Appendix O: How to find a selector Example ... 574
Example 1 ... 574
Finding selector for the Username field on the FortiPAM login page using the Google Chrome web browser ... 574
Example 2 ... 576
Finding selector for the Account ID field on AWS IAM user login page using the Microsoft Edge web browser ... 576
Appendix P: How to input the authentication path Example ... 578
Example 1 ... 578
Example 2 ... 578
Appendix Q: FortiPAM HA on AWS ... 579
How to configure FortiPAM HA on the AWS platform ... 580
Prerequisites ... 581

Appendix R: FortiPAM HA on Azure **598**
Appendix S: Installation on Alibaba Cloud **618**
Appendix T: FortiPAM HA on Alibaba Cloud **643**
Appendix U: FortiPAM HA on VMware **666**
Appendix V: Terraform- FortiPAM as a provider **671**
Appendix W: Installation on Proxmox **675**
Purpose 675
Scope 675
Prerequisites 675
Creating the FortiPAM-VM on Proxmox 675
Disk image transfer 678
Network configuration 679
Accessing the FortiPAM-VM 680
Appendix X: Deploying FortiPAM-VM HA on AWS between multiple zones **681**
How to configure FortiPAM HA on the AWS platform 681
Prerequisites 682
Installing and configuring FortiPAM instances on AWS 691

Change Log

Date	Change Description
2025-05-29	Initial release.
2025-08-07	Updated Secret gateway on page 384.
2025-11-18	Updated Appendix Q: FortiPAM HA on AWS on page 579 and Appendix X: Deploying FortiPAM-VM HA on AWS between multiple zones on page 681.

What's new in FortiPAM

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

- FortiPAM 1.5.1 on page 11
- FortiPAM 1.5.0 on page 11

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

FortiPAM 1.5.1

FortiPAM 1.5.1 is a patch release only. There are no new features and enhancements in this release. For more information, see the *FortiPAM 1.5.1 Release Notes* on *Fortinet Docs Library*.

FortiPAM 1.5.0

The following list contains new and expanded features added in FortiPAM 1.5.0.

Secret/Launch

1050160- Service gateway

Starting FortiPAM 1.5.0, the reverse gateway supports Service mode.

The reverse gateway operates under 2 modes:

- *Reverse mode*: The gateway working in the reverse mode is called the Reverse Gateway.
- *Service mode* (new): The gateway working in the service mode is called the Service Gateway.

When FortiPAM acts as the reverse gateway with the Service ability, it supports the client directly to start launching sessions from the client device itself rather than starting the session from the original FortiPAM and then proxying it to the reverse gateway.

In the Reverse mode, the launching session traffic flow is *Client machine* > *Central Server* > *Gateway* > *Target Server*.

In the Service mode, the launching session traffic is *Client machine* > *Gateway* > *Target Server*. This reduces the session delay and the central server stress when the gateway device is closer to the target server when the gateway device is closer to the target server. Here, videos are still uploaded to FortiPAM and the secret log is reported to FortiPAM instead of storing it on the gateway device.

See Creating a gateway on the FortiPAM GUI on page 387 and FortiPAM server on page 383.

1097062- New Agentless mode for web based secret launch

Starting FortiPAM 1.5.0, a new *Agentless* mode has been introduced for launching web based secrets without requiring the assistance of either FortiClient or the *Fortinet Privileged Access Agent* browser extension to be installed locally.

Supported web based launchers include the following:

- *Web SSH*
- *Web RDP*
- *Web VNC*
- *Web SFTP*
- *Web SMB*
- *Web Telnet*

Supported web browsers include the following:

- Google Chrome
- Microsoft Edge

The feature reduces dependency on environment resources and maintenance costs. Additionally, it enhances FortiPAM security, portability, and the overall efficiency.

Currently, the *Agentless* mode has the following 3 limitations:

- The feature does not work with the Mozilla Firefox browser.
- The feature does not work with the *Web Account* launcher.
- The feature does not work with a service gateway.

A new *Agentless* dropdown in the banner lists 3 modes for you to select from:

- *Automatic*
- *Extension*
- *Agentless*

See Banner on page 22 and Agentless mode on page 39.

1014580- Secret Event Subscription

Secret event subscription allows any user to receive email notifications when certain events happen on a specific secret.

The subscribable events are: secret entry change, password change failed, view password clear text, password verify failed, secret check-in, secret check-out, secret launch, and secret certificate expiry notification.

After subscribing to the event, once an event is triggered, an email is sent to the user email configured in the user profile.

See Subscribing to Secret related events on page 91.

875335, 1063325- New default secret templates and a default password changer

FortiPAM now includes the following four default secret templates:

- *Azure Credential*: A basic template designed to save Azure AD enterprise application (client) ID, Directory (tenant) ID, and client secret value information.
- *Azure AD Account*: A basic template designed to launch Azure AD portal as target.

- *VNC Server*: A basic template designed for VNC password authentication.
- *macOS*: A basic template for a macOS machine.

FortiPAM now includes the following new password changer:

- *Web API (Azure AD)*: A default password changer designed to change Azure AD password.

See Templates on page 153, Password changers on page 211.

1079201- New default launcher available

FortiPAM now includes a new default *RealVNC Viewer* secret launcher.

The secret launcher is designed to connect to a RealVNC server.

A RealVNC server supports the following two authentication methods:

- Standard VNC password with 8 digits/characters
- Windows username/password

See Launchers on page 167.

1033306- Support multiple OS launcher

FortiPAM now supports launchers on various OS types including Windows, macOS, or custom.

A new *OS Settings* pane when creating or editing a launcher.

For OS types including the macOS, the new FortiClient is needed to support native launchers.

After FortiClient running on a different OS(macOS) can support FortiPAM, FortiPAM can configure a different OS launcher to launch secrets.

Two new default launchers are introduced:

- *Remote Desktop* instead of previous *Remote Desktop-Windows* to support both Windows and macOS
- *Screen Sharing* for macOS

When you create a new launcher, you can define how to initiate the launcher in a different OS.

Note: Before you add a new OS for a launcher, ensure that your FortiClient supports FortiPAM in the OS.

When you add a new OS to a launcher, ensure that the FortiClient in the OS supports FortiPAM, e.g., for FortiClient 7.4.1, only Windows FortiClient supports FortiPAM.

See Creating a launcher on page 172 and Launchers on page 167.

1053876- Customize secret launcher start up timeout

A new *Timeout Duration* field when creating or editing a secret launcher.

The new *Timeout Duration* field allows you to set up a maximum duration to start a secret launcher before the timeout, in seconds.

This new feature needs FortiClient future support.

See Creating a launcher on page 172.

1058979- Support certificate authentication for the secret SSH launch

The SSH protocol offers multiple authentication options: passwords, public keys and certificates. Certificate-based authentication is the most secure of them all as it controls the certificate expiry date and the login username.

Starting 1.5.0, FortiPAM supports certificate authentication.

When you create a secret with the *SSH Key* template, you can choose *Public key with certificate* to use this feature.

A new *Public-key* dropdown in the *Fields* pane when creating or editing a secret that uses *FortiProduct (SSH Key)* or *Unix Account (SSH Key)* as the secret template.

The new *Public-key* dropdown allows you to select the type of public key to use.

The certificate based SSH authentication improves authentication security by controlling the certificate expiry date.

You can choose from the following two public key types:

- *Standard public key*
- *Public key with certificate*: Select to allow certificate based authentication.

See Creating a secret on page 71.

1056945- Secret approval via email

An approver can now approve the secret approval request by responding to the secret approval request email directly without the need to log in to FortiPAM.

When the reviewers click the *Approve* or *Deny* button in the email, a pre-set email template will be used for the reviewer to send their responses. FortiPAM will act as an email client to fetch the response emails periodically if approval email server settings are configured properly.

Use of this feature requires configuration of an approval email server in *System* > *Settings*.

See Approving secrets by Email on page 204

1078249- Secret GUI improvements

When creating a secret, in the *General* tab, the following two new tabs have been added. One of these tabs must be selected as part of the secret creation process:

- *To connect to a remote server*: Used to create a secret to connect to a remote server.
- *To store a certificate/file*: Used to create a secret for storing a certificate or a file.

The remaining secret settings presented in the GUI will change depending on the selection.

See Creating a secret on page 71.

1101756- Health checks are supported for Forward type Gateways

Health checks are now supported Forward type Gateways to assist in monitoring the gateway connectivity status.

The status shows on the right pane of the gateway page, the target page, and the secret page where the gateway is used.

See Creating a gateway on the FortiPAM GUI on page 387.

1044292- SQL server session log enhancement

New RPC parameter added to the SQL server session log.

See Launchers on page 167.

1098271- Web API password changer enhancements

When creating a password changer:

- A new *Web-API* type is available.
- *Web Changers* and *Web Verifiers* pane available where you can enter a series of `http` requests to execute `http` requests expect based on the previous `http execute` command.
- The *Change Auth Mode* option has been renamed to *Change Password Using*.
- The *Verify Auth Mode* option has been renamed to *Verify Password Using*.
- The *Association* option in *Change Password Using* and *Verify Password Using* has been renamed to *Associated Secret*.
- When creating a new web command in the *Web Changers* or *Web Verifiers* pane:
  - *Type*: *Execute*.

    A request is sent to the server using the configured URL, headers, and query parameters. This initiates actions such as authentication or password change commands.
  - *Type*: *Expect*.

    Verifies that the server response meets predefined criteria, such as, containing specific strings in the response body or matching expected status codes. If these criteria are not met, the password change process terminates. This step also allows for cookie and token extraction to support subsequent requests.

  For the Web API password changer:
  - In *Execute*:
    - Multi-header input is supported. Previously, only single header input was supported.
    - *Body Encoding*: FortiPAM decodes the input body fields using *XML/JSON/None* when selecting *HTTP POST/PUT/PATCH* methods.
  - In *Expect*:
    - Supports exact-match and regular expression.
    - New *Execute Next Command* setting with the following options:
      - *In Sequence*: Linear execution (legacy mode).
      - *Jump*: Depending on the current result or the step, jump to any step at will by importing the command number in the password changer process.
    - *Expect String In Body* has been renamed to *Response Body Match* and *Completion* has been renamed to *End Web Changing Process*.

  See Creating a password changer on page 213.

1063215- HTTP PATCH method for the Web API password changer

FortiPAM supports HTTP patch requests to the Web API password changer.

See Creating a password changer on page 213.

User/Group

957802- Force checkout

If a secret has been checked out by a user and the secret is not launched, the secret can be forced checked out by another user.

A new *Force Checkout Idle time* field is available when *Requires Checkout* is enabled for a secret.

Note that the *Force Checkout Idle time* field can only be set up when both *Proxy Mode* and *Session Recording* are already enabled.

See Creating a secret on page 71.

Force checkout works for all the users that can access a secret.

A user can force checkout a secret when the current user who has checked out the secret does not have an active launch session for at least the time set in the *Force Checkout Idle time* field.

See Launching a secret on page 99.

1054962- Show user logs in the user details page

When editing a user, new *Config & Login Logs* and *Secret Access Logs* tabs available.

The *Config & Login Logs* and *Secret Access Logs* tabs show related user log information.

See User list on page 258.

1061622- Third-party authenticators are supported for user login

You can now select *Third-party authenticator* as the method of two-factor authentication when creating or editing a user in FortiPAM.

Common third-party authenticators including Google Authenticator, Microsoft Authenticator, SafeAuth Authenticator, and others which use a standard SHA to calculate the token are supported.

When configuring a user with *Two-Factor Authentication* enabled, you can select *Third-Party Authenticator* in the method dropdown. A random shared seed is generated for each user who uses this method. Administrators can send this shared-key by QR code in email. Users must scan the QR code using their own authenticator (e.g. Google, Microsoft, etc.) to generate the one-time-password for login.

Options to view, renew and resend the QR code can be accessed when editing the user in the FortiPAM GUI.

See Creating a user on page 263.

1095266 - User profile menu added to the banner

A new *User Profile* option has been added to the Admin menu in the FortiPAM banner. The *User Profile* menu displays information about the user's username, last login time, last login IP, last failed login, and email address. Users can use the *User Profile* menu to edit the email address that is associated with their profile.

See Admin on page 24.

1097981- Viewing a user's related secrets and secret logs

Administrators can view a list of all of the secrets that a user can access, including the secret name, folder name, target, account, and permissions in a new *Secret List* tab when editing a user. With additional permissions enabled, the administrator can also view/edit secret details, and view secret logs.

See User list on page 258.

System/Log

1097958- FortiPAM Multiple language support

Beginning in FortiPAM 1.5.0, the FortiPAM GUI supports multiple languages, including:

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

Administrators can configure the language setting for new or existing users when creating or editing a user. See Creating a user on page 263.

Users can change their own language preferences at any time using the language dropdown in the banner. See Banner on page 22.

913200- Send videos to external storage through SFTP

FortiPAM 1.5.0 includes a new option to send videos to external storage.

When remote video storage is enabled, video files for recorded sessions will be moved to the configured remote server once a storage threshold is met, helping you to avoid large diskspace requirements for video storage on FortiPAM. You can send videos to external storage through the SFTP protocol.

See Remote video storage on page 457.

1071941- Support PAC file for the extension

FortiPAM now supports system proxy while applying web proxy on the FortiPAM extension.

A new *PAC Rule Url* field in the *Advanced* tab in *System* > *Settings* where you can provide the PAC script URL. Local FortiPAM settings will take precedence over PAC script settings.

See Settings on page 397.

964887, 924029- Graphical view in *Log & Report*

FortiPAM now displays a graphical summary view for *Secret Event & Video* and *Security Event* in *Log & Report*.

See Log & report on page 323.

1071009- Floating license support

FortiPAM 1.5.0 introduces support for a floating license model for both new and existing FortiPAM units (VMs only).

The floating license is primarily intended for the HA setup.

Previously, if the primary and the secondary FortiPAM unit each held 50 user seats, the total number of seats for the entire cluster was capped at 50.

In FortiPAM 1.5.0 floating license, if the primary and the secondary unit each have 50 user seats, the HA cluster supports up to 100 user seats in total. If the primary unit is offline, users have up to 7 days to restore it. After the grace period of 7 days, if the primary unit is still down, the administrator must reduce the number of active users on the secondary unit to match the license capacity.

For instance, if the cluster has 70 active users when the primary is offline, the administrator must disable 20 users after the grace period of 7 days has elapsed to stay within the license limit of the secondary FortiPAM unit.

When the primary FortiPAM unit is back online, the disabled users are reinstated automatically.



The floating license model is only available on FortiPAM VM instances.

See Licensing on page 49.

878459, 1068247- New setup wizard

The FortiPAM setup wizard gathers all essential settings to setup a FortiPAM from scratch and provide useful information to the new users.

To access the setup wizard, go to *System* > *Setup Wizard*.

See Setup wizard on page 462.

Others

1104270-FortiPAM integration with Terraform

FortiPAM supports secret and folder ID parsing, and secret field filter for the Terraform integration.

The FortiPAM Terraform provider can better support resource management including creating/updating/importing/deleting operations on the target FortiPAM.

Currently, the FortiPAM Terraform provider supports folder and secret resource management.

The FortiPAM Terraform Registry is available here:

https://registry.terraform.io/providers/fortinetdev/fortipam/latest

See Appendix V: Terraform- FortiPAM as a provider on page 671.

1078424- FortiPAM on Alibaba Cloud

FortiPAM now supports Alibaba Cloud virtualization software.

For information on installing FortiPAM on Alibaba Cloud, see the latest FortiPAM Alibaba Cloud Administration Guide.

See:

- Appendix S: Installation on Alibaba Cloud on page 618
- Appendix T: FortiPAM HA on Alibaba Cloud on page 643

1106254- FortiPAM on Proxmox

FortiPAM now supports the Proxmox virtual environment.

For information on installing FortiPAM on Proxmox, see the latest FortiPAM Proxmox Administration Guide.

See Appendix W: Installation on Proxmox on page 675.

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).

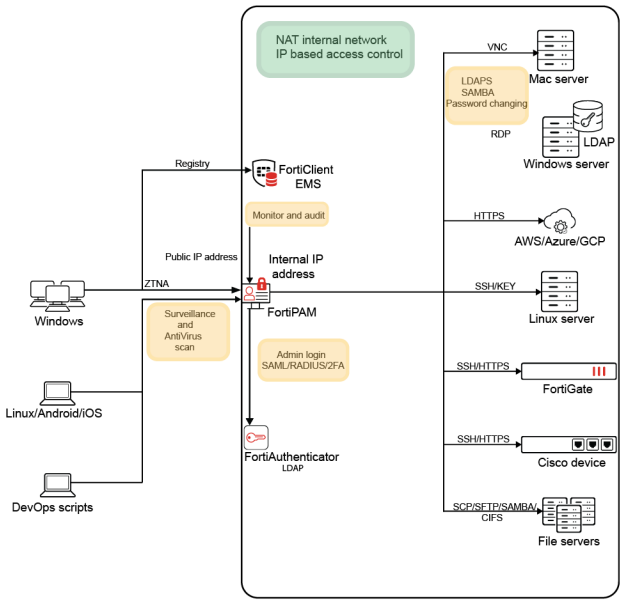
  FortiPAM offers secret permission control to access a target server. Admin users can define common policies and a hierarchical approval system for standard users to access sensitive information. FortiPAM also provides options to control risky user activities such as a user attempting to encrypt the disk.

  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 1.5.1 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 42 describes basic setup information for getting started with your FortiPAM.
- Licensing on page 49 describes how to register, download, and upload your FortiPAM-VM license.
- Dashboard on page 56 contains widgets providing performance and status information.

- Secrets on page 67 describes features and options related to secrets, targets, gateways, folders, secret and job requests, approval lists, jobs, and discovery.
- Secret settings on page 153 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 258 describes managing FortiPAM user database.
- Monitoring on page 319 contains information on user logins and active sessions on FortiPAM.
- Log & report on page 323 describes how to view logs and reports on FortiPAM.
- Network on page 367 describes configuring interfaces, static routes, DNS settings, fabric connectors, and packet capture.
- System on page 397 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 22
- Tables on page 29

For information about using the dashboards, see Dashboard on page 56.

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 23.
- 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 24.
- *Help ( )*: opens the online help document.
- *Notifications ( )*: shows latest notifications.
- *Language*: from the dropdown, select one of the available languages for the GUI. See the *FortiPAM Release Notes* for a list of supported languages.
- *Theme*: from the dropdown, select one of the available themes.

- *Agentless*: All the web based secrets (except Web Account) can be launched without requiring FortiClient or the *Fortinet Privileged Access Agent* browser extension to be installed locally.
  - *Automatic*: The default mode.

    FortiPAM attempts to launch using the priority: *FortiClient* > *Extension* > *Agentless*.
  - *Extension*: Force FortiPAM to use the extension to launch secrets and record secret sessions.

    This works with web based launchers.

    The option is unavailable if no extension is detected in the web browser.

    This has no impact when attempting to launch with a native launcher.
  - *Agentless*:

    New *Agentless* mode for launching web based secrets without requiring the assistance of either FortiClient or the *Fortinet Privileged Access Agent* browser extension to be installed locally.

    This works with web based launchers.

    This has no impact when attempting to launch with a native launcher.

    See Agentless mode on page 39.
- *Admin*: from the dropdown, see FortiPAM version and build, view your *User Profile*, go to *System* and *Configuration*, *Change Password*, or *Logout*. See Admin on page 24.

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.

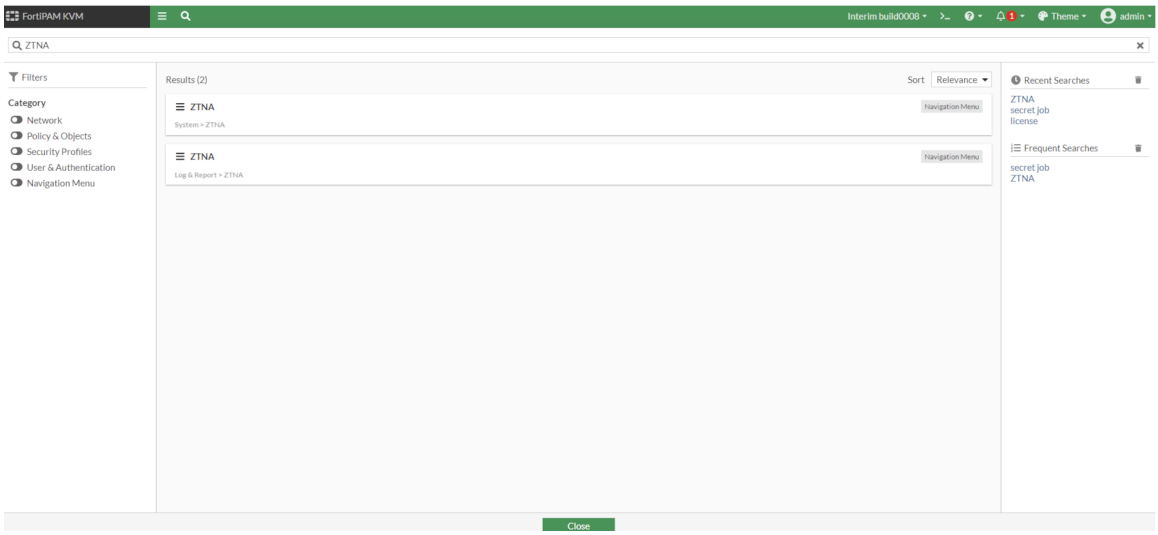
The global search includes the following features:

- 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.
- *User Profile*: access your user profile. The user profile displays information about the administrator's *Name*, *Last Login Time*, *Last Login IP*, *Last Failed Login Time*, and *Email*. Users can edit the email associated with their user profile through this menu. See Viewing your user profile on page 28.
- *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 26.
- Uploading a license. See Licensing on page 49.
- Restoring a configuration. See Backup and restore on page 27.

- *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 363.

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 289.



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

To deactivate glass breaking mode:

1. From the user 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*.



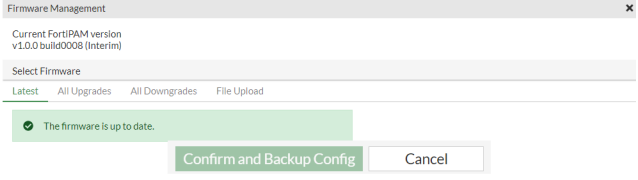
When in maintenance mode, select *Renew Maintenance Mode* in *System*, enter the new duration and reason and then click *OK* to renew the maintenance mode.



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.



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.

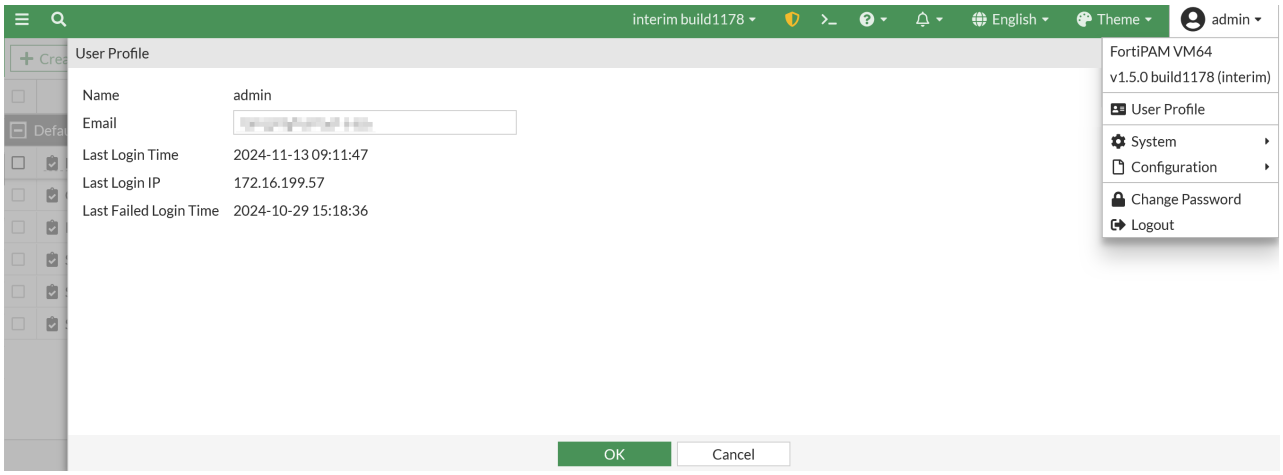
Viewing your user profile

1. In the user dropdown, go to *User Profile*.
   The *User Profile* window displays the following information:

Name	The username.
Email	The email address associated with your user profile. This field can be edited by the user.
Last Login Time	The last time the user logged in.
Last Login IP	The IP address used the last time the user logged in.
Last Filed Login Time	The last time the user attempted a login and failed.

2. Optionally, edit the email address associated with your user profile.

3. Click *OK*.



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

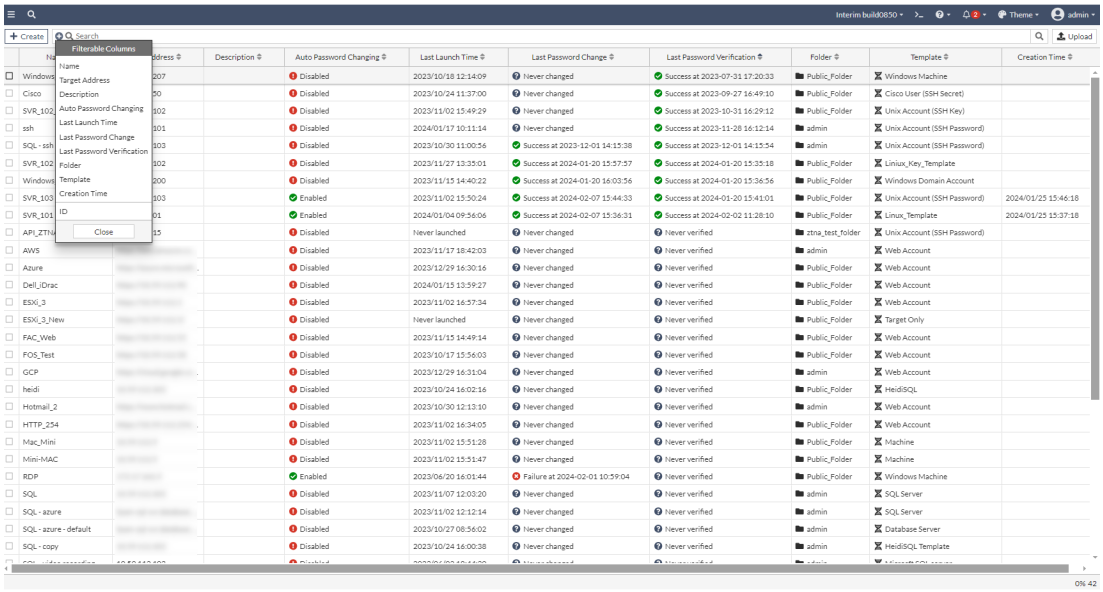
Filters are used to locate a specific set of information or content in a table. They can be particularly useful for locating specific log entries. The filtering options vary, depending on the type of information in the log.

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.

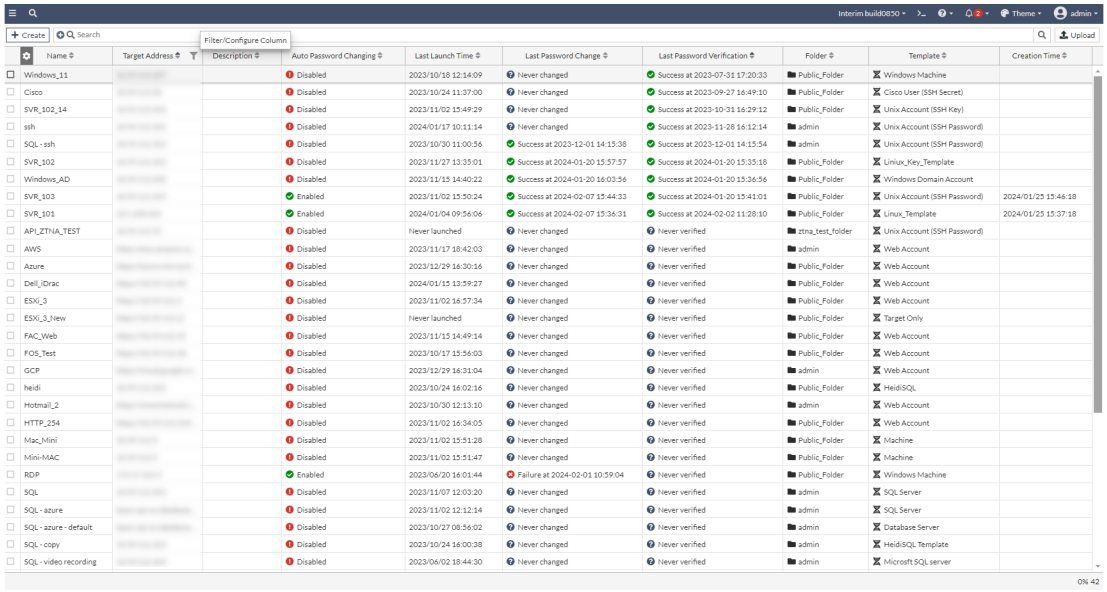
Administrators with read and write access can define filters. Multiple filters can be applied at one time.

To create a column filter:

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



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

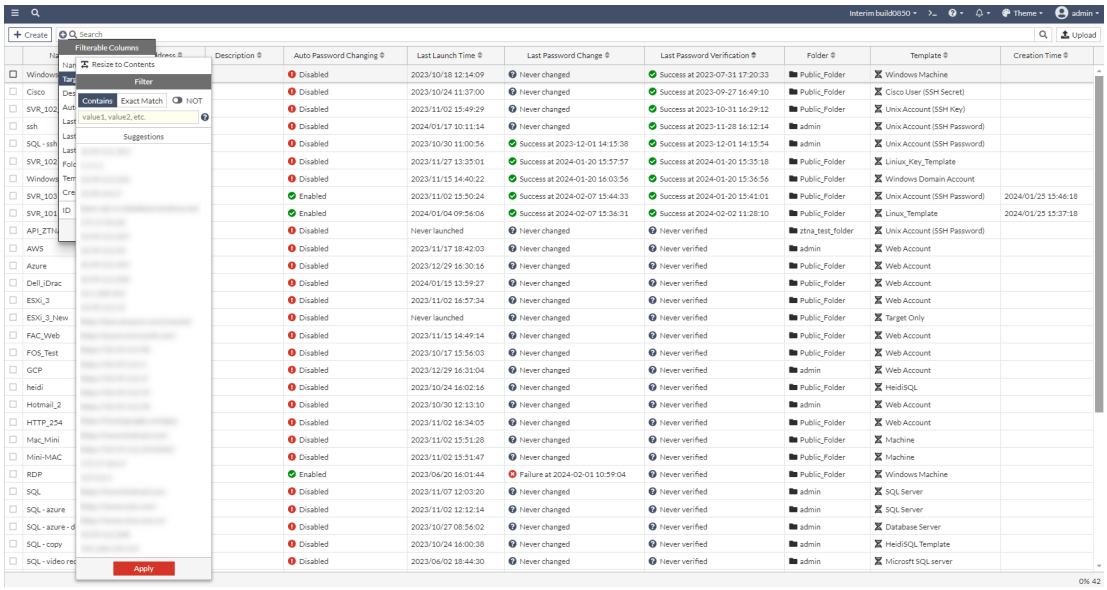




When importing users as shown in Importing LDAP users on page 277, the *Filter/Configure Column ( )* icon is available next to *All Users*.

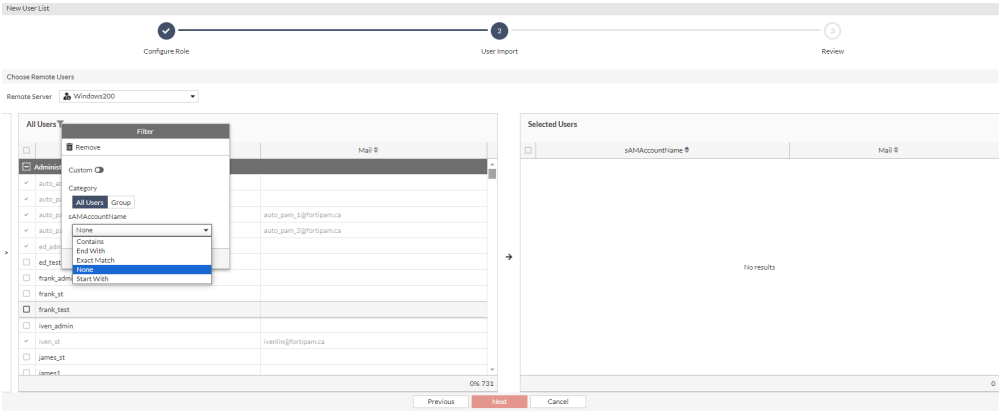
2. Select one of the columns as a filter.

3. In the window that opens, you can set combinations of *Contains*, *Exact Match*, and *NOT*.

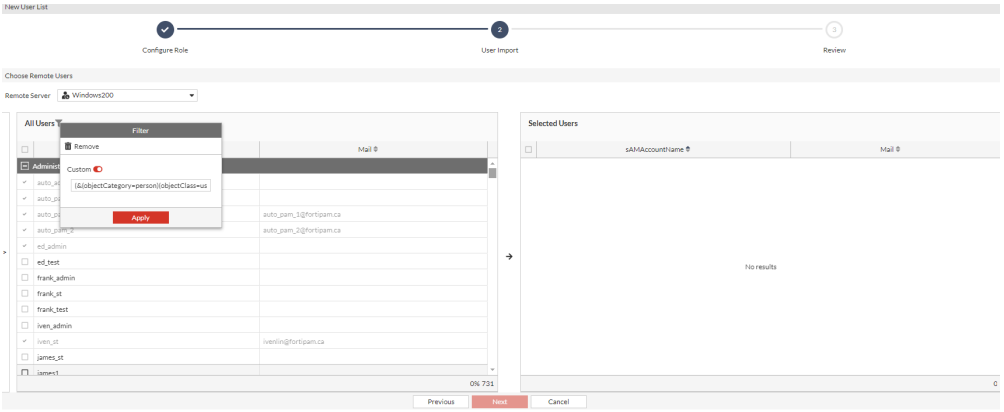


When importing users as shown in Importing LDAP users on page 277, the following options are available for *All Users* and *Group*:

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

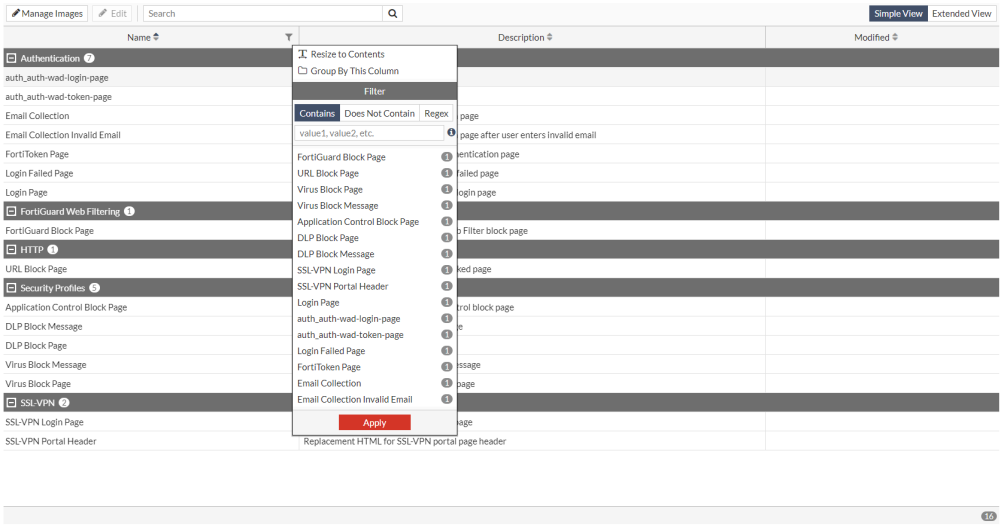


You can also create a custom filter by enabling *Custom* and setting up a filter:



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

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



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 71. Alternatively, see the *Proxy Mode* option when creating or editing a policy. See Creating a policy on page 180.

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.

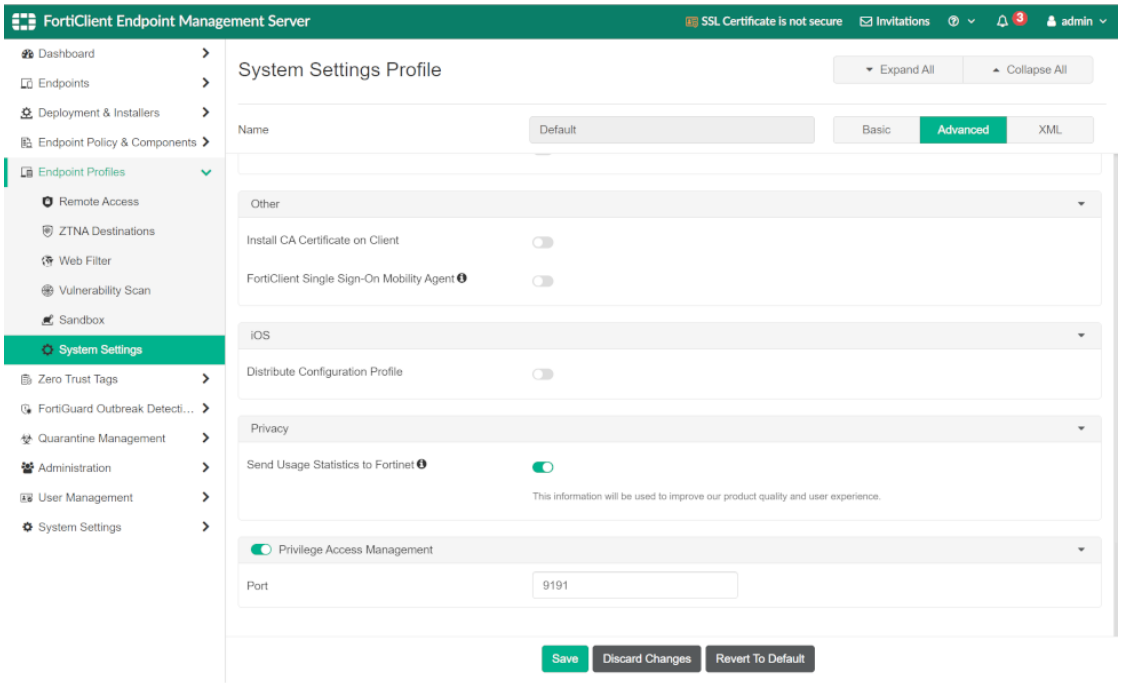
For information on installing FortiPAM browser extension and standalone FortiClient on an air-gapped computer, see Appendix M: FortiPAM browser extension and standalone FortiClient air-gapped installation on page 569.

For information about the over-the-shoulder monitoring (live recording) feature, see Over-the-shoulder monitoring (Live recording) on page 321.

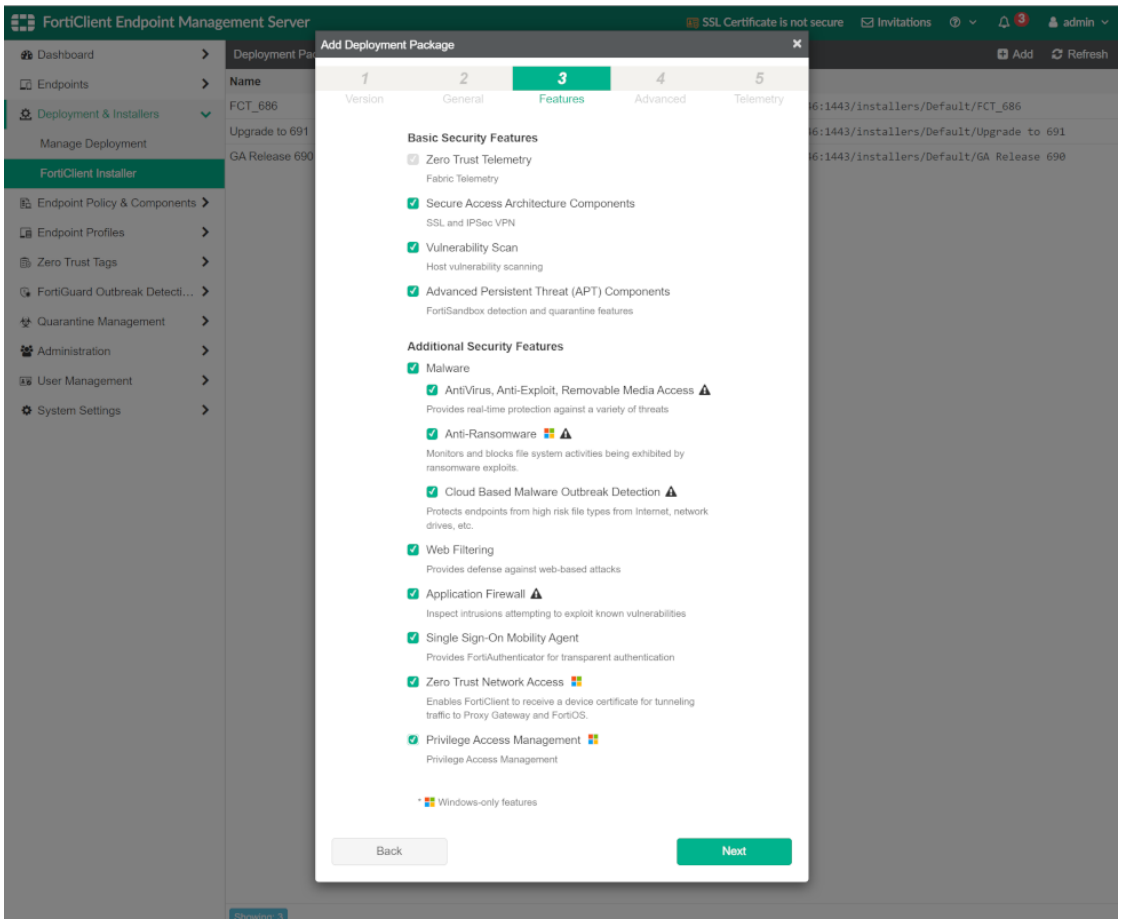
If FortiClient is not available, e.g., a user with Linux or MacOS system, Chrome and Edge extension called *Fortinet Privileged Access Agent* is available on Chrome Web Store and Microsoft Edge Add-ons. On this extension-only setup, web-based launchers and web browsing are supported. The extension can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

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

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



      ii. Push FortiClient (7.2.0 or later) to registered PC-
         i. Navigate to *Deployment & Installers* > *FortiClient Installer*.
         ii. Add a package with both *Zero Trust Network Access* and *Privilege Access Management* enabled on the third tab of the wizard.



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

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

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

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

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

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

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

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

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

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

Feature availability

The following table lists FortiPAM 1.5.1 feature availability based on the type of deployment being used:

Feature	FortiPAM with standard FortiClient	FortiPAM with standalone FortiClient	FortiPAM with browser extension	FortiPAM only
Windows OS	✓	✓	✓	✓
Linux OS	X	X	✓	✓
MacOS	X	X	✓	✓
ZTNA	✓	X	X	X
Web-based launchers, i.e, Web-SSH, Web 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

Agentless mode

In the new *Agentless* mode, FortiPAM provides the ability to all the web based launchers (except *Web Account*) to launch web based secrets without requiring the assistance of either FortiClient or the *Fortinet Privileged Access Agent* browser extension to be installed locally.

For information on the GUI options, see Banner on page 22.

Supported web based launchers include the following:

- *Web SSH*
- *Web RDP*
- *Web VNC*
- *Web SFTP*
- *Web SMB*
- *Web Telnet*

Supported web browsers include the following:

- Google Chrome
- Microsoft Edge

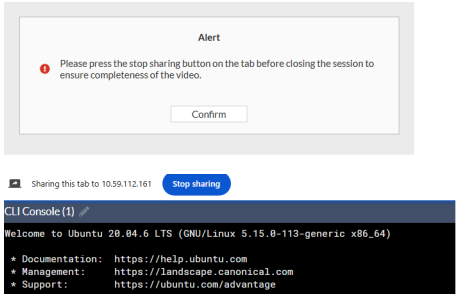
The feature reduces dependency on environment resources and maintenance costs. Additionally, it enhances FortiPAM security, portability, and the overall efficiency.

When in the *Agentless* mode:

- A warning tab appears asking you to: `Allow <FortiPAM_URL> to see this tab?`
  After launching the secret, you must select *Allow* in the `Allow <FortiPAM_URL> to see this tab?` to let secret video recordings work.

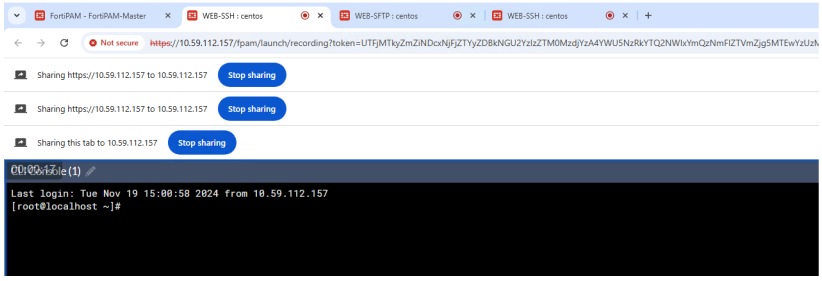


- Once the secret session is launched, there is a header with *Stop sharing* button on top of the browser. The session lifetime is also displayed.
  By clicking *Stop sharing*, the secret session is closed and the video is uploaded.

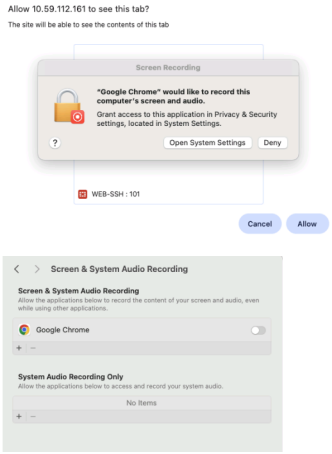


You can terminate the secret session by closing the browser tab.

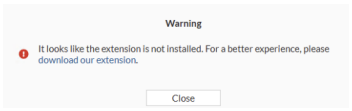
- Multiple headers show up when there are multiple ongoing secret launch sessions.
  When you terminate a secret launch session using the *Stop sharing* button, the message on the header changes to `Sharing this tab to....`
  You must click *Stop sharing* to terminate this session.



- On the macOS, you must provide *Screen & System Audio Recording* permission to the browser for the *Agentless* mode to work.



When the browser extension is not installed, a warning appears.



Limitations

Currently, the *Agentless* mode has the following 3 limitations:

- The feature does not work with the Mozilla Firefox browser.
- The feature does not work with the *Web Account* launcher.
- The feature does not work with a service gateway.

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 1.5.1:

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

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.

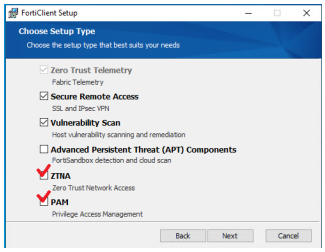
See Installing FortiClient with the FortiPAM feature on page 43 and FortiPAM appliance setup on page 43.

Installing FortiClient with the FortiPAM feature

To install FortiClient:

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

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



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

3. Reboot the PC.

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

Uninstalling FortiClient

To uninstall FortiClient:

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

FortiPAM appliance setup

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

FortiPAM-VM image installation and initial setup

See Appendix A: Installation on KVM on page 493.

See Appendix B: Installation on VMware on page 496.

See Appendix F: Installation on Hyper-V on page 506.

See Appendix G: Installation on Azure on page 518.

See Appendix J: Installation on AWS on page 534.

See Appendix K: Installation on GCP on page 547.

See Appendix S: Installation on Alibaba Cloud on page 618.

See Appendix W: Installation on Proxmox on page 675.

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 493.

```
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 46.
5. Optionally, to encrypt disk to protect logs and videos, see Configuring log and video disk encryption on page 357.
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 50.
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 467.

   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 361 and Email alert when the glass breaking mode is activated example on page 363.

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.

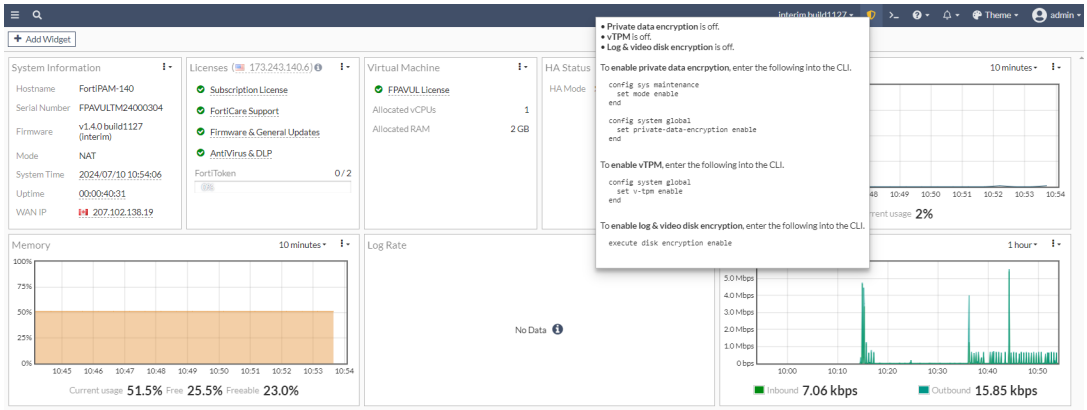
FortiPAM with TPM

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.



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 501 and Appendix D: vTPM for FortiPAM on VMware on page 503.



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 24.

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
```

Floating license

FortiPAM supports a floating license model for both new and existing FortiPAM units (VMs only).

The floating license is primarily intended for the HA setup.

Previously, if the primary and the secondary FortiPAM unit each held 50 user seats, the total number of seats for the entire cluster was capped at 50.

In FortiPAM 1.5.0 and above with floating license, if the primary and the secondary unit each have 50 user seats, the HA cluster supports up to 100 user seats in total. If the primary unit is offline, users have up to 7 days to restore it. After the grace period of 7 days, if the primary unit is still down, the administrator must reduce the number of active users on the secondary unit to match the license capacity.

For instance, if the cluster has 70 active users when the primary is offline, the administrator must disable 20 users after the grace period of 7 days has elapsed to stay within the license limit of the secondary FortiPAM unit.

When the primary FortiPAM unit is back online, the disabled users are reinstated automatically.



The floating license model is only available on FortiPAM VM instances.

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 54 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 61.

Email alert for license expiration

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

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

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

To set up email alerts for license expiry:

1. Ensure that *Email Service* is set up in *System* > *Settings*. See Settings on page 397.
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.

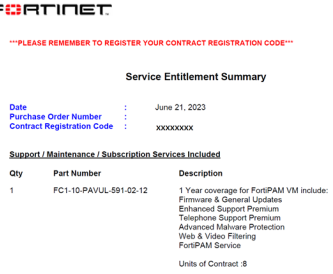
The Advanced Malware Protection (`AVDB & DLP`) licenses are related to the file scanning feature in file launchers. Once the Advanced Malware Protection license expires:

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

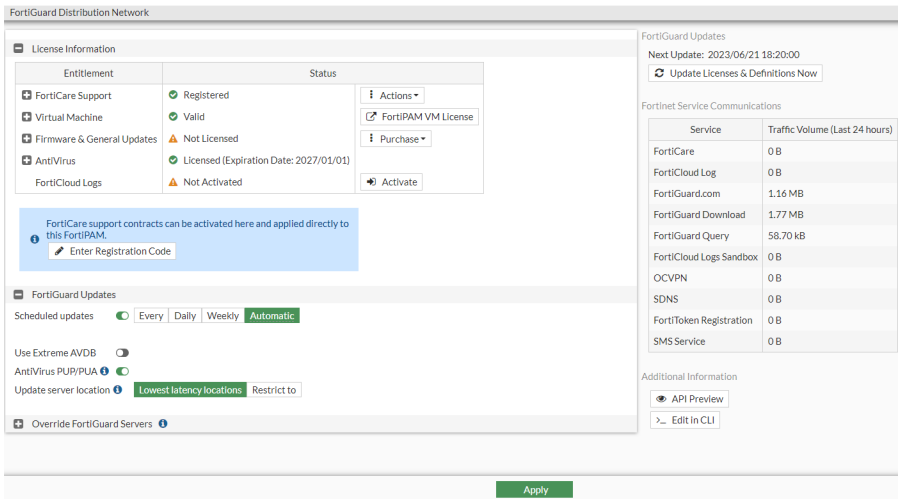
Service Entitlement Summary

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

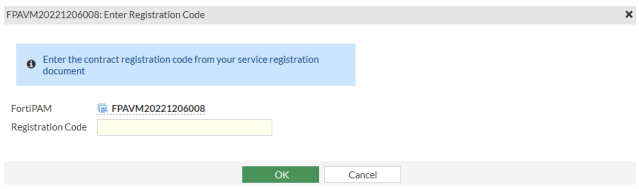
Support / Maintenance / Subscription Services Included

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*.

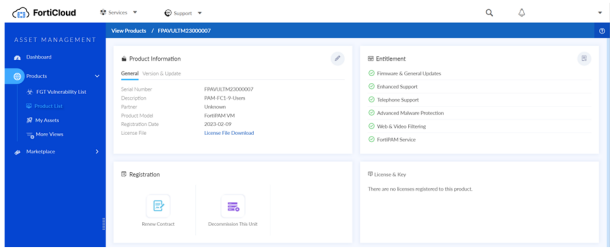


      ii. In *License Information*, click *Enter Registration Code*.
      The *Enter Registration Code* window opens.



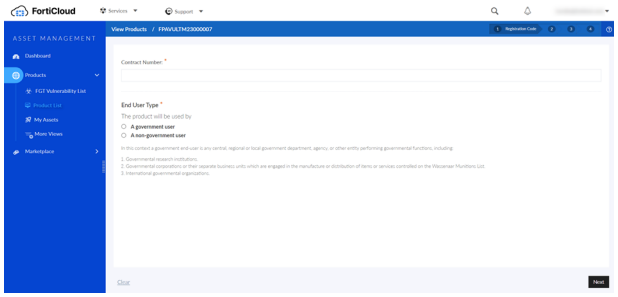
      iii. In *Registration Code*, enter the *Contract Registration Code* that you saved in step 2.
      iv. Click *OK*.
      v. Click *Apply*.
   b. **Registering directly on FortiCloud**:
      i. Go to FortiCloud and create a new account or log in with an existing account.
      The *Asset Management*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

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



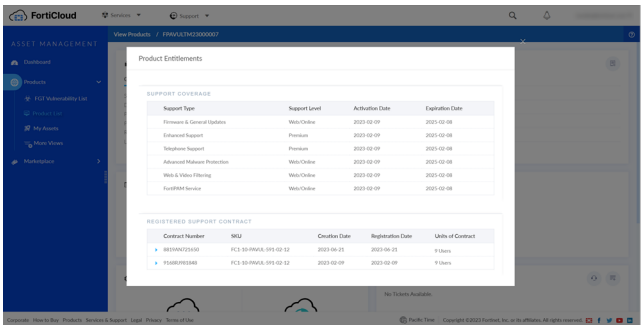
iv. Enter the *Contract Registration Code* that you earlier saved in step 2 in the *Contract Number* field.

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



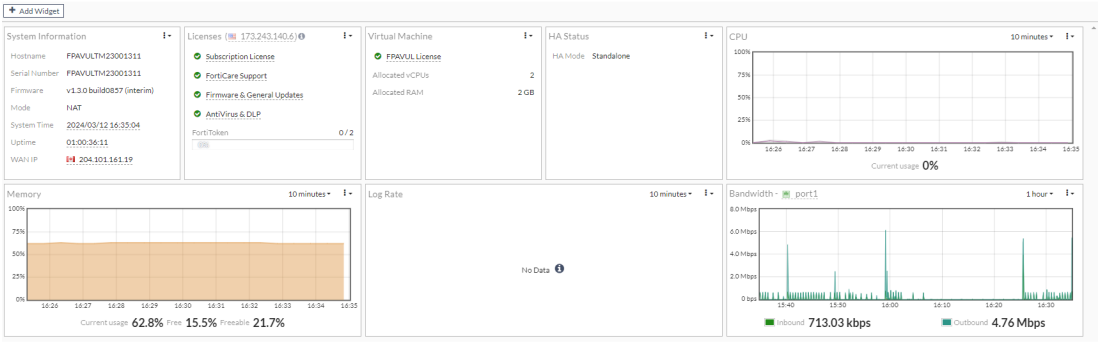
vi. Click *Next* and follow the prompts to complete renewing the license.

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



Dashboard

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



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

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

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

System Information	Displays basic information about the FortiPAM system including host name, serial number, firmware version, mode, system time, uptime, and WAN IP address. From this widget you can manually update the FortiPAM firmware to a different release. See Uploading a firmware on page 26 and System information widget on page 59. You can also configure system settings using this widget. For information on system settings, see Settings on page 397.
Licenses	Displays the status of your license and FortiGuard subscriptions. See Licenses widget on page 61.
Virtual Machine	Displays license information, number of allocated vCPUs, and how much RAM has been allocated. See VM license on page 65.
HA status	Displays HA mode. See High availability on page 414.
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 354.
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.

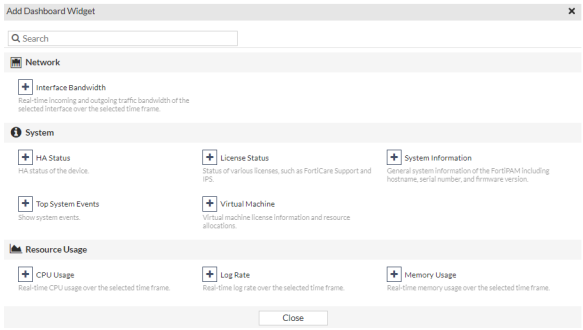
You can add the following *Resource Usage* widgets to the *Dashboard*:

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.



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

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

4. Click *Add Widget*.

Widget actions

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

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

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

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

Adding a custom dashboard

To add a custom dashboard:

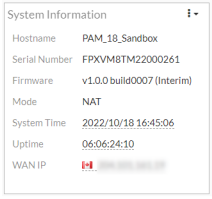
1. In the menu, go to *Dashboard* and select +.
   The *Add Dashboard* dialog opens.



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

System information widget

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



The following information is available on this widget:

Host Name	The identifying name assigned to this FortiPAM unit. For more information, see Changing the host name on page 60.
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 26.
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 60.
Uptime	The duration of time FortiPAM has been running since it was last started or restarted.
WAN IP	The WAN IP address and location. Additionally, if the WAN IP is blocked in the FortiGuard server, there is a notification in the notification area, located in the upper right-hand corner of the *Dashboard*. Clicking on the notification opens a window with the relevant blocklist information.

Changing the host name

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

To change the host name:

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

Configuring the system date, time, and time zone

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

To configure the date and time manually:

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

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

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

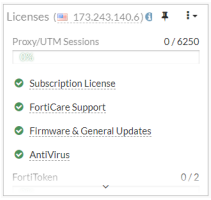


Custom server details must be configured in the CLI.

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

Licenses widget

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



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

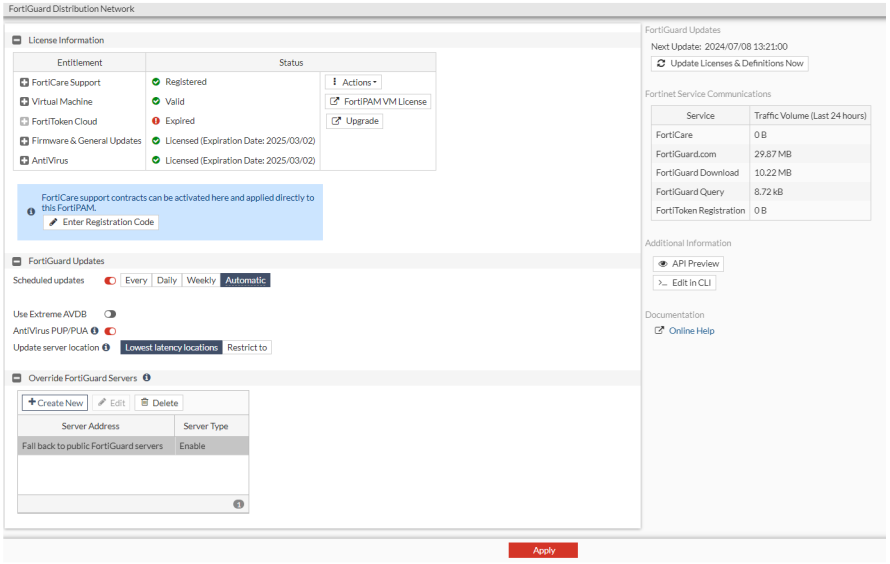
To view details on licenses, see FortiGuard Distribution Network on page 61.

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.



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.

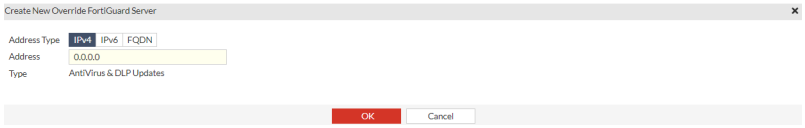
See Override FortiGuard Servers on page 64.

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.



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*.

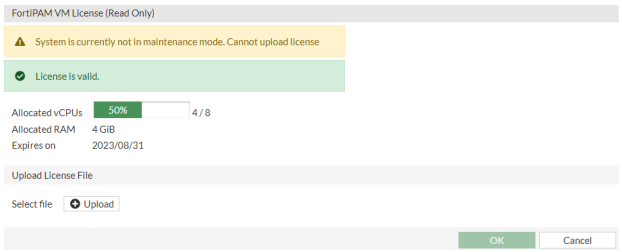
VM license

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 24.



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 68
- Targets on page 116
- Personal/public folder on page 127
- My requests list on page 136
- Approval list on page 140
- Job list on page 144
- Discovery on page 147

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 289.

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*



The *Description* column is not visible by default.

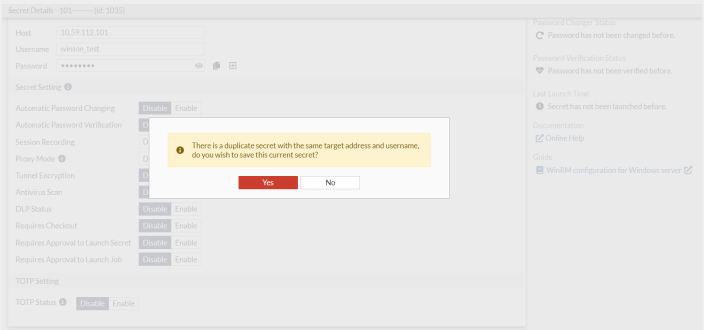
To display the *Description* column, select *Configure Table* icon as you click the header for the left-most column, select *Description* and then click *Apply*.

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.:

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 71. 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. 
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 101.
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 99.
Make Request	Make request to launch or perform a job on the secret. Make a request on page 137.
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:

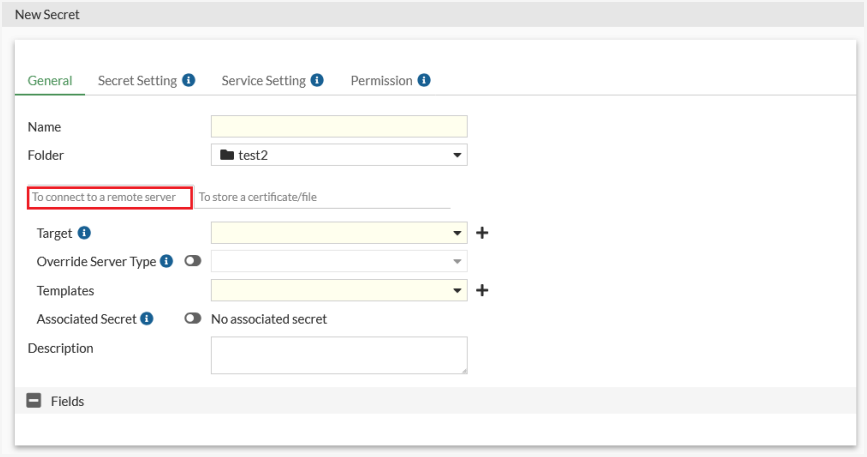
1. Go to *Secrets* > *Secrets*.
   Alternatively, go to *Personal Folder/Public Folder* in *Secrets*, select *Open Tree*, locate the folder where you intend to add the secret, and click *Open*.
   From the *Create* dropdown, select *Secret*, and skip to step 6.
2. In *Secrets*, select *Create*.
   The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

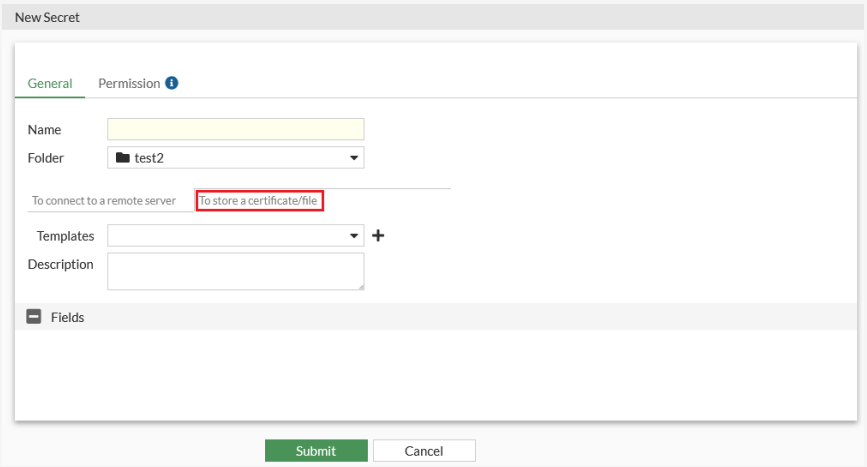
   The folder is already selected if you are creating secret from inside a folder.

4. Select *Create*.
   The *General* tab opens. To switch to *Secret Setting*, *Service Setting*, *Permission*, or *Dependency* tabs, select the tab.
5. Enter a *Name* for the secret, and choose the *Folder* where the secret is to be added. See Personal/public folder on page 127.

   The folder is already selected in step 2. Use the dropdown, if you want to change the folder.

6. Choose the type of secret that you are creating from one of the following tabs presented in the GUI. The remaining secret settings available in the GUI will change depending on the selection.

To connect to a remote server	Select this tab to create a secret which can be launched to connect to a remote server (example: a Linux Server by SSH, Windows Host by RDP, or a MacOS by VNC). 

To store a certificate/file	Select this tab to create a secret which is only used to save certificate or text content. 

7. Configure the remaining *General* settings.

Target	Select a target from the dropdown for the new secret being created. In the dropdown, select + to create a new target. See Creating a target on page 117.  The *Default Template* from the target will automatically 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 73.
Override Server Type	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* • FortiOS • *Cisco* • Windows • ESXi • *Other*
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.
Templates	From the dropdown, select a template. Select *Create* to create a new template. See Creating secret templates on page 157.

	 **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*.
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 Secret gateway on page 384.  The option is non-editable.  The option is only available when you select a target with gateway included. See Creating a target on page 117.
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 98. **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 225.

The options in the fields depend on the selected template.

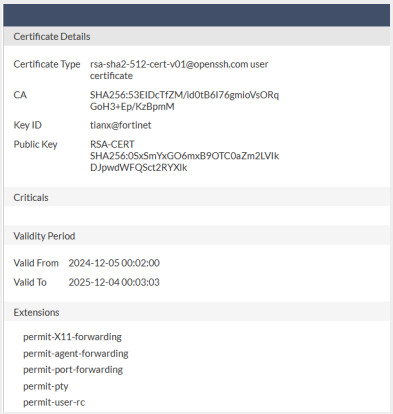
For fields where a host is required when using the FortiPAM browser extension, enter the URL instead.

The *Public-key* dropdown allows you to select the type of public key to use when the template is either *FortiProduct (SSH Key)* or *Unix Account (SSH Key)*.

You can choose from the following two public key types:

- *Standard public key*
- *Public key with certificate*: Select to allow certificate based authentication.

  By clicking the eye icon next to the public key, the certificate details are displayed.



  The certificate based SSH authentication improves authentication security by controlling the certificate expiry date.

On the *Secret Details* page, the certificate validity period and the status are displayed.



You can set email alerts for expiring certificates.

See the *Certificate* tab in Email alert settings on page 361.

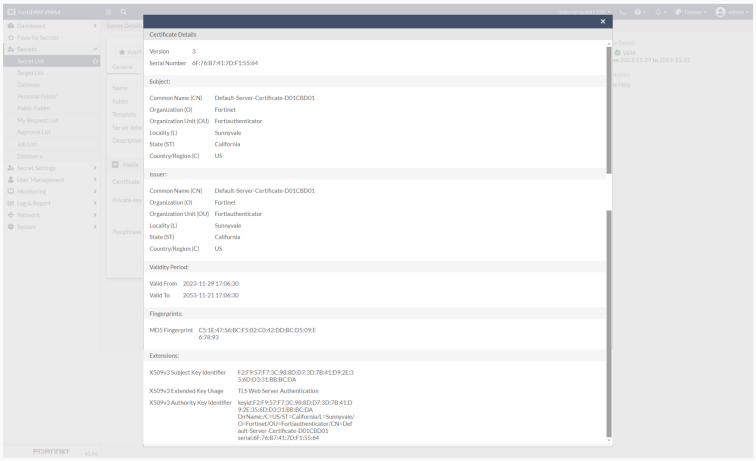
Certificate

You can create secrets to store certificates by choosing the *To store a certificate/file* option on the *General* tab.

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* template, click the view icon to view the uploaded certificate.



Click the delete icon to delete the uploaded certificate.

Notes:

- The option is only available when the *Template* is *Certificate*.
- Other fields for a secret created using the *Certificate* template include *Private-key* and *Passpharse*.

You can set email alerts for expiring certificates.

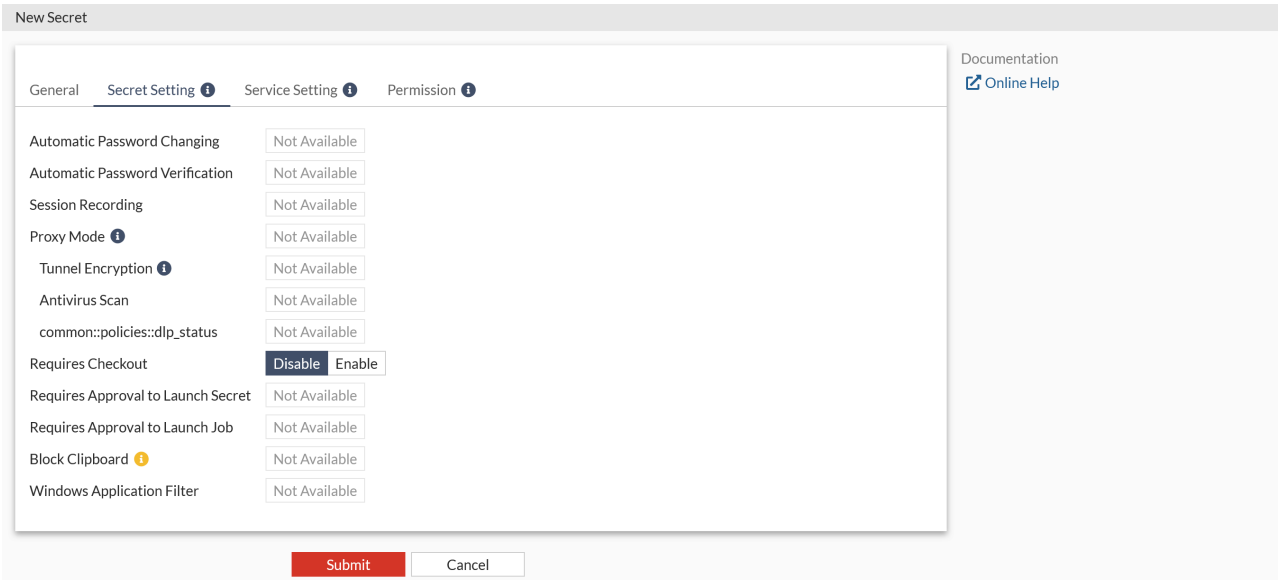
See the *Certificate* tab in Email alert settings on page 361.

Launcher	From the list, you can use a launcher to launch the secret.

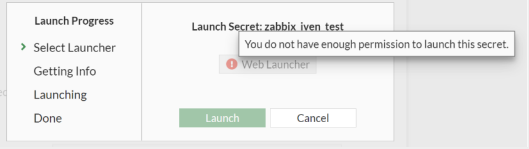
8. Configure the *Secret Settings* tab.

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 321.
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 34. 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: 

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 368.

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 117.
- When you edit the *Web Proxy* option, you are editing the *Web Proxy* option available from within the associated secret target.



When web proxy is enabled, FortiPAM uses `gui-service-fqdn` if `web-proxy.global.proxy-fqdn` is not set already.

See Changing the FortiPAM URL to an FQDN in the approval email bodyCLI on page 140.

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 232.
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 229.
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 101.
Checkout Duration	The checkout duration, in minutes (default = 30, 3 - 120).
Force Checkout Idle time	Force checkout works for all the users that can access a secret. A user can force checkout a secret when the current user who has checked out the secret does not have an active launch session for at least the time set in the *Force Checkout Idle time* field, in minutes (default = 5, 0 - 30). The default value of 5 implies that the current user has closed all their launch session and has not used/launched the secret for 5 minutes. Another user can force check out the secret now. **Note**: The *Force Checkout Idle time* field can be set up only when *Proxy Mode* and *Session Recording* are already enabled.
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 137 and Approval flow on page 194.
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 137 and Approval flow on page 194.
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 250.
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*.  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 94.

See Limitations of TOTP on FortiPAM on page 164.

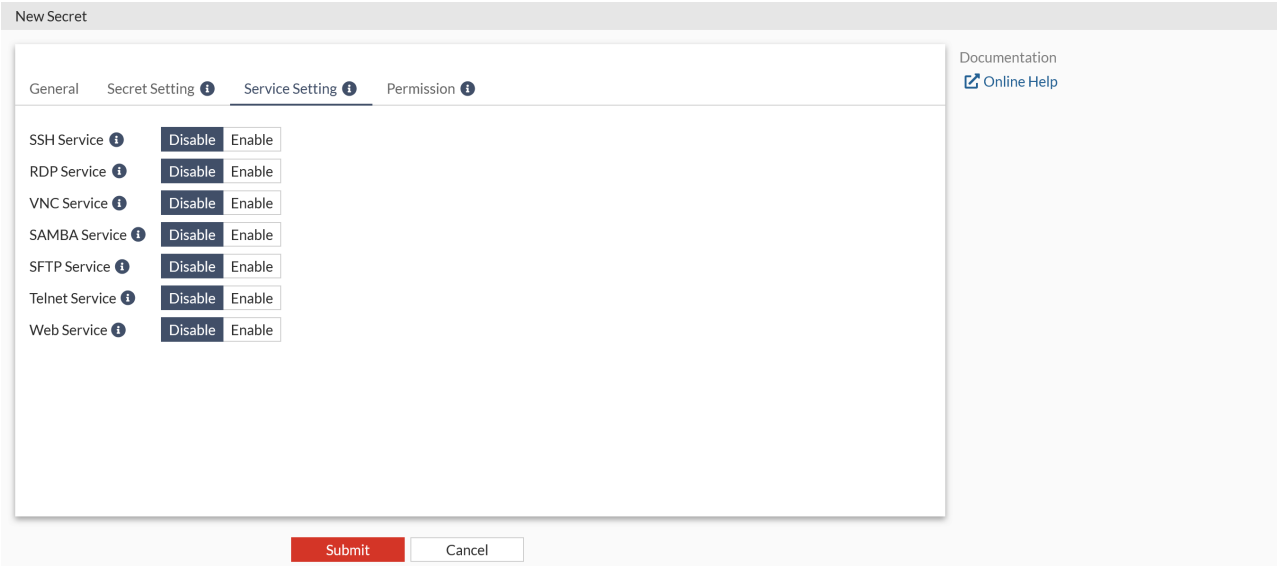
Note: The option is disabled by default.

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*.

9. Configure the *Service Settings* tab.



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 241.
	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-1 signing algorithm* (default) • *RSA SHA-256 signing algorithm* • *RSA SHA-512 signing algorithm* • *ssh-rsa-cert_v01@openssh.com* • *rsa-sha2-256-cert_v01@openssh.com* • *rsa-sha2-512-cert_v01@openssh.com*  If the SSH secret is using the key mode, select from one of the following three options: • *RSA SHA-1 signing algorithm* • *RSA SHA-256 signing algorithm* • *RSA SHA-512 signing algorithm*  If the SSH secret is using the key and the certificate mode, select from one of the following three options: • *ssh-rsa-cert_v01@openssh.com* • *rsa-sha2-256-cert_v01@openssh.com* • *rsa-sha2-512-cert_v01@openssh.com*
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.
Sudo Prompt	When *SSH Auto-Password* is enabled, you can configure the Sudo Prompt between *Use Default* or a custom configuration. This field defines the context that will show up after entering sudo. It is represented as the *$SUDO_PROMPT* environm ent variable in the Unix system. When *Use Default* toggle is disabled, you can enter the customized prompt based on user's account settings. Entering a custom prompt allows the SSH Auto-Password to function in non-english Linux based systems.

	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 247.
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.
Web Service	Enable/disable the web service. When the Web Service is disabled, the Web Launcher is disabled.

10. Configure the *Permissions* tab.



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. **To use the ZTNA control feature**: 1. Connect to the same EMS server for the client where the FortiClient runs (*Network* > *Fabric Connectors* > *FortiClient EMS*). 2. You must enable *ZTNA Control* in Editing an interface on page 368. Alternatively, see the ZTNA chapter in the latest *FortiPAM Examples Guide*.  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 89 and Group Permission on page 89.
Allowed Service	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*.

11. Configure the *Dependency* tab.

    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.

Dependency

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 192.

See Dependency updater on page 189.

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 190 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 117.  Use the search bar to look up a target.



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

12. Click *Submit*. See Launching a secret on page 99 and Example secret configurations example on page 107.

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 263, 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.

Viewing secret edit history



You must have *View Secret Log* permission to view the secret edit history. See Role on page 289.

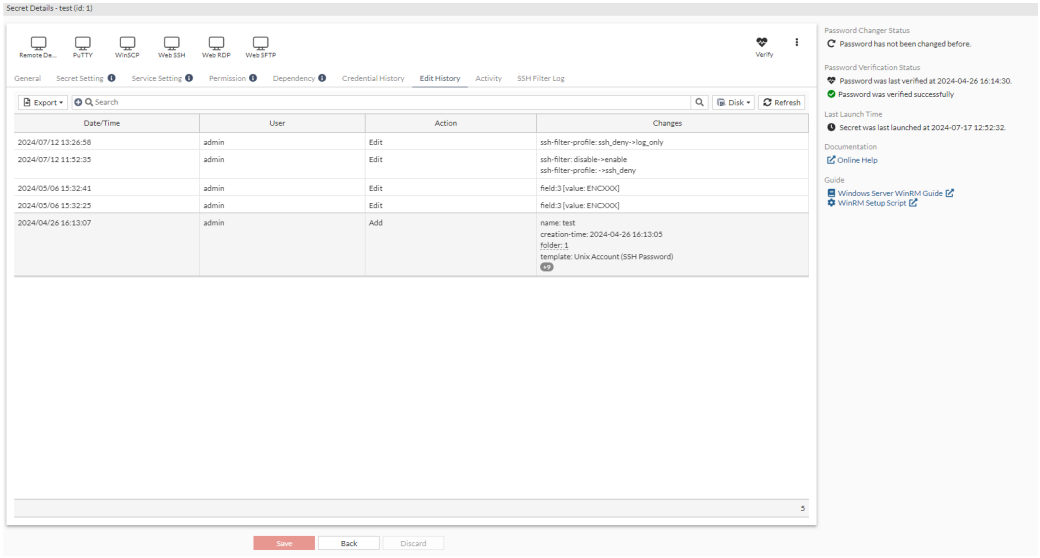


You must have at least *View* permission for the secret to see the *Edit History* tab.

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.



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.

Subscribing to Secret related events

Secret event subscription allows any user to receive email notifications when certain events happen on a specific secret.

The subscribable events are: secret entry change, password change failed, view password clear text, password verify failed, secret check-in, secret check-out, secret launch, and secret certificate expiry notification.

After subscribing to the event, once an event is triggered, an email is sent to the user email configured in the user profile.

Event subscription configurations are applied to the currently logged in user.

In order to receive alerts:

- *Enable Email Notification* must be enabled in *Log & Report* > *Email Alert Settings*. See Email alert settings on page 361.
- The subscribers must configure their own email in User Profile.

To configure event subscription for a Secret:

1. Go to *Secrets* > *Secrets*.
2. Edit a Secret in the Secret List table.
3. Click on the *Event Subscription* tab.
4. Select the events to which you want to subscribe. You will receive an email notification when the corresponding event is triggered.

   The following events are available for Secrets for connection to a remote server:

All Events	Subscribe to all events.
Secret Entry Change	When a Secret has changed.
Password Change Failed	A password change operation has failed.
View Password Clear Text	When a password is viewed in clear text.
Password Verify Failed	When password verification fails.
Secret Check-in	When a Secret check-in event occurs.
Secret Check-out	When a Secret check-out event occurs.
Secret Launch	When a Secret launch is attempted.

   The following events are available for Secrets for storing a certificate/file:

Secret Certificate	When a Secret certificate is expiring. The number of days before expiration that the notification will be sent can be configured in *Log & Report* > *Email Alert Settings* > *Certificate*.

5. Click *Save*.

Event subscription is automatically disabled for a user if that user loses permissions for the Secret.

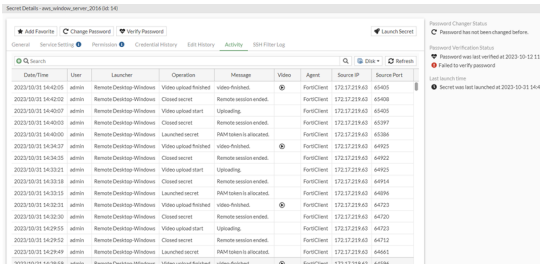
Viewing secret activity

You must have *View Secret Log* permission to view secret activity. See Role on page 289.

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.



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.

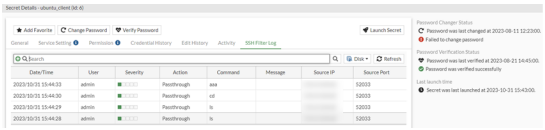
Viewing SSH filter logs for a secret

You must have *View Secret Log* permission to view SSH filter logs for a secret. See Role on page 289.

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.



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.

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-settings
   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`.

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.

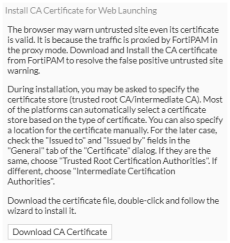
The browser may warn untrusted sites even if its certificate is valid. This is because the traffic is proxied by FortiPAM in the proxy mode. Download and install the CA certificate from FortiPAM to resolve the false positive untrusted site warning.

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.



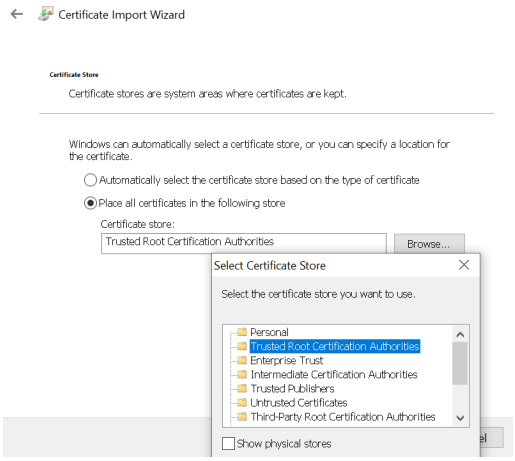
Also, when there are multiple certificates that you need to install, a *Download All CA Certificates* button is available instead.

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.



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.

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. 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`.

Launching a secret

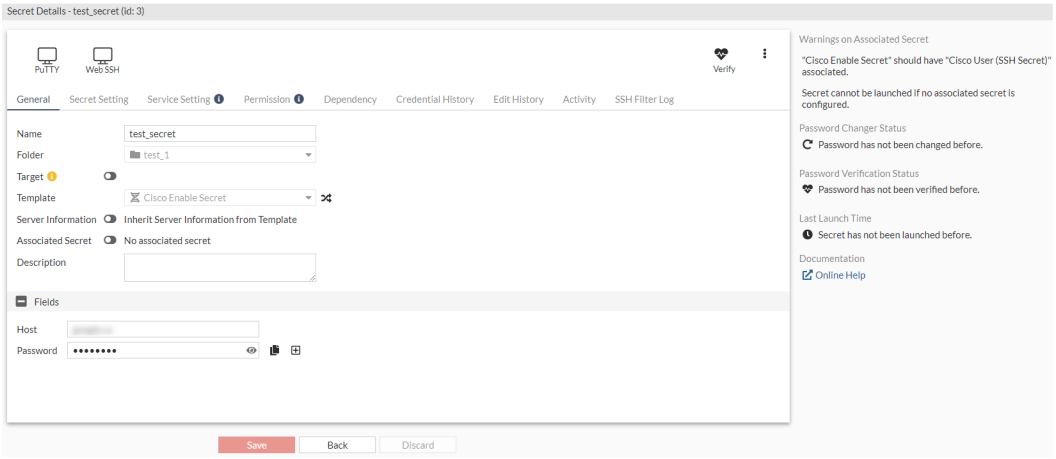
To launch a secret:

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.



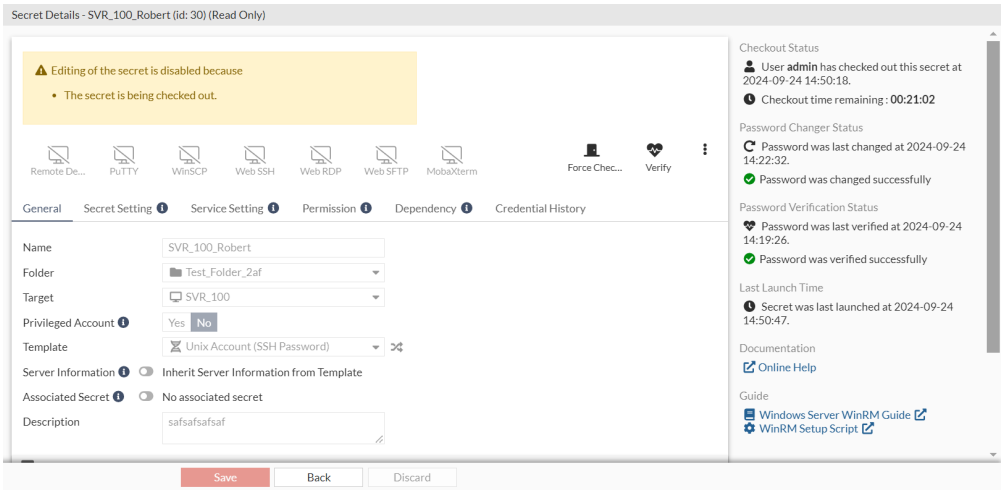
If the secret does not show up, it may be because you do not have the necessary permission to access the secret or the folder where the secret is located.

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



When a secret that has *Force Checkout Idle time* set up is checked out, a super administrator can override the checkout and force a check in using the *Force Checkin* option once the idle time set up in the *Force Checkout Idle time* field has elapsed.

A user can force checkout a secret when the current user who has checked out the secret does not have an active launch session for at least the time set in the *Force Checkout Idle time* field.



See Creating a secret on page 71.

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 180 and Creating a secret on page 71. Also, see AntiVirus on page 229.

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 232.

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

See Check out and check in a secret on page 101.

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 71.

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 71.



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 71.

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.

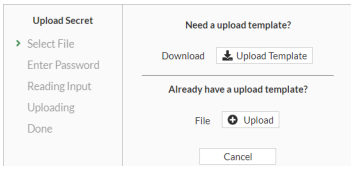
When importing a secret, FortiPAM first scans if a corresponding target exists by matching *Host*, *URL*, and *Domain*.

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.



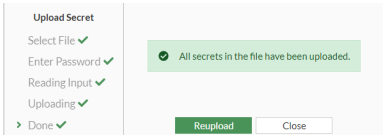
You can create custom secret templates in the secret upload template file by selecting *Customized* from the *Secret Template* column.

7. Fill in the fields highlighted in yellow.



The fields highlighted in red cannot be edited.

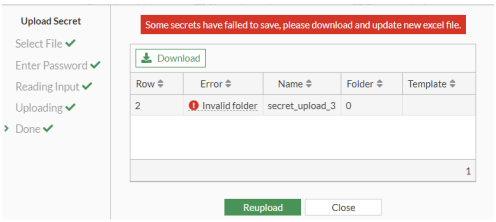
8. Save the file as `.xlsm`(Excel workbook) or a `.csv`(Comma delimited) file on your computer.
9. In the *Upload Secret* dialog, select *Upload*, locate the secret upload template file and click *Open*.
10. In *Password*, enter the password set in step 3 to decrypt the secret upload template, and click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



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



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



Change password

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

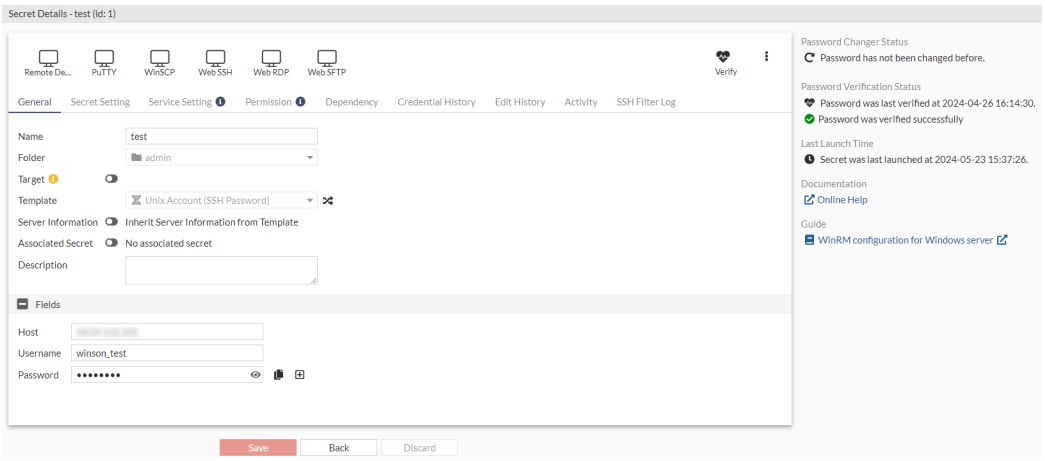
You can only manually change the passwords every 30 seconds.

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

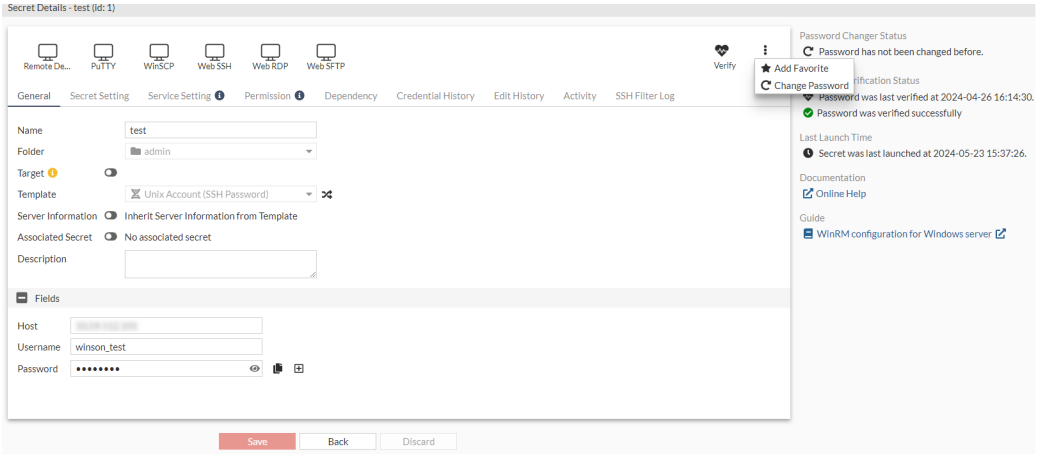
See Automatic password changing on page 224.

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.



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



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

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

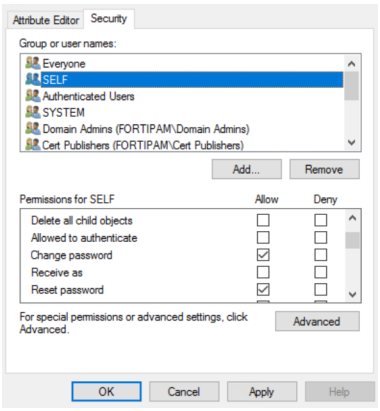
   To be able to successfully change the password manually, the password must follow password requirements set in Password policies on page 225.

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.

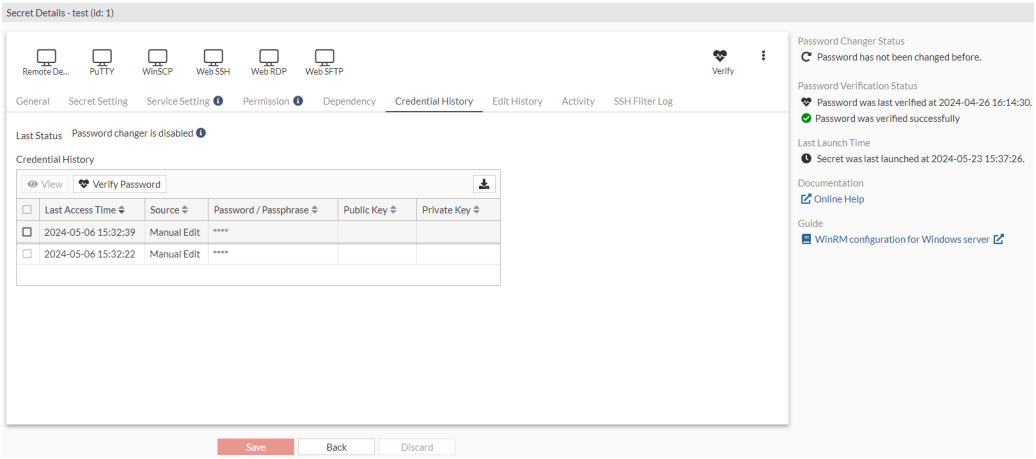
For example, in the screenshot below, *Change password* and *Reset password* are allowed for *SELF*, i.e., the user.



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.



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.

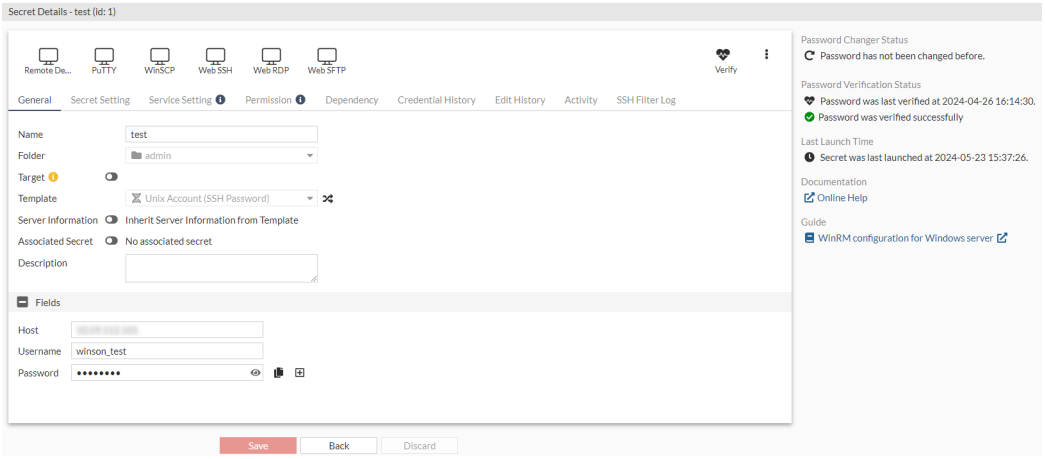


You can also set up a secret to automatically verify the password by enabling *Automatic Password Verification* when creating or editing a secret.

See Automatic password verification on page 225.

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.



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*.

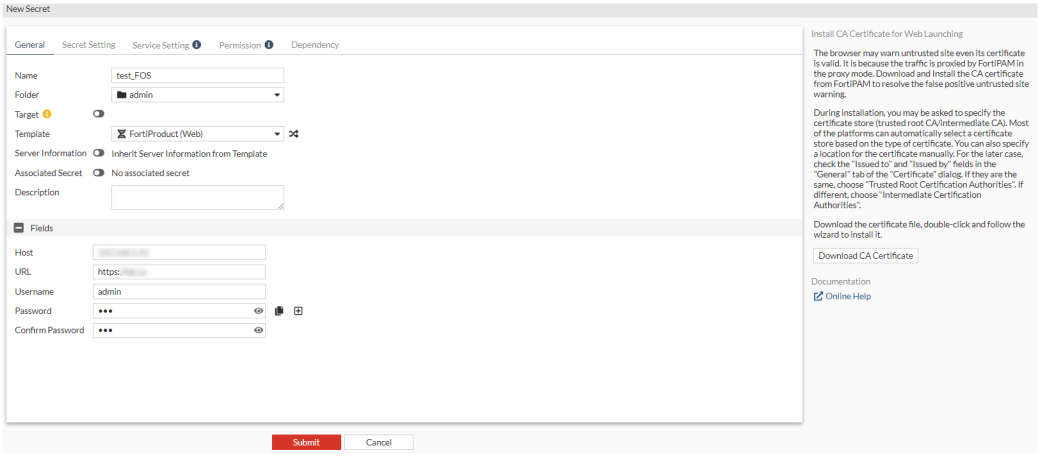
To configure an AWS web account secret:

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

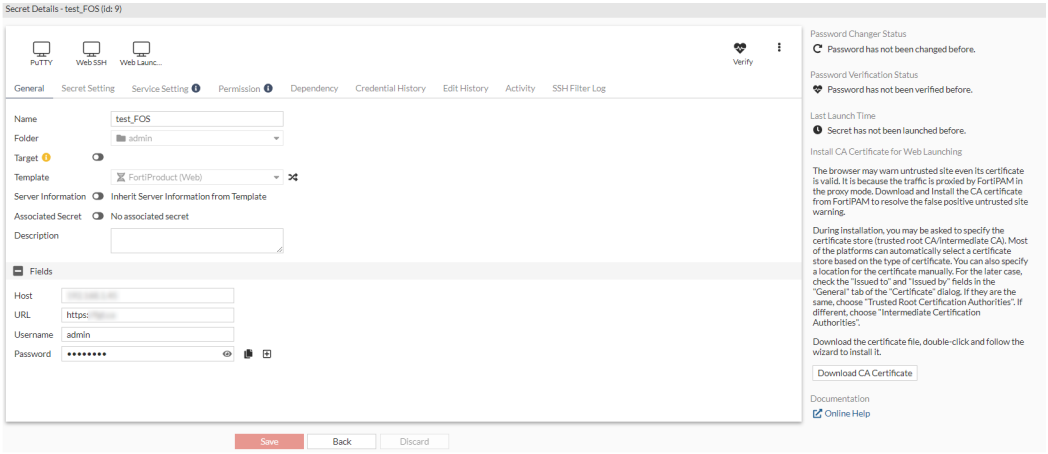
To configure a web FortiProduct secret:

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*.



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.

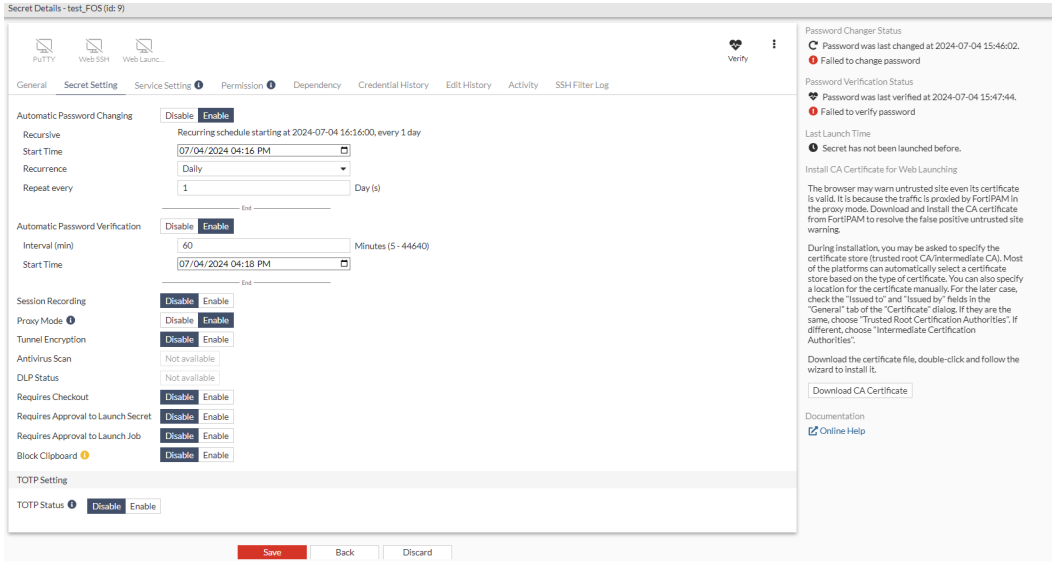


3. To change the password, from More options, select *Change Password*:
   The *Generate next password* dialog opens.
   a. In *Generate next password*, select *Randomly*.
   b. Click *OK*.
   c. Click *Save*.
4. To verify the password, select the *Verify* ( ) icon from the top-right.
   Once the password 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*.

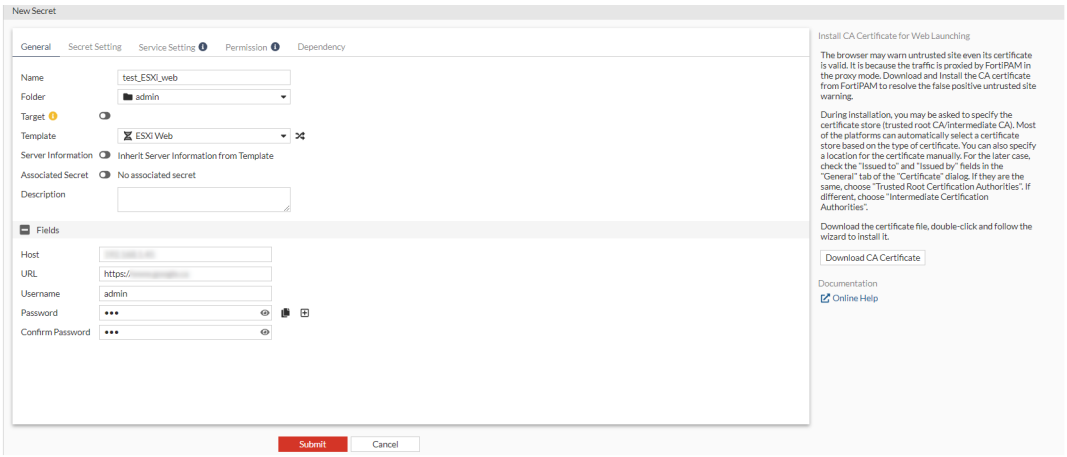


Configuring an ESXi web secret - Example

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*.



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 110.

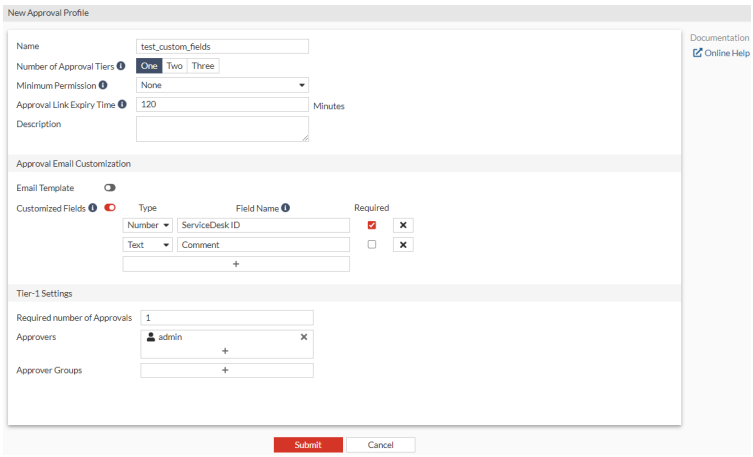
Configuring and accessing a secret that uses an approval profile with custom fields - Example

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*.



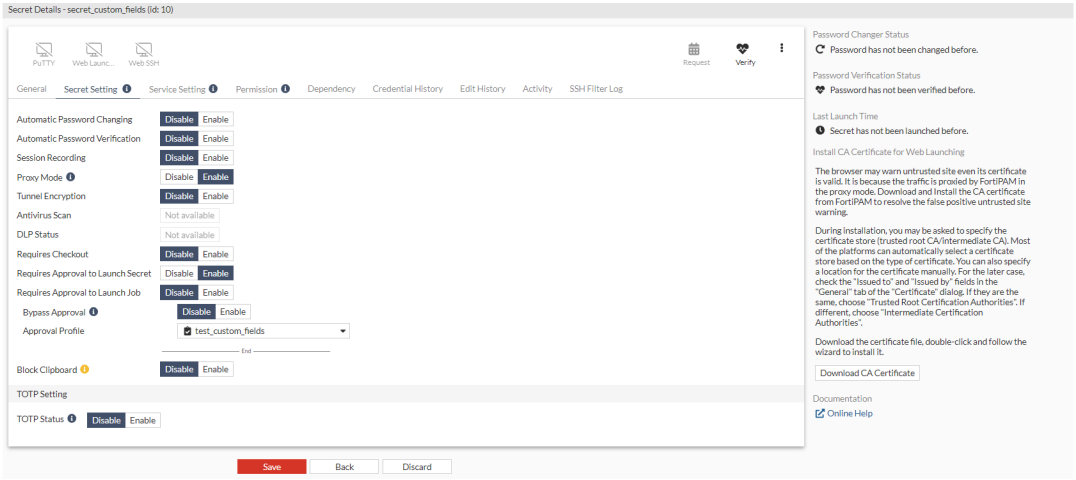
Alternatively, in the CLI console, enter the following commands to create a secret approval profile:

```
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*.



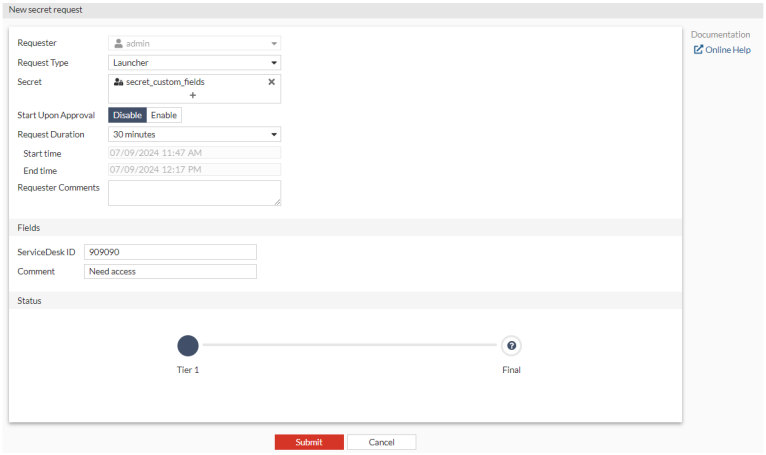
Alternatively, in the CLI console enter the following commands to apply the approval profile to a secret:

```
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.

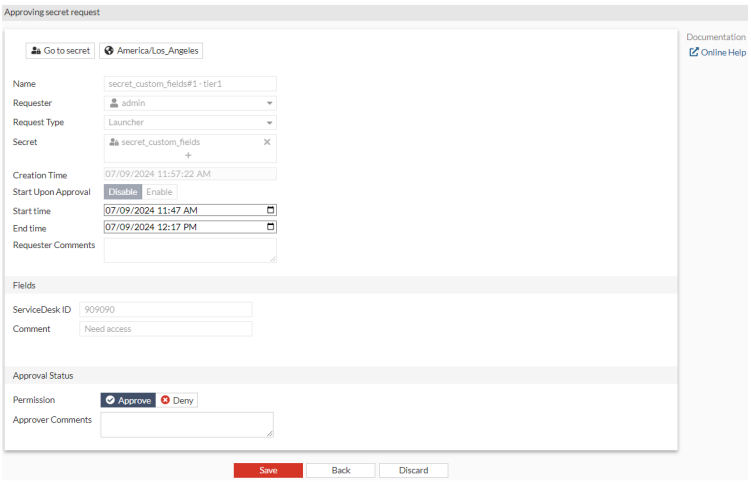
6. Click *Submit*.



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*.



Targets

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

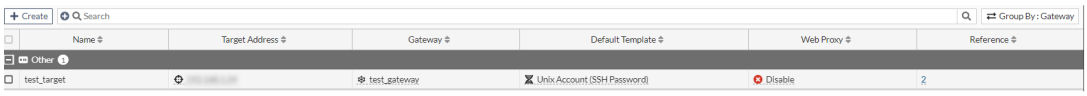
A target is a server/device with a privileged account supporting RDP, SSH, Web, or other admin protocols. Target systems include Windows workstation, Windows domain controller, Web server, Unix server, SQL- server, router, or firewall.

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.



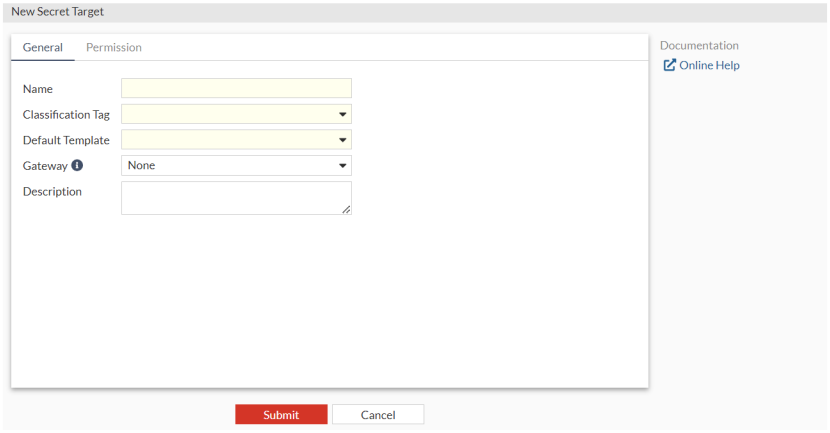
The *Targets* tab contains the following options:

+Create	Select to create a target. See Creating a target on page 117.
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.

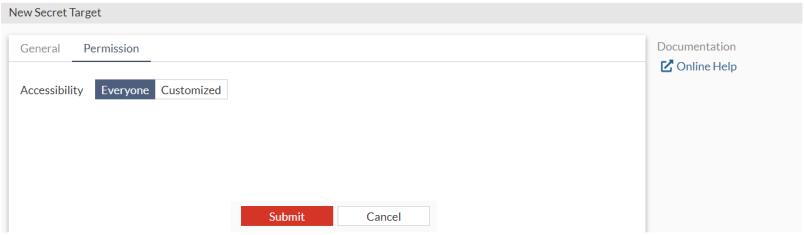
Creating a target

To create a secret target:

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

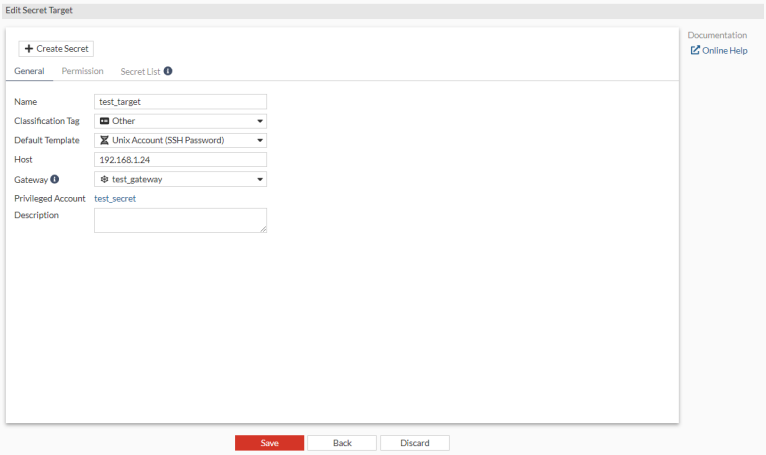


3. Select *Permission* from the top to switch to the *Permission* tab.



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 71. 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 123.
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 Secret gateway on page 384. 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. 
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.

When creating targets or secrets, it is recommended that you do not add an extra slash (/) to the end of the URL.

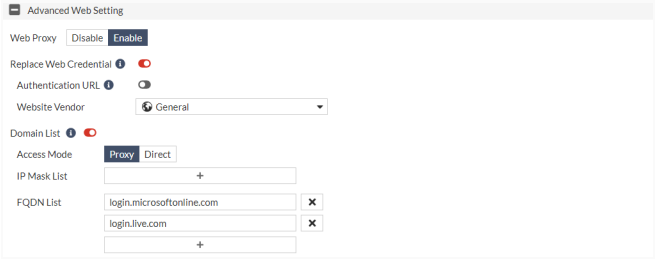
If the secret is launched and an error 404 is seen, add a slash to the end of the URL.

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.



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 368.

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 71. For more information on the web proxy feature, see Web proxy on page 125.
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

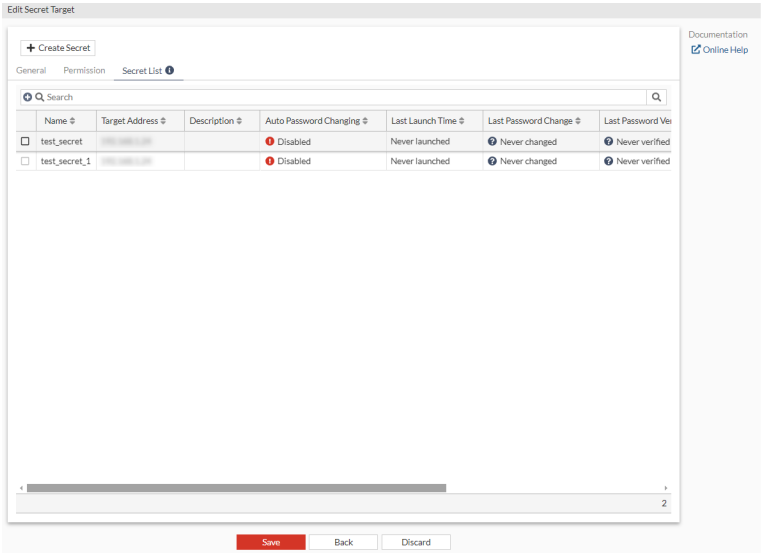
1. When creating a secret target, select *Customized* in *Accessibility*.
2. In the *Create Secret* dropdown, select user groups with the ability to see and use the target to create secrets.
3. In the *Owner* dropdown, select user groups with the highest possible permission level with the ability to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

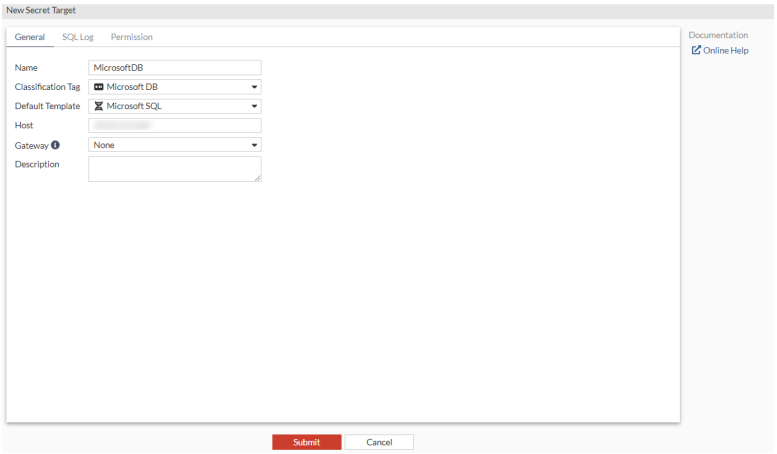
When editing a secret target, the *Secret List* tab displays all the associated secrets with the secret target.



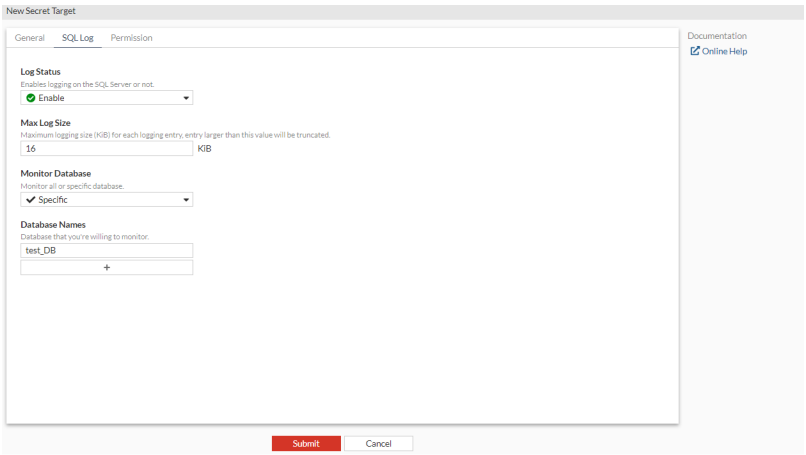
Microsoft SQL server Management Studio (SSMS) monitoring and logging

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.



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.

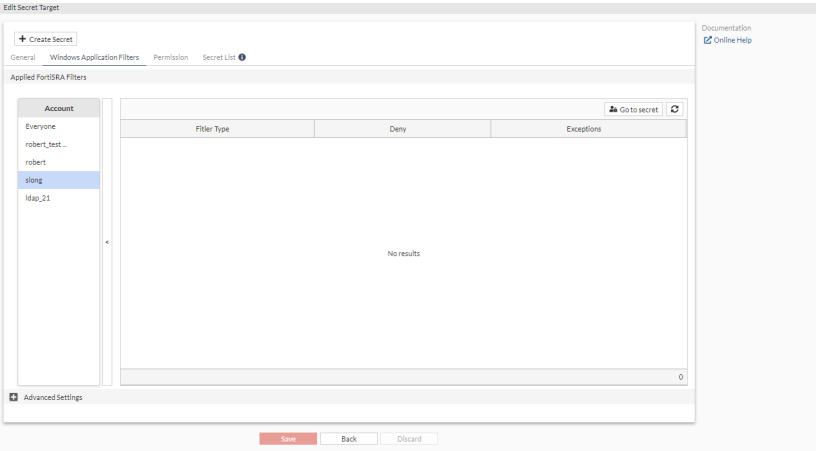


5. For the *Permission* tab, see User Permission on page 122 and Group Permission on page 122.
6. Click *Submit*.

Windows application filters

For information on Windows application filters, see Window app filter on page 250.

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
```

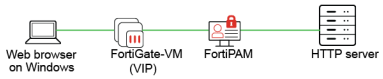
```
 next
end
```

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 368.

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 96.
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*.

Personal/public folder

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

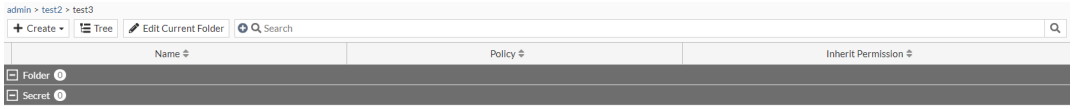
Before you create any secret, you should choose a folder where the secret is added.

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

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

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

The following shows a folder with secrets in it:



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

Create	From the dropdown, create a secret or a folder. See Creating a secret on page 71 and Creating a folder on page 131.
Tree	Select to open the folder tree. You can use this option to go to a folder. See Opening a folder on page 128.
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 131and Creating a secret on page 71.

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.

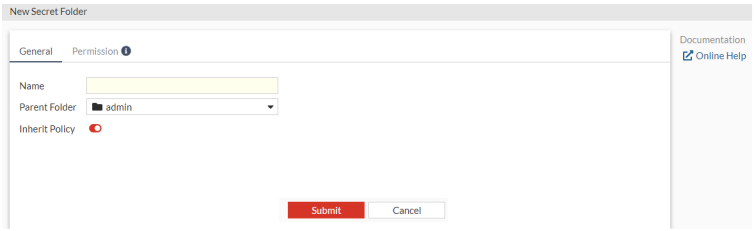
Creating a folder

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.



5. Enter the following information:

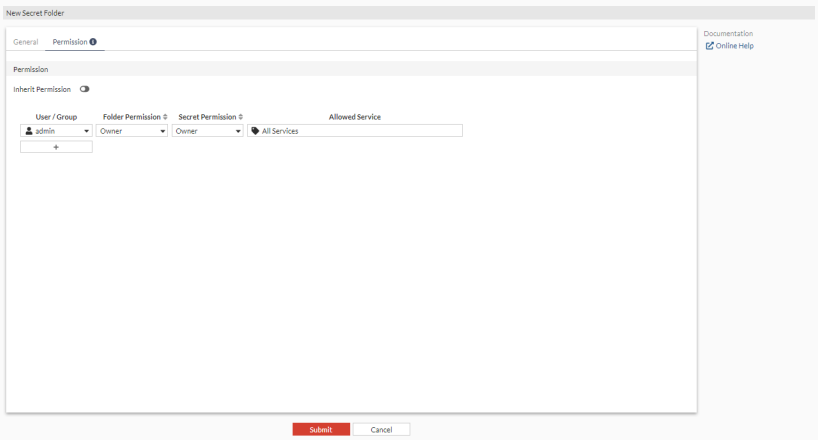
General	
Name	Name of the folder.
Parent Folder	From the dropdown, select a parent folder or select *Create* to create a new parent folder. The parent folder is set in step 2. The parent folder cannot be changed for a root folder. Use the search bar to look for a folder. Use the pen icon next to the 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 180.
	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.

	A public folder can only be shared to the ones listed in the parent folder permission table.



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 71.  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 134 and Group Permission on page 135.	

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 263, 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.

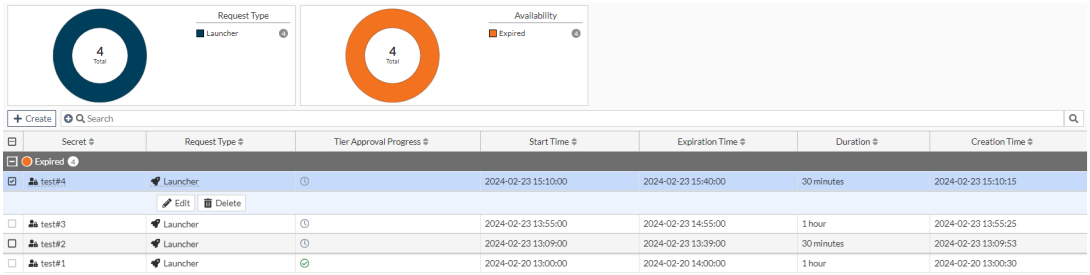
Go to *Secrets* > *My Request List* to see list of secret requests.

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*



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 137.
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.

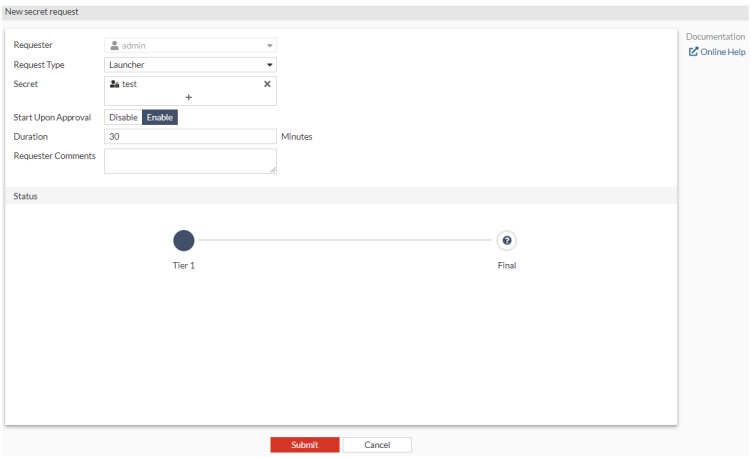
   If the secret does not show up, it may be because you do not have the necessary permission to access the secret or the folder where the secret is located.

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.

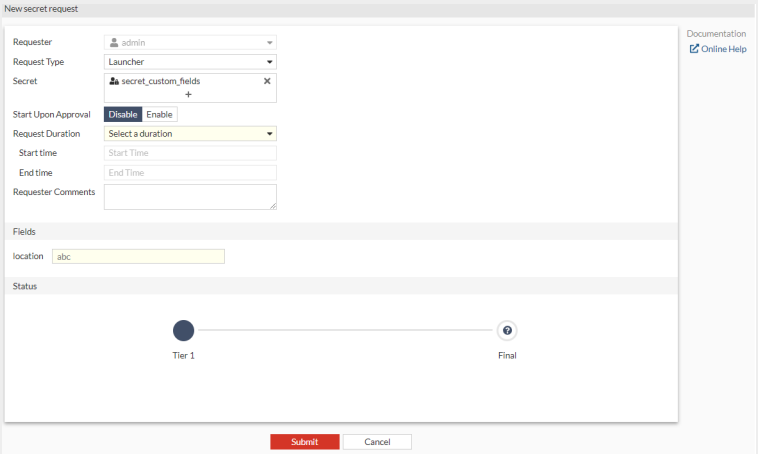
   See Creating a secret on page 71.

   The *New secret request* window opens.



4. Enter the following information:

Requester	The requester. **Note**: The option cannot be changed.
Request Type	Select from the following request types: • *Launcher* • *Job*
Secret	When the *Request Type* is *Launcher*, select + and select secrets from the *Select Entries* list. These are secrets with *Requires Approval to Launch Secret* enabled. See Creating a secret on page 71. 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. 
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 136 and Approval list on page 140.
   Reviewers specified in Approval profile on page 194 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.

Changing the FortiPAM URL to an FQDN in the approval email body- CLI

1. In the CLI console, enter the following command:
   The command changes the FortiPAM URL to the FQDN in the approval email body.

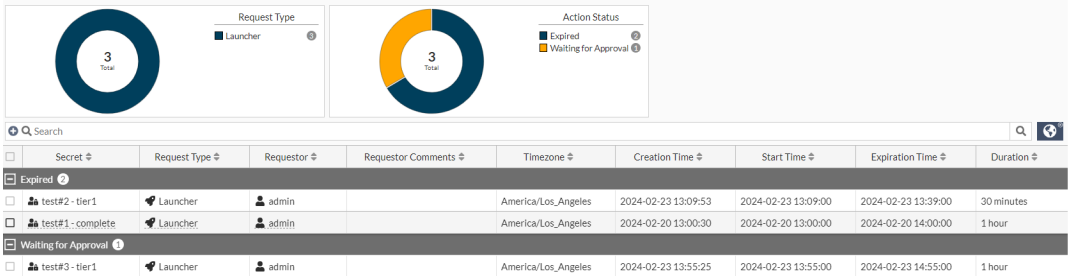
```
config secret setting
 set gui-fqdn-service fortipam.fortinet.com
end
```

The setting is only available via the CLI console.

Approval list

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

The *Approval List* tab looks like the following:



The widgets at the top display:

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

All requests stay in the list until they are deleted.

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*

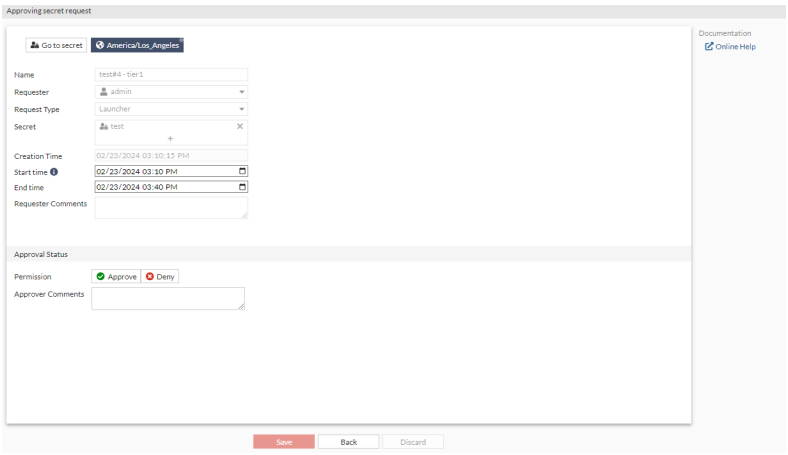
The *Approval List* tab contains the following options:

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 141.  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 143.
Deny	Select to deny the selected requests. See Reviewing multiple requests on page 143.

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.



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.

The *Revoke* button is only available in an approval tier with more than one approver.

In an approval tier with more than one approver, if not all the approvers approve a secret request, approvers who have already approved the request may revoke their approval.

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 136 tab.

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

To see the reviewer comments:

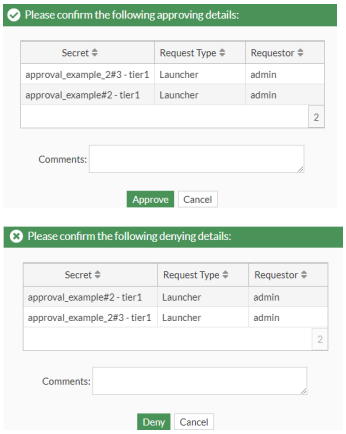
1. Go to *Secrets* > *My Request List*.
2. Double-click the denied request under *Denied/Expired*.
3. Select *View Approvers Comments* to see the reviewer comment.
   Alternatively, go to *Secrets* > *Approval List*, under *Denied/Expired Request*, double-click the request to see the reviewer comments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

Reviewing multiple requests

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

To review multiple requests:

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



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

Approver comments are visible to the requester.

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

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

Once a secret request is approved or denied, the request status appears in the *Approval List* tab and the status is updated in the My requests list on page 136 tab.

Job list

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

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

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

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



Jobs are not executed when FortiPAM is in maintenance mode.

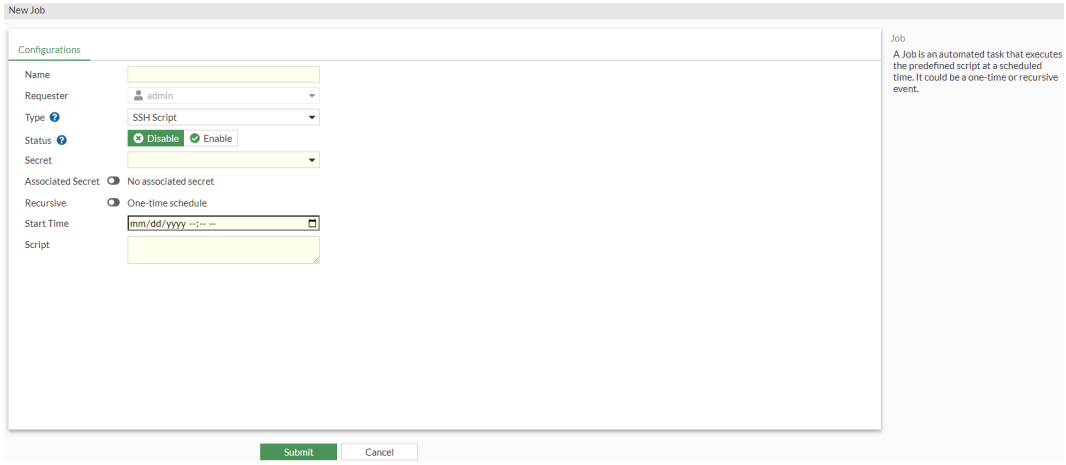
The *Job List* tab contains the following options:

+Create	Select to create a job. See Creating a job on page 144.
Edit	Select to edit the selected job.
Delete	Select to delete the selected jobs.
Search	Enter a search term in the search field, then hit `Enter` to search the jobs list. To narrow down your search, see Column filter.

Creating a job

To create a job:

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



3. Enter the following information:

Name	Name of the job.
Requester	From the dropdown, select a requester.
Type	From the dropdown, select from the following two options: • *SSH Script*: targeting secrets that work on linux-like machines (default). • *SSH Procedure*: targeting secrets that run on SSH server, e.g., FortiGate, Cisco, or Ubuntu.
Status	Enable/disable the execution of the job (default = disable).
Secret	From the dropdown, select a secret or create a new secret.  Use the search bar to look for a secret.  Use the pen icon next to a secret to edit it.
Associated Secret	Enable and then from the dropdown, select an associated secret or create a new secret. When enabled, changing password or verifying password requires credentials from the associated secret. **Note**: The option is disabled by default.  Use the search bar to look for a secret.

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

4. Click *Submit*.

When editing a job, select the *Make Request* option from the top to make a request to perform a job on the secret associated with the job. See Make a request on page 137.

When editing a job, select the *Log* tabs to see logs related to the job. See Log & report on page 323.

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.

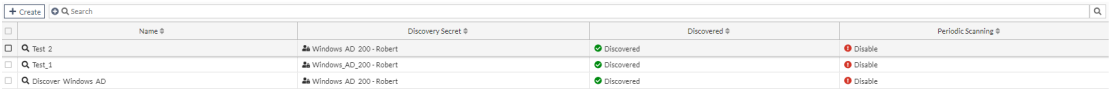
Users with the *Secret Discovery* permission for their role are able to see the *Discovery* tab in *Secrets*.

See Role on page 289.

Do not use the CLI console to configure discovery.

The following columns are available in the *Discovery* tab:

- *Name*
- *Discovery Secret*
- *Discovered*
- *Periodic Scanning*



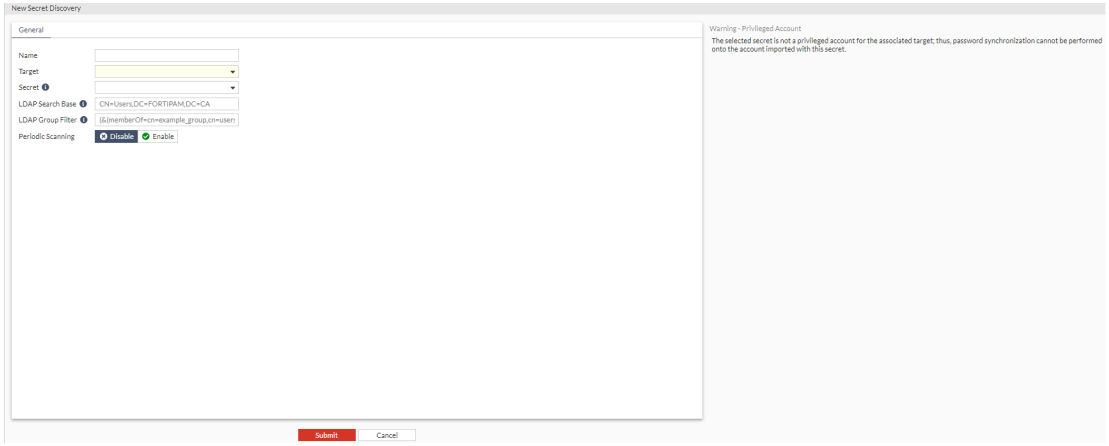
The *Discovery* tab contains the following options:

Create	Select to create a new discovery entry. See Creating discovery entry on page 148.
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.



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 117, 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 71, 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.

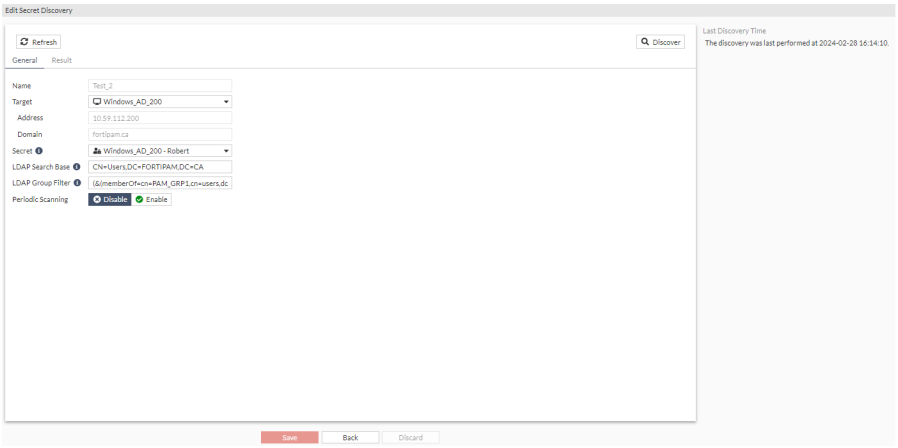
	Search base denotes the location in the directory where the search for a particular directory object begins, e.g., `CN = Users,DC=FORTINET,DC=COM`.
LDAP Group Filter	Enter the LDAP group filter.
	Standard LDAP filters to the LDAP search. Only the accounts that match the specified group filters are discovered, 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*.

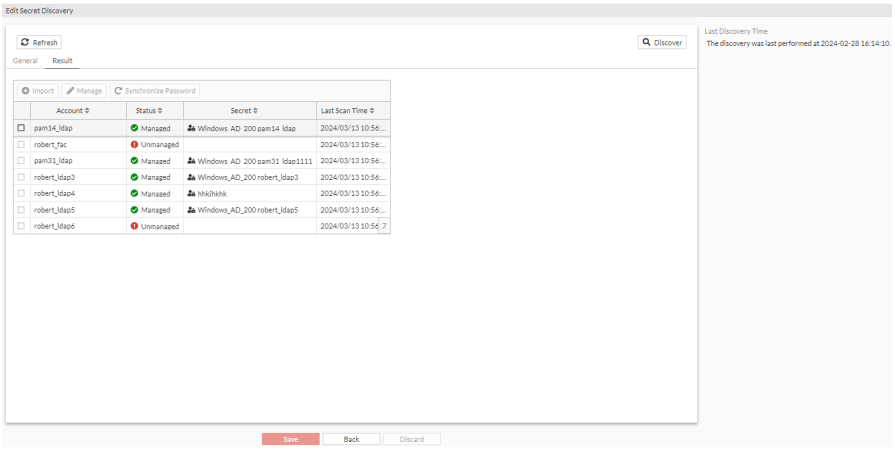
Manual discovery

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.



3. Form the right, click *Discover* to trigger a one-time discovery.
4. In the *Results* tab, you can see the discovered accounts.



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.



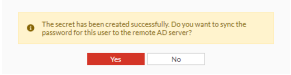
If an account is already managed by FortiPAM, you can see the corresponding secret in the *Secret* column.

Double-click a managed account to open the *Manage Account* window. Here, you can edit the secret.

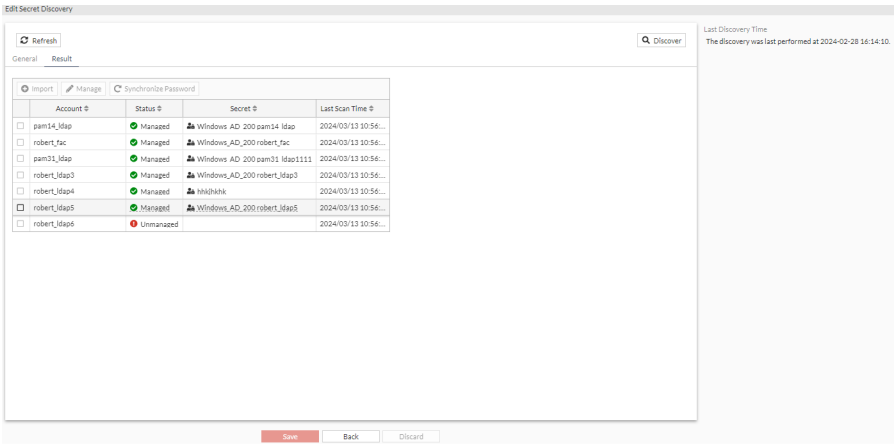


FortiPAM detects if it manages an account by looking for all the secrets that are currently using the discovery target.

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.



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.


Edit Secret Discovery
Refresh
Discover
General
Result
Import
Manage
Synchronize Password
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:...
Last Discovery Time
The discovery was last performed at 2024-02-28 16:14:10.
Save
Back
Discard

Secret settings

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

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

- Templates on page 153
- Launchers on page 167
- Policies on page 179
- Classification tags on page 185
- Addresses on page 186
- Dependency updater on page 189
- Approval profile on page 194
- Approval email template on page 198
- Password changers on page 211
- Password policies on page 225
- Character sets on page 228
- AntiVirus on page 229
- Data loss prevention (DLP) protection for secrets on page 232
- DLP file pattern on page 239
- SSH filter profiles on page 241
- Window app filter on page 250
- Event filter profile on page 247
- Integrity check on page 254

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 211.

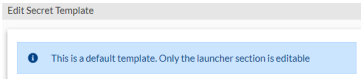
FortiPAM provides the following default templates:

AWS Web Account	A basic template for an AWS account.
Azure AD Account	A basic template designed to launch Azure AD portal as target.
Azure Credential	A basic template designed to save Azure AD enterprise application (client) ID, Directory (tenant) ID, and client secret value information.

VNC Server	A basic template designed for VNC password authentication.  In some cases, especially in a Unix-like environment, using a command line to start a VNC server often tells you its display is on :1. In this case, the VNC port `5901` connects to the VNC server. If this is applicable to you, change the launcher port from the default `5900` to `5901` in the *VNC Server* template or clone the default *VNC Server* template and then change the port number.
Certificate	A basic template designed to save certificate and its key.
Cisco Enable Secret	A basic template for a Cisco enabled secret account.
Cisco User (SSH Secret)	A basic template for a Cisco SSH account.
Cisco XR Router	A basic template for a Cisco server with XR IOS.
Database Server	A basic template for the SQL server using SQL username and password authentication.
ESXi Server	A basic template for the ESXi server using username and password.
ESXi Web	A basic template for an ESXi server using username and password with the web interface.
FortiProduct (SSH Key)	A basic template for a FortiProduct SSH Key account.
FortiProduct (SSH Password)	A basic template for a FortiProduct SSH Password account
FortiProduct (Web)	A basic template for web based products, e.g., FortiGate and FortiProxy.
HeidiSQL	A basic template for the SQL GUI launcher.
Machine	A basic template for a general machine, with all default launchers.
Microsoft SQL	A basic template for a Microsoft SQL database server account.
MySQL	A basic template for a MySQL database server account.
PostgreSQL	A basic template for a PostgreSQL database server 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.
Unix Account (SSH Key)	A basic template for a Unix SSH Key account.
Unix Account (SSH Password)	A basic template for a Unix SSH Password account.
Unix Account (Web CIFS)	A basic template for accessing a Unix system with SMB/CIFS service.
Unix OpenLDAP Account	A basic template for an Open LDAP account.
Web Account	A basic template for a Web account.
Windows Domain Account	A basic template for a Windows Domain account.
Windows Domain Account (Samba)	A basic template for a Samba Windows Domain account.
macOS	A basic template for a macOS machine.
Windows Machine	A basics template for a Windows machine.

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



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

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

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



The secret templates list contains the following options:

Create	Select to create a new template. See Creating secret templates on page 157.
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.

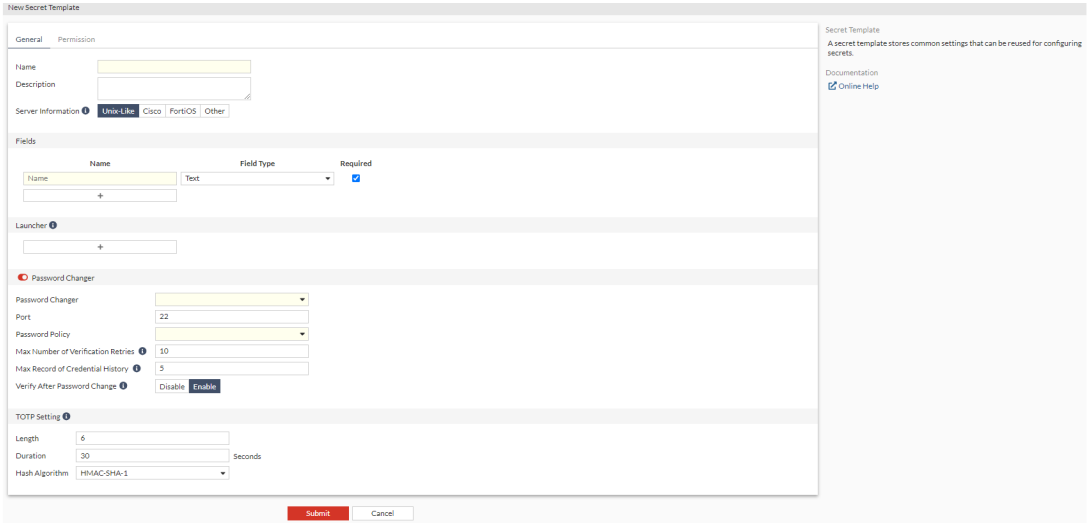
- Example

```
config secret template
 edit Windows Domain Account
  set server-info Windows
end
```

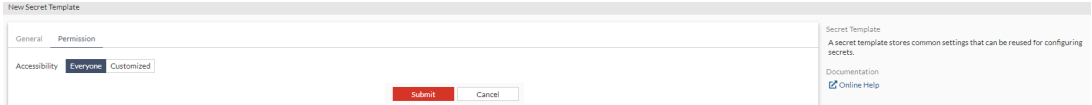
Creating secret templates

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.



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



4. Enter the following information:

General	
Name	Name of the template.
Description	Optionally, enter a description.
Server Information	The general type of server to which the template is intended to connect: • *Unix-Like* • *Cisco* • *FortiOS* • *Other*
Fields	Secrets require fields to enter the secret related information. To add new fields, select + 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. • *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.
Required	Enable to make this field required or disable if this field will be optional. **Note**: By default, all fields are marked as required.
	From the list, click *x* next to a field entry to delete it.
Launcher	Launcher helps you access a target server. See Launchers on page 167. 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 164.

Launcher	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*:

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 254.  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 254.  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 213.  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 226.  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 71.

See Limitations of TOTP on FortiPAM on page 164.

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 157, 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 157, 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.

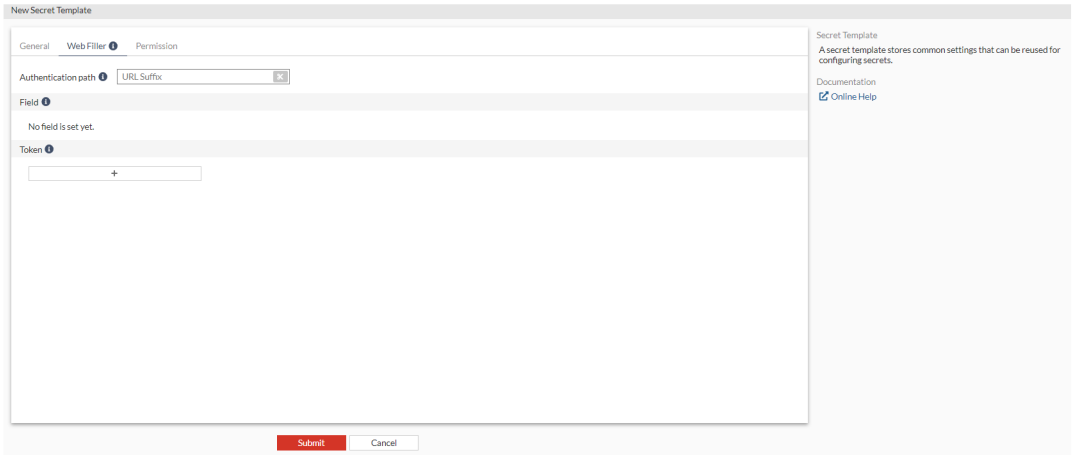


The feature needs Microsoft Edge and Google Chrome extension V3.

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.



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.

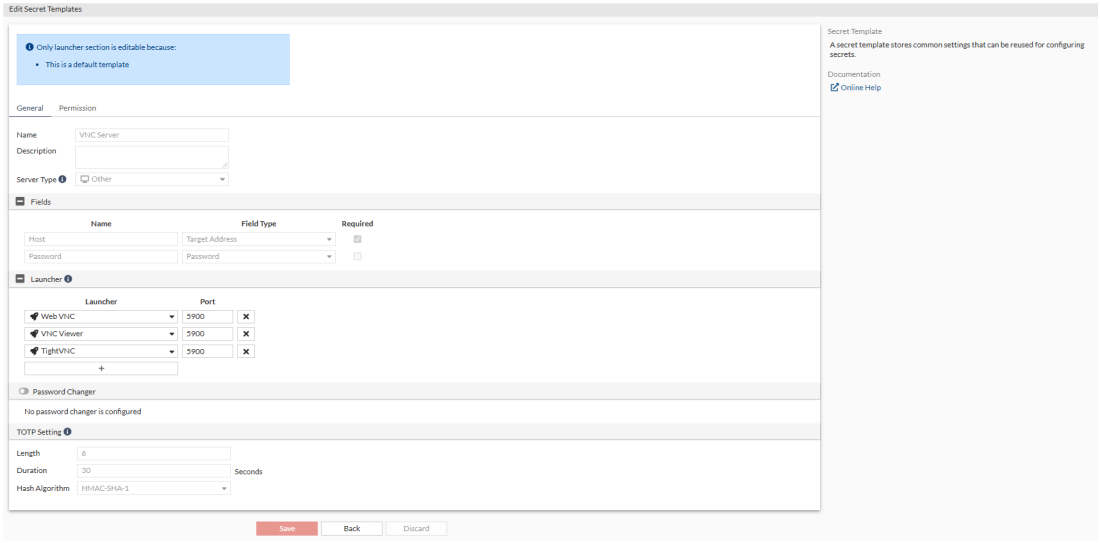
Setting up VNC connections - Example

For VNC connections, there are two methods:

- Non-VNC password authentication
- VNC password authentication

On FortiPAM versions before 1.5.0, we typically use the *Machine* template for the VNC launcher. However, the *Machine* template only works for non-VNC password authentication and does not support VNC password authentication required when connecting to a remote target that needs a VNC password.

The default *VNC Server* template supports VNC password authentication.



The *VNC Server* template only requires the following two fields:

- *Host*: The IP address/FQDN for the VM you are accessing.
- *Password*: The VNC password.

Using the *VNC Server* template to create and launch a secret:

1. Go to *Secrets* > *Secrets*.
2. In the Secrets List, select *Create*.
   The *Create New Secret in:* dialog appears.
3. Select the folder where you intend to add the secret.
4. Select *Create*.
   The *New Secret* window opens.
5. Enter the secret name.
6. In *To connect to a remote server*:
   a. In *Target*, select a target.
   b. From the *Templates* dropdown, select *VNC Server*.
7. In *Fields*:
   a. Fill in the required fields.
8. Click *Submit*.
9. From the Secrets List, double-click the recently created secret.
10. From the top, select a launcher to launch the secret.
    FortiPAM delivers the VNC password automatically. The user must enter the account username and password manually.

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.



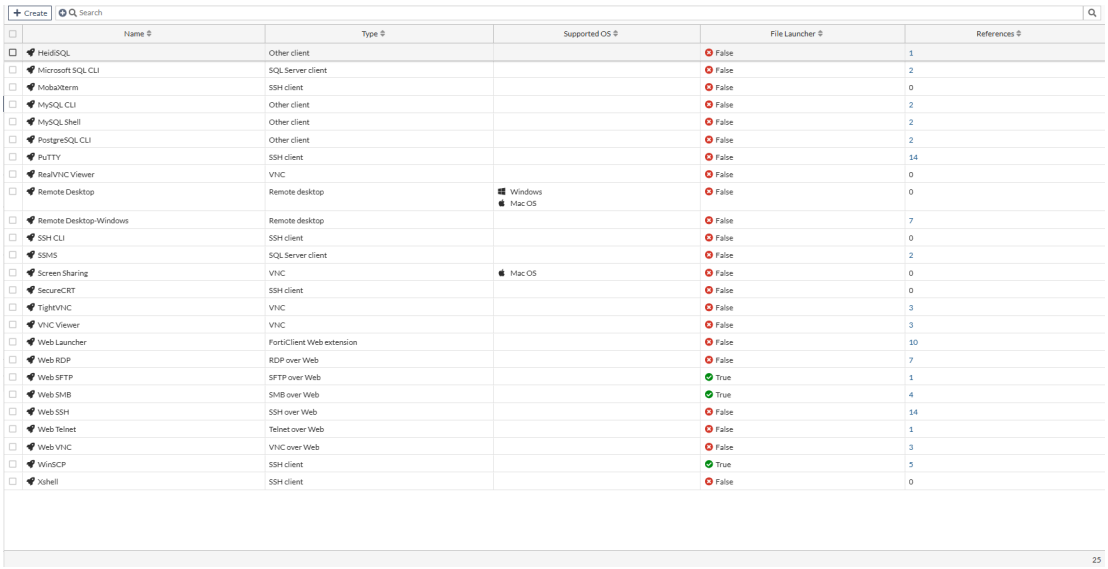
In proxy mode, browsing triggers ZTNA tunnel between the FortiClient and FortiPAM server.

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	Supported OS	File Launcher	References
HeidiSQL	Other client		False	1
Microsoft SQL CLI	SQL Server client		False	2
MobaXterm	SSH client		False	0
MySQL CLI	Other client		False	2
MySQL Shell	Other client		False	2
PostgreSQL CLI	Other client		False	2
PuTTY	SSH client		False	14
RealVNC Viewer	VNC		False	0
Remote Desktop	Remote desktop	Windows, Mac OS	False	0
Remote Desktop-Windows	Remote desktop		False	7
SSH CLI	SSH client		False	0
SSMS	SQL Server client		False	2
Screen Sharing	VNC	Mac OS	False	0
SecureCRT	SSH client		False	0
TightVNC	VNC		False	3
VNC Viewer	VNC		False	3
Web Launcher	FortiClient Web extension		False	10
Web RDP	RDP over Web		False	7
Web SFTP	SFTP over Web		True	1
Web SMB	SMB over Web		True	4
Web SSH	SSH over Web		False	14
Web Telnet	Telnet over Web		False	1
Web VNC	VNC over Web		False	3
WinSCP	SSH client		True	5
Xshell	SSH client		False	0

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.
- *RealVNC Viewer*: The secret launcher is designed to connect to a RealVNC server.

  A RealVNC server supports the following two authentication methods:
  - Standard VNC password with 8 digits/characters
  - Windows username/password
- *Remote Desktop*: A basic RDP client using remote desktop on Windows and macOS.
- *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.



In the CLI console, use the following commands to update the SSMS launcher:

```
config secret target
   edit <SQL server>
      set sql-server-log-status enable
      config sql-log
         set log-all enable
         set log-rpc-parameters enable
      end
   next
end
```

- *Screen Sharing*: For macOS.
- *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.



If connecting to a RealVNC server, use the *RealVNC Viewer* launcher instead of *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 131 and Creating a secret on page 71.

- *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.

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 172Creating a launcher on page 172.
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.

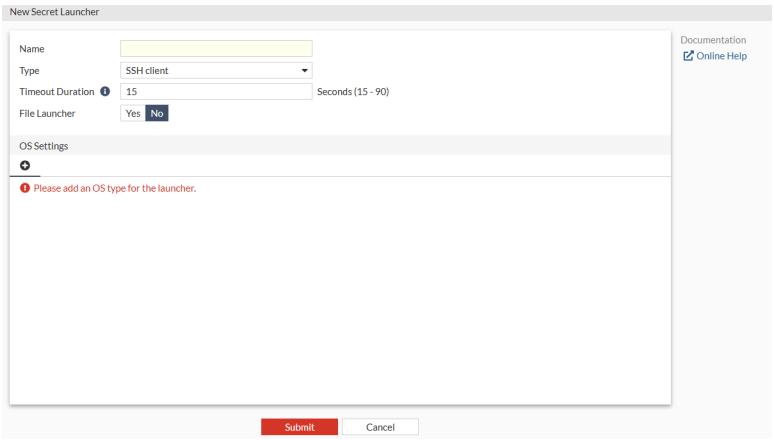
Once you have verified that these applications work correctly on your endpoint, you can seamlessly integrate them with FortiPAM for enhanced access control and security.

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: • *Remote desktop*: RDP client launcher type. • *SSH client*: SSH client launcher type (default). • *VNC*: VNC client launcher type. • *SQL Server client*: SQL server launcher type. • *Other client*: Other client launcher type.
Timeout Duration	The maximum duration to start the launcher before the timeout, in seconds (default = 15, 15 - 90)
File Launcher	Use as a file launcher (default = *No*).
OS Settings Select + and select the OS type: • *Windows* • *Mac OS* • *Custom* For OS types including the macOS, the new FortiClient is needed to support native launchers. When you add a new OS to a launcher, ensure that the FortiClient in the OS supports FortiPAM, e.g., for FortiClient 7.4.1, only Windows FortiClient supports FortiPAM.	
Name	An alias for the launcher.
Application Integrity Check	The executable to be compared against before launching. From the dropdown: • Select *Disabled* (default) if the launcher does not require validation. • Select a client software entry. See Integrity check on page 254.
	Use the search bar to look up a client software entry.

	Note: The option is disabled by default.
User Agent Name	The regular expression pattern for the user agent. **Note**: The field is only available when the OS type is *Custom*.

Executable Location/Application Name	The program file name, e.g., `putty.exe` for an SSH client. It can also be the absolute path to the executable.
	  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.
	Note:
	• The option is named *Executable Location* when the OS type is either *Windows* or *Custom*.
	• The option is named *Application Name* when the OS type is *Mac OS*.

Parameter	The command line parameters to execute to initialize the launch process. 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"
```

Initialization Commands	The set of commands to execute when the launch process is initialized. See Creating a new launcher command on page 176.
Clean Commands	The set of commands to execute when the launch process is terminating. See Creating a new launcher command on page 176.

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 4 when Creating a secret launcher, having selected an OS type, select + in *Initial Commands* or *Clean Commands*.
2. In *Command*, enter the command.



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



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 type rdp
  config os_app
   edit 1
    set exe "mstsc.exe"
    set parameter "/V:$HOST:$PORT /noConsentPrompt"
    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
 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 157 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 157 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 157 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.

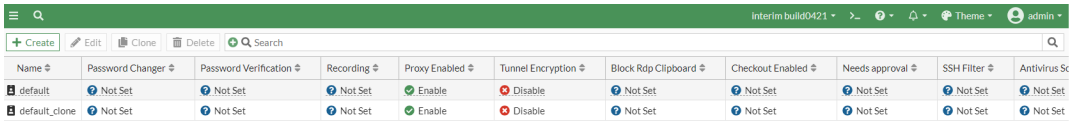
Policies in *Secret Settings* displays a list of secret policies.

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:



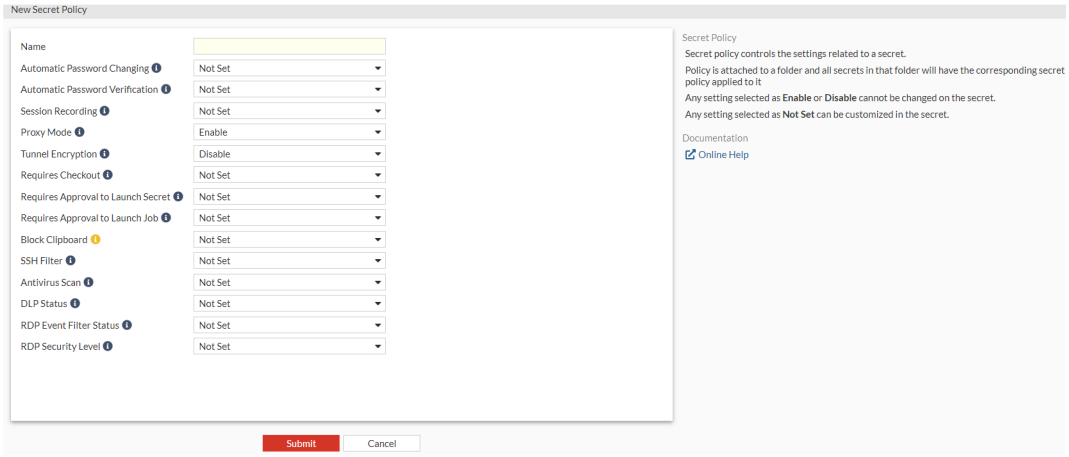
The *Policies* list contains the following options:

Create	Select to create a policy. See Creating a policy on page 180.
Edit	Select to edit the selected policy.
Clone	Select to clone the selected policy.
Delete	Select to delete the selected policies. The default secret policy cannot be deleted.
Search	Enter a search term in the search field, then hit `Enter` to search the policies list. To narrow down your search, see Column filter.

Creating a policy

To create a policy:

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



3. Enter the following information:

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

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

	When disabled, the non-proxy (direct) mode is used. See Modes of operation on page 34.
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 101.
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 137 and Approval flow on page 194.
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 137 and Approval flow on page 194.
Approval Profile	From the dropdown, select an approval profile, or select *Create* to create a new approval profile. See Approval profile on page 194.  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 229.

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 185.

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 180.



Use the search bar to look up a policy.



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

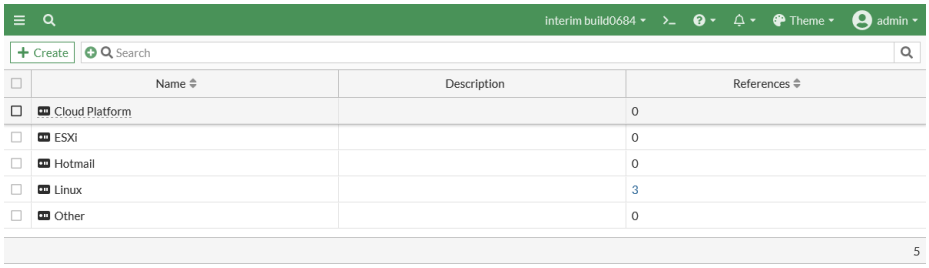
6. Click *Save/Submit*.

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 117.

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.



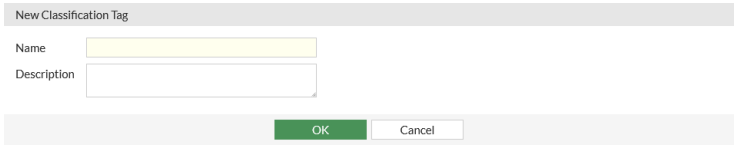
The *Classification Tag* tab contains the following options:

+Create	Select to create a classification tag. See Creating a classification tag on page 186.
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*.

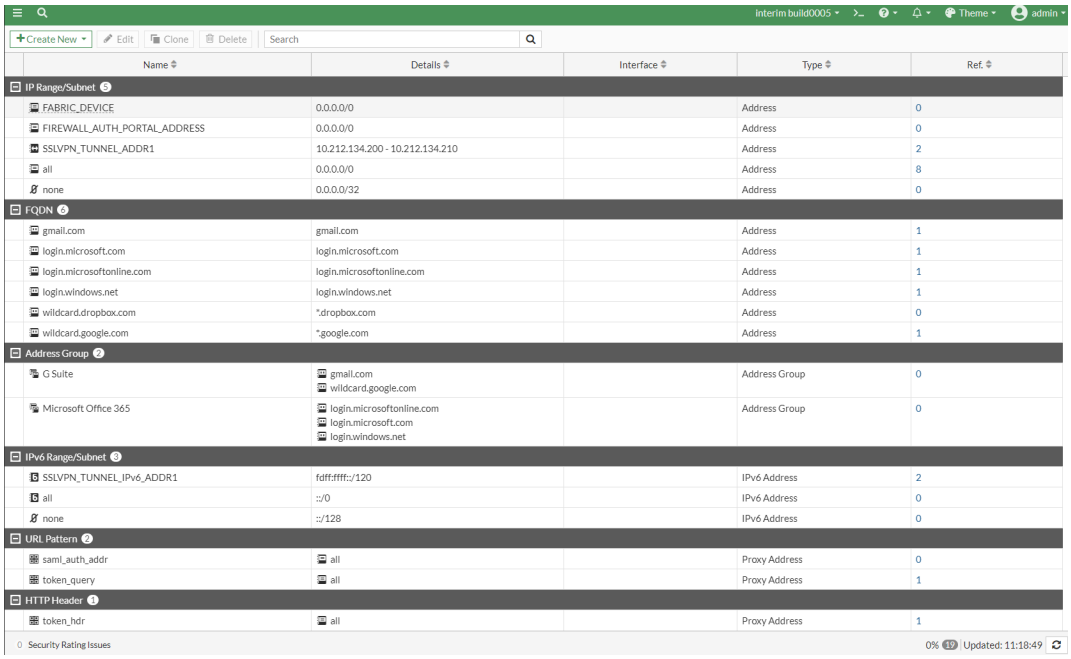
Addresses

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

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

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

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



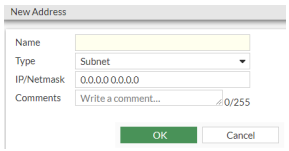
The *Addresses* tab contains the following options:

+Create New	From the dropdown, select *Address* or *Address Group* to create an address or an address group. See Creating an address on page 187 and Creating an address group on page 188
Edit	Select to edit the selected address or address group.
Clone	Select to clone the selected address or address group.
Delete	Select to delete the selected addresses or address groups.
Search	Enter a search term in the search field, then hit `Enter` to search the list. To narrow down your search, see Column filter.
Refresh	To refresh the contents, click the refresh icon on the bottom-right.

Creating an address

To create an address:

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



3. Enter the following information:

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

4. Click *OK*.

Creating an address using the CLI - example

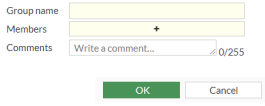
1. Enter the following commands in the CLI console:

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

Creating an address group

To create an address group:

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



3. Enter the following information:

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

4. Click *OK*.

Creating an address group using the CLI - example

1. Enter the following commands in the CLI console:

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

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

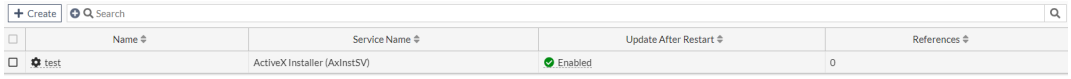
If a service running on a machine relies on a credential managed by FortiPAM, the dependency updater feature offers the ability to update the service credential immediately after FortiPAM changes the credential. FortiPAM ensures that the service does not fail during authentication.

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*



The *Dependency Updater* tab contains the following options:

Create	Select to create a new dependency updater. See Creating a dependency updater on page 190.
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.

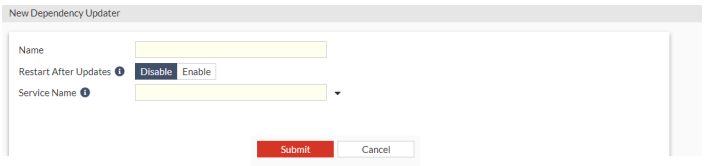
For updating the Windows server, WinRM service must be configured on the target machine, and there must be a privileged account for the target machine in FortiPAM.

See Updating a service account credential Example on page 192.

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.

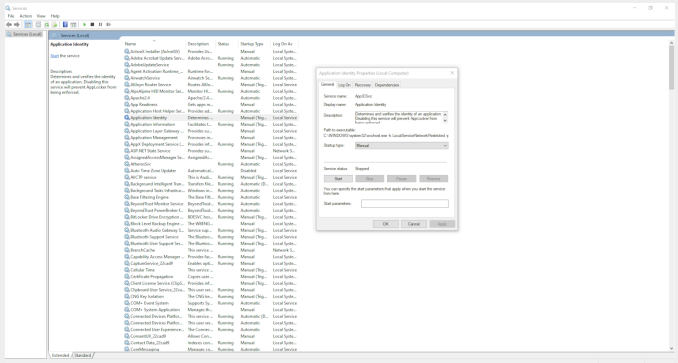


3. Enter the following information:

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
```

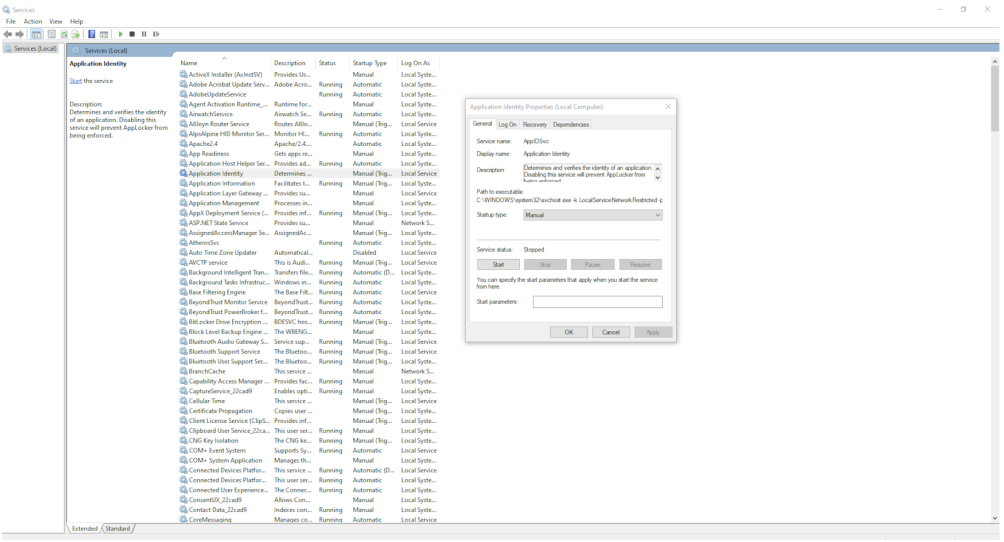
Updating a service account credential - Example

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*.

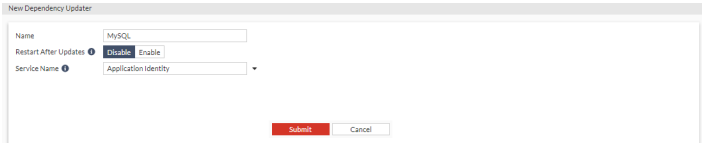
On Windows, the Service *Display name* is different from the *Service name*.

For example, in *Services* on Windows, when you double-click *Application Identity*, you see that the *Service name* is *AppIDSvc*.



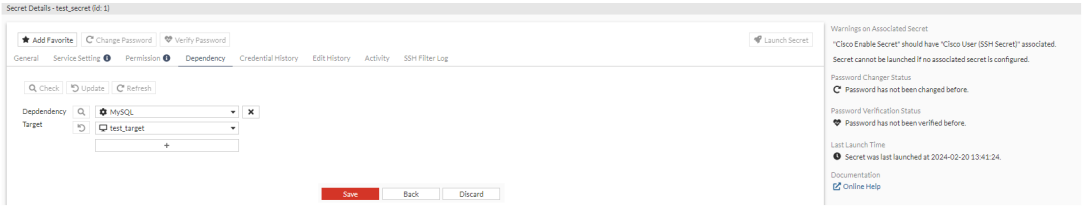
---

6. Click *Submit*.



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.

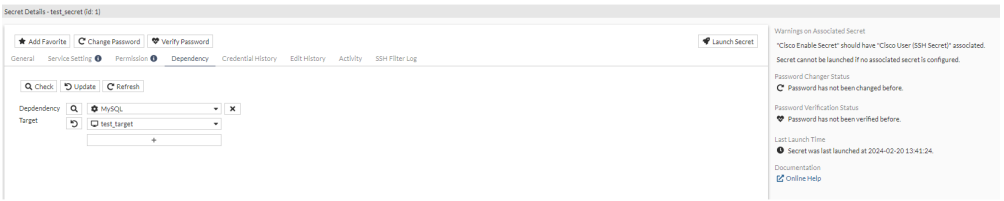
13. Click *Save*.



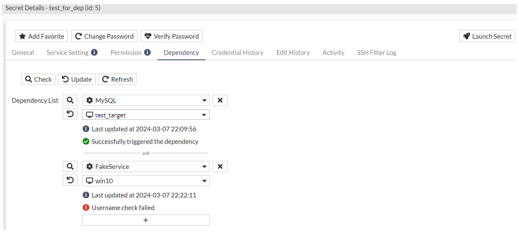
Once the secret password changer successfully rotates the secret password, all the dependencies in the secret are automatically updated.

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.



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.



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 195.

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.

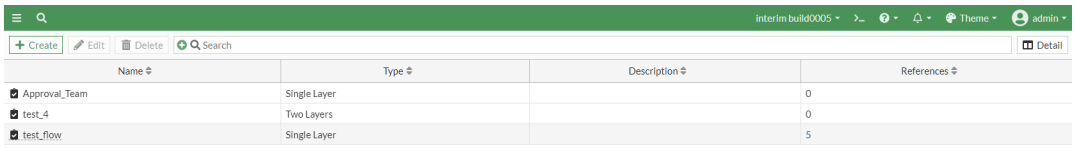
See Approval profile on page 194.

Approval profile

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

For every approval profile, the following fields are shown:

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



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

The *Approval Profile* tab contains the following information:

Create	Select to create a new approval profile. See Create an approval profile on page 195.
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

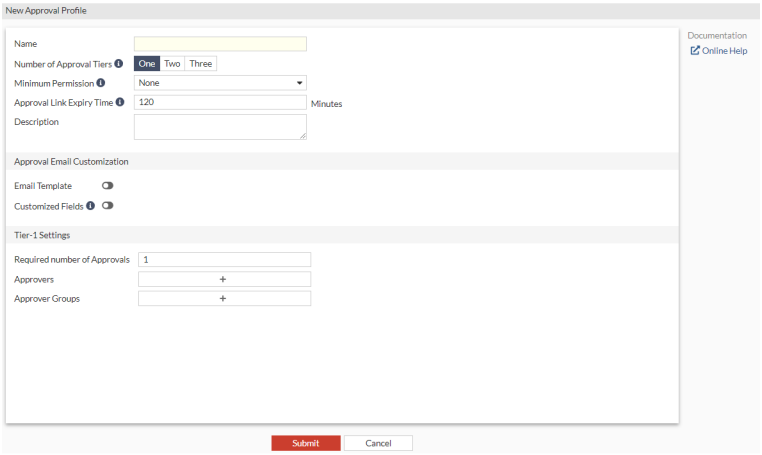
To enable approval profile:

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 195.
5. Click *Save*.

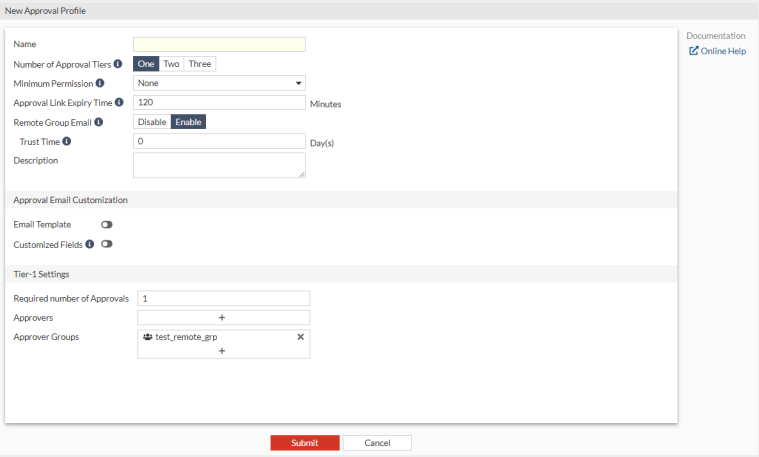
Create an approval profile

To create an approval request:

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



3. Enter the following information:

Name	The name of the approval profile.
Number of Approval Tiers	The number of approval tiers a secret request is processed through: • *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* (seeCreating a secret on page 71) 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*. 

	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 198.  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 263, 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.

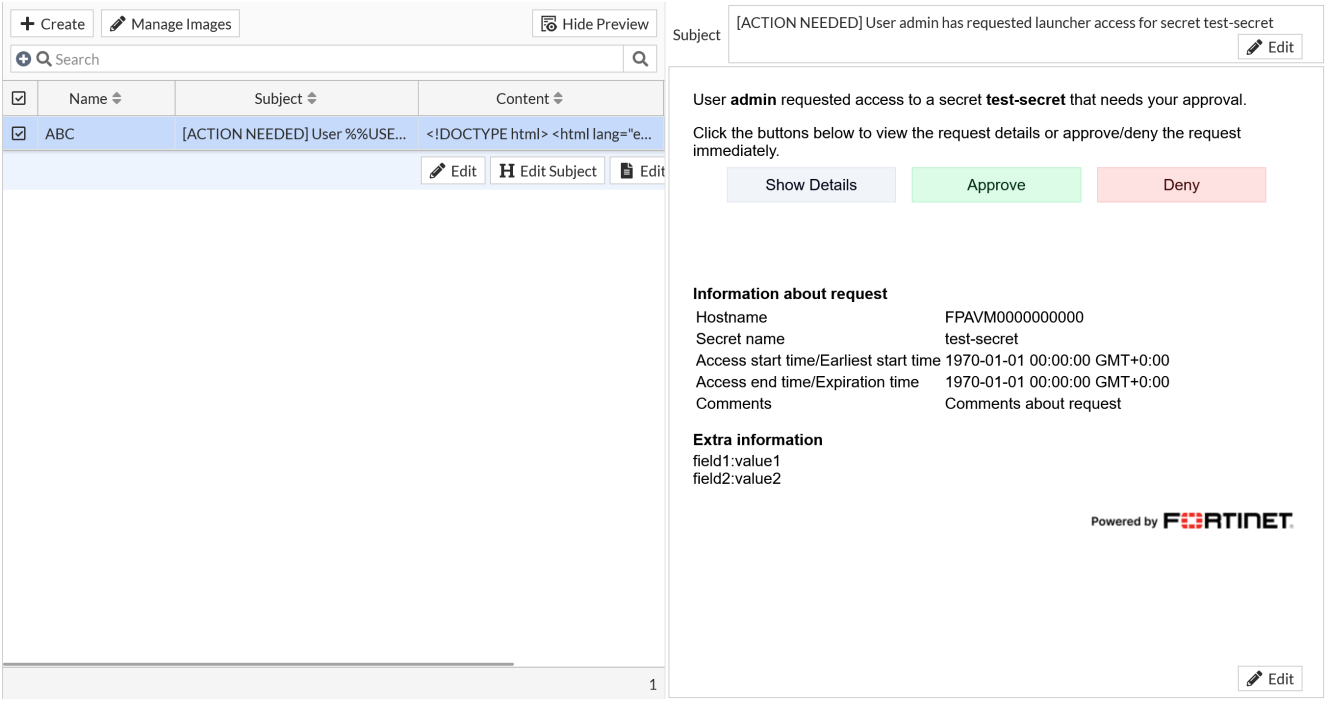
You can create a custom email template for the secret approval request email sent to the approvers.

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.



Approval email template list contains the following options:

Create	Select to create an approval email template. See Creating an approval email template on page 200.
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 438.
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.

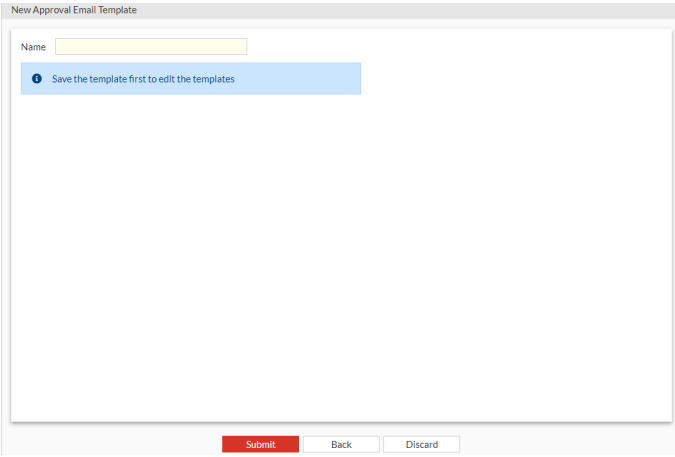
Edit Subject	Select to edit the subject of the selected approval email template.
Edit Content	Select to edit the content of the selected approval email template.
Delete	Select to delete the selected approval email template.

To create an approval email template using the CLI console, see Creating an approval email template using the CLI on page 204.

Creating an approval email template

To create an approval email template:

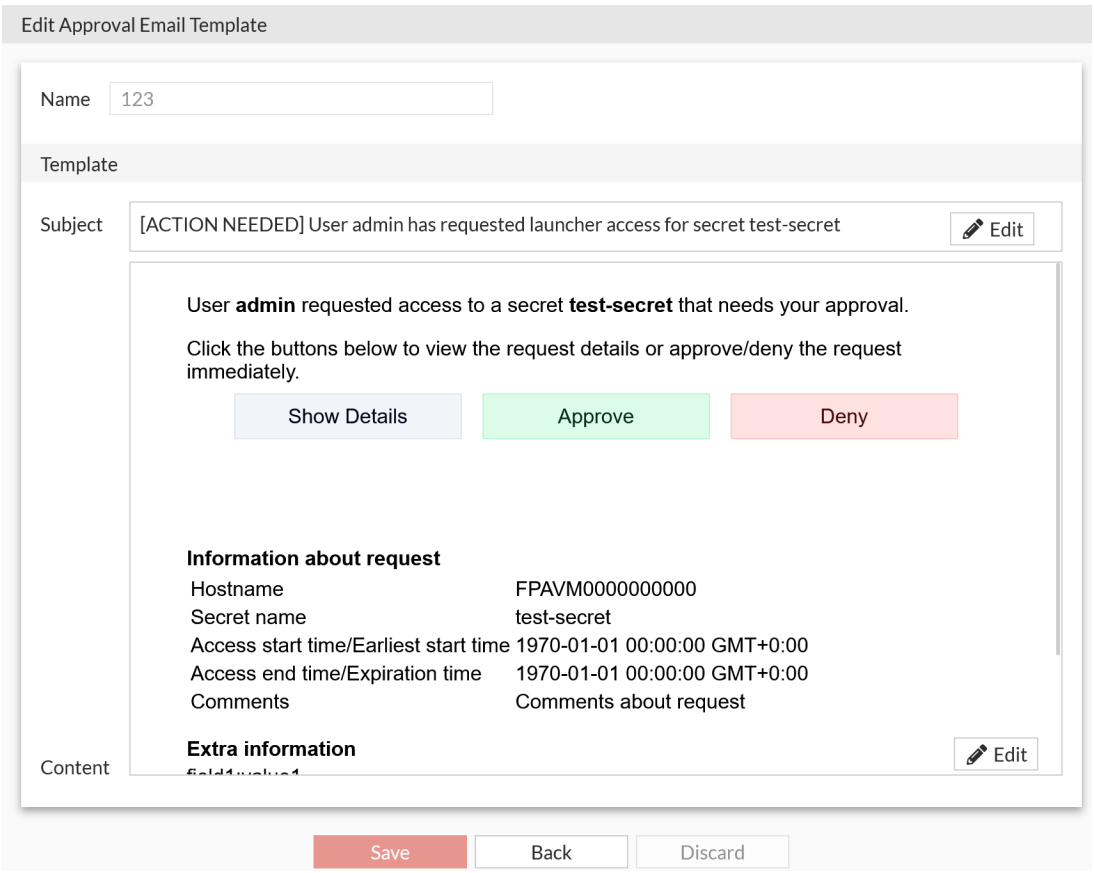
1. Go to *Secret Settings* > *Approval Email Template*.
2. Select *Create*.
   The *New Approval Email Template* window opens.



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.

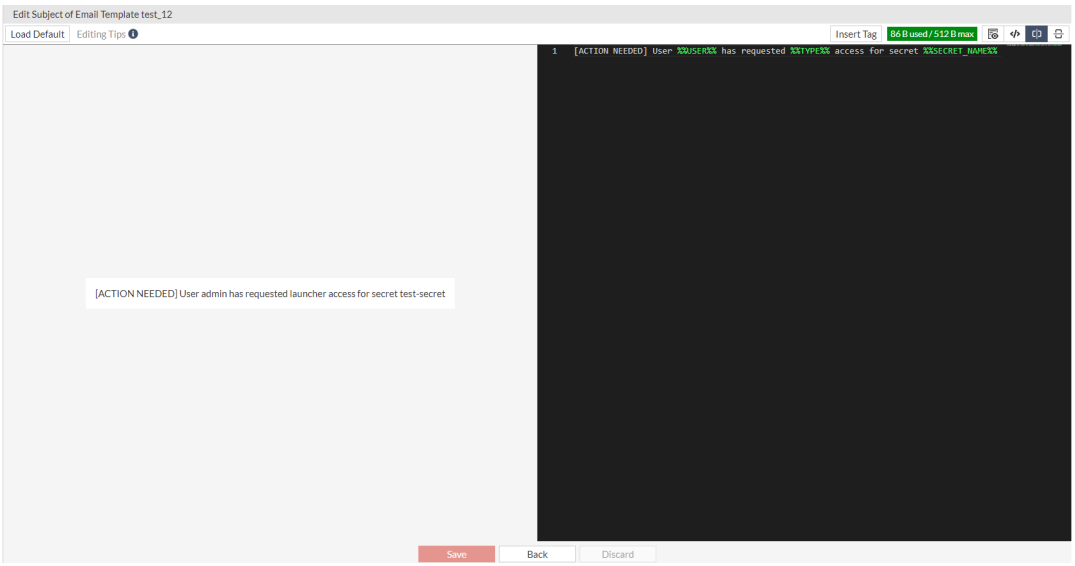
The *Edit Approval Email Template* window opens.



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.



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.

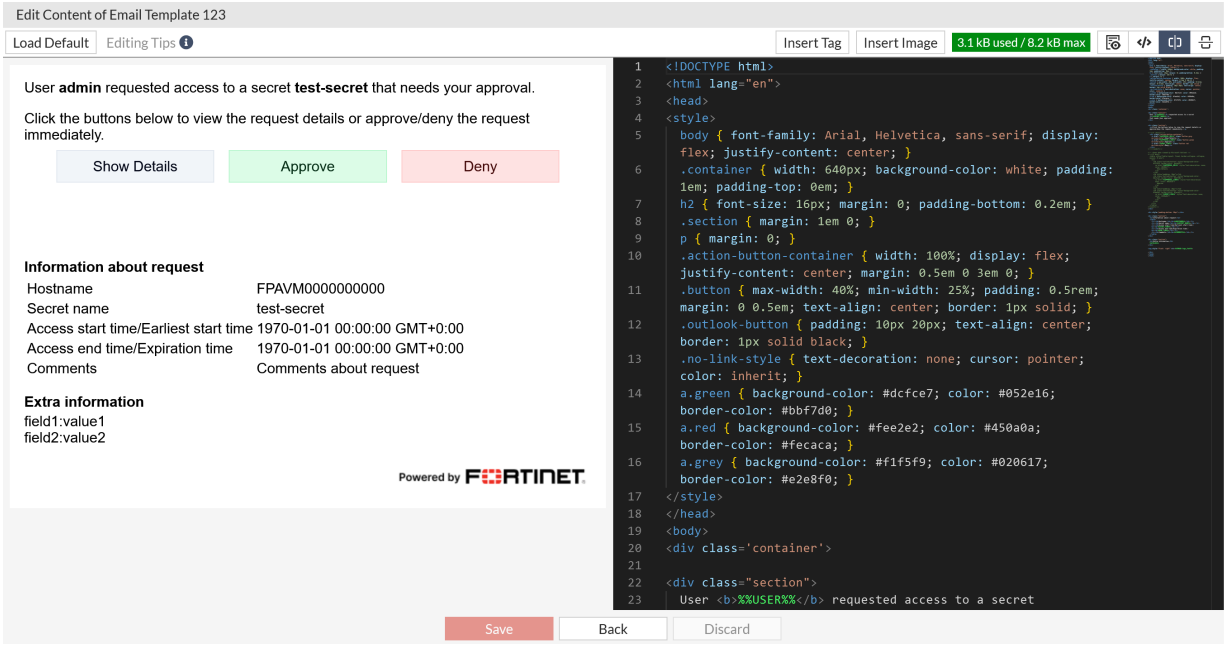
c. **To insert a tag:**

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.



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 195.

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.

Approving secrets by Email

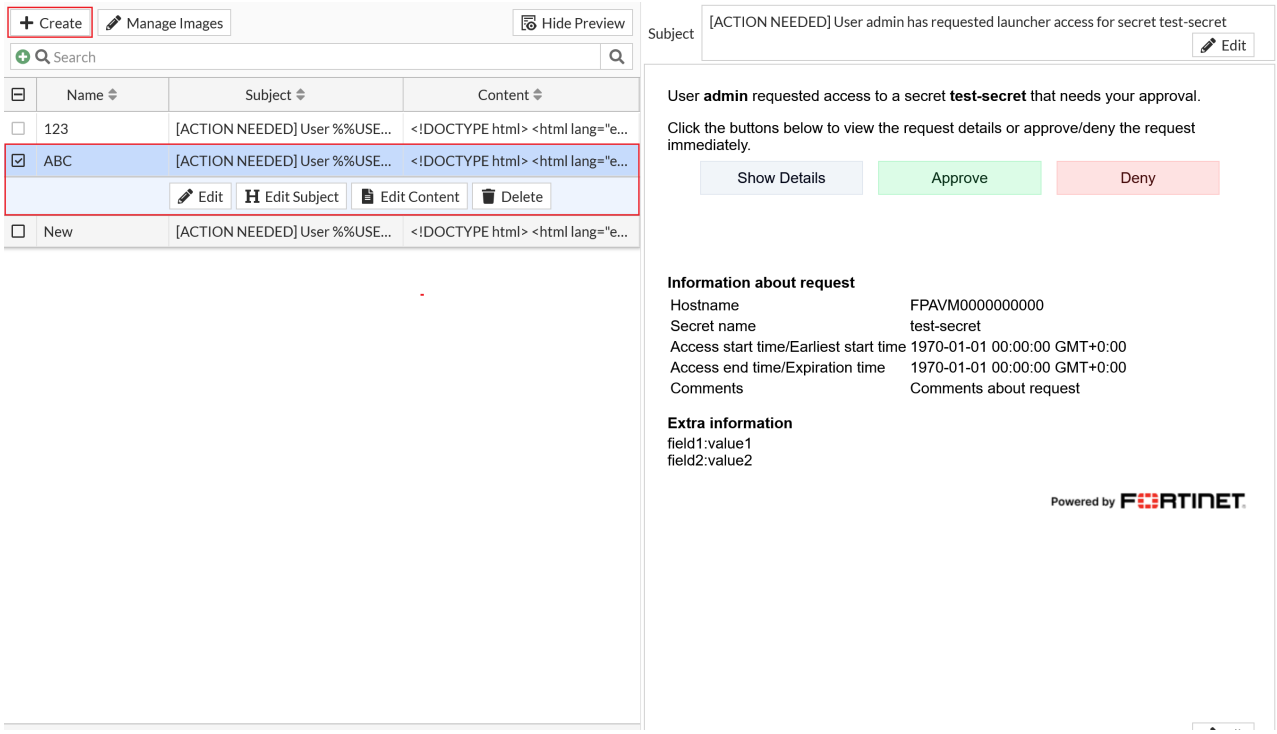
Submitted secret requests can be accepted or denied by approvers through email.

When approving secrets by email is configured, reviewers will first receive an email of the secret request that is sent automatically from FortiPAM if the email address is provided in the user profile.

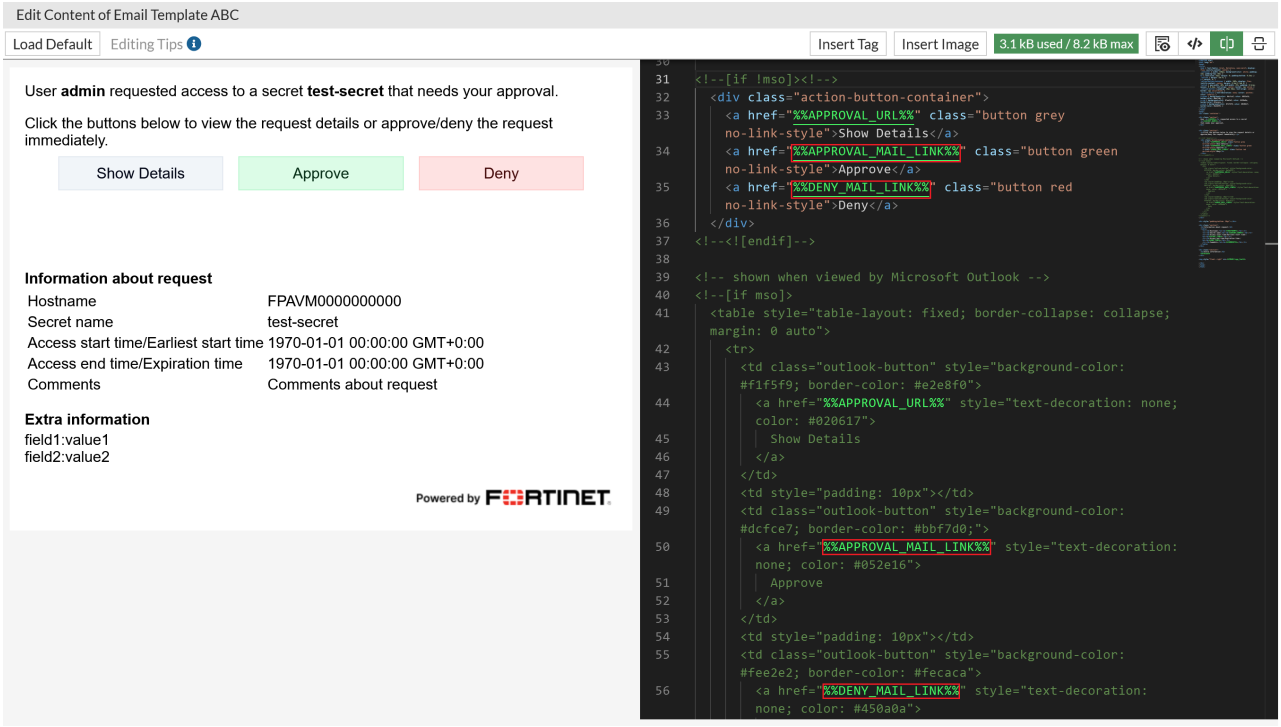
When the reviewers click the *Approve* or *Deny* button in the email, a pre-set email template will be used for reviewer to send their responses. FortiPAM will act as an email client to fetch the response emails periodically if approval email server settings are configured properly.

To enable response by email:

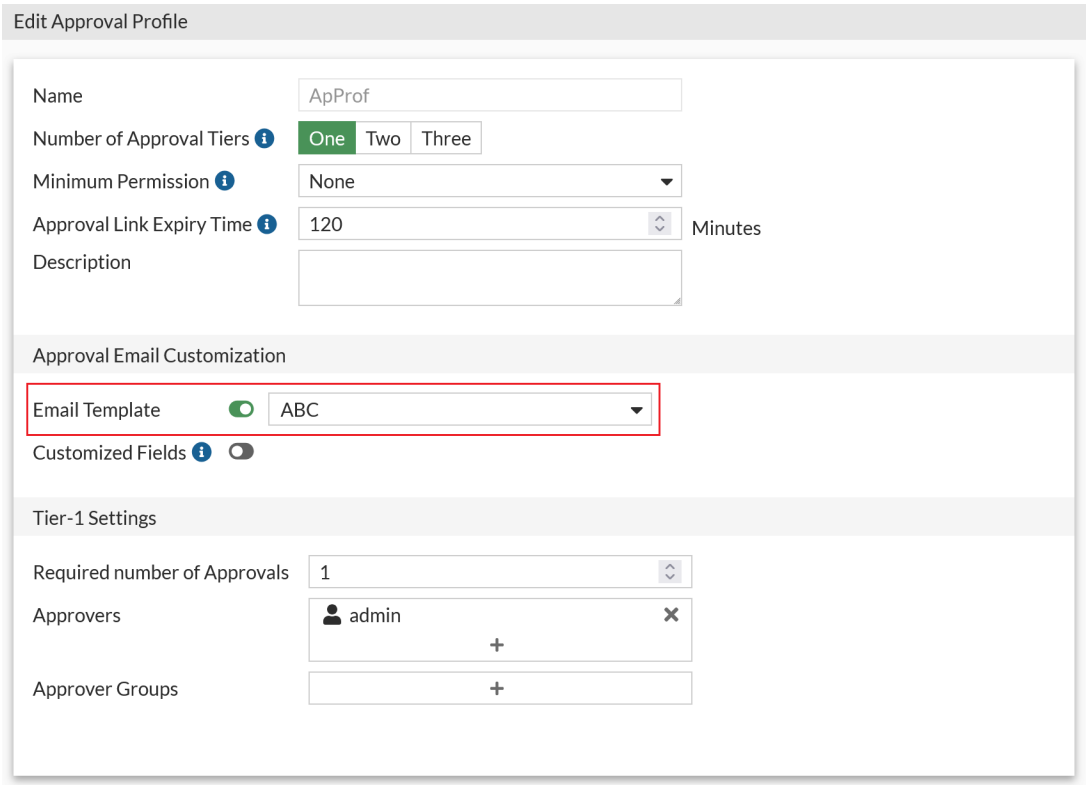
1. Go to *Secret Settings* > *Approval Email Template*, and create and edit a new email template, or double-click an existing entry to edit it.



2. In the HTML file, replace `%%APPROVAL_LINK%%` by `%%APPROVAL_MAIL_LINK%%`, and replace `%%DENY_LINK%%` by `%%DENY_MAIL_LINK%%`.

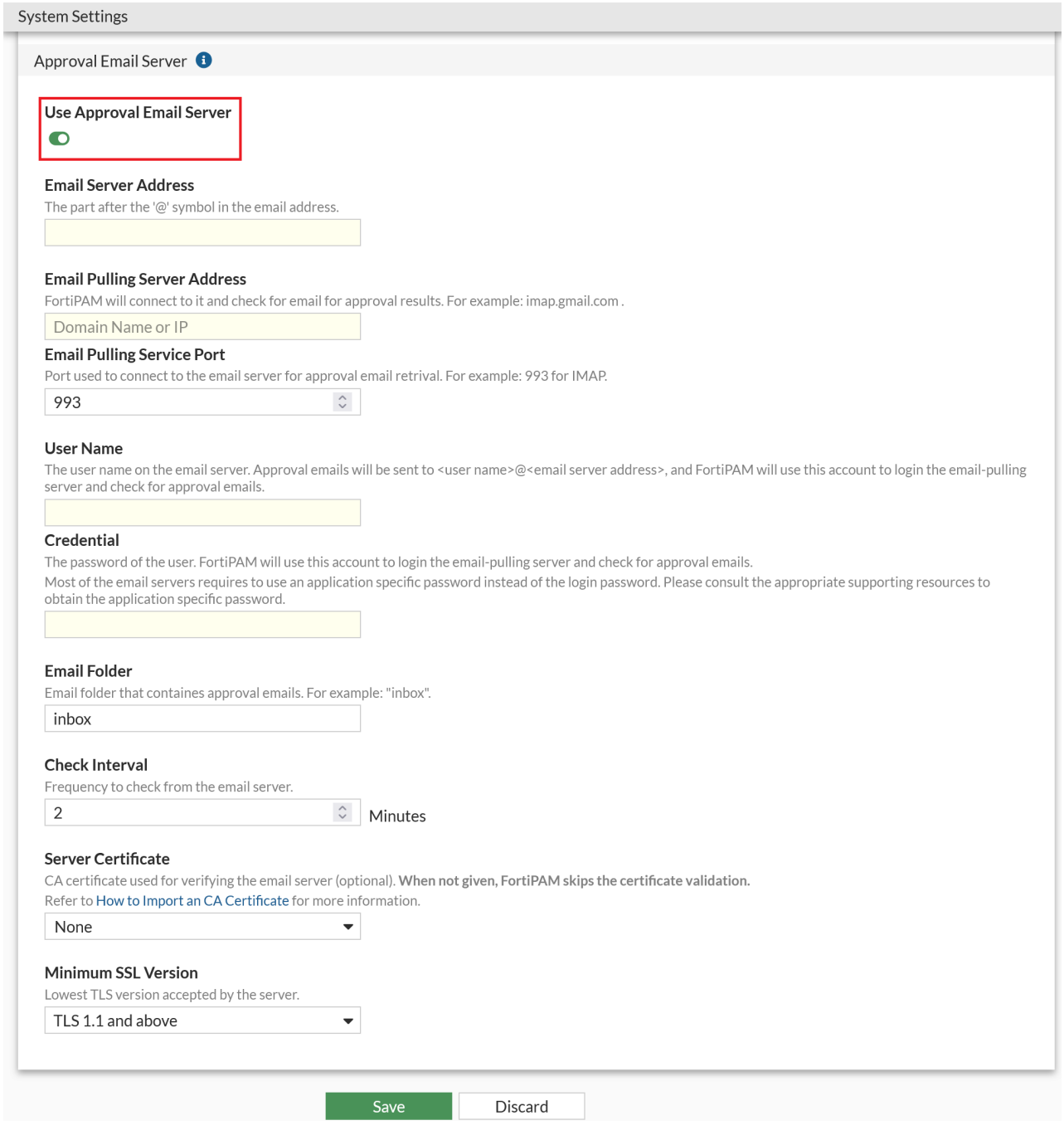


3. Go to *Secret Settings* > *Approval Profile*. In the selected entry, enable *Email Template* and select the template selected in the last step. Click *Save*.



To configure the approval email server in the GUI:

1. Go to *System* > *Settings*, and select the *Email Setting* tab.
2. In the *Approval Email Server* section, click the toggle to enable *Use Approval Email Server*, and fill in the fields according to the descriptions:



Email Server Address	The domain portion of your email address that appears after the @ symbol. Example: icloud.com, gmail.com

Email Pulling Server Address	The IMAP (Internet Message Access Protocol) server address that handles incoming email retrieval, support both fqdn and IP format. Example: imap.mail.me.com (icloud IMAP address)
Email Pulling Service Port	The network port number used for connecting to the email server. Example: 993 - Standard port for IMAP over SSL/TLS (secure).
User Name	The account identifier used for authentication on the email server. Usually the portion of your email address before the @ symbol.  The same *User Name* (i.e., the same email account) can only be configured in one FortiPAM at a time; otherwise, the approval email will be rejected because it was read by other FortiPAM instances.
Credential	The login password of the given user name.  For security reasons, most of the email servers don't allow you to use the plain password. Instead, you need to generate an "application specific password" and fill it in as the credential. The user need to consult appropriate supporting resources to obtain it. References: • Create App Password for Gmail - How to create app passwords | Google Workspace Knowledge Center • Create App Password for iCloud - Sign in to apps with your Apple Account using app-specific passwords - Apple Support
Email Folder	The specific folder where approval emails are stored and checked. Example: inbox (default value).
Check Interval	The frequency of checking the email server for new messages. Example: 2 minutes (the minimum allowed value is 1).
Server Certificate	It is used to validate the email server. This is an optional field. When not given, the verification is skipped.
Minimum SSL Version	The minimum acceptable TLS protocol version for secure communications.

 The approval response email in the *Approval Email Server* must be unread before the request is approved/denied.

To configure the approval email server in the CLI:

Below is an example CLI configuration:

```
config secret setting
  config approval-email-setting
    set email-pulling-server "imap.gmail.com"
```

```
        set server "gmail.com"
        set port 993
        set username “type your username”
        set credential “type your credential”
        set email-folder "inbox"
        set server-cert ''
        set ssl-min-version tls-1.3
        set check-interval 5
    end
end
```

The example CLI commands above include placeholder information. You can replace this information with details specific to your environment. See the table below for the type of information is expected for each setting.

Example setting	Required information
`set mail-pulling-server <string>`	Server address to pull the email from. For example: `"imap.gmail.com"`.
`set server <string>`	The email server address. For example: `"gmail.com"`
`set port <interger>`	Service port of email pulling. For example: `993` for IMAP.
`set username <string>`	Email user name. For example: `"user123"`
`set credential <passwd>`	Email credentials.
`set email-folder <string>`	Email folder that contains approval emails. For example: `"inbox"`.
`set server-cert <string>`	CA certificate used for verifying the server (optional).
`set ssl-min-version {tls-1.1 | tls-1.2 | tls-1.3}`	Lowest TLS version accepted by the server. For example: `"tls-1.3"`.
`set check-interval <interger>`	Frequency to check from the email server in minutes. Enter a value from 1 to 1440. The default is 2 minutes. For example: `5`.

Troubleshooting tips

1. Verify server addresses are correctly formatted.
2. Confirm port numbers are appropriate for your email provider.
3. Check credentials if authentication fails.
4. Ensure SSL/TLS settings match server requirements.
5. Verify folder names match exactly as they appear in your email client.
6. In addition, administrators can check the trace log of the fetching email process in the CLI. For example:

```
dia de en
dia test application wad 21400
dia wad debug enable category email-client
dia wad debug enable level verbose
```

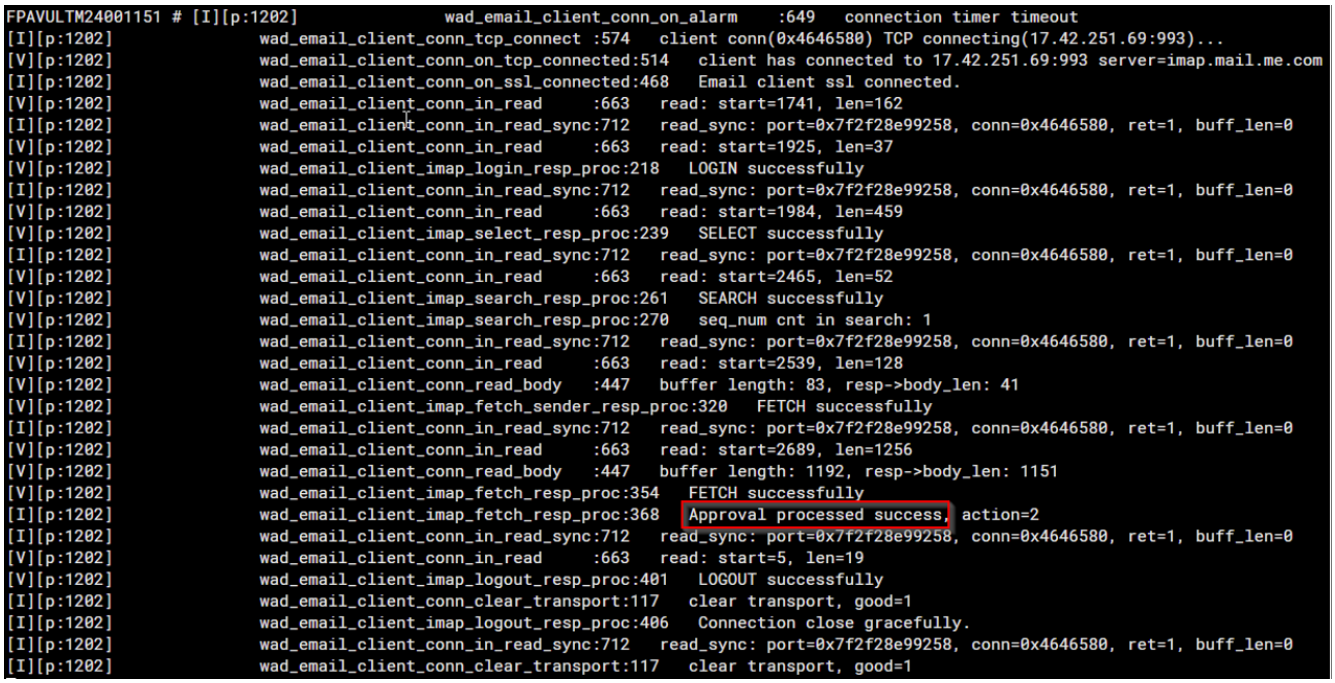
Example 1 (failure):

```
FPAVULTM24001151 # [I][p:1207]              wad_email_client_conn_on_alarm    :653   connection timer timeout
[I][p:1207]              wad_email_client_conn_tcp_connect :578   client conn(0x45c0ea0) TCP connecting(52.96.166.34:993)...
[V][p:1207]              wad_email_client_conn_on_tcp_connected:518   client has connected to 52.96.166.34:993 server=imap-mail.outlook.com
[I][p:1207]              wad_email_client_conn_on_ssl_connected:472   Email client ssl connected.
[V][p:1207]              wad_email_client_conn_in_read     :667   read: start=64, len=160
[I][p:1207]              wad_email_client_conn_in_read_sync:716   read_sync: port=0x7fbc40358258, conn=0x45c0ea0, ret=1, buff_len=0
[V][p:1207]              wad_email_client_conn_in_read     :667   read: start=253, len=23
[I][p:1207]              wad_email_client_imap_login_resp_proc:215   LOGIN failed
[I][p:1207]              wad_email_client_conn_in_read_sync:716   read_sync: port=0x7fbc40358258, conn=0x45c0ea0, ret=-1, buff_len=0
[V][p:1207]              wad_email_client_conn_proc_end    :160   proc end closing conn(0x45c0ea0).
[I][p:1207]              wad_email_client_conn_clear_transport:117   clear transport, good=-1
```

Example 2 (failure):

```
FPAVULTM24001151 # [I][p:1207]              wad_email_client_conn_on_alarm    :653   connection timer timeout
[I][p:1207]              wad_email_client_conn_tcp_connect :578   client conn(0x45c0ea0) TCP connecting(17.57.152.32:993)...
[V][p:1207]              wad_email_client_conn_on_tcp_connected:518   client has connected to 17.57.152.32:993 server=imap.mail.me.com
[I][p:1207]              wad_email_client_conn_on_ssl_connected:472   Email client ssl connected.
[V][p:1207]              wad_email_client_conn_in_read     :667   read: start=1741, len=162
[I][p:1207]              wad_email_client_conn_in_read_sync:716   read_sync: port=0x7fbc4031d258, conn=0x45c0ea0, ret=1, buff_len=0
[V][p:1207]              wad_email_client_conn_in_read     :667   read: start=1925, len=37
[V][p:1207]              wad_email_client_imap_login_resp_proc:218   LOGIN successfully
[I][p:1207]              wad_email_client_conn_in_read_sync:716   read_sync: port=0x7fbc4031d258, conn=0x45c0ea0, ret=1, buff_len=0
[V][p:1207]              wad_email_client_conn_in_read     :667   read: start=1984, len=441
[V][p:1207]              wad_email_client_imap_select_resp_proc:239   SELECT successfully
[I][p:1207]              wad_email_client_conn_in_read_sync:716   read_sync: port=0x7fbc4031d258, conn=0x45c0ea0, ret=1, buff_len=0
[V][p:1207]              wad_email_client_conn_in_read     :667   read: start=2447, len=51
[V][p:1207]              wad_email_client_imap_search_resp_proc:261   SEARCH successfully
[V][p:1207]              wad_email_client_imap_search_resp_proc:270   seq_num cnt in search: 1
[I][p:1207]              wad_email_client_conn_in_read_sync:716   read_sync: port=0x7fbc4031d258, conn=0x45c0ea0, ret=1, buff_len=0
[V][p:1207]              wad_email_client_conn_in_read     :667   read: start=2520, len=127
[V][p:1207]              wad_email_client_conn_read_body   :451   buffer length: 83, resp->body_len: 41
[V][p:1207]              wad_email_client_imap_fetch_sender_resp_proc:320   FETCH successfully
[I][p:1207]              wad_email_client_conn_in_read_sync:716   read_sync: port=0x7fbc4031d258, conn=0x45c0ea0, ret=1, buff_len=0
[V][p:1207]              wad_email_client_conn_in_read     :667   read: start=2669, len=1267
[W][p:1207]              wad_email_client_conn_read_line   :428   Error in preprocess response line
[I][p:1207]              wad_email_client_conn_in_read_sync:716   read_sync: port=0x7fbc4031d258, conn=0x45c0ea0, ret=-1, buff_len=1233
[V][p:1207]              wad_email_client_conn_proc_end    :160   proc end closing conn(0x45c0ea0).
[I][p:1207]              wad_email_client_conn_clear_transport:117   clear transport, good=-1
```

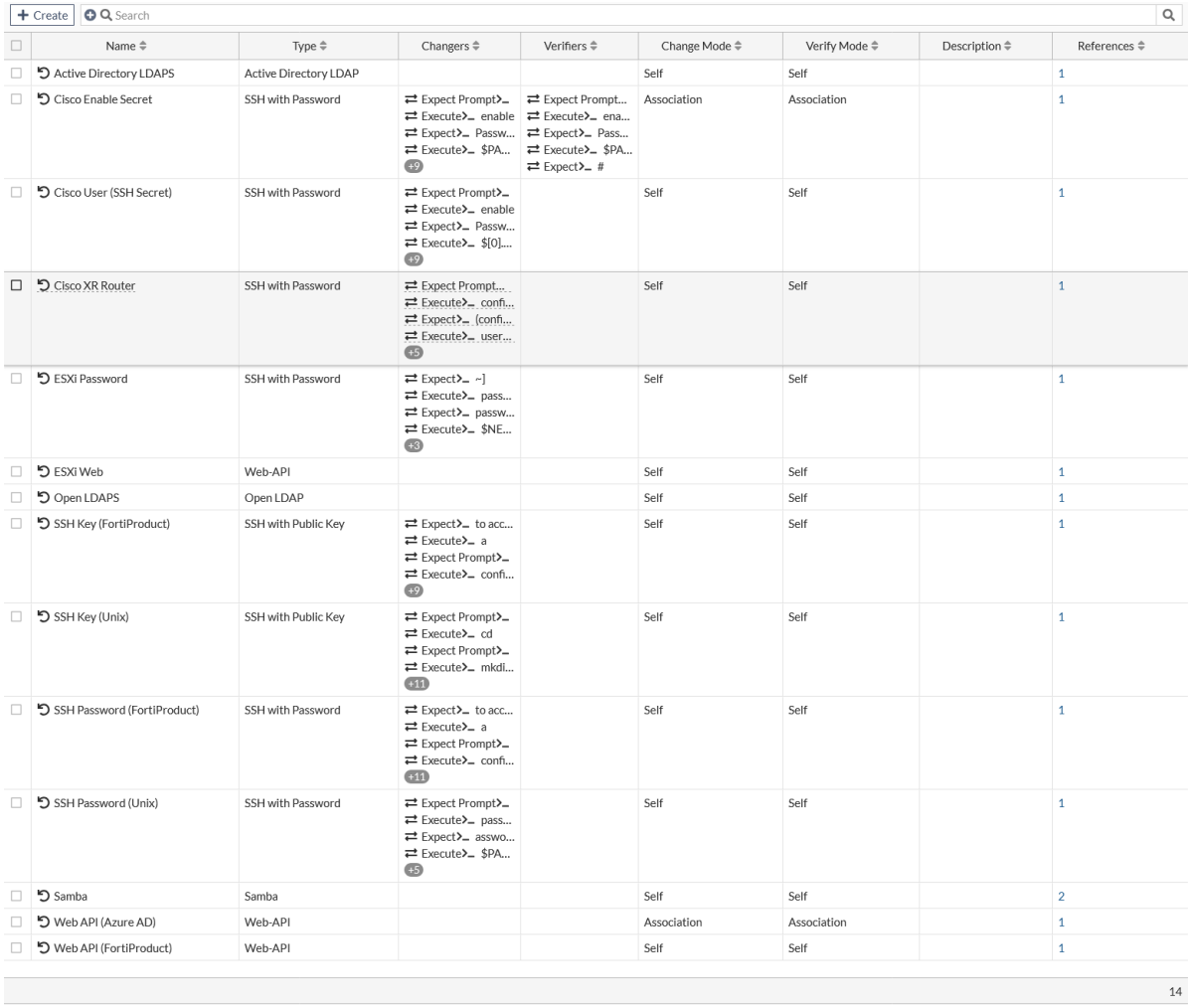
Example 3 (success):



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>_ Passw... Execute>_ $PA... +9	Expect Prompt... Execute>_ ena... Expect>_ Pass... Execute>_ $PA... Expect>_ #	Association	Association		1
Cisco User (SSH Secret)	SSH with Password	Expect Prompt>_ Execute>_ enable Expect>_ Passw... Execute>_ $[0].... +9		Self	Self		1
Cisco XR Router	SSH with Password	Expect Prompt... Execute>_ confi... Expect>_ (confi... Execute>_ user... +5		Self	Self		1
ESXi Password	SSH with Password	Expect>_ ~] Execute>_ pass... Expect>_ passw... Execute>_ $NE... +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 acc... Execute>_ a Expect Prompt>_ Execute>_ confi... +9		Self	Self		1
SSH Key (Unix)	SSH with Public Key	Expect Prompt>_ Execute>_ cd Expect Prompt>_ Execute>_ mkdi... +11		Self	Self		1
SSH Password (FortiProduct)	SSH with Password	Expect>_ to acc... Execute>_ a Expect Prompt>_ Execute>_ confi... +11		Self	Self		1
SSH Password (Unix)	SSH with Password	Expect Prompt>_ Execute>_ pass... Expect>_ asswo... Execute>_ $PA... +5		Self	Self		1
Samba	Samba			Self	Self		2
Web API (Azure AD)	Web-API			Association	Association		1
Web API (FortiProduct)	Web-API			Self	Self		1

14

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 (Azure AD)
- 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`.

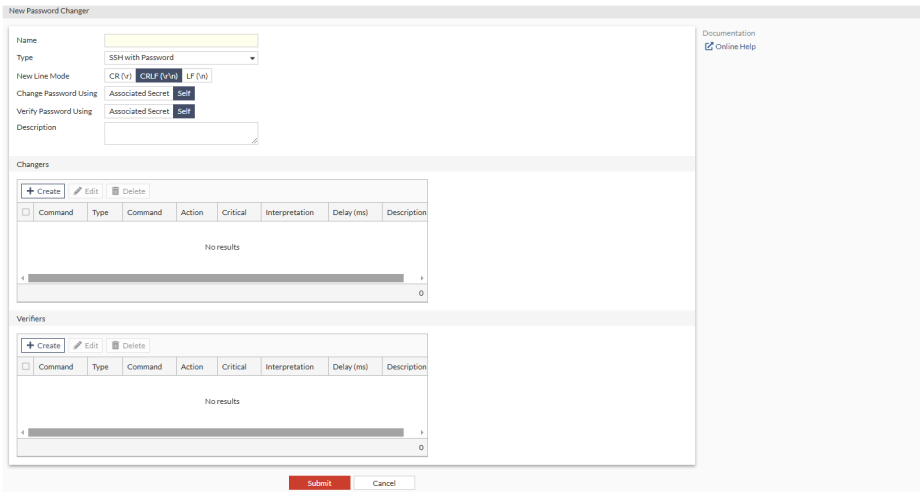
The *Password Changers* tab in *Secret Settings* contains the following options:

Create	Select to create a new password changer. See Creating a password changer on page 213.
Edit	Select to edit the selected password changer.
Delete	Select to delete the selected password changers.
Clone	Select to clone the selected password changer.
Search	Enter a search term in the search field, then hit `Enter` to search the password changers list. To narrow down your search, see Column filter.

Creating a password changer

To create a password changer:

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



4. Enter the following information:

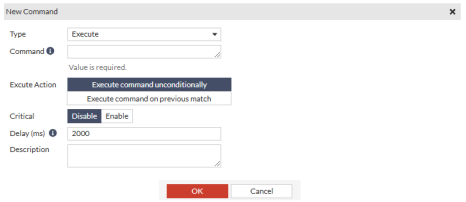
Name	The name of the password changer.
Type	From the dropdown, select a type: • *Active Directory LDAP* • *Open LDAP* • *Samba* • *SSH with Public Key* • *SSH with Password* (default) • *Web-API*
New Line Mode	Select from the following options: • *CR (\r)*: Carriage Return (\r) • *CRLF (\r\n)*: Carriage Return and Line Feed (\r\n) (default) • *LF (\n)*: Line Feed (\n) **Note**: The option is not available when the *Type* is *Web-API*.
Change Password Using	Select from the following two options: • *Associated Secret*: Changing password requires credentials from the associated secret. See *Associated Secret* option when Creating a secret on page 71. • *Self*: Secret can change its password (default).
Verify Password Using	Select from the following two options: • *Associated Secret*: Verifying password requires credentials from the associated secret. See *Associated Secret* option when Creating a secret on page 71. • *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*.
Web Changes	The web changer used to accomplish the password change. You can enter a series of `http` requests to execute `http` requests expect based on the previous `http execute` command. See Web changers on page 219. The option is available only when the *Type* is *Web-API*.
Web Verifiers	The web verifier used to verify that the password change was completed successfully. You can enter a series of `http` requests to execute `http` requests expect based on the previous `http execute` command. See Web verifiers on page 222. The option is available only when the *Type* is *Web-API*.

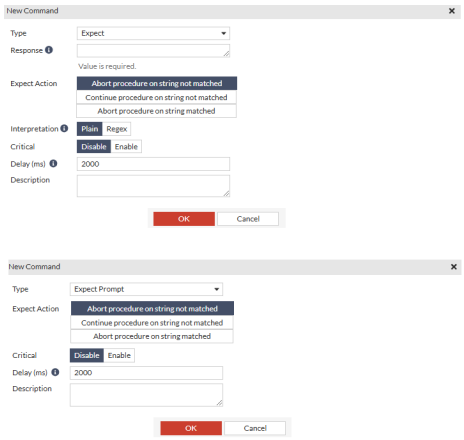
5. Click *Submit*.

Changers

1. In step 4 when Creating a password changer, select *Create* in *Changers*.
   The *New Command* window opens. By default, the *Type* is *Execute*.



   Different configuration options are available according to the *Type* selected.



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 = 2000, 50 - 20000).
Description	Optionally, enter a description.

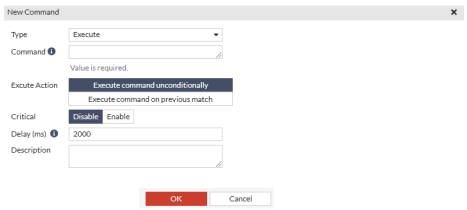
 To reorder the changer sequence, drag from the sequence number and then drop.

3. Click *OK*.

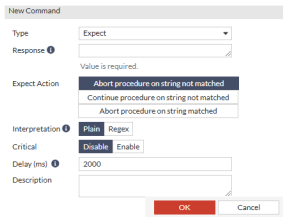
 From the list, select a changer and then select *Edit* to edit the changer.
From the list, select changer and then select *Delete* to delete the changer.

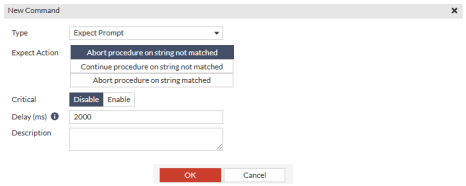
Verifiers

1. In step 4 when Creating a password changer, select *Create* in *Verifiers*.
The *New Command* window opens. By default, the *Type* is *Execute*.



Different configuration options are available according to the *Type* selected.





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 = 2000, 50 - 20000).
Description	Optionally, enter a description.

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

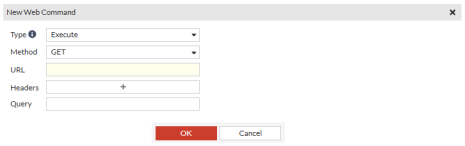
3. Click *OK*.

 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.

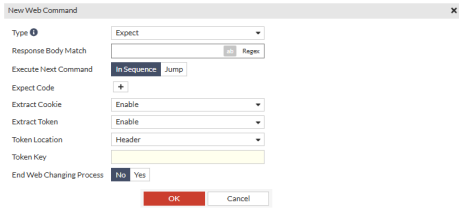
See Automatic password changing on page 224 and Automatic password verification on page 225.

Web changers

1. In step 4 when Creating a password changer, select *Create* in *Web Changers* when the *Type* is *Web-API*.
The *New Web Command* window opens. By default, the *Type* is *Execute*.



Different configuration options are available according to the *Type* selected.



2. Enter the following information:

Type	From the dropdown, select from the following options: • *Expect*: Verifies that the server response meets predefined criteria, such as, containing specific strings in the response body or matching expected status codes. If these criteria are not met, the password change process terminates. This step also allows for cookie and token extraction to support subsequent requests. • *Execute*: A request is sent to the server using the configured URL, headers, and query parameters. This initiates actions such as authentication or password change commands.
Method	From the dropdown, select a method: • *GET* • *POST* • *PUT* • *PATCH* • *DELETE* **Note**: The option is only available when the *Type* is *Execute*.
URL	The server URL. **Note**: The option is only available when the *Type* is *Execute*.
Headers	Select + and enter headers. **Note**: The option is only available when the *Type* is *Execute*.
Body	Enter the body for the web command. **Note**: The option is only available when the *Type* is *Execute* and the *Method* is *POST*, *PUT*, or *PATCH*.
Body Encoding	Select how FortiPAM decodes the input body fields: • *None* (default) • *URI* • *XML* **Note**: The option is only available when the *Type* is *Execute* and the *Method* is *POST*, *PUT*, or *PATCH*.

Query	Enter the query parameters. **Note**: The option is only available when the *Type* is *Execute*.
Response Body Match	Enter the response body match. This can be an exact match or a regular expression. See *Jump If Body Match*. **Note**: The option is only available when the *Type* is *Expect*.
Execute Next Command	Select from the following two options: • *In Sequence*: Linear execution (default) (legacy mode). • *Jump*: Depending on the current result or the step, jump to any step at will by importing the command number in the password changer process. Enter the command to jump to in *Jump To Command* (default = 2, 1 - 50). **Note**: The option is only available when the *Type* is *Expect*.
Jump If Body Match	Enable/disable jumping when the response body matches. **Note**: The option is available when *Response Body Match* is filled in and *Execute Next Command* is set to *Jump*.
Expect Code	Select + and enter code (1 - 500). **Note**: The option is only available when the *Type* is *Expect*.
Extract Cookie	Enable/disable extracting cookies (default = enable). **Note**: The option is only available when the *Type* is *Expect*.
Extract Token	Enable/disable extracting tokens (default = enable). **Note**: The option is only available when the *Type* is *Expect*.
Token Location	From the dropdown, select the token location: • *Body* • *Cookie* • *Header* (default) **Note**: The option is only available when the *Type* is *Expect*.
Token Key	Enter the token key. **Note**: The option is only available when the *Type* is *Expect*.
End Web Changing Process	Enable/disable ending the web changing process (default = *No*). **Note**: The option is only available when the *Type* is *Expect*.



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

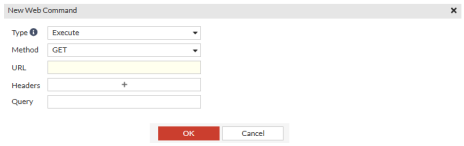
3. Click *OK*.



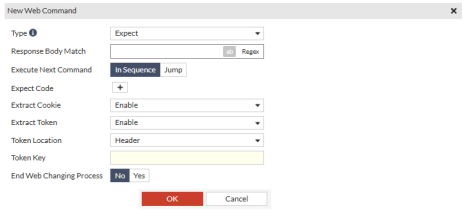
From the list, select a changer and then select *Edit* to edit the changer.
From the list, select a changer and then select *Delete* to delete the changer.

Web verifiers

1. In step 4 when Creating a password changer, select *Create* in *Web Verifiers* when the *Type* is *Web-API*. The *New Web Command* window opens. By default, the *Type* is *Execute*.



Different configuration options are available according to the *Type* selected.



2. Enter the following information:

Type	From the dropdown, select from the following options: • *Expect*: Verifies that the server response meets predefined criteria, such as, containing specific strings in the response body or matching expected status codes. If these criteria are not met, the password change process terminates. This step also allows for cookie and token extraction to support subsequent requests. • *Execute*: A request is sent to the server using the configured URL, headers, and query parameters. This initiates actions such as authentication or password change commands.
Method	From the dropdown, select a method: • *GET* • *POST* • *PUT* • *PATCH* • *DELETE* **Note**: The option is only available when the *Type* is *Execute*.
URL	The server URL. **Note**: The option is only available when the *Type* is *Execute*.
Headers	Select + and enter headers. **Note**: The option is only available when the *Type* is *Execute*.
Body	Enter the body for the web command. **Note**: The option is only available when the *Type* is *Execute* and the *Method* is *POST*, *PUT*, or *PATCH*.
Body Encoding	Select how FortiPAM decodes the input body fields: • *None* (default)

	• *URI* • *XML* **Note**: The option is only available when the *Type* is *Execute* and the *Method* is *POST*, *PUT*, or *PATCH*.
Query	Enter the query parameters. **Note**: The option is only available when the *Type* is *Execute*.
Response Body Match	Enter the response body match. This can be an exact match or a regular expression. See *Jump If Body Match*. **Note**: The option is only available when the *Type* is *Expect*.
Execute Next Command	Select from the following two options: • *In Sequence*: Linear execution (default) (legacy mode). • *Jump*: Depending on the current result or the step, jump to any step at will by importing the command number in the password changer process. Enter the command to jump to in *Jump To Command* (default = 2, 1 - 50). **Note**: The option is only available when the *Type* is *Expect*.
Jump If Body Match	Enable/disable jumping when the response body matches. **Note**: The option is available when *Response Body Match* is filled in and *Execute Next Command* is set to *Jump*.
Expect Code	Select + and enter code (1 - 500). **Note**: The option is only available when the *Type* is *Expect*.
Extract Cookie	Enable/disable extracting cookies (default = enable). **Note**: The option is only available when the *Type* is *Expect*.
Extract Token	Enable/disable extracting tokens (default = enable). **Note**: The option is only available when the *Type* is *Expect*.
Token Location	From the dropdown, select the token location: • *Body* • *Cookie* • *Header* (default) **Note**: The option is only available when the *Type* is *Expect*.
Token Key	Enter the token key. **Note**: The option is only available when the *Type* is *Expect*.
End Web Changing Process	Enable/disable ending the web changing process (default = *No*). **Note**: The option is only available when the *Type* is *Expect*.



To reorder the changer 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 changer.
From the list, select a verifier and then select *Delete* to delete the changer.

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 211.

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

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

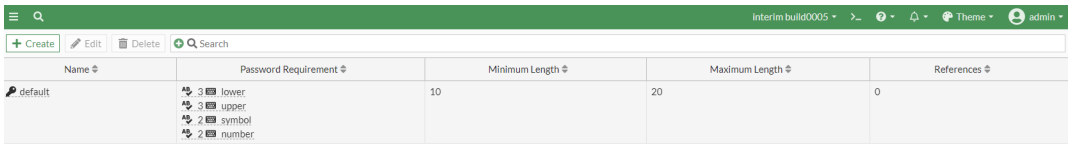


Password policies can only be applied to a secret template when *Password Changer* is enabled for the template.



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

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



The default password policy has the following features:

- *Minimum length*: 10
- *Maximum length*: 20
- *Password Requirements*: 3, 3, 2, and 2 minimum number of characters from the *lower*, *upper*, *symbol*, and *number* character sets respectively. See Character sets on page 228.

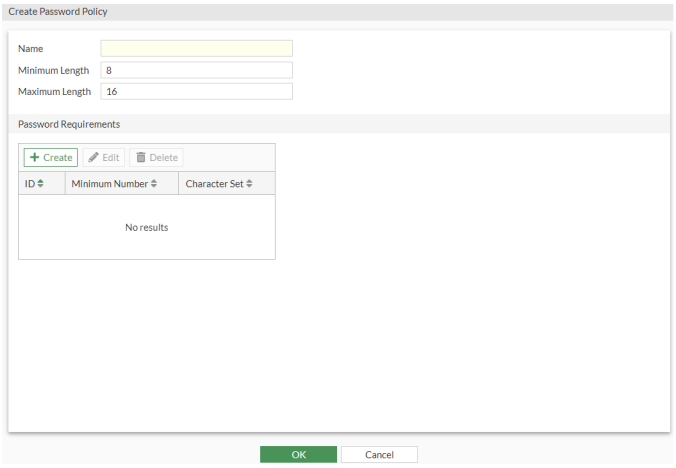
The *Password Policies* tab contains the following options:

Create	Select to create a new password policy. Password policies on page 225.
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.



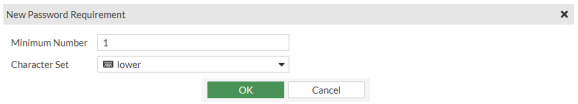
3. Enter the following information:

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 228.



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 227.

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.

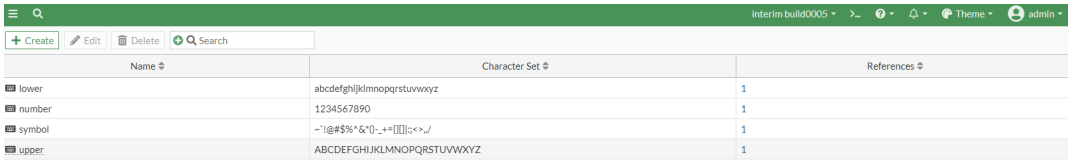
3. In the *Password Changer* pane, from the *Password Policy* dropdown, select a password policy or create a new password policy. See Creating a password policy on page 226 and Creating secret templates on page 157.
4. Click *Save*.

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 225.

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

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



The following default character sets are available in FortiPAM:

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

The *Character Sets* tab contains the following options:

Create	Select to create a new character set. See Creating a character set on page 228.
Edit	Select to edit the selected character set.
Delete	Select to delete the selected character sets.
Search	Enter a search term in the search field, then hit `Enter` to search the character sets list. To narrow down your search, see Column filter.

Creating a character set

To create a character set:

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



3. Enter the following information:

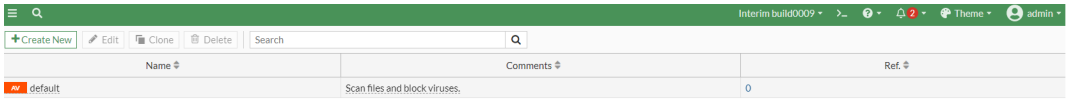
Name	The name of the character set.
Character Set	The character set.

4. Click *OK*.

AntiVirus

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

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



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

Once configured, you can add the antivirus profile to a secret. See Enabling antivirus scan in a secret on page 231.

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:

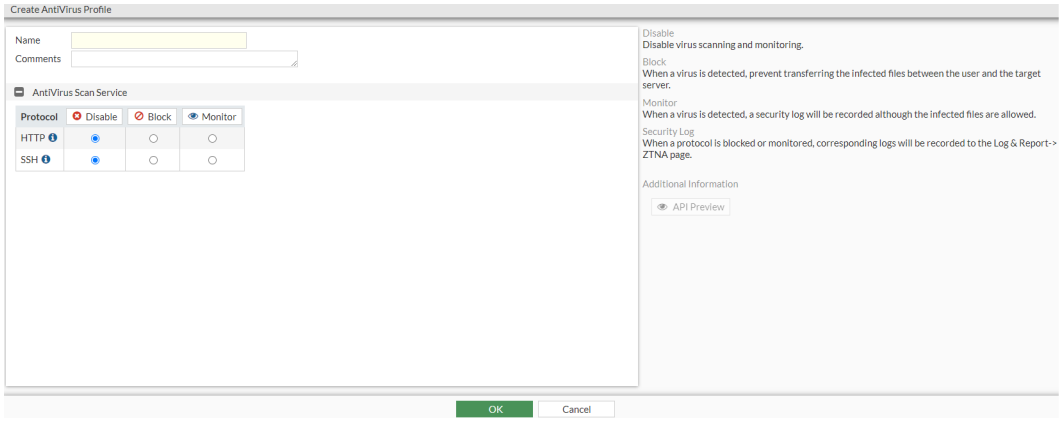
Create New	Select to create a new antivirus profile. See Creating an antivirus profile on page 230.
Edit	Select to edit the selected antivirus profile.

Clone	Select to clone the selected antivirus profile.
Delete	Select to delete the selected antivirus profiles.
Search	Enter a search term in the search field, then hit `Enter` to search the antivirus profile list.

Creating an antivirus profile

To create an antivirus profile:

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



2. Enter the following information:

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

AntiVirus Scan Service

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

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

Notes:

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

3. Click *OK*.

AV protection via the CLI - Example

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

```
config antivirus profile
  edit <profile-name>
```

```
        config http
           set av-scan block
        end
        config ssh
           set av-scan block
        end
     next
  end
```

Enabling antivirus scan in a secret

To enable antivirus scan in a secret:

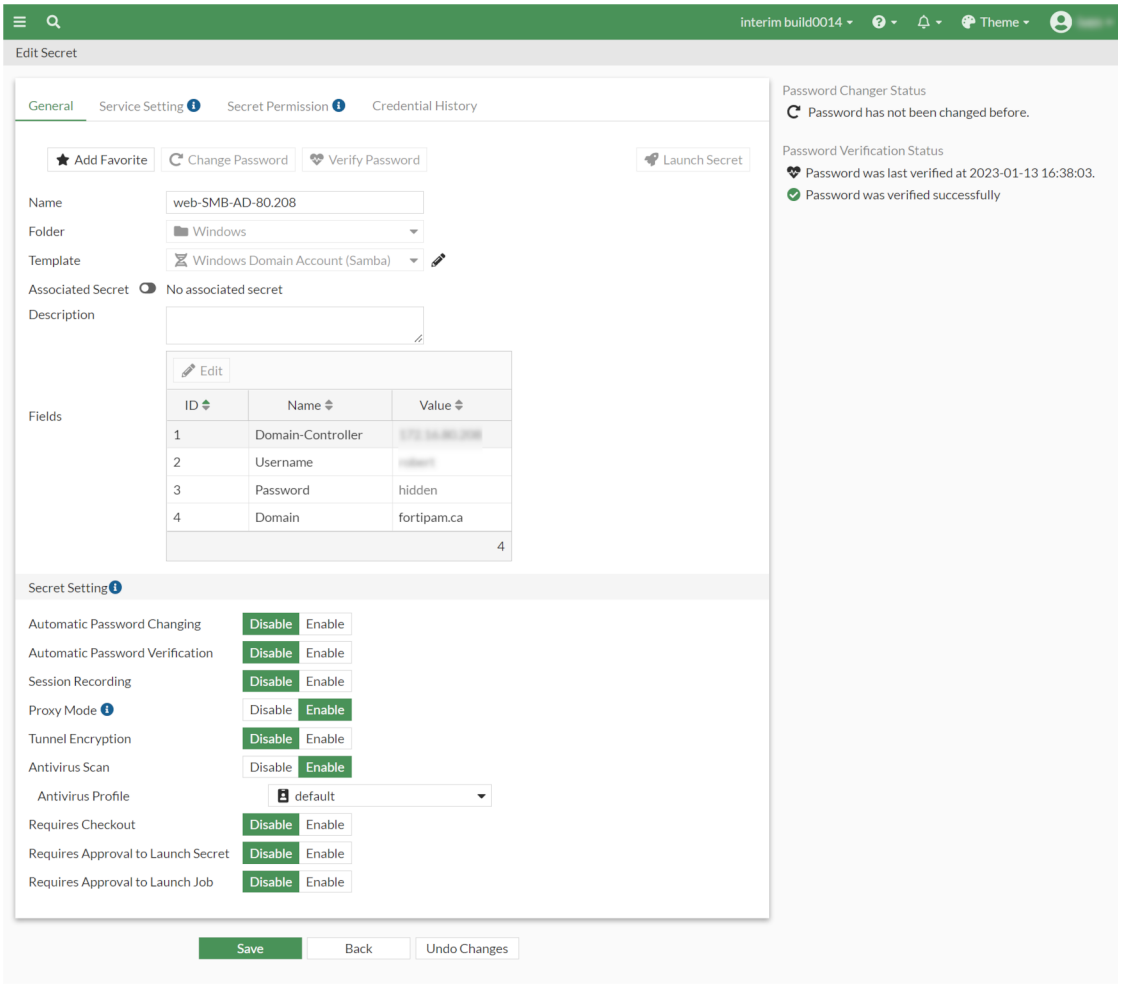
1. Go to *Secrets* > *Secrets*.
2. In the *Secrets*, double-click a secret to open.
   Alternatively, in *Secrets* > *Personal Folder/Public Folder*, go to the folder where the secret is located, and double-click the secret to open.



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 230.

5. Click *Save*.



Data loss prevention (DLP) protection for secrets

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

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

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

- Known files using DLP fingerprinting
- Known files using DLP watermarking
- Particular file types
- Particular file names

- Files larger than a specified size
- Data matching a specified regular expression

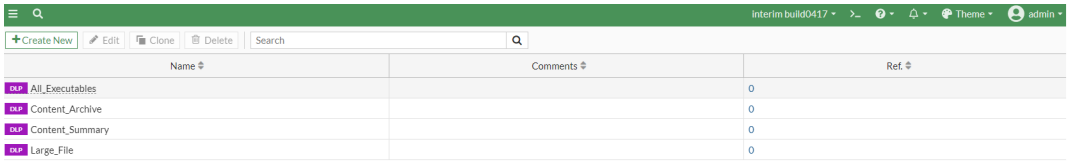
DLP is primarily used to stop sensitive data from leaving your network. DLP can also prevent unwanted data from entering your network and archive some or all of the content that passes through the FortiPAM. DLP archiving is configured per filter, which allows a single sensor to archive only the required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

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

- **File type and name**: A file type filter allows you to block, allow, log, or quarantine based on the file type specified in the file filter list. See Supported file types on page 237.
- **File size**: A file size filter checks for files that exceed the specific size and performs the DLP sensor's configured action on them.
- **Regular expression**: A regular expression filter filters files or messages based on the configured regular expression pattern.

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

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





FortiPAM offers the following preconfigured DLP sensors:

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



You cannot delete the default DLP sensors.

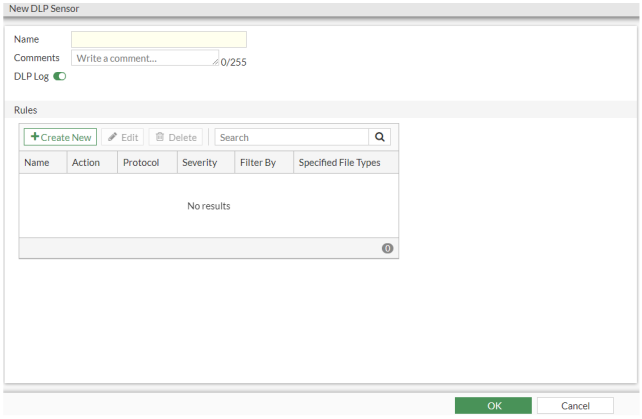
The *Data Leak Prevention* tab contains the following options:

Create New	Select to create a new DLP sensor. See Creating a DLP sensor on page 234.
Edit	Select to edit the selected DLP sensor.
Clone	Select to clone the selected DLP sensor.
Delete	Select to delete the selected DLP sensors.
Search	Search the DLP sensors list.

Creating a DLP sensor

To create a DLP sensor:

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



3. Enter the following information:

Name	Name of the DLP sensor.
Comments	Optionally, enter a description for the DLP sensor.
DLP Log	Enable to generate a log entry when data matches the configured patterns. The option is enabled by default.
Rules	Create or edit DLP filter rules. See Creating DLP filter rules on page 234.

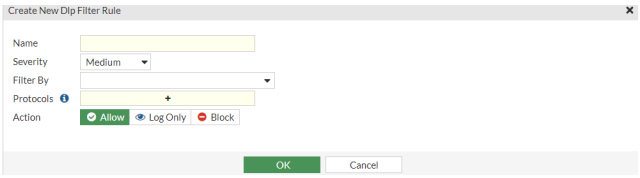
4. Click *OK*.

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 234, select *Create New* in *Rules*.
   The *Create New Dlp Filter Rule* window opens.



2. Enter the following information:

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

	 Filtering MAPI and SSH protocols only works in the proxy mode.
	 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

Type	Description
arj	Match ARJ compressed files
aspack	Match ASPack files
avi	Match AVI files
base64	Match Base64 files
bat	Match Windows batch files
binhex	Match BinHex files
bmp	Match BMP files
bzip	Match Bzip files
bzip2	Match Bzip2 files
cab	Match Windows CAB files
chm	Match Windows compiled HTML help files
class	Match CLASS files
cod	Match COD files
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

Type	Description
mime	Match MIME files
mov	Match MOV files
mp3	Match MP3 files
mpeg	Match MPEG files
msi	Match Windows Installer MSI Bzip files
msoffice	Match MS-Office files. For example, DOC, XLS, PPT, and so on.
msofficex	Match MS-Office XML files. For example, DOCX, XLSX, PPTX, and so on.
pdf	Match PDF files
petite	Match Petite files
png	Match PNG files
rar	Match RAR archives
rm	Match RM files
sis	Match SIS files
tar	Match TAR files
tiff	Match TIFF files
torrent	Match torrent files
unknown*	Match unknown files
upx	Match UPX files
uue	Match UUE files
wav	Match WAV files
wma	Match WMA files
xar	Match XAR archive files
xz	Match XZ files
zip	Match ZIP files

*This file type is only available in DLP profiles.

DLP file pattern

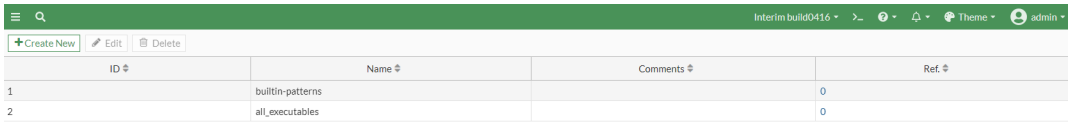
DLP file patterns match selected file types and file patterns. They are used as DLP filter rules in DLP sensors.

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

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

The *Ref.* column displays the number of times the object is referenced to other objects.

To view the location of the referenced object, select the number in *Ref.*; the *Object Usage* window opens and displays the various locations of the referenced object.



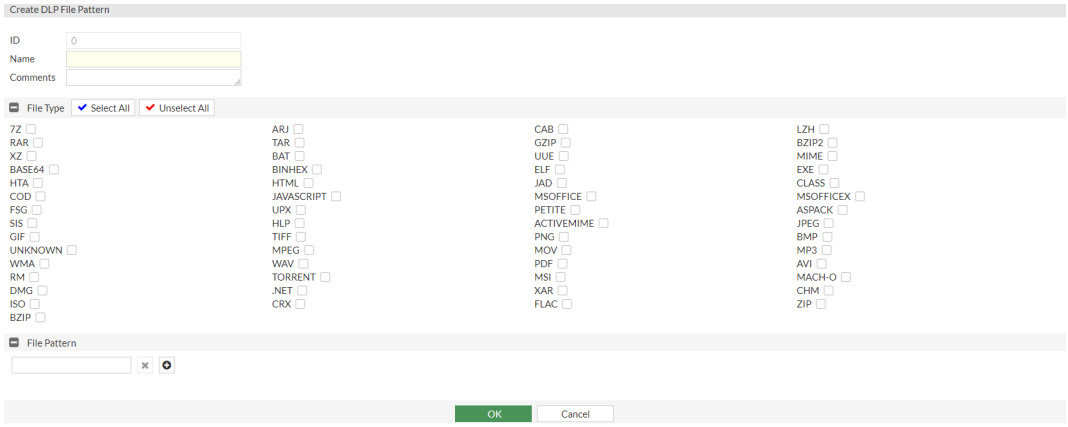
The *DLP File Pattern* tab contains the following options:

Create New	Create a DLP file pattern. See Creating a DLP file pattern on page 240.
Edit	Select to edit the selected DLP file pattern.
Delete	Select to delete the selected DLP file patterns.

Creating a DLP file pattern

To create a DLP file pattern:

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



3. Enter the following information:

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

4. Click *OK*.

SSH filter profiles

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

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

For each SSH profile; name, mode, shell commands, block channel, log activity, log all unlisted commands, and references are displayed by default.

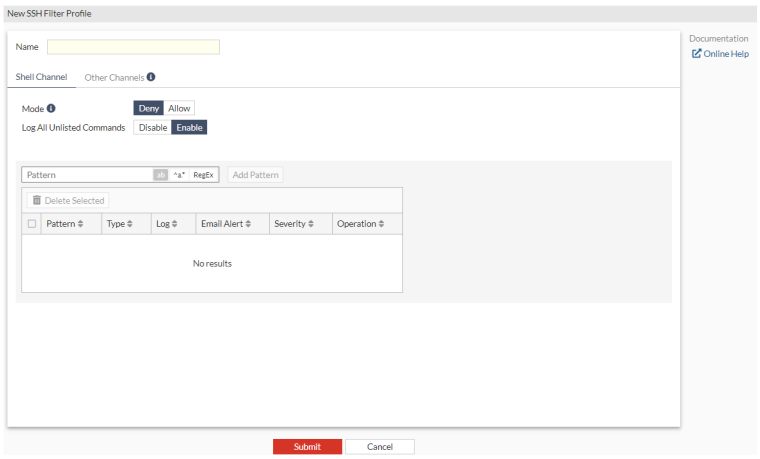
The *SSH Filter Profiles* tab contains the following options:

Create	Select to create a new SSH filter profile. See Creating an SSH filter on page 241.
Edit	Select to edit the selected SSH filter profile.
Delete	Select to delete the selected SSH filter profiles.
Search	Enter a search term in the search field, then hit `Enter` to search the SSH filter profiles list. To narrow down your search, see Column filter.

Creating an SSH filter

To create an SSH filter profile:

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



3. Enter the following information:

Name	Name of the SSH filter.
Shell 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.

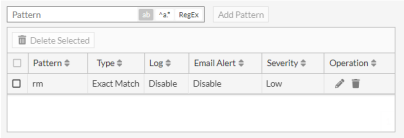
Block Channel	Select from the SSH blocking options (multiple options may be selected): • *X11*: X server forwarding • *SSH execution* • *Port forwarding*

	• *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*

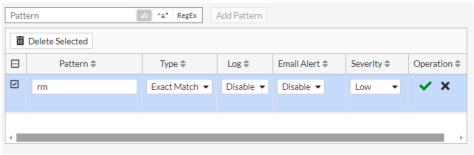
4. Click *Submit*.

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.



   d. From the pattern list, select the pen icon to edit the pattern.



   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.



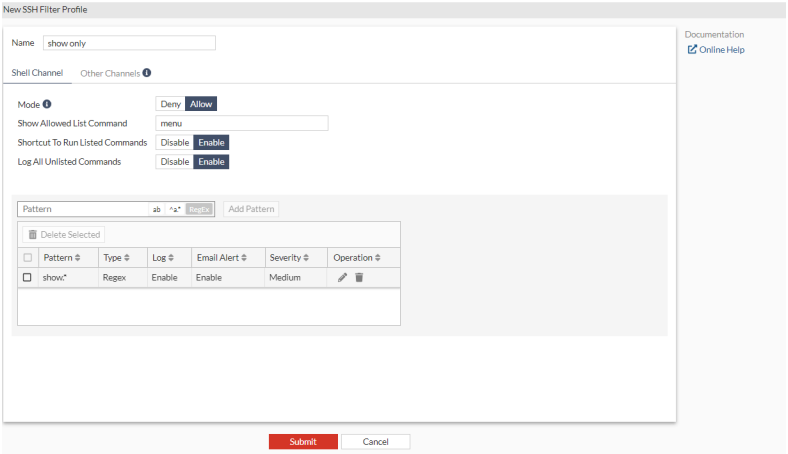
If the secret does not show up, it may be because you do not have the necessary permission to access the secret or the folder where the secret is located.

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):

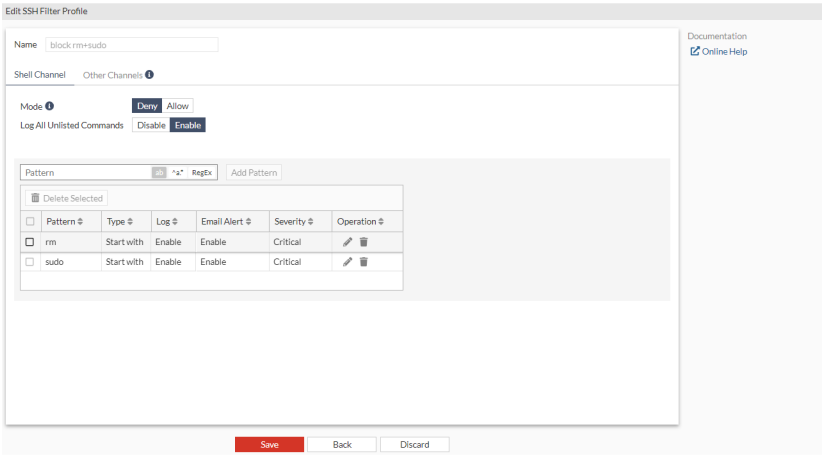
1. Go to *Secret Settings* > *SSH Filter Profiles*.
2. In *SSH Filter Profiles*, select *Create*.
   The *New SSH Filter Profile* window opens.
3. Enter a name for the SSH filter profile. In this example, the SSH filter profile is named `show only`.
4. In *Mode*, select *Allow*.
5. Leave *Show Allowed 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*.



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*.



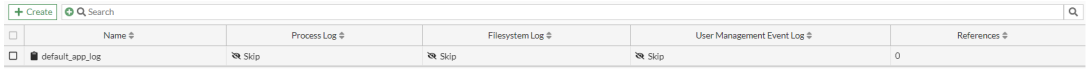
Event filter profile

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.



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 248.
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

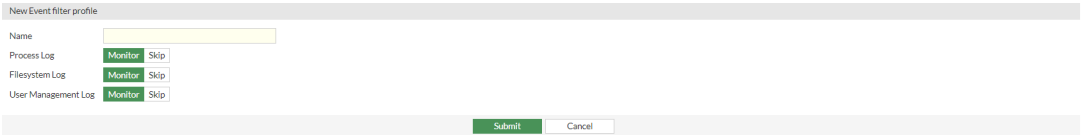
A secret event filter profile defines event categories pulled from the remote Windows server. Currently, users can monitor the following categories:

- 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 561.

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.



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 561.

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 252.
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.

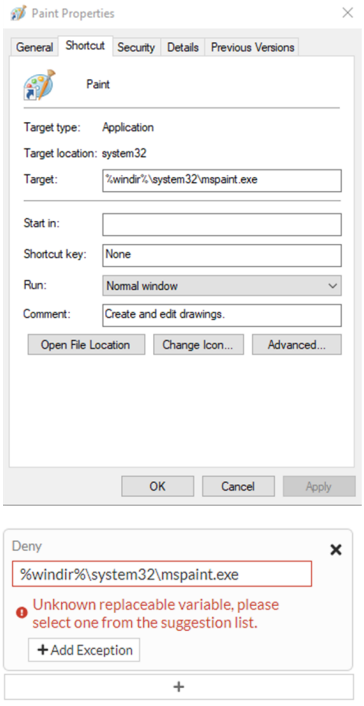
Limitations

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 117.

   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.



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.

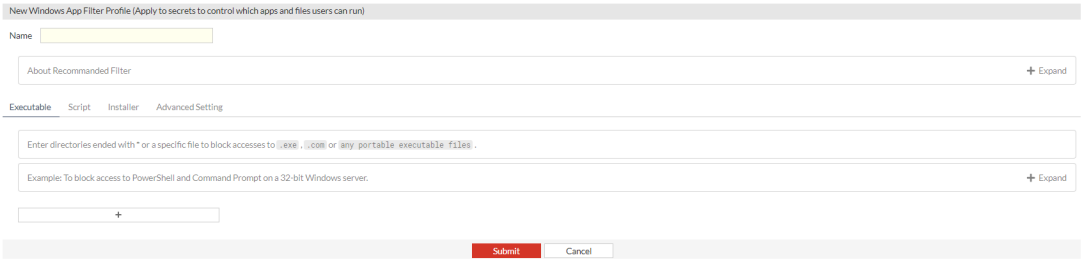
This interface allows for the creation and management of profiles that enforce security policies by restricting access to certain executables, scripts, and installers.

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.



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.

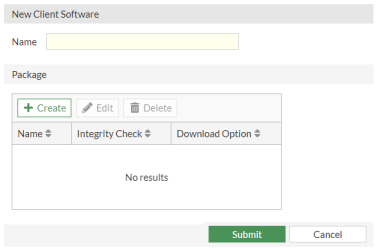
The *Integrity Check* tab contains the following options:

Create	Select to create a client software entry for integrity check. See Creating a client software entry for integrity check on page 255.
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 255.



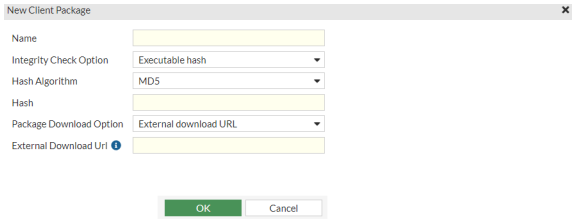
While creating a client software entry for integrity check, you can either store the software package locally, i.e., on the FortiPAM disk or provide an external URL to the package for downloading.

3. Click *Submit*.

Creating client software packages

To create a client software package

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



2. Enter the following information:

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

3. Click *OK*.

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

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

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

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

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

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

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

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

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

User management

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

- User list on page 258
- User groups on page 280
- Sponsored groups on page 286
- Role on page 289
- LDAP servers on page 301
- SAML Single Sign-On (SSO) on page 304
- RADIUS servers on page 312
- Auto provision rules on page 308
- Schedule on page 314
- FortiTokens on page 316

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:

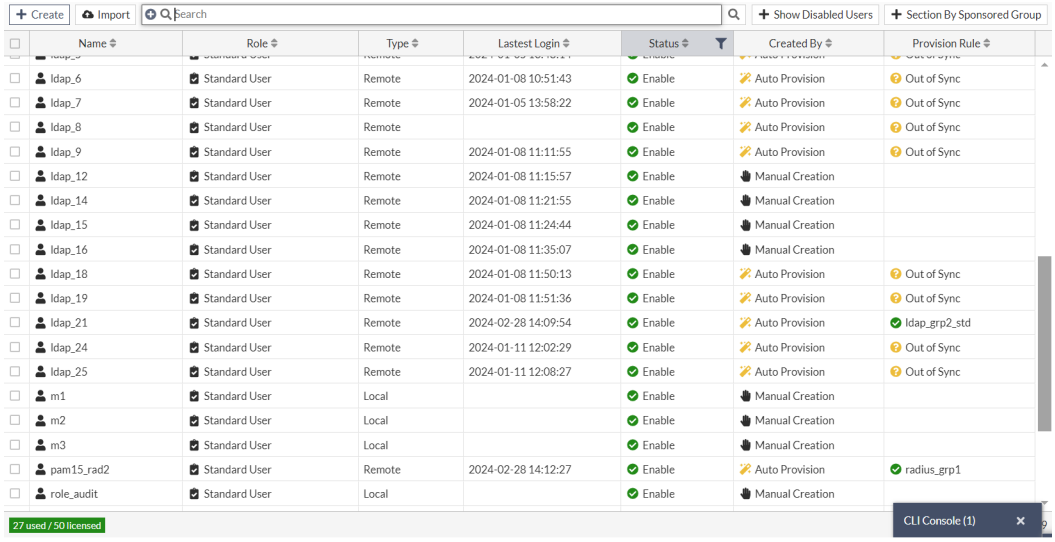
- *Name*
- *Sponsored Group*
- *Role*
- *Type*
- *Latest Login*
- *Status*
- *Two-factor Authentication*
- *References*
- *Created By*



By default, FortiPAM only lists enabled users.

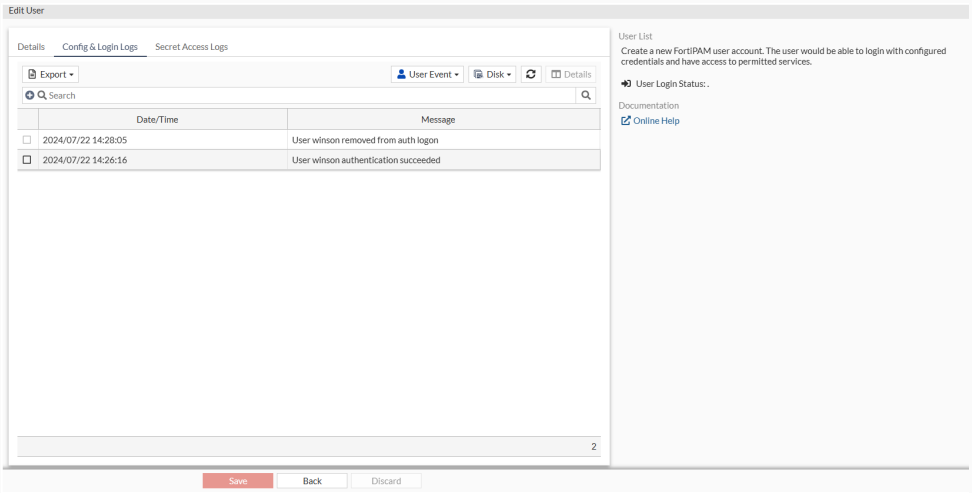


Enable *Show all users* to list all the users.



The user list contains the following options:

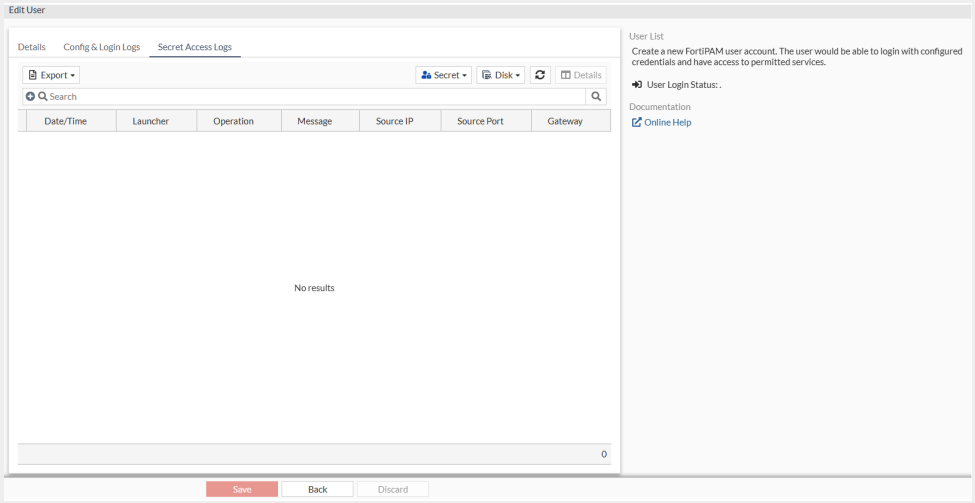
Create	Select to create a new user. See Creating a user on page 263.
Import	Select to import remote LDAP users from an LDAP server. See Importing LDAP users on page 277.
Edit	Select to edit the selected user account. When editing a user, new *Config & Login Logs* , *Secret Access Logs*, and *Secret List* tabs display related information.
Config & Login Logs	View config and login logs related to the selected user.

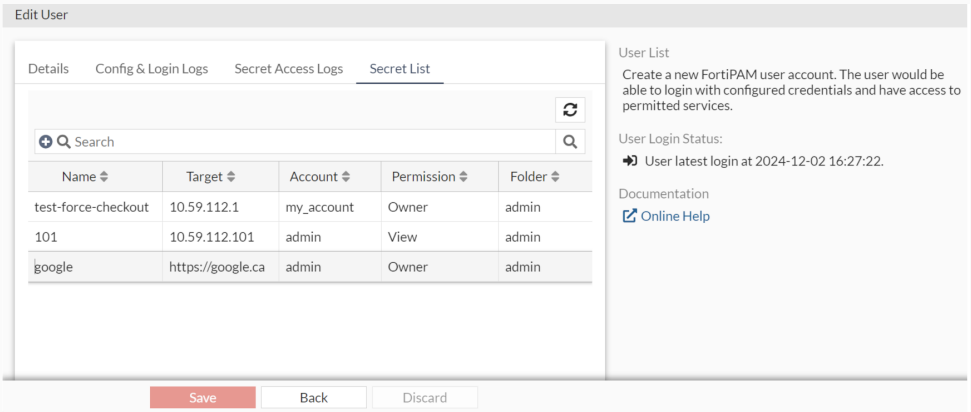


- Select the *Refresh* ( ) icon to refresh the logs table.
- Select *Details* to see details for the selected entry.

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` From the *User Event* dropdown, select from the following types of logs to display: • *User Event* • *System Event* • *ZTNA* From the *Log location* dropdown, select a source from where to retrieve logs: • Disk (FortiPAM)
Secret Access Logs	View secret access logs related to the selected user.  • Select the *Refresh* ( ) icon to refresh the logs table. • Select *Details* to see details for the selected log entry. 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` From the *Secret* dropdown, select from the following types of logs to display: • *Secret* • *SSH Filter* • *Antivirus* • *Data Leak Protection* From the *Log location* dropdown, select a source from where to retrieve logs: • Disk (FortiPAM)
Secret List	Displays the list of secrets that the user has access to. Administrators can view the secret name, folder name, target, account, and permissions.



- Select the *Refresh* ( ) icon to refresh the secrets table.
- Select a secret and click *Edit/View* to edit or view the secret details.
- Select a secret and click *View Logs* to view the related logs.

Permissions for Related Secrets

To view the *Secret List* tab, the administrator must have permissions enabled for *Administrator Users* and *View Reports*. With these permissions:

- If the user has *Edit* permissions for secrets, they can can edit secrets but cannot view the secret logs.
- If the user has *View* permissions for secrets, they can view the secrets but cannot view the secret logs.

To view secret logs, the administrator must also have the *View Secret Log* and/or *View Logs* permissions enabled:

- If the user has *Edit* permissions for secrets, they can can edit secrets and view the secret logs.
- If the user has *View* permissions for secrets, they can view the secrets and the secret logs.

With no permissions to view or edit secrets, the secrets are grayed out in the table, and you cannot view/edit the secret, or view the secret logs.

See Access control options on page 297.

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.

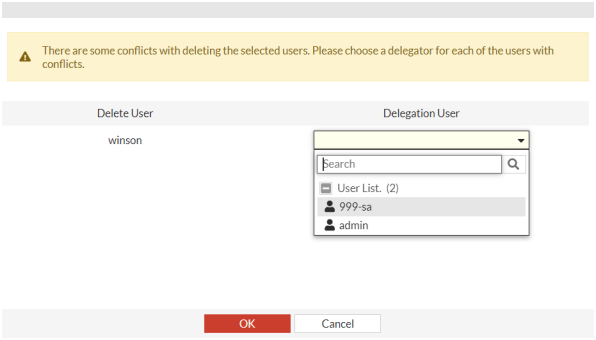
To enable/disable a user:

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.



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.



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.

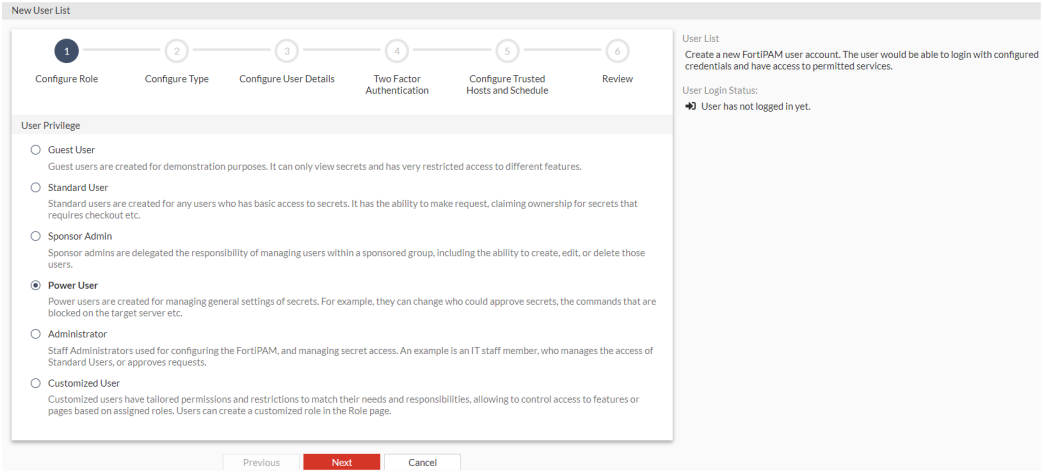
Creating a user

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.



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 286.
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 268 and Role on page 289.

Configure Type

User Type

Select a user type:

- *Local User*



To change the local user password, see Admin on page 24.

- *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.

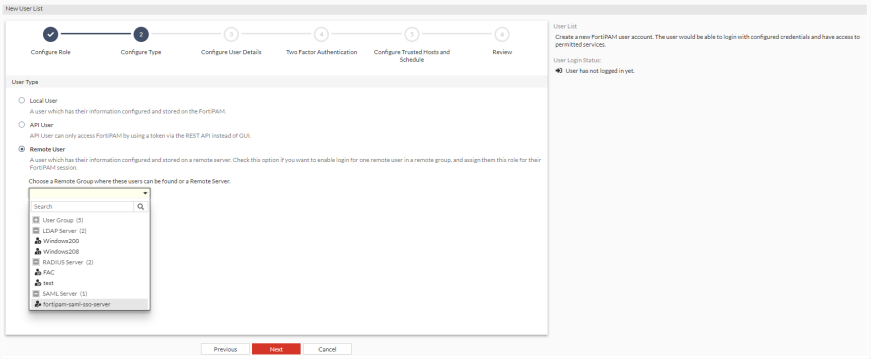
For *Remote User*, select a remote group where the user is found from the *Choose a Remote Group where these users can be found or a Remote Server* dropdown. See User groups on page 280.



Use the search bar to look for a remote group.

For information on the user types, see Users in FortiPAM on page 268.

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 301, SAML Single Sign-On (SSO) on page 304, and RADIUS servers on page 312.   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.
Language	Select a language for the user. This setting controls the language that the GUI will be presented in. Users with Administrator user roles are able to change the language settings for existing users. Users can change their language preferences once they have logged in by selecting a language from the language dropdown in the banner. See Banner on page 22.
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:
	• *Email* (default)
	• *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 269.
	• *Third-Party Authenticator*

	When using two-factor authenticator with a third-party authenticator, a random shared seed is generated for each user who uses this method. Administrators can send this shared-key by QR code in email. Users must scan the QR code using their own authenticator (e.g. Google, Microsoft, etc.) to generate the one-time-password for login. The QR code can also be retrieved through the GUI and resent through email.
	SMS based two factor authentication is not supported in FortiPAM 1.5.1.
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 314. **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 | third-party-authenticator>
      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 289.

- *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 289.

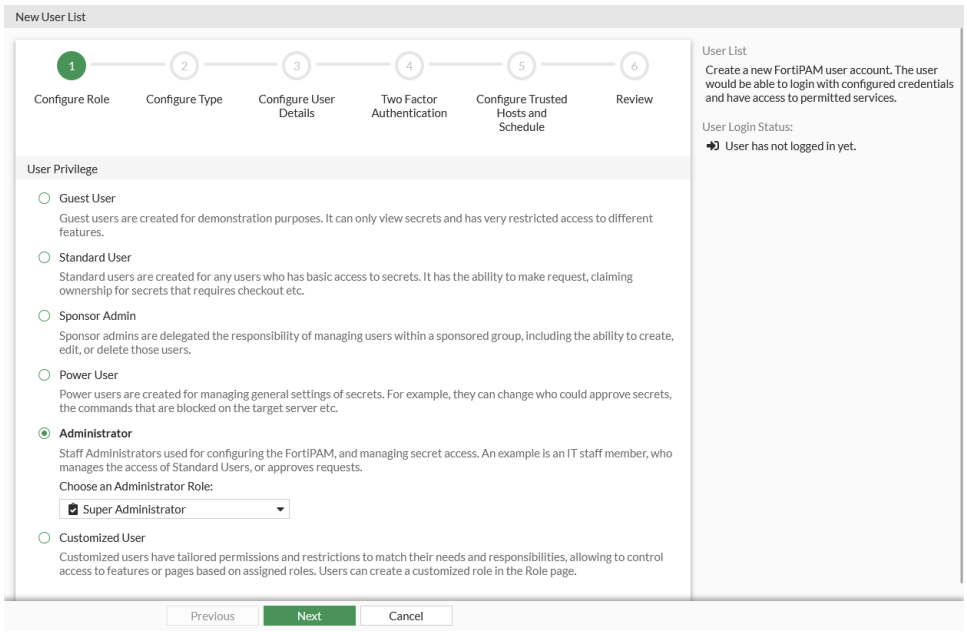
- *Customized User*: Customized users have tailored permissions and restrictions to match their needs and responsibilities, allowing them to control access to features or pages based on assigned roles. You can create a customized role in Role.

  See Creating a user on page 263.

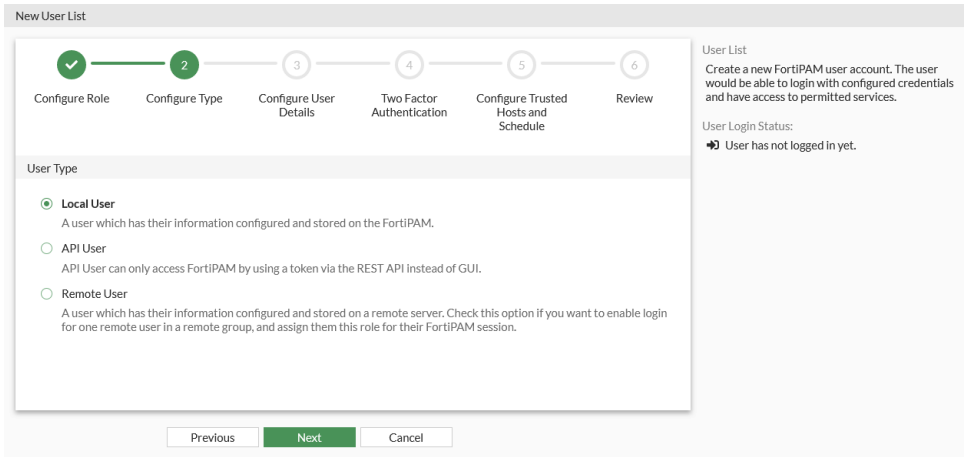
2FA with FortiToken Cloud - example

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*.



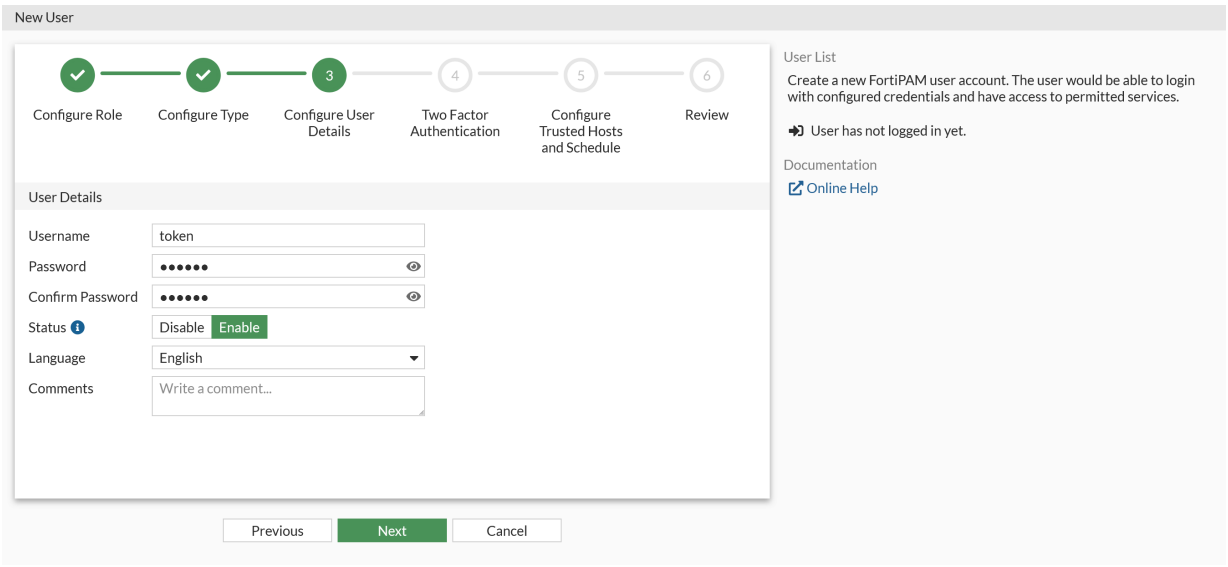
3. Click *Next*.
4. In *Configure Type*, select either *Local User* or *Remote User*.
   In this example, *Local User* is selected.



For *Remote User*, select a remote group where the user is found. See User groups on page 280.

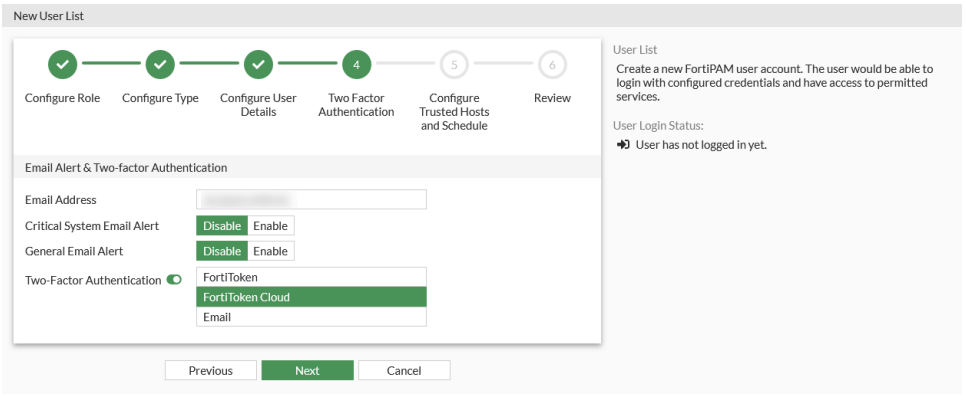
5. Click *Next*.
6. In *Configure User Details*:
   a. In *Username*, enter a name.
   b. In *Password*, enter a password.
   c. In *Confirm Password*, reenter password to confirm.
   d. In *Status*, enable logging in to FortiPAM.

e. In *Language*, select a language for the user.



f.

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*.



   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
```

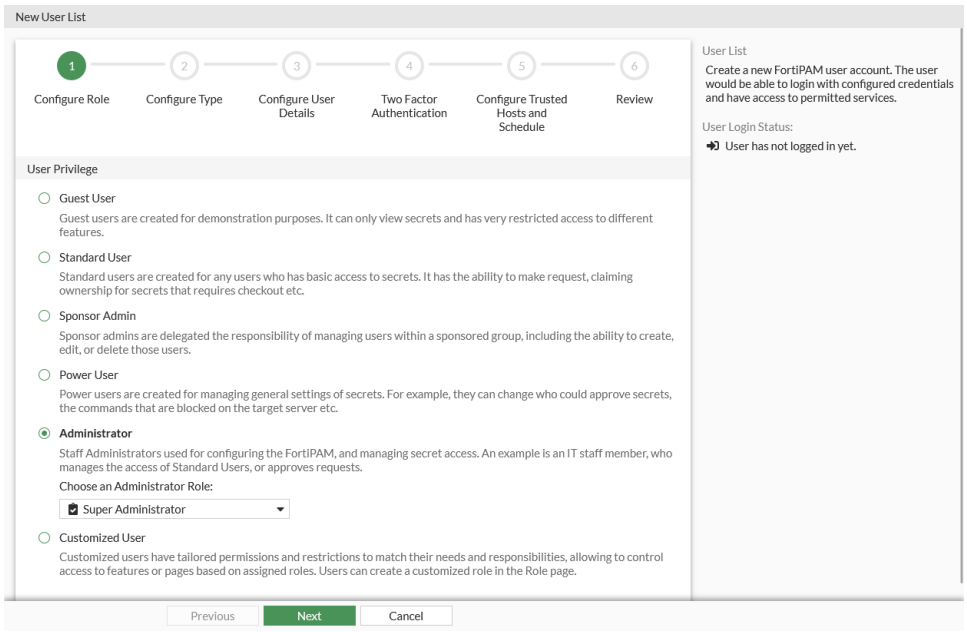
CLI configuration to set up a virtual IP address for FortiPAM - example**:**

```
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
```

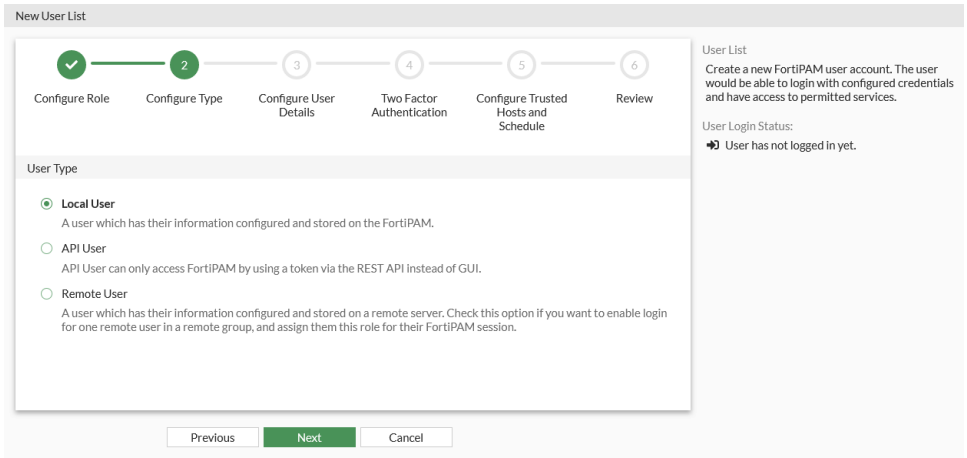
2FA with FortiToken - example

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*.



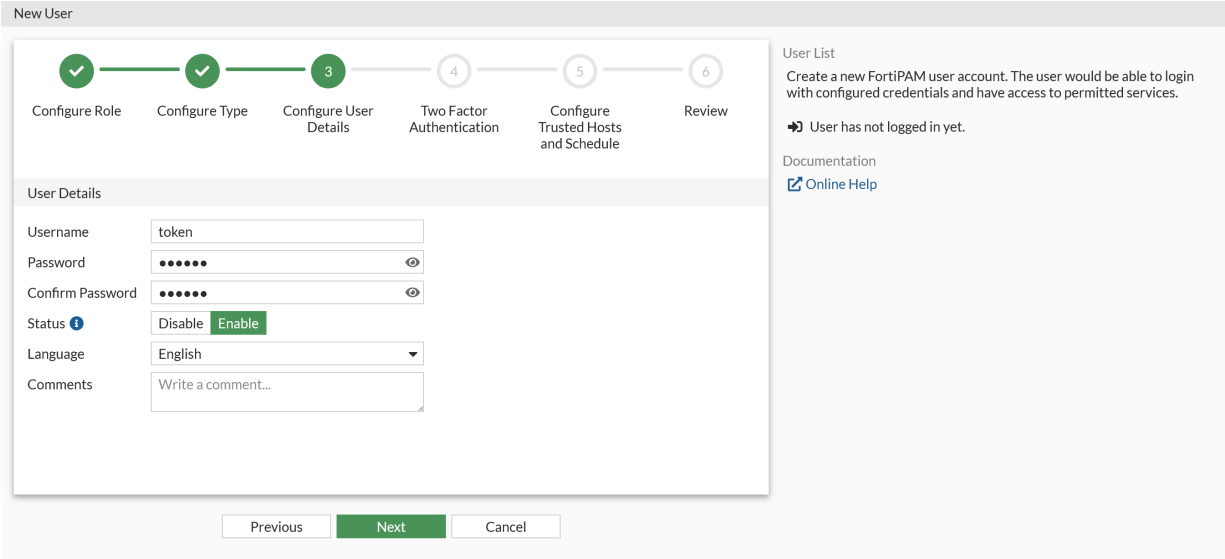
3. Click *Next*.
4. In *Choose a User type*, select either *Local User* or *Remote User*.
   In this example, *Local User* is selected.



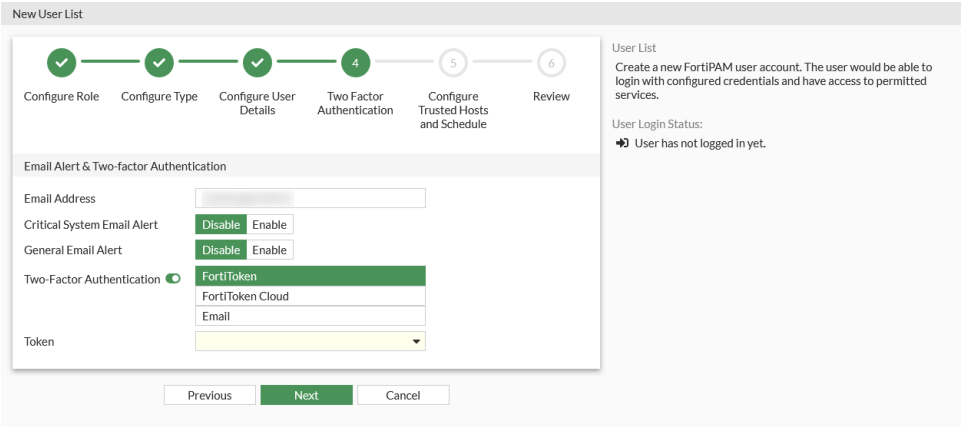
For *Remote User*, select a remote group where the user is found. See User groups on page 280.

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 *Language*, select a language for the user.



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.



   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 275.

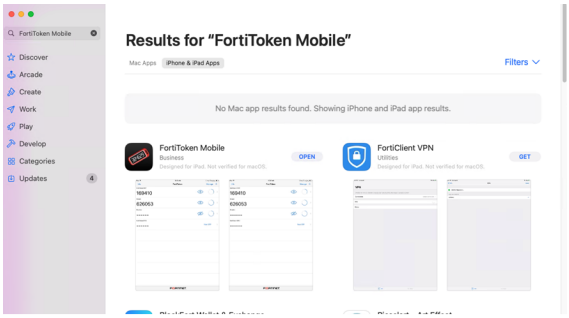
CLI configuration to set up a user with FortiToken as the authentication type - example**:**

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

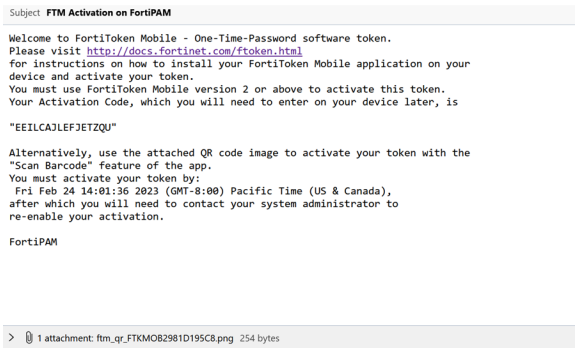
Setting up FortiToken Mobile

To set up FortiToken Mobile:

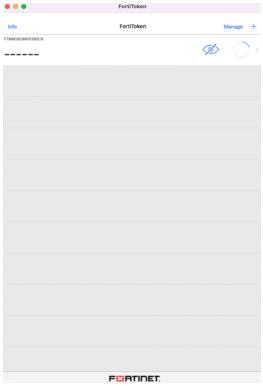
1. In the App Store, look for FortiToken Mobile and install the application.



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



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



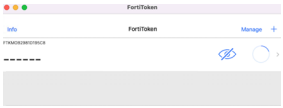
4. There are two ways to add a token to the FortiToken Mobile application:
   a. **Scan QR code**: If your device supports QR code recognition, select + in the FortiToken Mobile home screen and point your device camera at the QR code attached to the activation email.



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

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

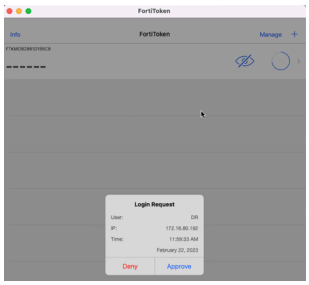
      iii. Click *Done*.
      FortiToken Mobile communicates with the secure provisioning server to activate your token. The token is now displayed in the token list view.



5. Click the eye icon to retrieve the token to be used in step 15 when configuring 2FA with FortiToken.



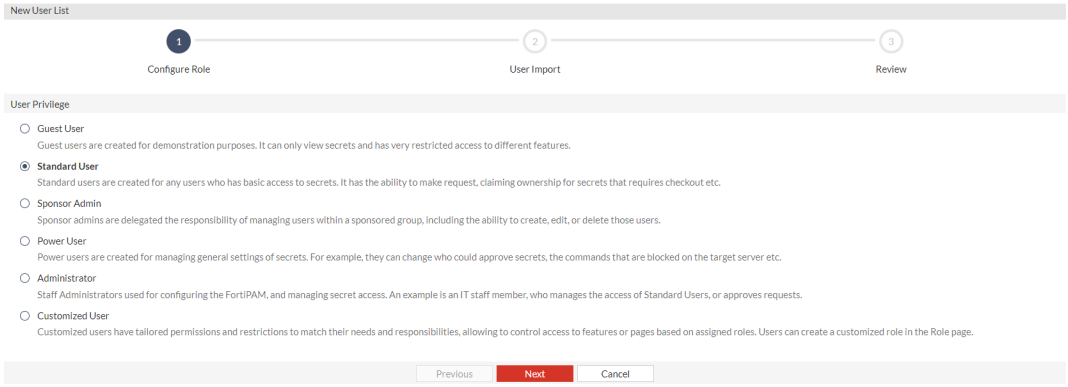
Alternatively, if approving the push login request in step 15 when configuring 2FA with FortiToken, click *Approve* in *Login Request*.



Importing LDAP users

To import LDAP users:

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



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 286. 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 268 and Role on page 289.

User Import

Remote Server

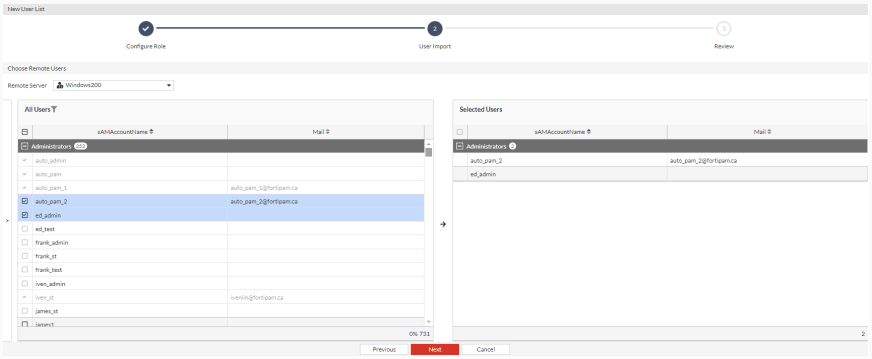
From the dropdown, select a remote LDAP server.

In the dropdown, select + to create a new remote LDAP server. See LDAP servers on page 301.

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.



By default, *LDAP DB Structure* is hidden.

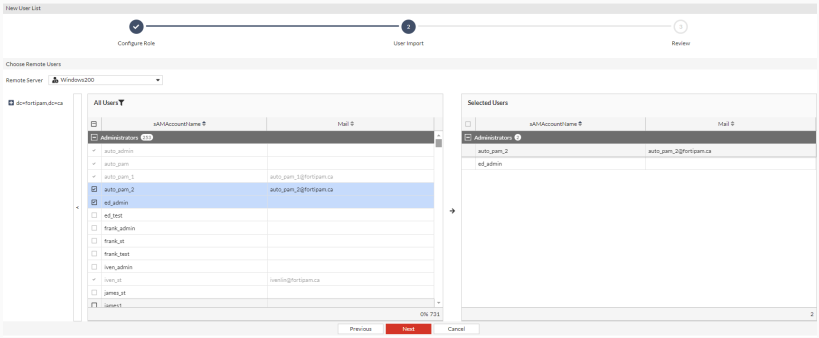
In the *All Users* table:

- 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.

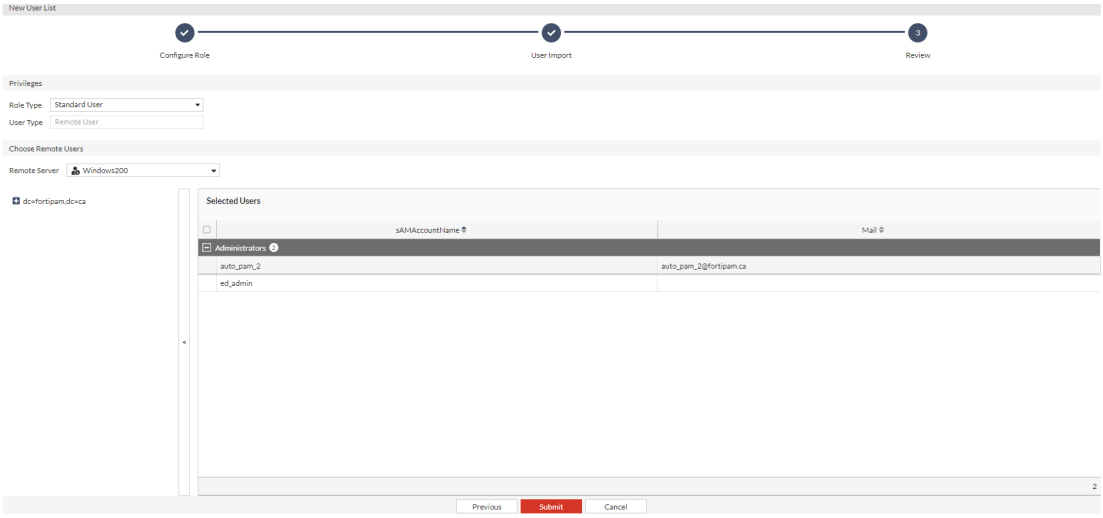
To define a filter to match username or group, see Filters on page 29 in Tables on page 29.

For other column related settings, see Column settings on page 33 in Tables on page 29.

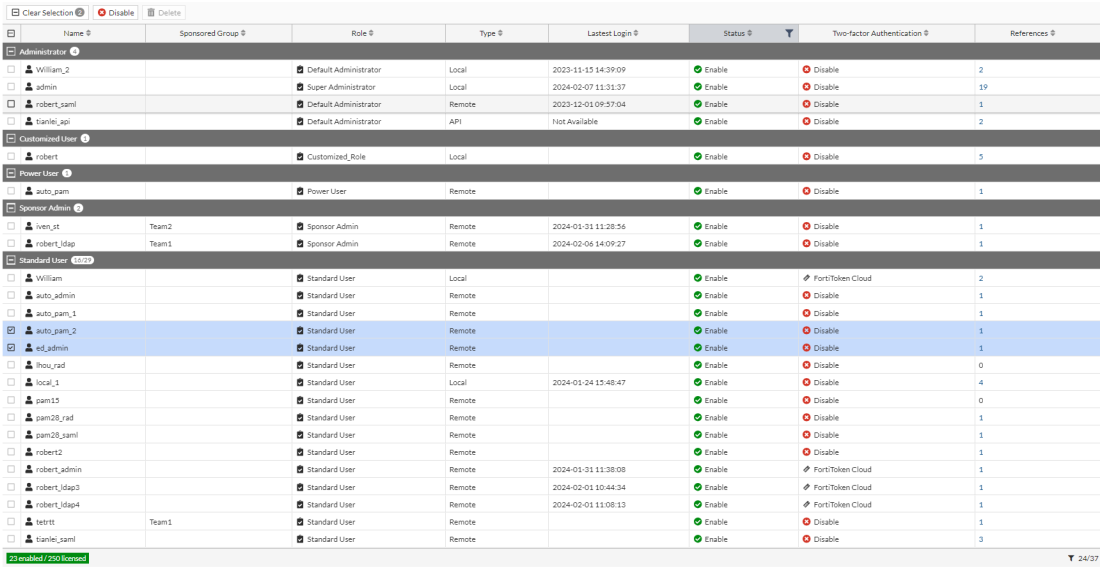
- Selected users from *All Users* are displayed in the *Selected Users* table.



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



The imported users are listed in *User Management* > *User List*.

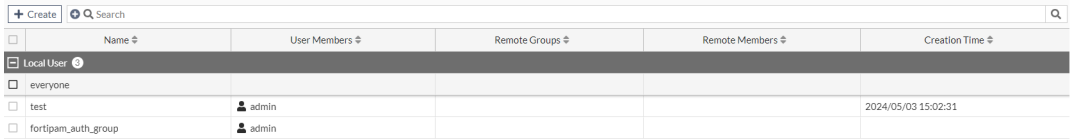


User groups

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.



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.

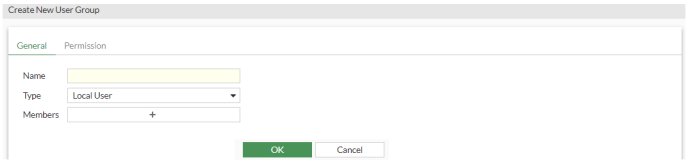
The *User Groups* tab contains the following options:

Create	Select to create a new user group.
Edit	Select to edit the selected user group.

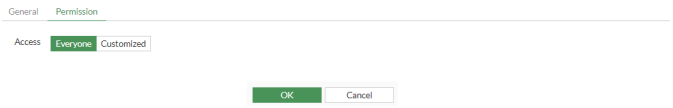
Delete	Select to delete the selected user groups.
Search	Enter a search term in the search field, then hit `Enter` to search the user groups list. To narrow down your search, see Column filter.

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.



3. To switch to the *Permission* tab, select the tab.



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 263. 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 284. **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 301.



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 312.

   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.

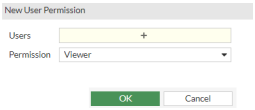


Alternatively, use the CLI commands to create a user group.

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.



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 263, 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.

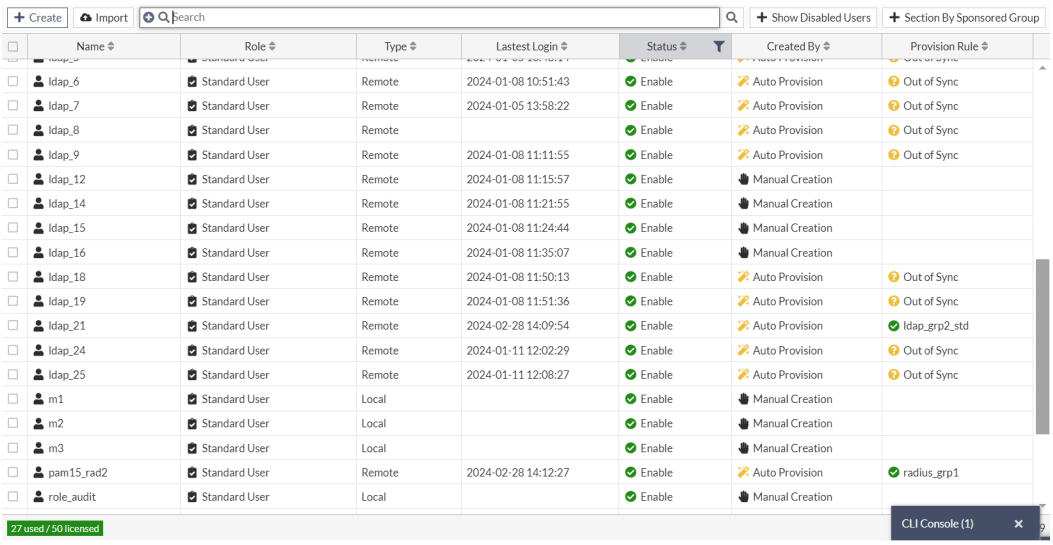
Based on the predefined auto provision rules, remote users can be auto provisioned upon their first successful login without requiring the manual creation of a user in the system prior to login:

- 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*.



The order of the rules impacts the login matching. First, the rule is matched from top to bottom.

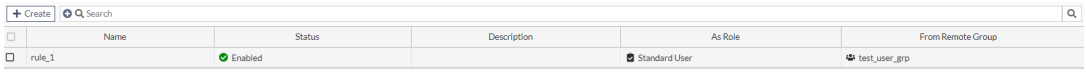
The rules can be reordered by dragging a rule up/down from the left-most row.

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*



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 309.
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 311.

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.

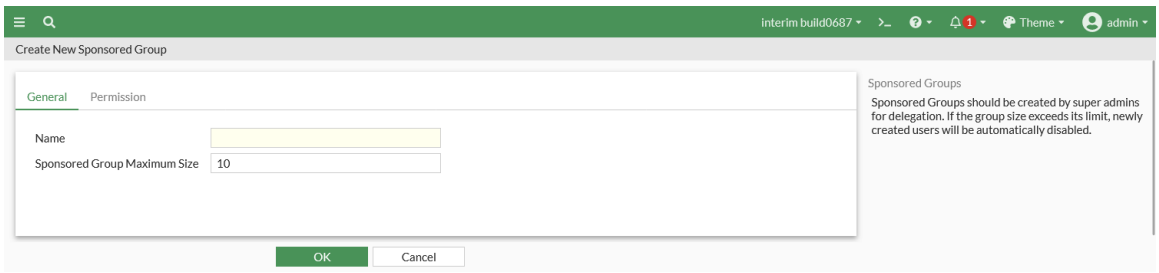


The *Sponsored Groups* tab contains the following options:

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:

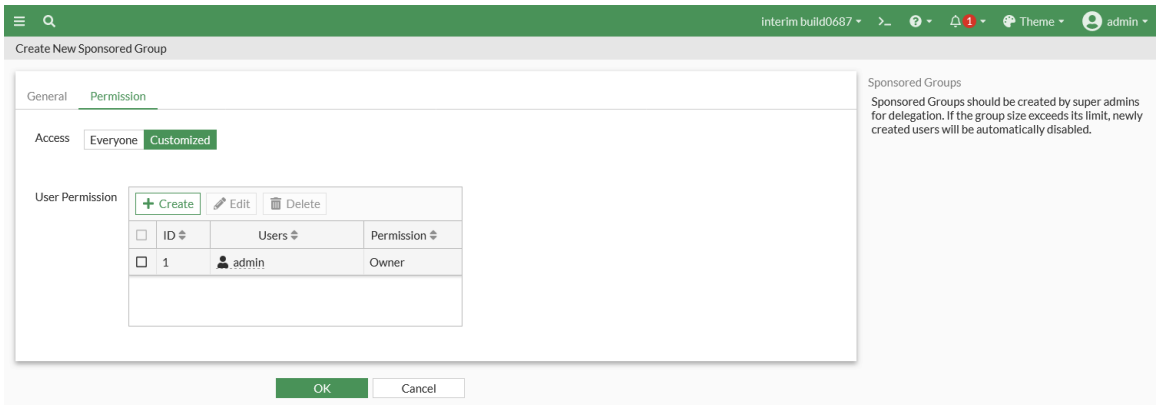
1. Go to *User Management* > *Sponsored Groups*.
2. Select *Create* to create a new user group.
   The *General* tab in the *Create New Sponsored Group* window opens.



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.



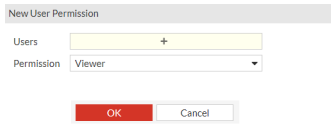
5. In the *Permission* tab, enter the following information:

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 288. **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.



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 263, 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 263.



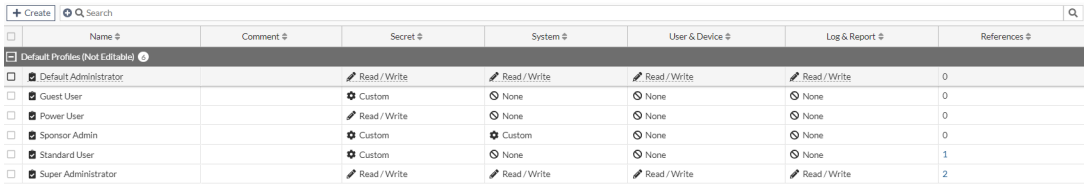
When you create a standard user, a default normal user role is assigned to the new user automatically.



When setting up an administrator, administrator roles can be selected from the *Choose an Adminstrator Role* dropdown. See Creating a user on page 263.

The administrator role decides what the administrator can see.

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



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.

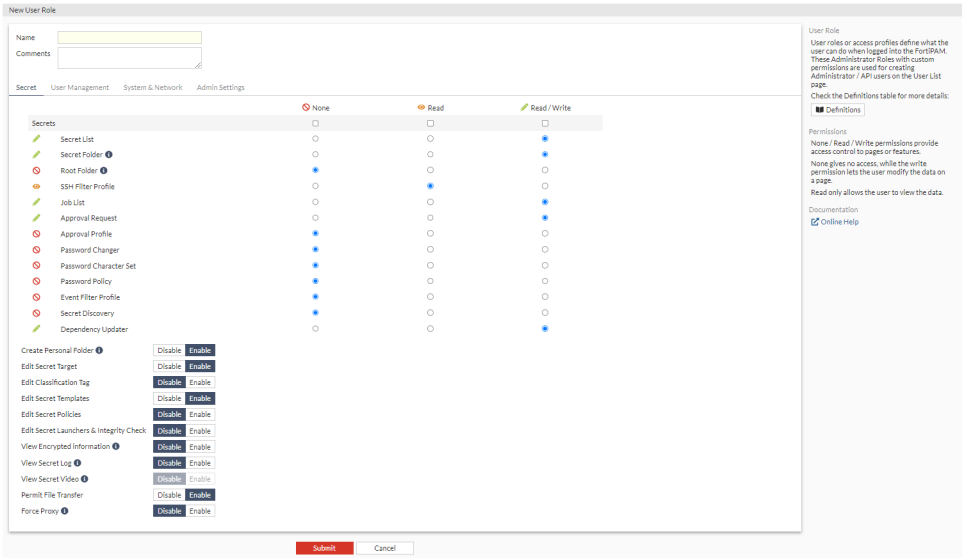
- *Super Administrator*: Privilege to manage and monitor the FortiPAM device.

  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.



   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.

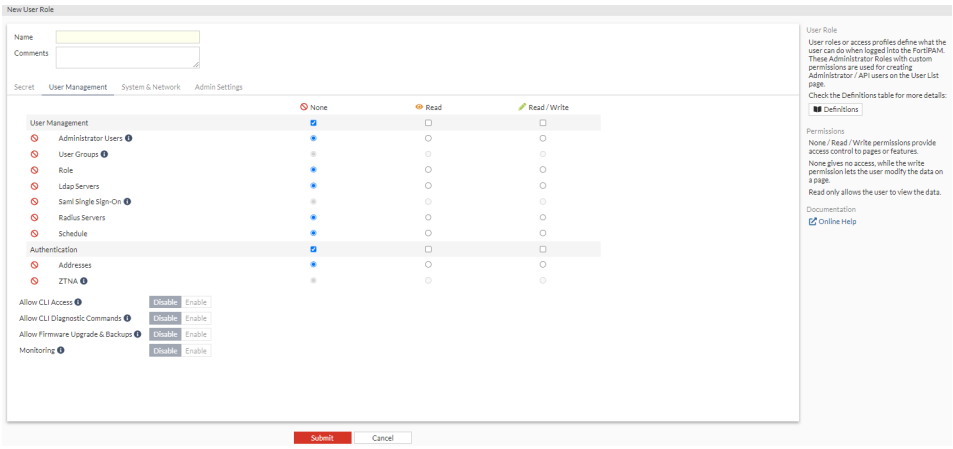
     Note: When an administrator has only read access to a feature, the administrator can access the GUI page and can use the `get` and `show` CLI command for that feature, but cannot make changes to the configuration.
   - *Read/Write*: View, change, and execute access.

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.

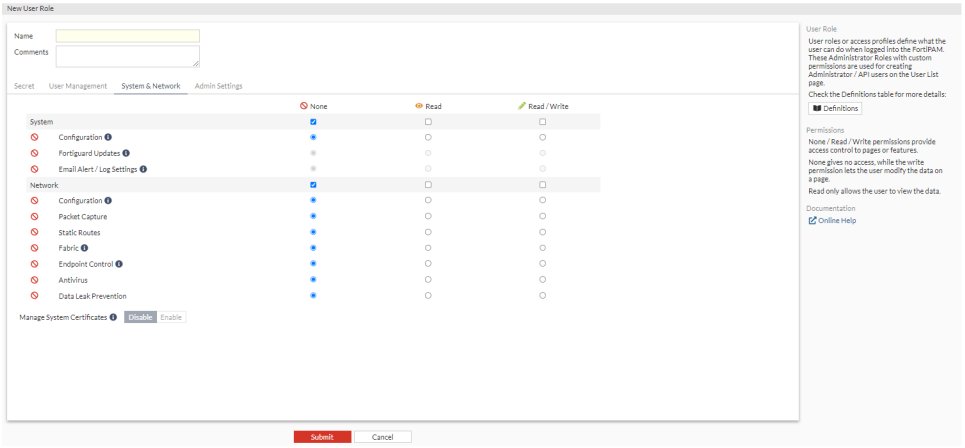


4. Enter the following information:

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.

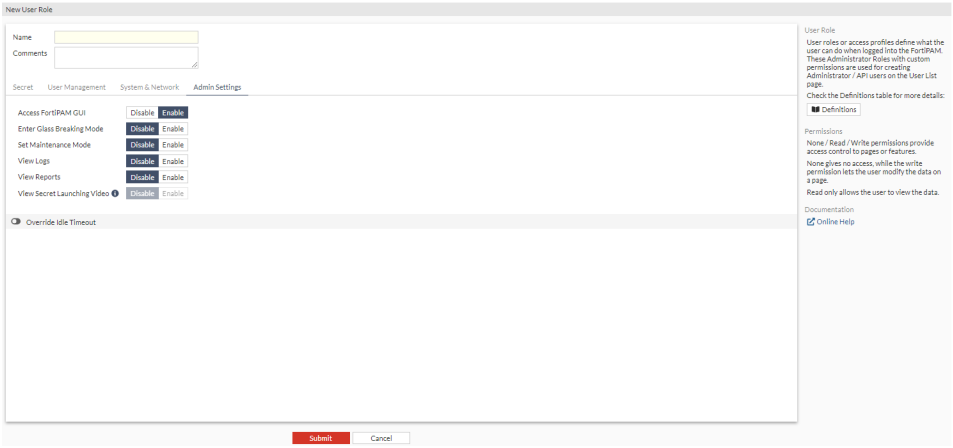


6. Enter the following information:

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 462 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.



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.

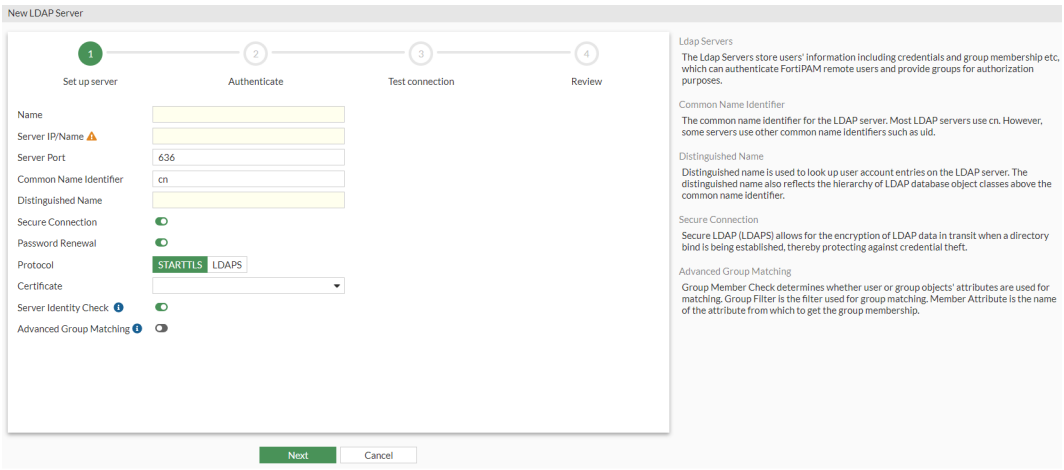


The *LDAP server* tab contains the following options:

Create	Select to create an LDAP server.
Edit	Select to edit the selected LDAP server.
Delete	Select to delete the selected LDAP roles.
Search	Enter a search term in the search field, then hit `Enter` to search the LDAP servers list. To narrow down your search, see Column filter.

To create an LDAP server:

1. Go to *User Management* > *LDAP servers*, and select *Create*.
   The *New LDAP Server* wizard opens.



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

Set up server	
Name	Name of the server.
Server IP/name	The IP address or FQDN for this remote server.
Server Port	The port number for LDAP traffic (default = 636).
Common Name Identifier	The common name identifier for the LDAP server. Most LDAP servers use `cn`. However, some servers use other common name identifiers such as `UID`. (default = `cn`).
Distinguished Name	The distinguished name is used to look up entries on the LDAP server. The distinguished name reflects the hierarchy of LDAP database object classes above the common name identifier.
Secure Connection	Enable to use a secure LDAP server connection for authentication. Secure LDAP (LDAPS) allows for the encryption of LDAP data in transit when a directory bind is being established, thereby protecting against credential theft. **Note**: This option is enabled by default.
Password Renewal	Enable to allow LDAP users to renew passwords. **Note**: This option is only available when *Secure Connection* is enabled. **Note**: This option is enabled by default.
Protocol	When *Secure Connection* is enabled, select either *LDAPS* or *STARTTLS* (default).
Certificate	When *Secure Connection* is enabled, select the certificate from the dropdown.  Use the search bar to look up a certificate.
Server Identity Check	Enable to verify server domain name/IP address against the server certificate.

	Note: This option is only available when *Secure Connection* is enabled. **Note**: This option is enabled by default.
Advanced Group Matching	Group member check determines whether user or group objects' attributes are used for matching. Group Filter is the filter used for group matching. Member attribute is the name of the attribute from which to get the group membership.  Depending on the LDAP server, you may need to configure additional properties to ensure LDAP groups are correctly matched. **Note**: The option is disabled by default.
Group Member Check	From the dropdown, select a group member check option (default = `Ldap::grp::member::check:user-attr`).
Group Filter	Enter the group filter for group matching.
Group Search Base	Enter the search base used for searching a group.
Member Attribute	Specify the value for this attribute. This value must match the attribute of the group in LDAP server. All users part of the LDAP group with the attribute matching the attribute will inherit the administrative permissions specified for this group (default = `memberof`).
Authenticate	
Username	The username.
Password	The password.

3. Click *Test connection* to test the connection to the LDAP server.

 *Test connection* is only available to users who have *Write* permission for *Ldap Servers*. See Role on page 289.

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 280.
3. Configuring the administrator account. See Creating a user on page 263.

SAML Single Sign-On (SSO)

SAML SSO can be configured in *User Management*.

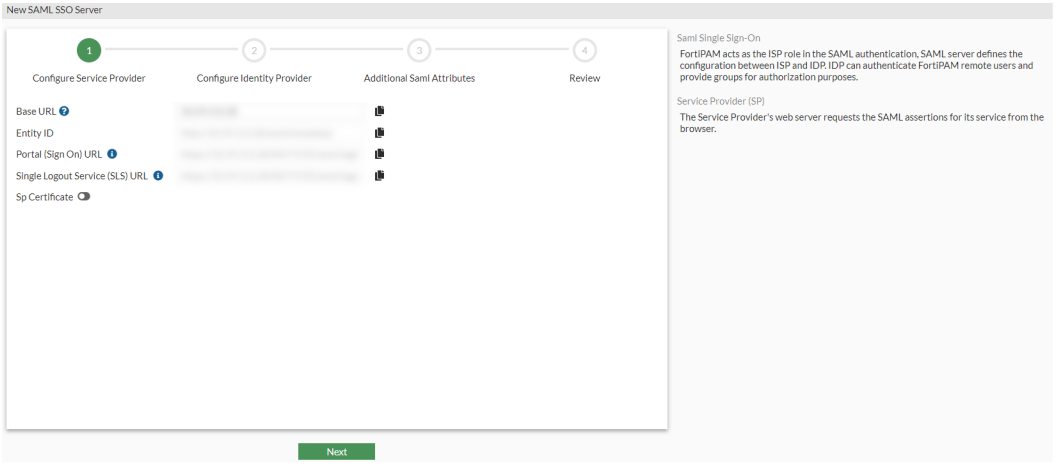
FortiPAM acts as the SP in SAML authentication. The SAML server defines the configuration between SP and IdP. An IdP can authenticate FortiPAM remote users and provide groups for authorization.

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 263.
Alternatively, you can automatically provision the remote SAML user.
See Creating an auto provision rule on page 309.

1. Go to *User Management* > *Saml Single Sign-On*.



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

Configure Service Provider	
Base URL	The URL where the Identity Provider (IdP) sends SAML authentication requests. **Note**: The address should be WAN-accessible and can be an IP address or an FQDN. **Note**: To include a port, append it after a colon. For example: `200.1.1.1.:443`.
Entity ID	Enter the SP entity ID.
Portal (Sign On) URL	The SAML service provider login URL. The URL is used to initiate a single sign-on. **Note**: Not all IdPs require a *Portal (Sign On) URL*. **Note**: The *Portal (Sign On) URL* is alternatively referred to as the Portal URL or the Sign On URL.
Single Logout Service (SLS) URL	The SP Single Logout Service (SLS) logout URL. The IdP sends the logout response to this URL. **Note**: The *Single Logout Service (SLS) URL* is alternatively referred to as the SLS URL, Single Logout Service URL, or the Logout URL.
Sp Certificate	Enable this option and import the SP certificate for authentication request signing by the SP. **Note**: This option is disabled by default.
Configure Identity Provider An IdP provides SAML assertions for the service provider and redirects the user's browser back to the service provider web server.	
Log in to the IdP to find the following information.	

Type	Select either *Fortinet Product* or a *Custom* IdP.
IdP Address	The IdP address. **Note**: This option is only available when the *Type* is *Fortinet Product*.
Prefix	Enter the IdP prefix. **Note**: The prefix is appended to the end of the IdP URLs. **Note**: This option is only available when the *Type* is *Fortinet Product*.
IdP Certificate	Select a server certificate to use for the SP.  Whenever the configuration changes on the IdP, you need to upload the new certificate reflecting the changes.
IdP entity ID	The IdP's entity ID, for example: `http://www.example.com/saml-idp/xxx/metadata/` **Note**: This option is only available when the *Type* is *Custom*.
IdP single sign-on URL	The IdP's login URL, for example: `http://www.example.com/saml-idp/xxx/login/` **Note**: This option is only available when the *Type* is *Custom*.
IdP single logout URL	The IdP's logout URL, for example: `http://www.example.com/saml-idp/xxx/logout/` **Note**: This option is only available when the *Type* is *Custom*.
Additional Saml Attributes FortiPAM looks for the attributes to verify authentication attempts. Configure your IdP to include the attributes in the SAML attribute statement.	
Attribute used to identify users	Enter the SAML attribute used to identify the users.
Attribute used to identify groups	Enter the SAML attribute used to identify the groups.
AD FS claim	Enable AD FS claim. **Note**: This option is disabled by default.
User claim type	From the dropdown, select a user claim type (default = `User Principal Name`).
Group claim type	From the dropdown, select a group claim type (default = `User Group`).

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

 Use the pen icon to edit tabs.



Alternatively, use the CLI commands to configure an IdP.

CLI configuration to set up a SAML IdP - example**:**

```
config user saml
   edit <SAML Name>
      set entity-id "http://<PAM_VIP>/saml/metadata/"
      set single-sign-on-url "https://<PAM_VIP>/XX/YY/ZZ/saml/login/"
      set single-logout-url "https://<PAM_VIP>/remote/saml/logout/"
      set idp-entity-id "http://<iDP URL>/<idp_entity_id>"
      set idp-single-sign-on-url "https://<iDP_URL>/<sign_on_url>"
      set idp-single-logout-url "https://<iDP_URL>/<sign_out_url>"
      set idp-cert <iDP Certificate>
      set user-name "username"
      set group-name "group"
      set digest-method sha256
   next
end
config firewall access-proxy
   edit "fortipam_access_proxy"
      set vip "fortipam_vip"
      config api-gateway
         edit 4
            set service samlsp
            set saml-server "fortipam-saml-sso-server"
         next
      end
   next
end
config authentication scheme
   edit "fortipam_saml_auth_scheme"
      set method saml
      set saml-server "fortipam-saml-sso-server"
   next
end
config authentication rule
   edit "fortipam_saml_auth_rule" #Create a new rule and move it above the default
        "fortipam_auth" rule.
      set srcaddr "all"
      set dstaddr "saml_auth_addr"
      set ip-based disable
      set active-auth-method "fortipam_saml_auth_scheme"
      set web-auth-cookie enable
   next
   edit "fortipam_auth"
      set srcaddr "all"
      set ip-based disable
      set active-auth-method "fortipam_auth_scheme"
      set web-auth-cookie enable
   next
end
```

CLI configuration to enable SAML authentication on the login page - example

```
config system global
   set saml-authentication enable
end
```

To log in to FortiPAM as a SAML user:

1. On the login page, from the *Local* dropdown, select *SAML*.
2. Select *Continue* to open the SAML login page.
3. Enter the username and password to log in to FortiPAM.

Auto provision rules

Auto Provision Rules in *User Management* displays a list of auto provision rules for remote users.

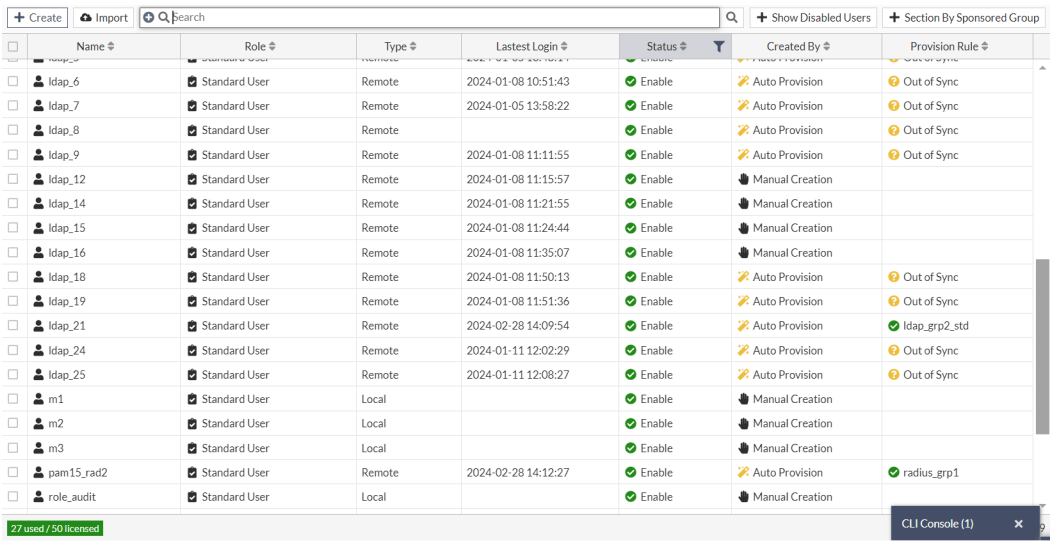
Based on the predefined auto provision rules, remote users can be auto provisioned upon their first successful login without requiring the manual creation of a user in the system prior to login:

- 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*.



The order of the rules impacts the login matching. First, the rule is matched from top to bottom.

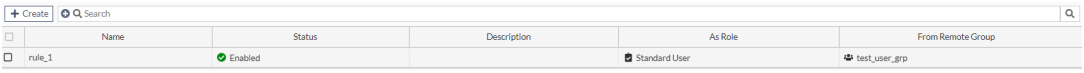
The rules can be reordered by dragging a rule up/down from the left-most row.

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*



The *Auto Provision Rules* tab contains the following options:

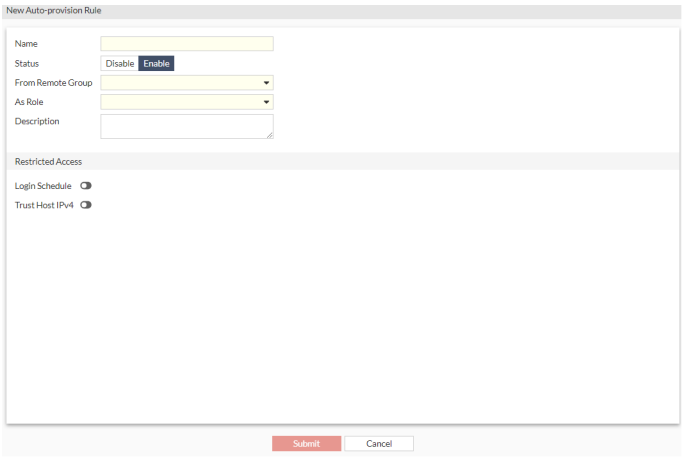
Create	Select to create a new auto provision rule. See Creating an auto provision rule on page 309.
Search	Enter a search term in the search field, then hit `Enter` to search the auto provision rules list. To narrow down your search, see Column filter.
Edit	Select to edit the selected auto provision 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 311.

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.



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 289, 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 314.
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.

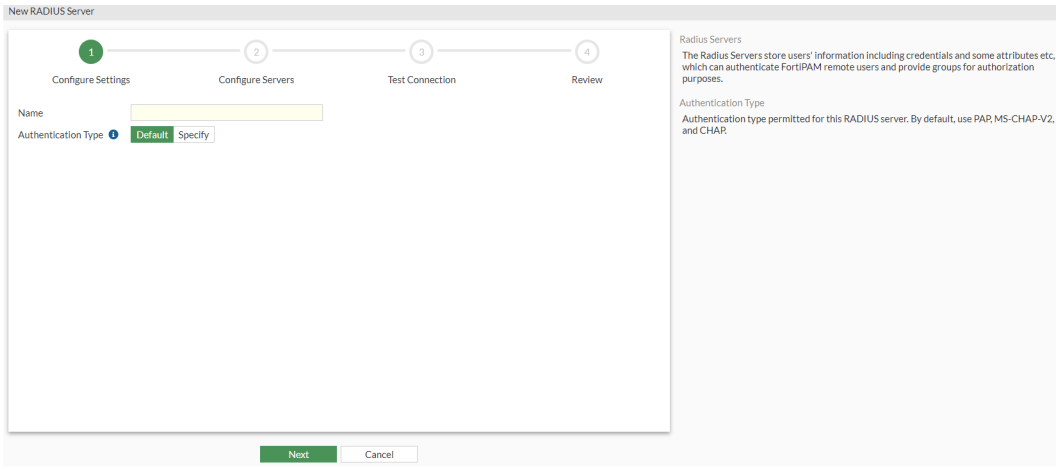


The *Radius servers* tab contains the following options:

Create	Select to create a new RADIUS server.
Edit	Select to edit the selected RADIUS server.
Clone	Select to clone the selected RADIUS server.
Delete	Select to delete the selected RADIUS servers.
Search	Enter a search term in the search field, then hit `Enter` to search the RADIUS server list. To narrow down your search, see Column filter.

To create a RADIUS server:

1. Go to *User Management* > *Radius Servers*, and select *Create*.
   The *New RADIUS Server* wizard opens.



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

Configure Settings	
Name	The name of the RADIUS server.
Authentication Type	Select either *Default* or *Specify*. If *Specify* is selected, from the dropdown, select from the following authentication types: • *CHAP*: Challenge Handshake Authentication Protocol.

	• *MS-CHAP*: Microsoft Challenge Handshake Authentication Protocol. • *MS-CHAP-V2*: Microsoft Challenge Handshake Authentication Protocol version 2. • *PAP*: Password Authentication Protocol.
Configure Servers	
Primary Server	The access request is always be sent to the primary server first. If the request is denied with an `Access-Reject`, then the user authentication fails.
IP/Name	The IP address or the FQDN.
Secret	The pre-shared passphrase used to access the RADIUS server.
Secondary Server	If there is no response from the primary server, the access request is sent to the secondary server.
IP/Name	The IP address or the FQDN.
Secret	The pre-shared passphrase used to access the RADIUS server.

3. Click *Test connection* to test the connection to the RADIUS server.
   If the credentials to the server are valid, it shows *Successful*.
4. In the *Review* tab, verify the information you entered and click *Submit* to create the RADIUS server.



Use the pen icon to edit tabs.



Alternatively, use the CLI commands to create RADIUS servers.

CLI configuration to set up a RADIUS server - example**:**

```
config user radius
   edit <radius_server_name>
      set server <server_ip>
      set secret <secret>
   next
end
config authentication scheme
   edit "fortipam_auth_scheme"
      set method form
      set user-database "local-admin-db" <radius_server_name>
   next
end
```

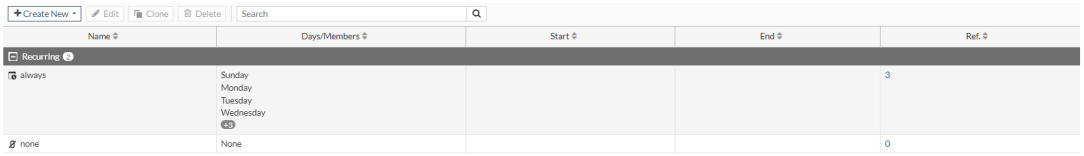
Setting up RADIUS authentication includes the following steps:

1. Configure the RADIUS server. Configuring a RADIUS server.
2. Adding the RADIUS server to a user group. User groups on page 280.
3. Configuring a RADIUS user. Creating a user on page 263.

Schedule

Schedule can be configured in *User Management*.

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

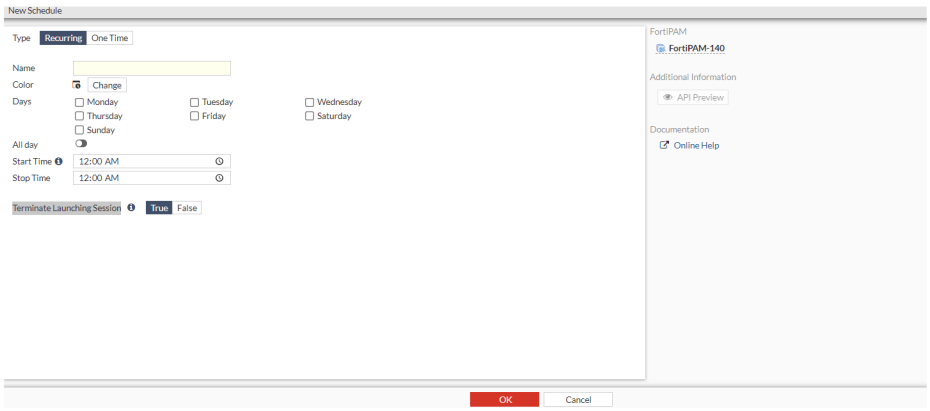


The *Schedule* tab contains the following options:

Create	Select to create a new schedule.
Edit	Select to edit the selected schedule.
Clone	Select to clone the selected schedule.
Delete	Select to delete the selected schedules.
Search	Enter a search term in the search field, then hit `Enter` to search the schedule list.

To create a schedule:

1. Go to *User Management* > *Schedule*.
2. From the *Create* dropdown, select *Schedule*.
   The *New Schedule* window opens.



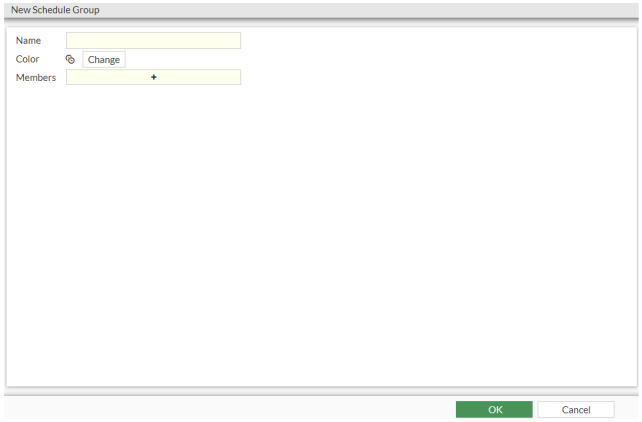
3. In the *New Schedule* window, enter the following information:

Type	Select either *Recurring* or *One Time*.
Name	The name of the schedule.
Color	Select *Change* and then select a color.
Days	Select the days of the week when the schedule applies. **Note**: This option is only available when the *Type* is *Recurring*.
All day	Enable to apply the schedule all day. **Note**: This option is only available when the *Type* is *Recurring*.
Start Date	Enter the start date and time. Alternatively, select the calendar icon and then select a date. Similarly, select the clock icon and then select a time. **Note**: This option is only available when the *Type* is *One Time*.
Start Time	Enter the start time. Alternatively, select the clock icon and then select a start time. **Note**: This option is only available when the *Type* is *Recurring* and *All day* is disabled.
End Date	Enter the end date and time. Alternatively, select the calendar icon and then select a date. Similarly, select the clock icon and then select a time. **Note**: This option is only available when the *Type* is *One Time*.
Stop Time	Enter the stop time. Alternatively, select the clock icon and then select a stop time.  If the stop time is set earlier than the start time, the stop time is the same time the next day. **Note**: This option is only available when *Type* is *Recurring* and *All day* is disabled.
Pre-expiration event log	Select to create an event log *Number of days* before the *End Date*. **Note**: This option is only available when the *Type* is *One Time*.
Number of days before	Enter the number of days (1 - 100, default = 3). **Note**: This option is only available when the *Type* is *One Time* and *Pre-expiration event log* is enabled.
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.



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

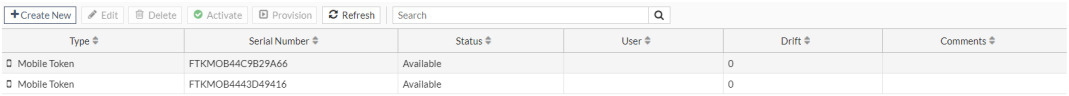
Go to *User Management* > *FortiTokens* to view a list of configured FortiTokens.

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 289.

For each FortiToken; type, serial number, status, user, drift, and comments are displayed by default.

To add the *License* column, click *Configure Table* when hovering over table headers, select *License*, and click *Apply*.

By default, two FortiTokens are available.

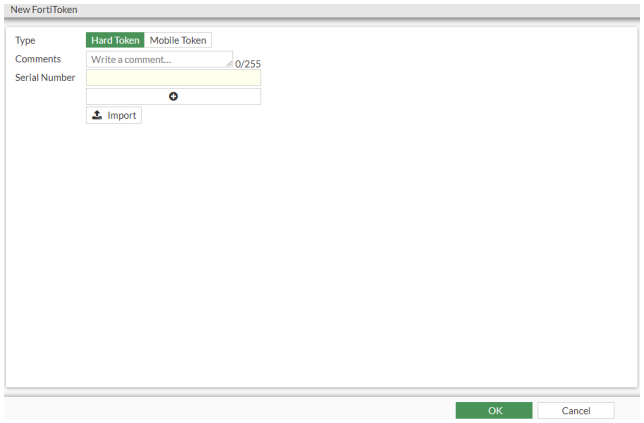


The following information is shown on the *FortiTokens* tab:

Create New	Create a new FortiToken.
Edit	Edit the selected FortiToken.
Delete	Delete the selected FortiToken(s).
Activate	Activate the selected FortiToken(s).
Provision	Provision the selected FortiToken(s).
Refresh	Refresh FortiToken(s).
Search	Search the FortiToken list.

To add FortiTokens:

1. Go to *User Management* > *FortiTokens*, and select *Create*.
   The *New FortiToken* window opens.



2. Enter the following information:

Type	The token type: • *Hard Token* • *Mobile Token*
Comments	Optionally, enter comments about the token. **Note**: This option is only available when the *Type* is *Hard Token*.
Serial Number	The FortiToken serial number.  To add multiple FortiTokens, select + and enter a new serial number. **Note**: This option is only available when the *Type* is *Hard Token*.
Activation Code	The activation code. **Note**: This option is only available when the *Type* is *Mobile Token*.
Import	Select the option to import multiple tokens by selecting one of the following and clicking *OK*: • *Serial Number File*: Select *Upload* to load a CSV file that contains token serial numbers.  FortiToken devices have a serial number barcode on the m used to create the import file. • *Seed File*: Select *Upload* to load a CSV file that contains token serial numbers, encrypted seeds, and IV values. **Note**: This option is only available when the *Type* is *Hard Token*.

3. Click *OK*.

Monitoring FortiTokens

You can also view the list of FortiTokens, their status, token clock drift, and which user they are assigned to from the FortiToken list found at *User Management* > *FortiTokens*.

Monitoring

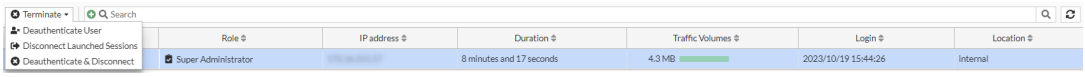
Go to *Monitoring* to access the following tabs:

- User monitor on page 319
- Active sessions on page 319

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.



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.

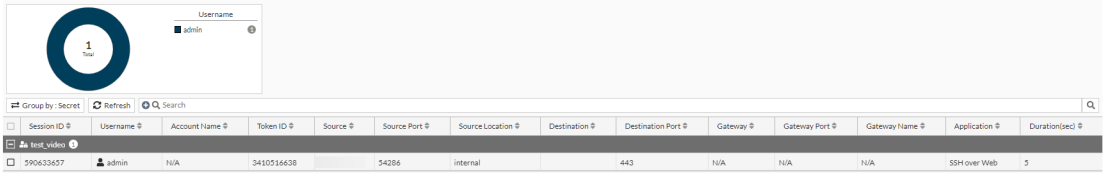
Disconnecting native non-proxy sessions is currently not supported.

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:

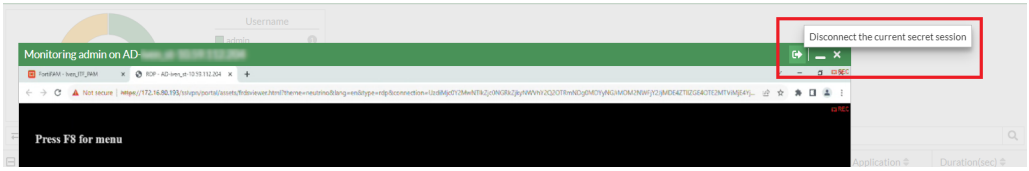
- *Session ID*
- *Username*
- *Account Name*
- *Token ID*
- *Source*
- *Source Port*
- *Source Location*
- *Destination*: The actual target server IP address.
- *Destination Port*
- *Gateway*: The gateway IP address.
- *Gateway Port*
- *Gateway Name*: The gateway name.
- *Application*
- *Duration (sec)*



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.



For information on over-the-shoulder monitoring, see Over-the-shoulder monitoring (Live recording) on page 321.

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.

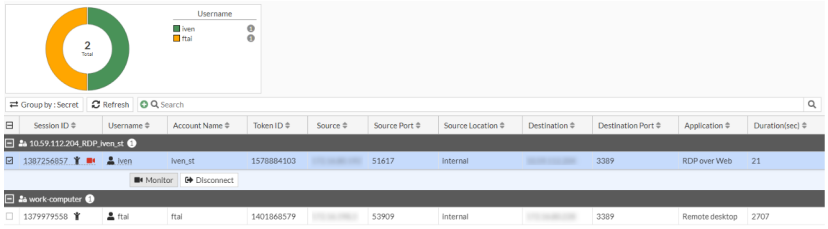
To ensure seamless real-time video recording and transmission to FortiPAM, consider the following system resource guidelines for launching multiple concurrent sessions:

- CPU: 8 logical processors
- Memory: 16 GB

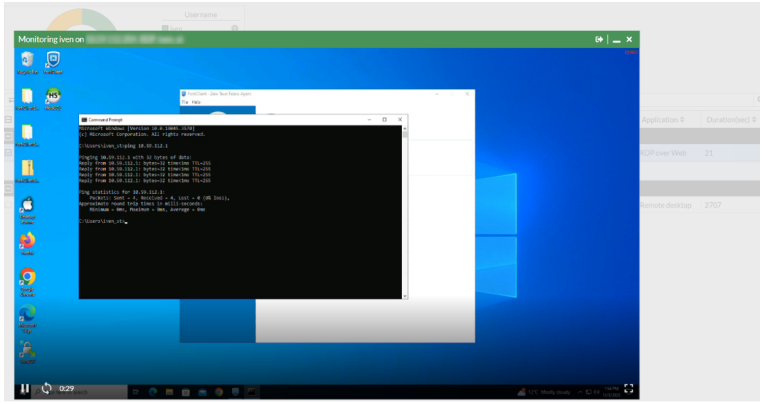
To monitor the user secret session in real-time:

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.



A new window opens. The window displays user activity in real-time.





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.

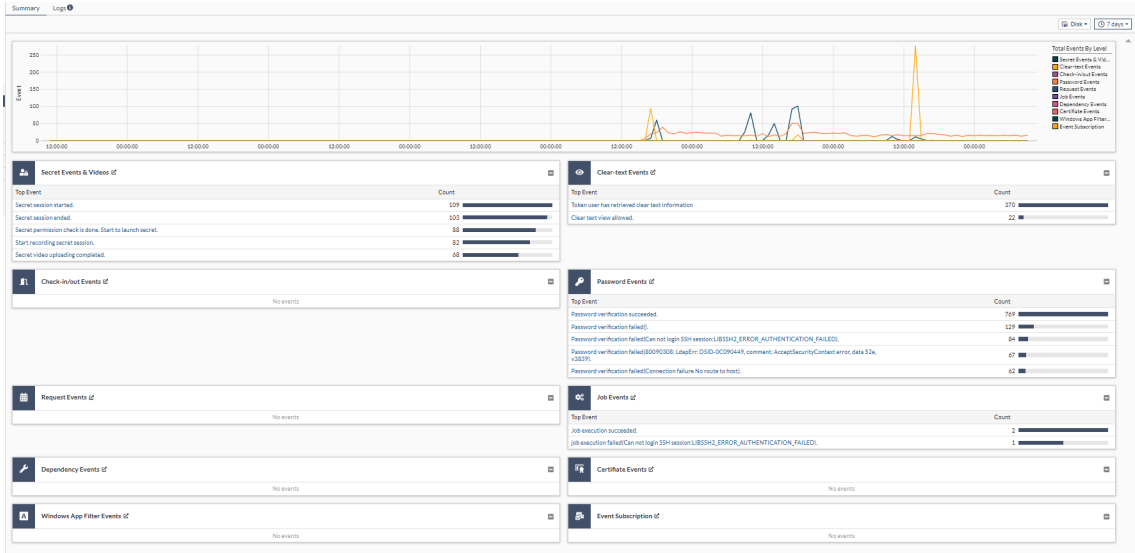
Go to *Log & Report* to access the following tabs:

- Secret event & video on page 323
- System event on page 328
- Security event on page 330
- ZTNA traffic on page 333
- Disk usage on page 334
- Automation on page 336
- Reports on page 346
- Log settings on page 354
- Email alert settings on page 361
- Debug settings on page 363

Secret event & video

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

- Secret Events & Videos on page 325
- Clear Text Events on page 325
- Check-in/out Events on page 326
- Password Events on page 326
- Request Events on page 327
- Job Events on page 327
- Dependency Events on page 327
- Certificate Events on page 327
- Windows App Filter Events on page 327
- Event Subscription on page 328



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

Log Location	Select a source from where to retrieve logs: • *Disk* (default) (FortiPAM)
Time frame	From the dropdown, select from the following time filters: • *5 minutes* • *1 hour* • *24 hours* • *7 days*

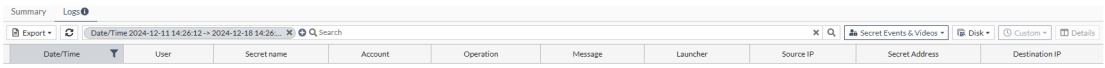
The following options are available in the *Logs* tabs:

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*
Refresh	To refresh the contents, click the refresh icon.
+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.

Secret Events & Videos	From the dropdown, select a tab to display: • *Secret Events & Videos* • *Clear-text Events* • *Check-in/out Events* • *Password Events* • *Request Events* • *Job Events* • *Dependency Events* • *Certificate Events* • *Windows App Filter Events* • *Event Subscription*
Log location	Select a source from where to retrieve logs: • *Disk* (default) (FortiPAM) • *FortiAnalyzer* See FortiAnalyzer logging on page 379 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* • *View All*
Details	Select to see details for the selected log entry.

Secret Events & Videos

Clicking *Secret Events & Videos* opens all the secret logs and videos. Different subcategories of secret logs are displayed when you click on a secret log.



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 Events

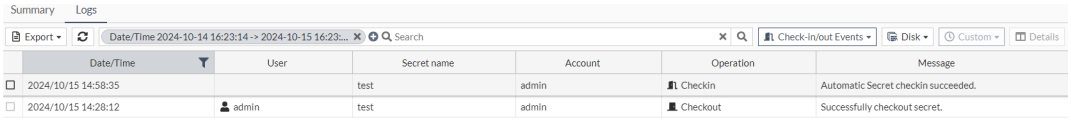
Selecting *Clear Text Events* shows logs related to viewing passwords. This category of the secret log shows all the information related to the launching of a secret, uploading of a video, termination of a launched session, and status of a

FortiPAM token.



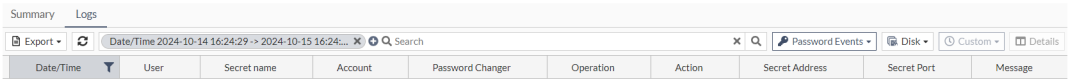
Check-in/out Events

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



Password Events

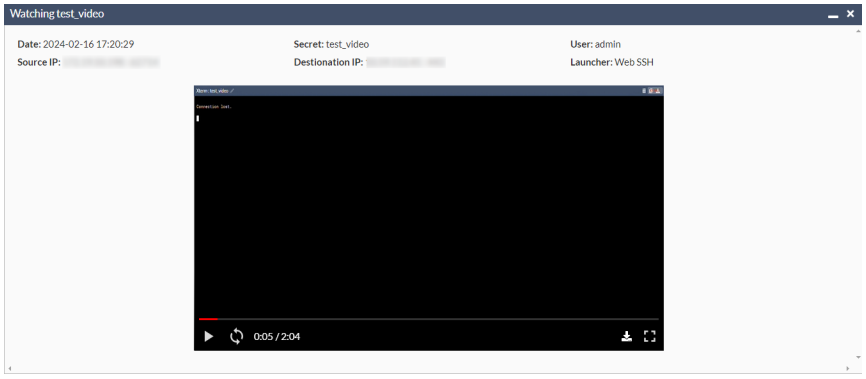
Selecting *Password Events* shows logs related to password changers. It displays all the information about when a password changer is triggered on a secret. It indicates whether the operation is successful and who initiated the operation. Operations such as password verification or change of password are recorded here.



For some column descriptions, see Secret Events & Videos on page 325.

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.



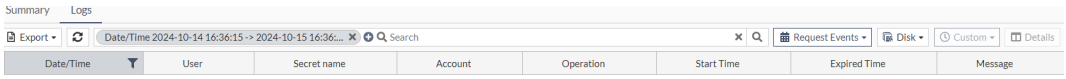
To download a recorded video of a launched secret:

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.

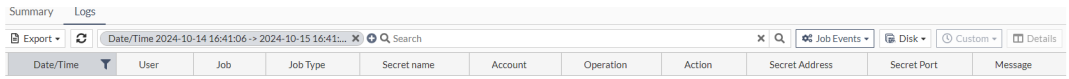
Request Events

Selecting *Request Events* shows logs related to secret requests. This category of the secret log shows all the information related to a secret that requires secret approval. It indicates when a request is submitted for a secret or when a request is approved or denied.



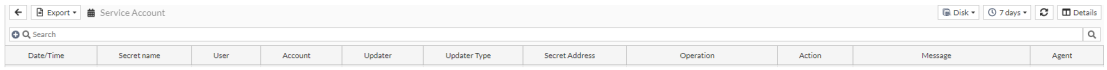
Job Events

Selecting *Job Events* 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.



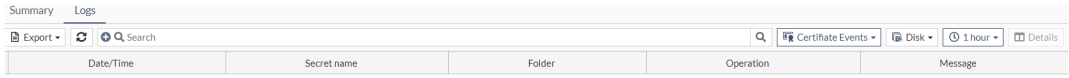
Dependency Events

Selecting *Dependency Events* 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.



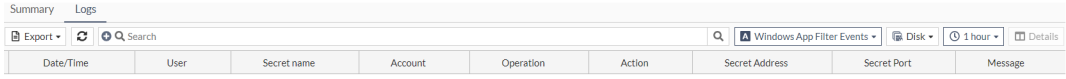
Certificate Events

Selecting *Certificate Events* shows all the logs related to *Certificate* secret. This category of the secret log shows information related to the certificate status.



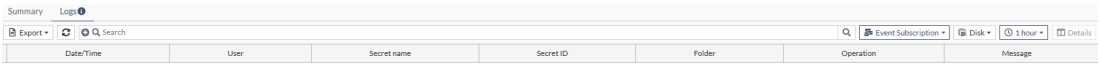
Windows App Filter Events

Selecting *Windows App Filter Events* 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.



Event Subscription

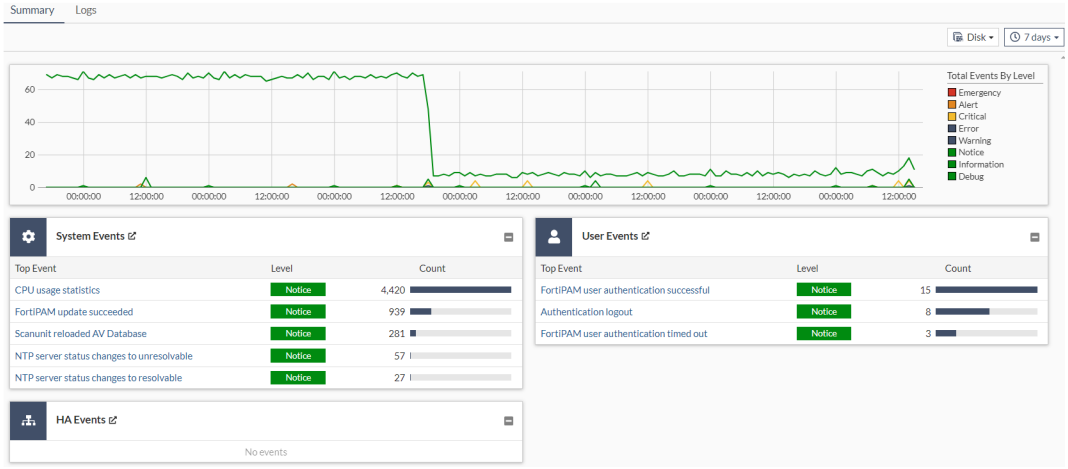
Selecting *Event Subscription* shows all the logs related to an RDP session from the target.



System event

The following two tabs are available in *System Event*:

- *Summary*
  The *Summary* tab displays the top five most frequent events in each type of event log and a line chart to show aggregated events by each severity level. Clicking on a peak in the line chart will display the specific event count for the selected severity level.
  There is an option for the line chart to change the time filter in which the events occurred, from 5 minutes to 7 days.
  The following shows the *Summary* tab:



  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:

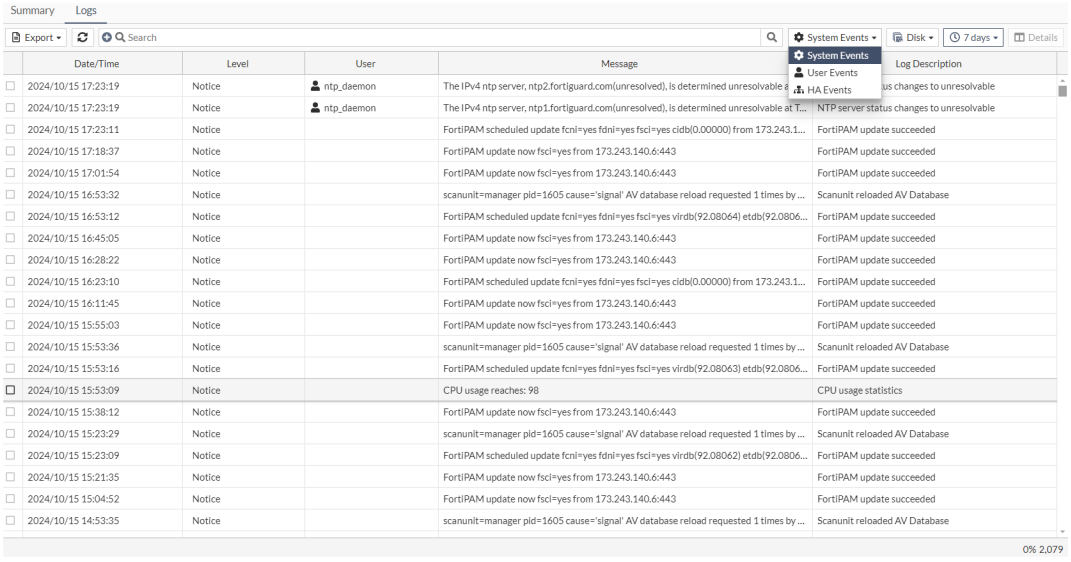
Log location	Logs sourced from the FortiPAM disk only.
Time frame	From the dropdown, select from the following time filters: • *5 minutes* • *1 hour* • *24 hours* • *7 days*
System Events	Top system events by count.
User Events	Top user events by count.
HA Events	Top HA events by count.



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.

- *Logs*

The tab displays the related information of each log for a specific event type. The event type can be toggled with the event type dropdown located right of the search bar. Different filters can be added, such as date/time to filter logs in a time range.



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

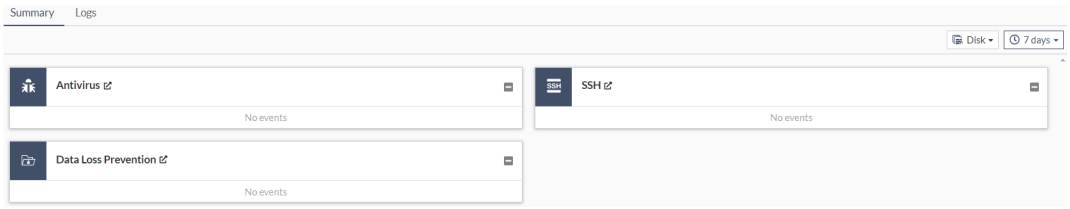
Export	From the *Export* dropdown, select to export the logs in the following three formats: • *JSON*: Export the selected log to your computer as a JSON file • *CSV*: Export the selected log to your computer as a CSV file

	• *TEXT*: Export the selected log to your computer as a text file
Refresh	To refresh the contents, click the refresh icon.
+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* • *View All*
Details	Select a log entry and then select *Details* to see more information about the log.

Security event

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

- Antivirus on page 332
- SSH on page 332
- Data Loss Prevention on page 333



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

Log Location	Select a source from where to retrieve logs: • *Disk* (default) (FortiPAM)
Time frame	From the dropdown, select from the following time filters: • *5 minutes* • *1 hour* • *24 hours* • *7 days*

The following options are available in the *Logs* tabs:

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*
Refresh	To refresh the contents, click the refresh icon.
+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.
Antivirus	From the dropdown, select a tab to display: • *Antivirus* • *SSH* • *Data Loss Prevention*
Log location	Select a source from where to retrieve logs: • *Disk* (default) (FortiPAM)
Time frame	From the dropdown, select from the following time filters: • *5 minutes* • *1 hour* • *24 hours* • *7 days* • *View All*
Details	Select to see details for the selected log entry.

Antivirus

Selecting *Antivirus* displays logs related to antivirus.

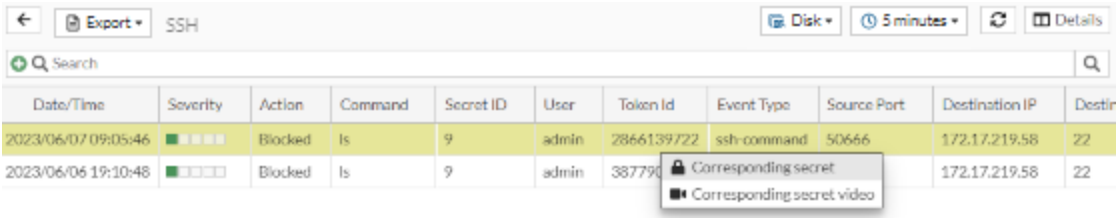
The antivirus log records when, during the antivirus scanning process, the FortiPAM unit finds a match within the antivirus profile, which includes the presence of a virus or grayware signature.

SSH

Selecting *SSH* displays logs related to SSH.

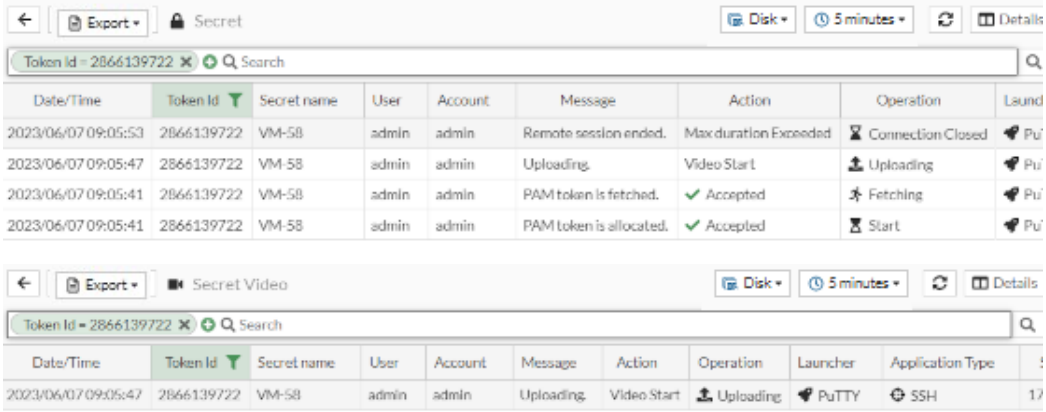
For each SSH log, the following columns are displayed:

- *Date/Time*
- *Severity*
- *Command*
- *Secret ID*
- *User*
- *Message*
- *Source IP*
- *Source Port*
- *Destination IP*
- *Destination Port*



Selecting the *Corresponding secret* or the *Corresponding secret video* buttons when you right-click an SSH log takes you to the corresponding secret log or the secret video log, respectively.





The SSH log keeps track of all the events related to the SSH filter profile. It contains information such as the severity of a command, the destination IP and port used to execute the command, and the action associated with the log. The action may be *Blocked*, indicating the command has been blocked from executing on the secret or *Passthrough*, representing it is allowed to execute on the secret.

Data Loss Prevention

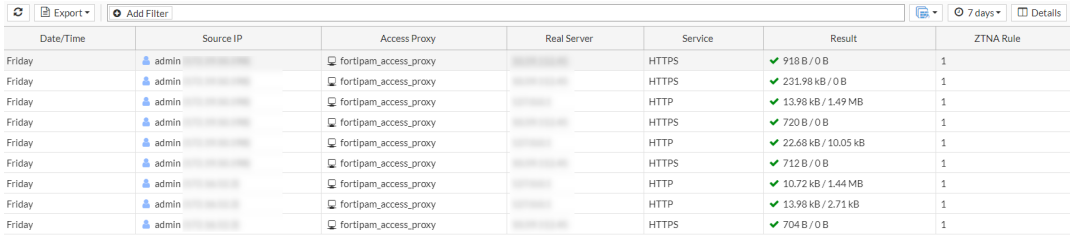
Selecting *Data Loss Prevention* displays logs related to DLP.

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.

ZTNA traffic

Go to *ZTNA traffic* in *Log & Report* to see ZTNA related logs.

The ZTNA log keeps track of ZTNA related traffics. This can include when a ZTNA rule cannot be matched, an API gateway cannot be matched, or when a secret configured with device permission fails to connect.



The following options are available in the *ZTNA traffic* tab:

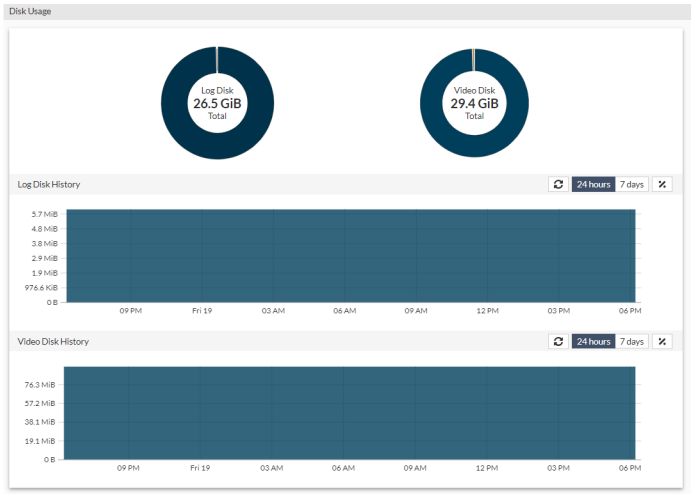
Refresh	To refresh the contents, click the refresh icon.
Export	From the *Export* dropdown, select to export the ZTNA logs in the following three formats: • *JSON*: Export the selected ZTNA log to your computer as a JSON file • *CSV*: Export the selected ZTNA log to your computer as a CSV file • *TEXT*: 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 System event on page 328, for an example on how to set up custom filters.
Details	Select to see details for the selected log entry.

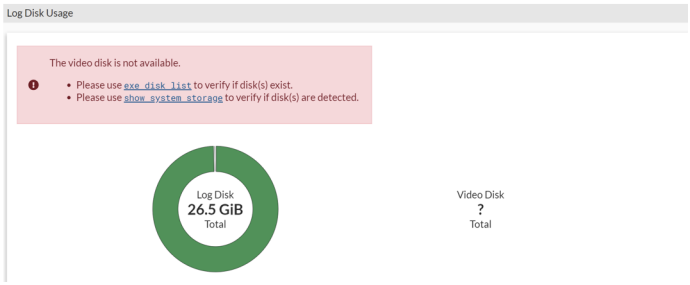
Disk usage

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.

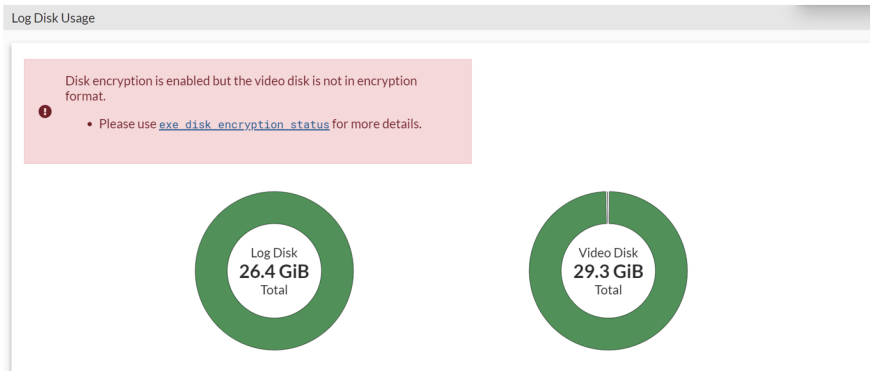


When the video disk is unavailable, the following warning is displayed:



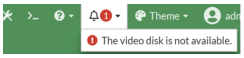
A similar warning is displayed when the log disk is unavailable.

When disk encryption is enabled but the video disk is not in encryption format, the following warning is displayed:



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.



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 336
- Trigger on page 343
- Action on page 345

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:

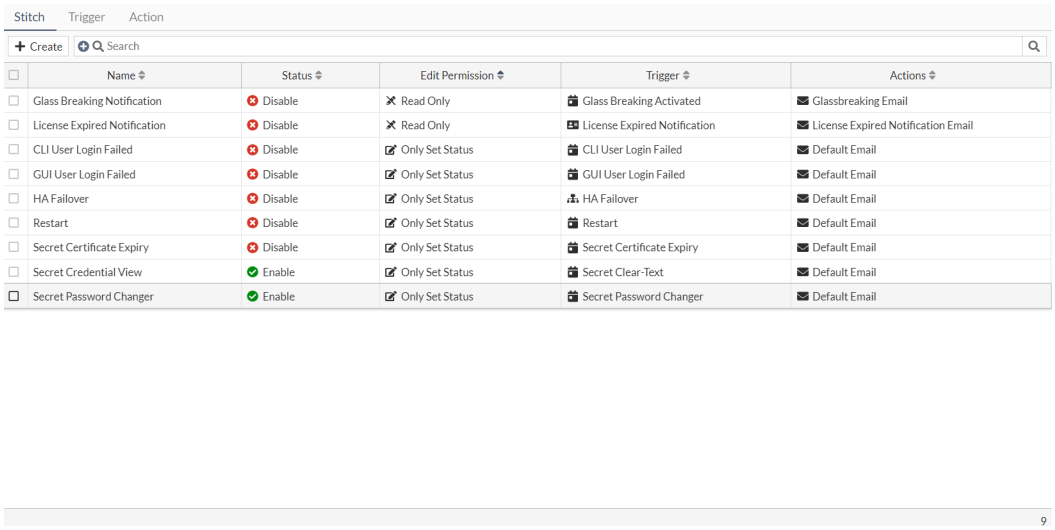
- *Name*
- *Status*
- *Edit Permission*
- *Trigger*
- *Actions*

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.



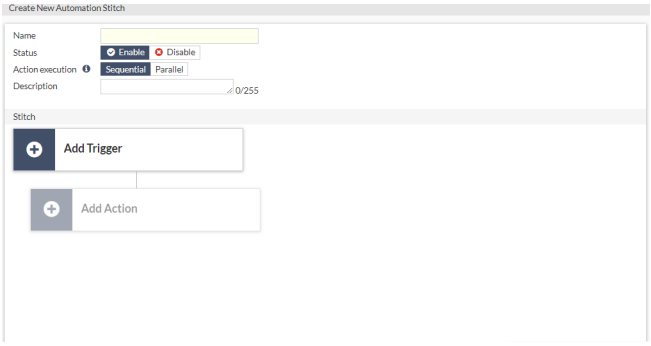
The *Stitch* tab contains the following options:

Create	Select to create a new automation stitch. See Creating an automation stitch on page 338.
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:

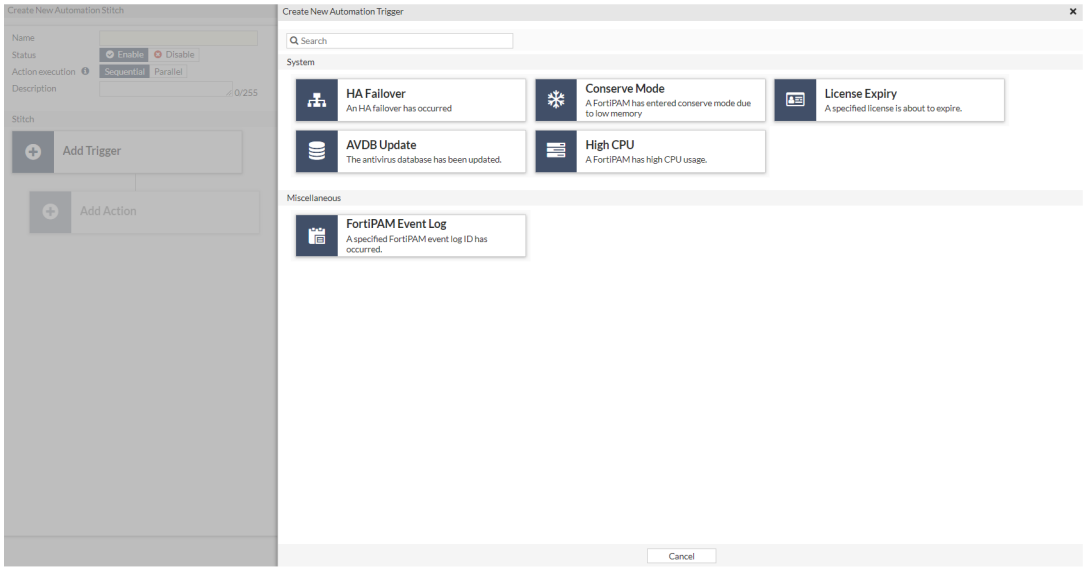
Name	The name of the automation stitch.
Status	Enable/disable the automation stitch.
Action execution	Select from the following two options: • *Sequential*: Actions execute one after another with a delay (if specified). If one action fails, the action chain stops (default). • *Parallel*: All actions 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 339.
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 341.

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.



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	

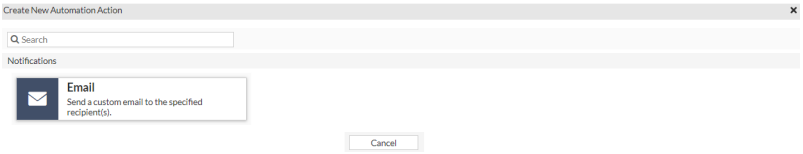
Note: The pane is only available the *FortiPAM Event Log* is selected from the category.	
Event	Select +, from *Select Entries*, select an event.  From the search bar, look up an event.
Field filter (s)	Select +, enter field name.
Value	Enter a field value.

5. Click *OK*.

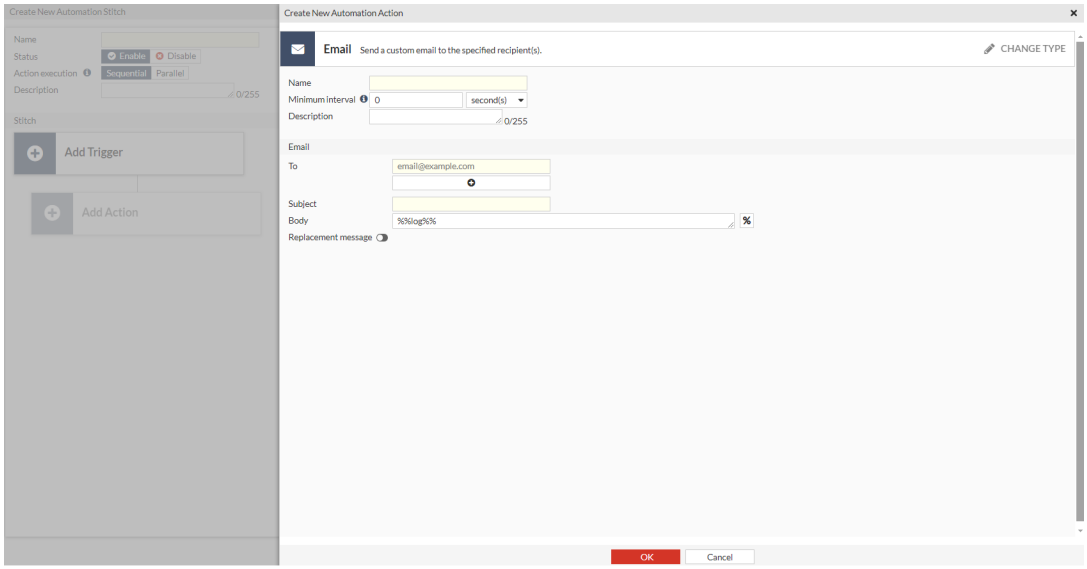
Creating new actions

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.



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.



4. Enter the following information:

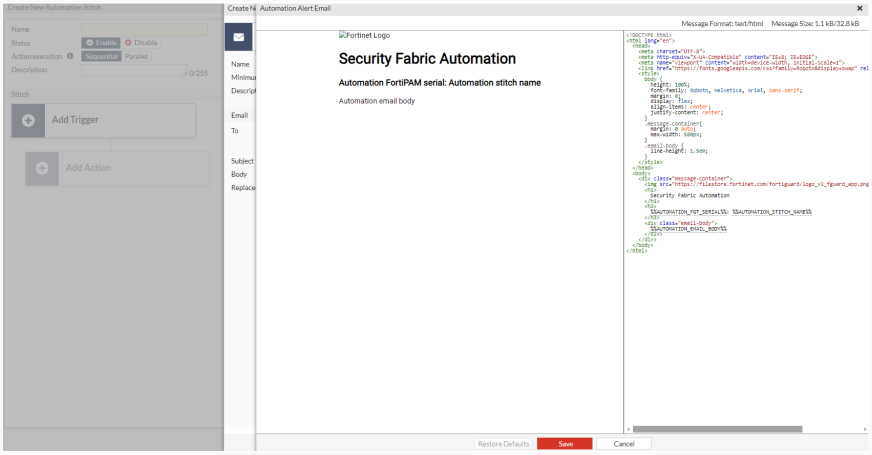
Name	The name of the automation action.

Minimum interval	Enter a time interval in hour(s)/minute(s)/second(s) Action triggered once within the time interval.
Description	Optionally, enter a description.
Email	
To	Enter the recipient email address. Select + to add additional recipients.
Subject	Enter a subject for the email.
Body	Enter the message for the email. **Note**: The field can use parameters from logs or previous action results.  Wrapping the parameter with `%%` replaces the expression with the JSON value for that parameter.  Click `%` to see examples on how to add parameters to the body. Click *Return* to return to the previous window. - Examples
Replacement message	Enable and click *Edit* to add a replacement message:  Click `%` to see examples on how to add parameters to the body. Click *Return* to return to the previous window.

`%%log%%`	All fields from the log or FortiAnalyzer event triggering this stitch.
`%%results%%`	The complete result from previous action, such as CLI script.
`%%results.source%%`	The "source" property from the previous action.
`%%results[aws_ban_ip].source%%`	The "source" property from the results of a previous action named "aws_ban_ip".
`%%results.sources.1%%`	The first index value in the array "sources" from the previous action.
`%%results.email.from%%`	The "from" property of an email object from the previous action.
`%%log.srcip%%`	The "srcip" field from the log or FortiAnalyzer event triggering this stitch.

For examples on adding parameters to replacement message, see Examples on page 342.

A new window opens:

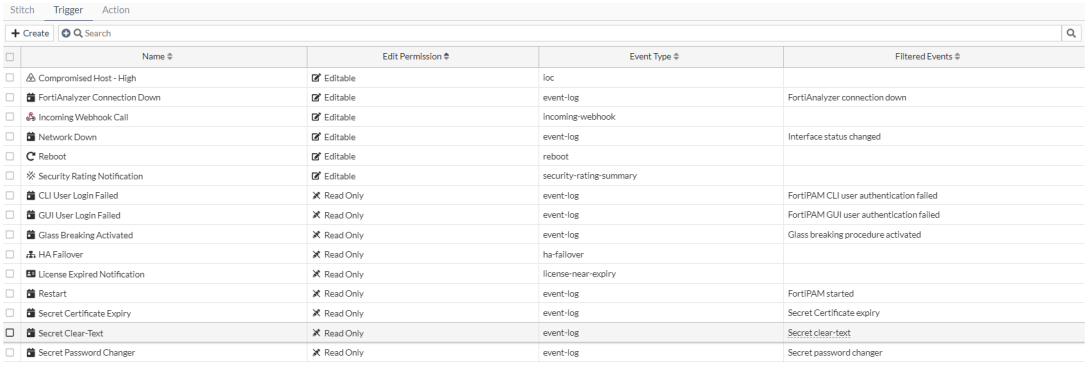


1. You can edit the replacement message by editing the HTML code.
   The preview appears in the left window.
2. Click *Save*.
   Click *Restore Defaults* if you want to restore the default replacement message.

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 345.
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.

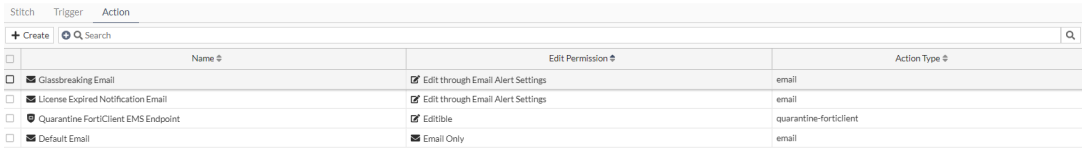
Creating a trigger

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 339.

Action

Go to *Log & Report* > *Automation* and select the *Action* tab to see the actions.



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 346.
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 341.

Reports

Go to *Log & Reports* > *Reports* to access the following:

- General on page 346
- Secret audit on page 353

General

In *General*, you can generate and view general FortiPAM reports. You can also customize the report layout and schedule the generation of reports.

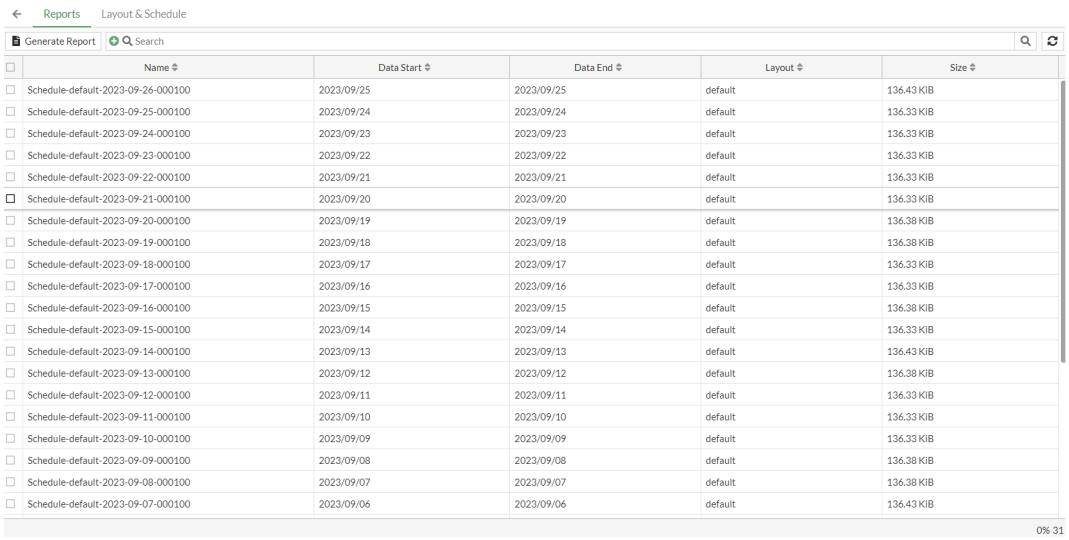
The following two tabs are available in *General*:

- Reports on page 346
- Layout & schedule on page 348

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.



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.

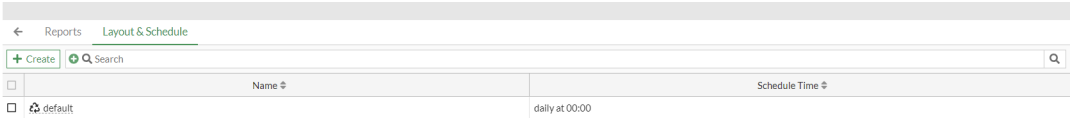
The following options are available for each of the generated report:

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:



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.

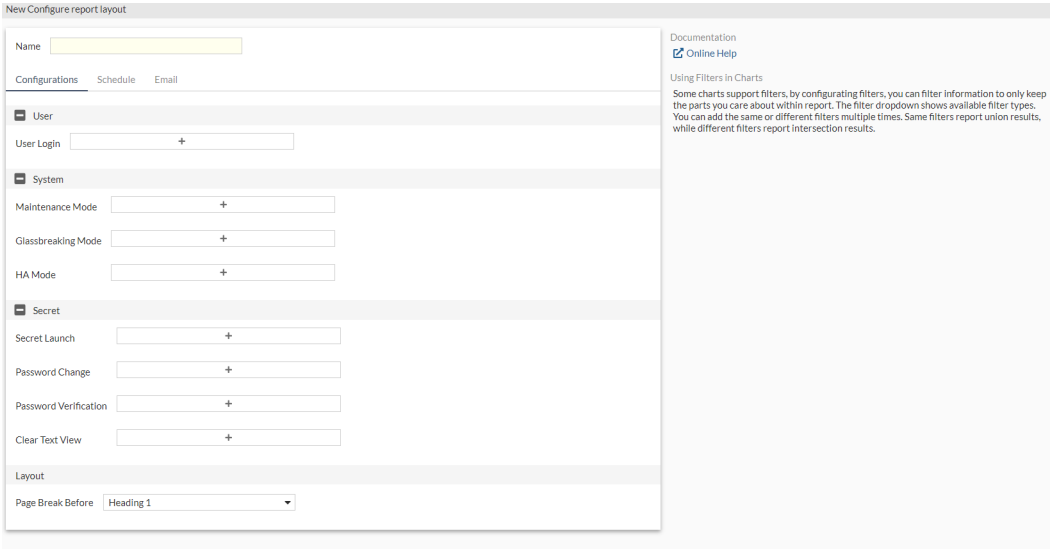
The *Layout & Schedule* tab contains the following options:

Create	Select to create a new report layout and schedule. See Creating a report layout and schedule on page 349.
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.

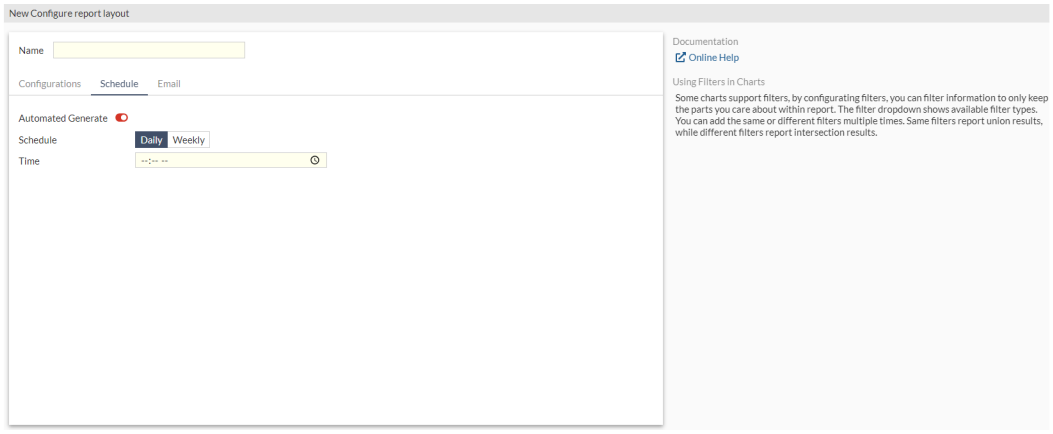
Creating a report layout and schedule

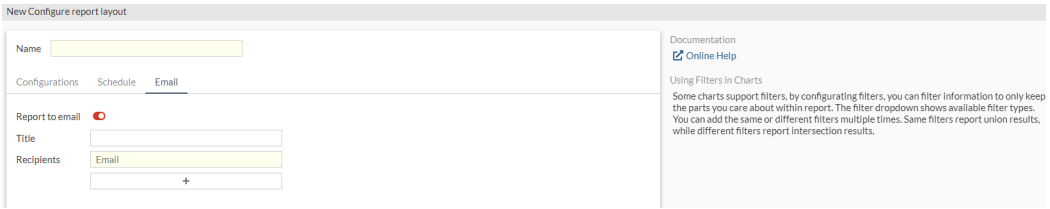
To create a report layout and schedule:

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.



3. To switch to either *Schedule* and *Email* tab, select the tab.





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 361 **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`

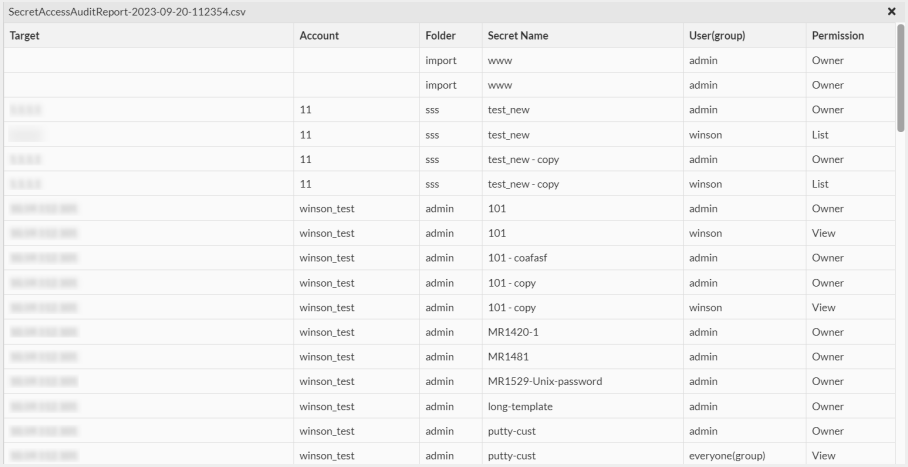


The *Secret Audit* tab includes the following options:

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:

View	Select to view the selected report. When viewed from within FortiPAM, a secret audit report looks like the following: 
Download	Select to export the selected report to your computer as a csv file.
Delete	Select to delete the selected reports.

SecretAccessAuditReport-2023-09-20-112354.csv

Target	Account	Folder	Secret Name	User(group)	Permission
		import	www	admin	Owner
		import	www	admin	Owner
[redacted]	11	sss	test_new	admin	Owner
[redacted]	11	sss	test_new	winson	List
[redacted]	11	sss	test_new - copy	admin	Owner
[redacted]	11	sss	test_new - copy	winson	List
[redacted]	winson_test	admin	101	admin	Owner
[redacted]	winson_test	admin	101	winson	View
[redacted]	winson_test	admin	101 - coafasf	admin	Owner
[redacted]	winson_test	admin	101 - copy	admin	Owner
[redacted]	winson_test	admin	101 - copy	winson	View
[redacted]	winson_test	admin	MR1420-1	admin	Owner
[redacted]	winson_test	admin	MR1481	admin	Owner
[redacted]	winson_test	admin	MR1529-Unix-password	admin	Owner
[redacted]	winson_test	admin	long-template	admin	Owner
[redacted]	winson_test	admin	putty-cust	admin	Owner
[redacted]	winson_test	admin	putty-cust	everyone(group)	View

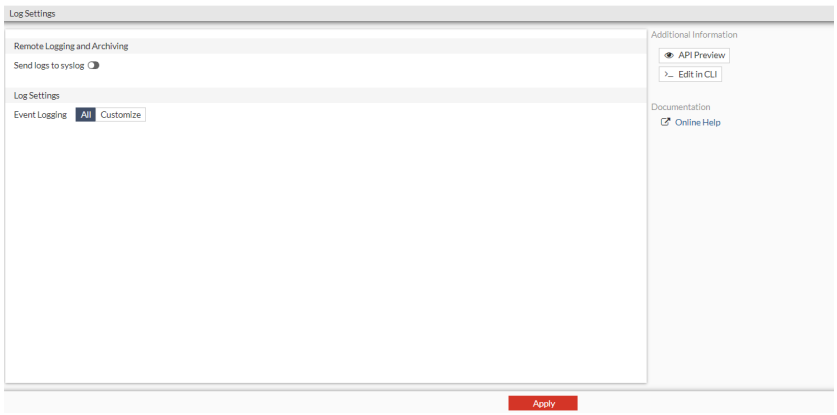
CLI configuration to generate secret audit report - example

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 356. **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.

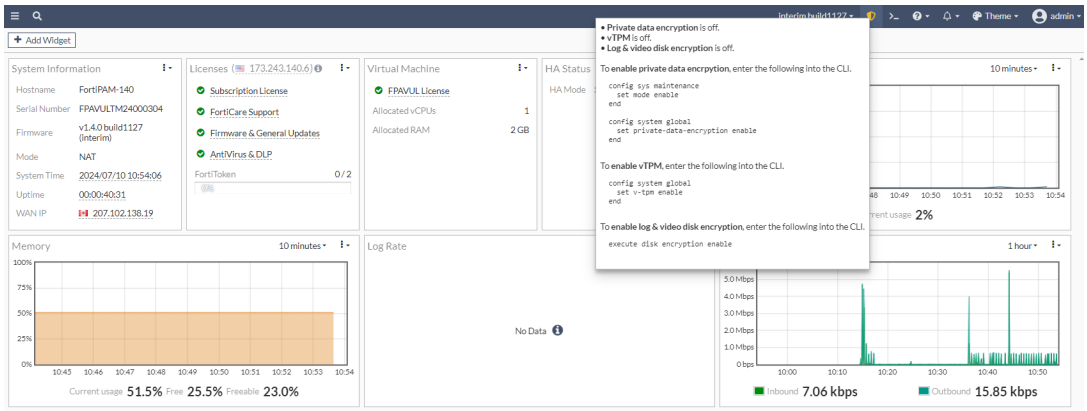


Enabling/disabling disk encryption erases all the existing logs and videos.



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.



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 474.

Email alert settings

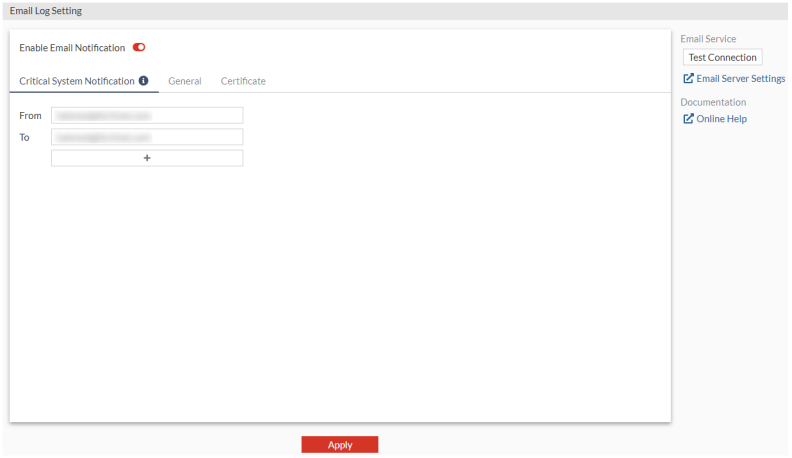
Enabling *Email Alert Settings* allows FortiPAM to send alert emails to administrators.

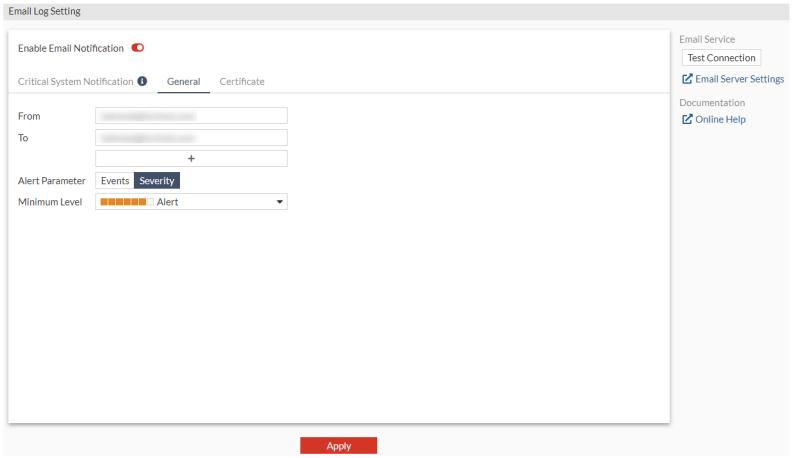
To configure a mail service:

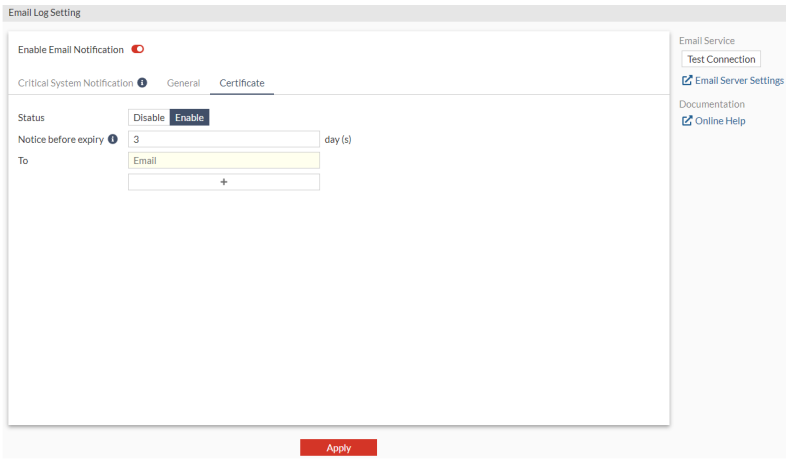
1. Go to *System* > *Settings*.
2. You can set up the email service from the *Email Service* pane. See Settings on page 397.
   By default, the Fortinet mail server is used. You can set up a custom email server by enabling *Use custom settings* in the *Email Service* pane and configuring the related 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*







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 System event on page 328. • *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 397.
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.

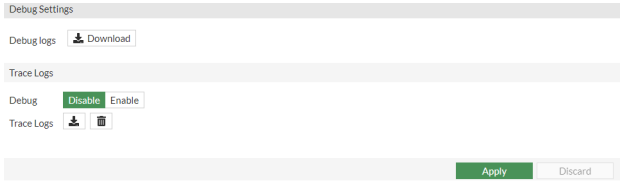
Go to *Log & Report* > *Debug Settings* and click *Download* in the *Debug Settings* pane to download the debug logs for troubleshooting.

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.



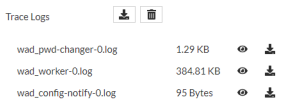
2. In the *Trace Logs* pane, enter the following information:

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 471. **Note**: The option is only available when *Debug* is enabled.
Overwrite	Enable/disable overwriting when the file reaches maximum size. **Note**:

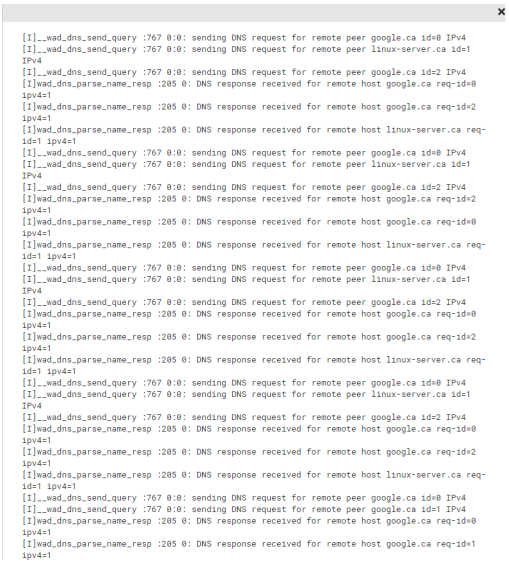
	• The option is disabled by default. • The option is only available when *Debug* is enabled.
Drop Unknown Session	Enable to drop unknown sessions. See FortiPAM HTTP filter on page 471. **Note**: • The option is disabled by default. • The option is only available when *Debug* is enabled.
Maximum File Size	The maximum size for each trace log file, in MB (default = 1, 1 - 10). **Note**: The option is only available when *Debug* is enabled.
Trace Logs	Select from the following two options: • : Download all the trace logs. • : Clear all the log traces.

3. Click *Apply*.
When FortiPAM is recording trace logs, a list of the logs appears in *Trace Logs*. You can download or view a trace log by clicking the eye or the download icon next to the trace log.

Viewing does not stop the trace recording, but downloading turns off the trace recording.



When you click the eye icon next to a trace log, you can view it.



4. When the diagnostic is finished, disable *Debug* to stop recording.

Automation trigger settings

FortiPAM can be configured to perform actions when an event log is triggered. This is in the system automation table.



Automation trigger settings can only be configured via the CLI.

Automation trigger settings via the CLI - Example

To configure automation trigger settings:

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

```
config system automation-trigger
 edit "fold_chg"
  set event-type event-log
  set logid 44547 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, packet capture, server, and secret gateways.

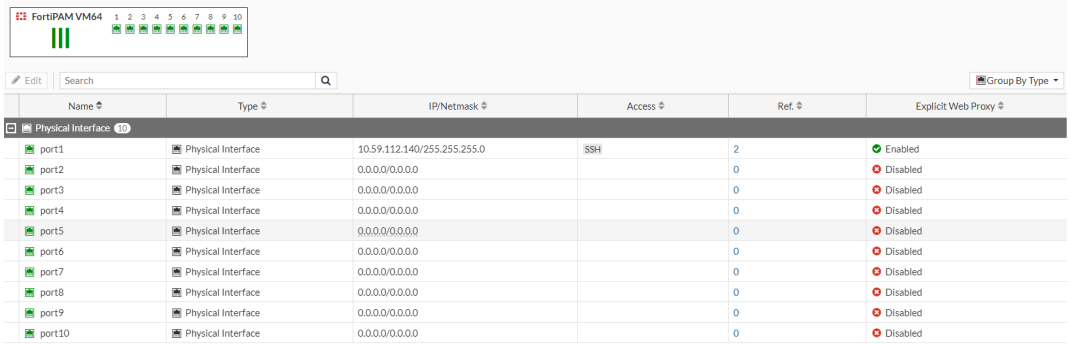
The *Network* tab contains the following tabs:

- Interfaces on page 367
- Static routes on page 371
- DNS settings on page 374
- Fabric Connectors on page 376
- Packet capture on page 381
- FortiPAM server on page 383
- Secret gateway on page 384

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.





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:

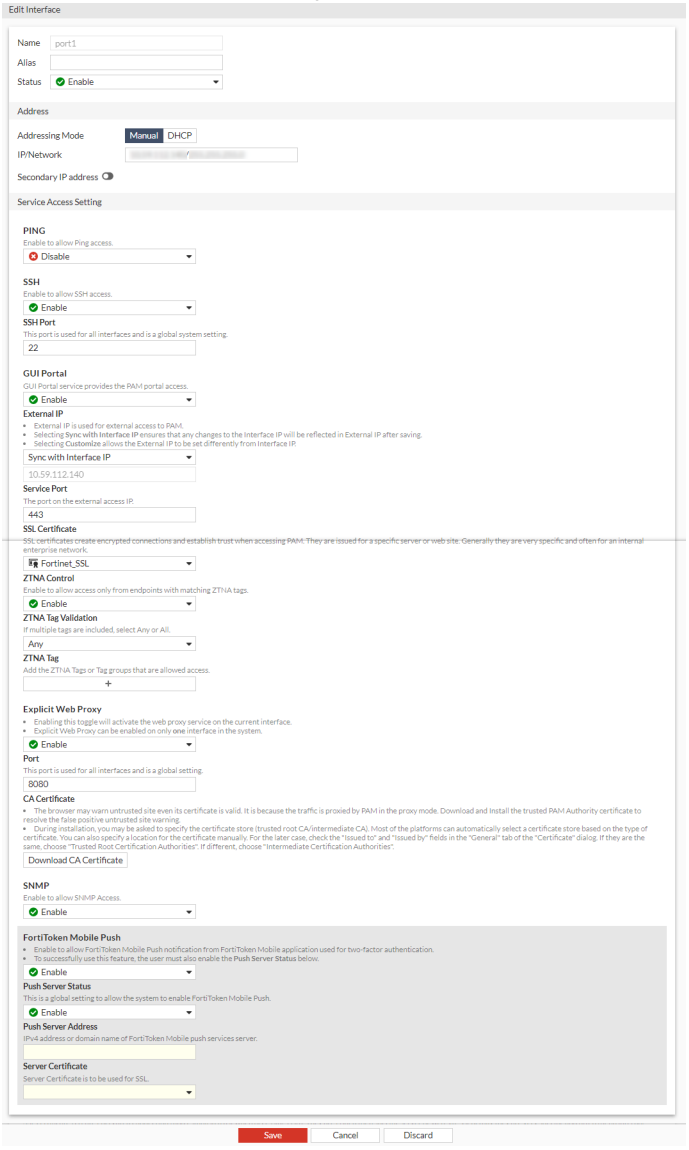
Edit	Select to edit the selected interface. See Editing an interface on page 368.
Search	Use the search bar to look for an interface.
Group By Type	From the dropdown, group the list of interfaces by type, role, status, or zone.

	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.



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 fro m 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.

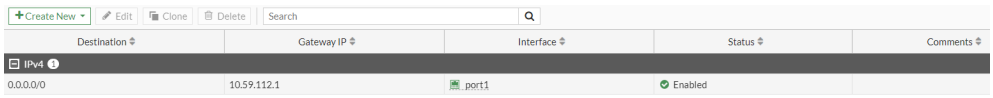
	During installation, you may be asked to specify the certificate store (trusted root CA/intermediate CA). Most platforms can automatically select a certificate store based on the type of certificate. You can also specify a location for the certificate manually. For the latter case, check the *Issued 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.





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:

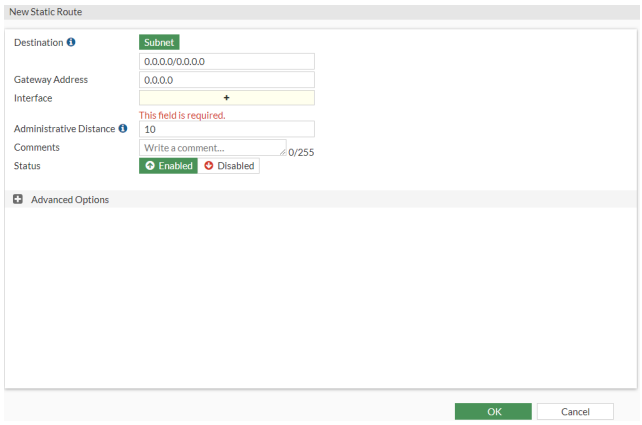
+Create New	From the dropdown, select to create an IPv4 static route. See Creating an IPv4 static route on page 372.
Edit	Select to edit the selected static route.

Clone	Select to clone the selected static route.
Delete	Select to delete the selected static route.
Search	Use the search bar to look for a static route.

Creating an IPv4 static route

To create an IPv4 static route:

1. Go to *Network* > *Static Routes*.
2. Select *Create New* to create a new IPv4 static route.
   The *New Static Route* window opens.



3. Enter the following information:

Destination	The destination IP addresses and network masks of packets that the FortiPAM unit intercepts. Enter the IPv4 address and netmask of the new static route.
Gateway Address	The IP addresses of the next-hop routers to which intercepted packets are forwarded. Enter the gateway IP address for those packets that you intend to intercept. **Note**: *Gateway Address* is unavailable when the *Interface* is *Blackhole*.
Interface	The interface the static route is configured to. Select + and in *Select Entries*, select the interface or create a new interface. A blackhole route is a route that drops all traffic sent to it. Blackhole routes are used to dispose of packets instead of responding to suspicious inquiries. This provides added security since the originator will not discover any information from the target network. Blackhole routes can also limit traffic on a subnet. If some subnet addresses are not in use, traffic to those addresses, which may be valid or malicious, can be directed to a blackhole for added security and to reduce traffic on the subnet.  Use the search bar to look for an interface.  Use the pen icon next to an interface to edit the interface.
Administrative Distance	The number of hops the static route has to the configured gateway. The administrative distance is used to determine the cost of the route. Smaller distances are considered "better" route that should be used when multiple paths exist to the same destination (default = 10, 1 - 255). The route with same distance are considered as equal-cost multi-path (ECMP).
Comments	Optionally, enter a description about the static route.
Status	Enable/disable the static route.
Advanced Options	
Priority	A number for the priority of the static route. Routes with a larger number will have a lower priority. Routes with the same priority are considered as ECMP (default = 1 when creating an IPv4 static route, 1 - 65535).  Priority can only be customized for statically configured route s. The priority of routes dynamically learned from the routing protocols is always 1.

API Preview	The *API Preview* allows you to view all REST API requests being used by the page. You can make changes on the page that are reflected in the API request preview. The feature is not available if the user is logged in as an administrator that has read-only GUI permissions.

4. Click *OK*.

To use API preview:

1. Click *API Preview*.
   The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* (enabled by default) to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

DNS settings

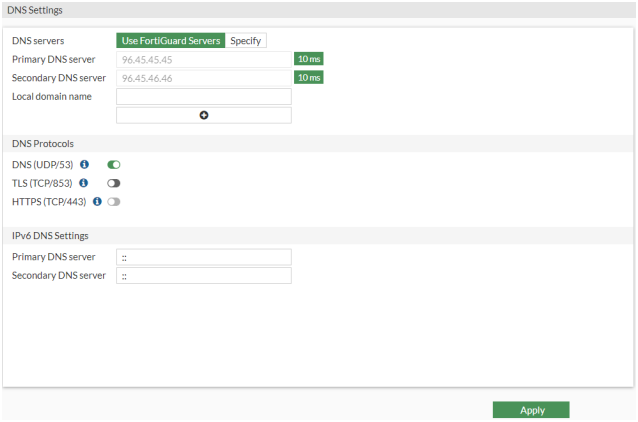
Domain name system (DNS) is used by devices to locate websites by mapping a domain name to a website's IP address.

You can specify the IP addresses of the DNS servers to which your FortiPAM unit connects.

To configure DNS settings, go to *Network* > *DNS Settings*.

To configure DNS settings:

1. Go to *Network* > *DNS Settings*.



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

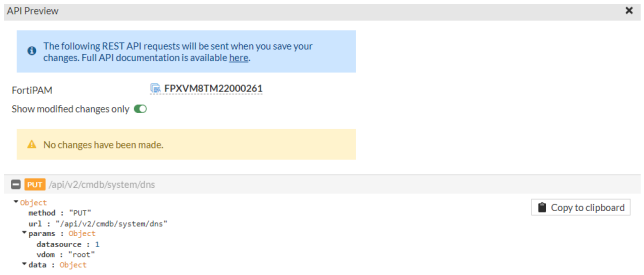
DNS servers	Select *Use FortiGuard Severs* or *Specify*. If you select *Specify*, enter the IP addresses for the primary and secondary DNS servers.
Primary DNS server	Enter the IPv4 or IPv6 address for the primary DNS server. **Note**: For an IPv4 address, the option is only available to edit when *DNS servers* is *Specify*.
Secondary DNS server	Enter the IPv4 or IPv6 address for the secondary DNS server. **Note**: For an IPv4 address, the option is only available to edit when *DNS servers* is *Specify*.
Local domain name	The domain name to append to addresses with no domain portion when performing DNS lookups.  Select + to add additional local domain names.  You can add up to 8 local domain names.
DNS Protocols	
DNS (UDP/53)	Enable or disable the use of clear-text DNS over port 53. **Note**: The option is disabled by default and only available to edit when *DNS servers* is *Specify*.
TLS (TCP/853)	Enable or disable the use of DNS over TLS (DoT). **Note**: The option is enabled by default and only available to edit when *DNS servers* is *Specify*.
HTTPS (TCP/443)	Enable or disable the use of DNS over HTTPS (DoH). **Note**: The option is disabled by default and only available to edit when *DNS servers* is *Specify*.
SSL certificate	From the dropdown, select an SSL certificate or click *Create* to import a certificate (default = `Fortinet_Factory`). SSL certificate is used by the DNS proxy as a DNS server so that the DNS proxy can provide service over TLS as well as normal UDP/TCP.  Use the search bar to look for an SSL certificate.
Server hostname	The host name of the DNS server (default = `globalsdns.fortinet.net`).

You can add up to 4 server hostnames.

3. Click *Apply*.

To use API preview:

1. Click *API Preview*.
   The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.



2. Enable *Show modified changes only* (enabled by default) to show the modified changes instead of the full configuration in the preview.
3. Click *Copy to Clipboard* to copy the JSON code shown on the preview screen to the clipboard.
4. Click *Close* to leave the preview.

Security fabric

The Security Fabric allows your network to automatically see and dynamically isolate affected devices, partition network segments, update rules, push out new policies, and remove malware.

The Security Fabric is designed to cover the entire attack surface and provide you with complete visibility into your network. It allows you to collect, share, and correlate threat intelligence between security and network devices, centrally manage and orchestrate policies, automatically synchronize resources to enforce policies, and coordinate a response to threats detected anywhere across the extended network. The unified management interface provides you with cooperative security alerts, recommendations, audit reports, and full policy control across the Security Fabric that will give you confidence that your network is secure.

See Fabric Connectors on page 376.

Fabric Connectors

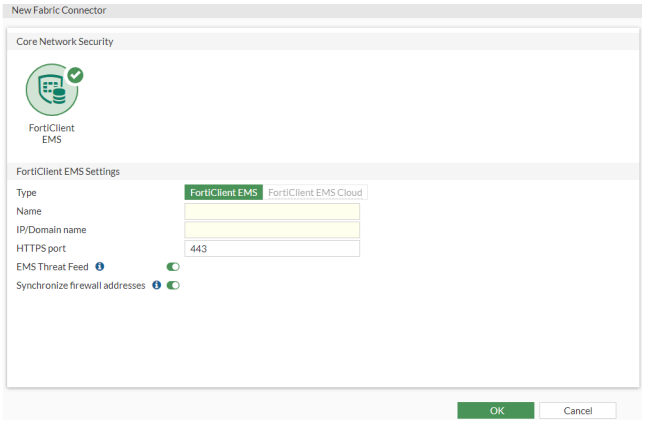
Fabric connectors provide integration with Fortinet products to automate the process of managing dynamic security updates without manual intervention.

In HA and DR setup, the EMS configuration, such as server name and IP, can be synced to secondary and DR nodes. However, secondary and DR nodes need to be authorized by EMS individually. It is recommended that after configuring

HA, admin test failover, log in to the new primary, and follow the same procedure to authorize secondary and DR nodes on the EMS server.

To create a FortiClient EMS fabric connector:

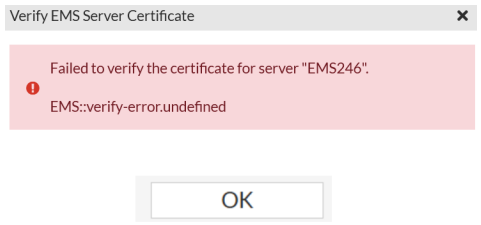
1. Go to *Network* > *Fabric Connectors*.
2. In the *Core Network Security* pane, select *FortiClient EMS* and then select *Edit*.
   The *New Fabric Connector* pane opens.



3. Enter the following information:

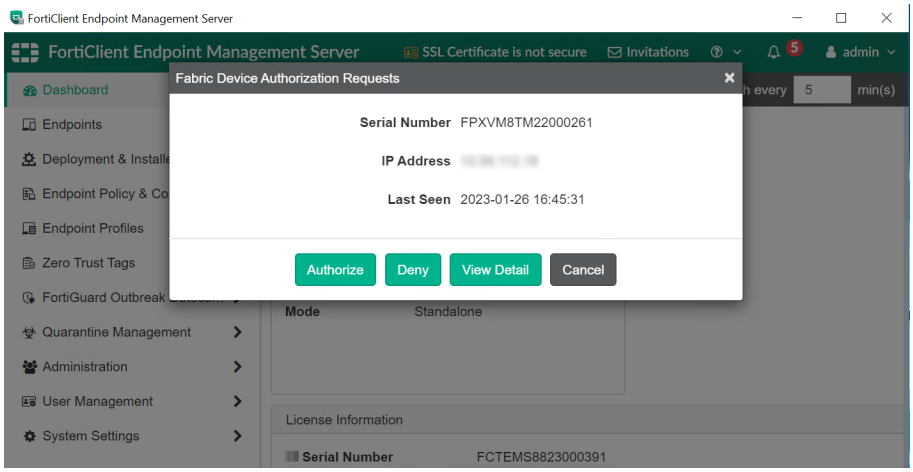
Type	Select from the following two options: • *FortiClient EMS* • *FortiClient EMS Cloud* The *FortiClient EMS Cloud* option requires FortiClient EMS Cloud entitlement.
Name	The name of the FortiClient EMS connector.
IP/Domain name	The IP address or the domain name of the FortiClient EMS.
HTTPS port	The HTTPS port number for the FortiClient EMS (default = 443, 1 - 65535).
EMS Threat Feed	Enable to allow FortiPAM to pull FortiClient malware hash from FortiClient EMS. **Note**: The option is enabled by default.
Synchronize firewall addresses	Enable to automatically create and synchronize firewall addresses for all EMS tags. **Note**: The option is enabled by default.

4. Click *OK*.
   FortiPAM attempts to verify the EMS server certificate.

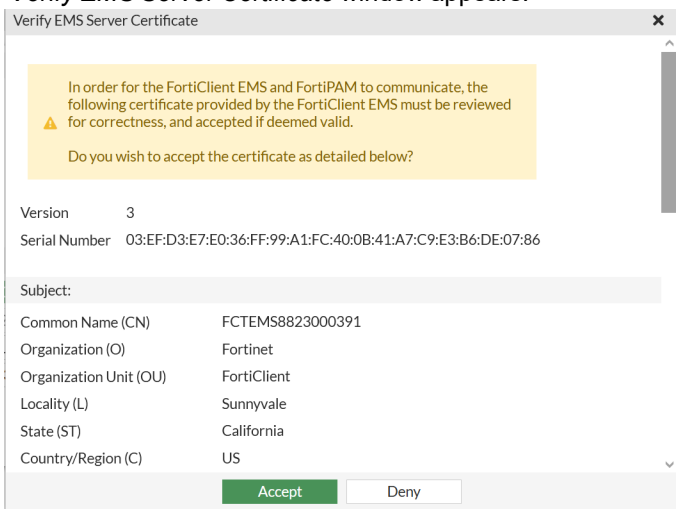


To delete a fabric connector, select *Delete* to delete the selected fabric connector.

5. Relogin to the EMS server.
   Fabric Device Authorization Requests prompt appears.



6. In *Fabric Device Authorization Requests*, click *Authorize* to authorize FortiPAM connection.
7. In the *Edit Fabric Connector* pane on FortiPAM (for the newly configured connector), click *Authorize* in *FortiClient EMS Status*.
   Verify EMS Server Certificate window appears.



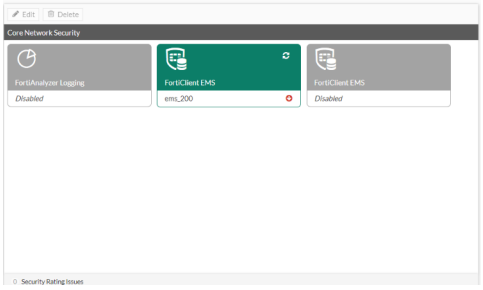
8. In the *Verify EMS Server Certificate* window, select *Accept* to accept the certificate from the EMS-side.
   FortiPAM is now successfully connected to the EMS server.

FortiAnalyzer logging

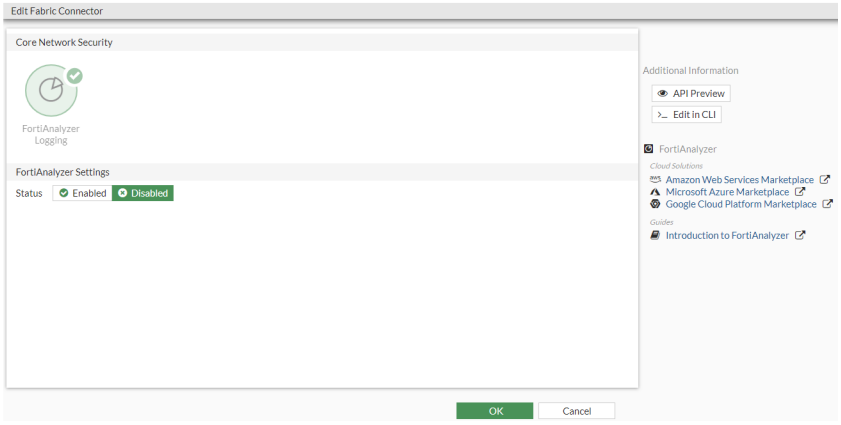
FortiAnalyzer is a remote logging server that helps keep an additional copy of logs from FortiPAM.

To configure FortiAnalyzer logging:

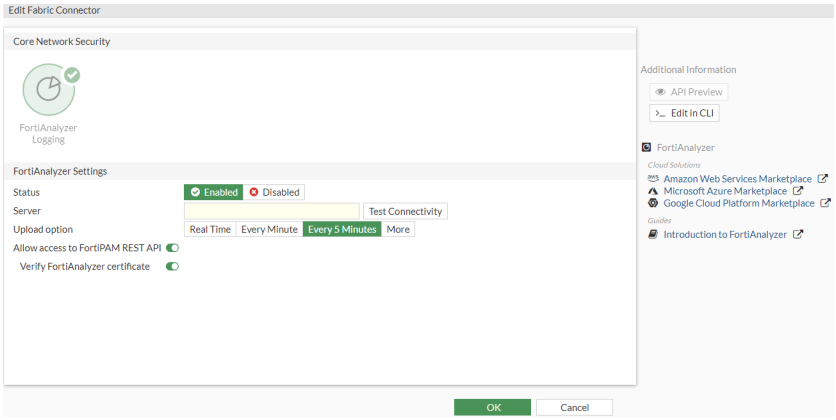
1. Go to *Network* > *Fabric Connectors*.
   Core Network Security opens.



2. Select *FortiAnalyzer Logging* and select *Edit*.
   The *Edit Fabric Connector* window opens.



3. In the *FortiAnalyzer Settings* pane, set the *Status* as *Enabled*.
   You now see new options in the *Edit Fabric Connector* window.



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 323.

To configure FortiAnalyzer logging via the CLI - Example

```
config log fortianalyzer setting
  set status enable
  set server faz.fortipam.ca
end
```

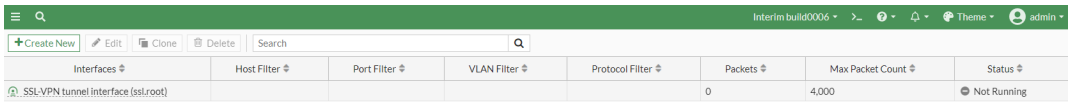
Packet capture

You can create a filter on an interface to capture a specified number of packets to examine.

Go to *Network* > *Packet Capture* to see existing packet capture filters.

For each packet capture filter the following are displayed:

- Interfaces
- Host filter
- Post filter
- VLAN filter
- Protocol filter
- Packets
- Maximum packet count
- Status



Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

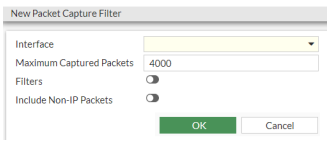
The following options are available in the *Packet Capture* tab:

+Create New	Select to create a new packet capture filter. See Creating a packet capture filter on page 381.
Edit	Select to edit the selected packet capture filter.
Clone	Select to clone the selected packet capture filter.
Delete	Select to delete the selected packet capture filter.
Search	Use the search bar to look for a packet capture filter.

Creating a packet capture filter

To create a packet capture filter:

1. Go to *Network* > *Packet Capture*.
2. Select *+Create New*.
   The *New Packet Capture Filter* window opens.



3. Enter the following information:

Interface	Select or create a new interface.  Use the search bar to look for an interface.  Use the pen icon next to an interface to edit the interface.
Maximum Captured Packets	Enter how many packets to collect (default = 4000, 1 - 1000000).
Filters	Enable *Filters*, you can create filters for host names, ports, VLAN identifiers, and protocols.  Use commas to separate items. Use a hyphen to specify a 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:

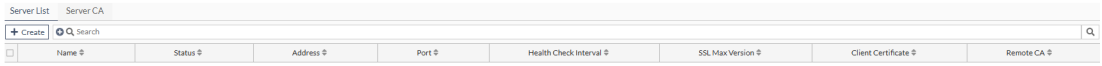
1. Click *API Preview*.
   The *API Preview* pane opens, and the values for the fields are visible (data). If a new object is being created, the POST request is shown.
2. Enable *Show modified changes only* (enabled by default) to show the modified changes instead of the full configuration in the preview.
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.

FortiPAM server

Go to *Network* > *FortiPAM Server* to create a FortiPAM server.

The *FortiPAM Server* tab is used to configure a reverse connection to the secret server when the current device or the instance works as a reverse gateway or a service gateway. The configuration works with *Network* > *Secret Gateway* > *Reverse Service* in the secret server.

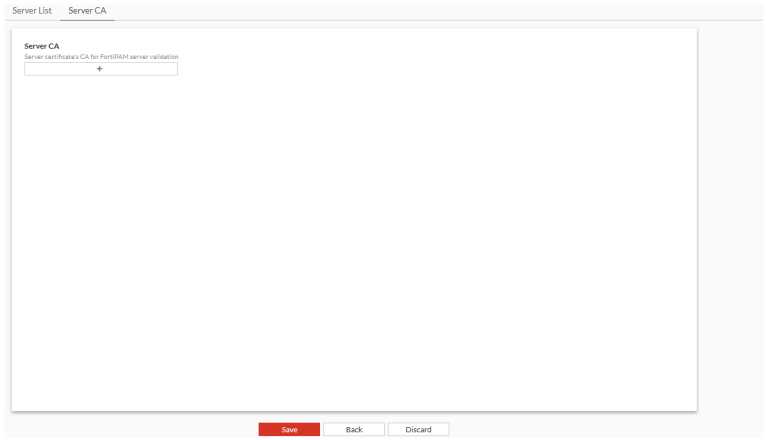
For each server; name, status, address, port, health check interval, SSL max version, client certificate, and remote CA are displayed.



The following options are available:

+Create	Select to create a server.
Search	Enter a search term in the search field, then hit `Enter` to search the servers. To narrow down your search, see Column filter.

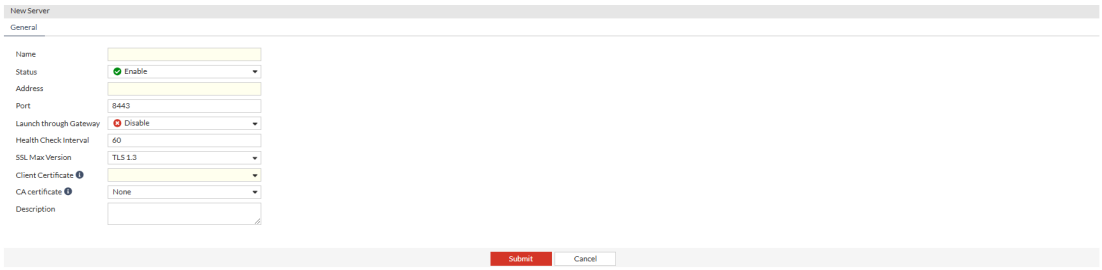
Switch to the *Server CA* tab to select server CAs for FortiPAM server validation.



Creating a server

To create a server:

1. Go to *Network* > *FortiPAM Server*.
2. Select *Create*.
   The *New Server* window opens.



3. Enter the following information:

Name	The name of the server.
Status	Enable/disable the server (default = enable).
Address	The IP address/FQDN for the server.
Port	The server port number (1 - 65535, default = 8443)
Launch through the Gateway	The service gateway launch proxy status (default = disable): • *Enable*: The gateway proxy launches traffic in the Service mode. The mode can automatically switch to Reverse mode if it is manually set to Reverse mode at the start of the secret launch. • *Disable*: The gateway proxies the launch traffic in the Reverse mode.
Health Check Interval	The health check interval, in seconds (0 - 600, default = 60). **Note**: If `0` is entered, the health check is disabled.
SSL Max Version	The highest TLS version acceptable from the server: • *TLS 1.1* • *TLS 1.2* • *TLS 1.3* (default)
Client Certificate	The client certificate for mTLS.
CA Certificate	CA certificate verification for mTLS.
Description	Optionally, enter a description.

4. Click *Submit*.

Secret gateway

Introduction

FortiPAM supports network gateway for distributed target deployment.

Secret Gateway in *Network* 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.

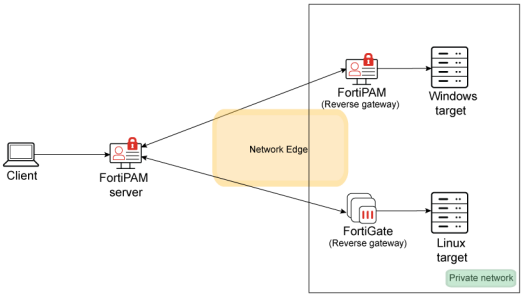
A FortiGate 7.6.3 or above version supports configuring FortiGate as a reverse gateway.

Forward type

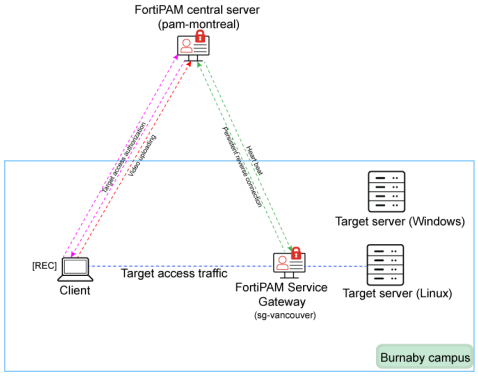


In the forward type scenario, the FortiPAM deployed on a public site cannot reach the target server directly. The target server is in the private enterprise network and deployable at multiple locations. A FortiGate or a FortiProxy device acts as a network gateway. The network gateway can be applied to the target. All connections to the target are now proxied by FortiPAM and the network gateway.

Reverse type



Service gateway



The reverse gateway supports Service mode.

The reverse gateway operates under 2 modes:

- *Reverse mode*: The gateway working in the reverse mode is called the Reverse Gateway.
- *Service mode* (new): The gateway working in the service mode is called the Service Gateway.

When FortiPAM acts as the reverse gateway with the Service ability, it supports the client directly to start launching sessions from the client device itself rather than starting the session from the original FortiPAM and then proxying it to the reverse gateway.

In the Reverse mode, the launching session traffic flow is *Client machine* > *Central Server* > *Gateway* > *Target Server*.

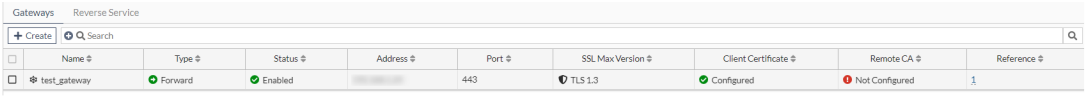
In the Service mode, the launching session traffic is *Client machine* > *Gateway* > *Target Server*. This reduces the session delay and the central server stress when the gateway device is closer to the target server. Here, videos are still uploaded to FortiPAM and the secret log is reported to FortiPAM instead of storing it on the gateway device.

Requirements

- The central FortiPAM server and the service gateway must be on the same image version (at least FortiPAM 1.5.0 GA), or the launch automatically falls back to the reverse mode.
- When the secret has DLP and antivirus scan enabled, the secret launching session always starts from the FortiPAM device.
- The web launcher session always starts from the FortiPAM device.

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

- *Name*
- *Type*
- *Status*
- *Address*
- *Port*
- *SSL Max Version*
- *Client Certificate*
- *Remote CA*
- *Reference*



The *Secret Gateway* tab contains the following options:

Create	Select to create a new gateway. See Creating a gateway on the FortiPAM GUI on page 387.
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.

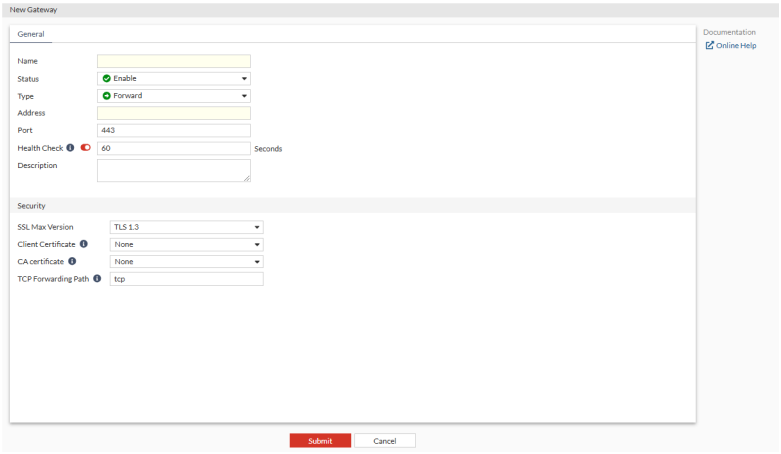
For gateway related CLI configurations, see:

- Creating a gateway on the FortiPAM CLI on page 393
- FortiPAM connects to a target through a FortiProxy acting as the gateway Example on page 395

Creating a gateway on the FortiPAM GUI

To create a gateway:

1. Go to *Network* > *Secret Gateway*.
2. In the gateway list, select *Create*.
   The *New Gateway* window opens.



3. Enter the following information:

4.

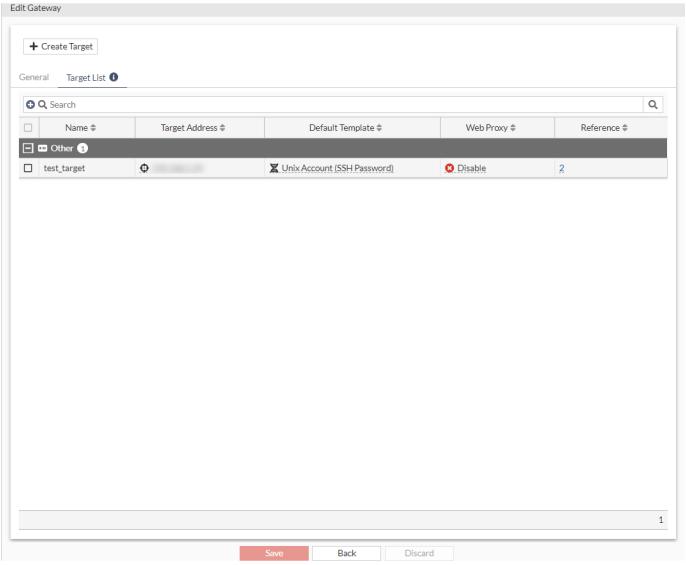
General	
Name	The name of the gateway.
Status	Enable/disable the gateway (default = *Enable*).
Type	The type of gateway: • *Forward* (default) • *Reverse* To set up a reverse gateway, you must first configure the following: • Reverse service on FortiPAM. See Reverse service on page 391. • Reverse service on the gateway for a reverse connection to the FortiPAM server. • Traffic proxy on the gateway for forwarding secret launch. See Configuring traffic proxy on gateway CLI on page 392.
Address	The gateway IP address or FQDN.
Port	The gateway port number (1 - 65535, default = 443).
Health Check	Enable and enter a time period to periodically check if the gateway is alive, in seconds (default = 60). When enabled, the connectivity status will show on the right panel.
Description	Optionally, enter a description for the gateway.
Reverse Gateway	
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*.
Mode	Select from the following three modes: • *Service Gateway*: When FortiPAM acts as the reverse gateway with the Service ability, it supports the client directly to start launching sessions from the client device itself rather than starting the session from the

	original FortiPAM and then proxying it to the reverse gateway. In the Service mode, the launching session traffic is *Client machine* > *Gateway* > *Target Server*. This reduces the session delay and the central server stress when the gateway device is closer to the target server. Here, videos are still uploaded to FortiPAM and the secret log is reported to FortiPAM instead of storing it on the gateway device. • *Reverse Gateway*: In the Reverse mode, the launching session traffic flow is *Client machine* > *Central Server* > *Gateway* > *Target Server*. • *On Demand* (default): The client can choose if the secret is connected with the service gateway or the reverse gateway mode during the secret launch process. **Notes**: • The option is only available when the *Type* is *Reverse*. • The option works when *Launch through Gateway* is enabled for a FortiPAM server in *Network* > *FortiPAM Server*. However, it can only provide the Service Gateway capability when the *Mode* is *Service Gateway* and the corresponding gateway's *Launch through Gateway* option is enabled. Otherwise, it falls back to the Reverse mode. See FortiPAM server on page 383.
Security	
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).

5. Click *Submit*.

Target list for gateways

When editing a gateway the *Target List* tab displays the targets using the gateway.



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.

When a FortiPAM device acts as a reverse gateway and you intend to use the Service feature, in the GUI go to *Network > FortiPAM Server* (see FortiPAM server on page 383), or use the following command:

```
config secret server
 edit "172.16.80.108"
  set status enable
  set address "172.16.80.108"
  set port 8443
  set service-gateway-launch enable #enable the service feature
  set health-check-internal 5
  set sni ''
  set ssl-max-version tls-1.2
  set client-cert "client_cert.pem"
  set ca "CA_Cert_1"
  set description ''
 next
end
```

Setting `service-gateway-launch` to disable will disable the routing traffic directly to the service gateway, i.e., the gateway works in the Reverse mode.

There is always a default firewall address and policy for the reverse mode.

```
config firewall address
 edit "fortipam_vip_gwy_addr"
  set uuid 71be08b0-9635-51ef-15dd-cc38fbd02e05
  set subnet 172.17.219.98 255.255.255.255
 next
end
```

The IP address in the default `firewall.address` is the same as the default VIP.

```
config firewall policy
 edit 2001
  set type access-proxy
  set name "fortipam_vip_gwy_pol"
  set uuid 71be3eca-9635-51ef-ee0f-1fd59c381492
  set srcintf "any"
  set srcaddr
  set dstaddr "all"
  set action accept
  set schedule "always"
  set access-proxy "fortipam_access_proxy"
  set ssl-ssh-profile "deep-inspection"
 next
end
```

Both the reverse and the service mode work on the default `fortipam_vip`, so when you switch the mode on the Gateway device, there is no need to change the corresponding `secret.gateway` entry on the FortiPAM device.

If the gateway device is required to function as both the forward and the reverse gateway, you must add a new `firewall.address` representing the source device IP address and add that address next to `fortipam_vip_gwy_addr` in the policy.

Notes:

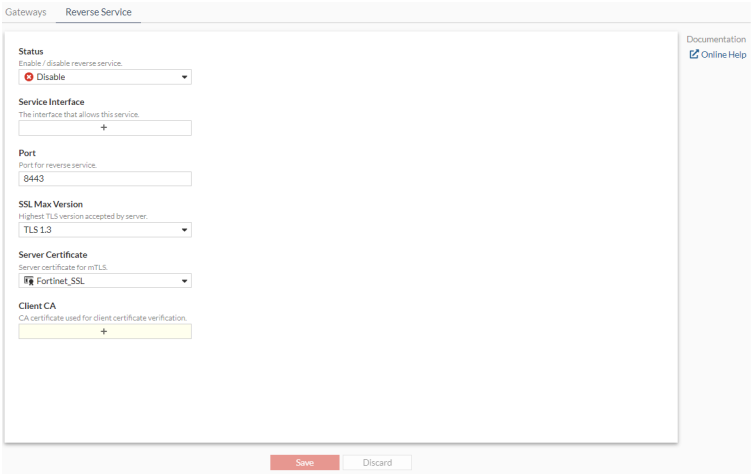
- *Agentless* web launching does not work with the service gateway.
- If the secret server and the gateway are different products, i.e., one is FortiPAM and the other is FortiSRA, the gateway always works on the reverse mode.

Reverse service

To use the reverse gateway feature, you must first configure reverse service on FortiPAM.

To configure the reverse service:

1. Go to *Network* > *Secret Gateway*.
2. Select the *Reverse Service* tab.
   The *Reverse Service* tab opens.



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 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:

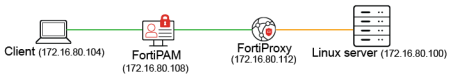
```
config secret target
 edit "172.16.80.101"
  set class "Other"
  set templete "Unix Account (SSH Password)"
```

```
    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 395.

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:
   Alternatively, go to *Network* > *Secret Gateway* to configure the secret gateway. See Creating a gateway on the FortiPAM GUI on page 387.

```
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):
   Alternatively, go to *Secrets* > *Targets* to configure the secret target. See Creating a target on page 117.

```
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
```

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:

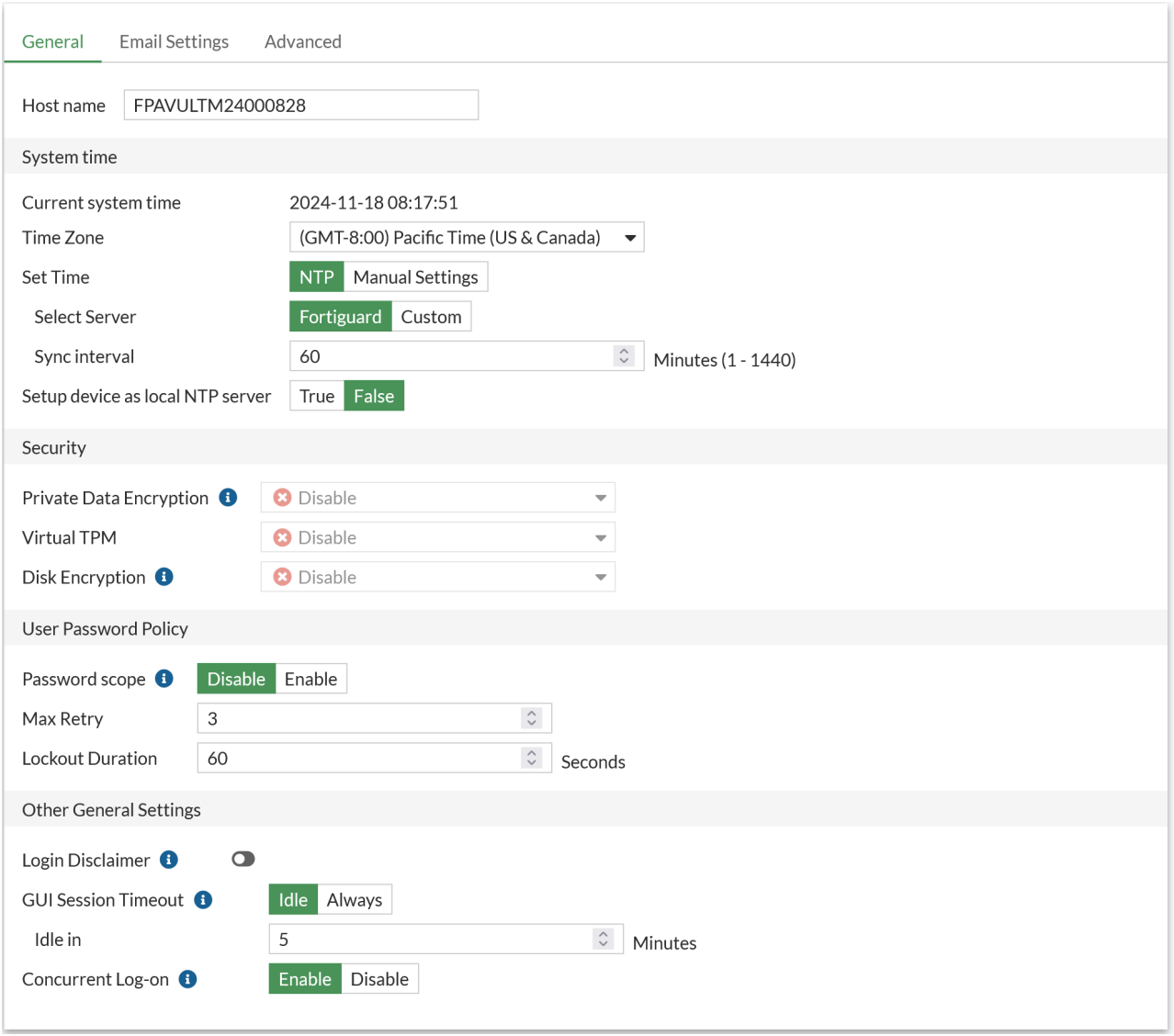
- Settings on page 397
- ZTNA tags on page 407
- High availability on page 414
- Certificates on page 423
- Replacement messages on page 433
- SNMP on page 441
- Configuration backup on page 448
- Firmware on page 460
- FortiPAM license on page 460
- FortiGuard license on page 462
- Setup wizard on page 462

Settings

Go to *System* > *Settings* to access system configuration that you can update after installing FortiPAM.

To update System Settings:

1. Go to *System* > *Settings*.
   The *General* tab in the *System Settings* window opens.



2. To switch to the *Email Settings* or *Advanced* tab, select *Email Settings* or *Advanced*.
3. In *System Settings*, enter the following information:

General tab

Host name	The identifying name assigned to this FortiPAM unit.

System time pane

System time	
Current system time	The current date and time on the FortiPAM internal clock or NTP servers.
Time Zone	From the dropdown, select a timezone.
Set Time	Select from the following options:

	• *NTP*: The NTP (Network Time Protocol) server (default). • *Manual Settings*
Select Server	Select a server from the following two options: • *FortiGuard* (default) • *Custom* **Note**: The option is only available when *Set Time* is *NTP*.
Custom Server IP Address	The custom server IP address.  Custom NTP server details must be configured via the CLI. **Note**: The option is only available when *Set Time* is *NTP* and the *Select Server* is *Custom*.
Sync internal	Enter how often, in minutes, that the device synchronizes its time with the NTP server (default = 60, 1 - 1440). **Note**: The option is only available when *Set Time* is *NTP*.
Date	Enter the date or select the calendar icon, and from the dropdown, select a date. **Note**: The option is only available when *Set Time* is *Manual Settings*.
Time	Enter the time or select the clock icon, and from the dropdown, select a time. **Note**: The option is only available when *Set Time* is *Manual Settings*.
Setup device as local NTP server	Select *True* to configure the FortiPAM as a local NTP server (default = *False*).
Listen on Interfaces	Set the interface or interfaces that the FortiPAM will listen for NTP requests on. **Note**: The option is only available when *Setup device on local NTP server* is set as *True*.

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 489.
Virtual TPM	Enable/disable vTPM. **Note**: Only the status is shown. Use the CLI to configure vTPM. See FortiPAM with TPM on page 46.
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 357.

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

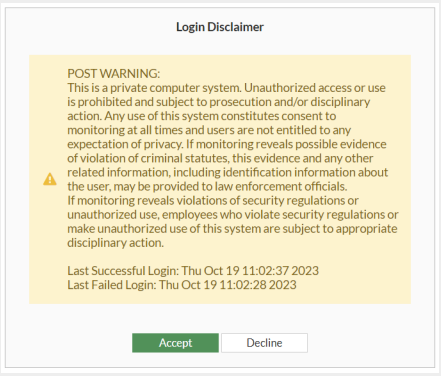
View Settings	
Language	From the dropdown, select a language.

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.



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 466.

Email Settings tab

Email Service See Testing the email service connection example on page 405.	
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 361.

Approval Email Server	Email server setup for the Approval by Email feature. It allows the approval to approve a secret request by sending an email to a specified email address. See Approving secrets by Email on page 204.
Use Approval Email Server	Enable to configure approval email server settings.
Email Server Address	The domain portion of your email address that appears after the @ symbol. Example: icloud.com, gmail.com
Email Pulling Server Address	The IMAP (Internet Message Access Protocol) server address that handles incoming email retrieval, support both fqdn and IP format. Example: imap.mail.me.com (icloud IMAP address)
Email Pulling Service Port	The network port number used for connecting to the email server. Example: 993 - Standard port for IMAP over SSL/TLS (secure).
User Name	The account identifier used for authentication on the email server. Usually the portion of your email address before the @ symbol.
Credential	The login password of the given user name.  For security reasons, most of the email servers don't allow you to use the plain password. Instead, you need to generate an "application specific password" and fill it in as the credential. The user need to consult appropriate supporting resources to obtain it. References: • Create App Password for Gmail - How to create app passwords | Google Workspace Knowledge Center • Create App Password for iCloud - Sign in to apps with your Apple Account using app-specific passwords - Apple Support
Email Folder	The specific folder where approval emails are stored and checked. Example: inbox (default value).
Check Interval	The frequency of checking the email server for new messages. Example: 2 minutes (the minimum allowed value is 1).
Server Certificate	It is used to validate the email server. This is an optional field. When not given, the verification is skipped.
Minimum SSL Version	The minimum acceptable TLS protocol version for secure communications.

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 321.
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:

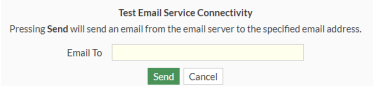
	• *Separate Emails*: Send the secret request notifications as separate emails (default). • *Single Email*: Send the secret request notifications as a single email.
Period	Enter the time interval at which multiple secret request notifications are sent, in seconds (default = 60, 60 - 600). **Note**: The option is only available when *Send Multiple Secret Requests in* is set to *Single Email*.
PAC Rule Url	Enter the URL of the PAC rules that will be followed. The PAC rules are followed in addition to the ones FortiPAM operates. See Web proxy on page 125.

4. Click *Save*.

Testing the email service connection - example

To test the email service connection:

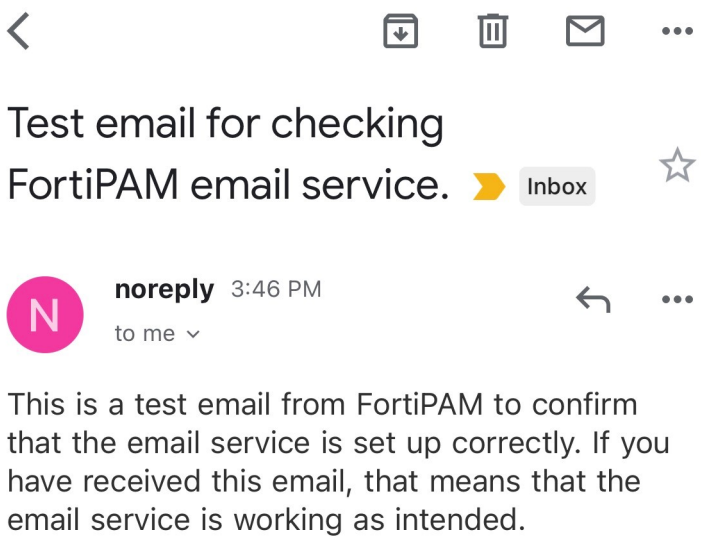
1. Go to *System* > *Settings*.
   In this example, we use the default Fortinet mail server (`notification.fortinet.net`).
2. In the *Email Service* pane:
   a. In *Default Reply To*, enter the email address that is used to send emails.
3. Click *Apply*.
   To configure alert emails, see Email alert settings on page 361.
4. Once the email service settings have been set up, click *Test Connection* from the top-right.
   The *Test Email Service Connectivity* dialog opens.



5. In *Email To*, enter an email address where the test email is sent to.
6. Click *Send*.
   Once the email is successfully sent, you see the following message on the bottom-right:



   The test email looks like the following:



To test the email service connection via the CLI:

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

   ```
   diagnose log alertmail test
   ```

   If the email service is correctly setup, you should receive a test email that looks like the following:

2. If you do not receive the test email:
   a. In the CLI console, enter the following CLI commands to collect the debug logs:

      ```
      diagnose debug reset
      diagnose debug enable
      diagnose debug console timestamp enable
      diagnose debug application alertmail -1
      ```

   b. In the CLI console, enter the following CLI command to send a test email:

      ```
      diagnose log alertmail test
      ```

   c. In the CLI console, enter the following CLI commands to disable debugging:

      ```
      diagnose debug disable
      diagnose debug reset
      ```

3. To save the output, select *Download* from the top-right of the CLI window or use PuTTY to log the output.

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.

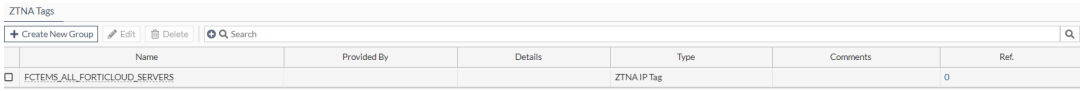
ZTNA servers can only be set using the CLI command:

- `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:



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 407
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.



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 376.

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 410.

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 413.

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.



Each node in an HA cluster can have a different number of license seats.

See Floating license on page 51.



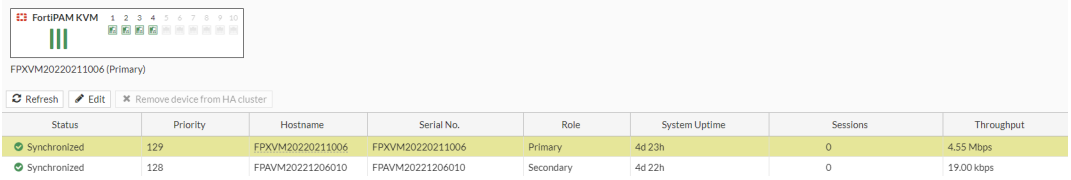
Each FortiPAM device in HA must be the same device model and version number.



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:



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

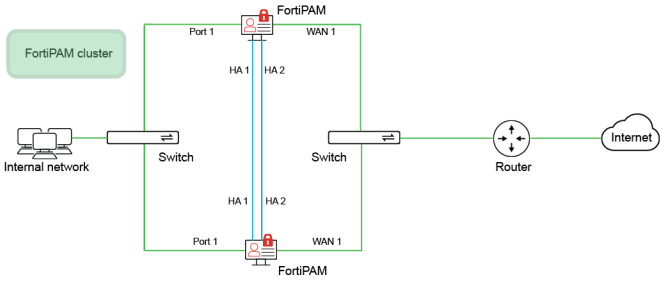
When primary FortiPAM is down, secondary will take the primary role and permanently enter maintenance mode. Under maintenance mode, all critical processes will be temporarily suspended.

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:

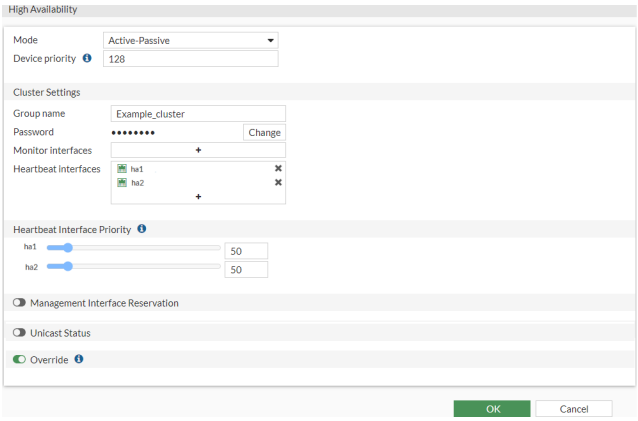


To set up an HA A-P cluster using the GUI:

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.



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 27.

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 26.
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.

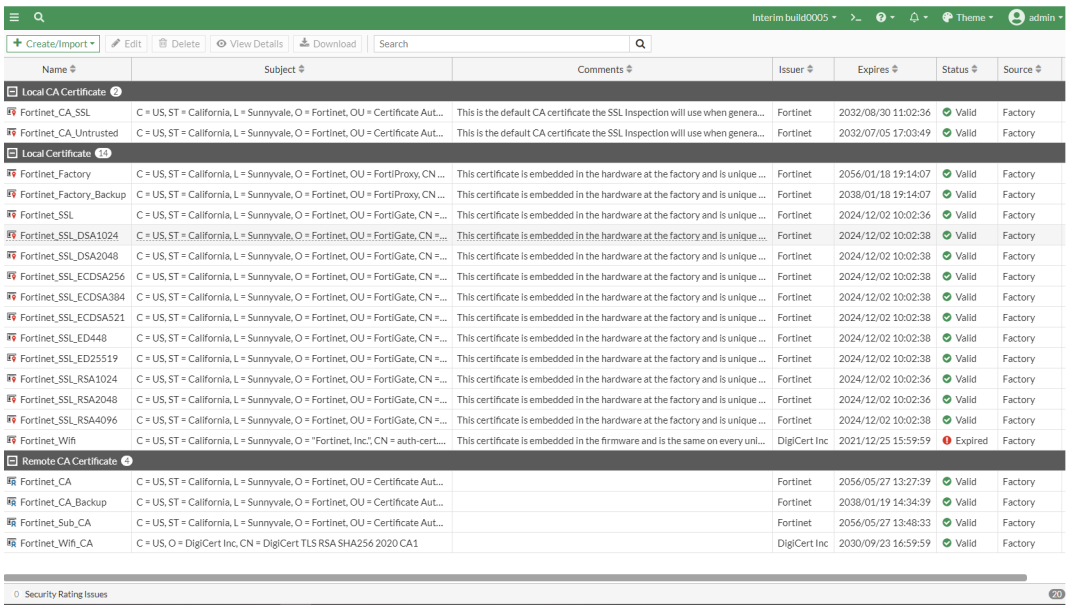
For example: After enabling the GUI portal on another interface, such as "port2," on the primary node, the following firewall VIP configuration is automatically created:

```
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.



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.

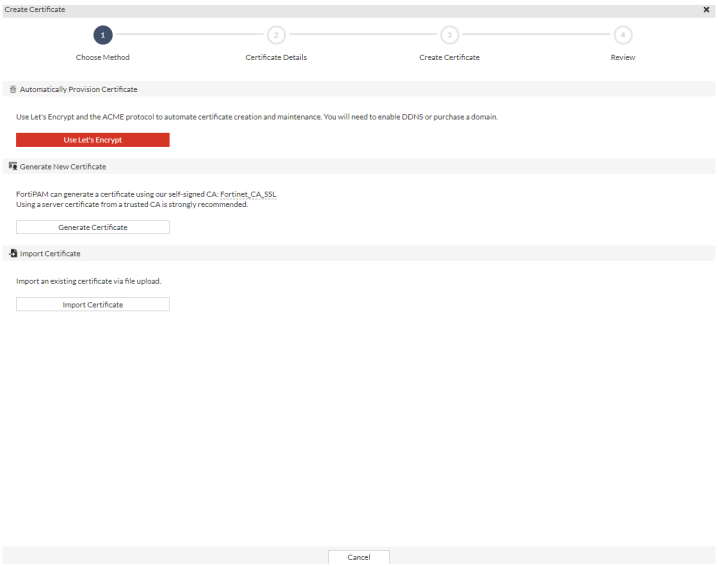
The *Certificates* tab contains the following options:

+Create/Import	From the dropdown, select *Certificate*, *Generate CSR*, *CA Certificate*, *Remote Certificate*, and *CRL*. See: • Creating a certificate on page 425 • Generating a CSR (Certificate Signing Request) on page 428 • Importing CA certificate on page 430 • Uploading a remote certificate on page 431 • Importing a CRL (Certificate revocation list) on page 431
Edit	Select to edit the selected certificate.
Delete	Select to delete the selected certificates.
View Details	Select to see details about the selected certificate.
Download	Select to download the selected certificate.
Search	Use the search bar to look for a certificate.

Creating a certificate

To create a certificate

1. Go to *System* > *Certificates*.
2. From *+Create/Import*, select *Certificate*.
   The *Create Certificate* wizard opens.



3. Enter the following information:

Choose Method	
Automatically Provision Certificate	Select *Use Let's Encrypt* to automatically create a certificate using the ACME protocol with Let's Encrypt service. You will need to enable DDNS or purchase a domain.
Generate New Certificate	Select *Generate Certificate* to generate a certificate using the self-signed `Fortinet_CA_SSL` CA. Using a server certificate from a trusted CA is strongly recommended.
Import Certificate	Select *Import Certificate* to import an existing certificate by uploading the file.
Certificate Details Enter the certificate details and click *Create* to create a certificate.	
Automatically Provision Certificate	The certificate will be automatically provisioned using the ACME protocol with the Let's Encrypt service. It is the easiest way to install a trusted certificate.

Certificate name	The name of the certificate.
Domain	The public FQDN of FortiPAM. **Note**: The option is only available when the *Chosen Method* is *Automatically Provision Certificate*.
Email	The email address. **Note**: The option is only available when the *Chosen Method* is *Automatically Provision Certificate*.
Set ACME Interface	If this is the first time enrolling a server certificate with Let's Encrypt on this FortiPAM unit, the *Set ACME Interface* pane opens. **Note**: The options in the pane are only available when the *Chosen Method* is *Automatically Provision Certificate*.
ACME Interface	Select + and from *Select Entries*, select ports, or create new interfaces on which the ACME client will listen for challenges to provision and renew certificates. Click *OK* when you have selected interfaces.  Use the search bar to look for an interface.  Use the pen icon next to the interface to edit it.
Generate New Certificate	
Certificate authority	The certificate authority. **Note**: The option is only available when the *Chosen Method* is *Generate New Certificate*.
Common name	The common name of the certificate. Enter an FQDN or an IPv4 address.  The common name should match the FQDN or the IP address of the primary SSL-VPN interface. **Note**: The option is only available when the *Chosen Method* is *Generate New Certificate*.
Subject alternative name	An IP address or FQDN. Subject alternative names (SAN) allow you to protect multiple host names with a single SSL certificate. SAN is part of the X.509 certificate standard. **Note**: The option is only available when the *Chosen Method* is *Generate New Certificate*.

Update Your List of Trusted Certificate Authorities	Select *Download CA Certificate* to download `Fortinet_CA_SSL` CA to your computer.  `Fortinet_CA_SSL` is a local CA certificate. To avoid certificate warnings, you must download it and install it on each client machine. **Note**: The option is only available when the *Chosen Method* is *Generate New Certificate*.
Import Certificate	
Type	Select from the following three options: • *Local Certificate* • *PKCS #12 Certificate* • *Certificate* **Note**: The option is only available when the *Chosen Method* is *Import Certificate*.
Certificate file	Select *+Upload* and locate the certificate file on your local computer. **Note**: The option is only available when the *Chosen Method* is *Import Certificate* and the *Type* is either *Local Certificate* or *Certificate*.
Certificate with key file	Select *+Upload* and locate the certificate with key file on your local computer. **Note**: The option is only available when the *Chosen Method* is *Import Certificate* and the *Type* is *PKCS #12 Certificate*.
Password	Enter the password. **Note**: The option is only available when the *Chosen Method* is *Import Certificate* and the *Type* is either *PKCS #12 Certificate* or *Certificate*.
Confirm Password	Reenter the password to confirm. **Note**: The option is only available when the *Chosen Method* is *Import Certificate* and the *Type* is *PKCS #12 Certificate* or *Certificate*.
Key file	Select *+Upload* and locate the key file on your local computer. **Note**: The option is only available when the *Chosen Method* is *Import Certificate* and the *Type* is *Certificate*.
Review	
Enable *ACME log* to see logs related to the certificate created using the ACME protocol. **Note**: The option is only available when *Chosen Method* is *Automatically Provision Certificate*.	
Update Your List of Trusted Certificate Authorities	If you have not already downloaded the `Fortinet_CA_SSL` CA to your computer, select *Download CA Certificate* to download it. **Note**: The option is only available when the *Chosen Method* is *Generate New Certificate*.

4. Click *OK*.

Generating a CSR (Certificate Signing Request)

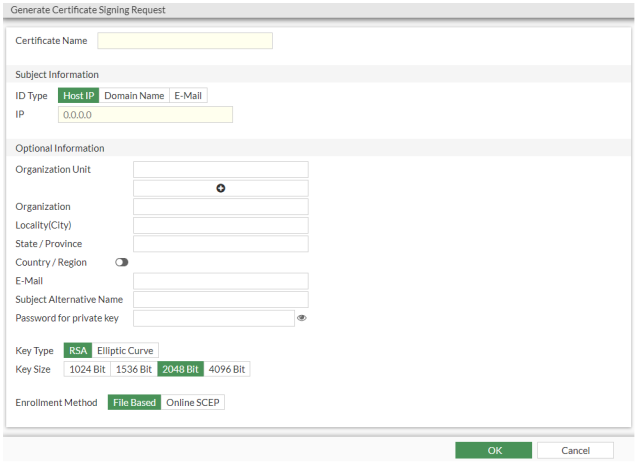
Whether you create certificates locally or obtain them from an external certificate service, you need to generate a Certificate Signing Request (CSR).

When a CSR is generated, a private and public key pair is created for FortiPAM. The generated request includes the public key of the device, and information such as the unit's public static IP address, domain name, or email address. The device private key remains confidential on the unit.

After the request is submitted to a CA, the CA verifies the information and register the contact information on a digital certificate that contains a serial number, an expiration date, and the public key of the CA. The CA then signs the certificate, after which you can install the certificate on FortiPAM.

To generate a CSR:

1. Go to *System* > *Certificates*.
2. From *+Create/Import*, select *Generate CSR*.
   The *Generate Certificate Signing Request* window opens.



3. Enter the following information:

Certificate Name	Enter a unique name for the certificate request, such as the host name or the serial number of the device.  Do not include spaces in the certificate to ensure compatibility as a PKCS12 file.
Subject Information	
ID Type	Select the ID type: • *Host IP*: Select if the unit has a static IP address. Enter the device IP address in the *IP* field (default). • *Domain Name*: Enter the device domain name or FQDN in the *Domain Name* field. • *E-mail*: Enter the email address of the device administrator in the *E-mail* field.
Optional Information Optional information to further identify the device.	
Organizational Unit	The name of the department.  Up to 5 OUs can be added.
Organization	The legal name of the company or organization.
Locality (City)	The name of the city where the unit is located.
State/Province	The name of the state or province where the unit is located.
Country/Region	Enable and then enter the country where the unit is located. Select from the dropdown.  The option is disabled by default.
E-mail	The contact email address.
Subject Alternative Name	One or more alternative names, separated by commas, for which the certificate is also valid. An alternative name can be: email address, IP address, URI, DNS name, or a directory name. Each name must be preceded by its type, for example: IP:`1.2.3.4`, or URL: `http://your.url.here/`.
Password for private key	The password for the private key.

Key Type	Select *RSA* or *Elliptic Curve*. **Note**: The default is RSA.
Key Size	If you selected *RSA* for the *Key Type*, select the *Key size*: *1024 Bit*, *1536 Bit*, *2048 Bit* (default), or *4096 Bit*.  Larger key sizes are more secure but slower to generate. If you selected *Elliptic Curve* for the *Key Type*, select the *Curve Name*: *secp256r1* (default), *secp384r1*, or *secp521r1*.
Enrollment Method	Select the enrollment method. • *File Based*: Generate the certificate request (default). • *Online SCEP*: Obtain a signed, Simple Certificate Enrollment Protocol (SCEP) based certificate automatically over the network. Enter the CA server URL and challenge password in their respective fields.

4. Click *OK*.

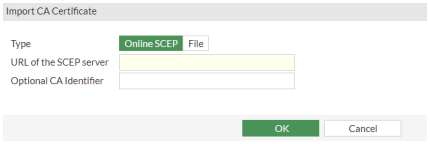
Importing CA certificate

CA root certificates are similar to local certificates, however they apply to a broader range of addresses or to whole company; they are one step higher up in the organizational chain. Using the local certificate example, a CA root certificate would be issued for all of `www.example.com` instead of just the smaller single web page.

You can import a CA certificate to FortiPAM.

To import a CA certificate:

1. Go to *System* > *Certificates*.
2. From *+Create/Import*, select *CA Certificate*.
   The *Import CA Certificate* window opens.



3. Enter the following information:

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

4. Click *OK*.

Uploading a remote certificate

Remote certificates are public certificates without a private key. Remote certificates can be uploaded to the FortiPAM unit.

To upload a remote certificate:

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



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

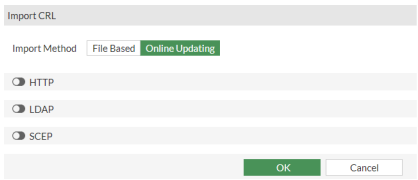
Importing a CRL (Certificate revocation list)

Certificate revocation list (CRL) is a list of certificates that have been revoked and are no longer usable. This list includes certificates that have expired, been stolen, or otherwise compromised. If your certificate is on this list, it will not be accepted. CRLs are maintained by the CA that issues the certificates and includes the date and time when the next CRL will be issued as well as a sequence number to help ensure you have the most current version of the CRL.

CRLs can be imported to FortiPAM.

To import a CRL:

1. Go *System* > *Certificates*.
2. From *+Create/Import*, select *CRL*.
   The *Import CRL* window opens.



3. Enter the following information:

Imported Method	Select either *File Based* or *Online Updating*.
+Upload	Select and locate the certificate file on your computer. **Note**: The option is only available when the *Imported Method* is *File Based*.

HTTP

Enable HTTP updating and enter the *URL of the HTTP server*.

Note: The option disabled by default.

Note: The pane is only available when the *Imported Method* is *Online Updating*.

LDAP

Enable LDAP updating and select an LDAP server from the dropdown or create a new one.

	Use the search bar to look for an LDAP server.
	Use the pen icon next to an LDAP server to edit the server.

Enter the *Username* and the *Password*.

Note: The option disabled by default.

Note: The pane is only available when the *Imported Method* is *Online Updating*.

SCEP

Enable SCEP updating and select a local certificate or create a new certificate for SCEP communication for the online CRL.

	Use the search bar to look for a certificate.

Enter the *URL of the SCEP server*.

Note: The option disabled by default.

Note: The pane is only available when the *Imported Method* is *Online Updating*.

4. Click *OK*.

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.

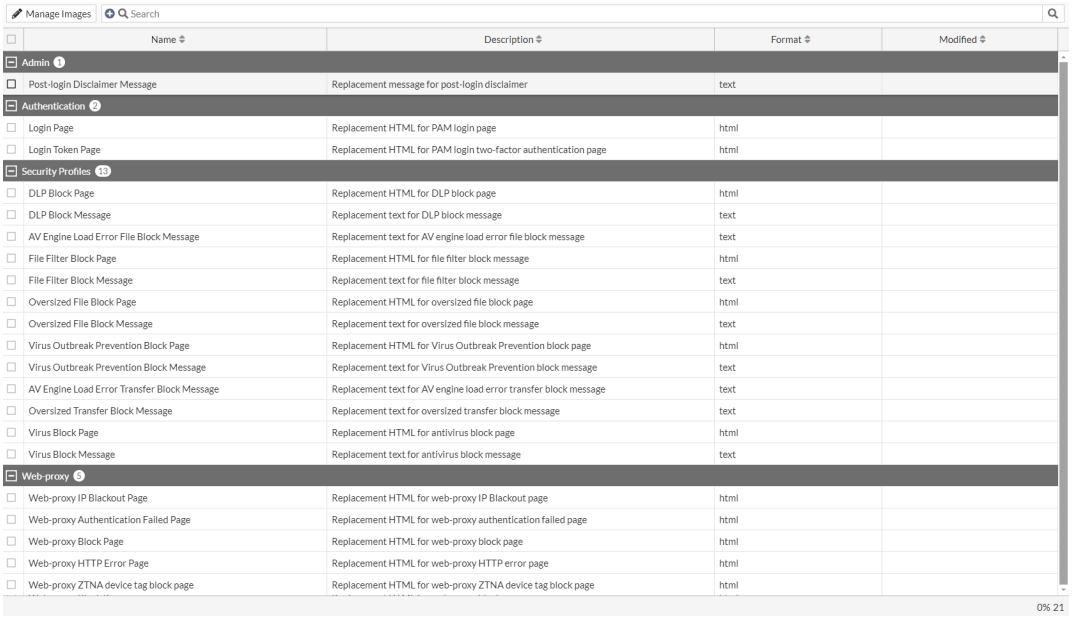
There are two types of replacement messages in FortiPAM:

- **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.



- 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 438.
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 436.



To define a filter, see Filters on page 29 in Tables on page 29.



For column related settings, see Column settings on page 33 in Tables on page 29.

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 438.

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.

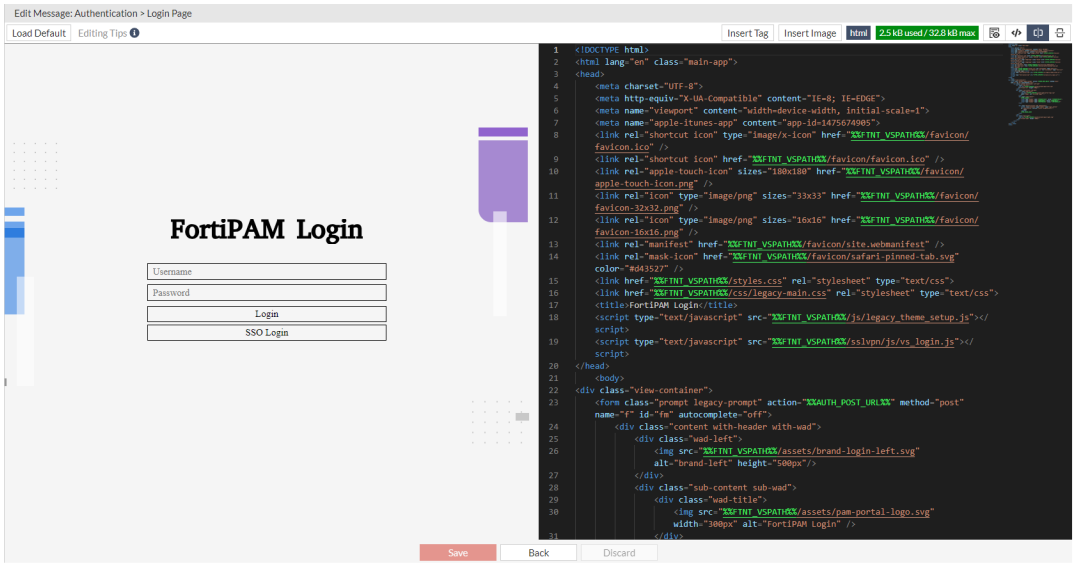


A replacement message cannot exceed the maximum size.

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.



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.

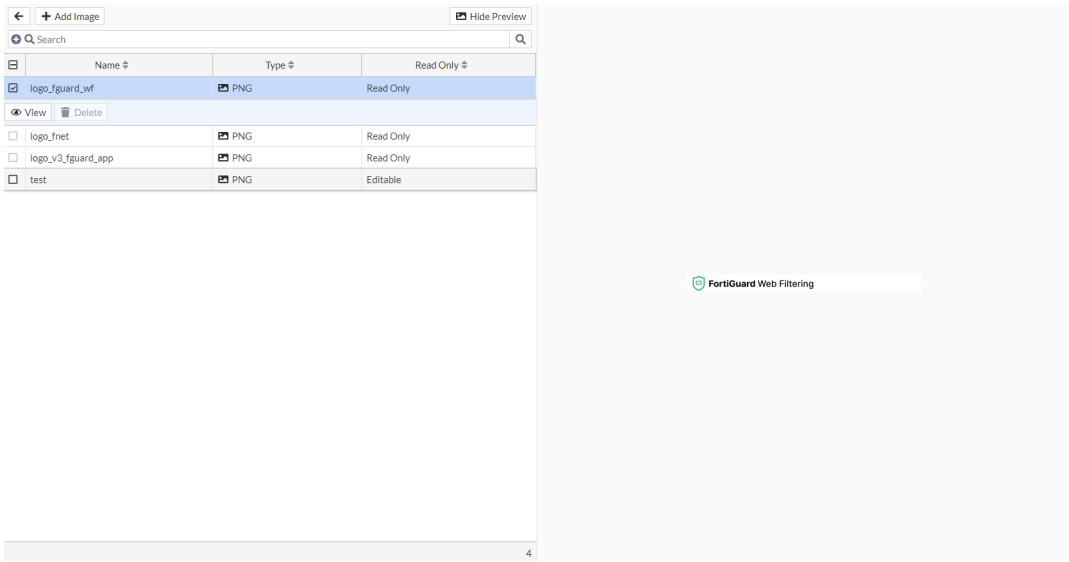
4. To insert a tag, see Inserting a tag.
5. To insert an image, see Inserting an image.
6. When you are finished editing the message, select *Save* to save your changes.
7. If you have made an error when editing the message, select *Load Default* to restore the message to its default value.
   See Adding an image on page 439.

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.



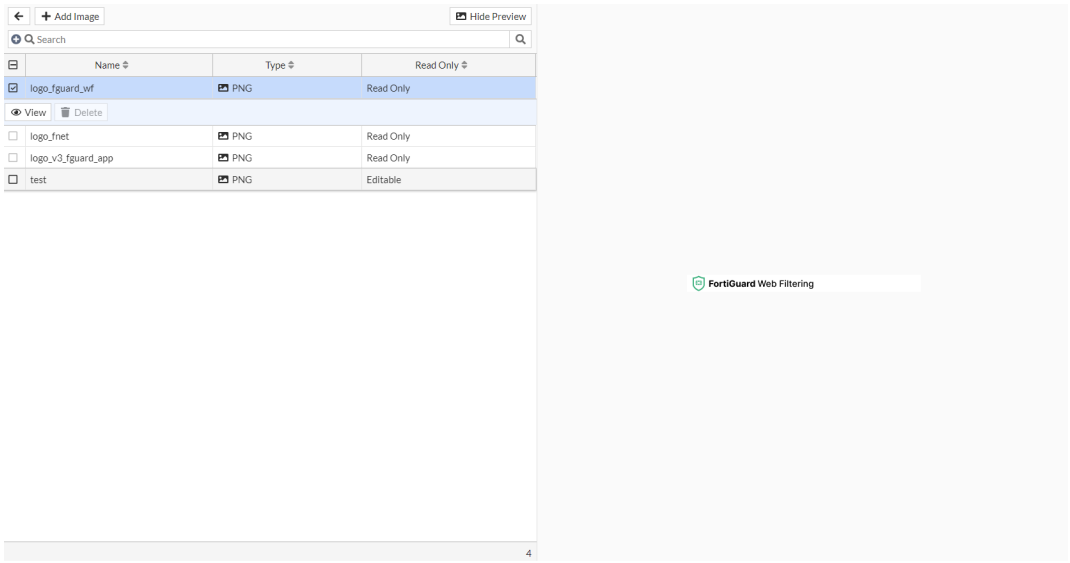
In the *Managing images* page, the following options are available:

Add Image	Select to add a new image file. See Adding an image on page 439.
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.

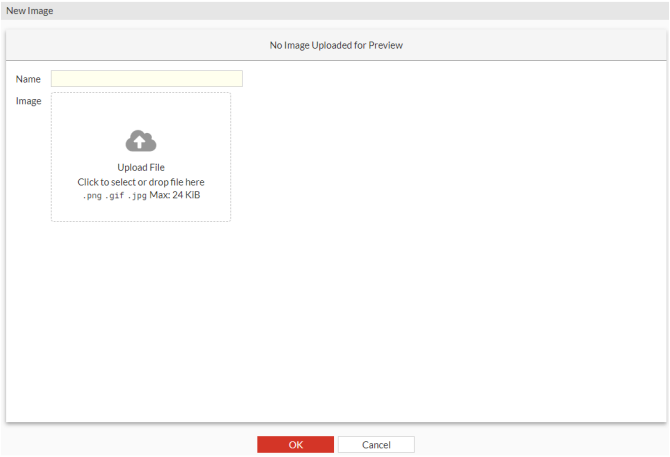
Adding an image

To add an image:

1. Go to *System* > *Replacement Messages* and select *Manage Images*.
   The *Manage Images* window opens.



2. Select *Add Image*.
   The *New Image* window opens.



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 443 for more information.

The FortiPAM SNMP implementation is read-only. SNMP v1, v2c, and v3 compliant SNMP managers have read-only access to FortiPAM system information through queries and can receive trap messages from the unit.

The FortiPAM SNMP v3 implementation includes support for queries, traps, authentication, and privacy. Authentication and privacy can be configured in the CLI or the GUI.

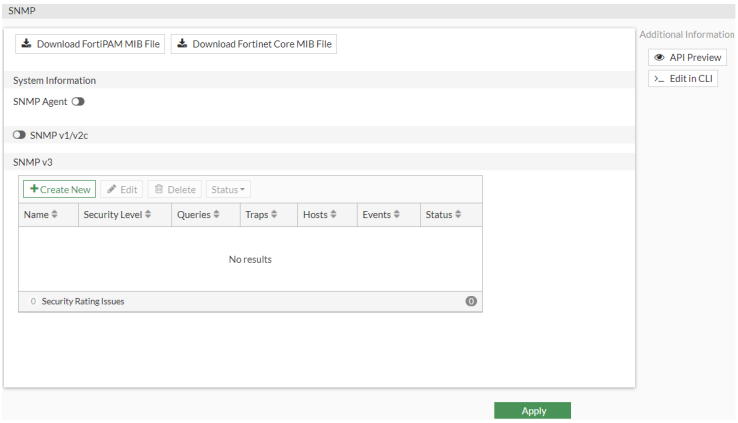


For security reasons, Fortinet recommends that neither “public” nor “private” be used for SNMP community names.



If you want to allow SNMP access on an interface, you must go to *Network* > *Interfaces* and select *SNMP* in *Administrative Access* in the settings for the interface that you want the SNMP manager to connect to.

For SNMP configuration, go to *System* > *SNMP*.





Hover over the leftmost edge of the column heading to display the *Configure Table* icon, which you can use to select the columns to display or to reset all the columns to their default settings. You can also drag column headings to change their order.

Configure the following settings and click *Apply*.

Download FortiPAM MIB File	Download the FortiPAM MIB file.
Download Fortinet Core MIB File	Download the Fortinet MIB file. See Fortinet MIBs on page 443.
System Information	
SNMP Agent	Enable the FortiPAM SNMP agent. See SNMP agent on page 444.
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 445.
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 447.
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 441.

Your SNMP manager may already include standard and private MIBs in a compiled database that is ready to use. You must add the Fortinet proprietary MIB to this database to have access to the Fortinet-specific information.



MIB files are updated for each version of FortiPAM. When upgrading the firmware, ensure that you update the Fortinet FortiPAM MIB file compiled in your SNMP manager as well.

MIB file name	Description
FORTINET-CORE-MIB.mib	The Fortinet MIB includes all system configuration information and trap information that is common to all Fortinet products. Your SNMP manager requires this information to monitor FortiPAM unit configuration settings and receive traps from the FortiPAM SNMP agent.

MIB file name	Description
FORTINET-FortiPAM-MIB.mib	The FortiPAM MIB includes all system configuration information and trap information that is specific to FortiPAM units. Your SNMP manager requires this information to monitor FortiPAM configuration settings and receive traps from the FortiPAM SNMP agent. FortiManager systems require this MIB to monitor FortiPAM units.

SNMP get command syntax

Normally, to get configuration and status information for a FortiPAM unit, an SNMP manager would use an SNMP get command to get the information in a MIB field. The SNMP get command syntax would be similar to:

```
snmpget -v2c -c <community_name> <address_ipv4> {<OID> | <MIB_field>}
```

where:

- `<community_name>` refers to the SNMP community name added to the FortiPAM configuration. You can add more than one community name to a FortiPAM SNMP configuration. The most commonly used community name is public. For security reasons, Fortinet recommends that neither public nor private be used for SNMP community names.
- `<address_ipv4>` is the IP address of the FortiPAM interface that the SNMP manager connects to
- `{<OID> | <MIB_field>}` is the object identifier for the MIB field or the MIB field name itself.

For example, to retrieve the serial number of the FortiPAM device, the following command could be issued:

```
snmpget -v2c -c fortinet 192.168.1.110 1.3.6.1.4.1.12356.100.1.1.1.0
```

```
iso.3.6.1.4.1.12356.100.1.1.1.0 = STRING: "FPXVM2TM22000445"
```

In this example, the community name is fortinet, the IP address of the interface configured for SNMP management access is `192.168.1.110`. The serial number of the FortiPAM device is queried using the OID:

`1.3.6.1.4.1.12356.100.1.1.1.0`.

SNMP agent

The FortiPAM SNMP agent must be enabled before configuring other SNMP options. Enter information about the FortiPAM unit to identify it so that when your SNMP manager receives traps from the FortiPAM unit, you will know which unit sent the information.

To configure the SNMP agent in the GUI:

1. Go to *System* > *SNMP*.
2. Enable *SNMP Agent*.
3. Enter a description for the agent. The description can be up to 255 characters long.
4. Enter the physical location of the unit. The system location description can be up to 255 characters long.
5. Enter the contact information for the person responsible for this FortiPAM unit. The contact information can be up to 255 characters.
6. Click *Apply* to save your changes.

To configure the SNMP agent with the CLI:

Enter the following CLI commands:

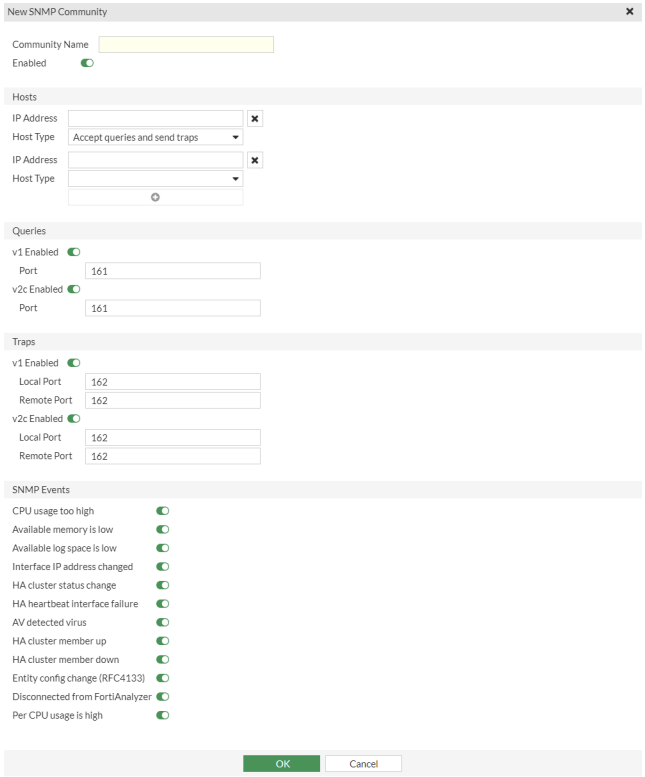
```
config system snmp sysinfo
   set status enable
   set contact-info <contact_information>
   set description <description_of_FortiPAM>
   set location <FortiPAM_location>
end
```

Creating or editing an SNMP community

An SNMP community is a grouping of devices for network administration purposes. Within that SNMP community, devices can communicate by sending and receiving traps and other information. One device can belong to multiple communities, such as one administrator terminal monitoring both a firewall SNMP and a printer SNMP community.

Add SNMP communities to your FortiPAM unit so that SNMP managers can view system information and receive SNMP traps. You can add up to three SNMP communities. Each community can have a different configuration for SNMP queries and traps and can be configured to monitor the FortiPAM unit for a different set of events. You can also add the IP addresses of up to sixteen SNMP managers to each community.

Enabling *SNMP v1/v2c* and selecting *Create New* in the *SNMP v1/v2c* pane opens the *New SNMP Community* page, which provides settings for configuring a new SNMP community. Double-clicking a community from the SNMP v1/v2c table opens the *Edit SNMP Community* page. Alternatively, select a community from the list and then select *Edit* to edit the SNMP community.

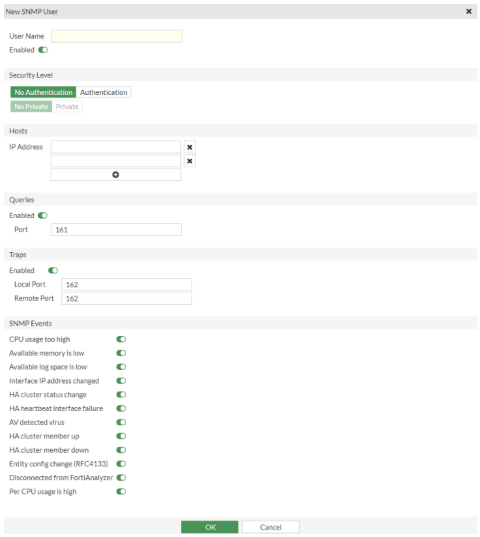


Configure the following settings in the *New SNMP Community* page or *Edit SNMP Community page* and click *OK*:

Community Name	Enter a name to identify the SNMP community. After you create the SNMP community, you cannot edit the name.
Enabled	Enable or disable the SNMP community.
Hosts Settings for configuring the hosts of an SNMP community.	
IP Address	Enter the IP address/netmask of the SNMP managers that can use the settings in this SNMP community to monitor the unit. You can also set the IP address to 0.0.0.0 to so that any SNMP manager can use this SNMP community.
Host Type	Select one of the following: *Accept queries and send traps*, *Accept queries only*, or *Send traps only*.
X	Removes an SNMP manager from the list within the *Hosts* section.
+	Select to add a blank line to the Hosts list. You can add up to 16 SNMP managers to a single community.
Queries Settings for configuring queries for both SNMP v1 and v2c.	
v1 Enabled	Enable or disable SNMP v1 queries.
Port	Enter the port number (161 by default) that the SNMP managers in this community use for SNMP v1 and SNMP v2c queries to receive configuration information from the unit. The SNMP client software and the unit must use the same port for queries.
v2c Enabled	Enable or disable SNMP v2c queries.
Traps Settings for configuring local and remote ports for both v1 and v2c.	
v1 Enabled	Enable or disable SNMP v1 traps.
Local Port	Enter the local port numbers (162 by default) that the unit uses to send SNMP v1 or SNMP v2c traps to the SNMP managers in this community. The SNMP client software and the unit must use the same port for traps.
Remote Port	Enter the remote port number (162 by default) that the unit uses to send SNMP traps to the SNMP managers in this community. The SNMP client software and the unit must use the same port for traps.
v2C Enabled	Enable or disable SNMP v2c traps.
SNMP Events Enable each SNMP event for which the unit should send traps to the SNMP managers in this community. **Note**: The **CPU usage too high** trap's sensitivity is slightly reduced by spreading values out over 8 polling cycles. This reduction prevents sharp spikes due to CPU intensive short-term events such as changing a policy.	

Creating or editing an SNMP user

Selecting *Create New* in the *SNMP v3* pane opens the *New SNMP User* page, which provides settings for configuring a new SNMP v3 user. Double-clicking a user from the SNMP v3 table opens the *Edit SNMP User* page. Alternatively, select an SNMP user and then select *Edit* to edit the SNMP user.



Configure the following settings in the *New SNMP User* page or *Edit SNMP User* page and click *OK*:

User Name	Enter the name of the user. After you create an SNMP user, you cannot change the user name.
Enabled	Enable or disable this SNMP user.
Security Level Select the type of security level the user will have: • *No Authentication* • *Authentication* and *No Private*—Select the authentication algorithm and enter password to use. • *Authentication* and *Private*—Select the authentication and encryption algorithm and enter the passwords to use.	
Authentication/Encryption Algorithm	If the security level is set to *Authentication* and *No Private*, you can select from the following authentication algorithms: • *MD5* • *SHA1* (default) • *SHA224* • *SHA256* • *SHA384* • *SHA512* If the security level is set to *Authentication* and *Private*, you can also select from the following encryption algorithms in addition to authentication algorithms: • *AES* (default) • *DES* • *AES256*

	• *AES256 Cisco*
Password	If the security level is set to *Authentication*, select *Change* and enter a password in the *Password* field.
Hosts Settings for configuring the hosts of an SNMP community.	
IP Address	Enter the IP address of the notification host. If you want to add more than one host, select + to add another host. Up to 16 hosts can be added. Select *X* to delete any hosts.
Queries Settings for configuring queries for both SNMP v1 and v2c.	
Enabled	Enable or disable the query. By default, the query is enabled.
Port	Enter the port number in the *Port* field (161 by default).
Traps Settings for configuring local and remote ports for both v1 and v2c.	
Enabled	Enable or disable the trap.
Local Port	Enter the local port number (162 by default).
Remote Port	Enter the remote port numbers (162 by default).
SNMP Events Select the SNMP events that will be associated with the user.	

Configuration 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 24.
- 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.

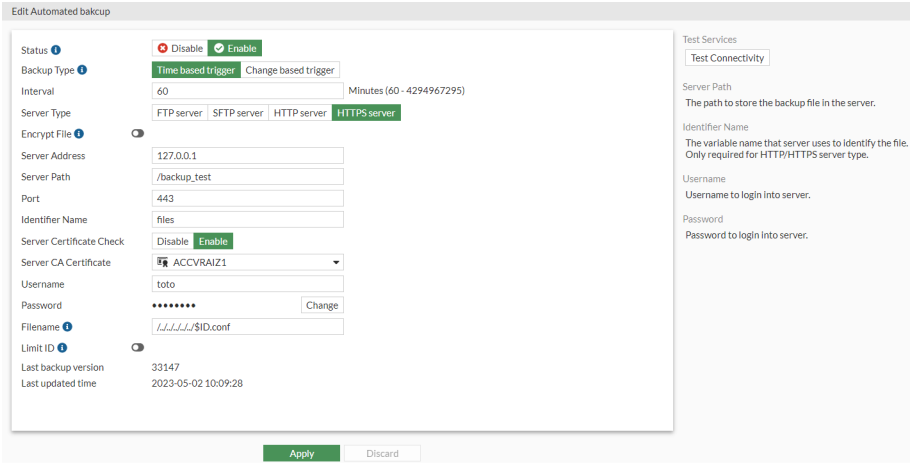
To ensure that all credentials are correct in a configuration file, you can enable maintenance mode first so that no password changer is executed. And then manually trigger the configuration backup. See *Activate maintenance mode* in Admin on page 24.

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*.
2. Open the *Configuration Backup* tab.

   The *Edit Automated backup* window opens.



3. 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).

4. Click *Apply*.
5. 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:

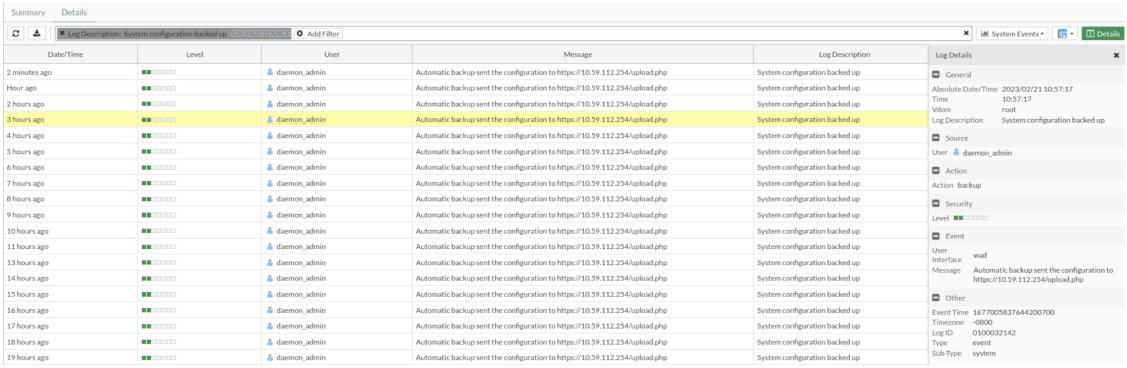
```
    diagnose test application wad
WAD process 1080 test usage:

....
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.



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 455
- Back up video files on page 455
- Restore log files on page 456
- Restoring video files on page 456
- Breakpoint resume for video files on page 457



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 455.



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 455.



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

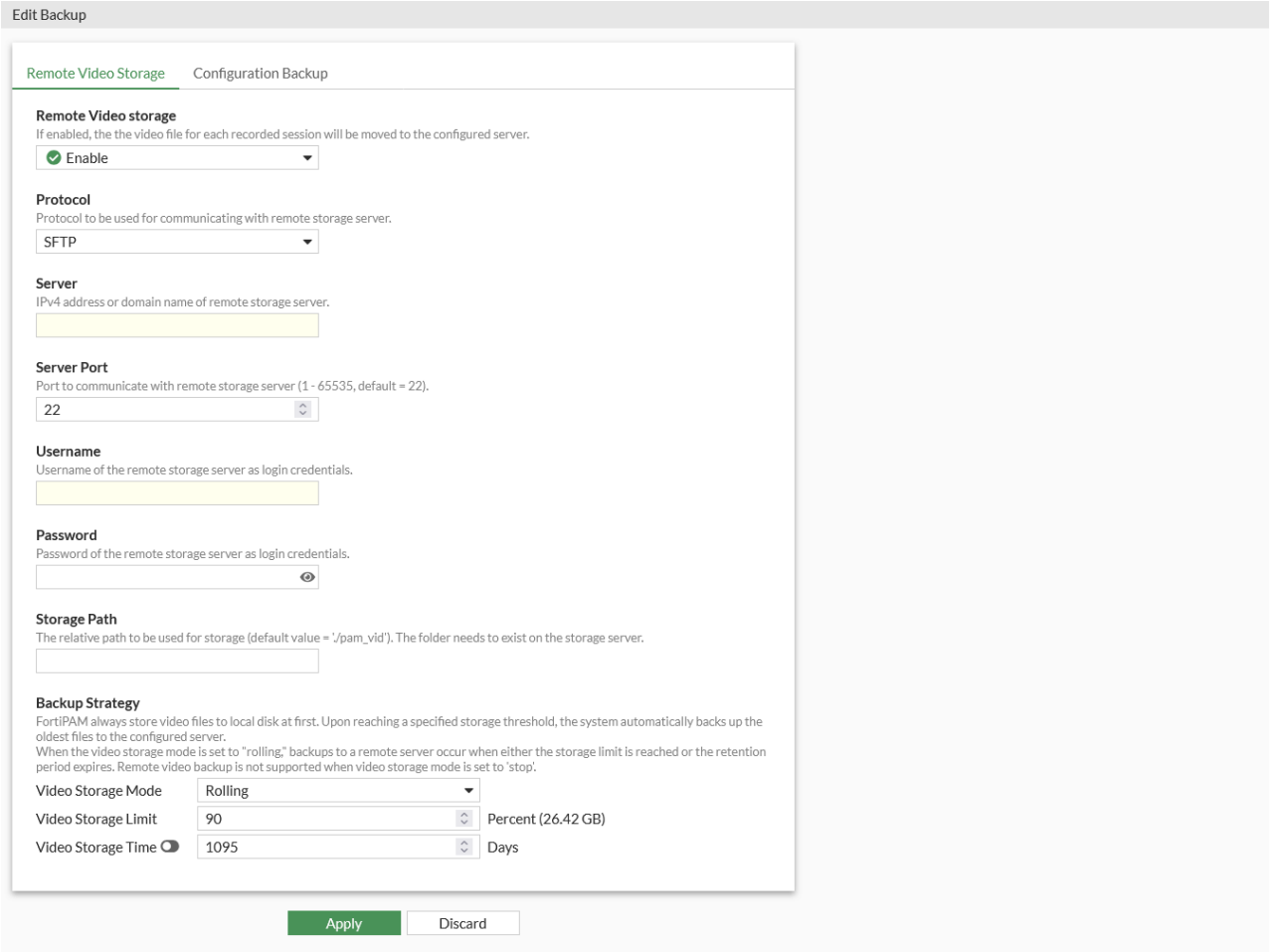
If a backup/restore process is broken, the file already backed up and restored is not transferred again to the following backup/restore process.

Remote video storage

You can configure remote video storage settings on FortiPAM. When remote video storage is enabled, video files for recorded sessions will be moved to the configured remote server once a storage threshold is met, helping you to avoid large diskspace requirements for video storage on FortiPAM. You can send videos to external storage through the SFTP protocol.

To update remote video storage settings:

1. Go to *System* > *Backup*.
2. Open the *Remote Video Storage* tab.
3. Configure the remote video storage settings:



Remote Video storage	Enable or disable remote video storage. When enabled, the video file for each recorded session will be moved to the configured server.  The remote video storage feature only works when the *Video Storage Mode* is *Rolling*.
Protocol	Select the protocol to be used for communicating with the remote storage server. Supported protocols include SFTP.
Server	Enter the IPv4 address or domain name of the remote storage server.
Server Port	Enter the port used for communication with the remote storage server (1 - 65535). The default port is 22.
Username	Enter the username for the remote storage server as login credentials.
Password	Enter the password for the remote storage server as login credentials.
Storage Path	The relative path to be used for storage (default value = './pam_vid'). The folder needs to exist on the storage server.
Backup Strategy	Configure the backup strategy settings. FortiPAM always stores video files to local disk first. Upon reaching a specified storage threshold, the system automatically backs up the oldest files to the configured server. When certain conditions are met, the system automatically backs up the oldest (or expired) video files to the configured remote server. There are two events that can trigger FortiPAM to start backing up the local video files to the remote server: • When the local video disk used space reaches a configured storage threshold, i.e., it reaches the value set in *Video Storage Limit*. • A video file stored in the FortiPAM local disk is longer than the configured *Video Storage Time*. Configure the following:

Video Storage Mode	Choose the storage mode. When the video storage mode is set to *Rolling* backups to a remote server occur when either the storage limit is reached or the retention period expires. Remote video backup is not supported when video storage mode is set to set to *Stop*.
Video Storage Limit	Configure the video storage limit as a percentage. When the storage is exceeded, videos are rolled to external storage, beginning with the oldest available videos.

Video Storage Time	Set the number of days that videos will remain in storage, or select the toggle button to configure storage for unlimited days.



Once the video files are successfully backed up to the remote server, they will be deleted from the local disk and cannot be played back on FortiPAM.

4. Click *Apply*.

Updating the remote video storage settings using the CLI

To update the remote video storage settings using the CLI:

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

```
config secret remote-storage
 set status enable
 set server "192.168.1.100"
 set username "pam_user1"
 set password "ENC xxx"
 set storage-path '' #leave it empty for the default value = './pam_vid'
end
```

How to play back FortiPAM videos from the external server

To play back FortiPAM videos from the external server:

1. Locate the video folder on the remote server.
   To externally view the video recording of a secret launch session, you first need to locate the folder path of the video.
   a. On the FortiPAM GUI, go to *Log & Report* > *Secret Event & Video* and locate the *video upload finished* log entry for the video.
   b. Double-click the video log entry to open the *Log Details* window.
   c. Make note of *Video Folder Name* and the *Token Id*.
      `$(Video Storage Path)/$(Video Folder Name)/$(Token Id)` is the folder path for the video session in the remote server where `$(Video Storage Path)` is the configured root folder in the remote server used for FortiPAM remote video storage.
      For example, for a customer using video storage path `/home/josh/pam_vid` with `10,211,445` as the `$(Token Id)` and `1,797` as the `$(Video Folder Name)`, `/home/josh/pam_vid/1797/10211445` is the video recording folder path on the remote storage server.
2. For customers not using *Live Recording*, there is a `WebM` file in the folder that can be played back with the video player or the web browser.
3. For customers using *Live Recording*, you can see `.chk` files and a manifest file in the folder.
   Use the following command to assemble the chunk files:

```
ffmpeg -allowed_extensions ALL -i manifest.mpd -codec copy out.mkv
```

   The generated `out.mkv` is a playable video file.

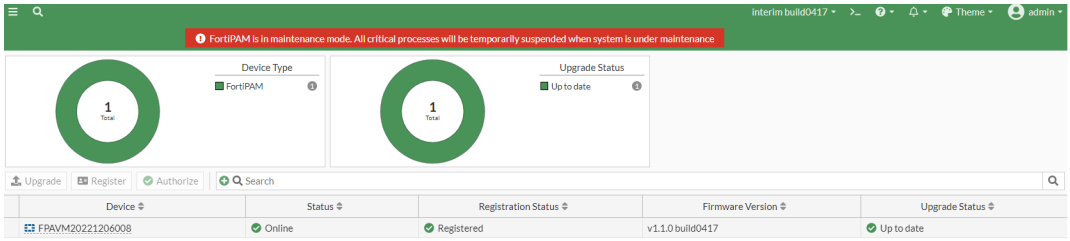
Firmware

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

The widgets at the top display:

- The total number of FortiPAM devices.
- The upgrade status of the FortiPAM devices.

The *Firmware* tab displays the device name, device status, registration status, firmware version, and the upgrade status.



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

Upgrade	Upgrade the FortiPAM firmware. See Uploading a firmware on page 26.
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 27.

To be able to upgrade the firmware, you must first register your FortiPAM with Fortinet. See Licensing on page 49.

To upgrade the firmware from FortiPAM GUI, see Uploading a firmware on page 26.



Always review all sections in *FortiPAM Release Notes* prior to upgrading your device.

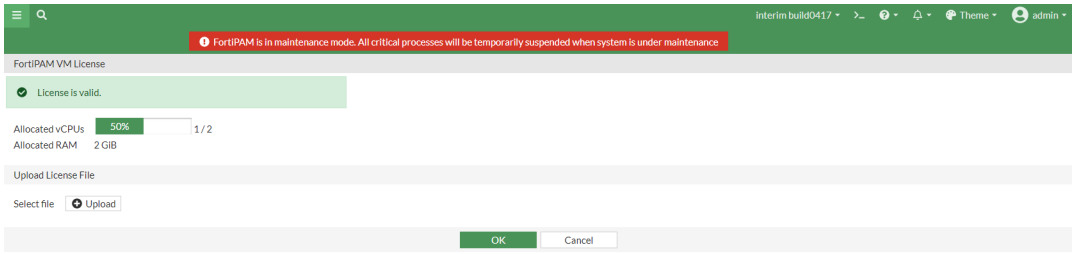
FortiPAM license

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 24.

To upload a new license:

1. Go to *System* > *FortiPAM License*.
   The *FortiPAM VM License* window opens.



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

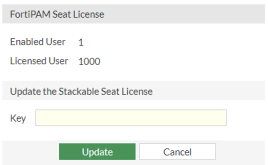
Use the CLI command `get system status` to verify the license status.

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.



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 61.

Setup wizard

The FortiPAM setup wizard gathers all essential settings to setup a FortiPAM from scratch and provide useful information to the new users.

To access the setup wizard, go to *System* > *Setup Wizard*.

Prerequisites

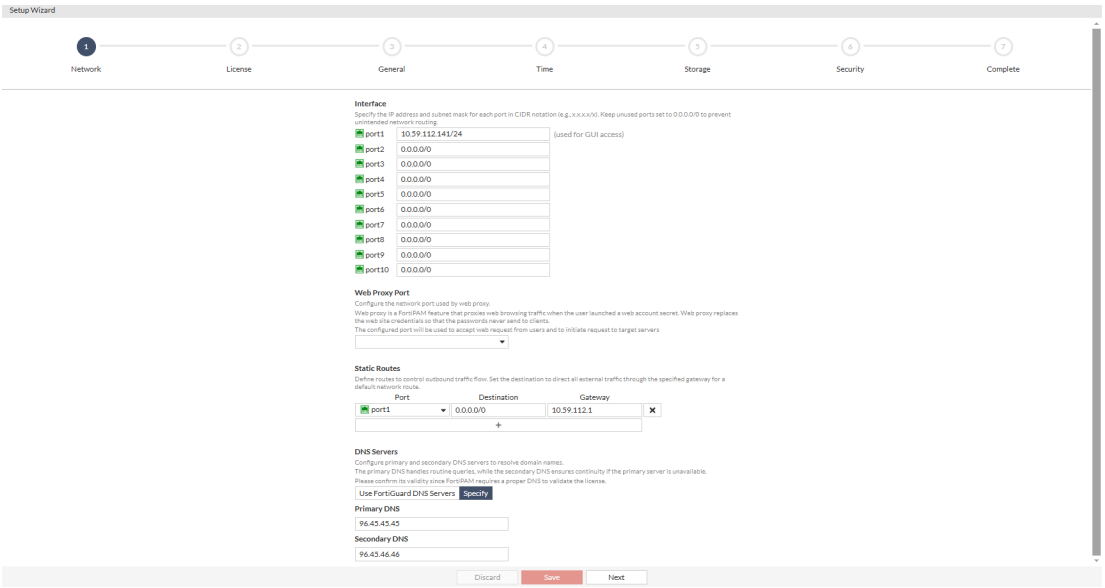
- Installed FortiPAM
- The GUI IP address is already set up

If this is a fresh FortiPAM setup, the wizard is the default page once you log in to FortiPAM.

For an existing FortiPAM instance, the wizard is available in *System*.

Setting up FortiPAM

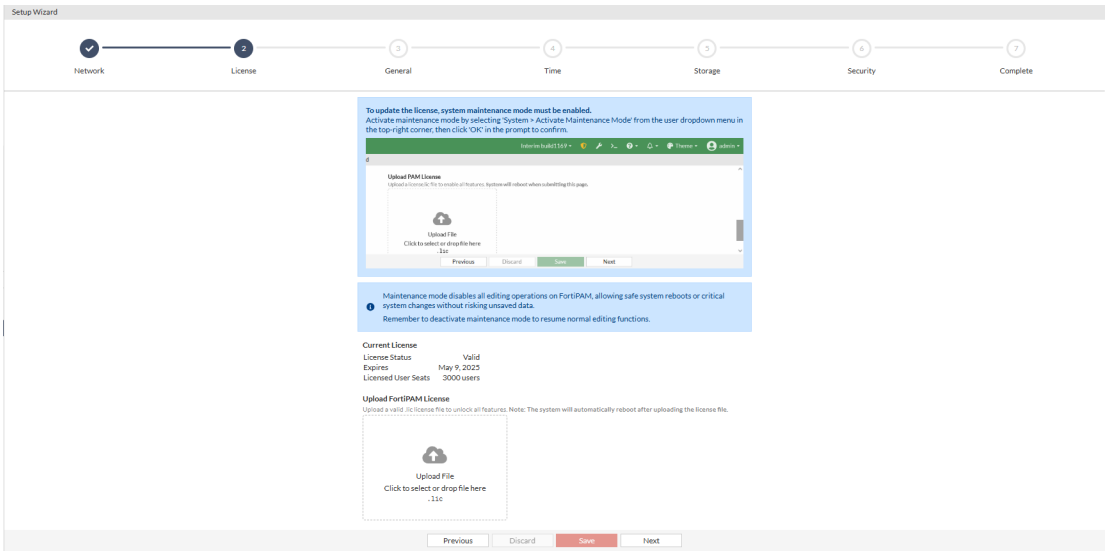
1. Go to *System* > *Setup Wizard*.
   The *Network* tab opens.



The following information is displayed:

Interface	Specify the IP address and the subnet mask for each port in CIDR notation, e.g., `x.x.x.x/x`. Keep the unused ports set to `0.0.0.0/0` to prevent unintended network routing.
Web Proxy Port	Configure the network port used by the web proxy. Web proxy allows FortiPAM to proxy the web browsing traffic when you launch a web account secret. Web proxy replaces the web credentials so that the password is never available to the client. The configured port is used to accept web requests to initiate request to the target server.
Static Routes	Define routes to control the outbound traffic. Set the destination to direct all the external traffic through the specified gateway for the default network route.
DNS Servers	Configure the primary and the secondary DNS servers to resolve the domain names. The primary DNS handles routine queries while the secondary DNS ensures continuity if the primary server is unavailable. FortiPAM requires DNS to validate the license.

2. Click *Next*.
   The *License* tab opens.
   The *License* tab displays how to update the license



See FortiPAM license on page 460.

To update the license, maintenance mode must be enabled. See Maintenance mode.

The maintenance mode disables editing operations on FortiPAM to allow safe system reboots or critical system changes without risking the unsaved data.

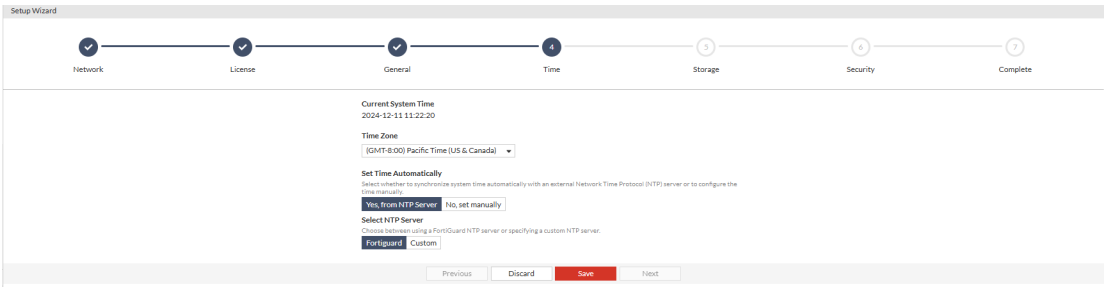
Note: Remember to deactivate the maintenance mode to resume normal editing functions.

In *Upload FortiPAM License*, you can upload a valid `.lic` file.

3. Click *Next*.
The *General* tab opens.
The following information is available.

Hostname	Specify the hostname for the FortiPAM unit.
Max Secret Launching Duration	Set the maximum duration for sessions. Any session exceeding the time list is terminated automatically (default = 120). For example, if set to 60 minutes and you launch a secret through remote desktop and forget to end the session, the session will be automatically terminated after 60 minutes.
Live Recording	Enable live recording to monitor the user session in real-time (default = disable). If disabled, recordings are accessible only after the session ends.

4. Click *Next*.
The *Time* tab opens.

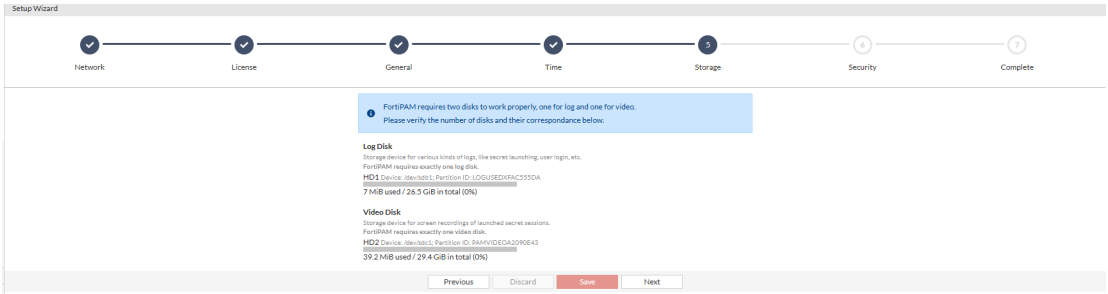


The following information is displayed.

Current System Time	The current system time.
Timezone	From the dropdown, select the timezone.
Set Time Automatically	Select whether to synchronize the system time automatically with an external Network Time Protocol (NTP) server or to configure the time manually. When you select *No, set manually*, enter the date and time.
Select NTP Server	Choose between using a FortiGuard NTP server or specify a custom NTP server. When you select *Custom*, enter the NTP server IP address.

5. Click *Next*.
The *Storage* tab opens.

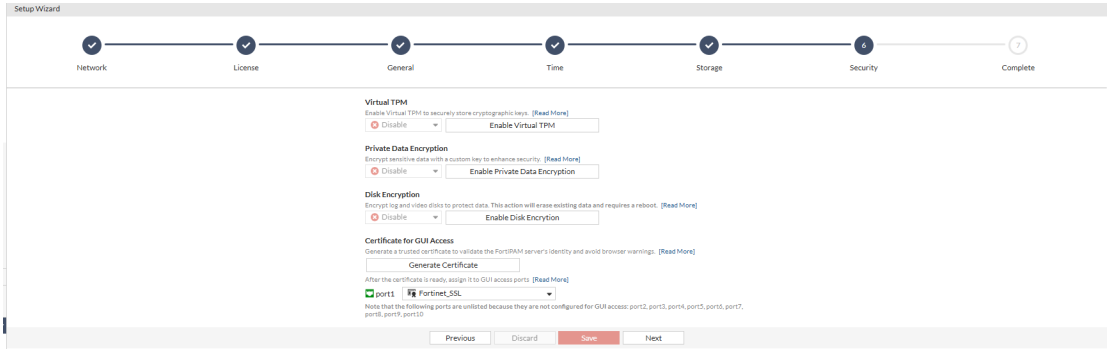
Note: FortiPAM requires two disks to work; one for log and another for video.



The following information is displayed.

Log Disk	The storage device for various kinds of logs, e.g., secret launching, user login, etc.
Video Disk	The storage device for screen recording the launched secret sessions. **Note**: FortiPAM requires exactly one video disk.

6. Click *Next*.
The *Security* tab opens.

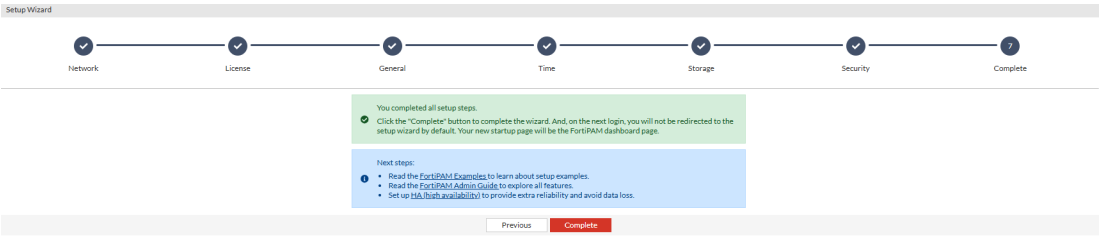


The following information is displayed.

Virtual TPM	Enable vTPM to securely store cryptographic keys. Click *Enable Virtual TPM* to see the related CLI command.

	``` config system global set v-tpm enable end ``` You can either run the command yourself or click *Run the Command in CLI*. This opens a CLI console and the command runs automatically. **Note**: Maintenance mode is enabled.
Private Data Encryption	Encrypt sensitive date with a custom key to enhance security. Click *Enable Private Data Encryption* to see the related CLI command. ``` execute disk encrption enable ``` You can either run the command yourself or click *Run the Command in CLI*. This opens a CLI console and the command runs automatically. **Note**: Maintenance mode is enabled.
Disk Encryption	Encrypt log and video disks to protect data. **Note**: The action erases existing data and requires a reboot. Click *Enable Disk Encryption* to see the related CLI command. ``` execute disk encryption enable ``` You can either run the command yourself or click *Run the Command in CLI*. This opens a CLI console and the command runs automatically. **Note**: Maintenance mode is enabled.
Certificate GUI Access	Generate a trusted certificate to validate the FortiPAM server identity and avoid browser warnings. Select *Generate Certificate*. After the certificate is ready, assign it to the GUI access ports. **Note**: Ports not configured for GUI access are not listed.

7. Click *Next*.



8. Click *Complete*.

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 397.

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:

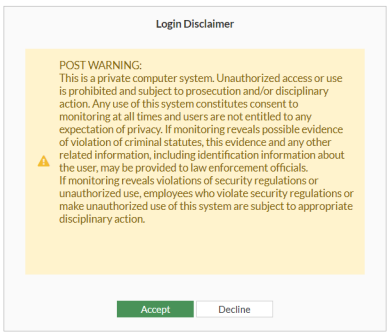
- Block additional concurrent admin sessions while an admin session is active (default).
- Terminate any previous sessions when the admin opens a new session.

See Settings on page 397.

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.





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 289.



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 473.

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 469.

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.

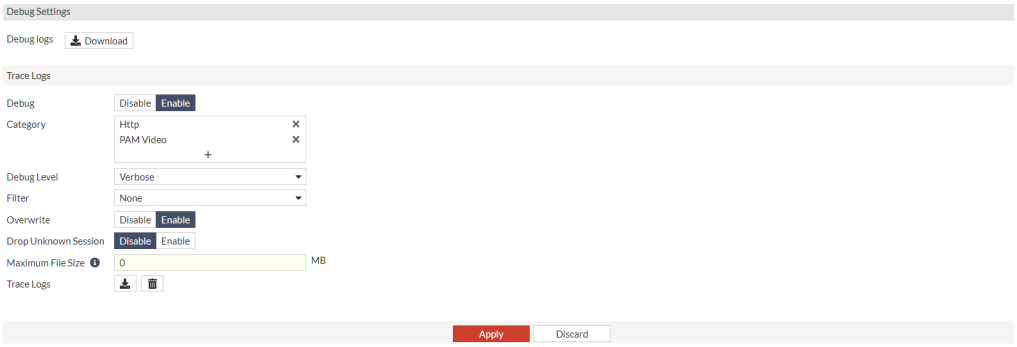
b. In the *Trace Logs* pane:

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*.



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\`.

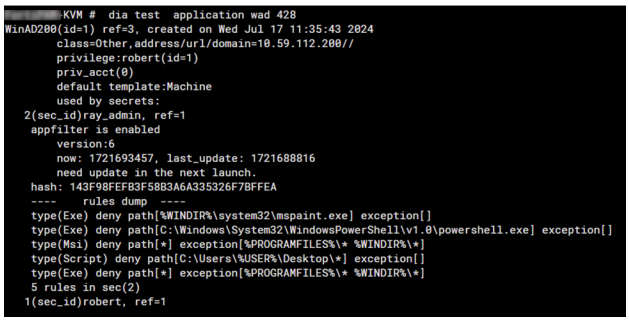


For the secret session video recordings and metadata files, go to the Windows Temp directory `C:\Windows\Temp`.

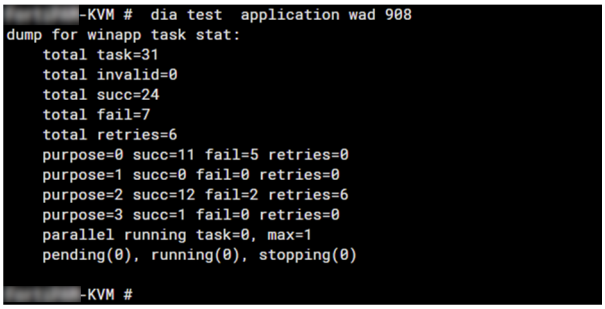
Troubleshooting Windows application filter

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
```




```
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.
```



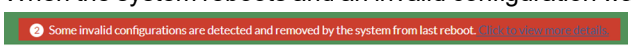
Issue: Some configurations are removed after last reboot

A new warning message appears alerting you that invalid configurations were detected and removed after a system reboot.

If needed, you can restore the invalid configuration.

To check the invalid configuration:

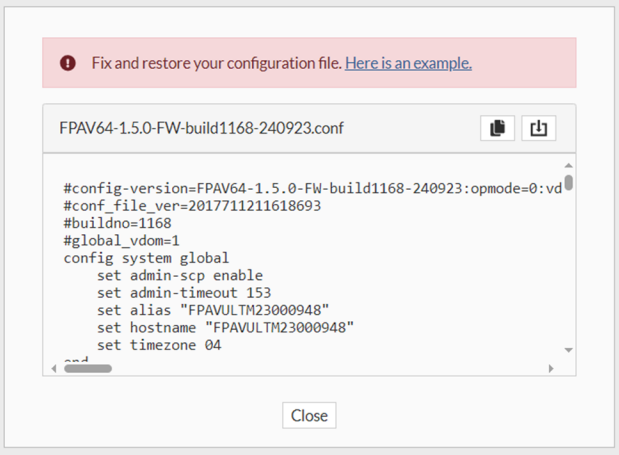
1. When the system reboots and an invalid configuration was detected, an alert is displayed on the banner.



Only an administrator with a role that has *Allow Firmware Upgrade & Backups* permission can see the alert message.

2. Select *Click to view more details* to see the old configuration file before the reboot.

If the administrator uses a role with *Allow CLI Diagnostic Commands* permission, they are able to see and execute the debug command.

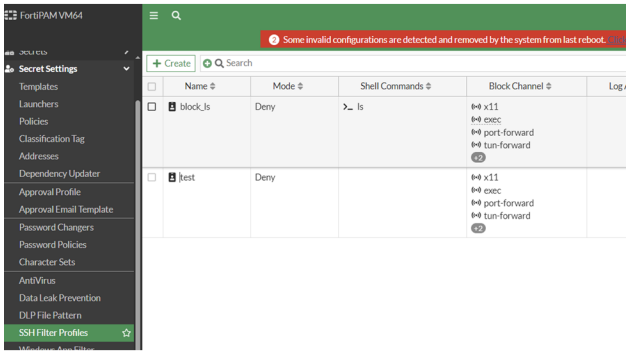


For example - Example:

A secret with ID 3 was removed. The secret is invalid as the *SSH Filter* option is enabled, but no SSH filter profile is applied.

To fix this:

a. Go to *Secret Settings* > *SSH Filter Profiles* and locate the desired SSH filter profile. Here, it is *block_ls*.

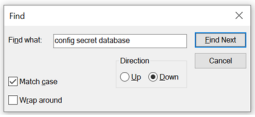


b. Download the previous configuration file shown in step 2 by clicking *Download file*.



c. Open the configuration file and locate `config secret database`.

```
        set creation-time 2024-06-28 13:27:52
        set web-proxy-status disable
        set sql-server-log-status disable
    next
end
config secret database
    edit 1
        set name "123"
        set uuid 99f351de-2dd3-51ef-537a-277e8d94d8c4
        set target "gavin test target"
```



d. Scroll to the secret with ID 3.

```
    edit 3
        set name "test_ssh"
        set uuid 1a8678be-7d2d-51ef-c7a5-30744db02d44
        set target "test"
        set creation-time 2024-09-27 17:03:34
        set folder 2
        set policy "policy"
        set template "FortiProduct (SSH Password)"
        set proxy enable
        set ssh-filter enable
        set ssh-service-status up
        config credentials-history
        end
        config field
            edit 1
                set name "Username"
                set value "345"
            next
        end
    next
nd
```

You will see that `ssh-filter` is enabled, but there is no attached `ssh-filter-profile`.

e. Add `set ssh-filter-profile "block_ls"` to the secret configuration.

```
set proxy enable
set ssh-filter enable
set ssh-filter-profile "block_ls"
set ssh-service-status up
```

f. Save the configuration file.

g. Enable the maintenance mode by going to the user dropdown on the top-right and selecting *Activate Maintenance Mode* in *System*.



The maintenance mode can only be activated by an administrator with *Set Maintenance Mode* permission enabled.

h. In the *Warning* dialog:

i. Enter the maximum duration, in minutes.

ii. Enter a reason for activating the maintenance mode.

iii. Click *OK*.

i. Go to the user dropdown on the top-right and select *Restore* in *Configuration*.

j. In *File*, select *Upload*:

i. Locate the updated configuration file from your management computer.

ii. Click *Open*.

k. Click *OK*.

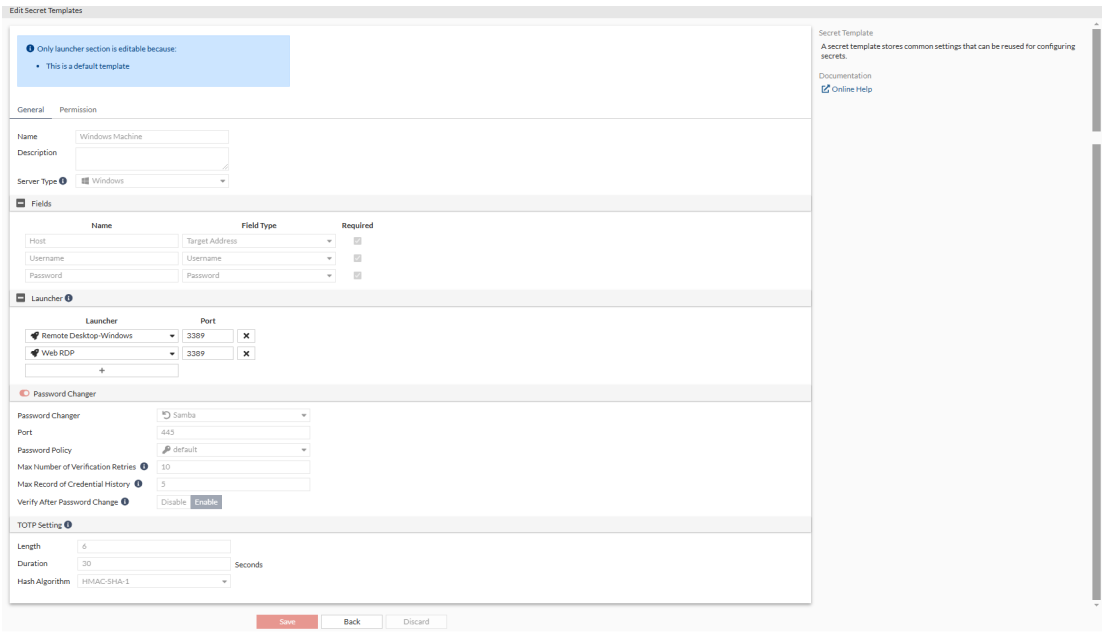
The system reboots. This may take a few minutes.

l. Verify that the configurations are fixed.

The warning message in the banner about the invalid configuration disappears.

Troubleshooting a secret that uses Windows Machine template with the default SAMBA password changer

This topic includes troubleshooting tips for the *Windows Machine* template that uses the default *SAMBA* password changer.



Verifying password

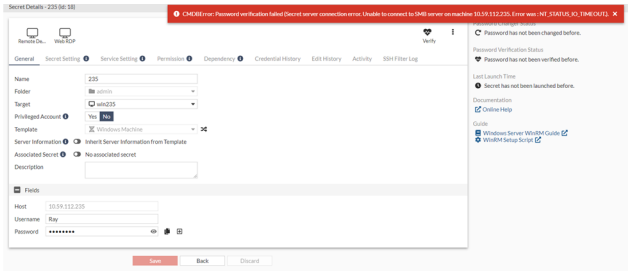
Prerequisite

- A secret with *Windows Machine* template that uses *SAMBA* password changer.

Scenario 1

When attempting to verify the password, the following error is displayed:

```
CMDBError: Password verification failed (Secret server connection error. Unable to
connect to SMB server on machine. Error was: NT_STATUS_IO_TIMEOUT.).
```



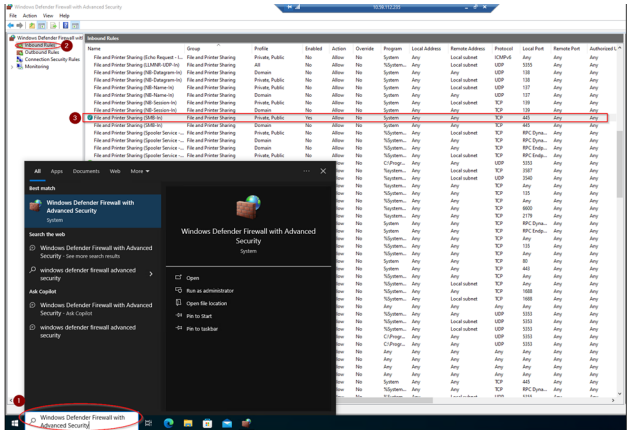
Cause

A firewall policy blocking the SMB traffic.

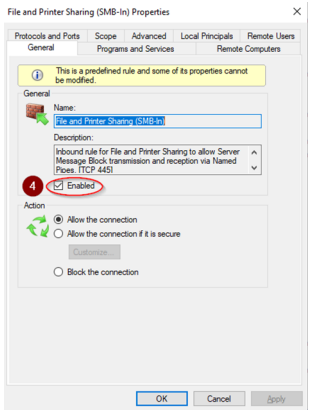
Resolution

Execute the following on the target machine:

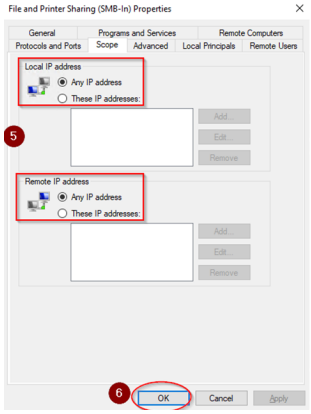
1. In the search bar on Windows, search for *Windows Defender Firewall with Advanced Security*.
2. Click *Inbound Rules*.



3. Go to *File and Printer Sharing (SMB-In)*.
4. Open and select *Enabled*.



5. Adjust the scope to include the FortiPAM IP address.



6. Click *OK*.

Change password

Prerequisites

- A secret with *Windows Machine* template that uses *SAMBA* password changer.
- The target machine has opened SMB in the firewall.
- Verify the password.

Scenario 1

When attempting to change the password, the following error is displayed:

```
Password change failed(machine rejected the password change: Error was : When trying to update a password, this return status indicates that the value provided as the current password is not correct.).
```

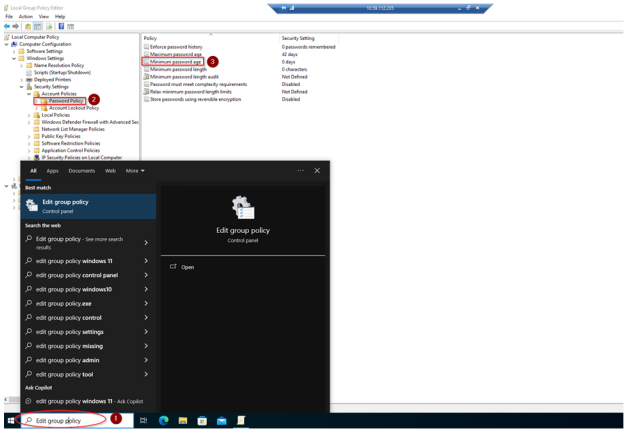
Cause

The target machine sets the *Minimum Password Age* preventing the users from changing the password frequently.

Resolution

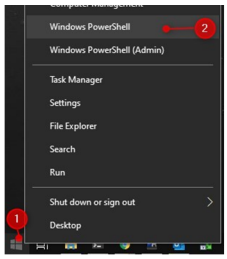
Resolution

1. In the search bar on Windows, search for *Edit group policy*.
2. Go to *Computer Configuration* > *Windows Settings* > *Security Settings* > *Account Policies* > *Password Policy*.

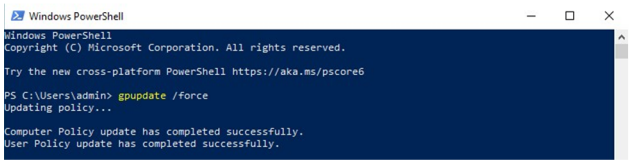


3. Select *Minimum password age* policy and modify the value to ensure it meets your requirements.
4. Additionally, review other policies in this directory to confirm that the FortiPAM password policy is compliant.

5. Update the group policy changes:
   a. Right-click the start menu and open Windows PowerShell.



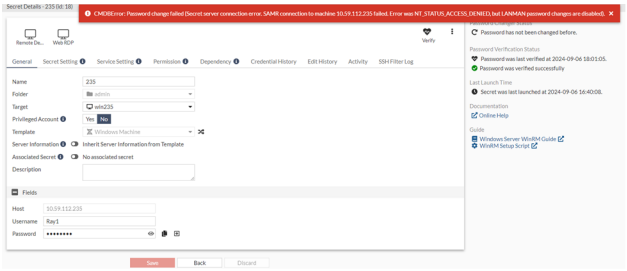
   b. Enter `gpupdate /force` and hit `Enter`.



Scenario 2

When attempting to change the password, the following error is displayed:

`CMDBError: Password change failed (Secret server connection error. SAMR connection to machine failed. Error was NT_STATUS_ACCESS_DENIED, but LANMAN password changes are disabled).`



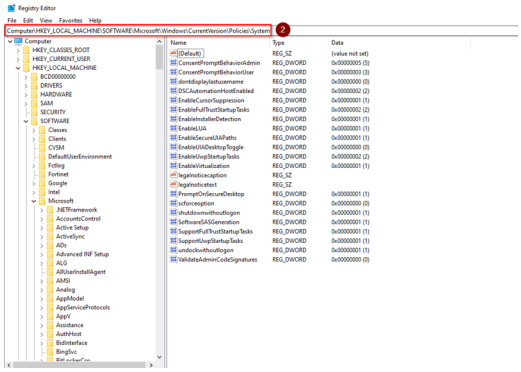
Cause

The target machine does not disable the UAC remote restrictions.

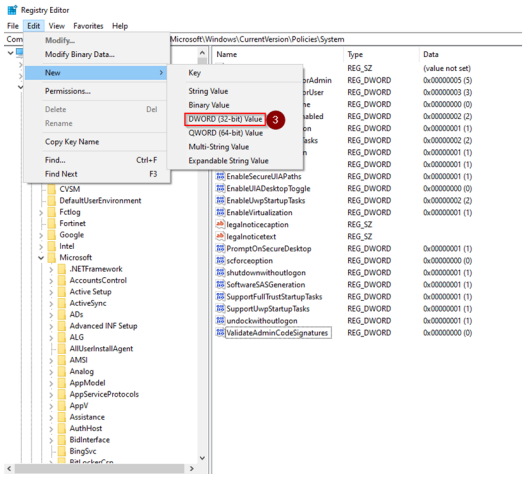
Resolution

1. Click *Windows Key* + *R*, enter `regedit`, and hit `Enter`.
2. Locate and click the following registry subkey:

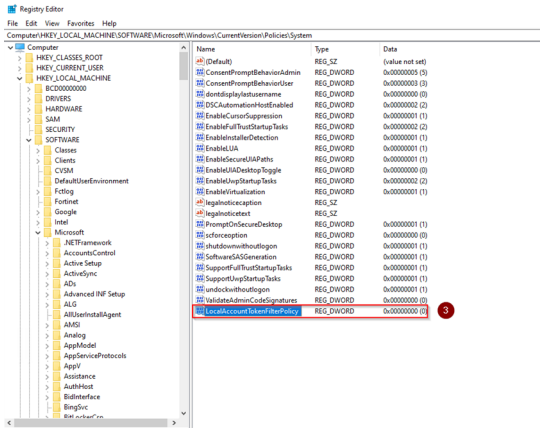
   `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`



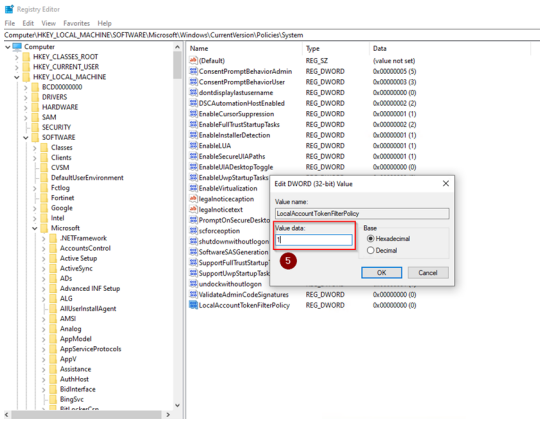
3. If the `LocalAccountTokenFilterPolicy` registry entry does not exist:
   a. In the *Edit* menu, go to *New*, and select *DWORD (32-bit) Value*.



   b. Right-click `LocalAccountTokenFilterPolicy` and select *Modify*.



4. In *Value data*, enter `1`, select *OK*.



5. Exit *Registry Editor*.

Abnormal traffic detection and resolution

Issue

When FortiPAM is behind a FortiGate and an access proxy is configured to access FortiPAM using a Virtual IP (VIP), on the FortiGate side, enabling `svr-pool-multiplex` on the access proxy can cause abnormal traffic to FortiPAM.

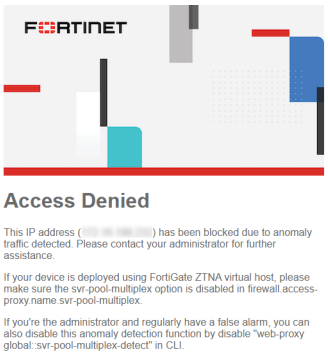
To detect the abnormal traffic on the FortiPAM side, a new global web proxy configuration has been introduced.

Web proxy global configuration

Use the following CLI configuration:

```
config web-proxy global
 set svr-pool-multiplex-detect {enable | disable} #default = enable
end
```

When abnormal traffic is detected, a warning page is displayed.



In this situation, FortiPAM is not accessible via the configured FortiGate access proxy VIP, but FortiPAM can still be accessed through its own instance VIP.

Resolution

To prevent this issue, it is suggested to disable the `firewall.access-proxy.svr-pool-multiplex` configuration on the FortiGate.

Firewall access proxy configuration

```
config firewall access-proxy
 edit "pam_test"
  set svr-pool-multiplex disable
 next
end
```

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 489
- Verify the private-data-encryption feature Example on page 490
- How to restore a backup configuration file with private-data-encryption enabled Example on page 490
- Enabling private-data-encryption on an HA cluster Example on page 491

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 46.

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 490.

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 489.

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 489, 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*.

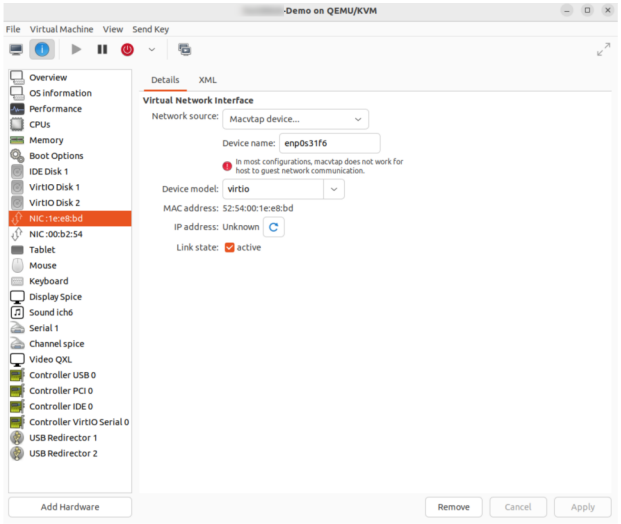
To add ethernet interfaces:

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*.



4. In the *Device model* dropdown, select *virtio*.
5. Click *Apply*.
6. Click *Add Hardware*, and select the option to add an additional interface.
7. In the *Device model* dropdown, select *virtio*.
8. Select *Finish*.
9. Click *Begin Installation* to start installing the new VM.

To add log/video disks or modify disk sizes after first powering up FortiPAM-VM:

1. In the CLI console, enter `sh sys storage` to verify that the disk size change was successful:

```
config system storage
  edit "HD1"
     set status enable
     set media-status enable
     set order 1
     set partition "LOGUSEDX83555B0F"
     set device "/dev/vda1"
     set size 20029
     set usage log
  next
  edit "HD2"
     set status enable
     set media-status enable
     set order 2
     set partition "PAMVIDEOBAED79CD"
     set device "/dev/vdb1"
     set size 301354
     set usage video
  next
  edit "HD3"
```

```
        set status enable
        set media-status disable
        set order 3
        set partition ''
        set device ''
```



If the displayed disk size is not what you had configured, enter the following command to format the log and the video disk:

```
execute disk format <disk_ref>
```

Note: `<disk_ref>` can be checked using the command execute disk list.



HD1 is used for the log disk and the `disk_ref` is 256.

HD2 is used for the video disk and the `disk_ref` is 16.

In the above example, disks can be formatted by entering the following commands:

```
execute disk format 256 #HD1
execute disk format 16 #HD2
```



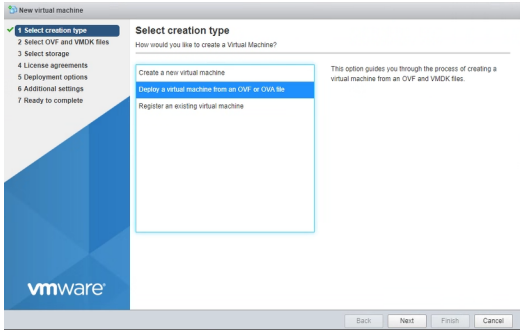
Disk formatting results in the loss of all existing logs and videos.

Appendix B: Installation on VMware

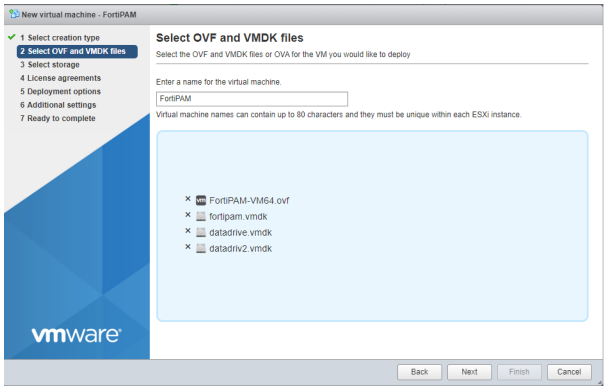
Once you have downloaded the `out.ovf.zip` file and extracted the package contents to a folder on your management computer, you can deploy it into your VMware environment.

To deploy the FortiPAM-VM OVF template:

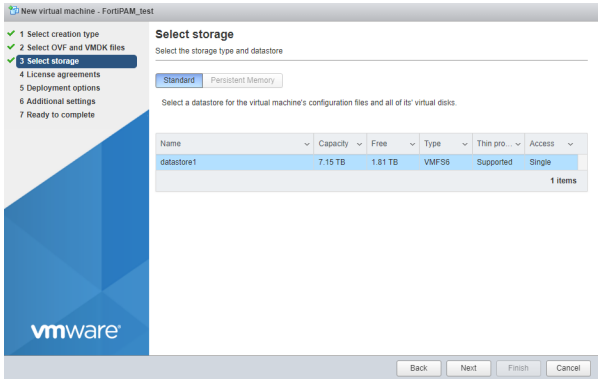
1. Connect to your VMware ESXi server by visiting its URL in your browser. Enter your username and password, and click *Log in*.
2. Select *Create/Register VM*.
   The VM creation wizard opens.
3. Select *Deploy a virtual machine from an OVF or OVA file*, and click *Next*.



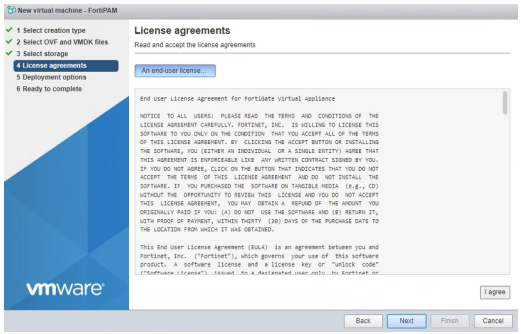
4. Enter a name for your VM and select the files (FortiPAM-VM64.ovf, fortipam.vmdk, datadrive.vmdk, and datadriv2.vmdk) previously extracted to your management computer, and click *Next*.



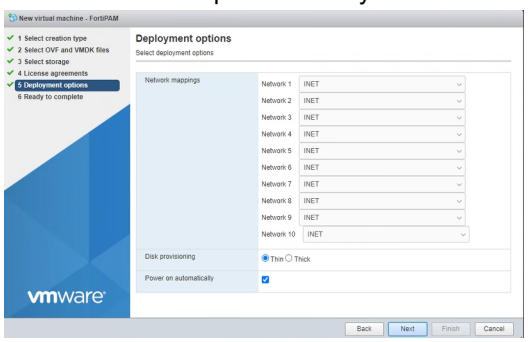
5. Select which ESXi server's datastore to use for the deployment of FortiPAM-VM, and click *Next*.



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

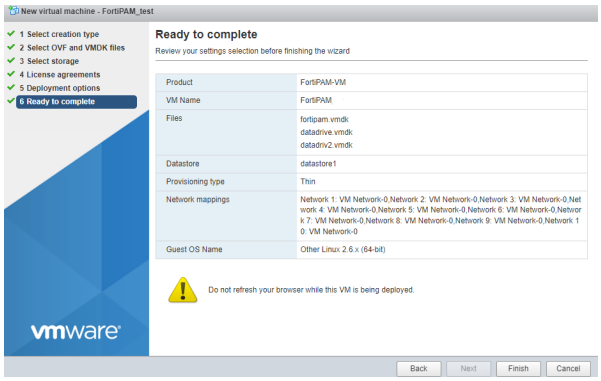


7. Select the appropriate network mappings, disk provisioning, and power on options for your deployment, and click *Next*.
   - **Thin Provision**: This option optimizes storage use at the cost of sub-optimal disk I/O rates. It allocates disk space only when a write occurs to a block, but the total volume size is reported by VMFS to the OS. Other volumes can take the remaining space. This allows you to float between your servers and expand storage when your size monitoring indicates there is a problem. Once a Thin Provisioned block is allocated, it remains in the volume regardless of whether you have deleted data, etc.
   - **Thick Provision**: This option has higher storage requirements, but benefits from optimal disk I/O rates. It allocates the disk space statically. No other volumes can take the allocated space.

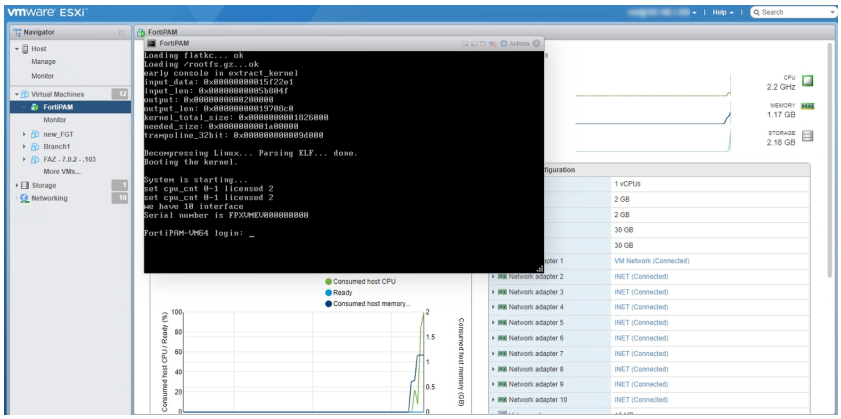


   By default, the log disk and video disk size are 30 GB. If you want to change the size, unselect *Power on automatically* to ensure that any disk size change is made before first powering on the VM.

8. Review the summary of your VM settings, and click *Finish*.



9. Select your newly created VM and launch it.
The VM console will be displayed where you can monitor the booting progress of your FortiPAM-VM.



See FortiPAM appliance setup on page 43 for CLI related settings to verify the disk usage type and set up FortiPAM.

10. The default size for the log and the video disk is 30 GB. If the size does not meet your requirement, see *Log and video disk size guidelines* in *System requirements* in the *VMware ESXi Admin Guide*.

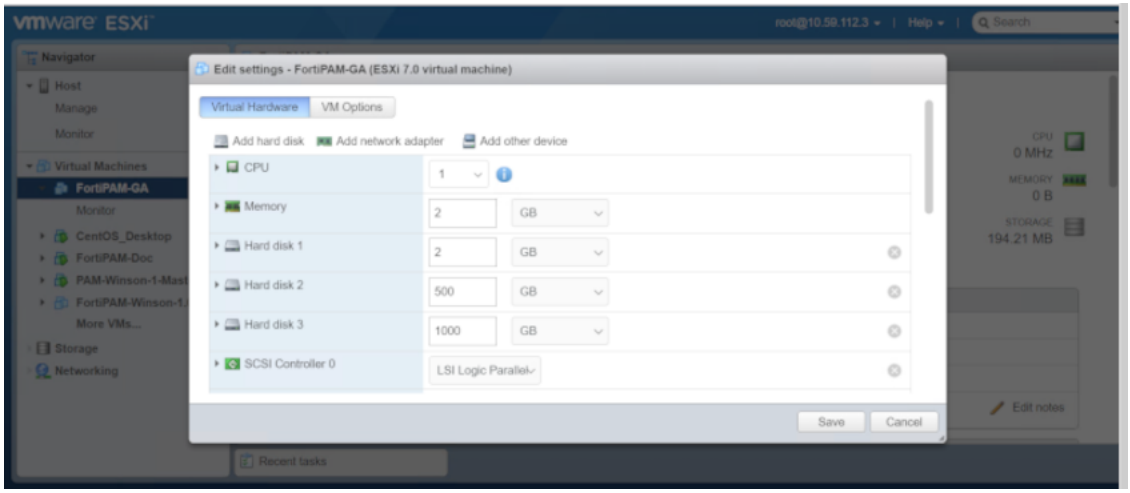
To adjust the log or video disk size:

Disk size tuning results in the loss of existing logs and videos.

---

a. Shutdown your VM.
b. In the VMware vSphere Client, right-click the name of the virtual appliance, and select *Edit settings*.
The *Edit settings* page is displayed.
c. Ensure that you are in the *Virtual Hardware* tab.
d. Keep *Hard disk 1* as 2 GB. *Hard disk 1* is used for FortiPAM bootup.

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



f. Click *Save* to save the changes.
You can now power on the VM.

11. If *Power on automatically* is unselected in step 7 and the VM has never been powered on, any disk size change automatically takes effect after the VM is powered on the first time.
If the disk sizes are tuned after powering on the VM for the first time, enter `sh sys storage` CLI command to verify that the disk size change was successful:

```
config system storage
   edit "HD1"
      set status enable
      set media-status enable
      set order 1
      set partition "LOGUSEDX83555B0F"
      set device "/dev/vda1"
      set size 20029
      set usage log
   next
   edit "HD2"
      set status enable
      set media-status enable
      set order 2
      set partition "PAMVIDEOBAED79CD"
      set device "/dev/vdb1"
      set size 301354
      set usage video
   next
   edit "HD3"
      set status enable
      set media-status disable
      set order 3
      set partition ''
      set device ''
```



If the displayed disk size is not what you had configured, enter the following command to format the log and the video disk:

```
execute disk format <disk_ref>
```

Note: `<disk_ref>` can be checked using the command execute disk list.



HD1 is used for the log disk and the `disk_ref` is 256.

HD2 is used for the video disk and the `disk_ref` is 16.

In the above example, disks can be formatted by entering the following commands:

```
execute disk format 256 #HD1
execute disk format 16 #HD2
```



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

Appendix C: Installing vTPM package on KVM and adding vTPM to FortiPAM-VM

For added security when installing FortiPAM on KVM, vTPM package must be installed, and vTPM added to the FortiPAM-VM.

To install vTPM package on KVM (Ubuntu):

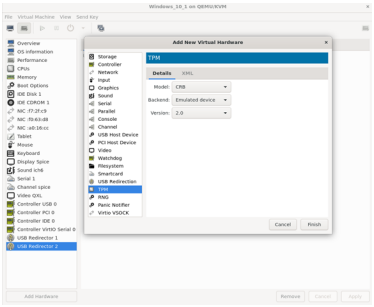
1. In the command line, enter the following commands:

```
 mkdir TPM_WorkSpace
cd TPM_WorkSpace/
git clone https://git.seabios.org/seabios.git
git clone https://github.com/stefanberger/libtpms.git
ls
cd libtpms
sudo apt-get -y install automake autoconf libtool gcc build-essential libssl-dev dh-
     exec pkg-config gawk
./autogen.sh --with-openssl --with-tpm2
make dist
dpkg-buildpackage -us -uc -j$(nproc)
cd ..
ls
sudo dpkg -i libtpms0_0.10.0~dev1_amd64.deb libtpms-dev_0.10.0~dev1_amd64.deb
git clone https://github.com/stefanberger/swtpm.git
cd swtpm
sudo su
ln -s /dev/null /etc/systemd/system/trousers.service
exit
sudo apt-get -y install libfuse-dev libglib2.0-dev libgmp-dev expect libtasn1-dev
     socat tpm-tools python3-twisted gnutls-dev gnutls-bin softhsm2 libseccomp-dev
     dh-apparmor libjson-glib-dev
dpkg-buildpackage -us -uc -j$(nproc)
dpkg -i swtpm_0.8.0~dev1_amd64.deb swtpm-dev_0.8.0~dev1_amd64.deb swtpm-libs_
     0.8.0~dev1_amd64.deb swtpm-tools_0.8.0~dev1_amd64.deb
```

To add vTPM when creating a FortiPAM-VM:

1. Deploy FortiPAM, see Appendix A: Installation on KVM on page 493.
2. Before opening the virtual machine for the first time, in the Virt-manager application, click *Add Hardware*.
3. From the menu, select *TPM*.
4. In the *Details* tab:
   a. In *Model*, select *CRB*.
   b. In *Backend*, select *Emulated device*.
   c. In *Version*, select *2.0*.

d. Click *Finish*.



This adds *TPM v2.0* to the list of hardware devices on the left.

Appendix D: vTPM for FortiPAM on VMware

To successfully enable vTPM, you must configure a key provider on the VMware vSphere client.



Ensure that TPM is set up as part of the initial configuration, i.e., before powering on the FortiPAM-VM for the first time.

To configure a key provider:

1. Select the virtual appliance in the VMware vSphere client and go to *Configure* > *Security* > *Key Providers*.
2. In *Key Providers*, from the *Add* dropdown, select *Add Native Key Provider*.
3. In the *Add Native Key Provider* window:
   a. Enter a name for the native key provider.
   b. Deselect *Use key provider only with TPM protected ESXi hosts*.
   c. Select *ADD KEY PROVIDER*.
4. Select the new key provider from the key providers list and then select *BACK UP*.
   The *Back up Native Key Provider* window opens.
5. Select *BACK UP KEY PROVIDER*.
   The key provider is saved on your computer.

To enable vTPM for FortiPAM:

1. Right-click the virtual appliance in the VMware vSphere client and select *Edit Settings*.



Ensure that the *Guest OS Version* in *VM Options* tab is set to *Other 4.x or later Linux (64-bit)* or higher.



Ensure that *Bootup* in *VM Options* is set as *EFI* rather than BIOS for firmware.

2. In *Edit Settings*, click *Add New Device* and select *Trusted Platform Module*.
3. Click *OK*.

Appendix E: Enabling soft RAID on KVM or VMware

To expand hard disk capacity, you can enable RAID on the FortiPAM-VM. After RAID is enabled, hard disk capacity can be expanded from 2 TB to 16 TB.

Individual disks of sizes up to 2 TB are supported.



Starting FortiPAM 1.1.0, the disk size is limited by the GPT partition size.

Soft RAID is supported on KVM and VMware platforms. Hyper-V and other platforms are not supported yet.

Note: Soft RAID for VMware requires disks of the same size.



RAID can only be configured using the CLI commands.



Enabling, disabling, and changing the RAID level, erases all the data on the log and video disk. Also, the FortiPAM device reboots every time RAID is enabled, disabled, or the RAID level is changed.

To configure RAID via CLI:

1. Before enabling RAID, enter the following command in the CLI console to verify that the FortiPAM has multiple disks:
   ```
   execute disk list
   ```
   or
   ```
   diagnose hardware deviceinfo disk
   ```

   Use `diagnose system disk info` to check the disk-related information.

2. In the CLI console, enter the following command to enable RAID:
   ```
   execute disk raid enable <RAID level> #The default value is Raid-0
   ```
   Two partitions will be created after RAID is enabled. One partition for log and one for video.

   To disable RAID, enter `execute disk raid disable`.



When there are two disks, RAID `level 0` and `1` are available. Only when there are four disks, RAID `level 5` and `10` are available.

3. From the *Admin* dropdown in the banner, go to *System* > *Reboot* to reboot FortiPAM.



Reboot is only available when FortiPAM is in maintenance mode.
To enable the maintenance mode, see Enabling maintenance mode.

4. In the *Reboot* window, click *OK* to confirm.
   Optionally, enter an event log message.
5. For the FortiPAM-VM, in the CLI console, check the RAID status by entering the following command:

```
execute disk raid status #Raid is now available
```



If the above steps do not enable RAID on FortiPAM-VM, use the following workaround:

1. Factory reset your FortiPAM-VM.
2. Remove disk from your FortiPAM-VM, then add the disk again.
3. Now follow the steps in Configuring RAID via CLI.

Rebuilding a RAID with a different RAID level

Admin can only rebuild RAID at the same RAID level if a RAID error has been detected. Also, changing the RAID level takes a while and deletes all data on the disk.

Use the following CLI command to rebuild RAID:

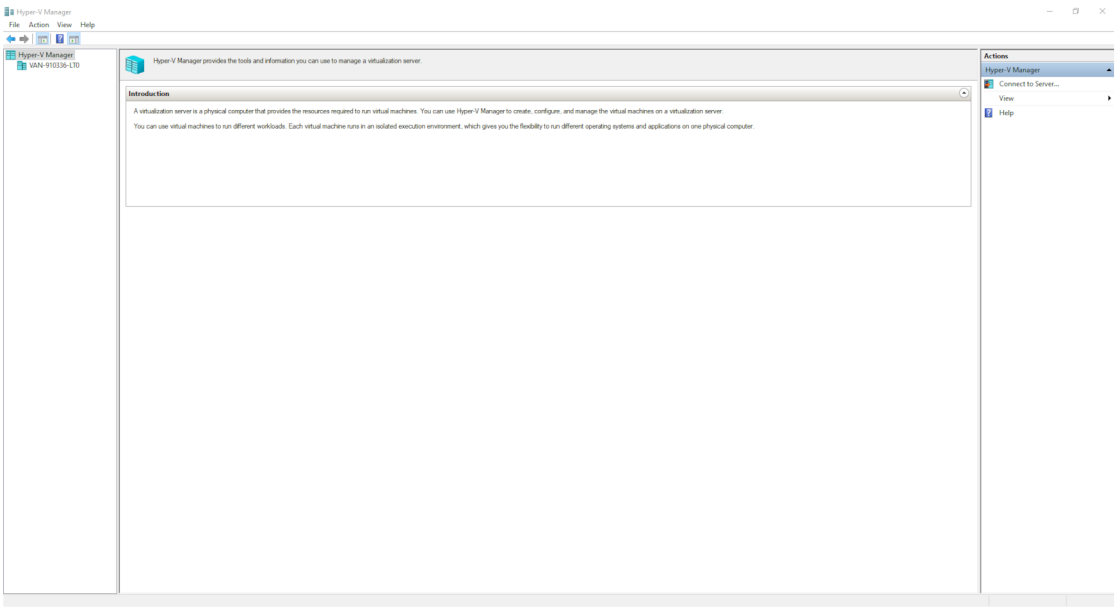
```
execute disk raid rebuild-level <RAID level>
```

Appendix F: Installation on Hyper-V

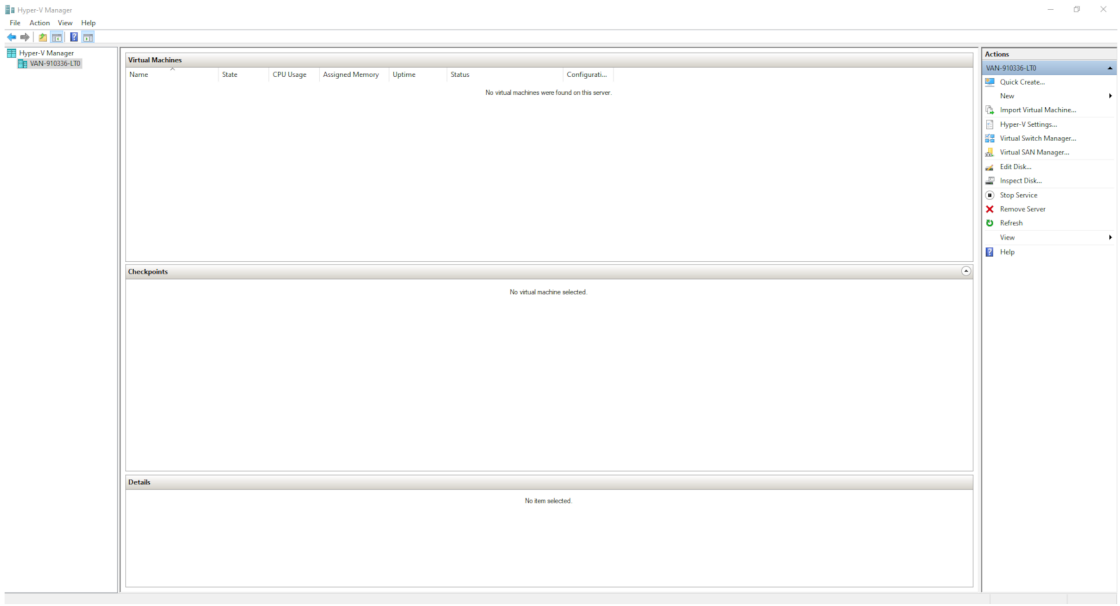
Once you have downloaded the `out.hyperv.zip` file and extracted the package contents to a folder on your management computer/Microsoft server, you can deploy the VHD package to your MS Hyper-V environment.

To deploy FortiPAM-VM on MS Hyper-V without TPM support:

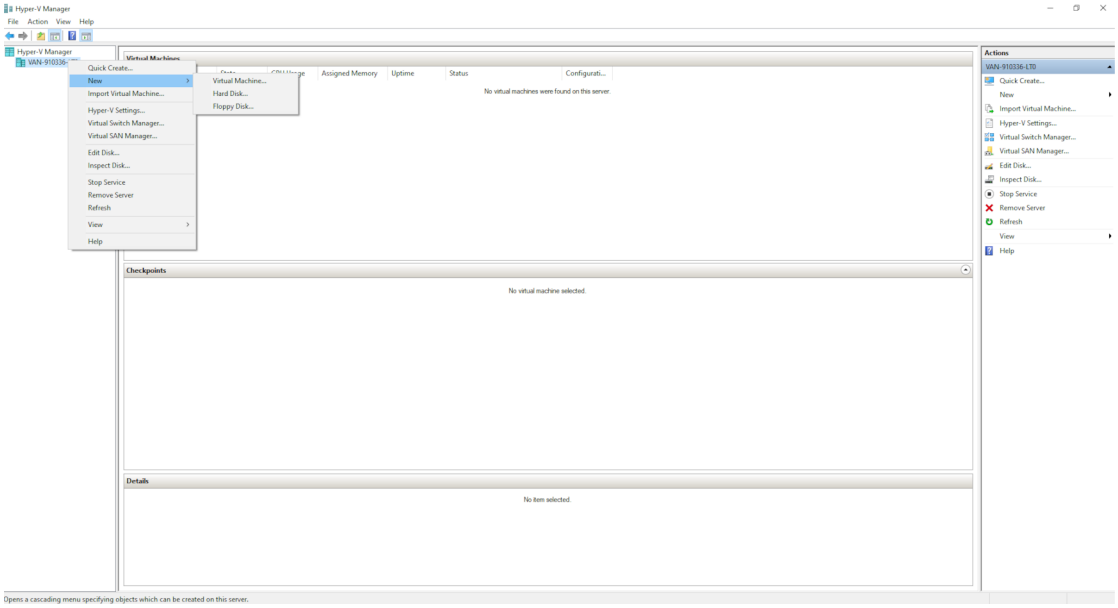
1. Launch the Hyper-V Manager on your management computer.
   The *Hyper-V Manager* homepage opens.



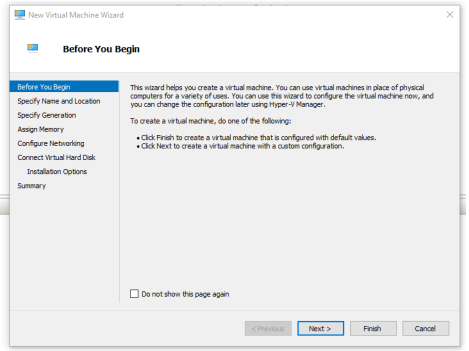
2. In the left tree menu, select your management computer.
   The server details page is displayed.



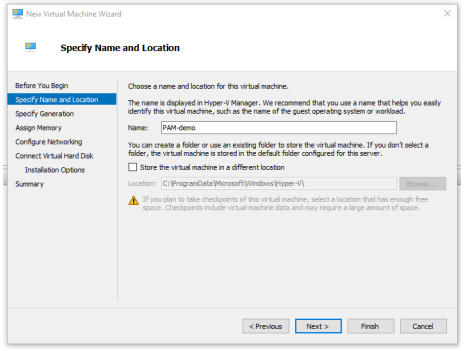
3. Right-click the server/management computer and select *New* > *Virtual Machine*. Optionally, in the *Action* menu, select *New* and select *Virtual Machine*.



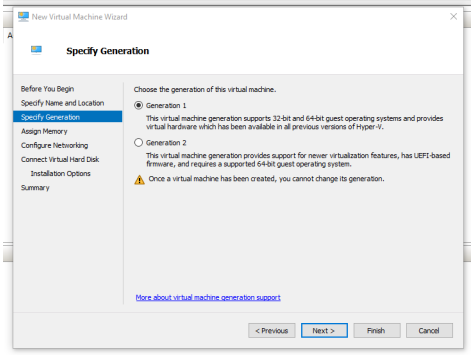
The *New Virtual Machine Wizard* opens.



4. In *New Virtual Machine Wizard*, click *Next* to create a VM with a custom configuration.
   The *Specify Name and Location* tab is displayed.
5. In *Specify Name and Location*, enter a name for this VM, and click *Next*.
   The *Hyper-V Manager* displays the name you enter for the VM.



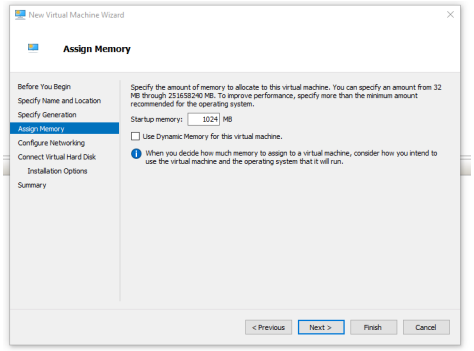
6. In *Specify Generation*, select *Generation 1*, and click *Next*.





Generation 1 does not support TPM. To install FortiPAM-VM on Hyper-V with TPM, see Deploying FortiPAM on Hyper-V with TPM.

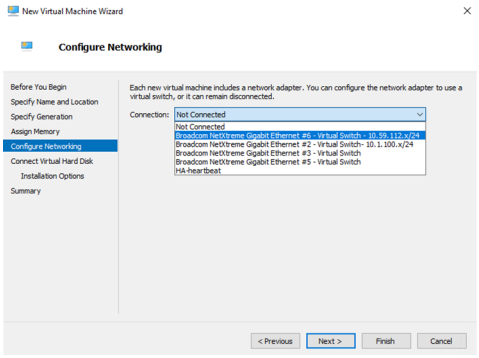
7. In *Assign Memory*, specify the amount of memory to allocate to this VM in *Startup memory*, and click *Next*.
   Ensure that *Use Dynamic Memory for this virtual machine* is unchecked.



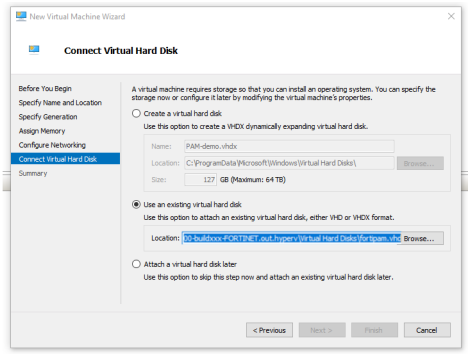


FortiPAM configured with less than 2 CPUs and 2048 MB of RAM works in the evaluation mode until licensed. Otherwise, a valid license is required.

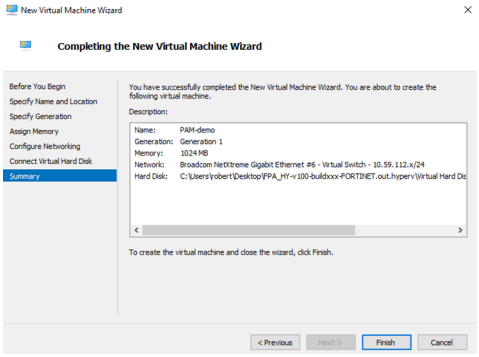
8. In *Configure Networking*, from the *Connection* dropdown, select a network adapter, and click *Next*.
   Each new VM includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected. You can configure more network adapters in the *Settings* window later.



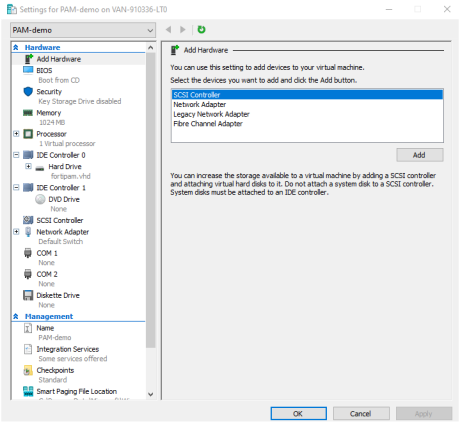
9. In *Connect Virtual Hard Disk*, select *Use an existing virtual hard disk*, click *Browse* and locate the `fortipam.vhd` file that you downloaded from FortiCloud, and click *Next*.



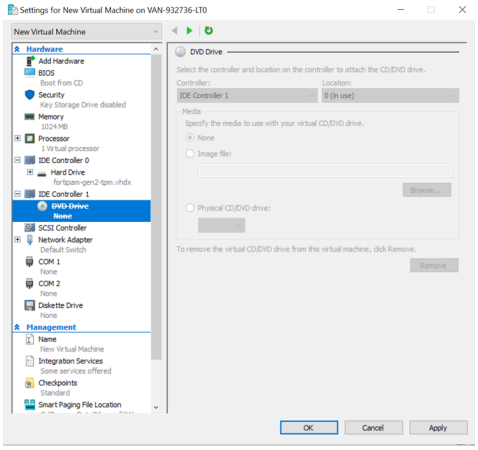
10. In *Completing the New Virtual Machine Wizard*, the installation summary is displayed.



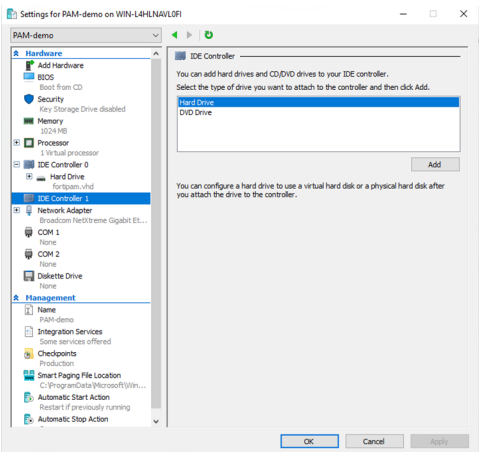
11. To create the VM and close the wizard, click *Finish*.
12. Right-click the VM and select *Settings* from the menu. Optionally, having selected the VM, in the *Action* menu, click *Settings*.



13. In *Hardware*, to remove a DVD drive:
    a. Select a DVD drive in *IDE Controller 1*.
    b. Click *Remove*.
    c. Click *Apply*.



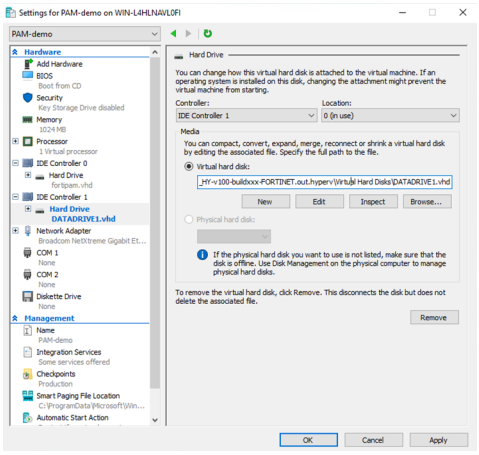
14. In *Hardware*, to add a hard drive:
    a. Click *IDE Controller 1*.
    b. Select *Hard Drive*.



    c. Click *Add*.

d. In *Hard Drive*, click *Browse* and locate the `DATADRIVE1.vhd` file that is in the same folder as `fortipam.vhd` file.

e. Click *Apply*.



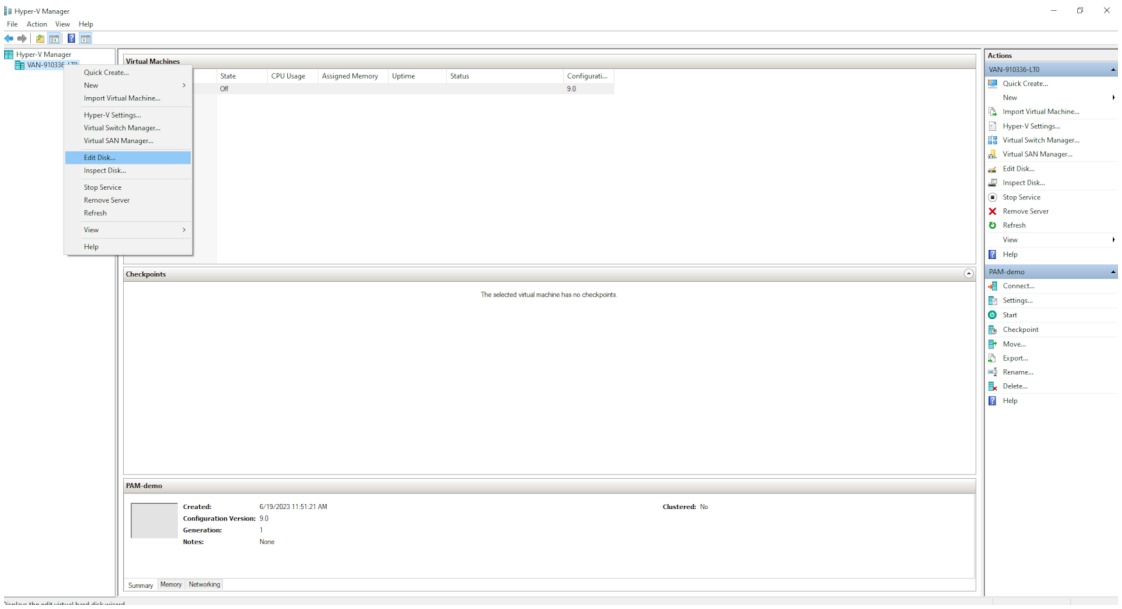
f. Click *OK*.

15. Repeat step 14 to add a second disk, `DATADRIVE2.vhd`.
16. From the virtual machines list, right-click the FortiPAM-VM and select *Start* to power on the VM.
17. Select your newly created VM and launch it.
    See FortiPAM appliance setup on page 43 for CLI related settings to verify the disk usage type and set up FortiPAM.

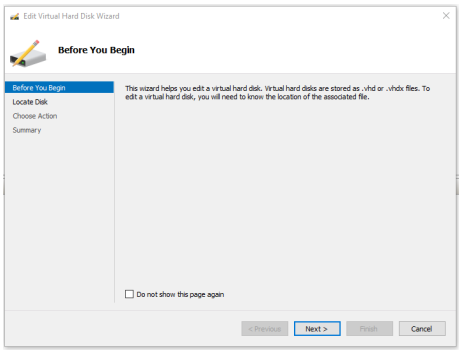
To deploy FortiPAM-VM on MS Hyper-V with TPM support:

To use FortiPAM with TPM on a Hyper-V platform, first, you must convert the virtual hard disk from `*.vhd` to `*.vhdx` format (step 1) and then specify *Generation 2* when creating a new VM (step 2). Finally, you must enable TPM on Hyper-V before powering on the VM (step 3).

1. **Converting hard disk to `*.vhdx`**:
   a. In the left tree menu, right-click the server/management computer and select *Edit Disk*. Optionally, having selected the server, select *Action* and then select *Edit Disk*.

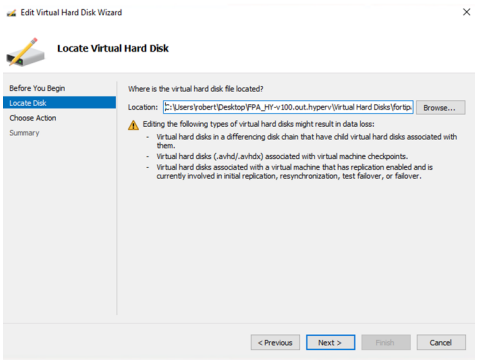


The *Edit Virtual Hard Disk Wizard* opens.

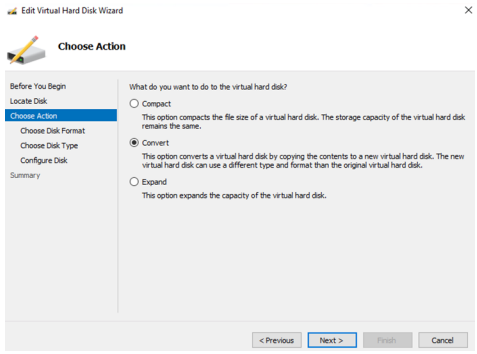


b. In the *Edit Virtual Hard Disk Wizard*, click *Next*.

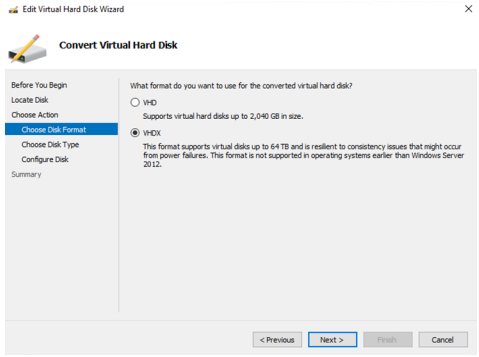
c. In *Locate Virtual Hard Disk*, click *Browse* and locate the `fortipam.vhd` file that you downloaded from FortiCloud, and click *Next*.



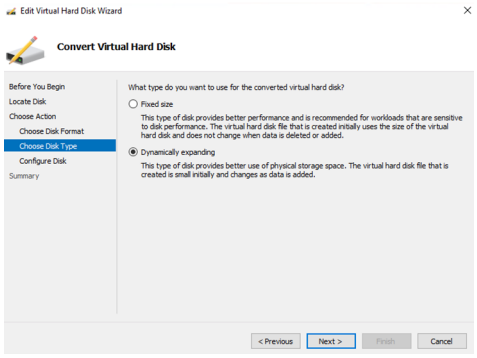
d. In *Choose Action*, select *Convert*, and click *Next*.



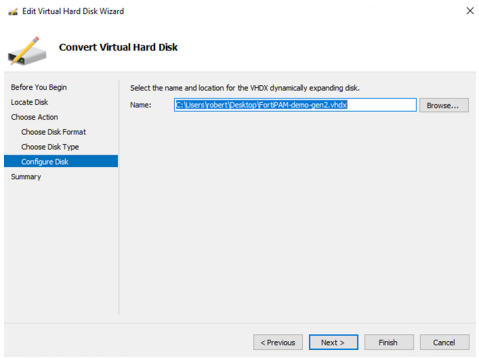
e. In *Choose Action* > *Choose Disk Format*, select *VHDX*, and click *Next*.



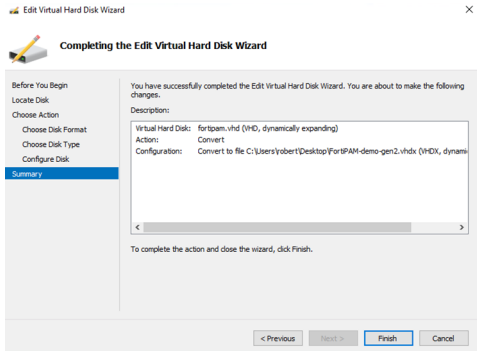
f. In *Choose Action* > *Choose Disk Type*, select *Dynamically expanding*, and click *Next*.



g. In *Choose Action* > *Configure Disk*, enter a name for the VHDX disk, click *Browse* to configure a location for this disk, and click *Next*.



h. In *Completing the Edit Virtual Hard Disk Wizard*, the summary is displayed.



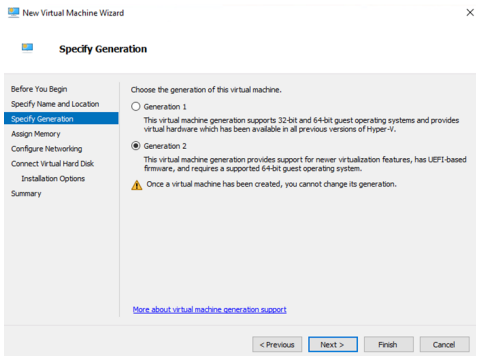
i. Click *Finish*.

j. Repeat steps *a* to *i* to convert `DATADRIVE1.vhd` and `DATADRIVE2.vhd`.

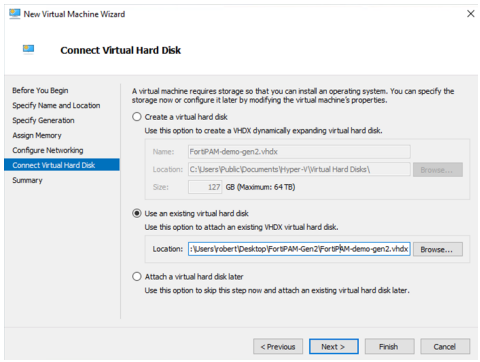
2. Creating a 2nd generation Hyper-V VM:

Follow the same procedure as detailed in Deploying FortiPAM-VM on Hyper-V without TPM, except:

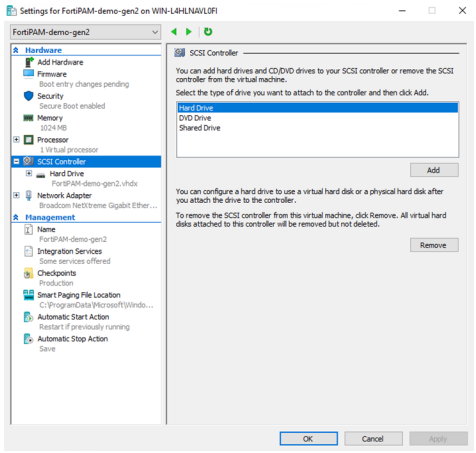
a. In Step 6, select *Generation 2*.



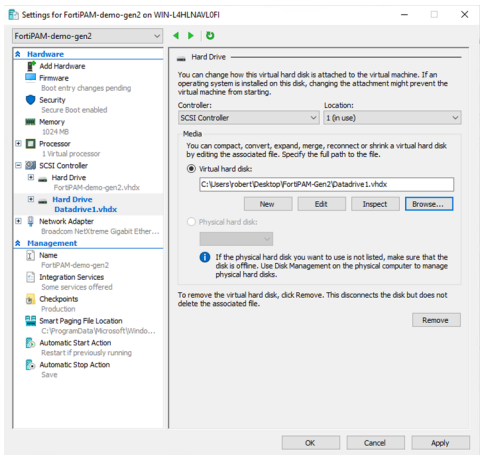
b. In Step 9, click *Browse* and locate the `*.vhdx` file that you converted from `fortipam.vhd`.



c. In step 14 (a, b, and c), click *SCSI Controller*, select *Hard Drive*, and click *Add*.



d. In step 14 d, in *Hard Drive*, click *Browse* and locate the `*.vhdx` file for `DATADRIVE1.vhd` that you earlier converted in Converting hard disk to *.vhdx.

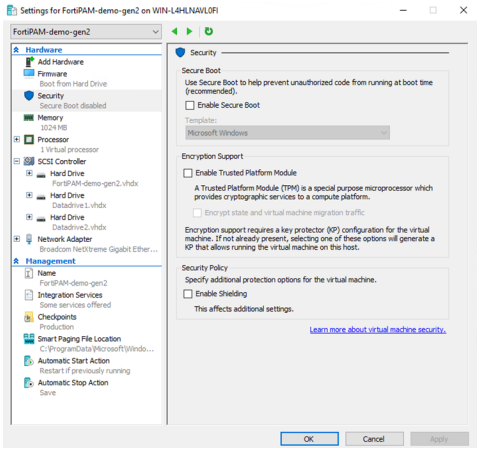


e. Repeat steps *c* and *d* to add `*.vhdx` file for `DATADRIVE2.vhd`.

Secure boot must be disabled before starting the VM.

To disable secure boot:

1. From the virtual machines list, right-click the VM and select *Settings*. Optionally, having select the VM, select *Action* and then select *Settings*.
2. Go to *Security* and uncheck *Enable Secure Boot*.
3. Click *Apply*.



4. Click *OK*.

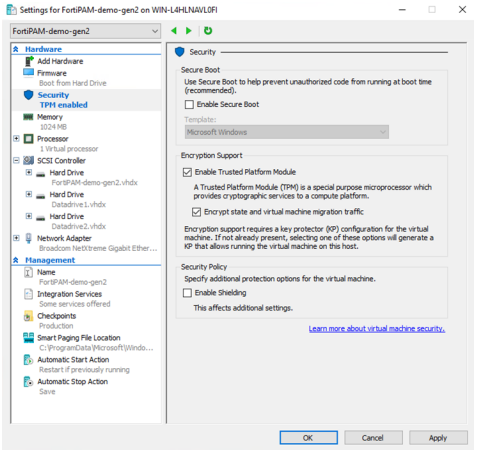
3. Enabling TPM on Hyper-V:

Ensure that TPM is set up as part of the initial configuration, i.e., before powering on the FortiPAM-VM for the first time.

a. From the virtual machines list, right-click the VM and select *Settings*. Optionally, having select the VM, select *Action* and then select *Settings*.

b. Go to Security and check *Enable Trusted Platform Module*. Optionally, enable *Encrypt state and virtual machine migration traffic*.

c. Click *Apply*.



d. Click *OK*.
You can now power on your VM.

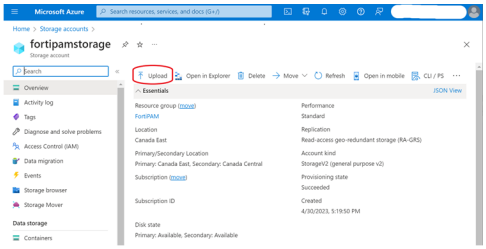
Appendix G: Installation on Azure

If deploying FortiPAM from the Marketplace, skip to Creating the FortiPAM-VM on page 519.

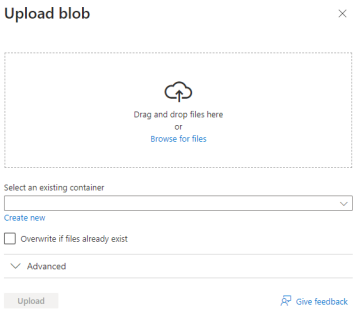
Uploading the VHD file to an Azure storage account

To upload the VHD file to an Azure storage account:

1. Unzip the `FPA_AZURE-v100-buildXXXX-FORTINET.out.hyperv.zip` file and store the `fortipam.vhd` file on your management computer.
2. Go to your storage account on the Microsoft Azure Portal and click *Upload*.



The *Upload blob* window opens.

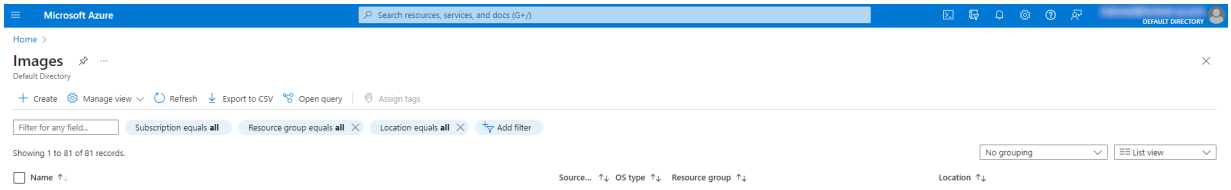


3. Select *Browse for files* and locate the `fortipam.vhd` file that you downloaded and unzipped in step 1.
4. Click *Upload*.

Creating an image on Azure Images

To create an image:

1. Go to *Images* on the Azure Portal and select *Create*.

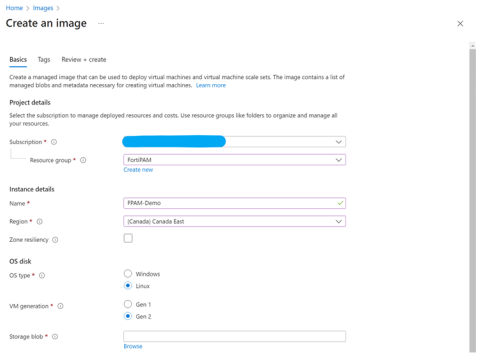


The *Create an image* wizard opens.

2. From the *Resource group* dropdown, select a resource group.
3. In *Name*, enter the name for the image.
4. In the *Region* dropdown, select a region.
5. In *OS type*, select *Linux*.
6. In *VM generation*, you can select *Gen 1* or *Gen 2*.



Gen 1 VMs use BIOS-based architecture, whereas *Gen 2* VMs use the new UEFI-based boot architecture.

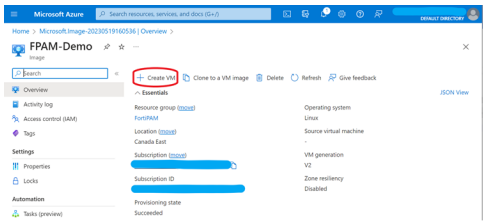


7. In the *Storage blob*, click *Browse*, locate the `fortipam.vhd` file that you uploaded to your storage account in Uploading the VHD file to an Azure storage account on page 518, and click *Next : Tags*.
8. Optionally, in *Tags*, enter tags, and click *Next : Review + Create*.
9. Review your settings and then click *Create*.
   Note: The deployment may take several minutes to finish.

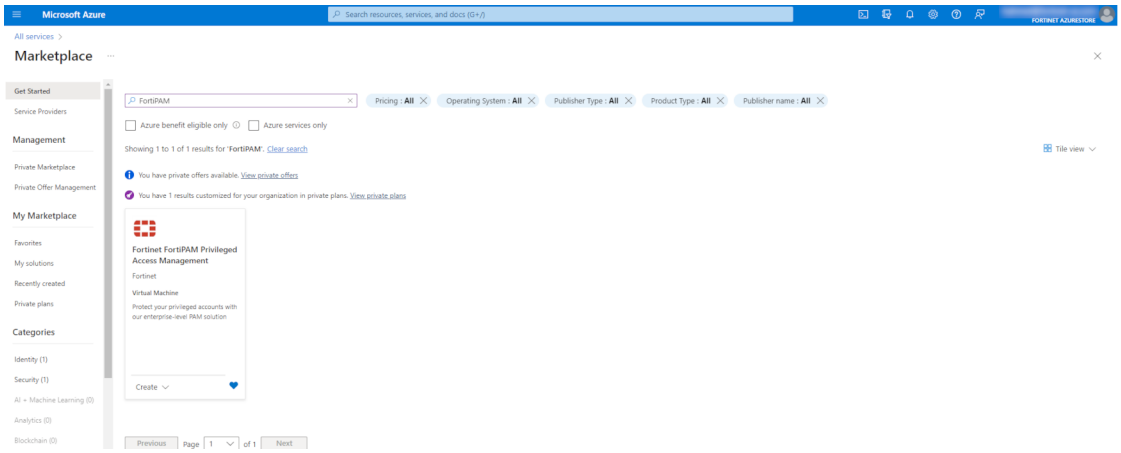
Creating the FortiPAM-VM

To create the FortiPAM-VM:

1. On the Azure Portal, open the image you created in Creating an image on Azure Images on page 518, and click *Create VM*.



Alternatively, go to the *Marketplace* on the Azure Portal and look for FortiPAM.

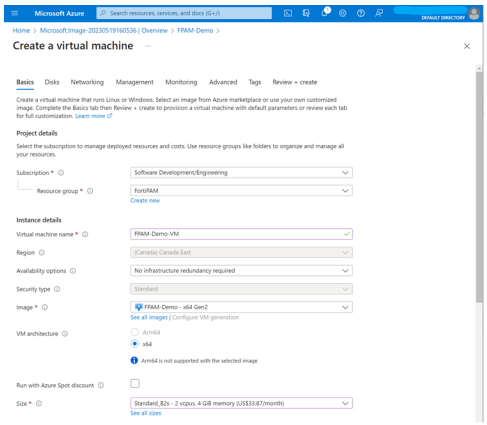


Click on the *Fortinet FortiPAM Privileged Access Management* card and select *Create*.

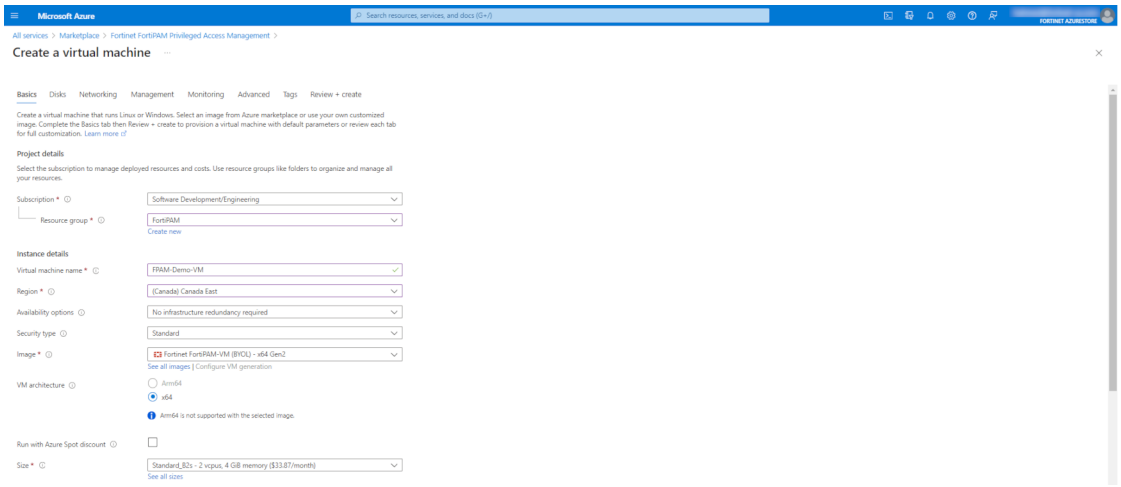
The *Create a virtual machine* wizard opens.

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 518 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 518.



The following shows a screenshot when FortiPAM is deployed from the *Marketplace*.



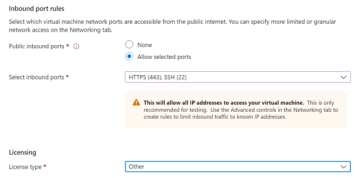
6. In the *Administrator account* pane:
   a. In *Authentication type*, select *Password*.
   b. In *Username*, enter a username.
   c. In *Password*, enter the password.
   d. In *Confirm password*, enter the password again to confirm.



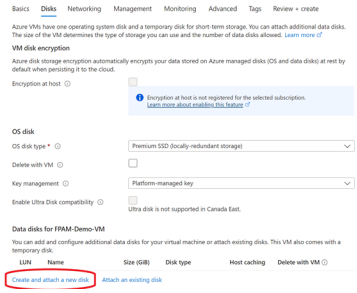
The account is created with the *Super Administrator* role on FortiPAM.



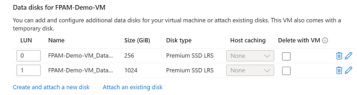
7. In the *Inbound port rules* pane:
   a. In *Public inbound ports*, select *Allow selected ports*.
   b. In the *Select inbound ports* dropdown, select *HTTPS (443), SSH (22)*.
8. In the *License Type* dropdown, select *Other*, and click *Next*.



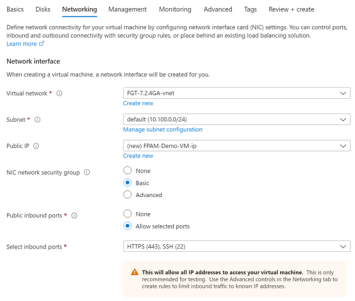
9. In *Data disks for FPAM-demo-VM*, select *Create and attach a new disk*.



10. Create a disk for the log and another for the video, and click *Next*.



11. In the *Networking* tab:
    a. In the *Virtual network* dropdown, select a virtual network.
    b. In the *Subnet* dropdown, select a subnet.
    c. In the *Public IP* dropdown, select a public IP address or create a new public IP address.
    d. In *NIC network security group*, select *Basic*.
    e. In *Public inbound ports*, select *Allow selected ports*.
    f. In the *Select inbound ports* dropdown, select *HTTPS (443), SSH (22)*, and click *Next*.

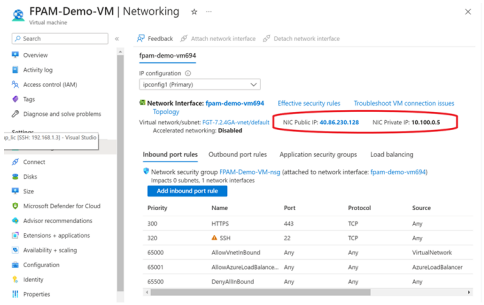


12. Click *Next* and navigate through the remaining tabs.
13. Finally, review your settings and then click *Create*.

    Note: The VM deployment may take several minutes to finish.

Initial configuration

1. On the FortiPAM-VM *Networking* page, copy and save the network interface's private and public IP addresses.



2. In the VM serial console, log in as the default super admin set up in step 6 of Creating the FortiPAM-VM on page 519.
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 357.
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 519.
   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 530	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 534
2. Creating an S3 bucket on AWS on page 535
3. Uploading RAW file to the AWS S3 bucket on page 536
4. Creating a snapshot from the RAW file in the AWS S3 bucket on page 536
5. Creating AMI from the snapshot on page 539
6. Configuring a security group on page 540
7. Launching the FortiPAM instance from AMI on page 542
8. Initial configuration on page 543
9. Licensing on page 545

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
   ```

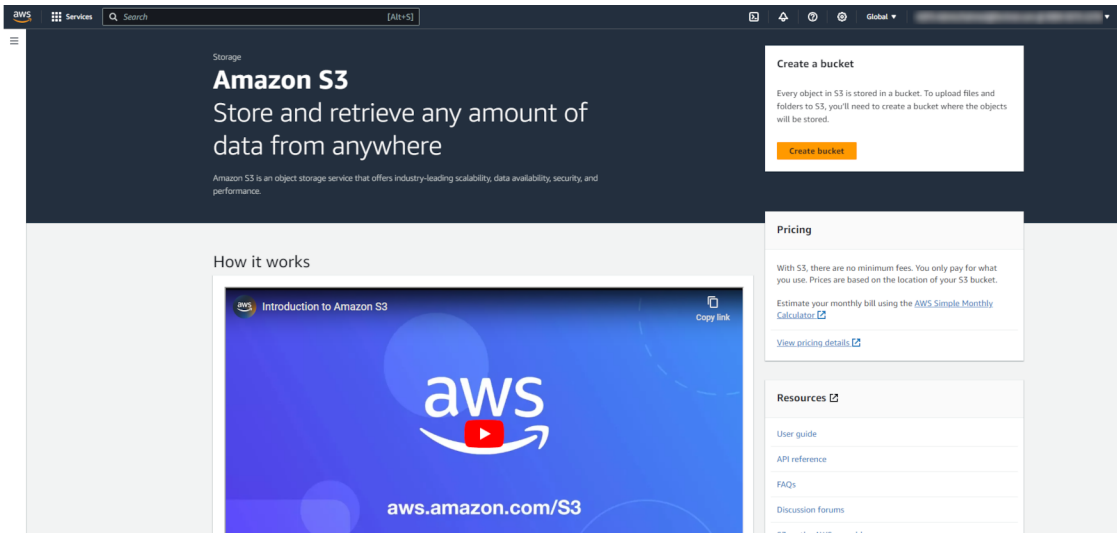
3. Use `qemu-img` to convert the image into RAW format:

   ```
   $ qemu-img convert fortipam.qcow2 fortipam.raw
   ```

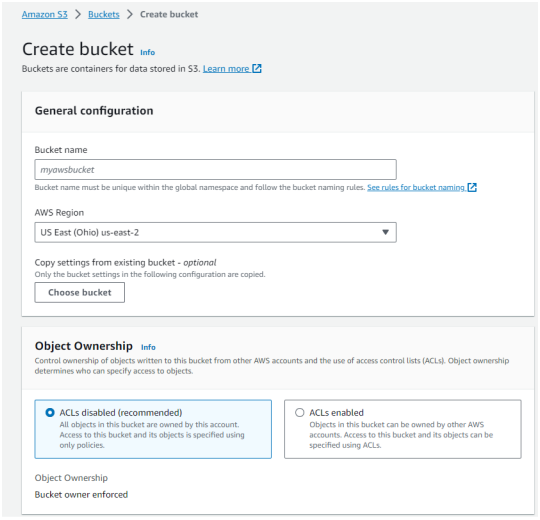
Creating an S3 bucket on AWS

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*.



The *Create bucket* page opens.



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:

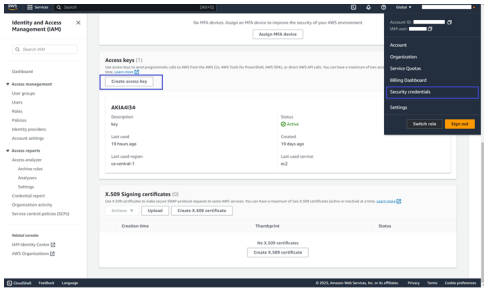
1. Using the following command, install the AWS CLI :

```
$ 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=ACR8XXXXXXXXXXXXXXXXXXXX
region = us-west-1
```

Note: Access key can be created from *Security credentials* in your IAM Account.



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:
   a. 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": []
  }
```

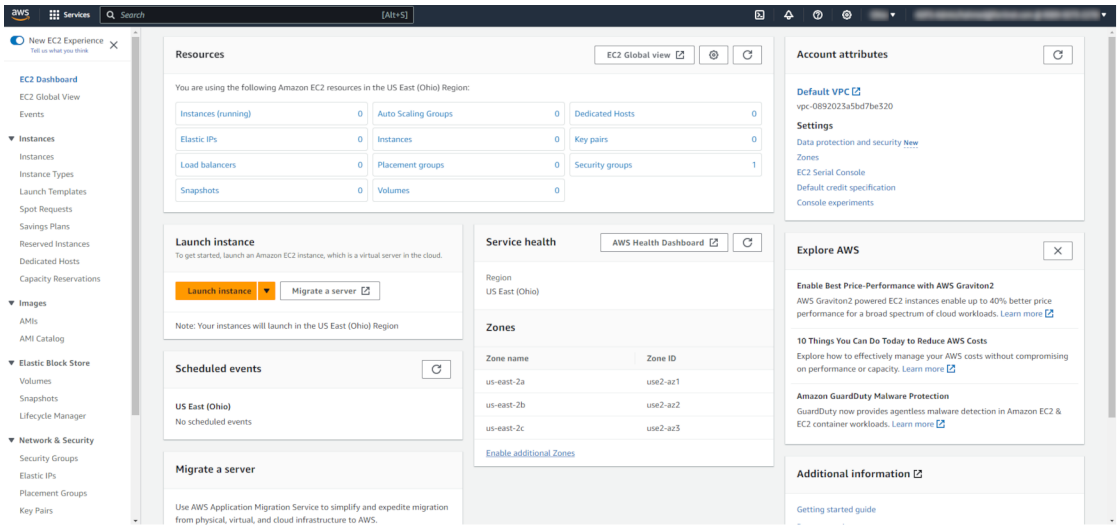
Importing the image may take some time. You can use the following AWS CLI command to monitor the progress of import:

```
$ 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": []
    }
   ]
  }
```

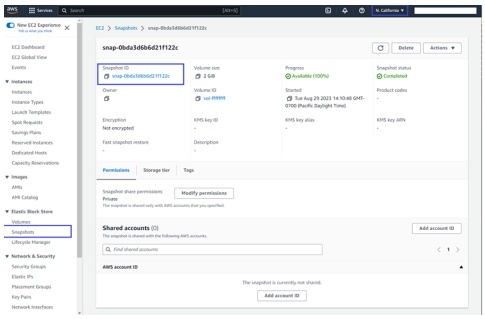
Creating AMI from the snapshot

To create AMI from snapshot:

1. In the AWS console, from the *Services* menu, go to *Compute* > *EC2*.



2. From the menu, go to *Elastic Block Store* > *Snapshots* and look for the snapshot ID.





Alternatively, the `describe-import-snapshot-tasks` command used to Monitor the progress of FortiPAM image import can be used find the snapshot ID.

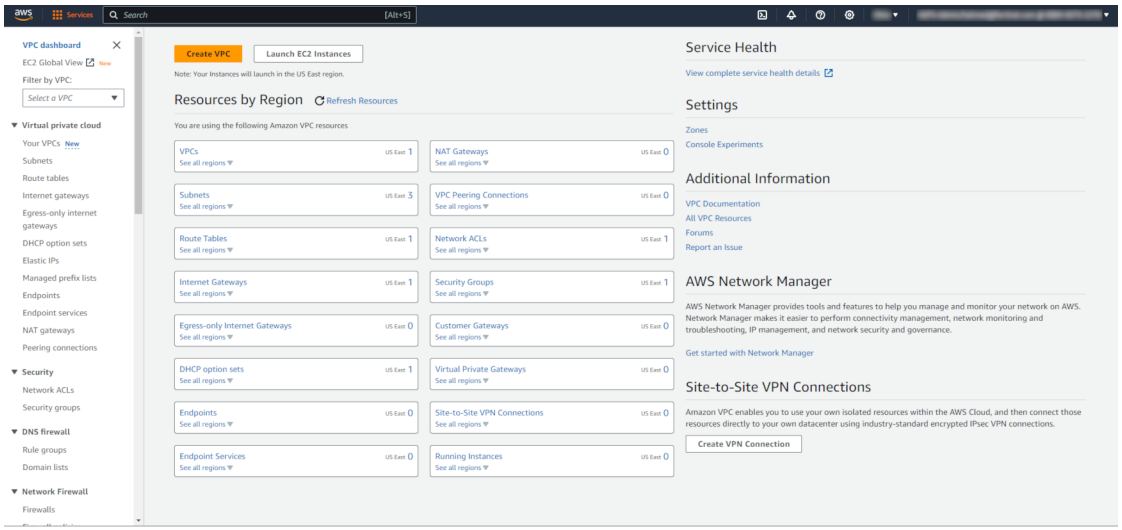
3. Using the following AWS CLI command, create a FortiPAM image:

```
$ 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
```

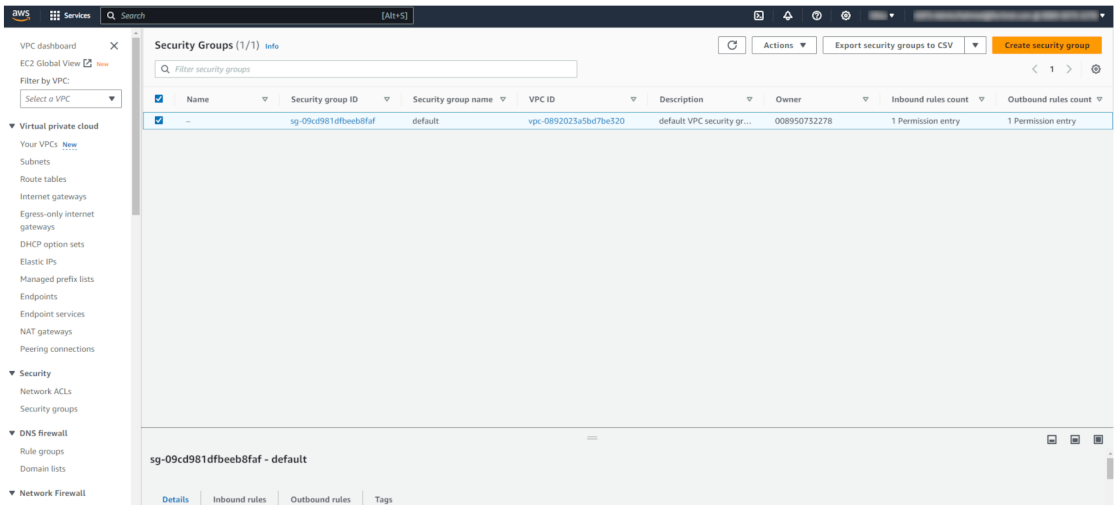
Configuring a security group

To configure a security group

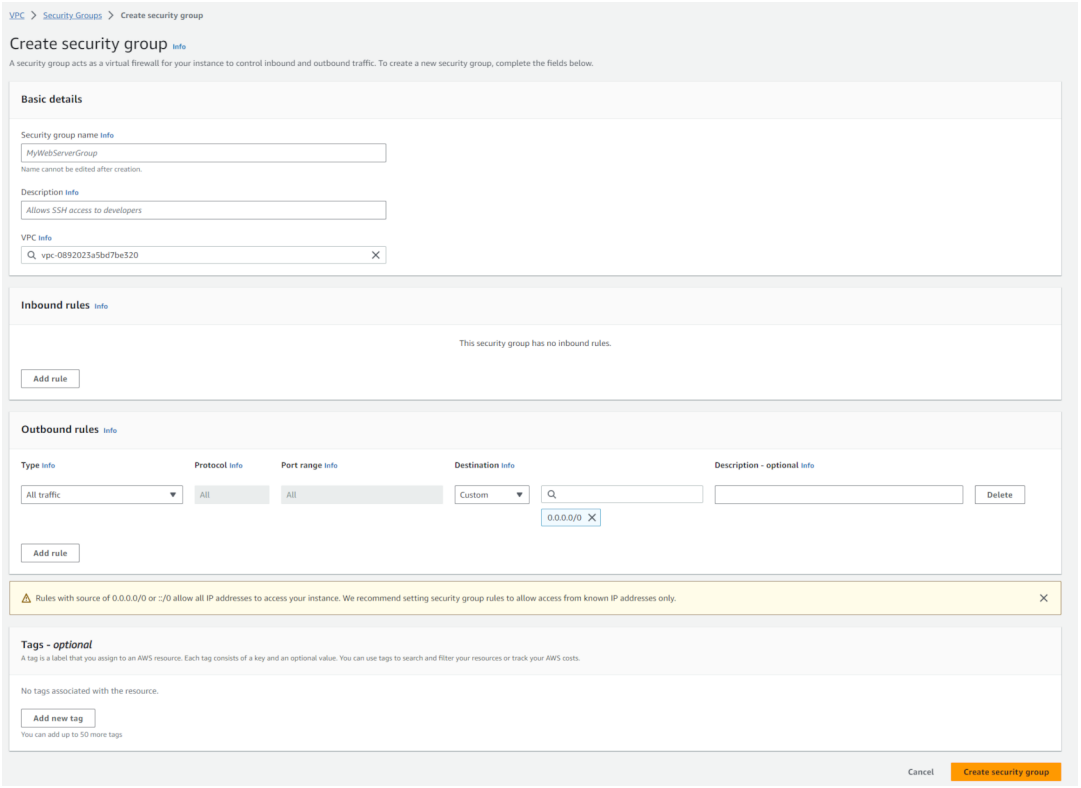
1. In the AWS console, search *VPC* and select VPC from the search result.
   The *VPC dashboard* opens.



2. In the *VPC dashboard*, select *Security Groups*.
   The *Security Groups* window opens.

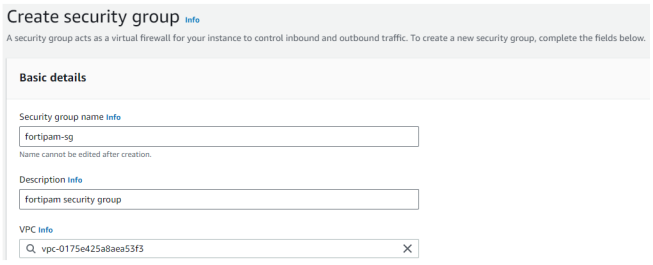


3. In the *Security Groups* window, select *Create security group*.
   The *Create security group* page opens.

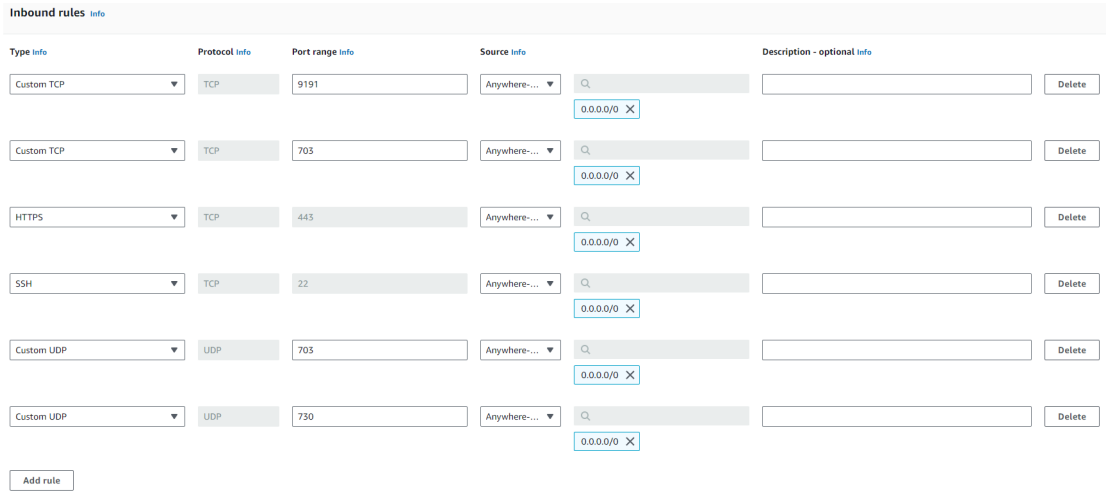


4. In the *Basic details* pane, enter the following information:

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.



5. In the *Inbound rules* pane, add the following inbound rules:

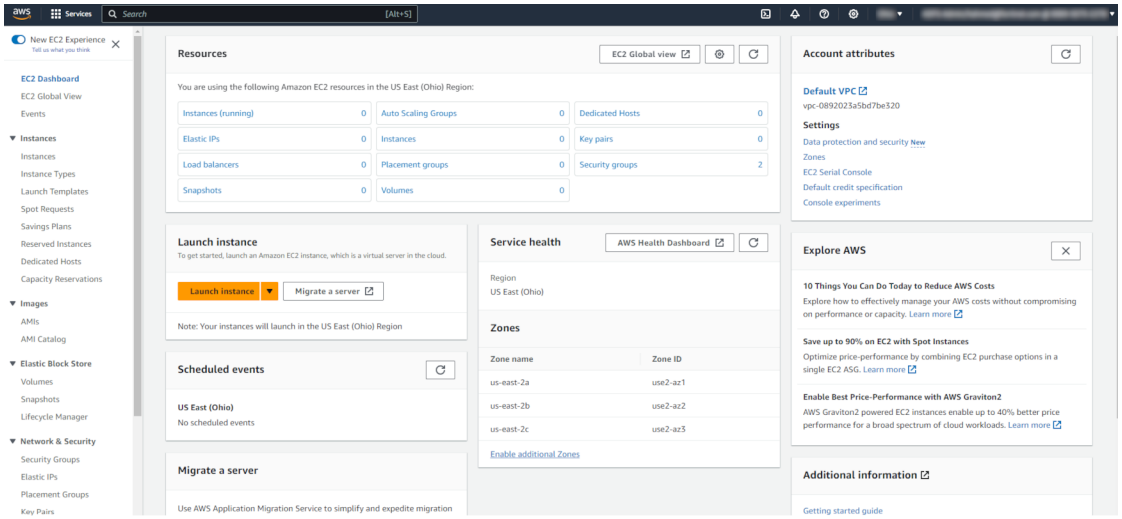


6. Use the default outbound rule that allows all the traffic.
7. Click *Create security group*.

Launching the FortiPAM instance from AMI

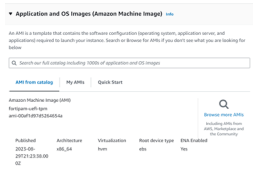
To launch the FortiPAM instance:

1. In the AWS console, from the *Services* menu, go to *Compute* > *EC2*.
   The *EC2 Dashboard* opens.



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.



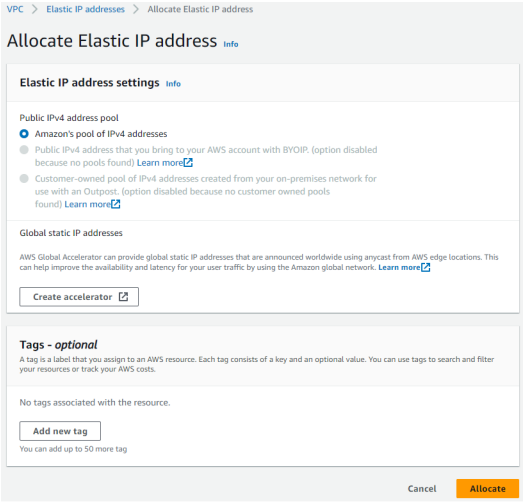
5. In the *Instance type* pane, select *m5.xlarge*.

> 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 540.
   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

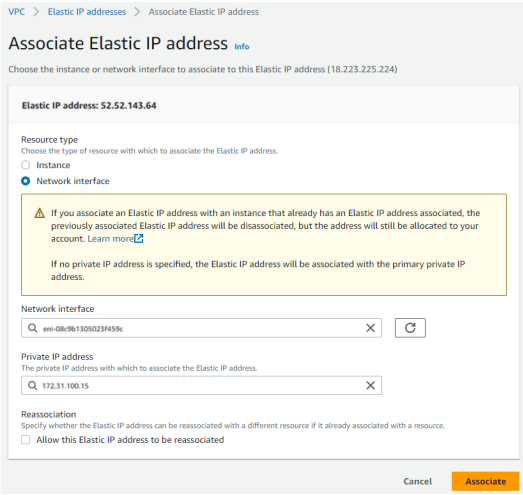
1. In the AWS console, search *VPC* and select VPC from the search result.
   The *VPC dashboard* opens.
2. In *Virtual private cloud* on the left, select *Elastic IPs*.
   The *Elastic IP addresses* window opens.



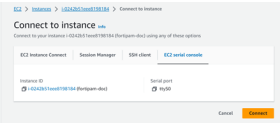
3. In the *Elastic IP addresses* window, click *Allocate* to create a new public IP address.
4. Select an IP address from the elastic IP addresses list, and from the *Actions* dropdown, select *Associate Elastic IP address*.

The *Associate Elastic IP address* page opens.

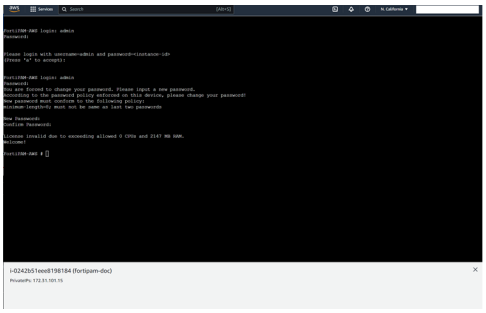
5. In *Resource type*, select *Network* interface.
6. In the *Network interface* dropdown, select a network interface.
7. In the *Private IP address* dropdown, select a private IP address.



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*.



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.



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.

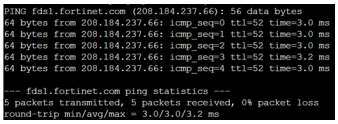
15. Use the following FortiPAM CLI commands to configure a static route if the interface is configured as static mode:

```
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:



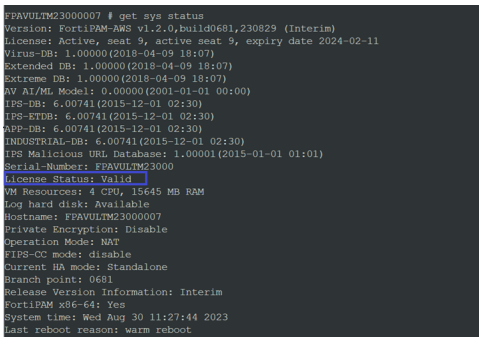
17. Optionally, to encrypt disk to protect logs and videos, see Configuring log and video disk encryption on page 357.

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
```



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

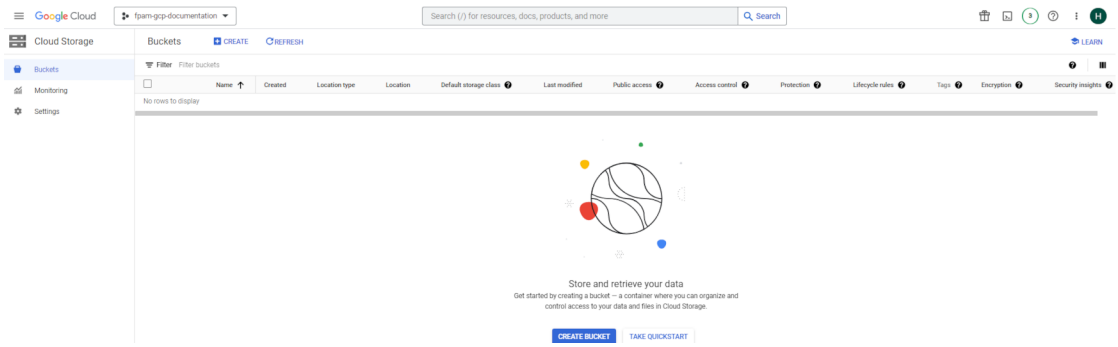
FortiPAM installation on GCP and initial setup:

1. Creating a cloud storage bucket on GCP on page 547
2. Adding the FortiPAM image file to the storage bucket on page 548
3. Creating a FortiPAM image on GCP on page 549
4. Creating VM instance from the image on page 551
5. Licensing on page 555
6. Static interface IP address on page 556
7. Setting up HA on page 557
8. Enabling vTPM on page 559

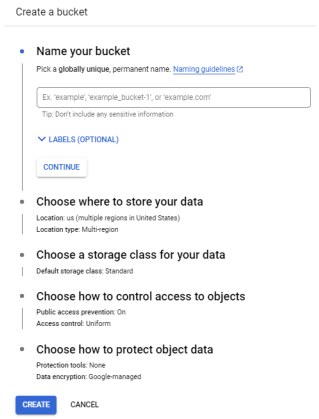
Creating a cloud storage bucket on GCP

To create a cloud storage bucket on GCP:

1. From the navigation pane, go to *Cloud Storage* > *Bucket*.
   The *Buckets* window opens.

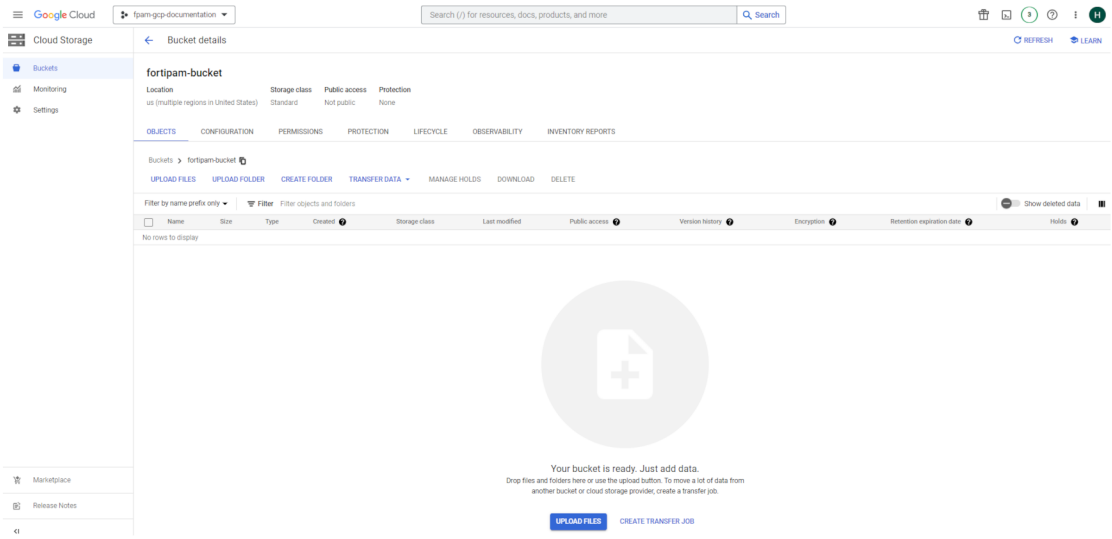


2. Select *+CREATE/CREATE BUCKET* to create a new storage bucket.



3. In *Name*, enter a name for the storage bucket, and click *CONTINUE*.

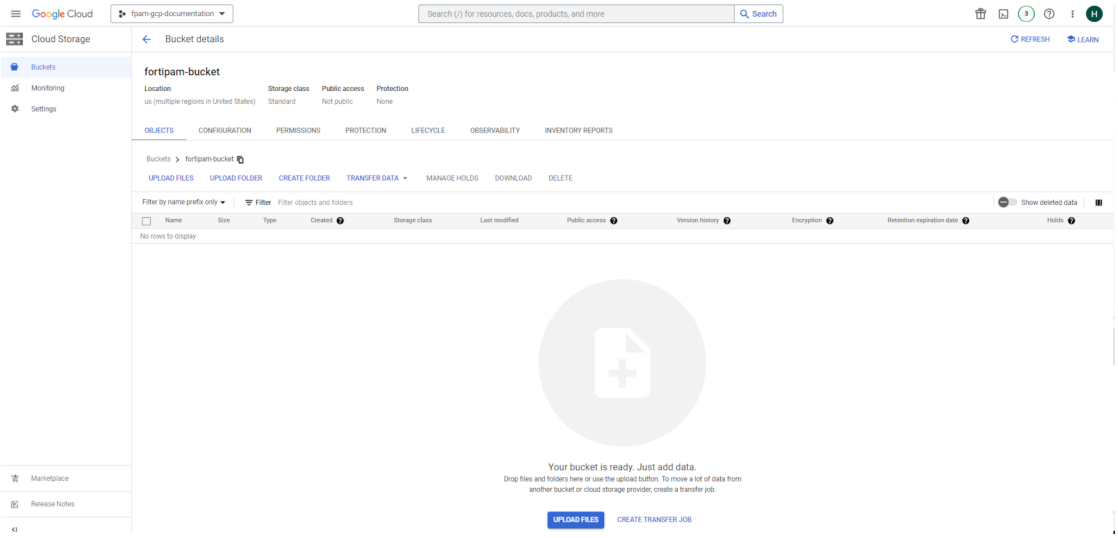
4. In *Choose where to store your data*, select *Multi-region*, from the dropdown select a location, and click *CONTINUE*.
5. In *Choose a storage class for your data*, keep the default settings, and click *CONTINUE*.
6. In *Choose how to control access to objects*, keep the default settings, and click *CONTINUE*.
7. In *Choose how to protect object data*, keep the default settings, and click *CONTINUE*.
8. Select *Create*.
   The storage bucket is created.



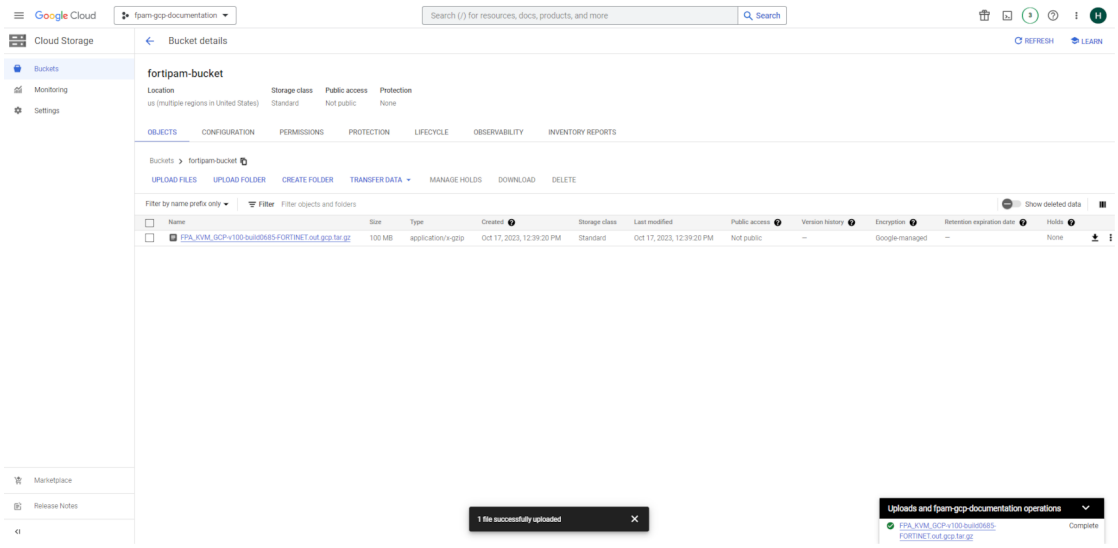
Adding the FortiPAM image file to the storage bucket

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 547 to open it.



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.

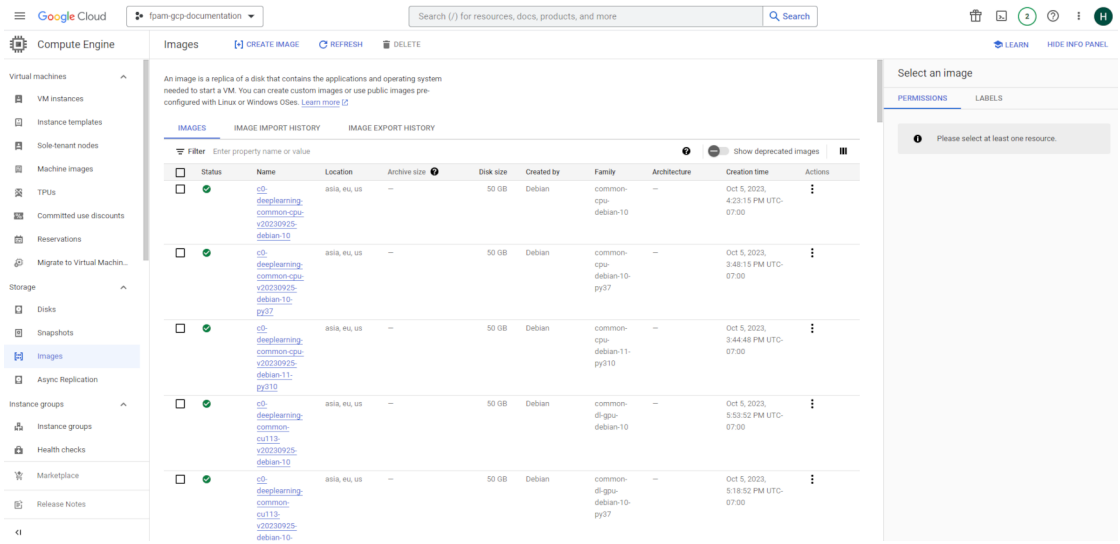


Creating a FortiPAM image on GCP

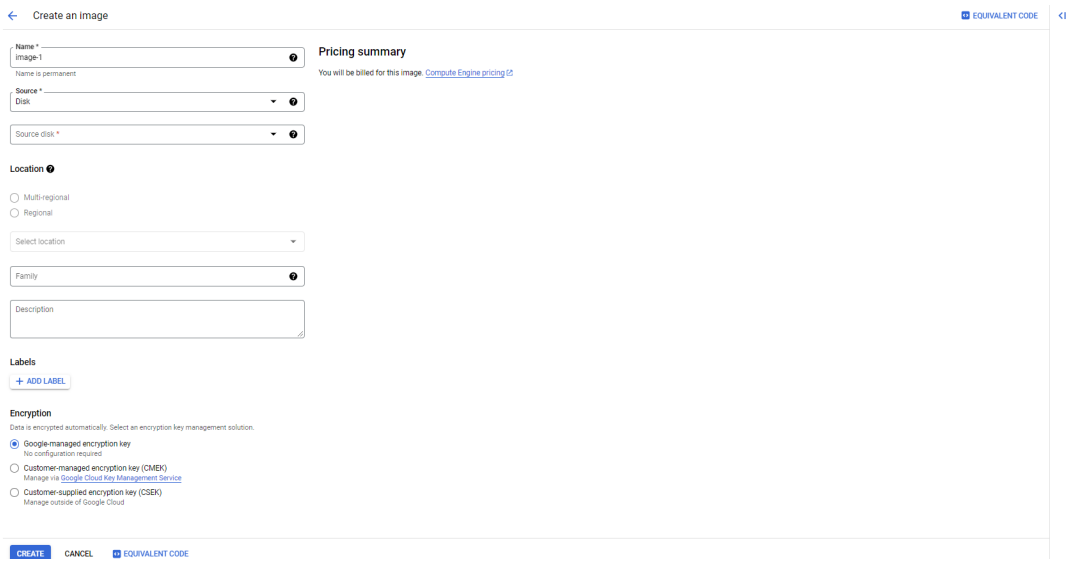
If you want to use vTPM, see Enabling vTPM on page 559 to create an image.

To create a FortiPAM image on GCP:

1. From the navigation pane, go to *Compute Engine* > *Storage* > *Images*.
   The *Images* window opens.



2. In the *Images* window, select *Create Image*, and click *CONTINUE*.
   The *Create an image* window opens.

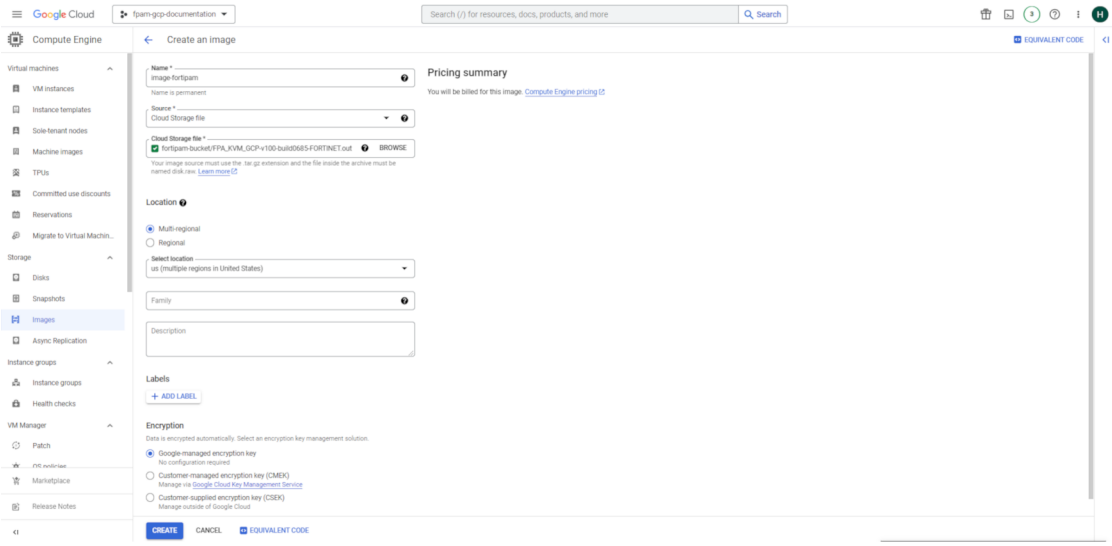


3. In *Name*, enter a name for the image.
4. In the *Source* dropdown, select *Cloud Storage file*.
5. Select *BROWSE*, from the *Select object* pane that opens, go to the FortiPAM image file, and click *SELECT*.

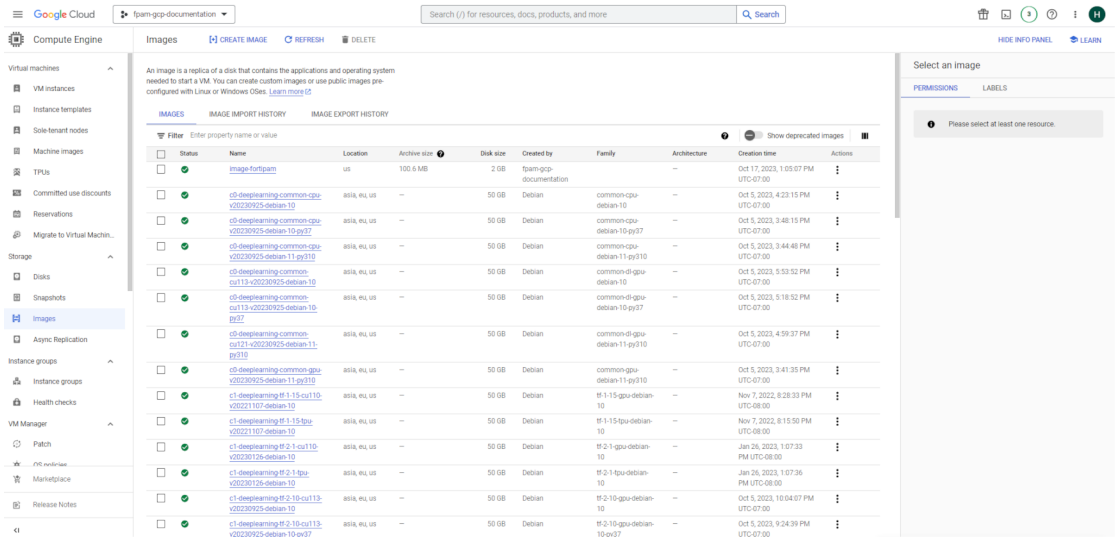


The image source must have `.tar.gz` as its extension and the file in it must be named `disk.raw`.

6. Ensure that the *Location* is set to *Multi-regional*.
7. Leave the rest of the settings in the default state.



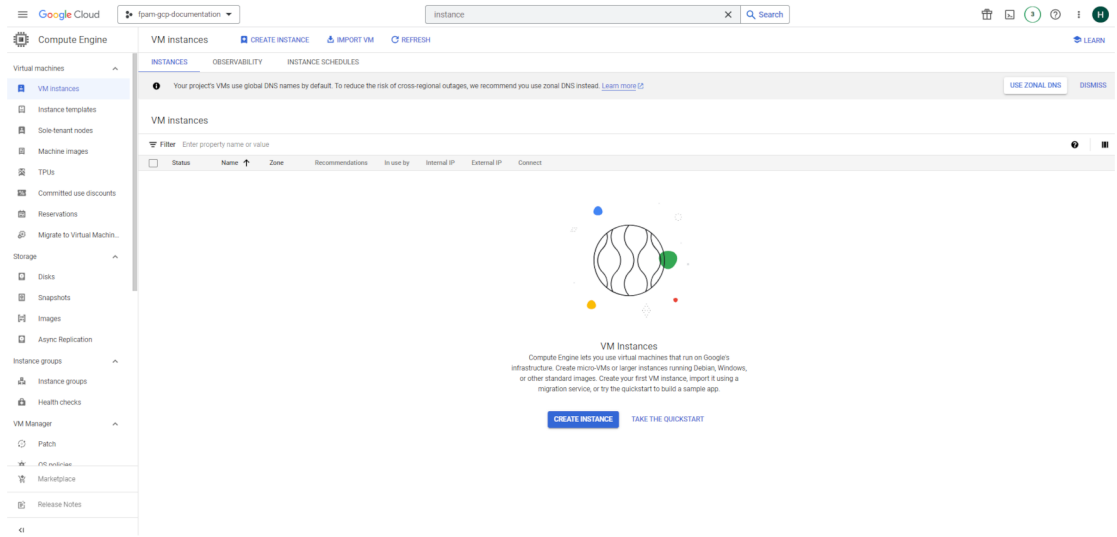
8. Click *CREATE*.
   The new FortiPAM image is now listed at the top in the *Images* window.



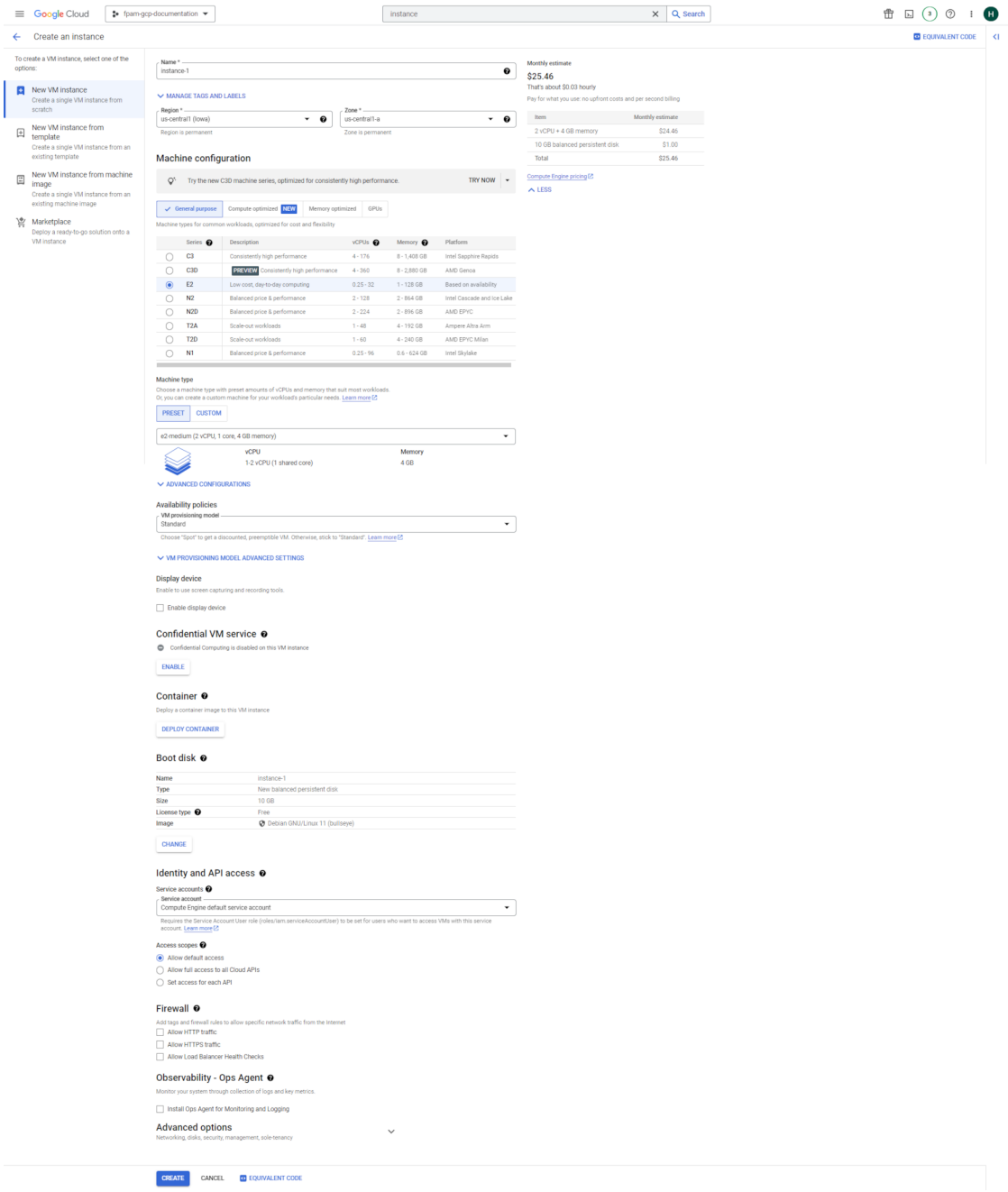
Creating VM instance from the image

To create VM instance from the image:

1. From the navigation pane, go to *Compute Engine* > *VM instances*.
   The *VM instances* window opens.

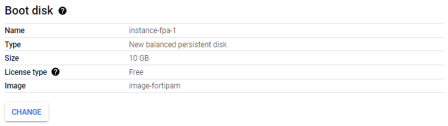


2. Select CREATE INSTANCE.
   The *Create an instance* window opens.

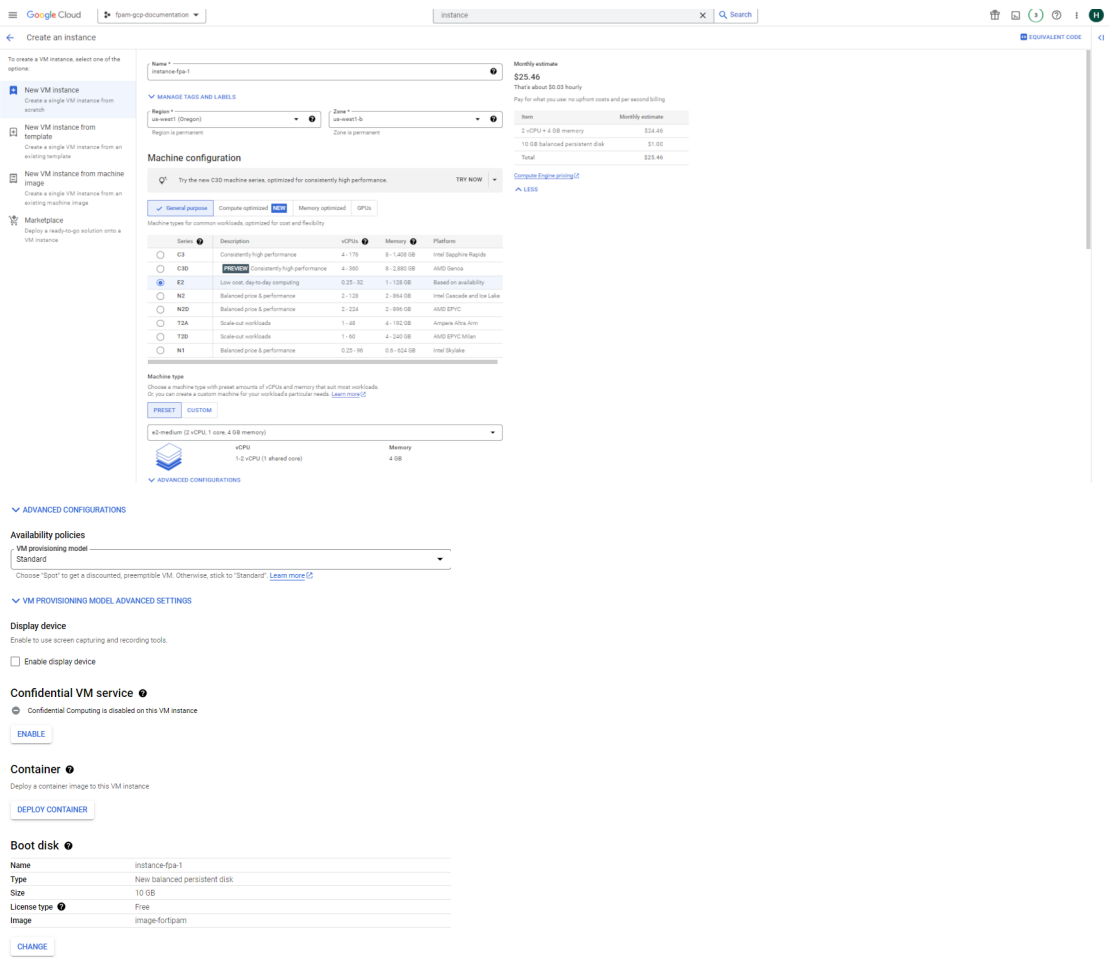


3. In *Name*, enter a name for the VM instance.
4. From the *Region* dropdown, select a region where the resource is located.
5. From the *Zone* dropdown, select a zone within the region where the resource is located.
6. In *Machine configuration*, select a machine type for deployment.
7. In *Boot disk*, 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 549.

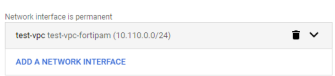
c. Click *SELECT*.



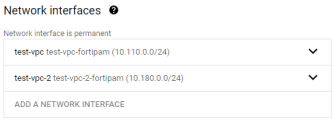
8. Leave the following settings in the default state:
   - *ADVANCED CONFIGURATIONS*
   - *Display device*
   - *Confidential VM service*
   - *Container*
   - *Identity and API access*
   - *Firewall*
   - *Observability - Ops Agent*



9. Expand *Advanced options* > *Networking*:
   a. In *Network interfaces*, ensure that a network interface with a subnetwork is selected.

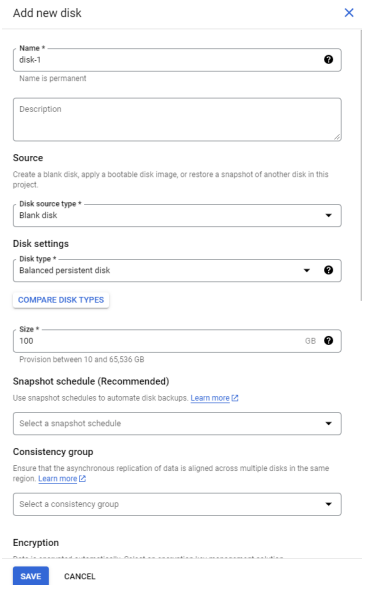


b. In *Network interfaces*, add another network if the FortiPAM will be used in an HA cluster.



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.



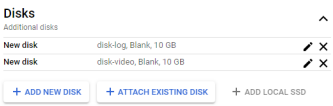
b. In *Name*, enter a name for the disk.

c. In *Size*, enter `10` (in GB) to add a new volume for the log.

d. Leave the remaining settings in the default state.

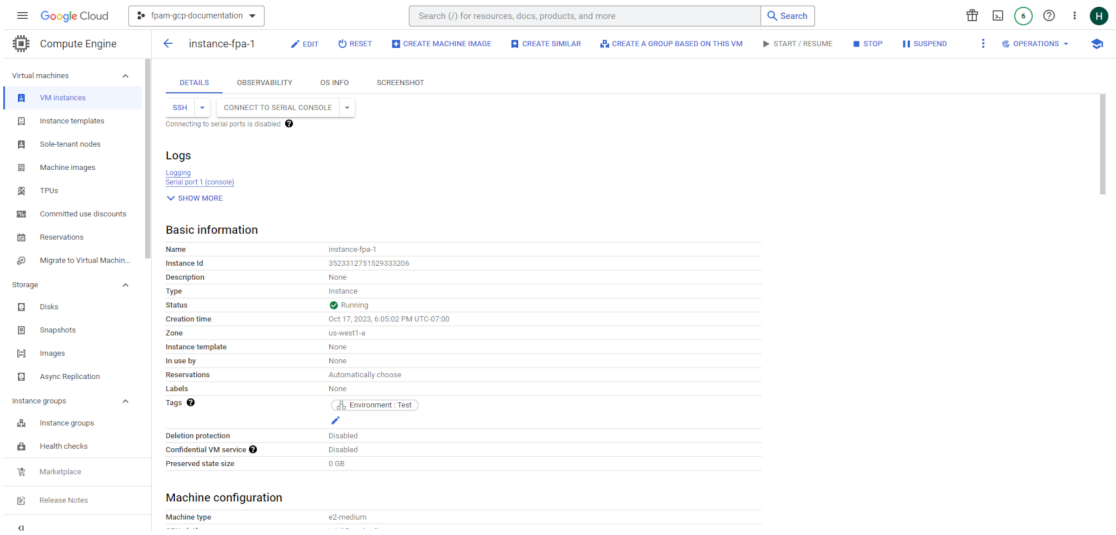
e. Click *Save*.

f. Repeat steps `a` to `e` to add a new volume for storing videos.

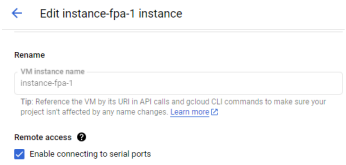


11. Click *CREATE*.

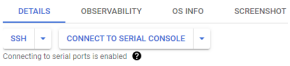
12. From the VM instance list, click the name of the VM instance you created.
The instance page opens.



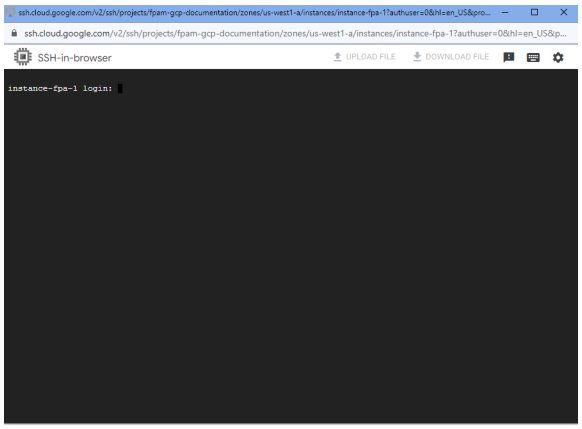
13. Select *EDIT* and in *Remote access*, select *Enable connecting to serial ports*.



14. Click *SAVE*.
15. In the instance page, select *CONNECT TO SERIAL CONSOLE*.



The SSH serial console opens.



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 551.
   Note down the IP addresses.



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:

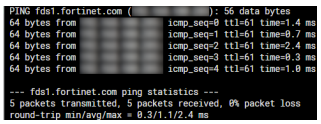
```
config router static
 edit 1
  set device port1
  set gateway 10.110.0.1
 next
end
```

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:





Optionally, to encrypt disk to protect logs and videos, see Configuring log and video disk encryption on page 357.

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 49.
  - 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 556, 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.



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.

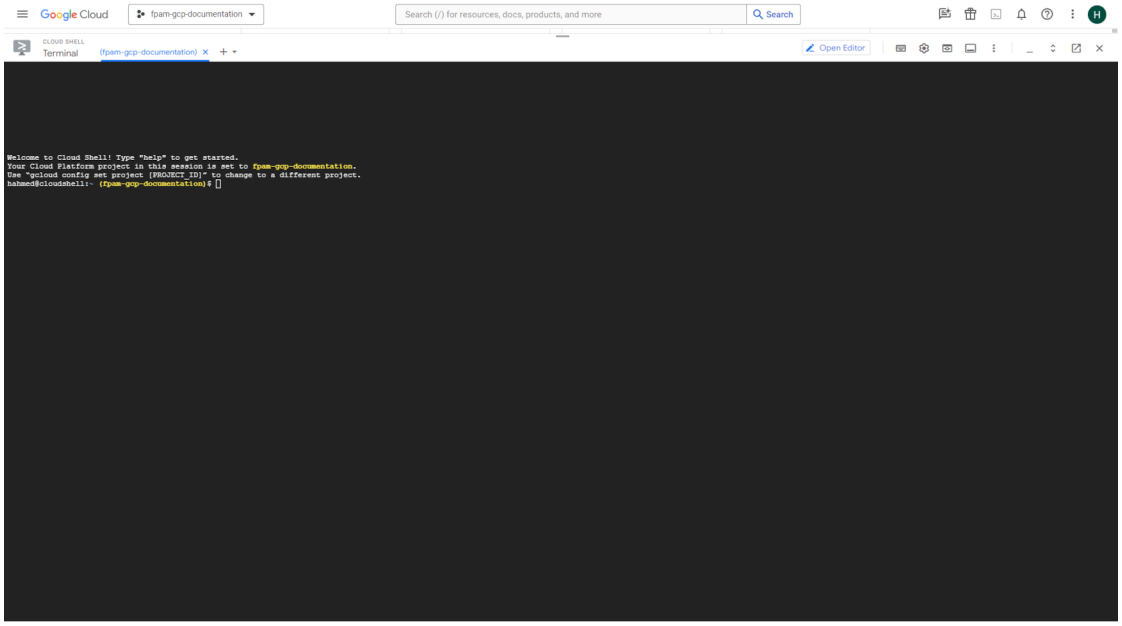
For more information, see Disaster recovery on page 421

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 548.

2. From the top-right, select *Activate Cloud Shell*.
   The *CLOUD SHELL Terminal* opens.



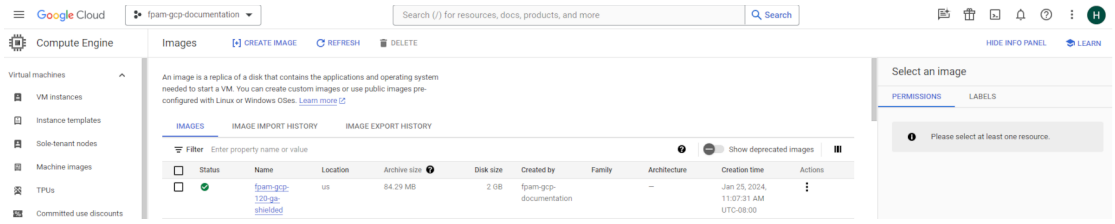
3. In the terminal, use the following commands to create a FortiPAM image:

```
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*.



4. Create the FortiPAM VM using the image created in step 3. See Creating VM instance from the image on page 551.
   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.

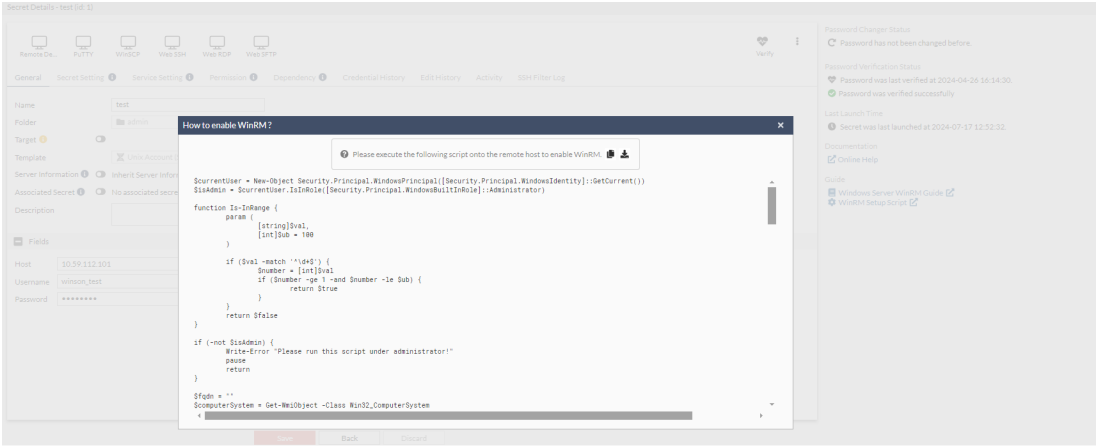
Use the commands as shown below to enable WinRM and set authentication on the target Windows servers.

1. Quick setup with script from FortiPAM on page 561
2. Executing the script on the sever with administrative privileges on page 561
3. Configuring WinRM on the server manually on page 562
4. Creating a privileged account on page 565

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.



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 = 2864518ED F2ADEA78C1046139 3A985AD661B1B8F
    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`.

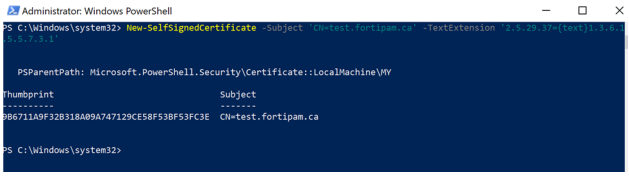
Choose one and copy the thumbprint for later use.

   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.



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
```

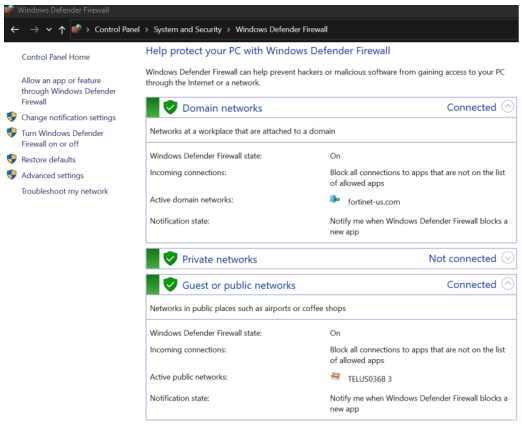
The above command should display the corresponding listener in the console.

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

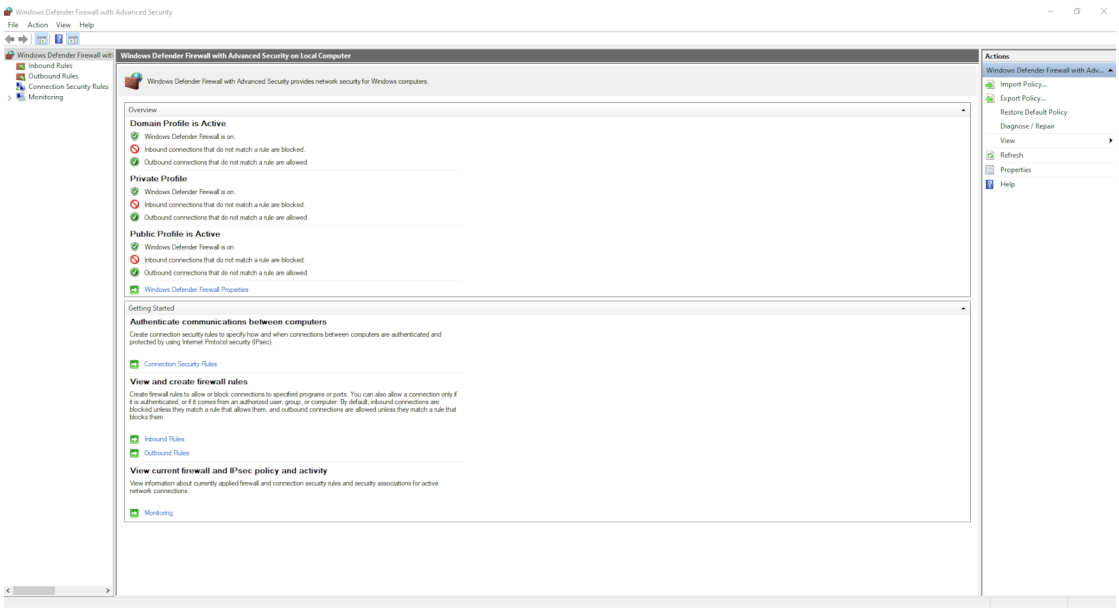
a. On the target Windows server, go to *Control Panel* > *System and Security* > *Windows Defender Firewall*.



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.



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**:

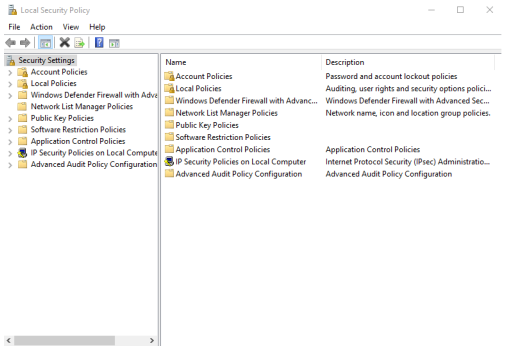
a. Log in to the Windows machine to configure the policy as an administrator.

b. Go to *Control Panel* > *System and Security*.

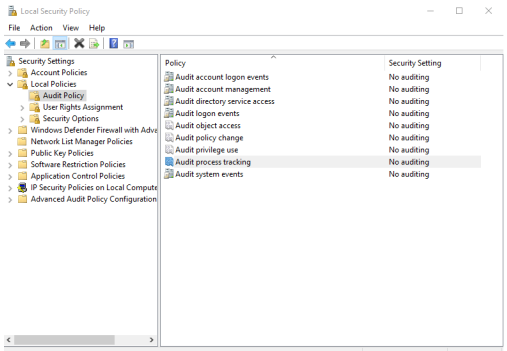
c. Click *Administrative Tools* and in the new window that opens, double-click *Local Security Policy*.

d. In the the *User Account Control* dialog that opens, click *Yes*.

The *Local Security Policy* window opens.



e. From the navigation pane on the left, expand *Local Policies* > *Audit Policy*.



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*.

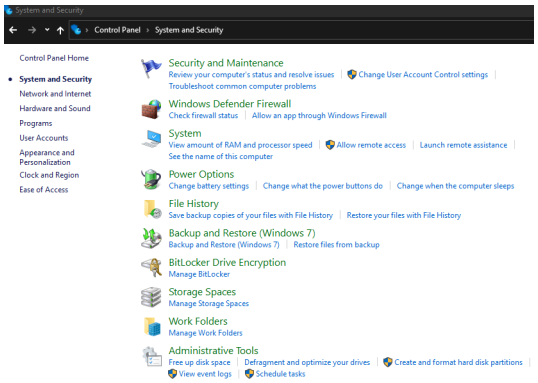
The configuration is now complete. Windows will generate audit events when the users you have specified takes actions on the files or folders for which you have set up audit policies.

Creating a privileged account

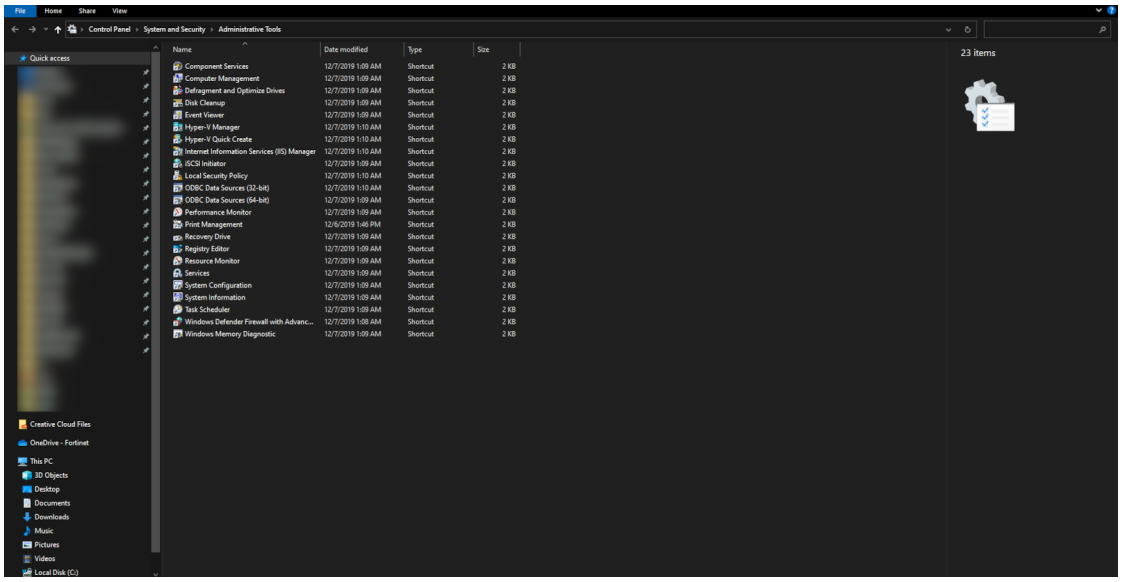
We create a new user belonging to the administrators groups.

To create a privileged account:

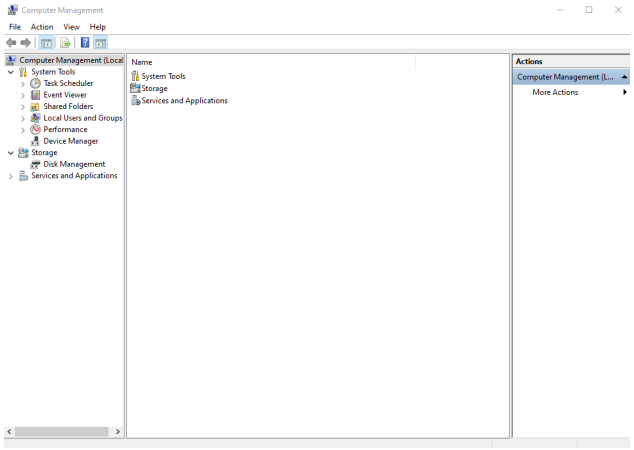
1. Go to *Control Panel* > *System and Security*.



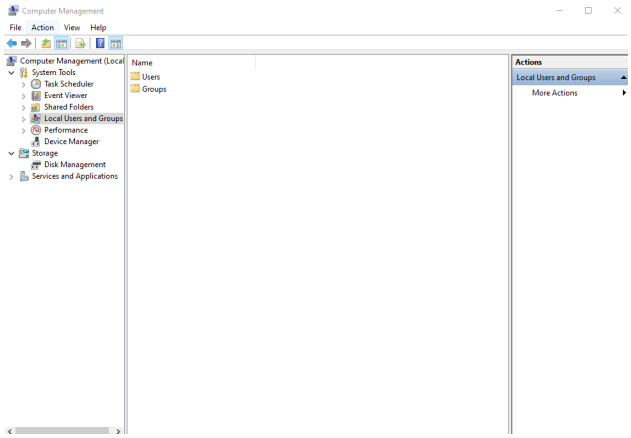
2. Click *Administrative Tools*.
3. In the *User Account Control* dialog that opens, click *Yes*.
   A new window opens.



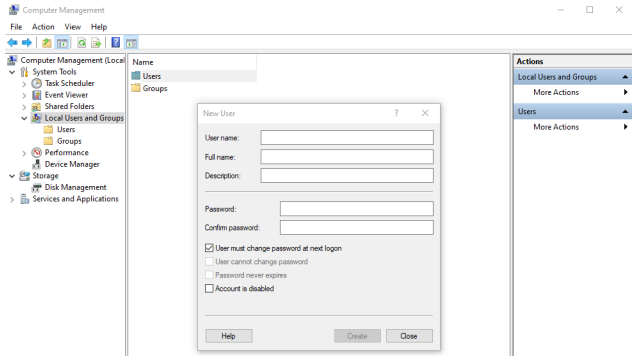
4. Double-click *Computer Management* to open it.
5. In the *User Account Control* dialog that opens, click *Yes*.
   The *Computer Management* window opens.



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.



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.



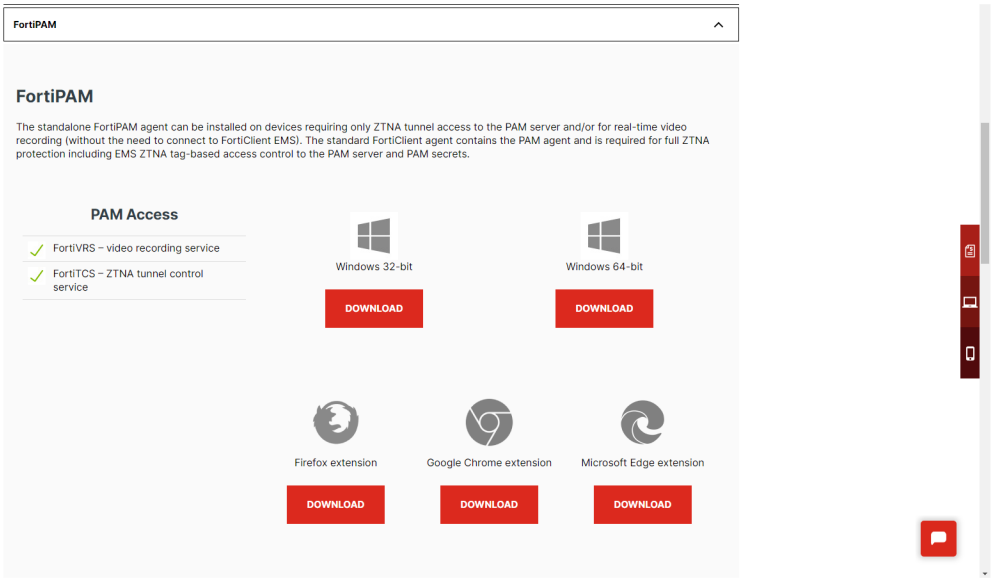
If you intend to retrieve RDP logs for the privileged account, you must create a secret for the privileged account with a Windows target. See Creating a secret on page 71.

Appendix M: FortiPAM browser extension and standalone FortiClient air-gapped installation

To install FortiPAM browser extension:

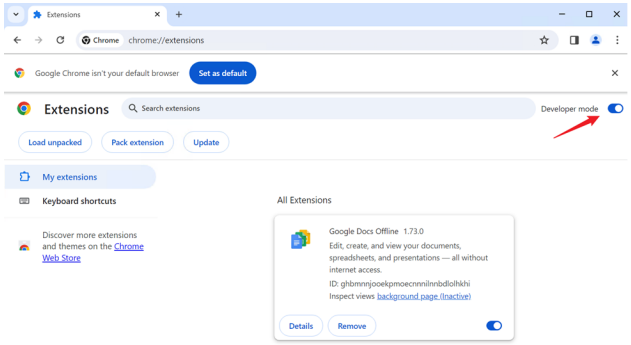
The FortiPAM Firefox extension is installed automatically when you install the standalone FortiClient.

1. Go to Fortinet Product Downloads center.
2. From the list, click *FortiPAM* to expand it.

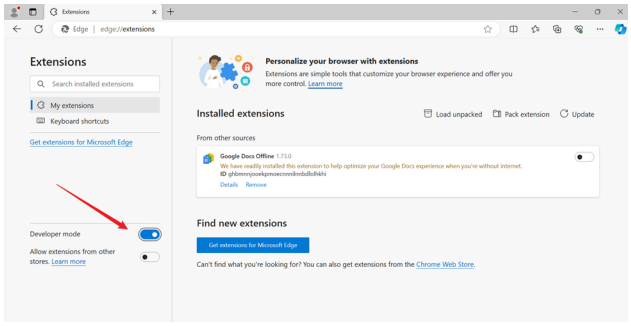


3. Click the *DOWNLOAD* button below the browser icon to download the required FortiPAM browser extension:
   a. *Google Chrome*: `fortipam-chrome-extension.crx`
   b. *Microsoft Edge*: `fortipam-edge-extension.crx`
   c. *Mozilla Firefox*: `fortipam-firefox-extension.xpi`
4. Copy the downloaded FortiPAM 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:

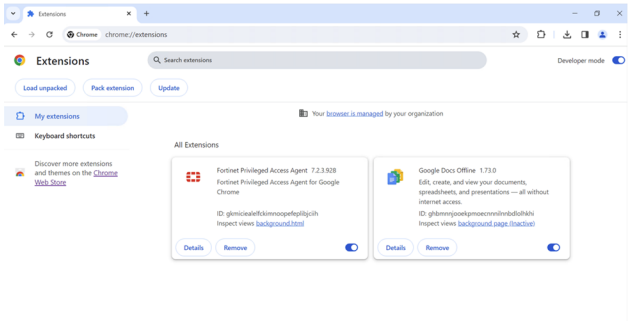


b. On Microsoft Edge:

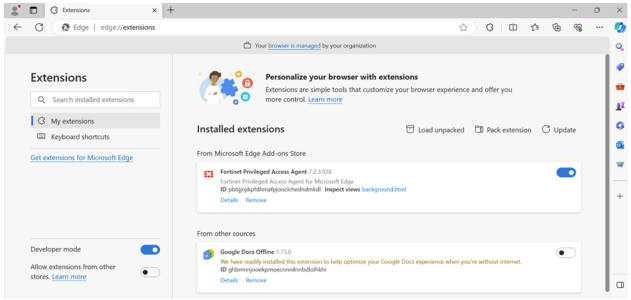


7. Drag and drop the FortiPAM browser extension file to the extension page, and install the browser extension by clicking *Add Extension*.

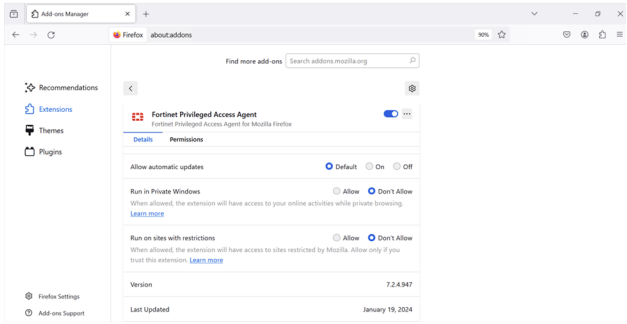
a. On Google Chrome:



b. On Microsoft Edge:



c. On Mozilla Firefox:



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

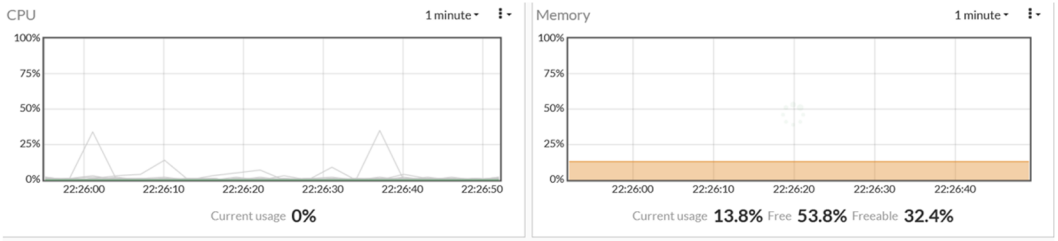
- 16 GB

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

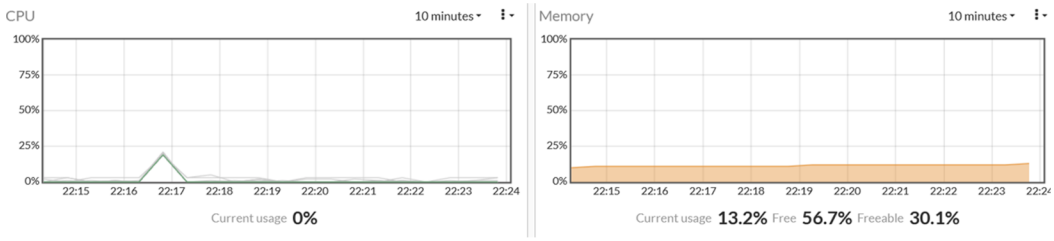


Note: The data was collected from the test performed in the FortiPAM lab.

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.

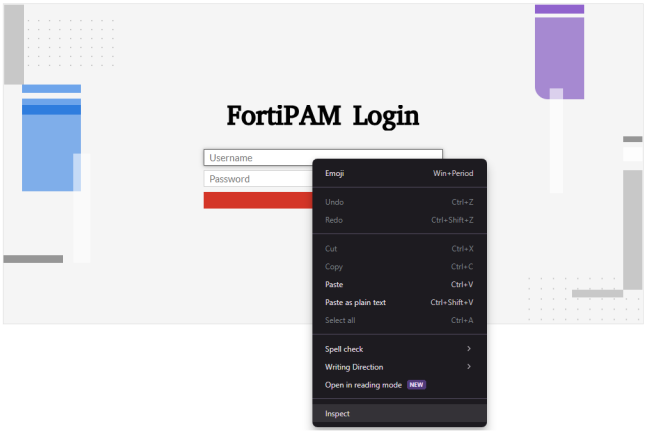
To find the appropriate selector for an input field, you can use the web browser inspection tool.

Example 1

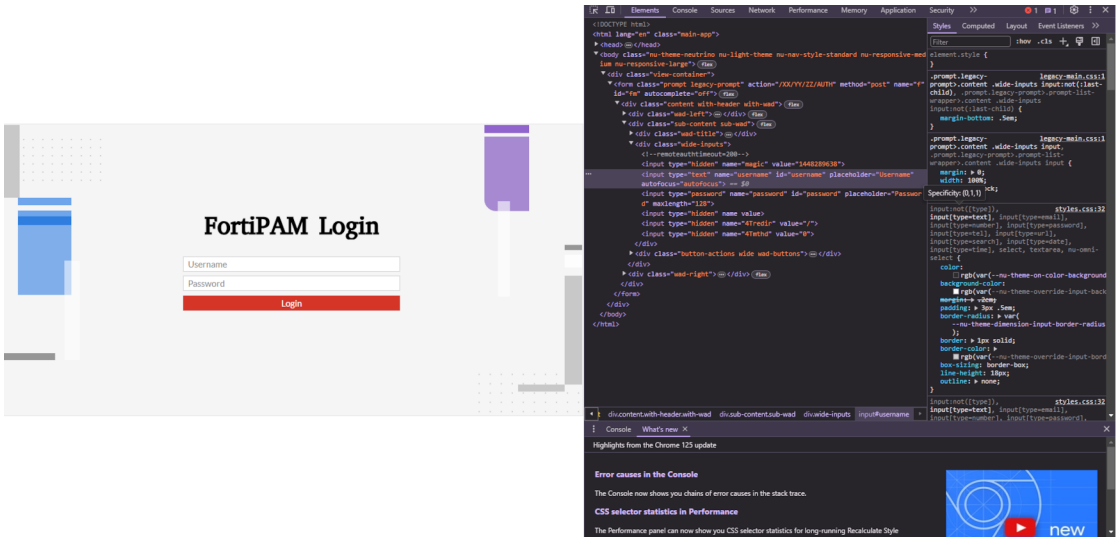
Finding selector for the *Username* field on the FortiPAM login page using the Google Chrome web browser

To find the selector for the *Username* field:

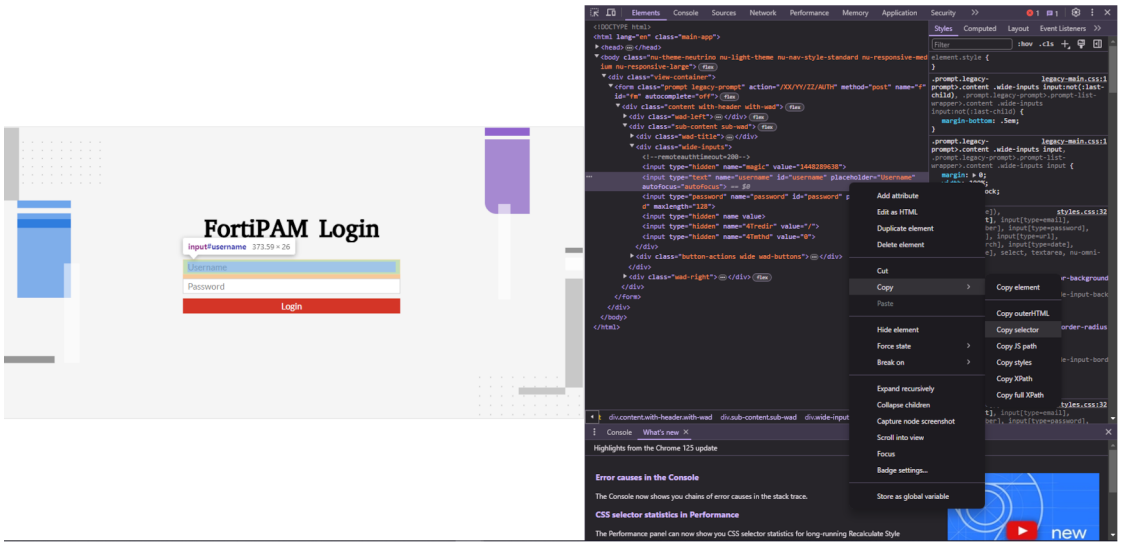
1. On the FortiPAM login page, right-click the *Username* field and select *Inspect*.



The HTML code for the *Username* field is highlighted in the Chrome developer tool.



2. Right-click the highlighted area and select *Copy* > *Copy selector*.



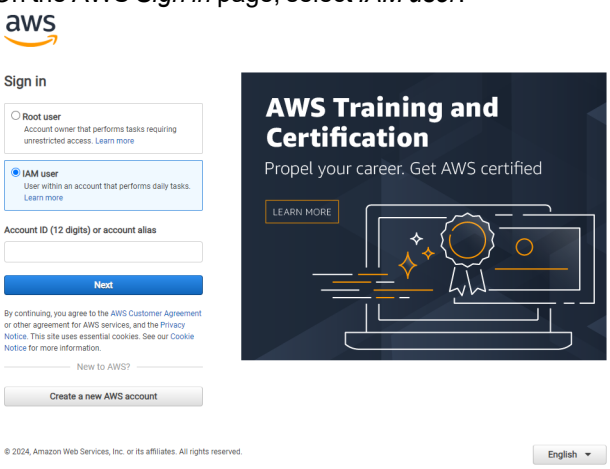
3. Paste the selector `#username` to the web filler configuration in secret template.

Example 2

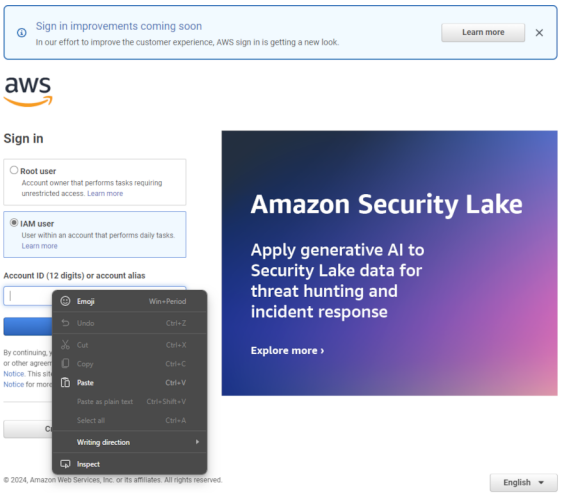
Finding selector for the *Account ID* field on AWS IAM user login page using the Microsoft Edge web browser

To find the selector for the *Account ID* field:

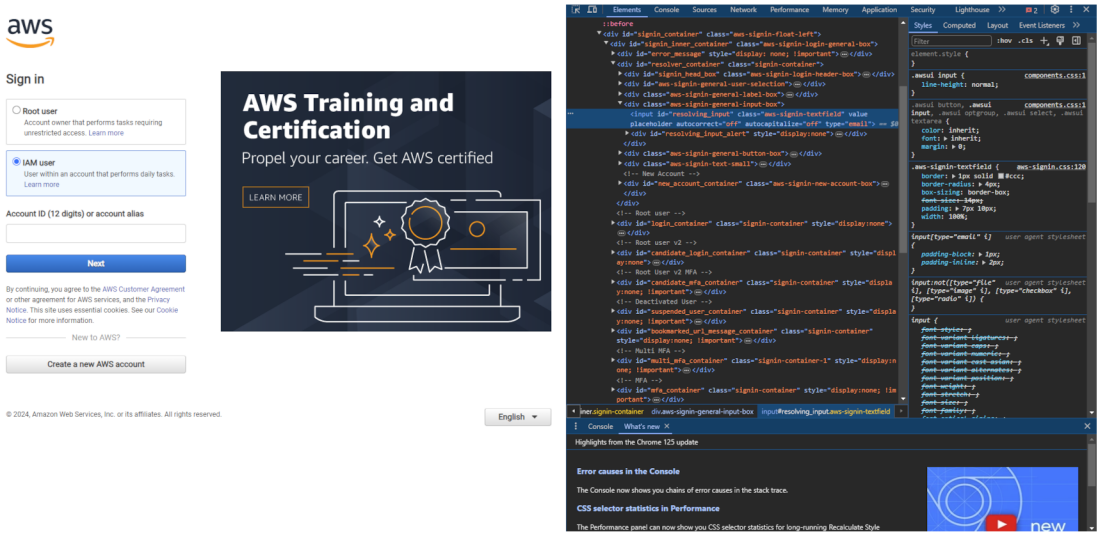
1. On the AWS *Sign in* page, select *IAM user*.



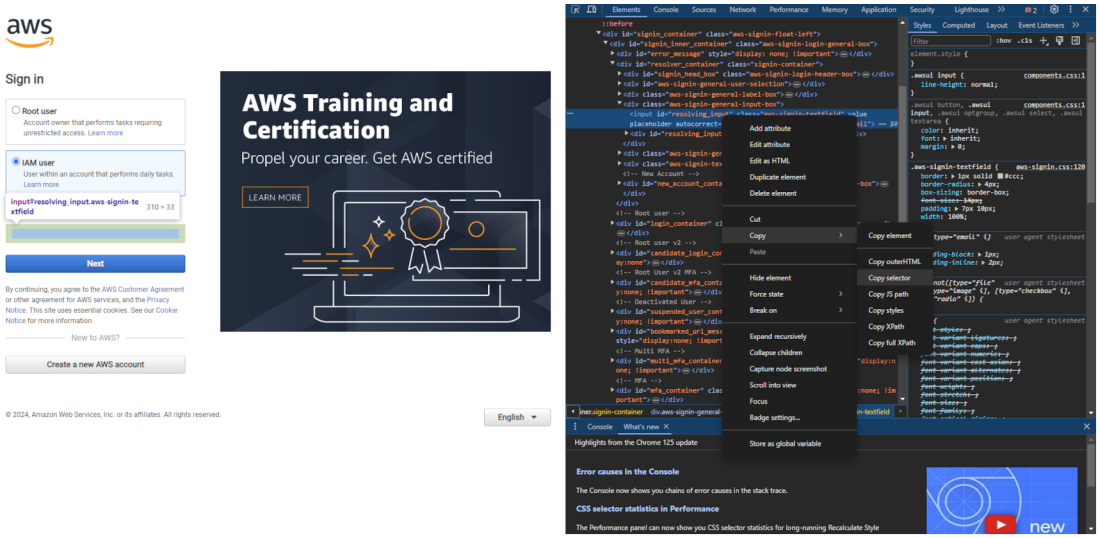
2. Right-click the *Account ID (12 digits) or account alias* field and select *Inspect*.



The HTML code for the *Account ID (12 digits) or account alias* field is highlighted in the Edge developer tool.



3. Right-click the highlighted area and select *Copy* > *Copy selector*.



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

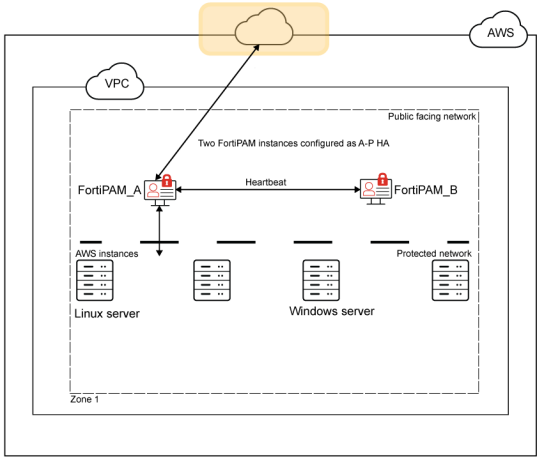
This chapter provides a sample configuration of active-passive (A-P) FortiPAM high availability (HA).

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 the same AZ, they must share the same subnet.

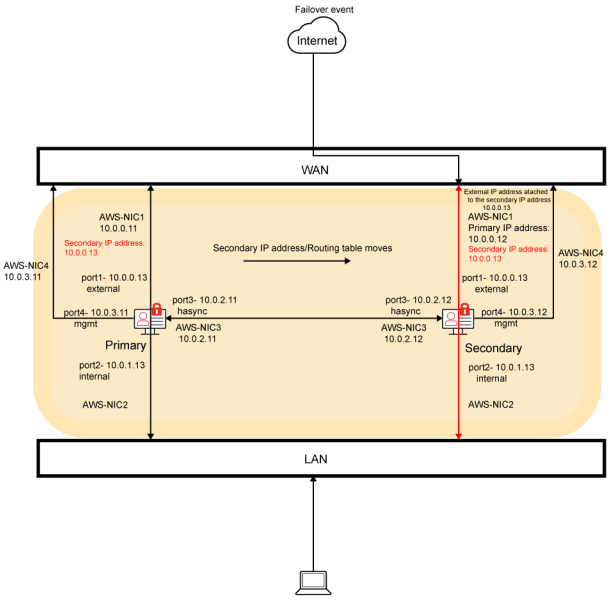
Configuring the primary and secondary nodes to use the same VIP allows users to connect to the same IP address after a failover.

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

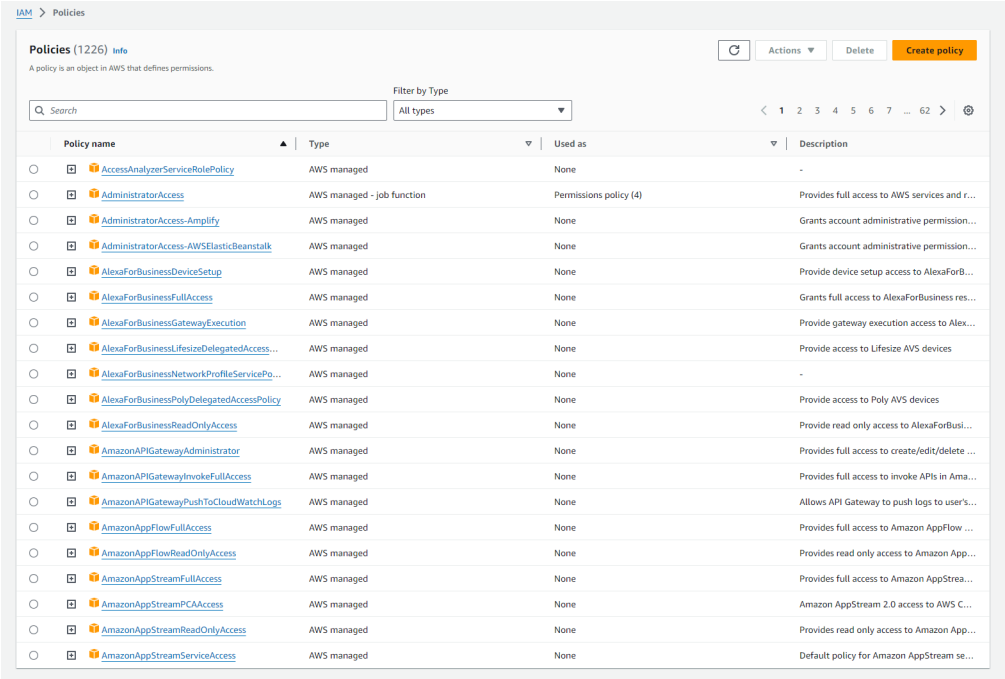
Prerequisites

- Creating a custom permission policy on page 581
- Creating an IAM role on page 582
- Creating a VPC on page 585
- Creating subnets on page 586
- Creating an internet gateway on page 587
- Configuring routing tables on page 588
- Creating network interfaces on page 590
- Creating elastic IP addresses on page 591

Creating a custom permission policy

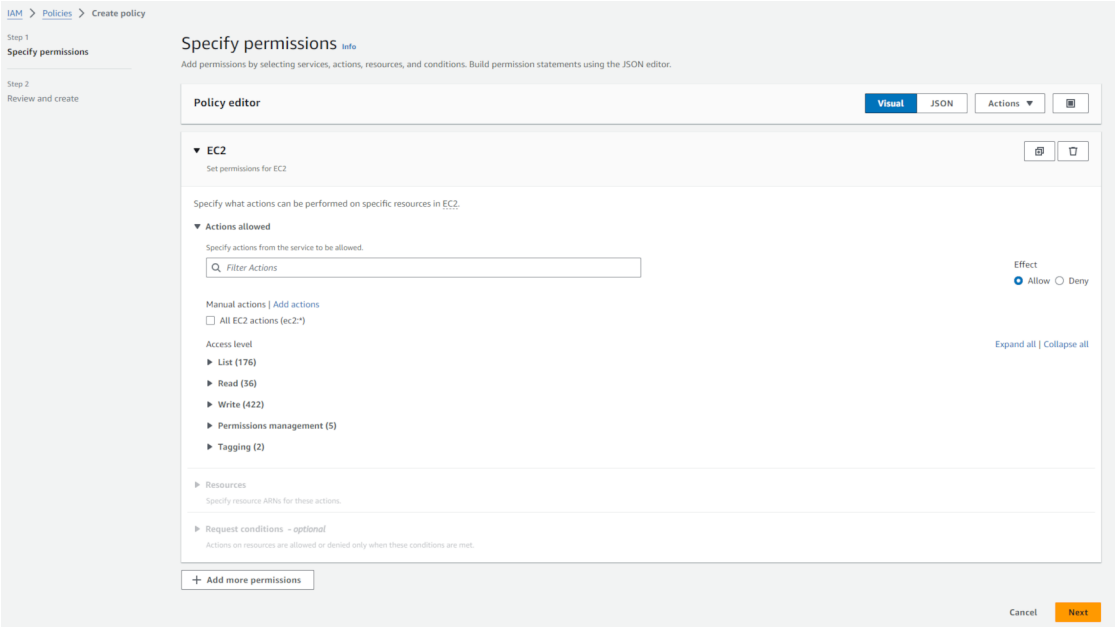
To create a custom permission policy:

1. In the AWS console, open *IAM*.
2. From the *Dashboard*, go to *Access management* > *Policies*.
   The *Policies* window opens.

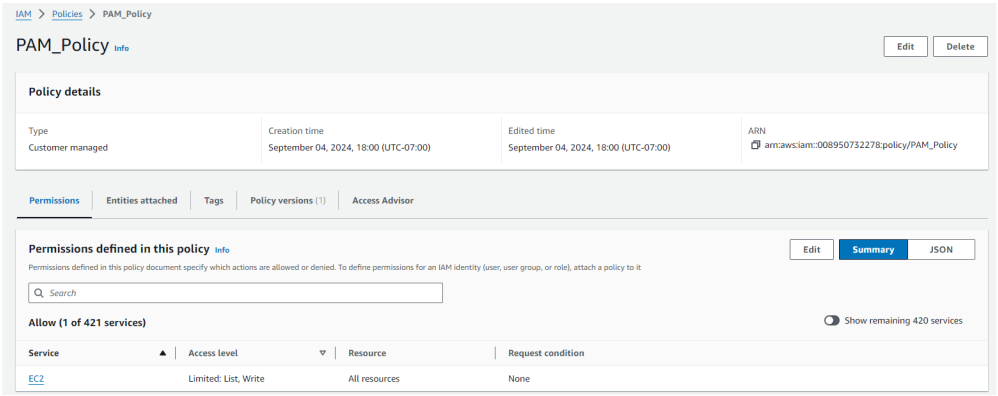


3. From the list, select *Create policy*.

4. In the *Service* dropdown, select *EC2*.



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*.



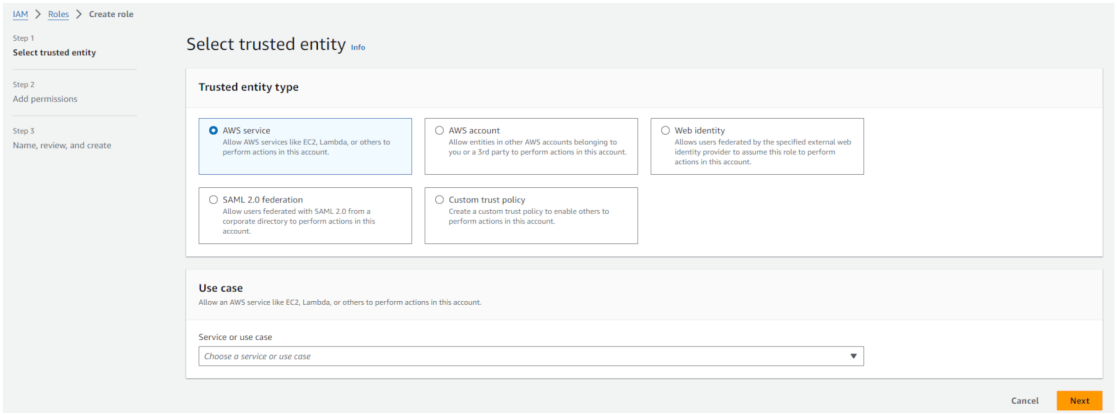
Creating an IAM role

The IAM role is necessary for HA failover.

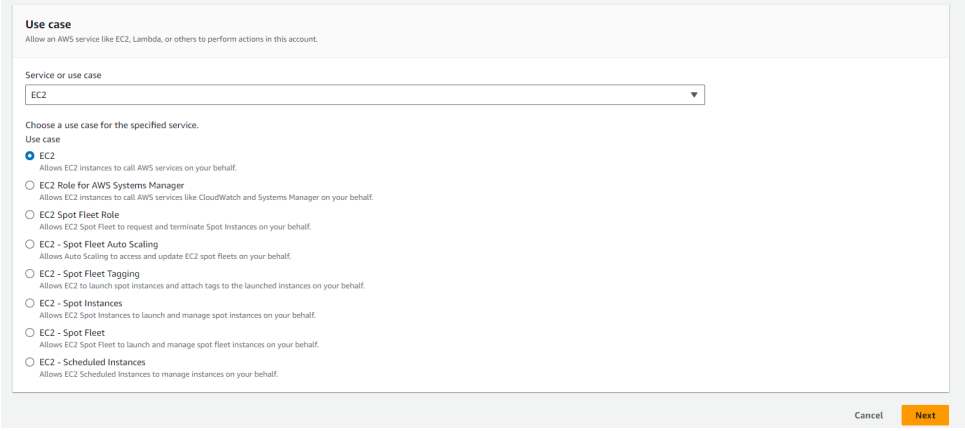
Ensure that the IAM role can read and write EC2 information to read, detach, and reattach network interfaces and edit routing tables.

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.

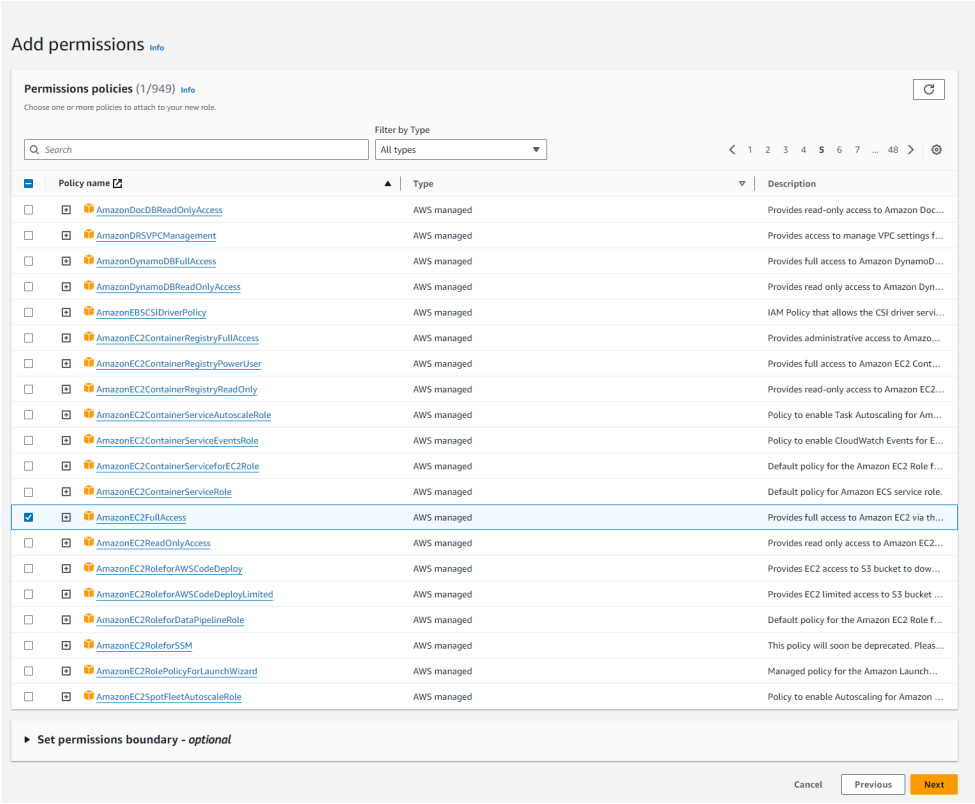


4. From *Trusted entity type*, select *AWS service*.
5. In the *Use case* dropdown, select *EC2*.

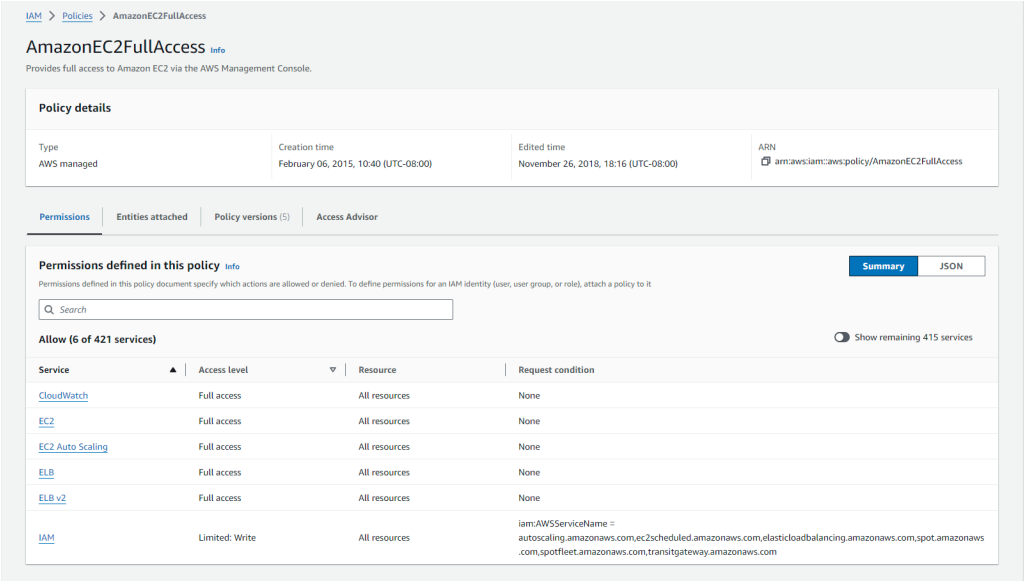


6. Click *Next*.
   The *Add permissions* window opens.

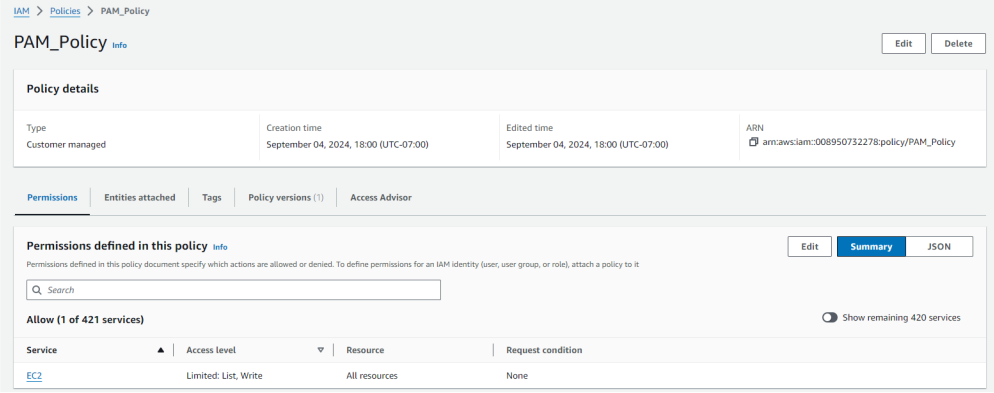
7. From the permission policies list, select *AmazonEC2FullAccess*.



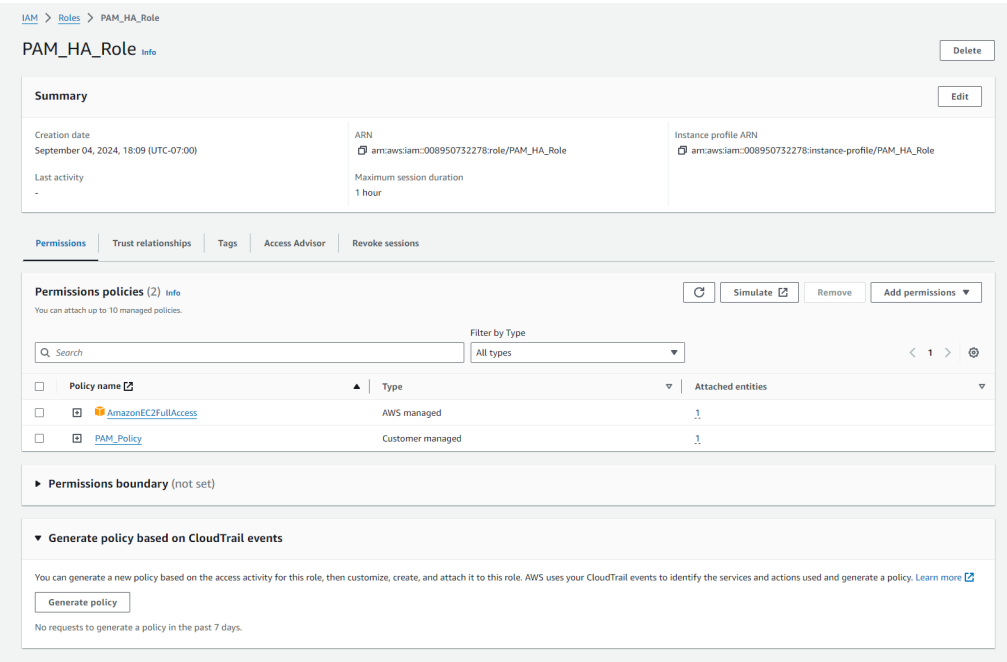
Click the *AmazonEC2FullAccess* role to see it in a new window.



8. From the permissions policies list, look for the policy created in Creating a custom permission policy on page 581, and select it.
   Click the *PAM_Policy* role to see it in a new window.



9. Click *Next*.
10. In *Role* details, enter a role name.
11. Optionally, enter a description.
12. Click *Create role*.



Creating a VPC

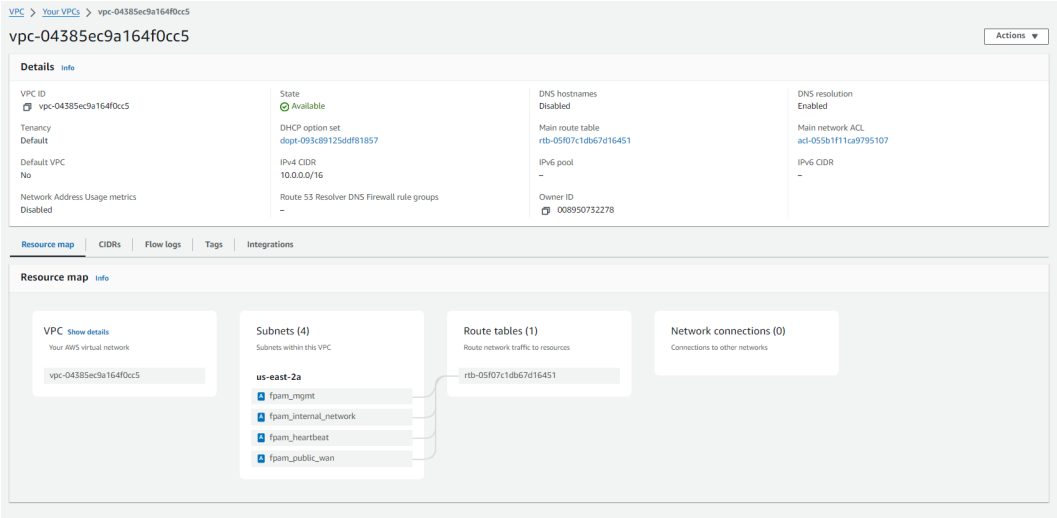
We create a VPC with four subnets.

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.



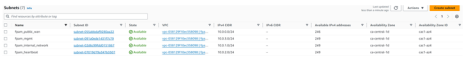
Creating subnets

We create four subnets.

The four subnets are the following:

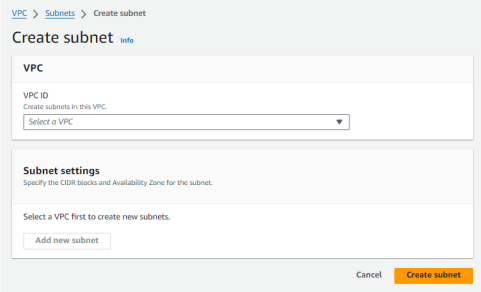
- Public WAN
  `10.0.0.0/24`
- Internal network
  `10.0.1.0/24`
- Heartbeat network
  `10.0.2.0/24`
- Management network
  `10.0.3.0/24`

The VPC created in Creating a VPC on page 585 is used in both the primary and the secondary FortiPAM.

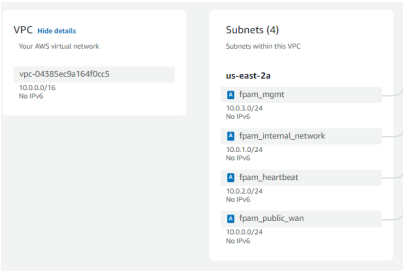


To create a subnet:

1. In the VPC created in Creating a VPC on page 585, go to *Virtual private cloud* > *Subnets*.
2. Select *Create subnet*.
   The *Create subnet* wizard opens.



3. From the *VPC ID* dropdown, select the VPC created in Creating a VPC on page 585.
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.



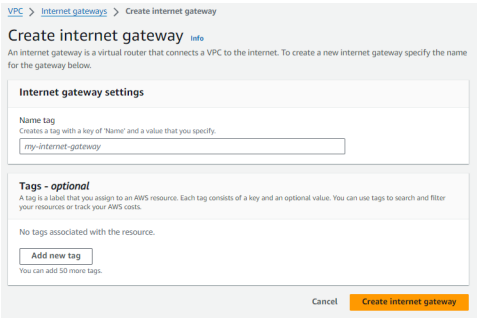
Creating an internet gateway

We create a new gateway and attach it to the newly created VPC in Creating a VPC on page 585.

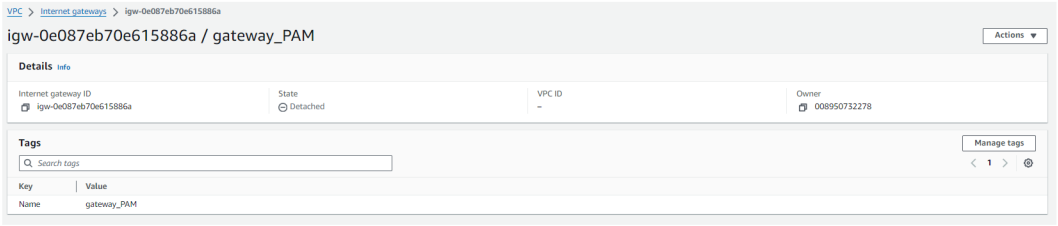
The internet gateway takes charge of the VPC to communicate to the public internet.

To create an internet gateway:

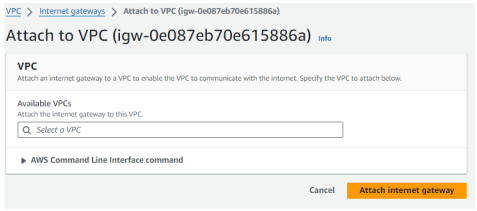
1. In VPC, go to *Virtual private cloud* > *Internet gateways*.
2. From the internet gateways list, select *Create internet gateway*.
   The *Create internet gateway* wizard opens.



3. Enter a name for the tag.
4. Click *Create internet gateway*.
   The internet gateway is created.



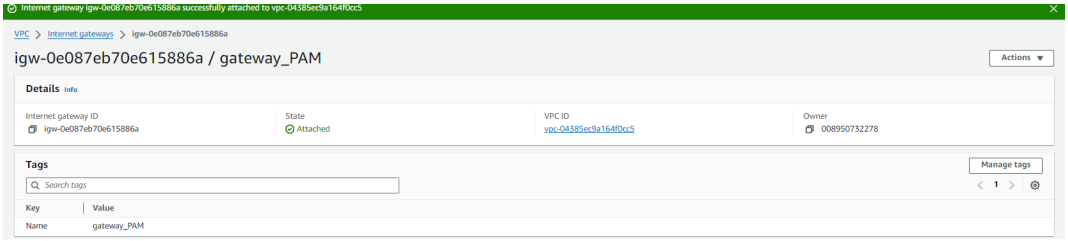
5. From the *Actions* dropdown on the right, select *Attach to VPC*.
   The *Attach to VPC* window opens.



6. From *Available VPCs*, select the VPC created in Creating a VPC on page 585.



7. Click *Attach internet gateway*.
   The internet gateway is attached to the VPC.



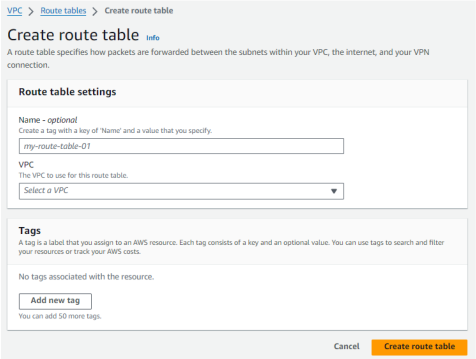
Configuring routing tables

We configure two routing tables under the recently created VPC and gateway.

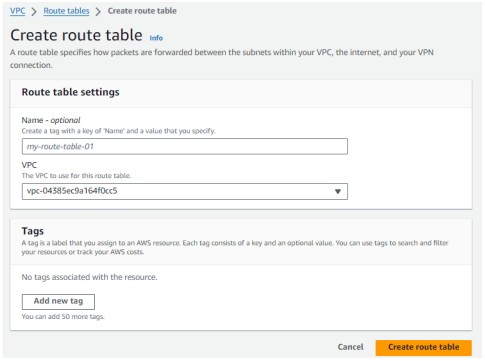
The following shows the public WAN, internal network, heartbeat routing table, and subnets association information.

To configure routing table:

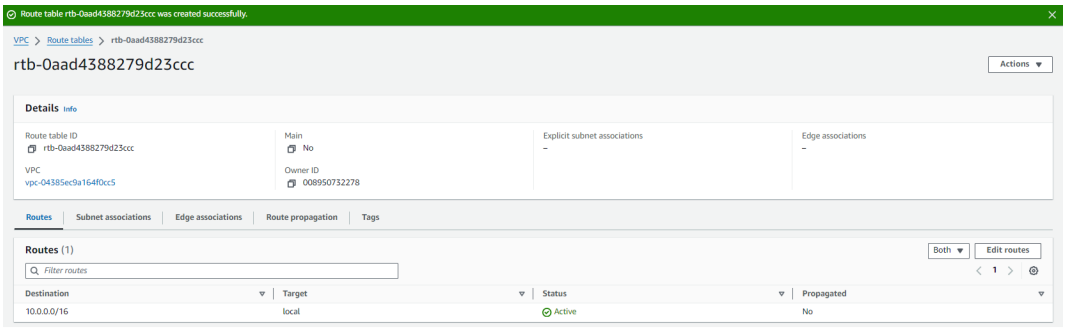
1. In *VPC*, go to *Virtual private cloud* > *Route tables*.
   a. From the right, select *Create route table*.
      The *Create route table* wizard opens.



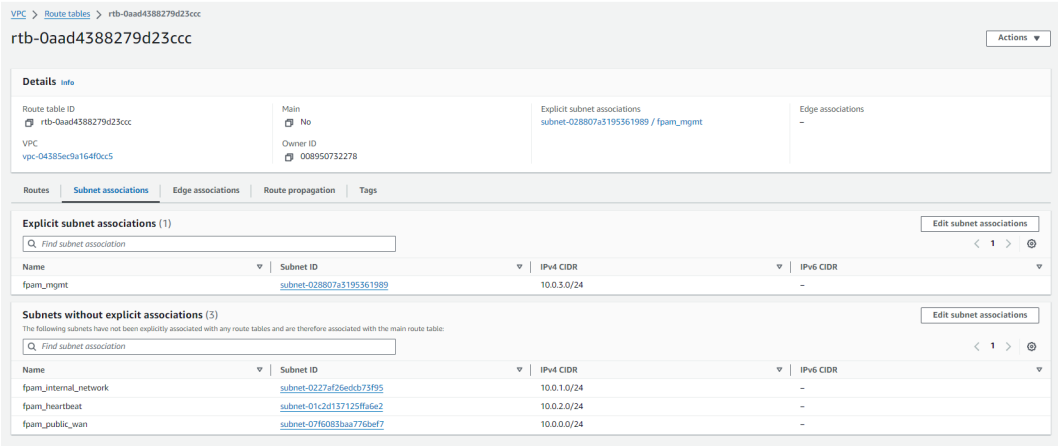
2. From the *VPC* dropdown, select the VPC created in Creating a VPC on page 585.



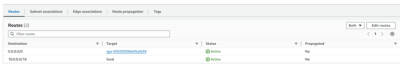
3. Select *Create route table*.
   The routing table is created.



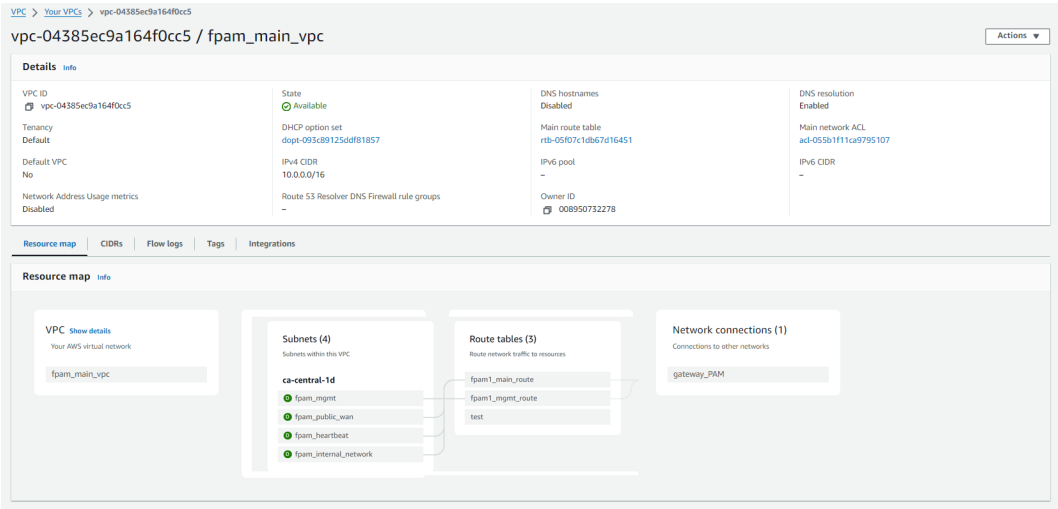
4. In the *Subnet associations* tab, from the right, select *Edit subnet associations*.
5. Select the subnet with *IPv4 CIDR* as `10.0.3.0/24` and click *Save association*.
   The subnet associations are updated for the routing table.



6. Create another routing table with a target.



After VPC, subnets, gateways, and routing tables have been set up, the VPC configuration looks like the following:

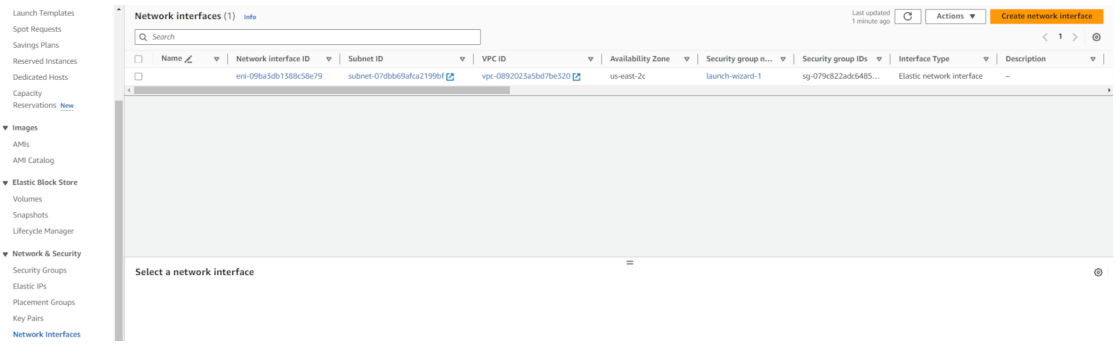


Creating network interfaces

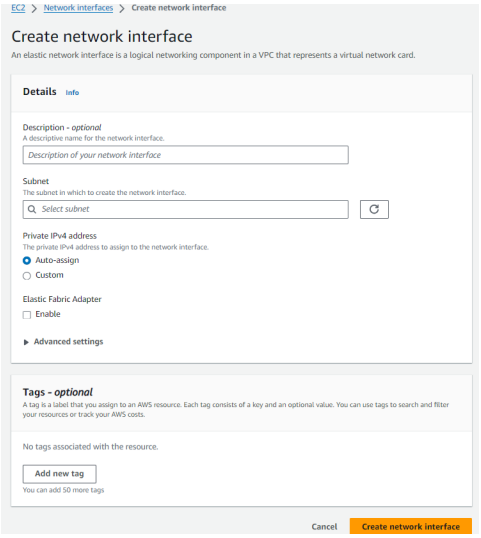
We create a network interface in every VPC subnet.

To create network interface:

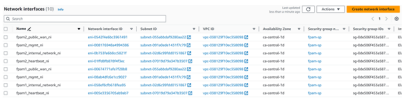
1. Go to *EC2 > Network & Security > Network Interfaces*.
   The *Network interfaces* window opens.



2. From the right, select *Create network interface*.
   The *Create network interface wizard* opens.



3. From the *Subnet* dropdown, select one of the subnets created in Creating subnets on page 586.
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.

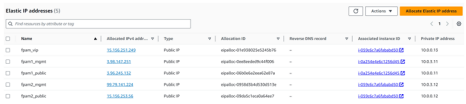


Creating elastic IP addresses

To create elastic IP address:

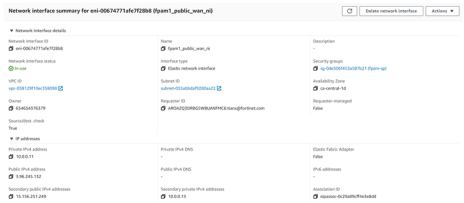
1. Go to *EC2 > Network & Security > Elastic IPs*.
   You should have five elastic IP addresses.
   Setting up the environment requires five elastic IP addresses:
   - One public WAN IP address. This is the FortiPAM GUI VIP.
   - One FortiPAM primary management IP address.
   - One FortiPAM secondary 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.



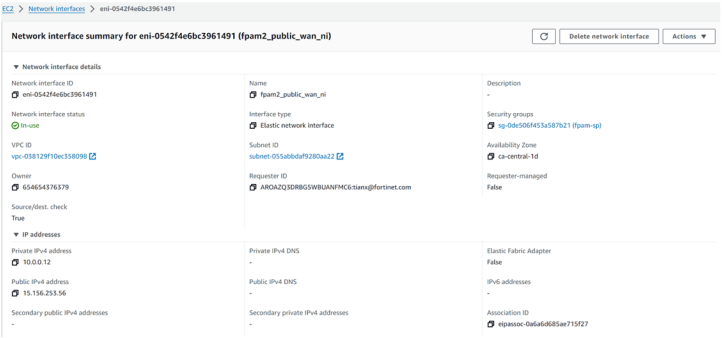
We take a look at the current FortiPAM primary and secondary WAN interface configuration by going to *Network & Security* > *Network Interfaces* and opening the network interface.

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.



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.



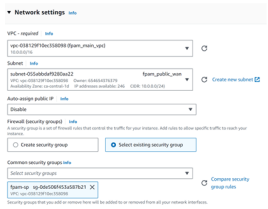
Configuring the FortiPAM instances on AWS

To configure FortiPAM instance:

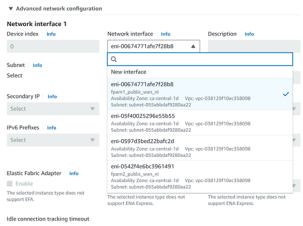
1. Upload FortiPAM image and create the FortiPAM AMI.
   See Appendix J: Installation on AWS on page 534.

Before launching the FortiPAM instance from AMI, you must create a FortiPAM security group.

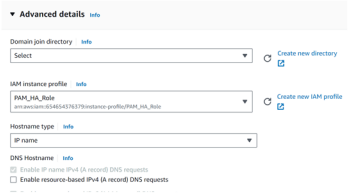
The following shows the FortiPAM instance network settings with VPC, public WAN subnet, and the security group created beforehand.



2. In *Advanced network configuration*, attach the four network interfaces created in Creating network interfaces on page 590 to the FortiPAM instance.



3. In *Advanced details*, attach HA role to the FortiPAM instance.

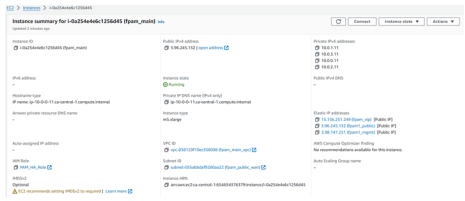


Launching the FortiPAM instance

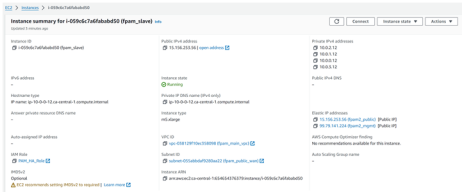
The following shows the main configurations and network settings for the primary and the secondary FortiPAM instances.

Currently, both the FortiPAM GUI VIP and the `port1` IP address are attached to the main FortiPAM instance.

FPAM_MAIN



FPAM_SECONDARY





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`.



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.

For more information, see Disaster recovery on page 421

Testing and debugging HA failover

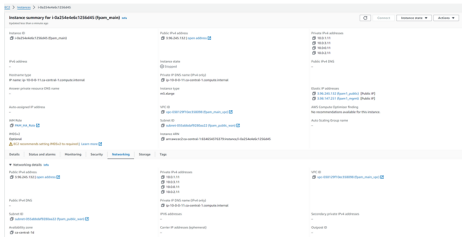
1. In the CLI console, enter the following command to verify that FortiPAM units are in sync:

   ```
   get system ha
   ```

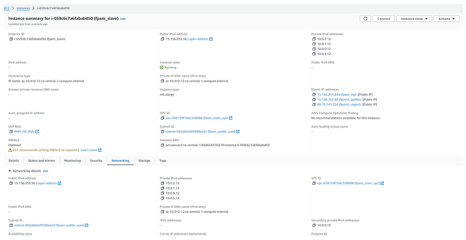
   

2. In the FortiPAM GUI, create a secret.
   To create a secret, see Creating a secret on page 71.
   Verify that you can launch the secret.
   See Launching a secret on page 99.
3. Before you power off `PAM_MAIN`, you can see that the second IP address (`10.0.0.0.13`) and the VIP (`15.156.251.249`) are 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



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`).



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:

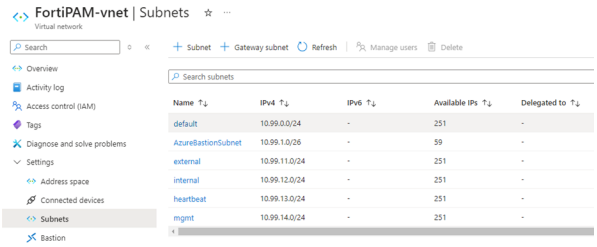
1. Configuring Azure virtual network and subnets on page 598
2. Creating public IP addresses on page 599
3. Creating the FortiPAM-VM on Azure on page 600
4. Enabling HA on FortiPAM on page 601
5. Accessing the FortiPAM GUI portal on page 605
6. Accessing HA management interface on page 605
7. Setting up SDN connector on page 606
8. Configuring SDN connector on FortiPAM on page 609
9. Accessing the GUI portal after the HA failover on page 611
10. Adding a DR node on page 611
11. Verification on page 616

Configuring Azure virtual network and subnets

We configure a virtual network with four subnets:

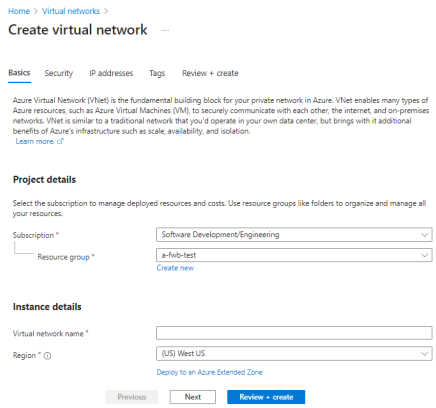
- One to access to the FortiPAM GUI portal
- (Optional) One to connect to the internal target servers
- One for HA heartbeat
- One for dedicated HA management

The following shows a virtual network with four subnets: *external*, *internal*, *heartbeat*, and *mgmt*.



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.



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:

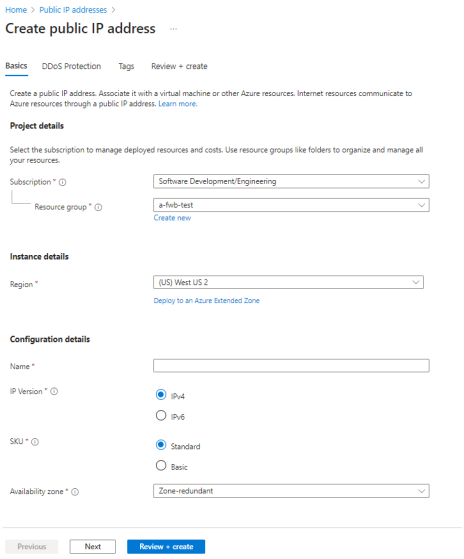
- One for traffic to the active (primary) FortiPAM. In case of failover, the IP address moves from the primary FortiPAM to the secondary.
- Two for management access to each FortiPAM.



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.

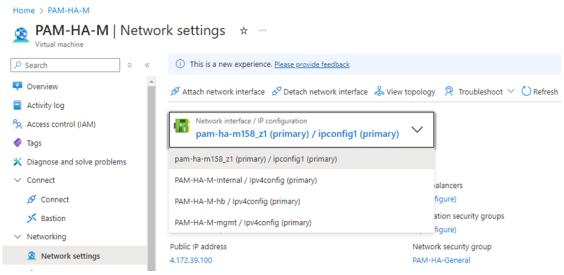


3. From the *Subscription* dropdown, select a subscription.
4. From the *Resource group* dropdown, select a resource group.
5. In *Region*, select a region where the public IP address is created.
6. In *Name*, enter the name for the public IP address.
7. In *IP Version*, select *IPv4*.
8. Click *Next*.
9. Click *Review+create* to create the public IP address.
10. Repeat steps 1 - 9 to create two additional public IP addresses.

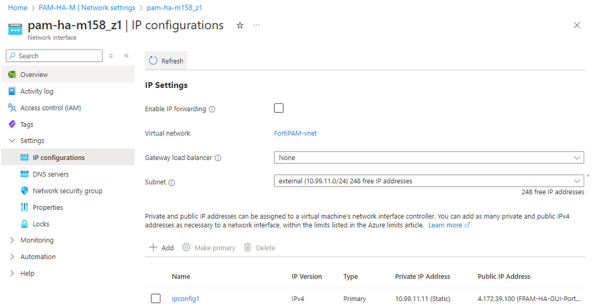
Creating the FortiPAM-VM on Azure

To create the FortiPAM-VM on Azure:

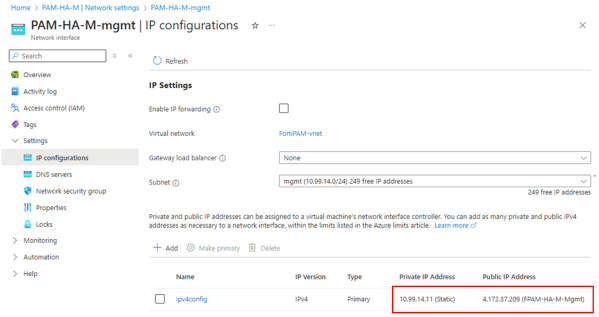
1. Create two FortiPAM VMs on Azure.
   See Appendix G: Installation on Azure on page 518.
   Ensure that the following are correctly configured:
   a. Each FortiPAM-VM should be in the same region and they must have the same VM and disk size.
   b. Add four network interfaces to the FortiPAM-VM.
      One interface for every subnet in the same order.
      Following is the network settings for the primary FortiPAM node:



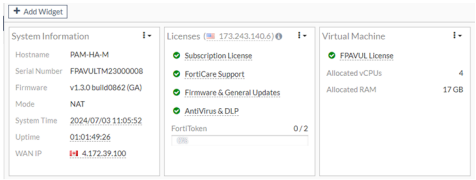
   c. Assign the public IP address to the external interface of the primary FortiPAM.
      Go to *Settings* > *IP configurations* in the network interface for the primary FortiPAM node.
      Following is the IP configuration for the FortiPAM primary node external interface:



d. Assign the public IP addresses to the *mgmt* interface of the primary FortiPAM.
Following is the FortiPAM primary node management interface IP configuration:



e. Each FortiPAM instance must have its own valid license.



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 368.
   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
```



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.

For more information, see Disaster recovery on page 421

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

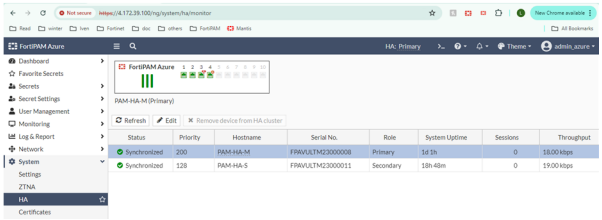
```
config system ha
 set group-name "Azure_PAM_HA"
 set mode active-passive
 set password ENC XghDJZtZmoAMNt2RcCq
 set hbdev "port3" 0
 set ha-mgmt-status enable
 config ha-mgmt-interface
  edit 1 #gateway for the private IP address of the mgmt interface
   set interface "port4"
   set gateway 10.99.14.1
  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.



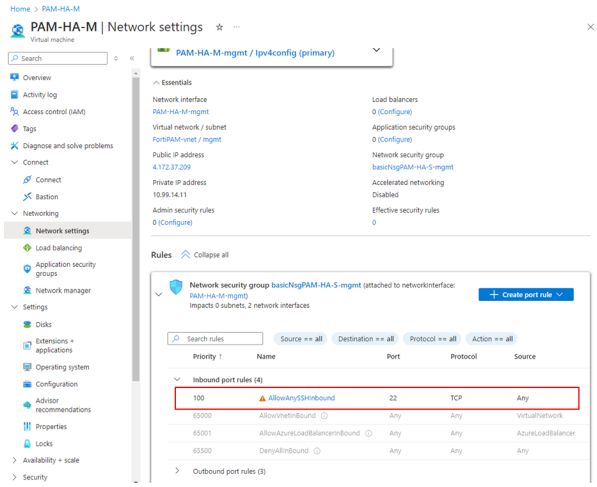
Accessing HA management interface

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.



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
```

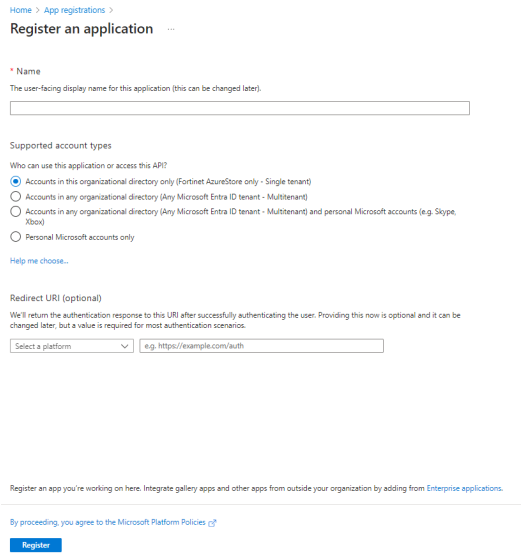
Setting up SDN connector

Adding Azure application registration

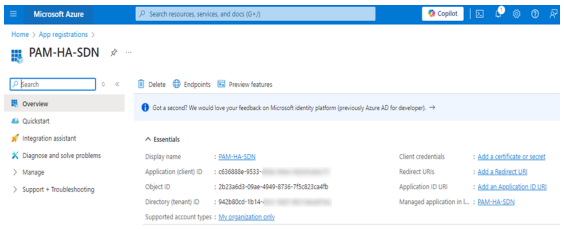
We add the Azure application registration to allow FortiPAM to make the API call.

To add Azure application registration:

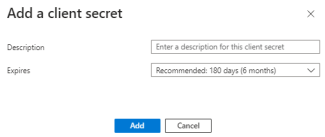
1. In the Azure portal, using the search bar, open *App registrations*.
2. Select *New registration*.
   The *Register an application* wizard opens.



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.



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.

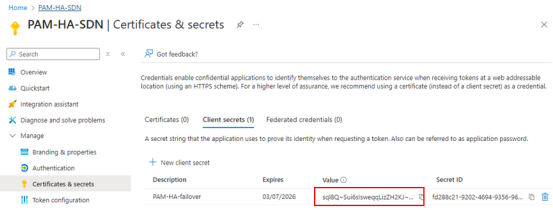


   d. From the *Expires* dropdown, choose an expiration time for the client secret.

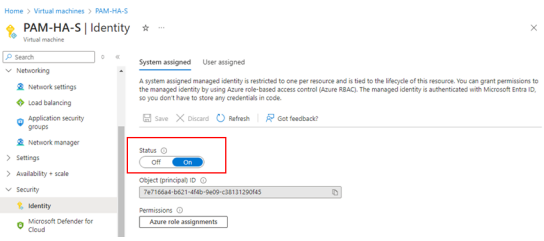


You must renew the client secret on time for HA to failover properly.

   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.

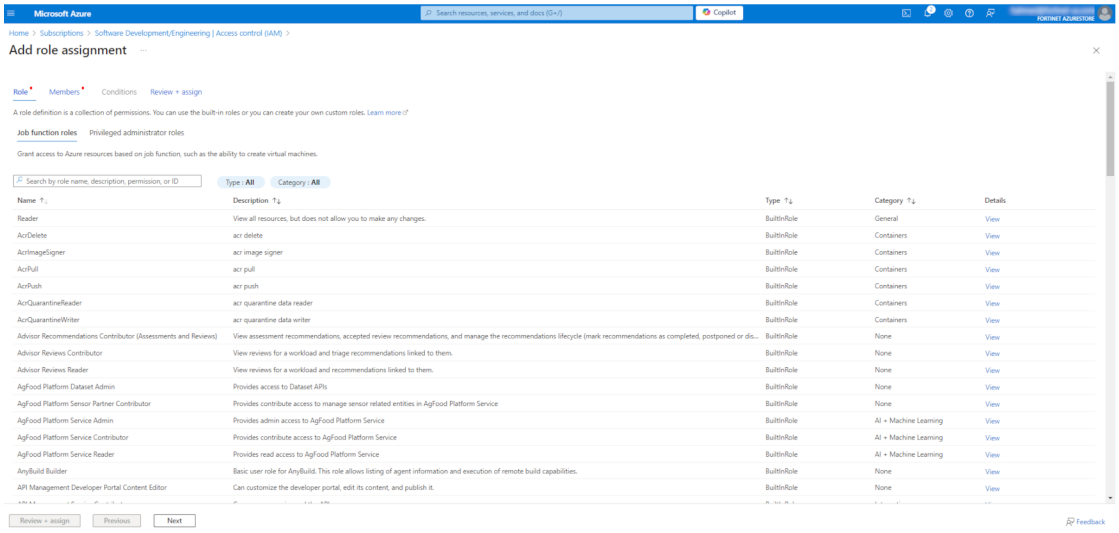


7. Adding an Azure IAM role:
   Add IAM role for the FortiPAM-VM and the SDN application.
   a. In the Azure portal, using the search bar, open *Virtual machines*.
   b. From the list, click to open the secondary FortiPAM-VM.
   c. Go to *Security* > *Identity* and ensure that the FortiPAM-VM has the system assigned managed identity status enabled.

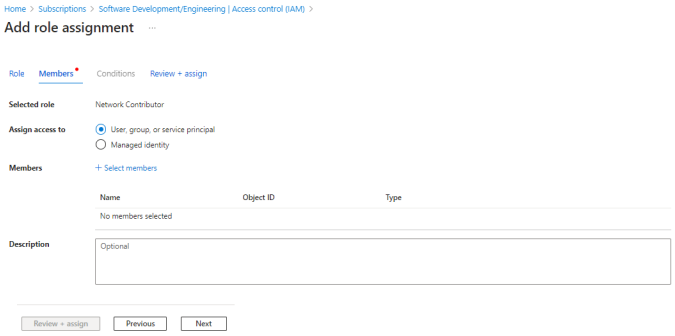


   d. Adding role assignment:
      i. In the Azure portal, using the search bar, open *Subscriptions*.
      ii. Click to open the subscription and go to *Access Control (IAM)*.

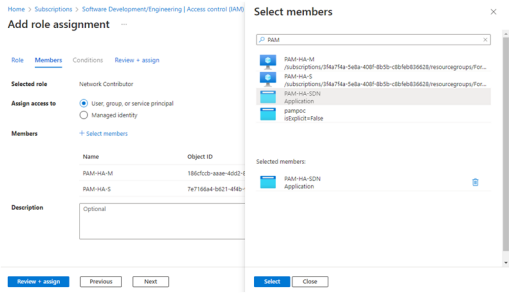
iii. Select *Add* > *Add role assignment* to add a role assignment.



iv. From the list, select *Network Contributor*, and click *Next*.
The *Add role assignment* wizard opens.

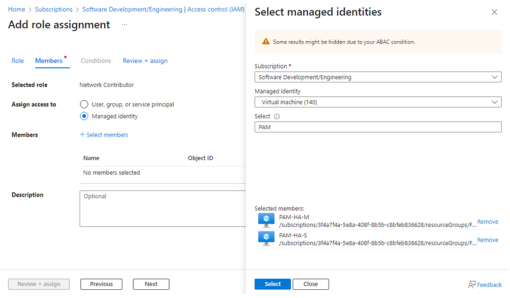


v. In *Assign access to*, for *User, group, or service principal*:
   i. In *Members*, select *+Select members*, from *Select members*, select the SDN application.



   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.



ii. Click *Select*.

vii. Click *Review+assign*.

Configuring SDN connector on FortiPAM

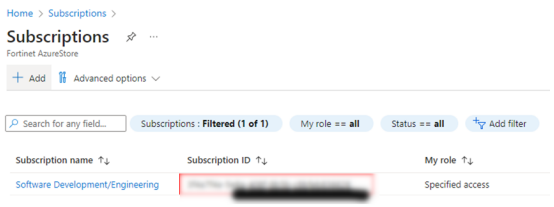
To configure an SDN connector on FortiPAM:

1. On the primary FortiPAM, enter the following commands:

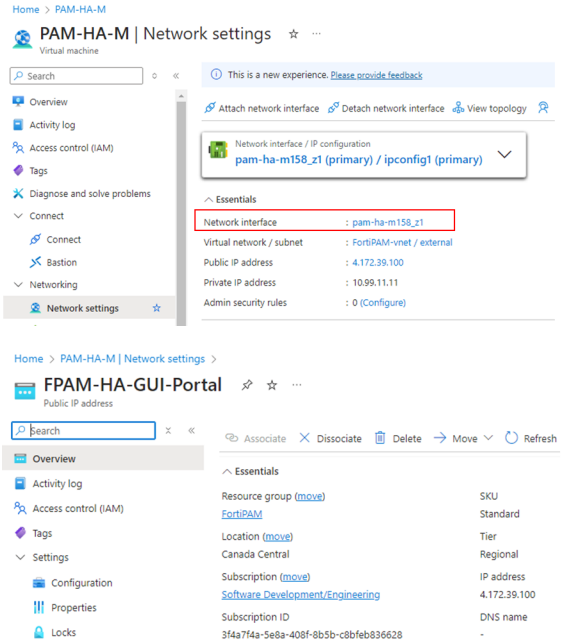
```
config system sdn-connector
 edit "azure-ha"
  set type azure
  set use-metadata-iam disable
  set ha-status enable
  set tenant-id ""
  set client-secret ""
  set subscription-id ""
  set resource-group "FortiPAM"
  config nic
   edit "pam-ha-m158_z1"
    config ip
     edit "ipconfig1"
      set 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 606.
- `client-secret` is the secret value created in Creating a client secret.
- `subscription-id` is in *Subscriptions* in the Azure portal.



- In `config nic`, add the network interface used to access the GUI portal and the public IP address name.



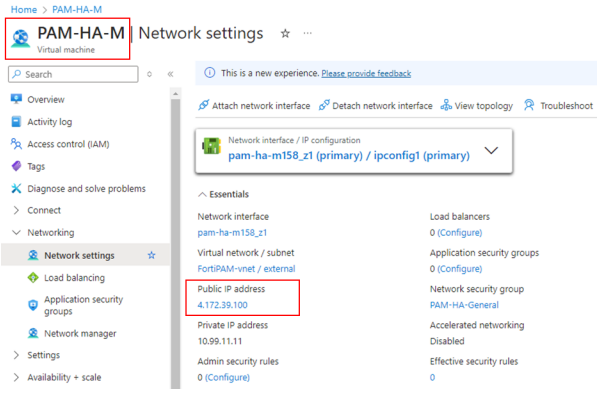
2. On the secondary FortiPAM, enter the following commands to configure the SDN connector on the HA secondary node. The settings are similar to those on the primary node. The only difference is in `config nic`. You must change the interface name to that of the secondary node.

```
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
```

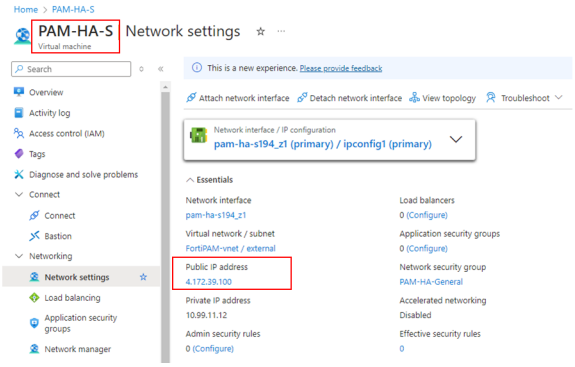
Accessing the GUI portal after the HA failover

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.



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.



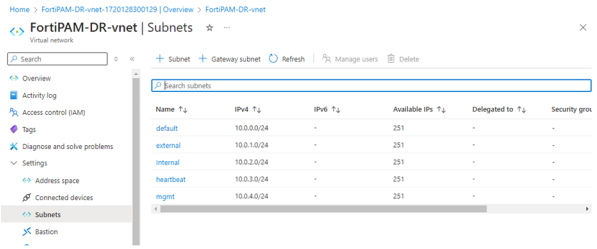
Adding a DR node

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*.



- 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.

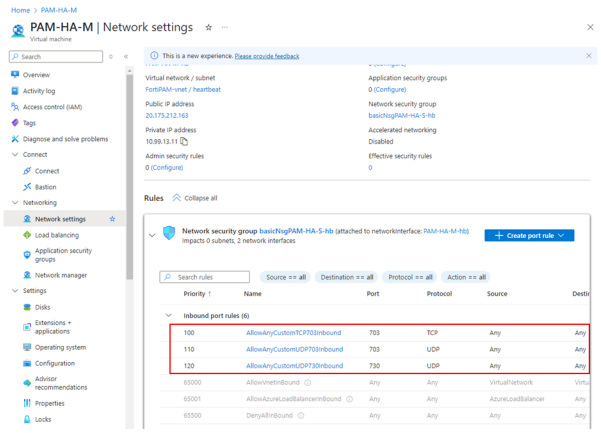
  The IP assignment for the HA nodes is shown below.

	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 518.
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:



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
  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:

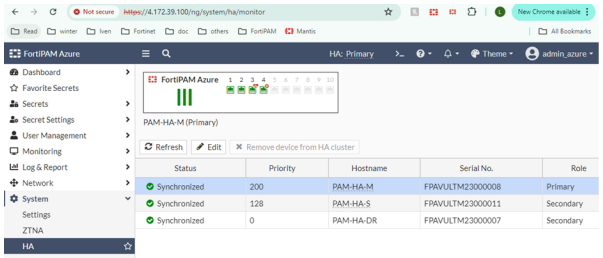
```
config system ha
 set group-name "Azure_PAM_HA"
 set mode active-passive
 set password ENC
 set hbdev "PORT3" 0
 set ha-mgmt-interfaces
 config ha-mgmt-interfaces
  edit 1
   set interface "port4"
   set gateway 10.0.4.1
  next
 end
```

```
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
```

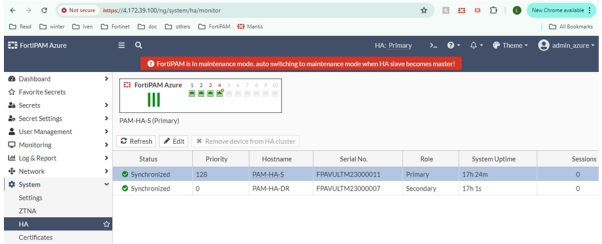
ix. Click *OK*.

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.

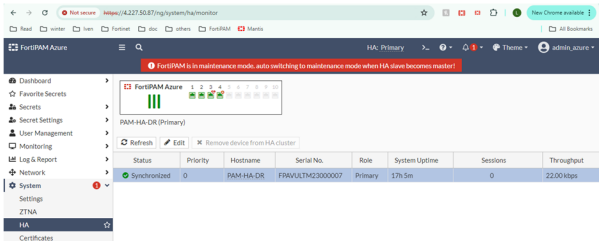


2. Shutdown the primary node.
   The secondary node becomes the active node.
3. Access the GUI portal using the same public IP address (`FPAM-HA-GUI-Portal: 4.172.39.100`) and verify that the original secondary node and the DR node are in sync.



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`).



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.

Appendix S: Installation on Alibaba Cloud

Alibaba Cloud does not support RAID under UEFI booting.

To deploy FortiPAM on Alibaba Cloud:

1. Creating a resource group on page 618
2. Creating a virtual private cloud on page 619
3. Creating a security group on page 621
4. Creating a RAM role on page 623
5. Creating a custom image on page 628
6. Creating a FortiPAM-VM instance on page 637
7. Connecting to the FortiPAM-VM on page 641

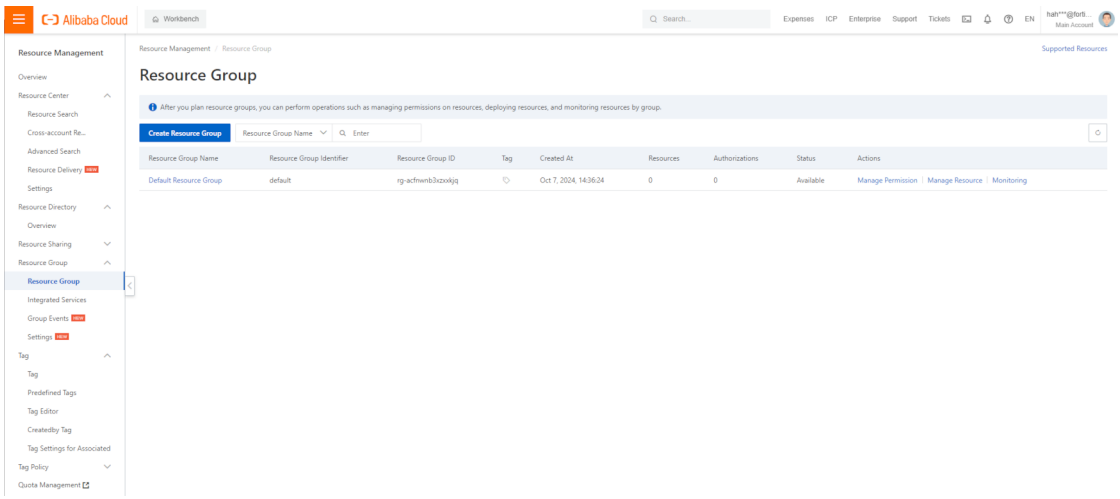
Creating a resource group

A resource group in Alibaba Cloud is a way to organize and manage cloud resources across multiple services and projects within an account. It allows users to group resources (like ECS instances, VPCs, EIPs, etc).

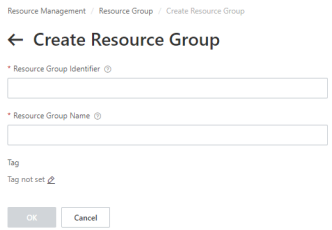
Therefore, it is strongly recommend that you create a resource group to include all the resources under it.

To create a resource group:

1. In the Alibaba Cloud console, from the search bar, look for *Resource Management*.
2. From the tree menu on the left, go to *Resource Group* > *Resource Group*.
   The *Resource Group* window opens.



3. Select *Create Resource Group*.
   The *Create Resource Group* wizard opens.

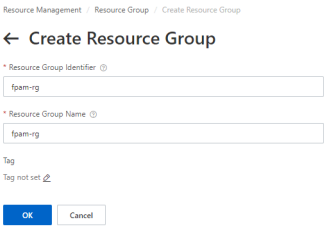


4. In *Resource Group Indentifier*, enter the resource group name.



The identifier cannot be changed once the resource group is created.

5. In *Resource Group Name*, enter the resource group name.
6. Click *OK*.

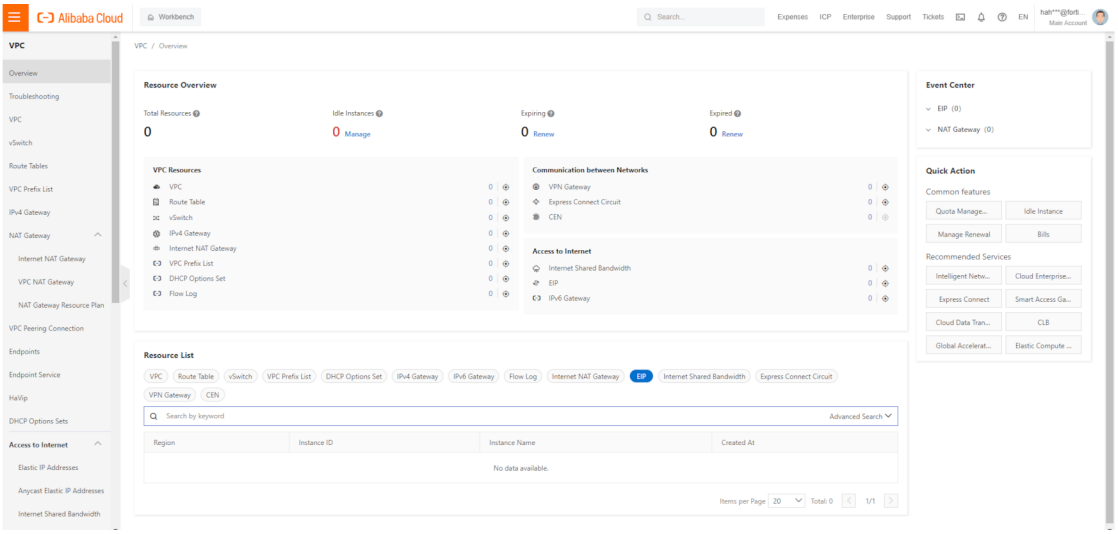


Creating a virtual private cloud

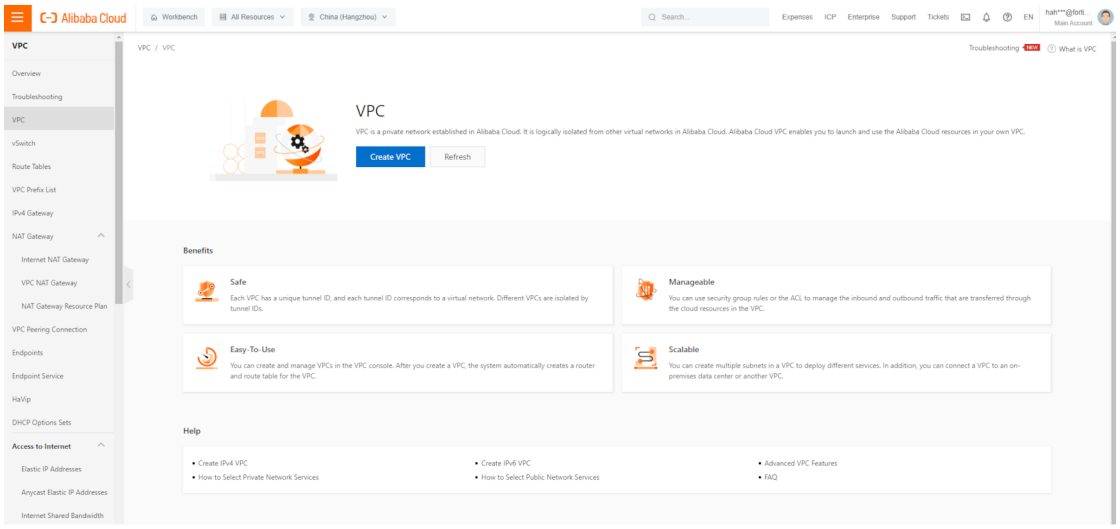
A Virtual Private Cloud (VPC) in Alibaba Cloud is a logically isolated network environment that allows users to define and control their network settings, including IP address ranges, subnets, and network gateway.

To create a virtual private cloud:

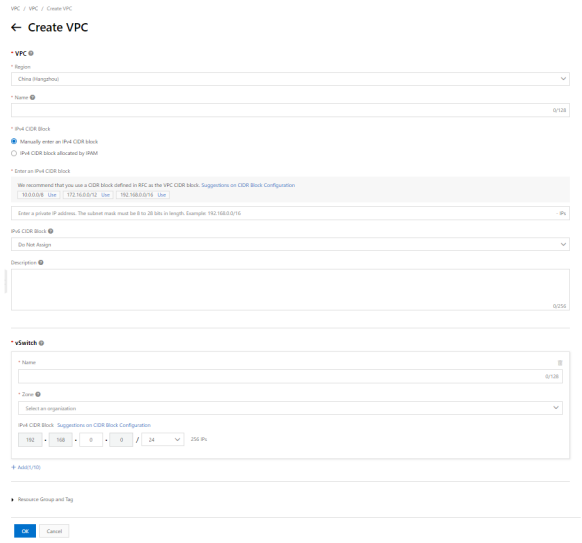
1. In the Alibaba Cloud console, from the search bar, look for Virtual Private Cloud.
   The VPC console opens in a new tab.



2. From the tree menu, go to *VPC*.



3. Select *Create VPC* to create a virtual private cloud.

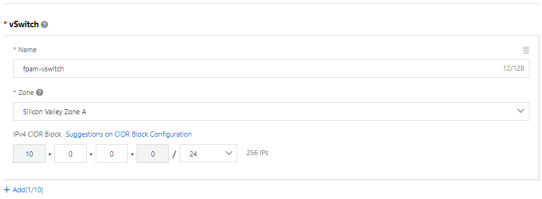


4. In *Region*, select a region where the FortiPAM-VM instance is located. In this example, *US (Silicon Valley)*.
5. In *Name*, enter a name for the VPC.
6. Keep the default value in *IPv4 CIDR Block*, i.e., *Manually enter an IPv4 CIDR block*.
7. In *Enter an IPv4 CIDR block*, enter `10.0.0.0/8`.
8. Keep the default value in IPv6 CIDR Block, i.e., *Do Not Assign*.
9. Optionally, enter a description.
10. In *vSwitch*:



A vSwitch is a basic network component of a VPC.

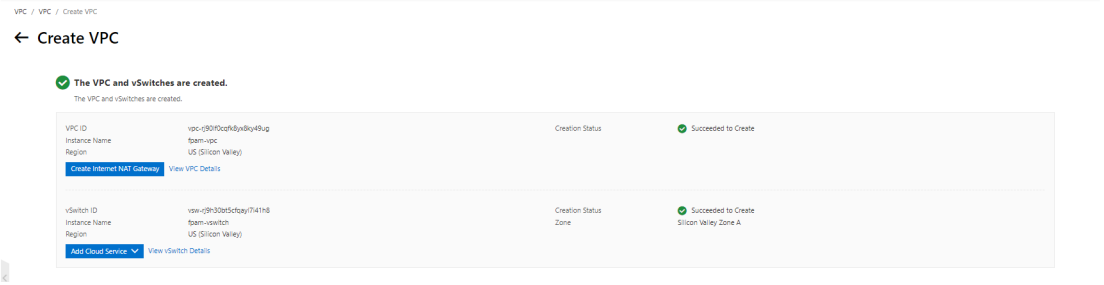
a. In *Name*, enter a name for the vSwitch.
b. In *Zone*, select a zone.



11. In *Resource Group and Tag*:
    a. In *Resource Group*, select the resource group created in Creating a resource group on page 618.
    The *Architecture Preview* appears on the right.



12. Click *OK*.
    The VPC and vSwitch is created.



Creating a security group

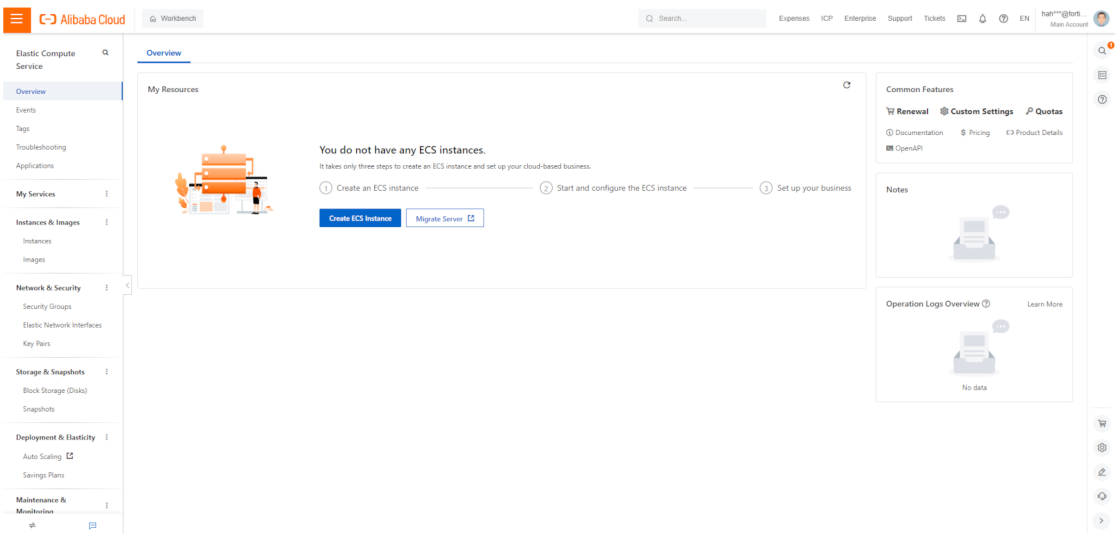
A security group is a set of firewall rules that control the traffic for your VM instances.

When you create a VPC, a default security group protects instances in it.

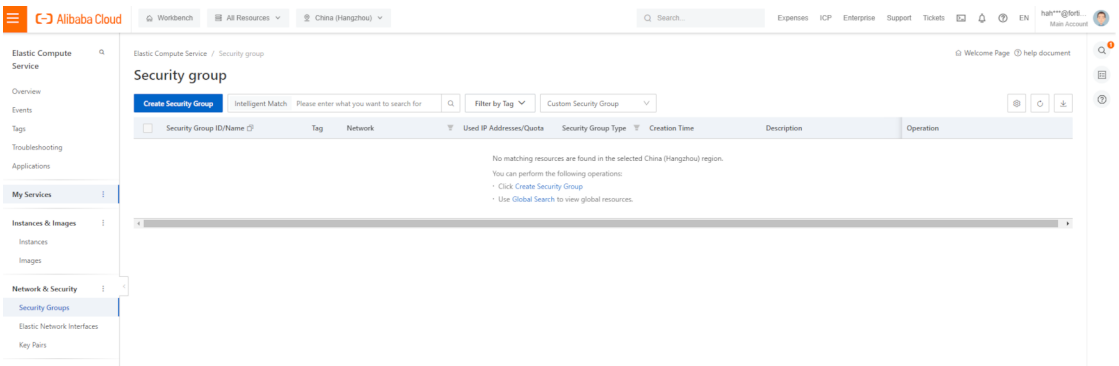
It is recommended to add inbound rules so that the traffic will be allowed to flow on the specified ports.

To create a security group:

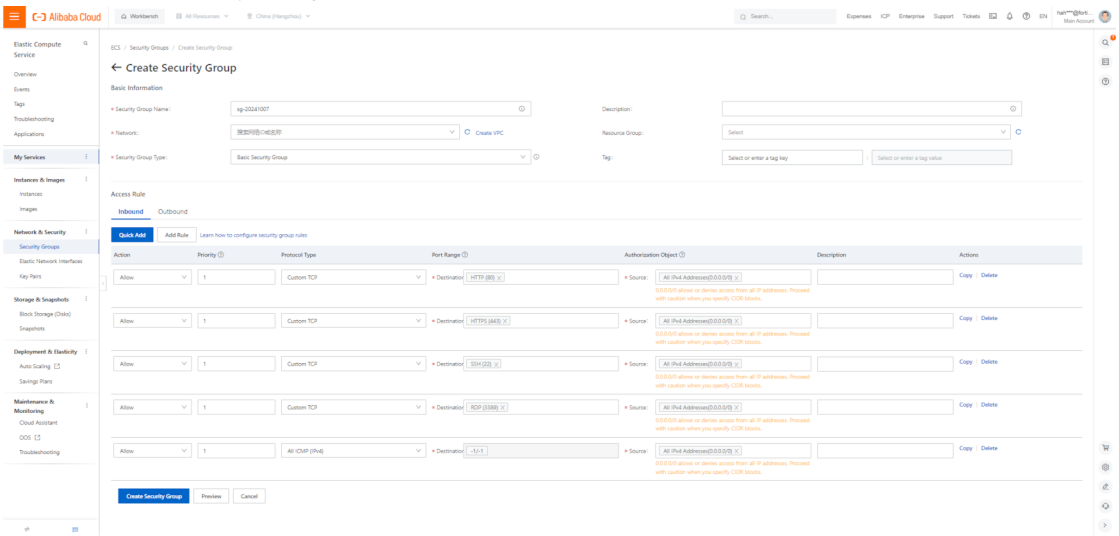
1. In the Alibaba Cloud console, from the search bar, look for *Elastic Compute Service*.
   The *Elastic Compute Service* opens in a new tab.



2. Go to *Network & Security* > *Security Groups*.
   The *Security group* window opens.



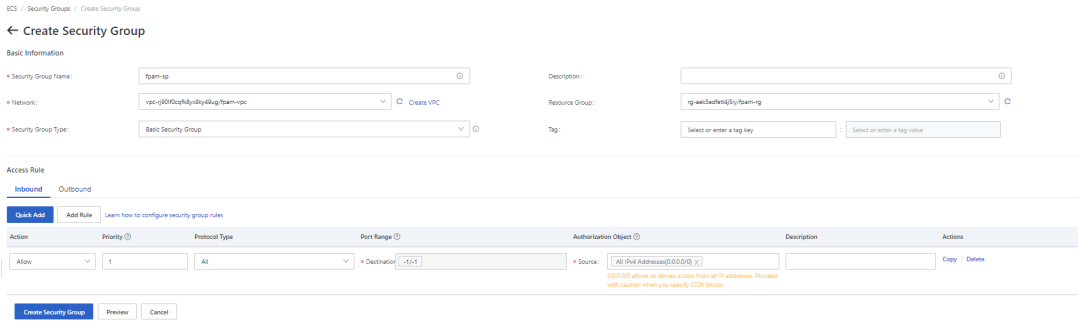
3. Select *Create Security Group*.



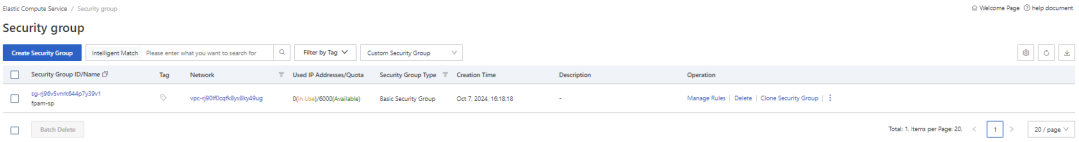
4. In *Basic Information*:
   a. In *Security Group Name*, enter a name for the security group.
   b. In *Network*, select the VPC created in Creating a virtual private cloud on page 619.

c. In *Security Group Type*, select either *Basic Security Group* or *Advanced Security Group*.
d. Optionally, in *Description*, enter a description.
e. In *Resource Group*, select the resource group created in Creating a resource group on page 618.

5. In *Access Rule*:
We manually configure rules to inbound and outbound traffic.
   a. In the *Inbound* tab:
   We manually add rules to allow ports according to your needs. See FortiPAM Ports.
   b. In the *Outbound* tab:
   By default, security groups allow all outbound traffic.
   ECS instances in a security group are allowed to access external networks.
   c. In this example, we allow all the inbound and outbound traffic:



6. Select *Create Security Group* to create the security group.



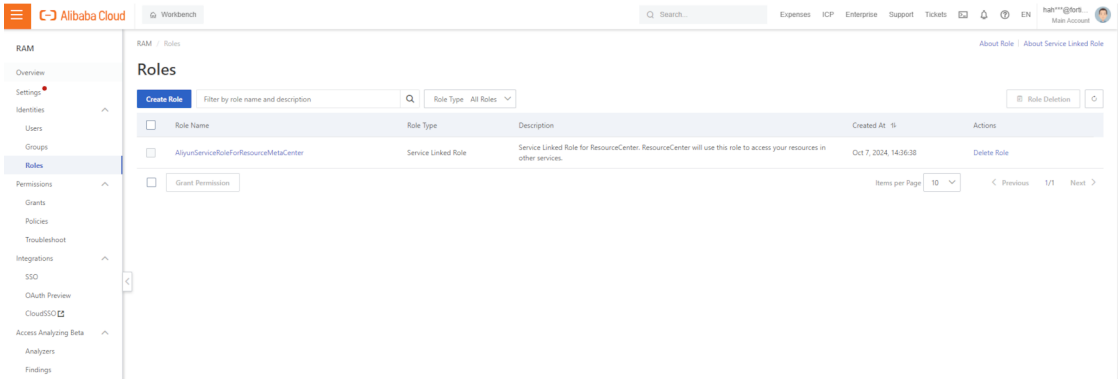
Creating a RAM role

The RAM role allows you to delegate specific permissions or access rights to Alibaba Cloud resources without needing to share your primary account credentials.

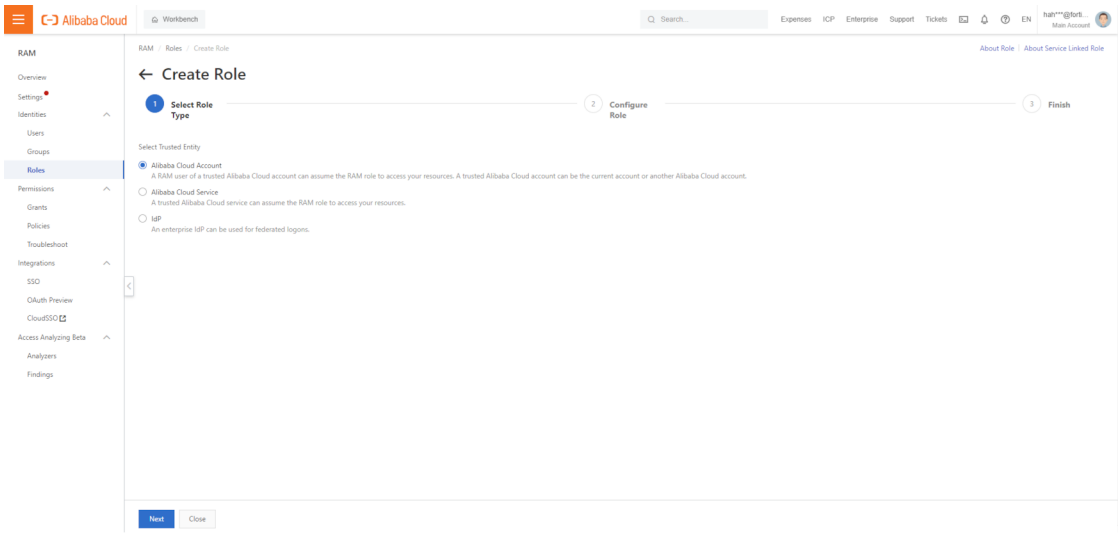
A RAM role is used primarily to improve security, simplify management, and allow fine-grained control over access to your resources. It is the most important part in both deploying standalone and HA mode.

To create a RAM group:

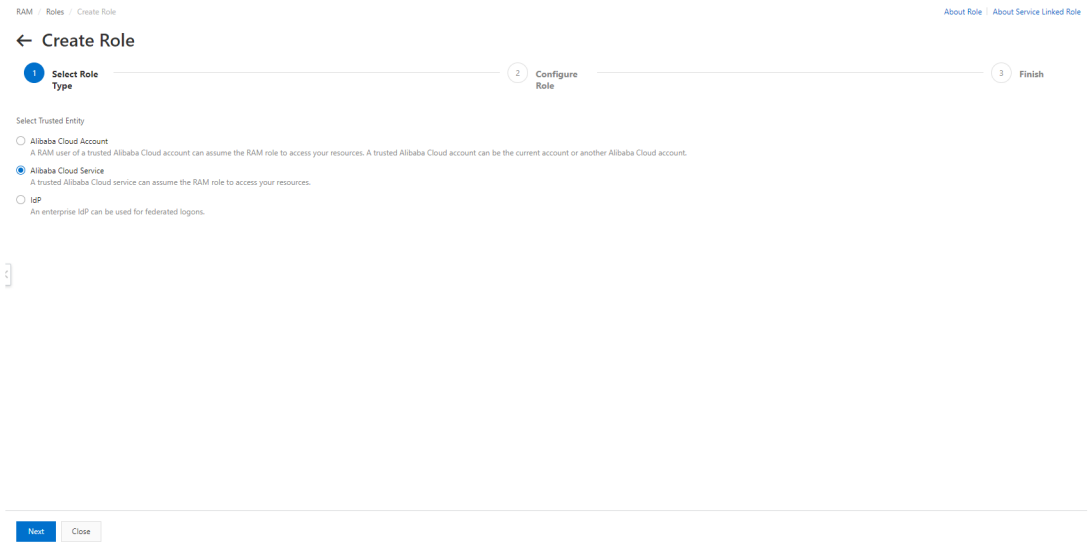
1. In the Alibaba Cloud console, from the search bar, look for *Resource Access Management*.
2. From the tree menu on the left, go to *Identities* > *Roles*.



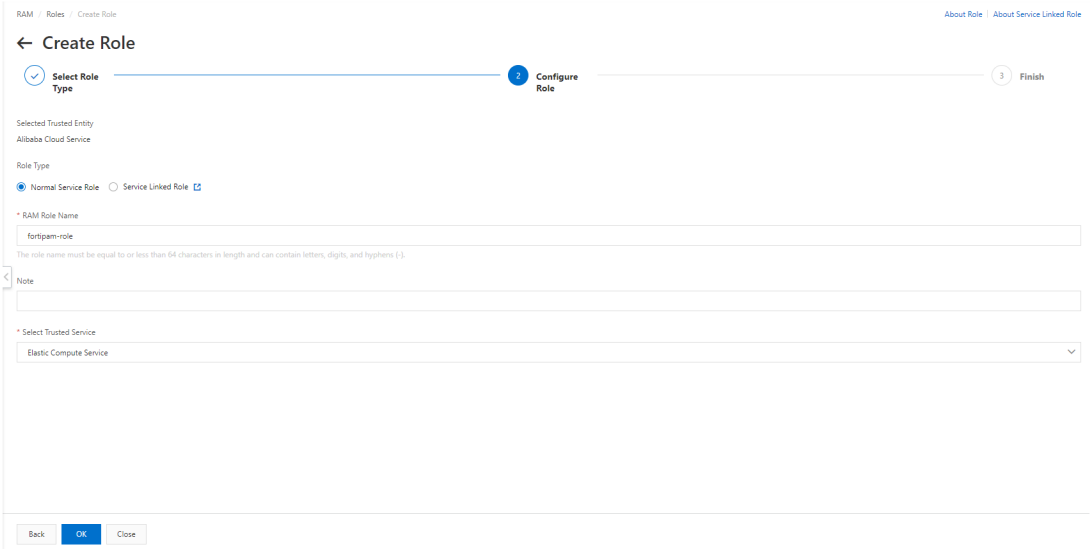
3. Select *Create Role*.
   The *Create Role* wizard opens.



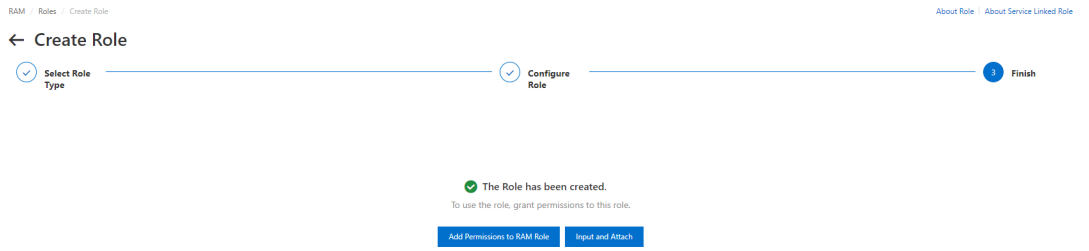
4. In Select *Trusted Entity*, select *Alibaba Cloud Service*, and click *Next*.



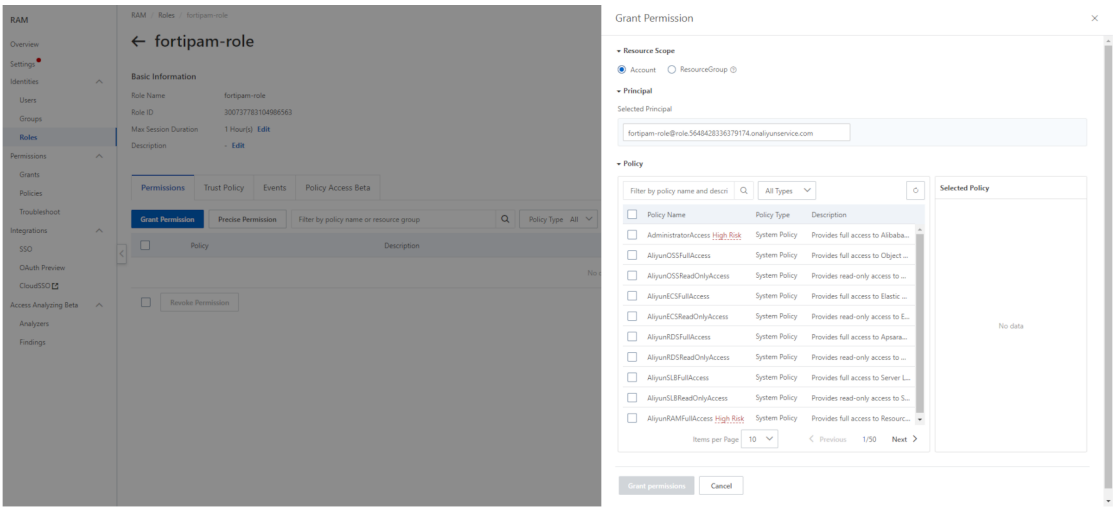
5. In *Configure Role* tab:
   a. In *Role Type*, select *Normal Service Role*.
   b. In *RAM Role Name*, enter the role name.
   c. Optionally, enter a note.
   d. In *Select Trusted Service*, select *Elastic Computer Service*.
6. Click *OK*.



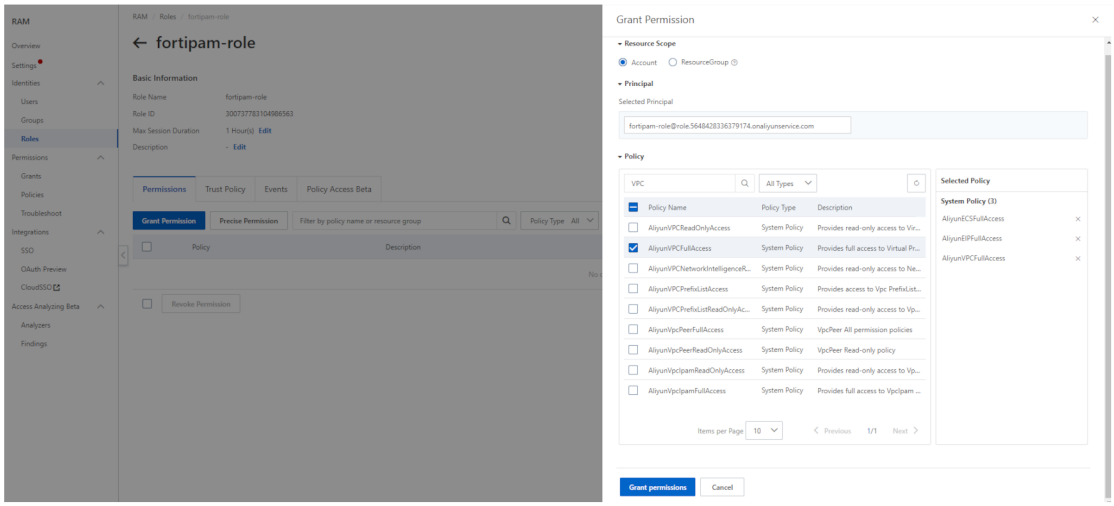
The role was created.



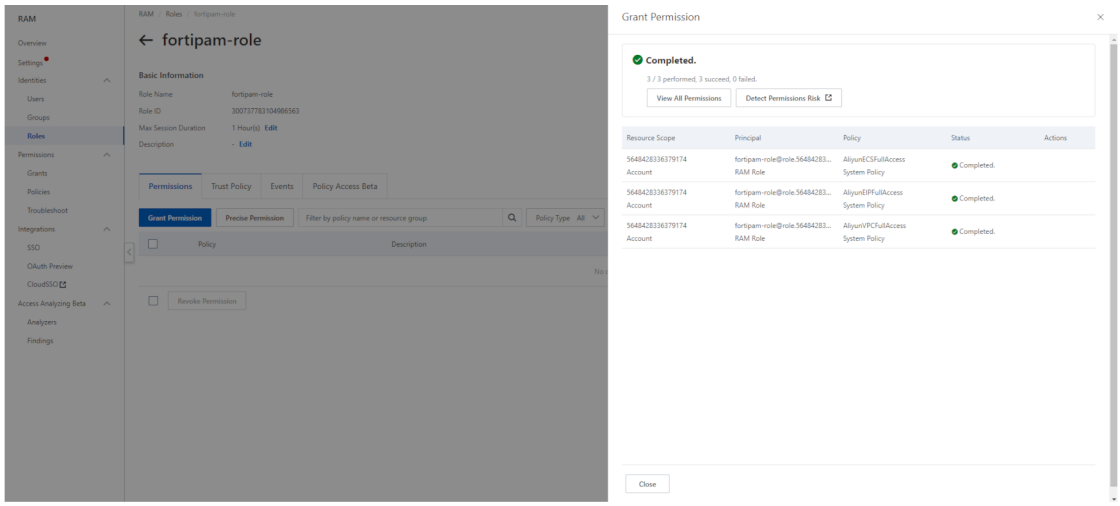
7. We now grant related permissions to the recently created role:
   a. Select *Add Permission to RAM Role*.
      A new window opens.
   b. Select *Grant Permission*.
      The *Grant Permission* window opens.

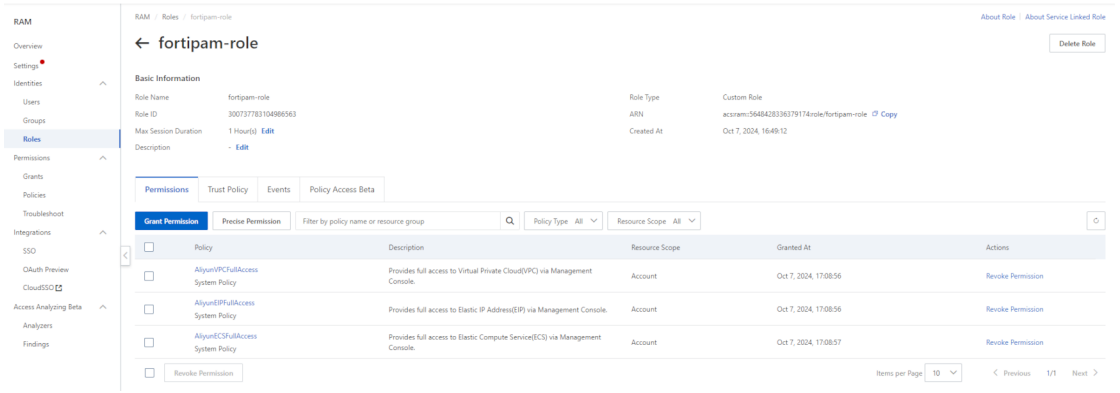


   c. From the grant permission window, select *AliyunECSFullAccess*, *AliyunEIPFullAccess*, and *AliyunVPCFullAccess* policies.



d. Select *Grant permissions*.





Note: The actual role configurations may differ depending on your environment. Check with your organization's public cloud administrator for information.

In case the HA does not work, create a new RAM rule :

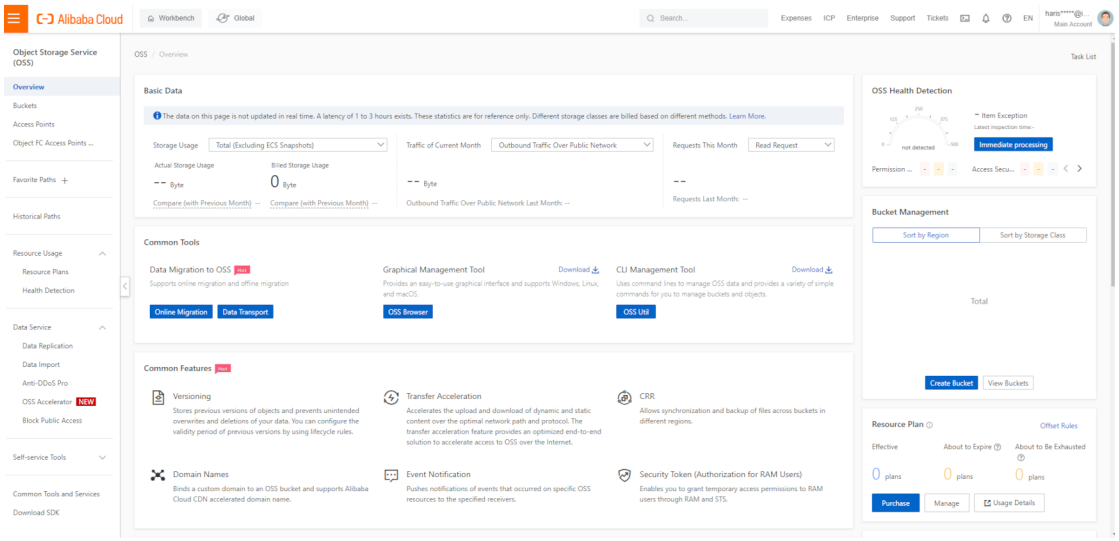
```
{
 "Version":"1",
 "Statement:" [
  {
   "Effect":"Allow"
      "Action": [
        "ecs:DescribeInstances",
        "vpc:DescribeEipAddresses",
        "vpc:DescribeVpcAttribute",
        "vpc:DescribePublishedRouteEntries",
        "vpc:DescribeRouteTables",
        "vpc:AssociateEipAddress",
        "vpc:UnassociateEipAddress",
        "vpc:ReleaseEipAddress",
        "vpc:PublishRouteEntries",
        "vpc:CreateRouteEntry",
        "vpc:DeleteRouteEntry",
        "vpc:ConvertNatPublicIpToEip",
        "ecs:AddTags"
      ],
```

```
            "Resource": "*"
        }
    ]
}
```

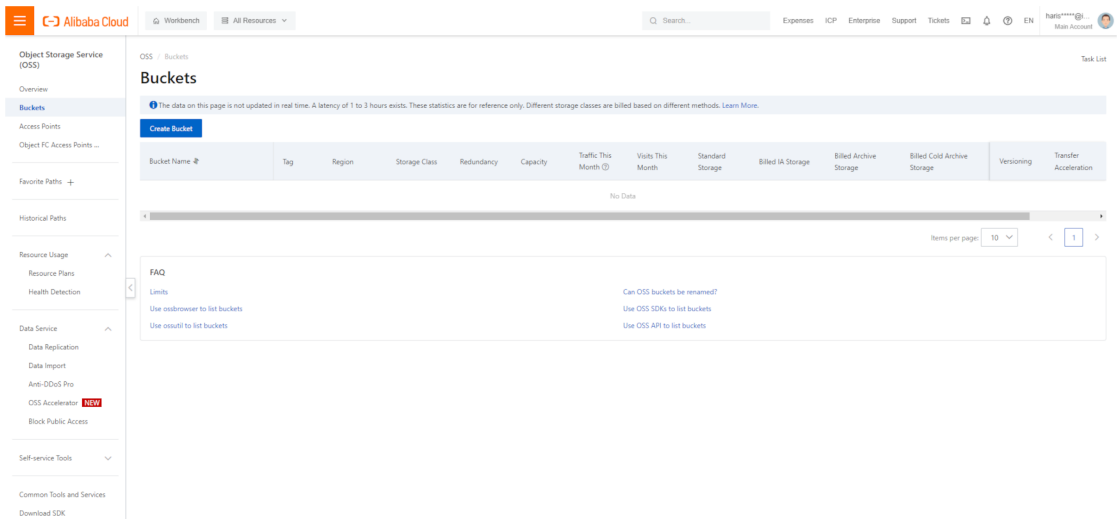
Creating a custom image

To create a custom image:

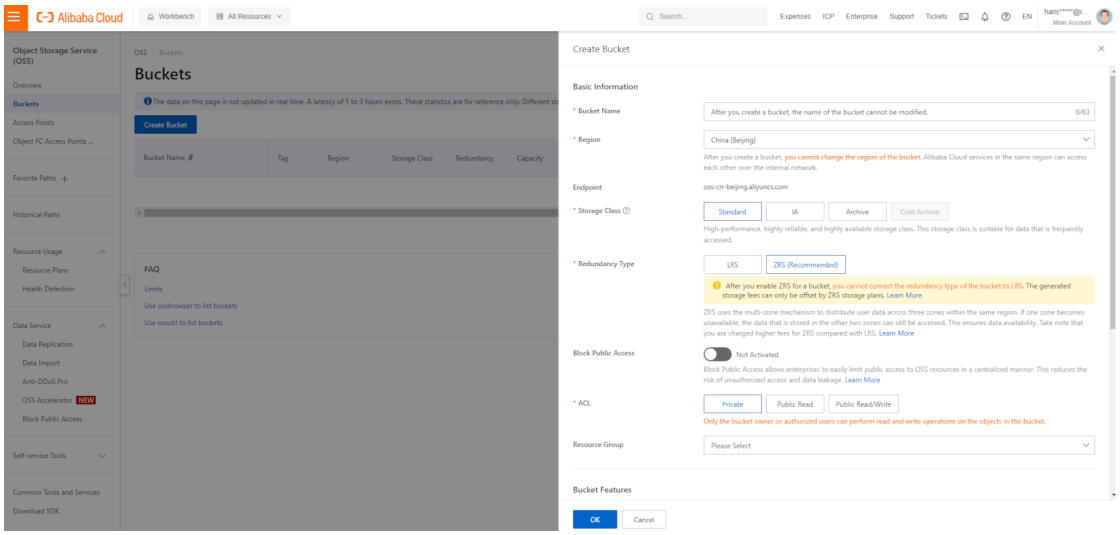
1. Download the FortiPAM image from FortiCloud.
   a. Go to *Support* > *Downloads*, and select *Firmware Download* from the dropdown list.
   The *Firmware Images* page opens.
   b. In the *Firmware Images* page, select *FortiPAM.*
   c. On the *Download* tab, browse to the appropriate directory in the FTP site for the version that you would like to download.
   d. Download the `FPA_KVM_ALI-vxxx.F-buildxxxx-FORTINET.out.kvm.zip` file and *FortiPAM Release Notes*, save these files to your management computer.
   e. Select the `.zip` file on your management computer and extract the files to a new file folder.
2. Upload the FortiPAM image to Alibaba Cloud:
   a. In the Alibaba Cloud console, from the search bar, look for *Object Storage Service*.
   The *Object Storage Service* window opens as a new tab.



b. From the tree menu, go to *Buckets*.



c. Select *Create Bucket*.



d. In *Bucket Name*, enter a bucket name.

e. In *Region*, select region where the FortiPAM instance will be deployed.

f. In *Storage Class*, select *Standard*.

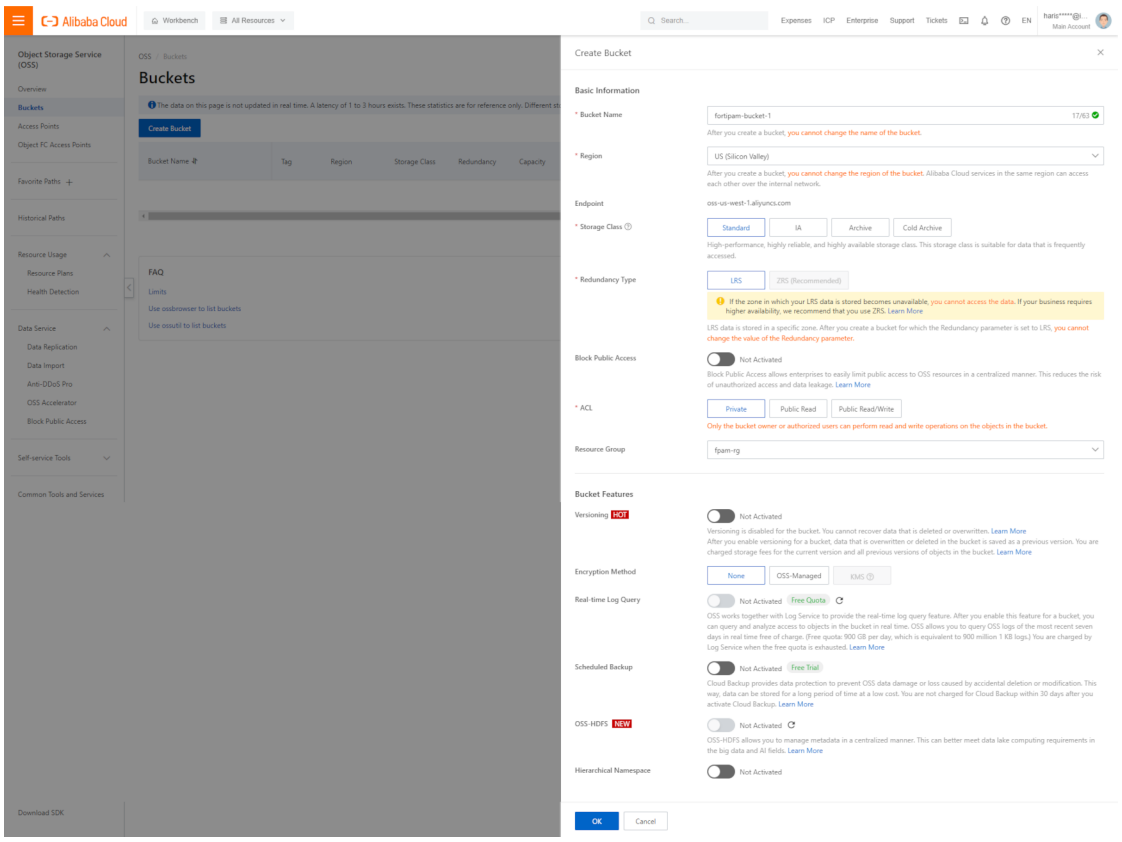
g. In *Redundancy Type*, select *LRS*.

h. In *ACL*, select *Private*.

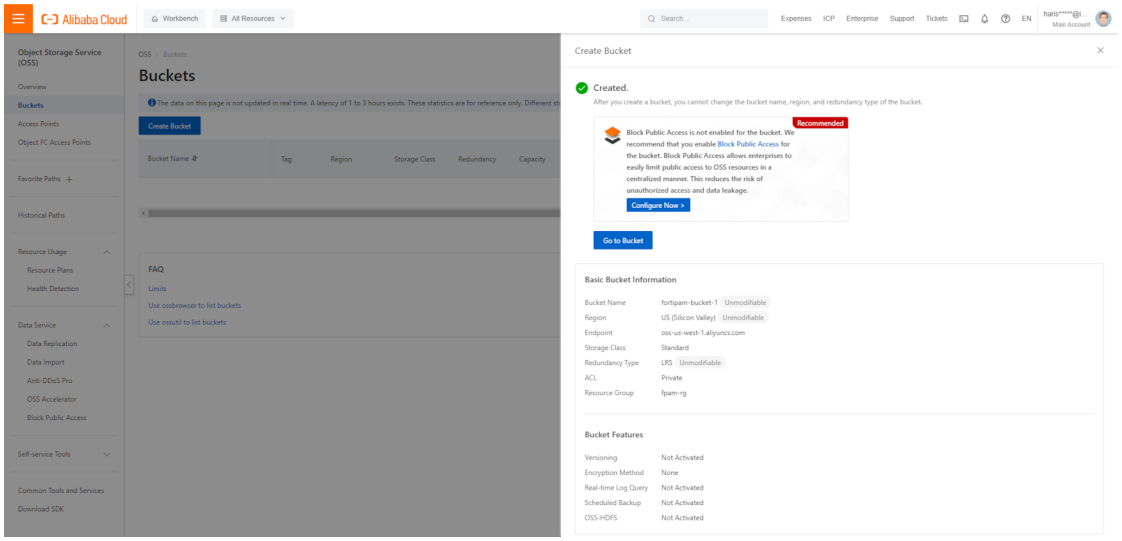
i. In *Resource Group*, select the resource group created in Creating a resource group on page 618.

j. Keep the default value in *Bucket Features* pane.

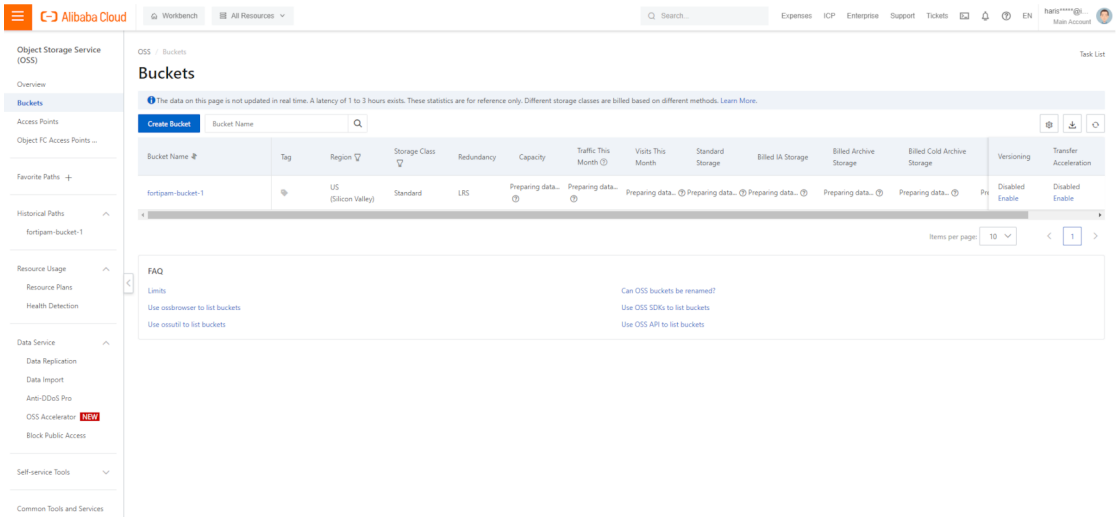
k. Click *OK*.



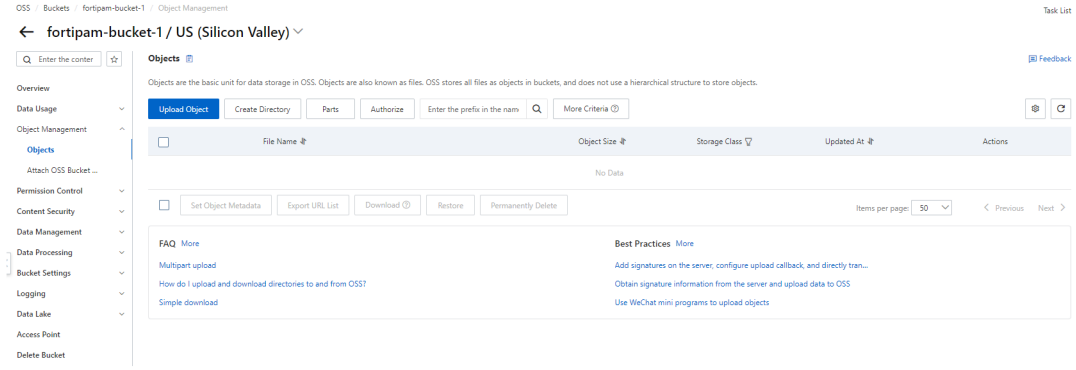
The bucket is created.



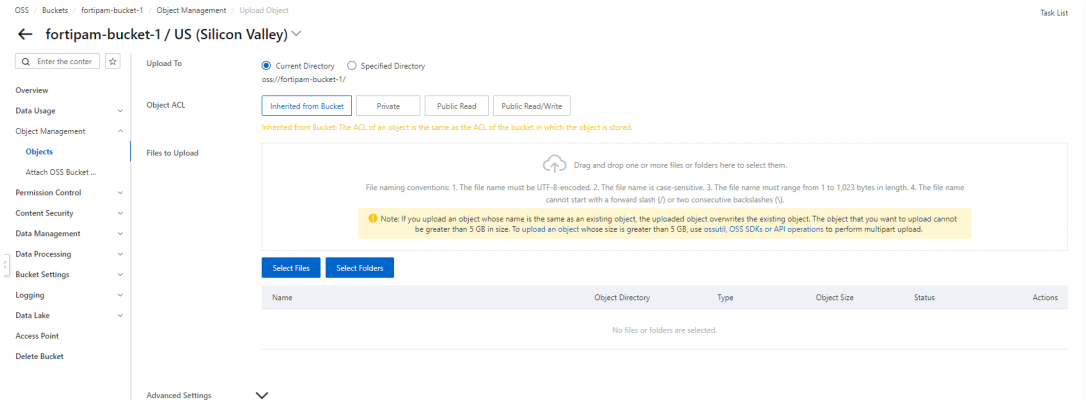
l. In *Object Storage Service*, go to *Buckets*.



m. Select the recently created bucket to open it.

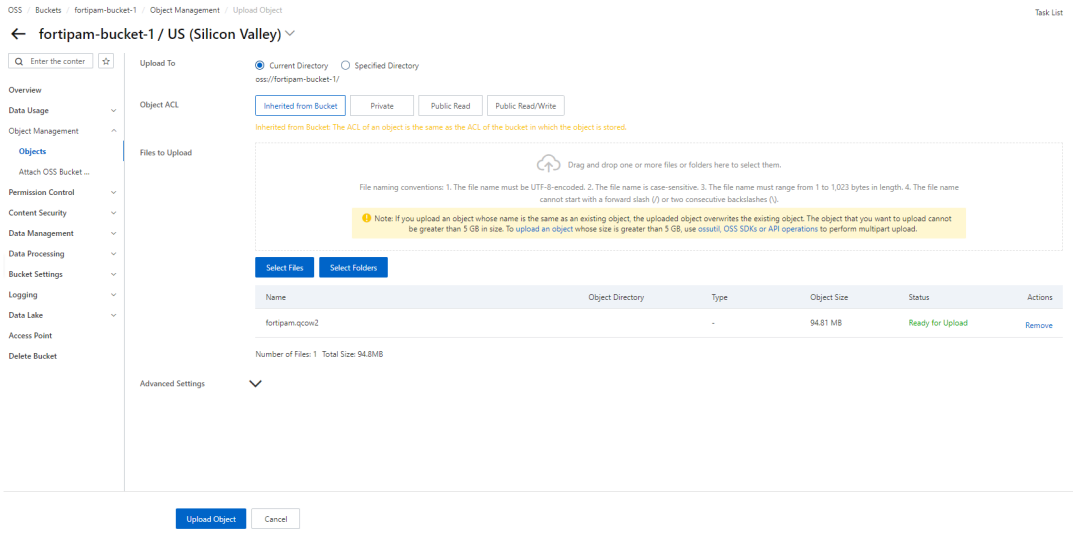


n. Select *Upload Object*.



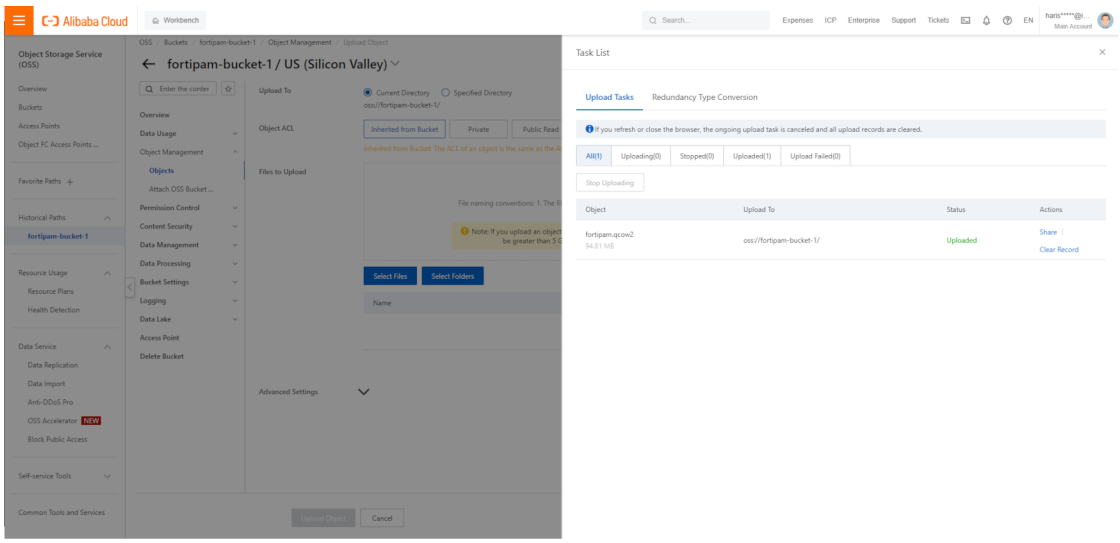
o. Ensure that *Upload To* is *Current Directory*.

p. Drag and drop the `fortipam.qcow2` file to *Files to Upload* from your management computer.



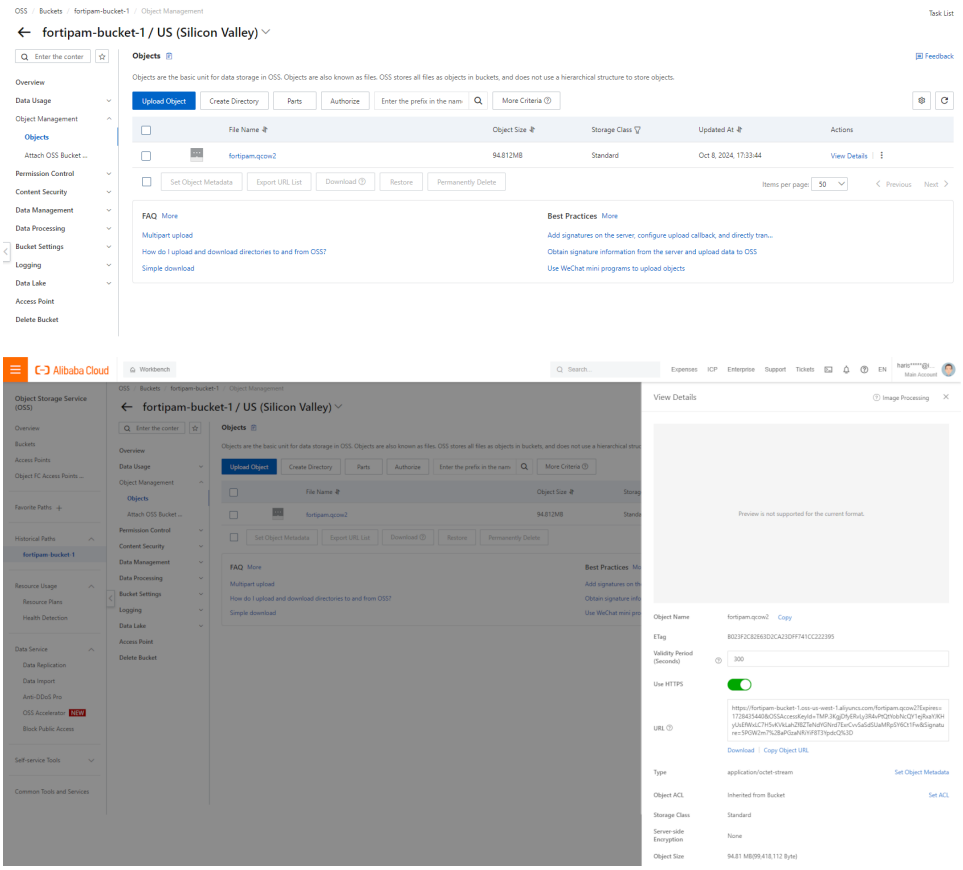
q. Click *Upload Object*.
The image is uploaded to the bucket.

Click *Share* to copy the URL link when creating a custom image.
You can save this URL on your management computer.

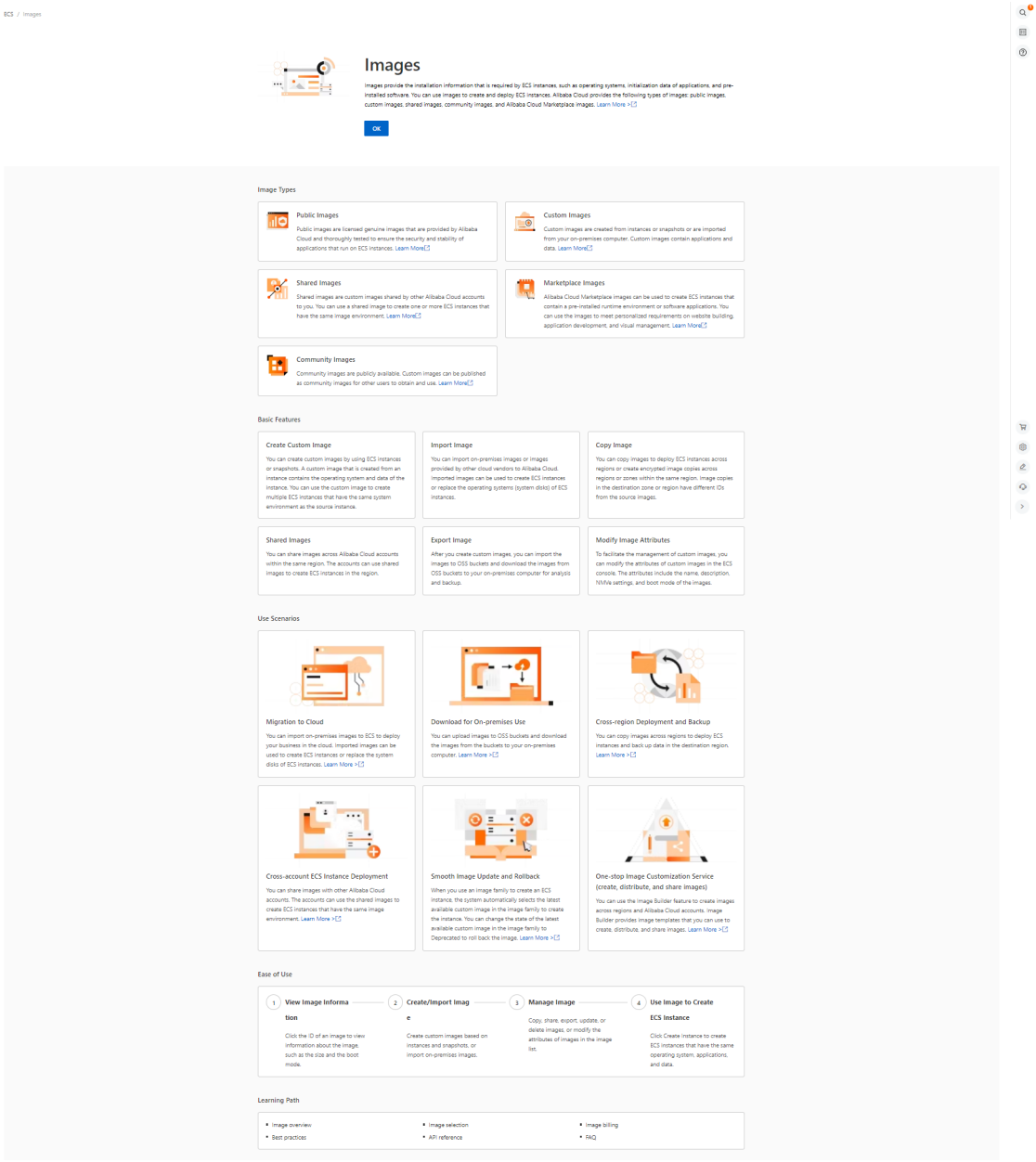


Alternatively, from the bucket, select *View Details* and copy the URL by clicking *Copy Object URL*.

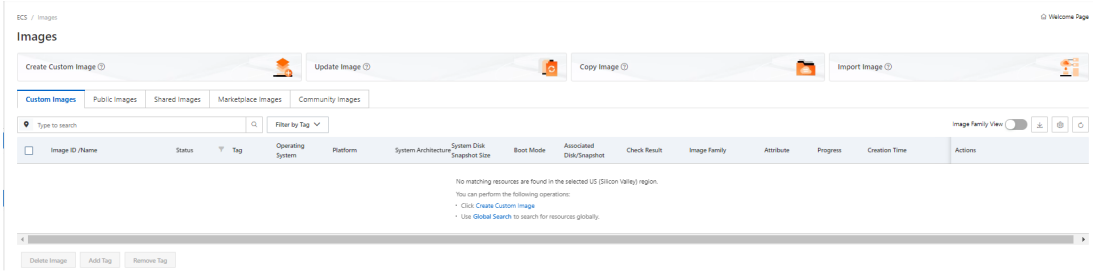
You can save this URL on your management computer.



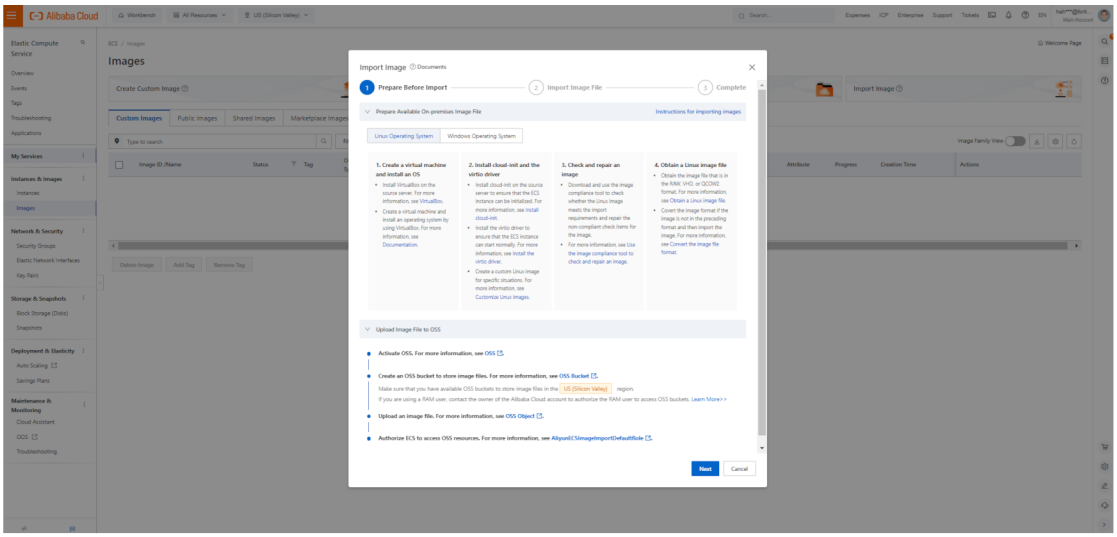
3. Create the custom image:
   a. In the Alibaba Cloud console, from the search bar, look for *Elastic Compute Service*.
   b. Go to *Instances & Images* > *Images*.
      The *Images* window opens.


ECS / Images
Images
Images provide the installation information that is required by ECS instances, such as operating systems, initialization data of applications, and pre-installed software. You can use images to create and deploy ECS instances. Alibaba Cloud provides the following types of images: public images, custom images, shared images, community images, and Alibaba Cloud Marketplace images. Learn More >
OK
Image Types
Public Images
Public images are licensed genuine images that are provided by Alibaba Cloud and thoroughly tested to ensure the security and stability of applications that run on ECS instances. Learn More
Custom Images
Custom images are created from instances or snapshots or are imported from your on-premises computer. Custom images contain applications and data. Learn More
Shared Images
Shared images are custom images shared by other Alibaba Cloud accounts to you. You can use a shared image to create one or more ECS instances that have the same image environment. Learn More
Marketplace Images
Alibaba Cloud Marketplace images can be used to create ECS instances that contain a pre-installed runtime environment or software applications. You can use the images to meet personalized requirements on website building, application development, and visual management. Learn More
Community Images
Community images are publicly available. Custom images can be published as community images for other users to obtain and use. Learn More
Basic Features
Create Custom Image
You can create custom images by using ECS instances or snapshots. A custom image that is created from an instance contains the operating system and data of the instance. You can use the custom image to create multiple ECS instances that have the same system environment as the source instance.
Import Image
You can import on-premises images or images provided by other cloud vendors to Alibaba Cloud. Imported images can be used to create ECS instances or replace the operating systems (system disks) of ECS instances.
Copy Image
You can copy images to deploy ECS instances across regions or create encrypted image copies across regions or zones within the same region. Image copies in the destination zone or region have different IDs from the source images.
Shared Images
You can share images across Alibaba Cloud accounts within the same region. The accounts can use shared images to create ECS instances in the region.
Export Image
After you create custom images, you can import the images to OSS buckets and download the images from OSS buckets to your on-premises computer for analysis and backup.
Modify Image Attributes
To facilitate the management of custom images, you can modify the attributes of custom images in the ECS console. The attributes include the name, description, NMVe settings, and boot mode of the images.
Use Scenarios
Migration to Cloud
You can import on-premises images to ECS to deploy your business in the cloud. Imported images can be used to create ECS instances or replace the system disks of ECS instances. Learn More >
Download for On-premises Use
You can upload images to OSS buckets and download the images from the buckets to your on-premises computer. Learn More >
Cross-region Deployment and Backup
You can copy images across regions to deploy ECS instances and back up data in the destination region. Learn More >
Cross-account ECS Instance Deployment
You can share images with other Alibaba Cloud accounts. The accounts can use the shared images to create ECS instances that have the same image environment. Learn More >
Smooth Image Update and Rollback
When you use an image family to create an ECS instance, the system automatically selects the latest available custom image in the image family to create the instance. You can change the state of the latest available custom image in the image family to Deprecated to roll back the image. Learn More >
One-stop Image Customization Service (create, distribute, and share images)
You can use the Image Builder feature to create images across regions and Alibaba Cloud accounts. Image Builder provides image templates that you can use to create, distribute, and share images. Learn More >
Ease of Use
1 View Image Information
Click the ID of an image to view information about the image, such as the size and the boot mode.
2 Create/Import Image
Create custom images based on instances and snapshots, or import on-premises images.
3 Manage Image
Copy, share, export, update, or delete images, or modify the attributes of images in the image list.
4 Use Image to Create ECS Instance
Click Create Instance to create ECS instances that have the same operating system, applications, and data.
Learning Path
Image overview
Best practices
Image selection
API reference
Image billing
FAQ

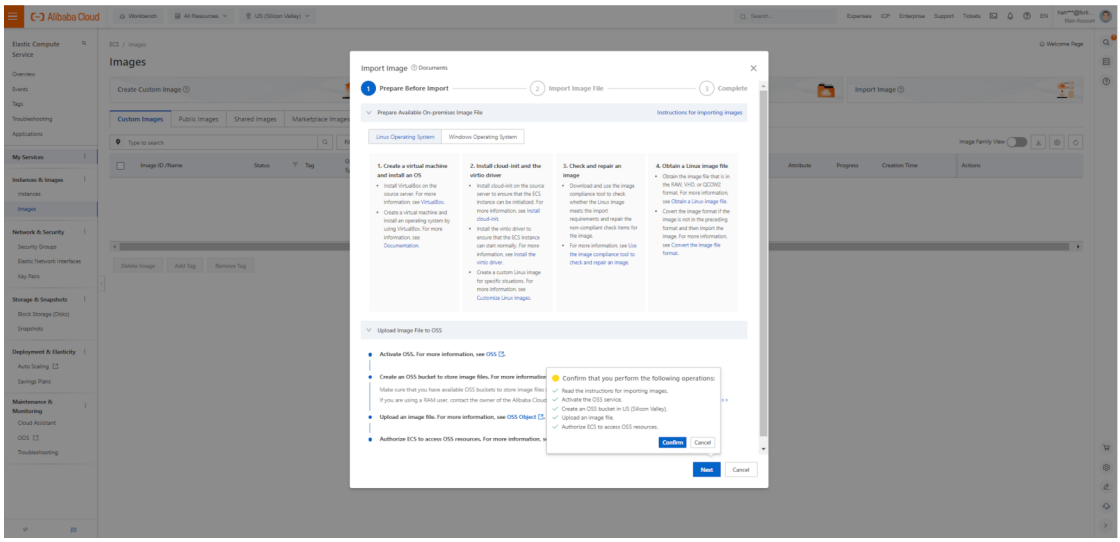
c. Click *OK*.


ECS / Images
Welcome Page
Images
Create Custom Image
Update Image
Copy Image
Import Image
Custom Images
Public Images
Shared Images
Marketplace Images
Community Images
Type to search
Filter by Tag
Image Family View
Image ID /Name
Status
Tag
Operating System
Platform
System Architecture
System Disk Snapshot Size
Boot Mode
Associated Disk/Snapshot
Check Result
Image Family
Attribute
Progress
Creation Time
Actions
No matching resources are found in the selected US (Silicon Valley) region.
You can perform the following operations:
Click Create Custom Image
Use Global Search to search for resources globally.
Delete Image
Add Tag
Remove Tag

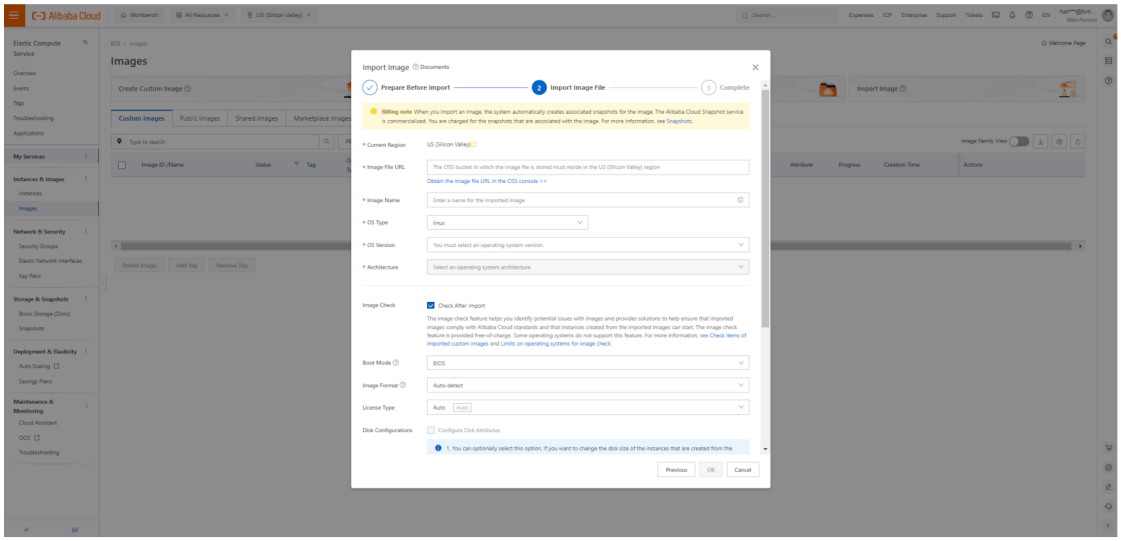
d. From *Import Image*, select *Import Image*, and click *Next*.



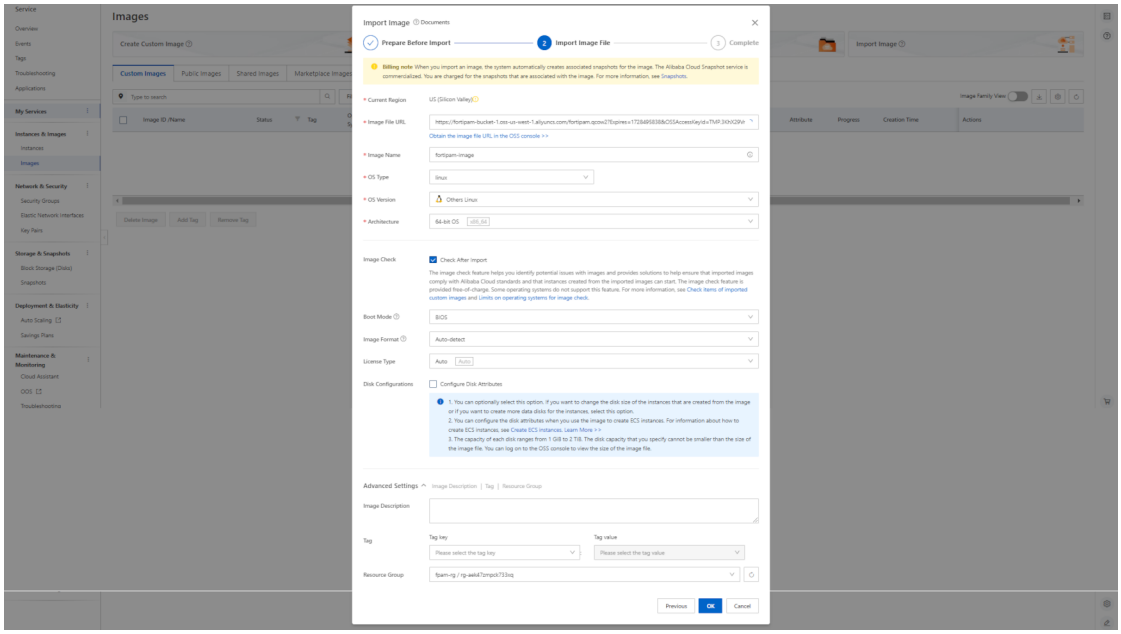
e. Click *Confirm*.



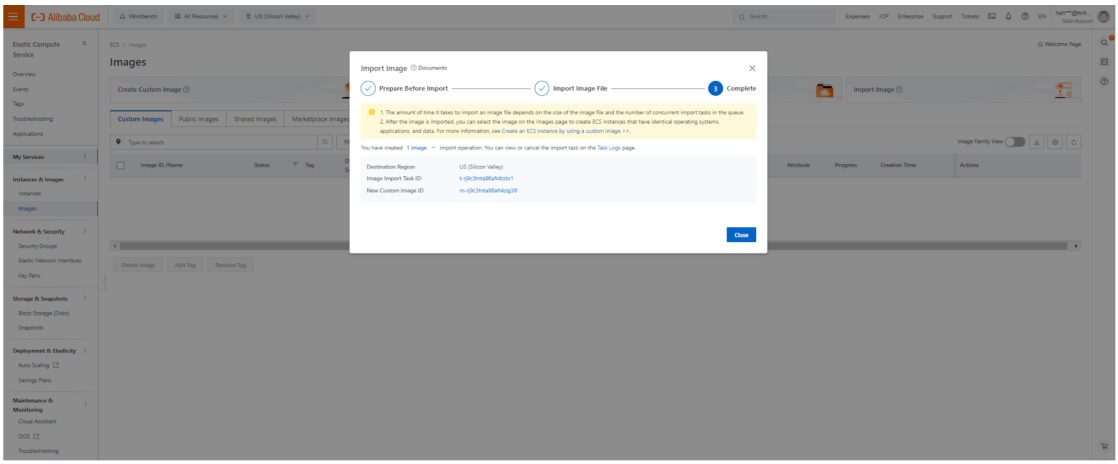
The *Import Image* wizard opens.



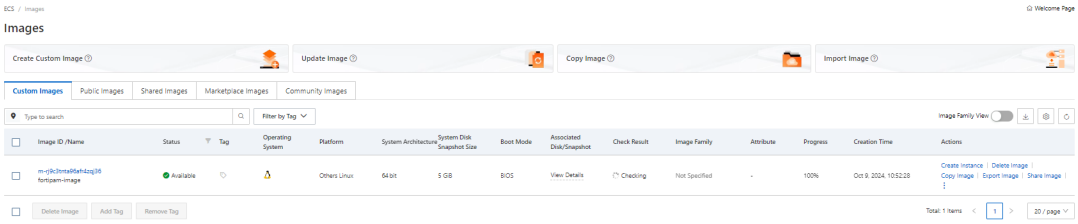
4. In the *Import Image* file tab:
   a. In *Image File URL*, paste the image file URL that you saved in Copy the URL.
   b. In *Image Name*,enter the image name.
   c. In *OS Type*, select *linux*.
   d. In *OS Version*, select *Others Linux*.
   e. In *Architecture*, select *64-bit OS (x86_64)*.
   f. In *Boot Mode*, select *BIOS*.
   g. In *Advanced Settings*, in *Resource Group*, select the resource group created in Creating a resource group on page 618.
5. Click *OK*.



The image is created.



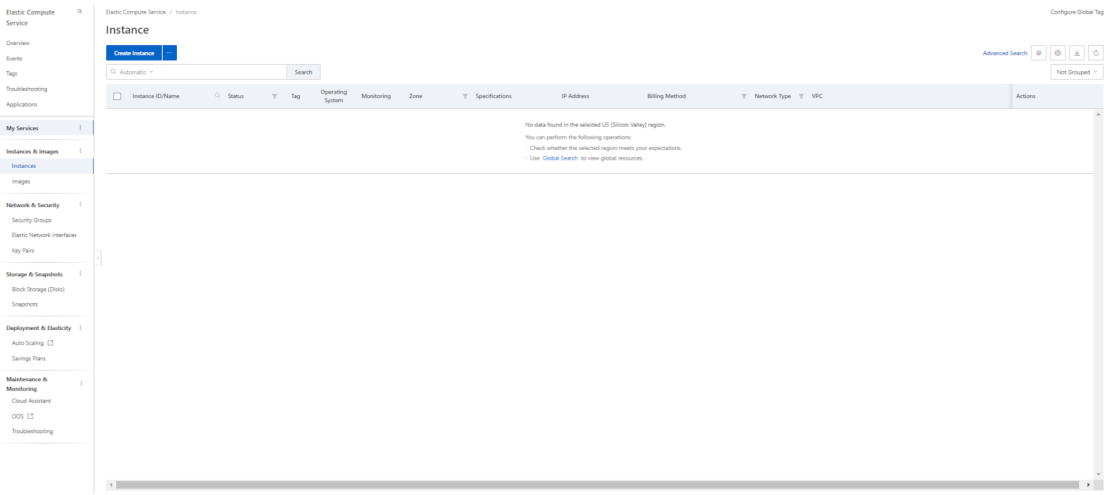
6. Click *Close*.
   The image is listed on the *Custom Images* tab.



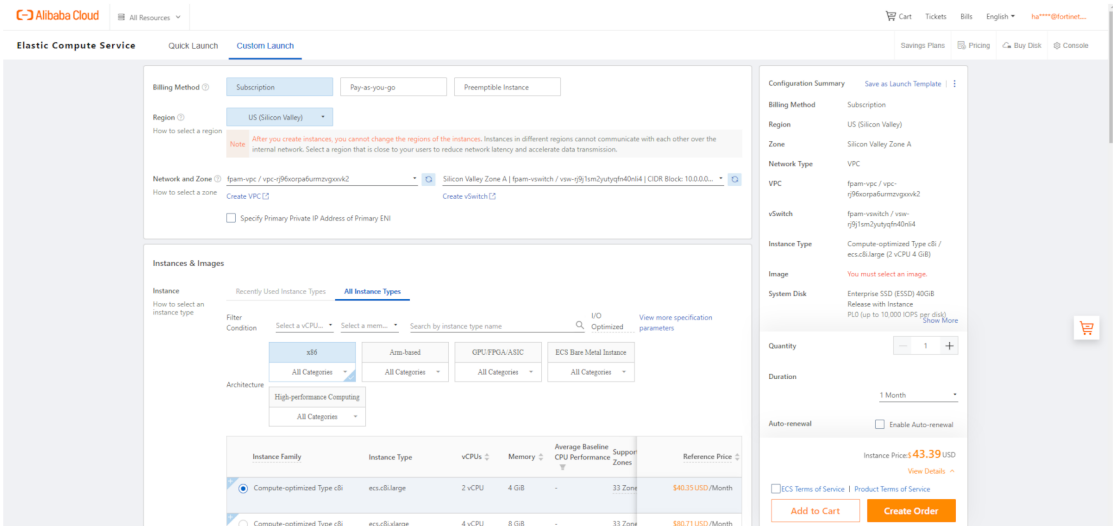
Creating a FortiPAM-VM instance

To create a FortiPAM-VM instance:

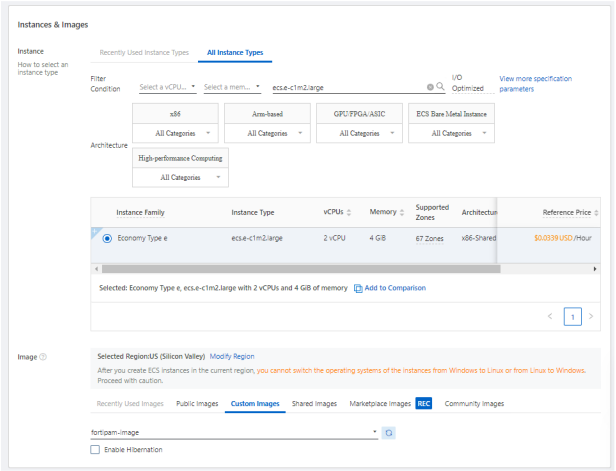
1. In the Alibaba Cloud console, from the search bar, look for *Elastic Compute Service*.
2. Go to *Instances & Images* > *Instances*.



3. Select *Create Instance*.
   A new window opens.



4. From the *All Resources* dropdown on the top-left, select the resource group created in Creating a resource group on page 618.
   Settings including VPC, security group, etc, are configured automatically based on the selected resource group.
5. In *Billing Method*, select *Pay-as-you-go*.
6. In *Region*, select the same region where the VPC and vSwitch is located.
7. Select *Specify Primary Private IP Address of Primary ENI*.
8. In the *Instances & Images* pane:
   a. In *Instance*, select an instance type based on the System requirements. In this example, `ecs.e-c1m2.large`. See Overview of ECS instance families.
   b. In *Image*, select *Custom Images*.
   c. From the *Select a custom image* dropdown, select FortiPAM image imported in Creating a custom image on page 628.



9. In the *Storage* pane:
   We require three storage units in total.

   One for the general system (minimum 2 GB).

   minimum The other two for storing logs and videos (minimum 10 GB each).
   See System requirements.
   a. From *Category*, select *Enterprise SSD (ESSD)*.

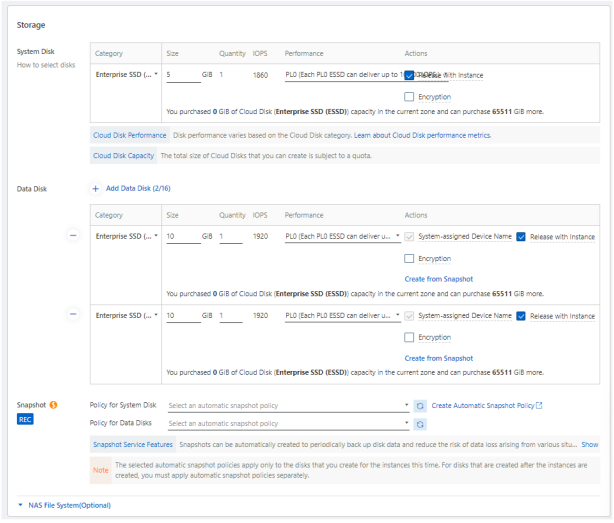
b. In *Size*, enter `5` (GB).
Note: Select standard or enterprise SSD, or and other desired disk type based on the FortiPAM instance needs and specify a desired storage size.

c. Select *Add Data Disk*:

i. In *Size*, enter `10` (GB).

d. Select *Add Data Disk*:

i. In *Size*, enter `10` GB.



10. In *Bandwidths & Security Groups* pane:

a. In *Public IP Address*, enable *Assign Public IPv4 Address*.
You access the FortiPAM GUI and CLI console through this IP address.

You can change to auto assign the public IP address into Elastic IP Address (EIP) after the FortiPAM instance is running.

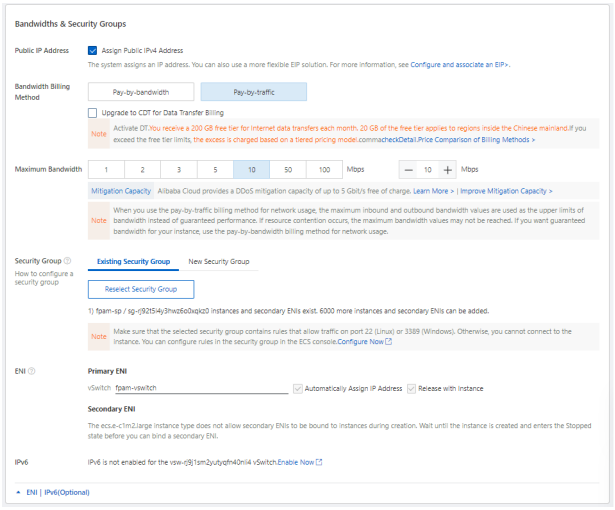
Also, if you have already created an EIP and want to use that IP address to access the FortiPAM instance, you do not need to check auto public IP address.

Remember to associate the EIP address to this ECS instance after instance is created.

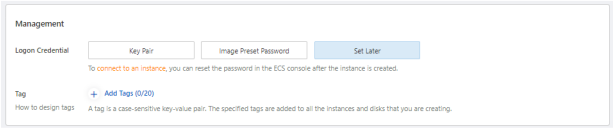
11. In *Bandwidth Billing Method*, select *Pay-by-bandwidth* or *Pay-by-traffic*.
In this example, *Pay-by-traffic* is selected.

12. In *Maximum Bandwidth*, select *10*.

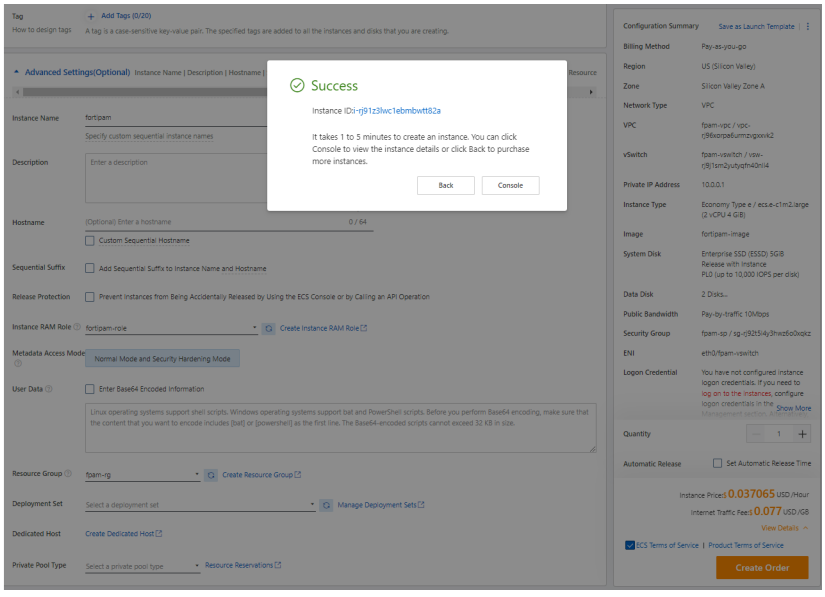
13. In *vSwitch*, ensure that the previously created vSwitch in vSwitch.



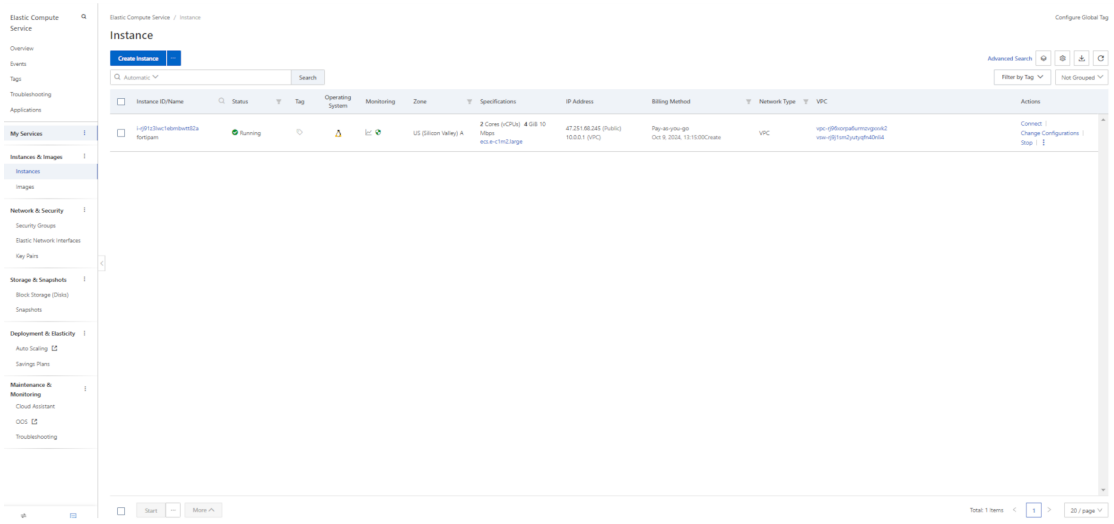
14. In the *Management* pane:
    a. In *Logon Credential*, select *Select Later*.



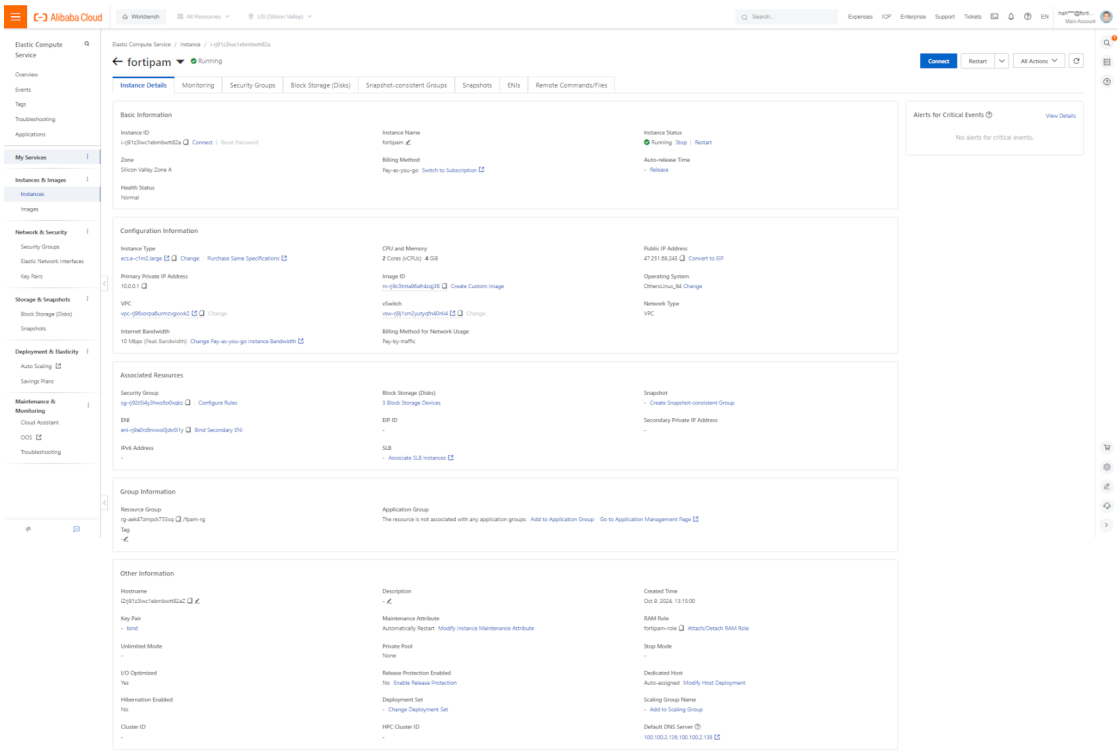
15. In *Advanced Settings (Optional)* pane:
    a. In *Instance Name*, enter the instance name.
    b. Optionally, enter a description.
    c. In *Instance RAM Role*, select the RAM role created in Creating a RAM role on page 623.
    d. In *Resource Group*, select the resource group created in Creating a resource group on page 618.
16. Click *Create Order*.
17. In the dialog that appears, select *Agree and Place Order*.
    The instance is created.



18. Go to *Instances & Images* > *Instances*.
The FortiPAM instance is running.



The following shows the FortiPAM instance status.

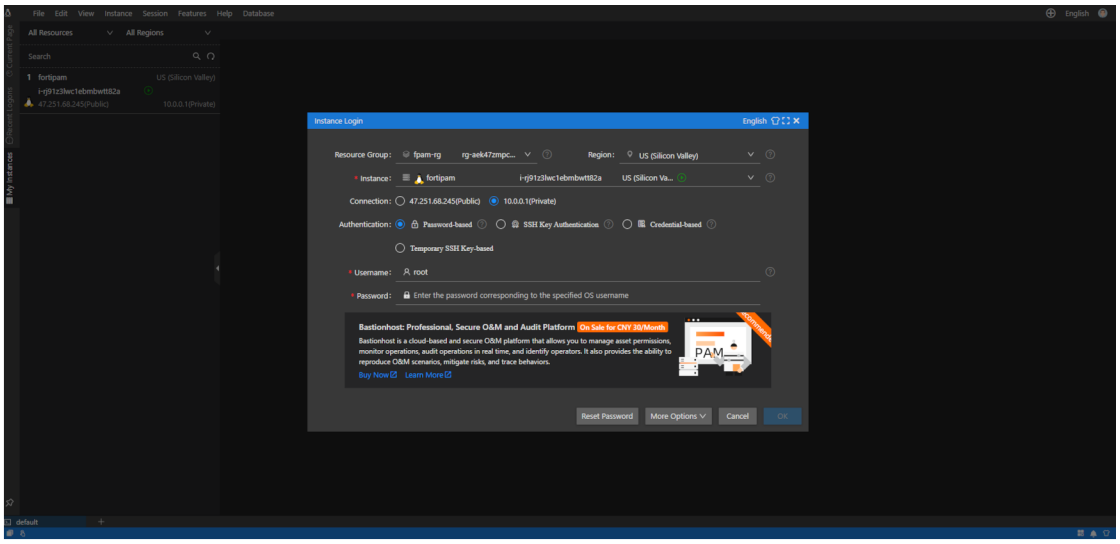


Connecting to the FortiPAM-VM

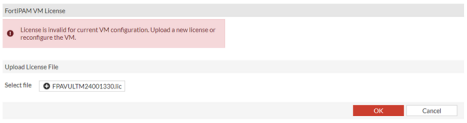
To connect to the FortiPAM-VM:

1. In *Instances & Images* > *Instances*.
2. Select *Connect* to connect to the FortiPAM-VM.

3. In the dialog that appears, select *Sign in now*.
   A new *ECS-Workbench* tab opens.



4. In *Connection*, select the public IP address.
5. In *Username*, enter `admin`.
6. For the first login, in *Password*, enter the instance ID.
7. Click *OK*.
8. In the dialog that appears, click *OK*.
9. You are prompted to change the default password during the first login.
   After changing password successfully, you are prompted to upload the license.
10. In the *Upload License* file pane, select *Upload* and browse to the license file on your management computer.



11. Click *OK*.
    After the boot up, the license status changes to valid.

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

Alternatively, you can upload the license through the public IP address using SCP.

See Uploading the license using SCP.

Appendix T: FortiPAM HA on Alibaba Cloud

This chapter provides a sample configuration of active-passive (A-P) FortiPAM HA on Alibaba Cloud within one availability zone using routing tables and EIPs.

To deploy and configure FortiPAM Active-Passive HA solution:

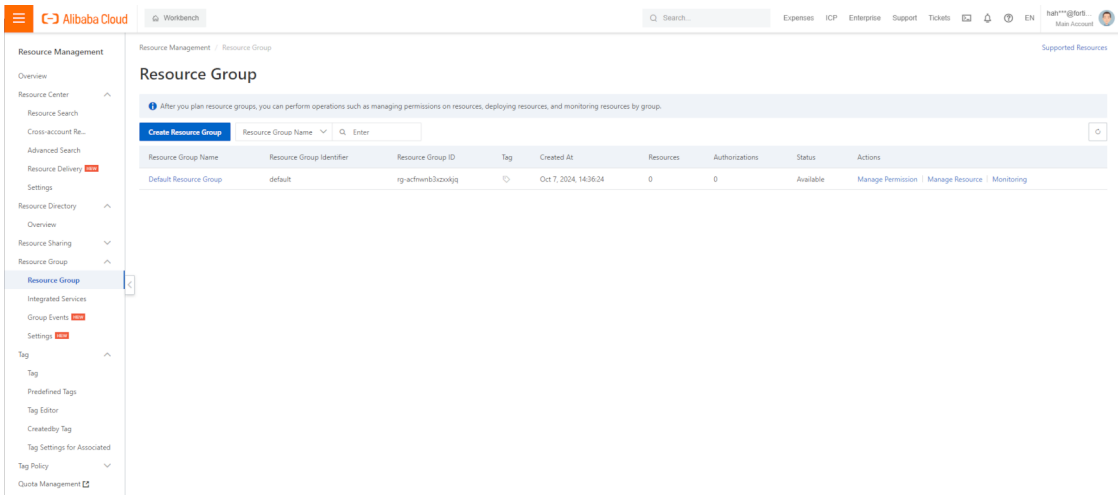
1. Creating a resource group on page 643
2. Setting up a Virtual Private Cloud (VPC) on page 644
3. Creating a security group on page 648
4. Creating Elastic Network Interfaces (ENI) on page 650
5. Creating a routing table on page 651
6. Creating Elastic IP Addresses (EIP) on page 653
7. Creating a RAM role on page 657
8. Creating two FortiPAM instances for HA on page 661
9. Configuring HA settings on the FortiPAM-VMs on page 662
10. Verification on page 665

Creating a resource group

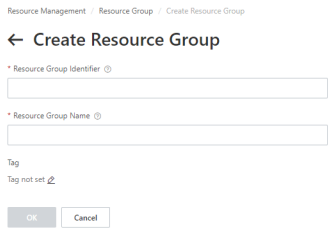
For information on resource groups, see Creating a resource group on page 618.

To create a resource group:

1. In the Alibaba Cloud console, from the search bar, look for *Resource Management*.
2. From the tree menu on the left, go to *Resource Group* > *Resource Group*.
   The *Resource Group* window opens.



3. Select *Create Resource Group*.
   The *Create Resource Group* wizard opens.

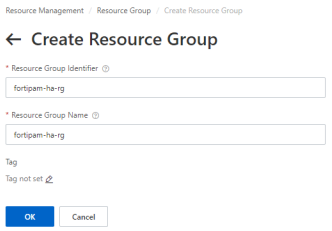


4. In *Resource Group Indentifier*, enter the resource group name.



The identifier cannot be changed once the resource group is created.

5. In *Resource Group Name*, enter the resource group name.
6. Click *OK*.

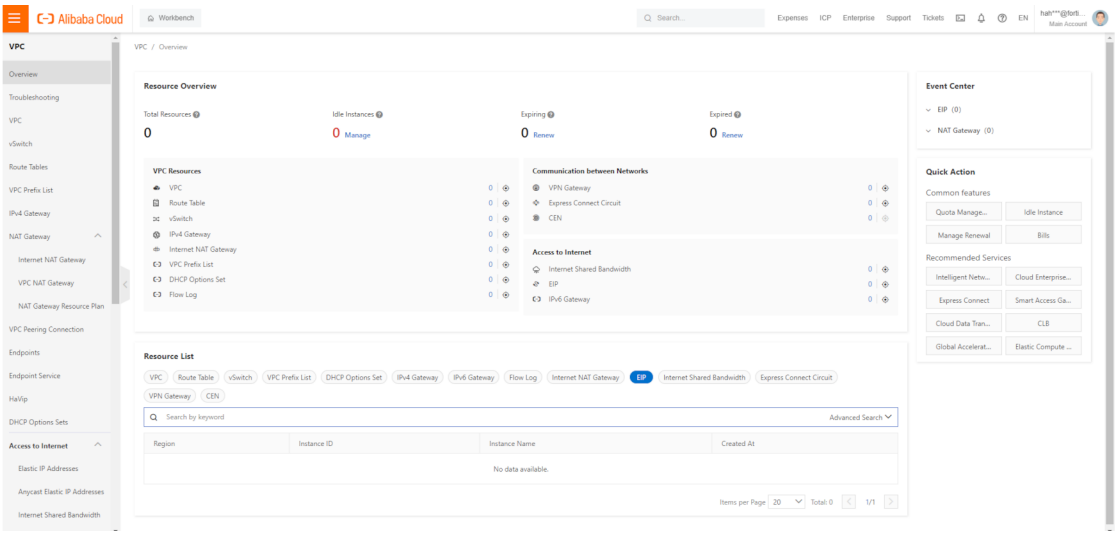


Setting up a Virtual Private Cloud (VPC)

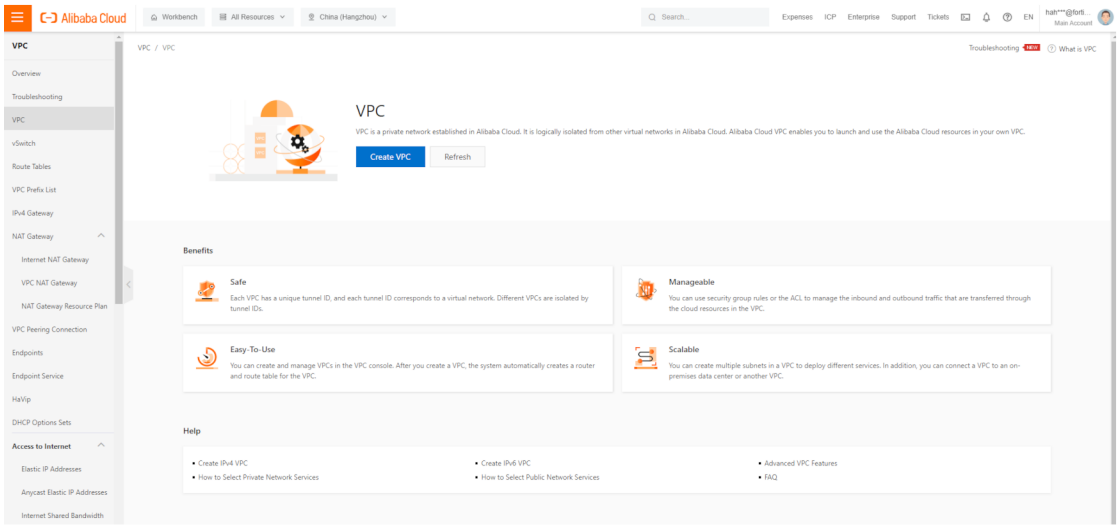
For information on VPC, see Creating a virtual private cloud on page 619.

To set up a VPC:

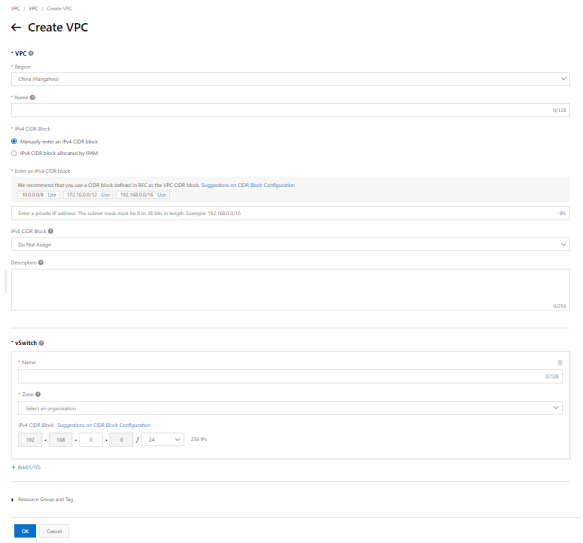
1. In the Alibaba Cloud console, from the search bar, look for Virtual Private Cloud.
   The VPC console opens in a new tab.



2. From the tree menu, go to *VPC*.

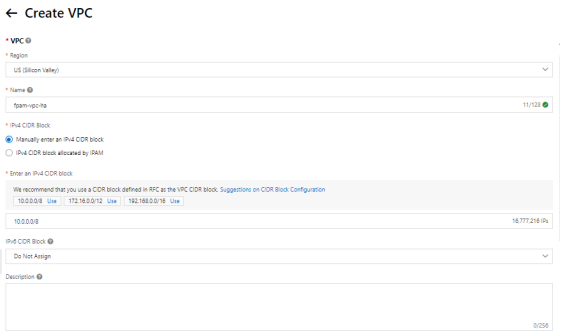


3. From the *All Resources* dropdown on the top, select the resource group created in Creating a resource group on page 643.
4. Select *Create VPC* to create a virtual private cloud.



5. In *Region*, select a region where the FortiPAM-VM instance is located. In this example, *US (Silicon Valley)*.
6. In *Name*, enter a name for the VPC.
7. Keep the default value in *IPv4 CIDR Block*, i.e., *Manually enter an IPv4 CIDR block*.
8. In *Enter an IPv4 CIDR block*, enter `10.0.0.0/8`.
9. Keep the default value in IPv6 CIDR Block, i.e., *Do Not Assign*.

10. Optionally, enter a description.



11. In *vSwitch*, we create four vSwitches with the following subnets under the VPC:
    - `external`: For the external data traffic on the public network side.
    - `internal`: For internal data traffic on the private network side.
    - `hasync`: For heartbeat traffic between the two HA members. This is the unicast communication.
    - `mgmt`: For dedicated management.

Port	Subnet
port1	10.0.1.0/24
port2	10.0.2.0/24
port3	10.0.3.0/24
port4	10.0.4.0/24



A vSwitch is a basic network component of a VPC.

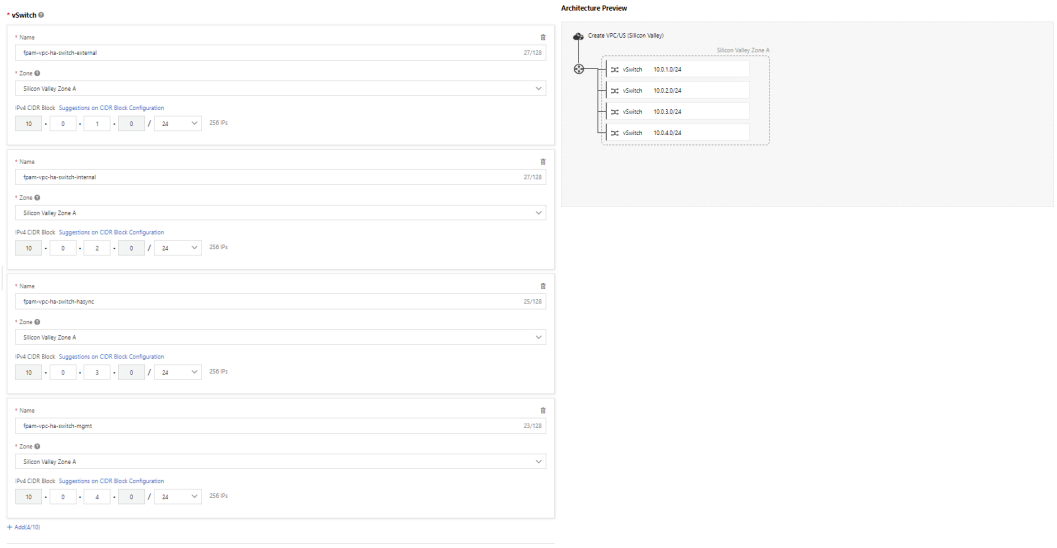
    a. In *Name*, enter a name for the vSwitch.
    b. In *Zone*, select a zone.



It is recommended that all the vSwitches are in the same zone.

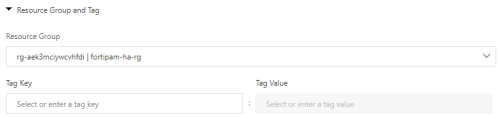
    c. In *IPv4 CIDR Block*, enter the IP address assigned to the vSwtich.

d. Select *Add* and repeat steps `a` – `d` to create three additional vSwitches.

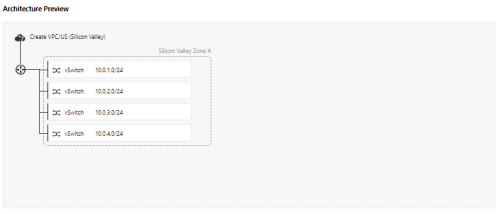


12. In *Resource Group and Tag*:

a. In *Resource Group*, select the resource group created in Creating a resource group on page 643.

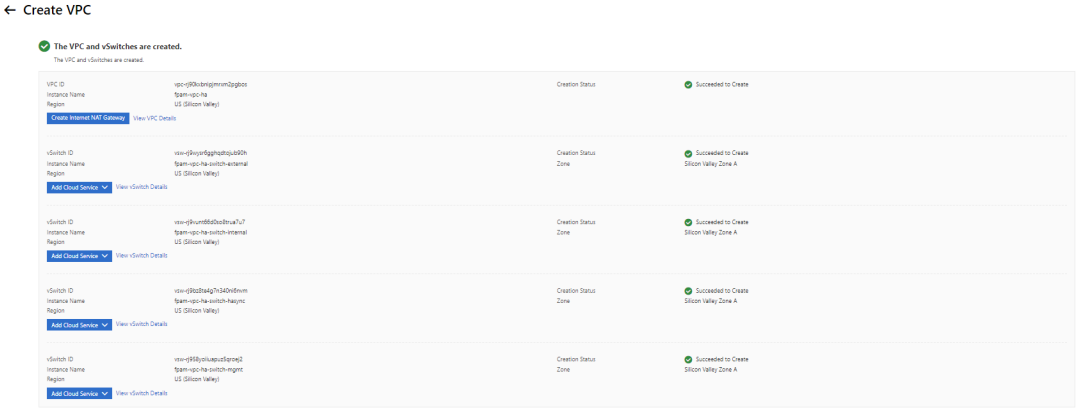


The *Architecture Preview* appears on the right.



13. Click *OK*.

The VPC and vSwitches are created.

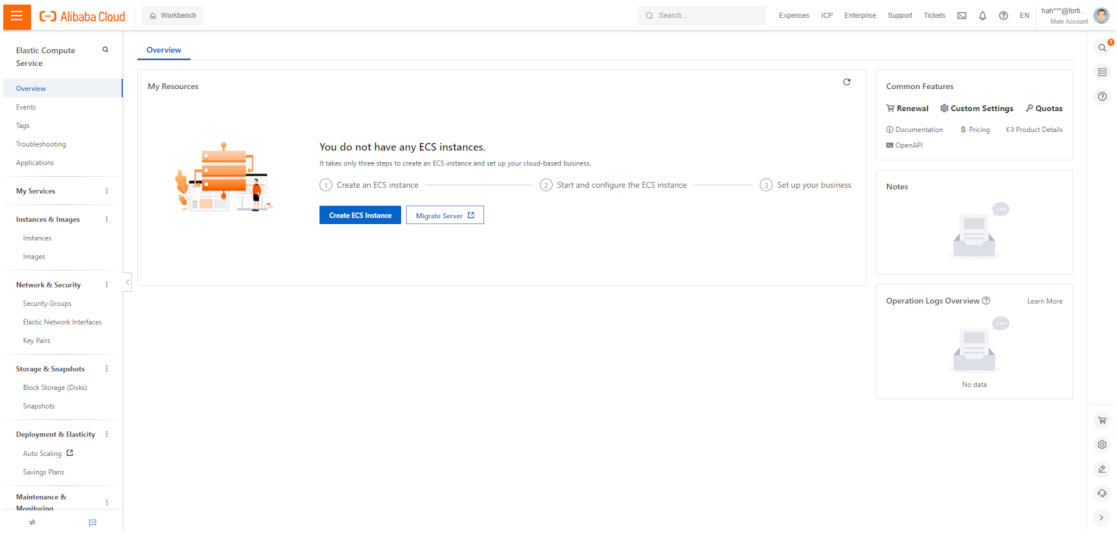


Creating a security group

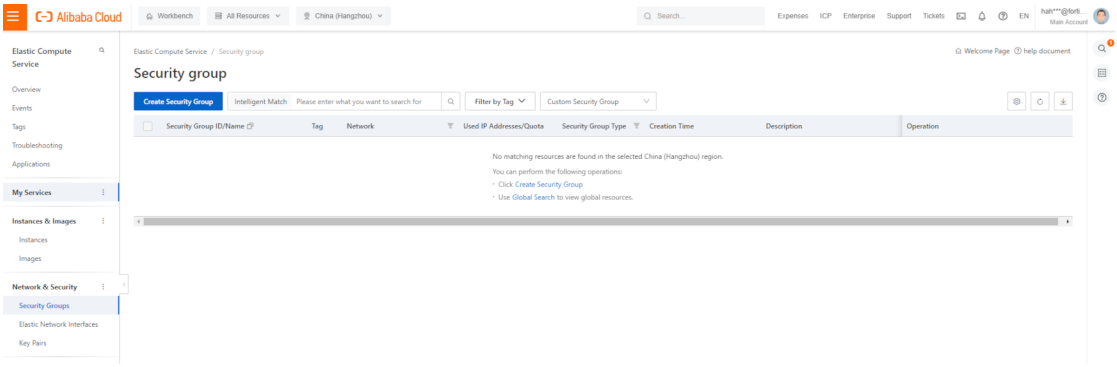
For information for security group, see Creating a security group on page 621.

To create a security group:

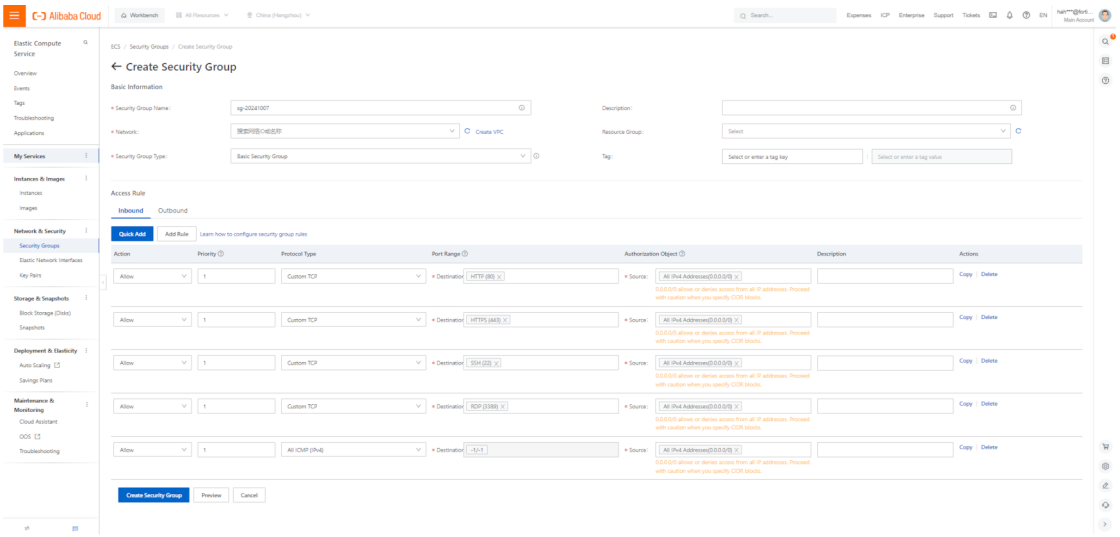
1. In the Alibaba Cloud console, from the search bar, look for *Elastic Compute Service*.
   The *Elastic Compute Service* opens in a new tab.



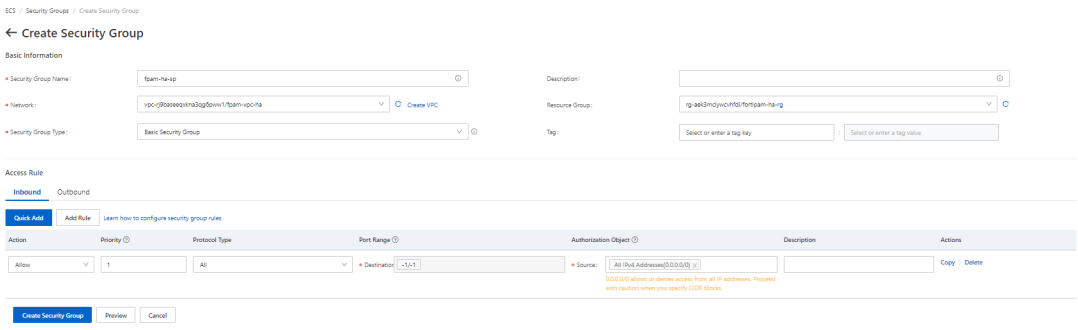
2. Go to *Network & Security* > *Security Groups*.
   The *Security group* window opens.



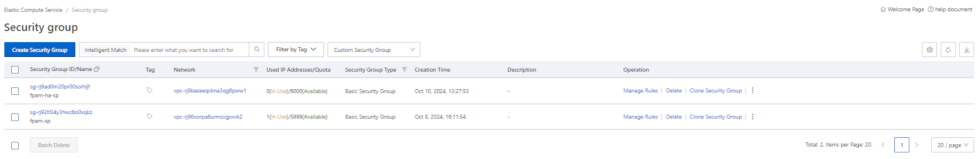
3. Select *Create Security Group*.



4. In *Basic Information*:
   a. In *Security Group Name*, enter a name for the security group.
   b. In *Network*, select the VPC created in Setting up a Virtual Private Cloud (VPC) on page 644.
   c. In *Security Group Type*, select either *Basic Security Group* or *Advanced Security Group*.
   d. Optionally, in *Description*, enter a description.
   e. In *Resource Group*, select the resource group created in Creating a resource group on page 643.
5. In *Access Rule*:
   We manually configure rules to inbound and outbound traffic.
   a. In the *Inbound* tab:
      We manually add rules to allow ports according to your needs. See FortiPAM Ports.
   b. In the *Outbound* tab:
      By default, security groups allow all outbound traffic.
      ECS instances in a security group are allowed to access external networks.
   c. In this example, we allow all the inbound and outbound traffic:



6. Select *Create Security Group* to create the security group.



Creating Elastic Network Interfaces (ENI)

We specify the primary private IP address for each vSwitch. It should be in the same subnet as your backend server.

The following lists the IP address assignments for this sample deployment for FortiPAM primary and the FortiPAM secondary units:

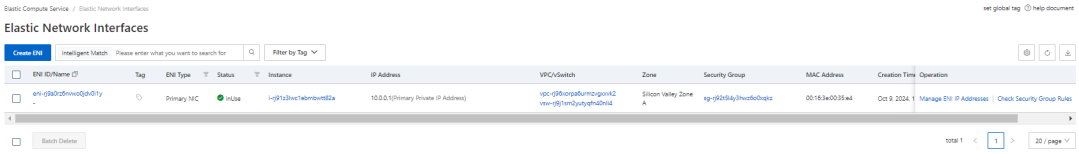
Port	Primary address- FortiPAM primary	Secondary address- FortiPAM secondary
port1	10.0.1.11	10.0.1.12
port2	10.0.2.11	10.0.2.12
port3	10.0.3.11	10.0.3.12
port4	10.0.4.11	10.0.4.12

When creating the two instances, the primary ENI for the external traffic `port1` is automatically generated and the primary IP address is assigned.

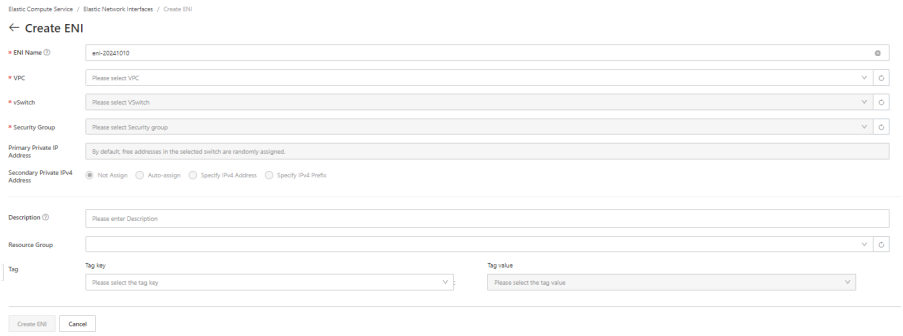
Therefore, we need to create six ENIs in total- two for the internal data traffic, two for the heartbeat traffic, and two for management.

To create ENI:

1. In the Alibaba Cloud console, from the search bar, look for *Elastic Compute Service*.
2. Go to *Network & Security* > *Elastic Network Interfaces*.
   The *Elastic Network Interfaces* window opens.

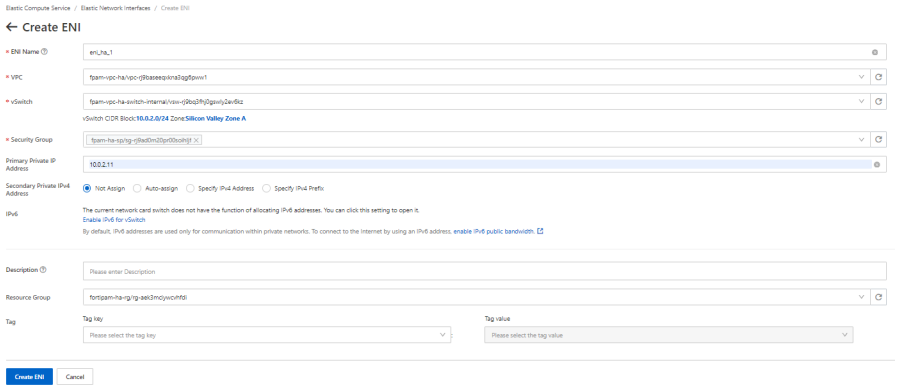


3. Select *Create ENI*.
   The *Create ENI* window opens.



4. In *ENI Name*, enter the name for the ENI.
5. In *VPC*, select the VPC created in Setting up a Virtual Private Cloud (VPC) on page 644.
6. In *vSwitch*, select a vSwitch previously created in vSwitch.
7. In *Security Group*, select the security group created in Creating a security group on page 648.

8. In *Primary Private IP Address*, enter the related primary address from the table above.
   Note: The IP address must be in same subnet as the vSwitch.
9. In *Description*, optionally enter a description.
10. In *Resource Group*, select the resource group created in Creating a resource group on page 643.
11. Click *Create ENI*.



12. Repeat steps `2 - 11` to create five additional ENIs.

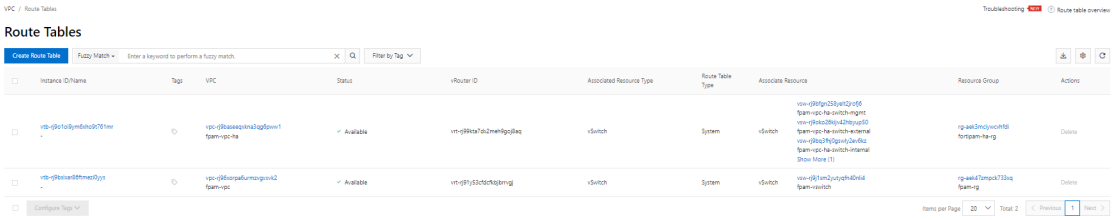
Creating a routing table

Alibaba Cloud creates a default routing table for the VPC.

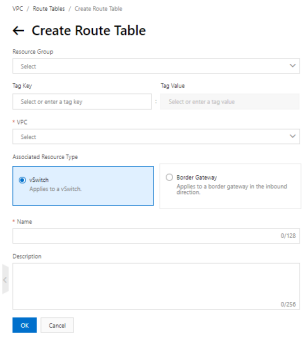
We create a route table to associate with the internal VPC vSwitch.

To create a routing table:

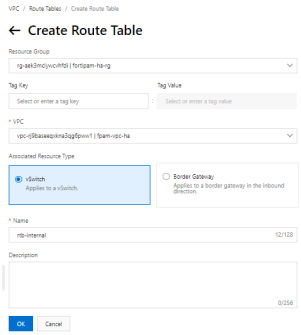
1. In the Alibaba Cloud console, from the search bar, look for *Virtual Private Cloud*.
2. From the tree menu, go to *Route Tables*.
   The *Route Tables* window opens.



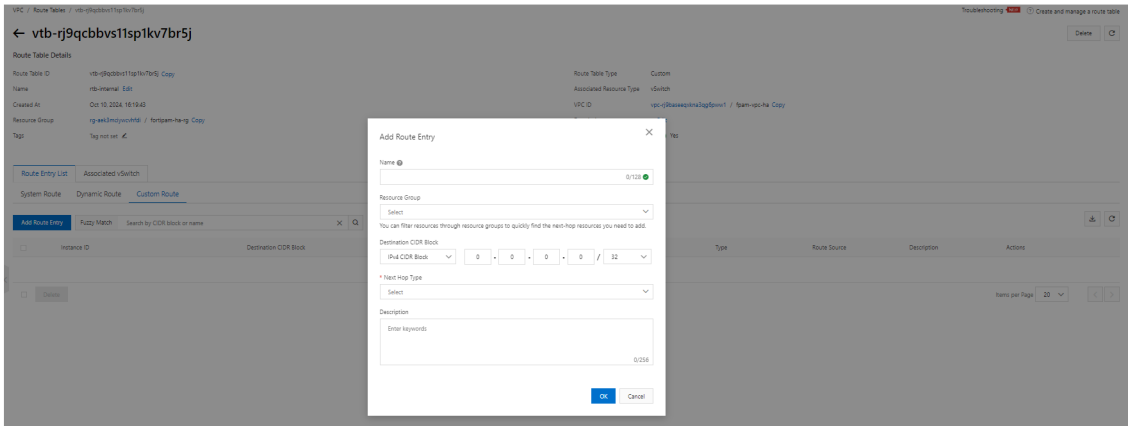
3. Select *Create Route Table*.
   The *Create Route Table* window opens.



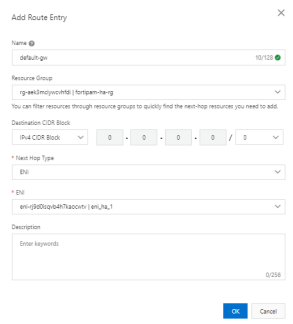
4. In *Resource Group*, select the resource group created in Creating a resource group on page 643.
5. In *VPC*, select the VPC created in Setting up a Virtual Private Cloud (VPC) on page 644.
6. In *Name*, enter the name for the routing table.
7. Optionally, enter a description.
8. Click *OK*.



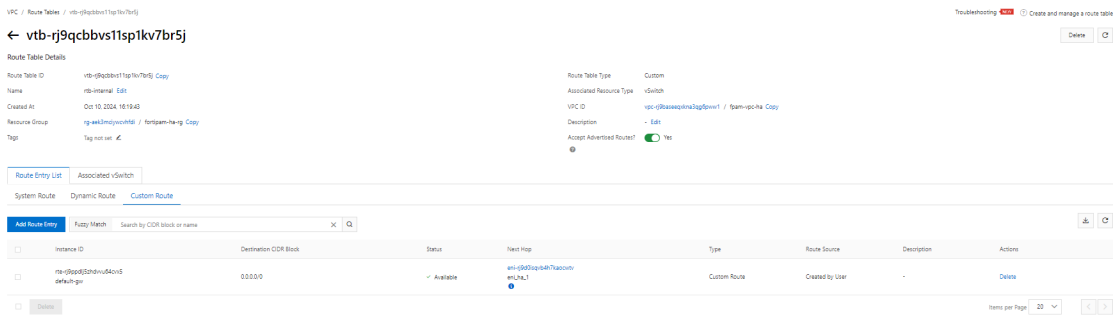
9. From the list, select the recently created route table.
10. In the *Custom Route* tab, select *Add Route Entry*.
    The *Add Route Entry* window opens.



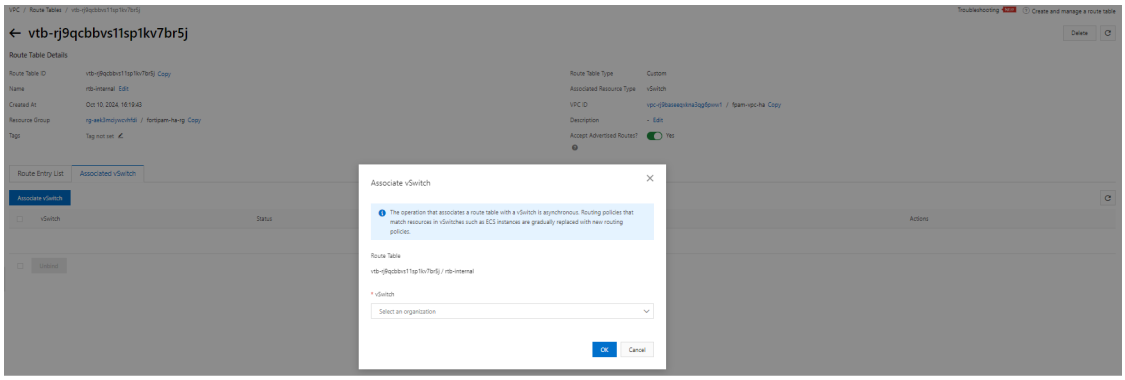
11. In *Name*, enter a name for the route entry.
12. In *Resource Group*, select the resource group created in Creating a resource group on page 643.
13. In the *Destination CIDR Block* dropdown, ensure that *IPv4 CIDR Block* is selected, and enter `0.0.0.0/0`.
14. In the *Next Hop Type* dropdown, select *ENI*.
15. In ENI, select the interface (ENI) of the primary FortiPAM.
16. Optionally, enter a description.
17. Click *OK*.



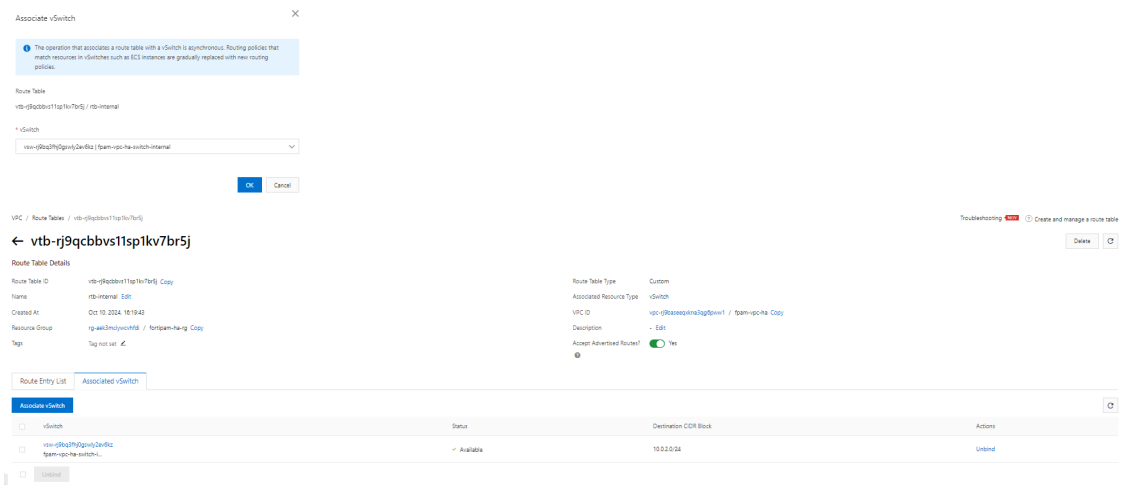
The following shows the custom route configuration:



18. Go to the *Associated vSwitch* table.
19. Select *Associate vSwitch*.
    The *Associate vSwitch* window opens.



20. In *vSwitch*, select the internal switch created in vSwitch.
21. Click *OK*.



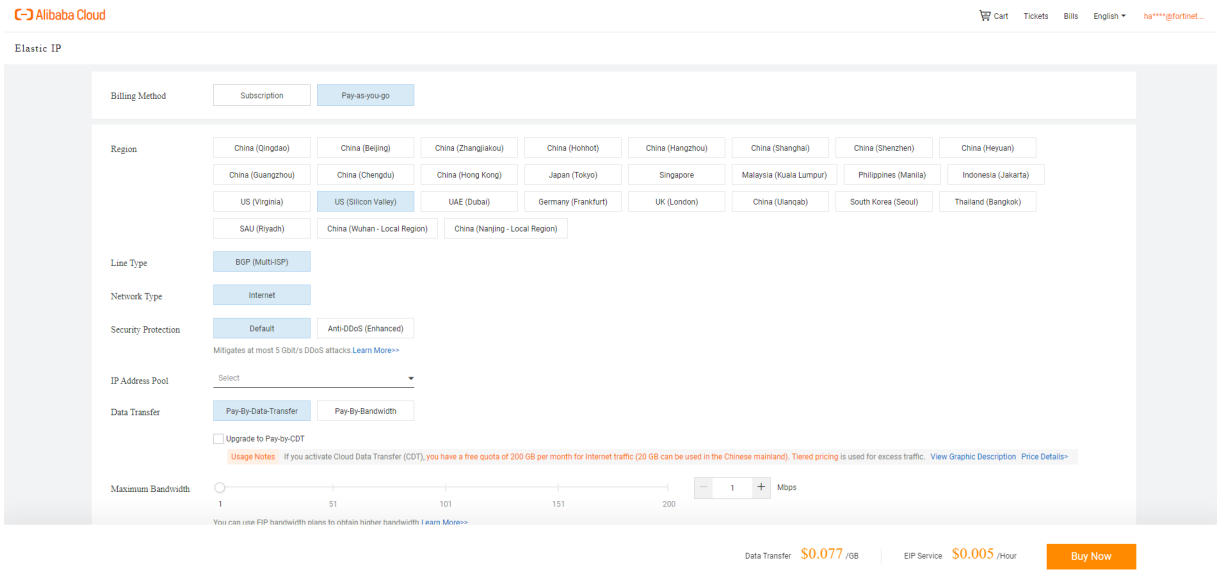
Creating Elastic IP Addresses (EIP)

In FortiPAM HA mode, we require three EIPs:

- EIP1 for HA external traffic IP address.
- Two EIPs- One for the primary FortiPAM and the other for the secondary FortiPAM.

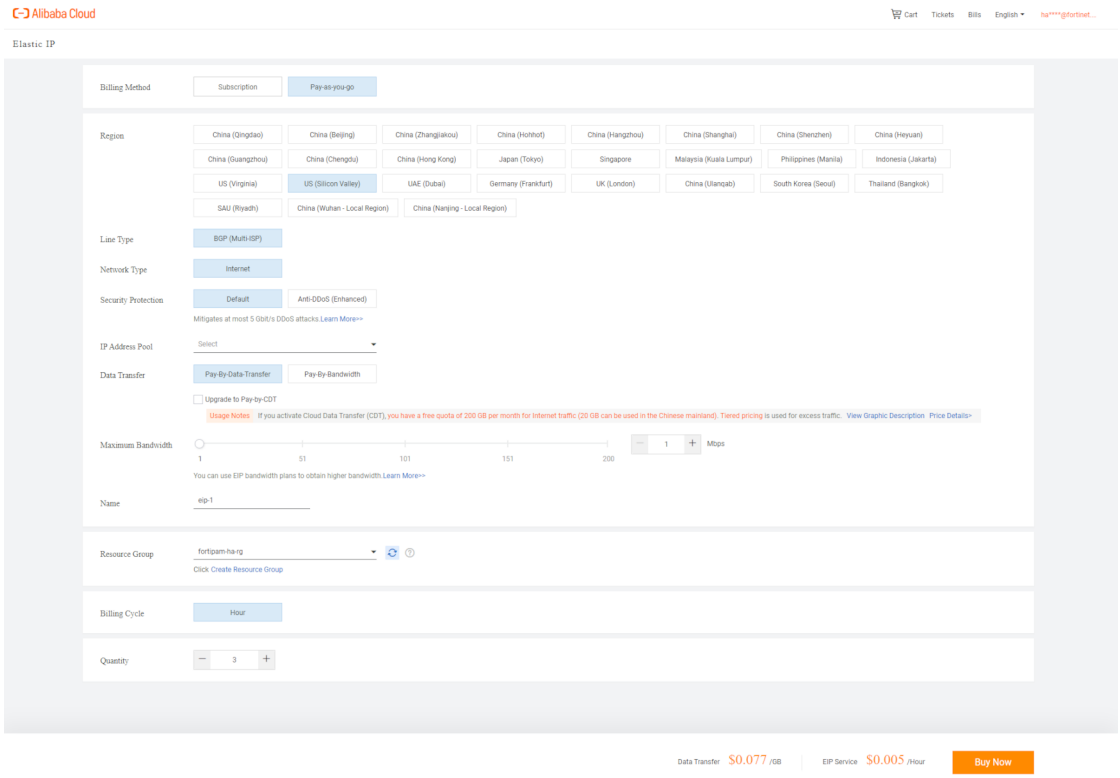
To create EIPs:

1. In the Alibaba Cloud console, from the search bar, look for *Virtual Private Cloud*.
2. From the tree menu, go to *Elastic IP Addresses*.
3. Select *Create EIP*.
   Elastic IP window opens as a new tab.

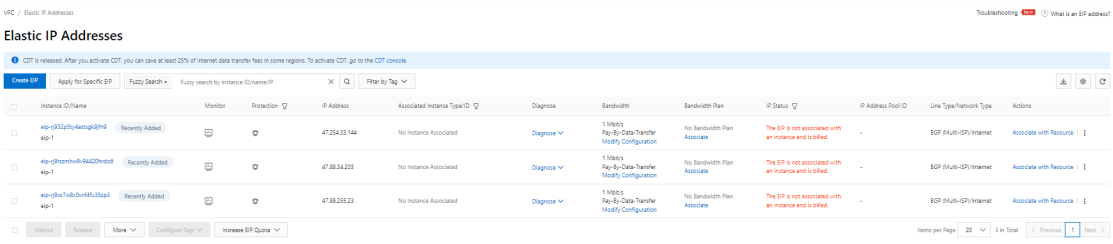


4. In *Billing Method*, select *Pay-as-you-go*.
5. In *Region*, select *US (Silicon Valley)*.
6. In *Line Type*, select *BGP (Multi-ISP)*.
7. In *Network Type*, select *Internet*.
8. In *Security Protection*, select *Default*.
9. In *Data Transfer*, select either *Pay-By-Data-Transfer* or *Pay-By-Bandwidth*.
   Note: *Pay-By-Bandwidth* is often more expensive because it involves guaranteeing a certain level of performance and speed regardless of actual data usage.
   Therefore, if there is no need to keep the bandwidth at a certain level, *Pay-By-Data-Transfer* is recommended.
10. In *Maximum Bandwidth*, enter the desired bandwidth (in Mbps).
11. In *Name*, enter a name for the EIP.
12. In *Resource Group*, select the resource group created in Creating a resource group on page 643.
13. In *Quantity*, enter `3`.

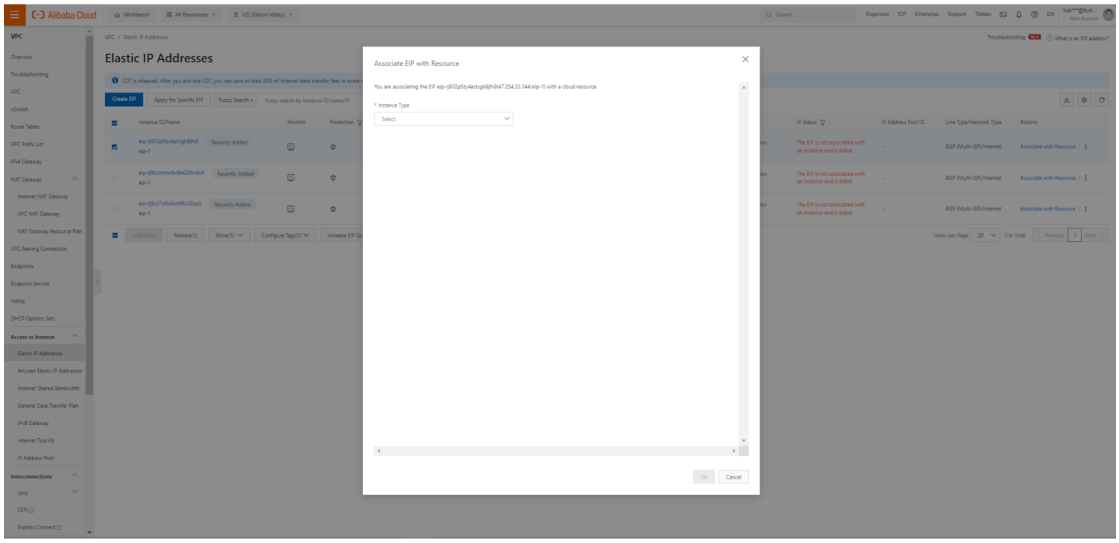
14. Click *Buy Now*.



15. Select *Elastic IP Agreement of Service* to read the terms of service in a new tab and select *Terms of Service* to agree to the terms of service.
16. Click *Activate Now*.
    The service is activated.
17. Select *Management Console* and go to *Elastic IP Addresses*.



18. Associate two of the three EIPs to the primary and the secondary FortiPAM unit management ENIs created in Creating Elastic Network Interfaces (ENI) on page 650.
    a. From the *Elastic IP Addresses* list, select *Associate with Resource*.
       The *Associate EIP with Resource* window opens.



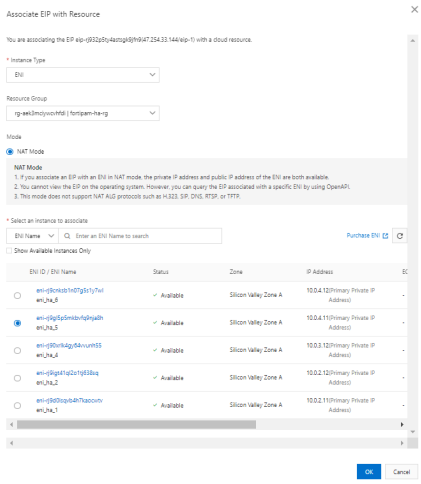
b. In *Instance Type*, select *ENI*.

c. In *Resource Group*, select the resource group selected in Creating a resource group on page 643.

d. In *Mode*, ensure that *NAT Mode* is selected.

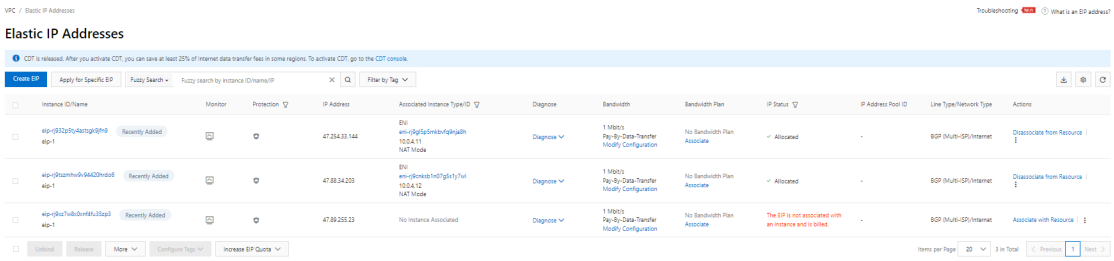
e. In *Select an instance associate*, select the primary FortiPAM unit ENI.

f. Click *OK*.



The elastic IP address is associated with the primary FortiPAM unit management ENI.

g. Repeat steps `a – g` to associate the second elastic IP address with the secondary FortiPAM unit management ENI.



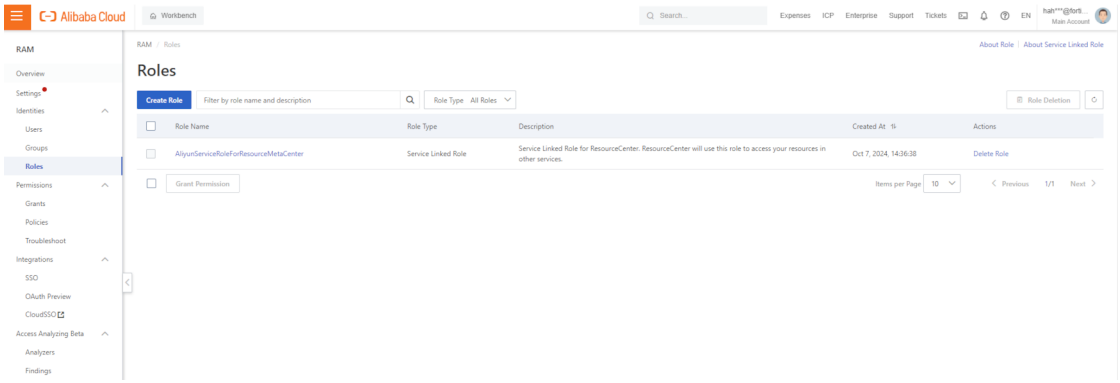
19. Associate the third EIP to the primary FortiPAM instance.

Creating a RAM role

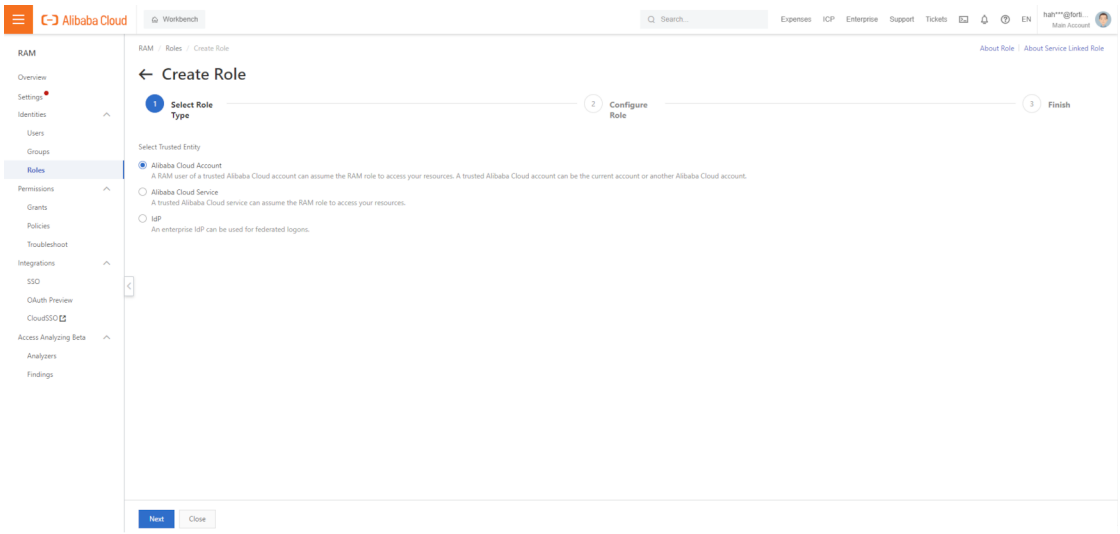
For information on RAM role, see Creating a RAM role on page 623.

To create a RAM role:

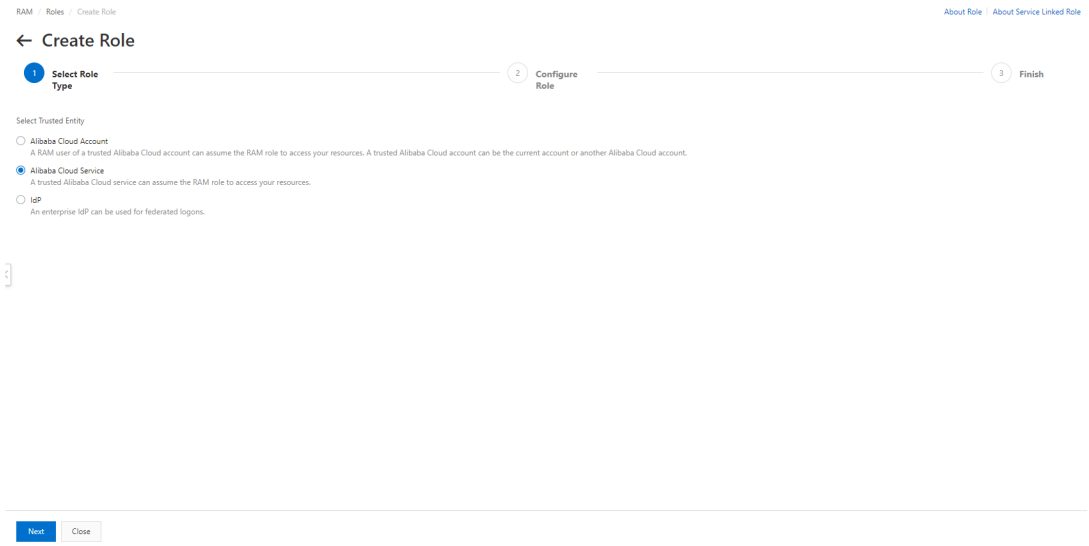
1. In the Alibaba Cloud console, from the search bar, look for *Resource Access Management*.
2. From the tree menu on the left, go to *Identities* > *Roles*.



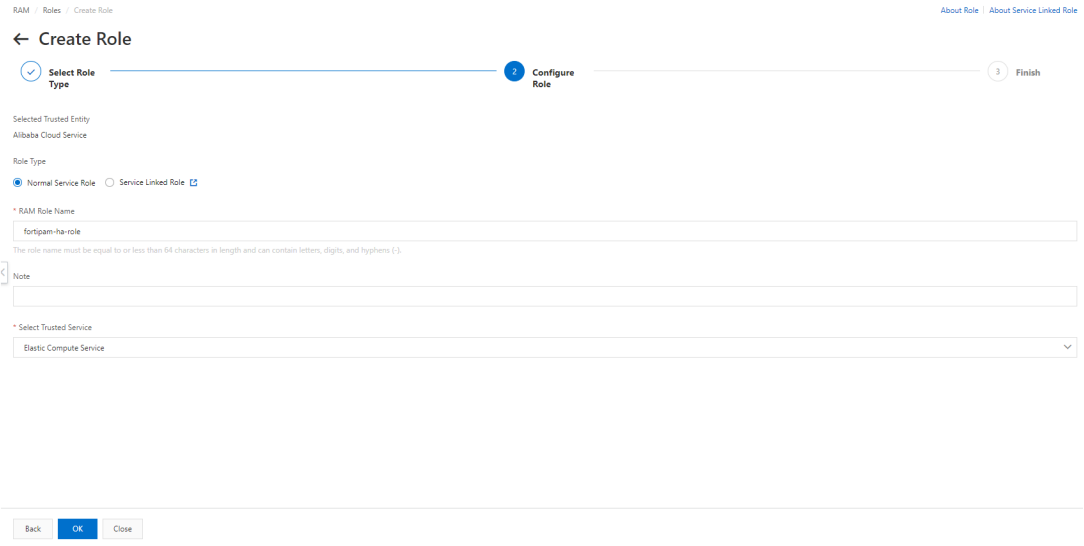
3. Select *Create Role*.
   The *Create Role* wizard opens.



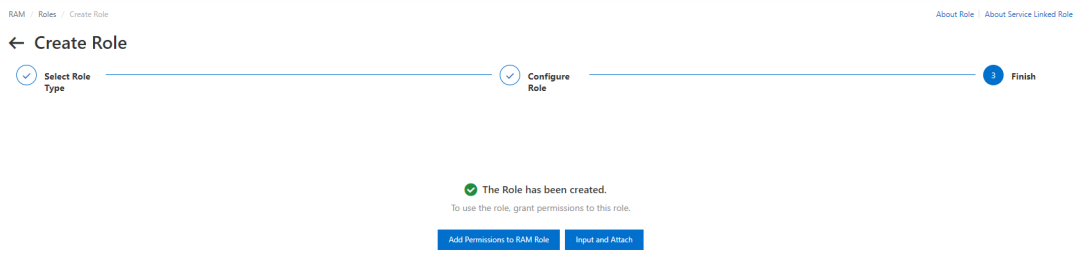
4. In Select *Trusted Entity*, select *Alibaba Cloud Service*, and click *Next*.



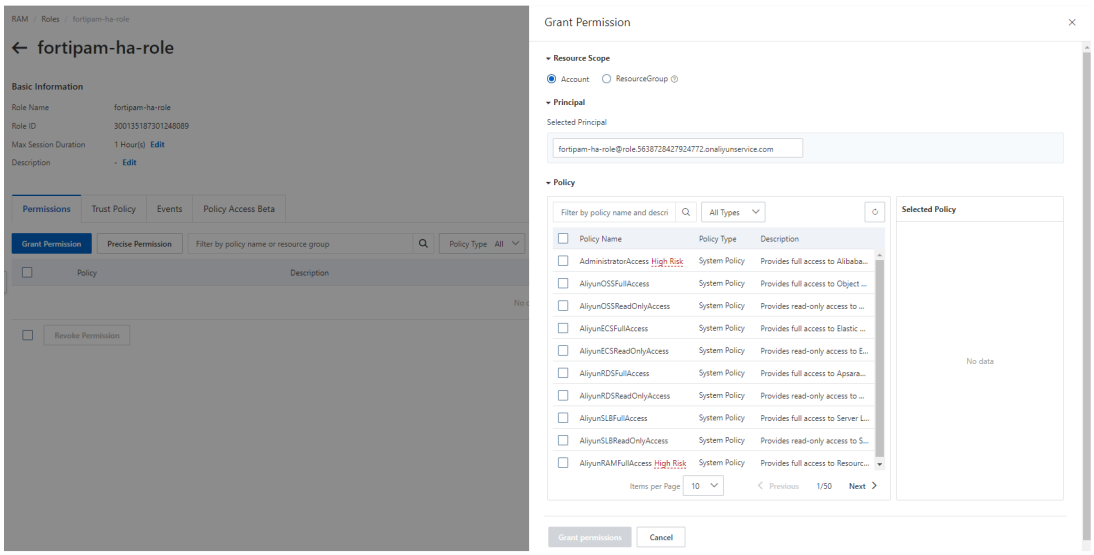
5. In *Configure Role* tab:
   a. In *Role Type*, select *Normal Service Role*.
   b. In *RAM Role Name*, enter the role name.
   c. Optionally, enter a note.
   d. In *Select Trusted Service*, select *Elastic Computer Service*.
6. Click *OK*.



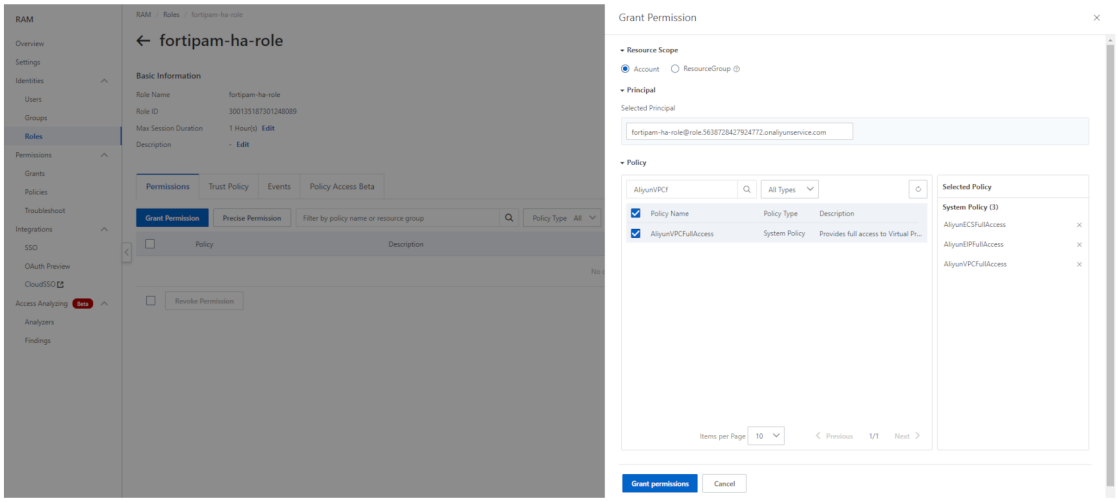
The role was created.



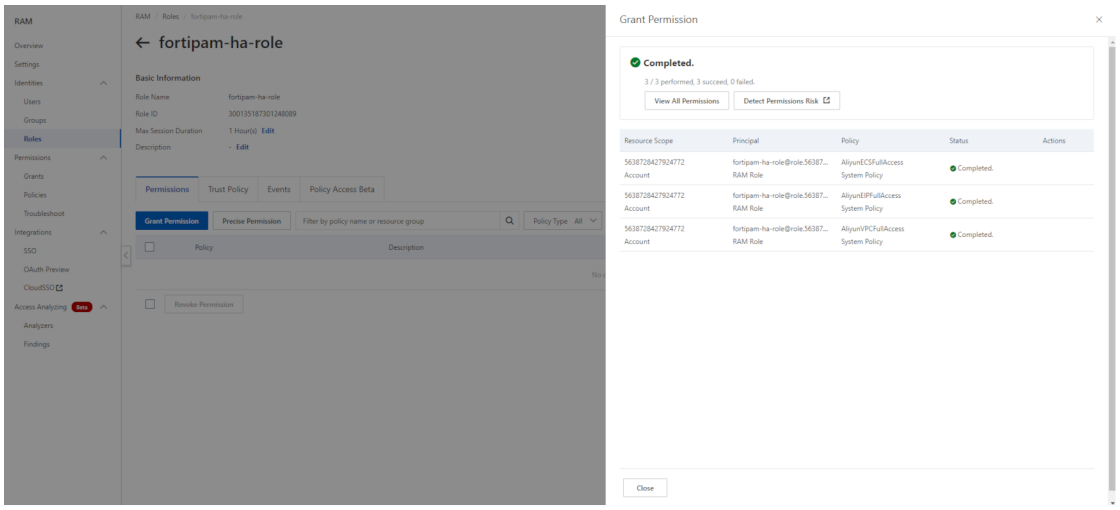
7. We now grant related permissions to the recently created role:
   a. Select *Add Permission to RAM Role*.
      A new window opens.
   b. Select *Grant Permission*.
      The *Grant Permission* window opens.

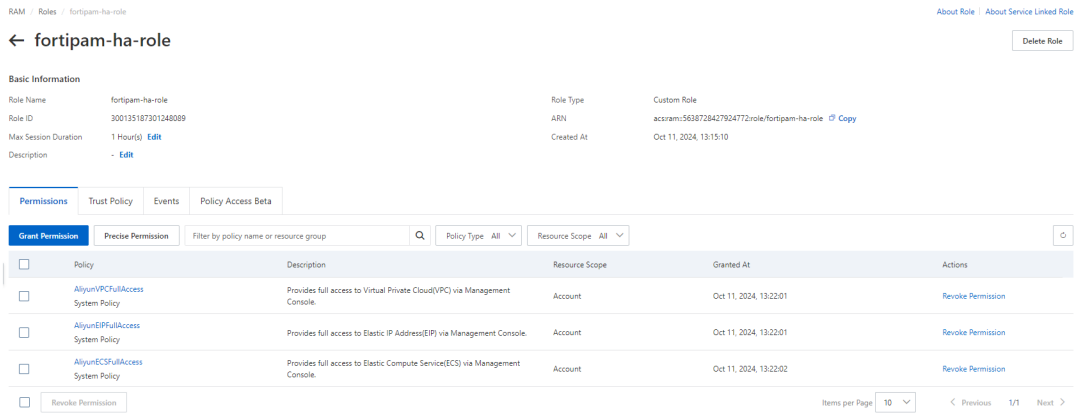


   c. In *Resource Scope*, ensure that *Account* is selected.
      Note: Select *Account* so that the RAM role can be shared by other resource groups.
   d. From the grant permission window, select *AliyunECSFullAccess*, *AliyunEIPFullAccess*, and *AliyunVPCFullAccess* policies.



e. Select *Grant permissions*.





Note: The actual role configurations may differ depending on your environment. Check with your organization's public cloud administrator for information.

In case the HA does not work, create a new RAM rule with a custom policy that includes:

```
{
 "Version":"1",
 "Statement:" [
  {
   "Effect":"Allow"
      "Action": [
        "ecs:DescribeInstances",
        "vpc:DescribeEipAddresses",
        "vpc:DescribeVpcAttribute",
        "vpc:DescribePublishedRouteEntries",
        "vpc:DescribeRouteTables",
        "vpc:AssociateEipAddress",
        "vpc:UnassociateEipAddress",
        "vpc:ReleaseEipAddress",
        "vpc:PublishRouteEntries",
        "vpc:CreateRouteEntry",
        "vpc:DeleteRouteEntry",
        "vpc:ConvertNatPublicIpToEip",
        "ecs:AddTags"
```

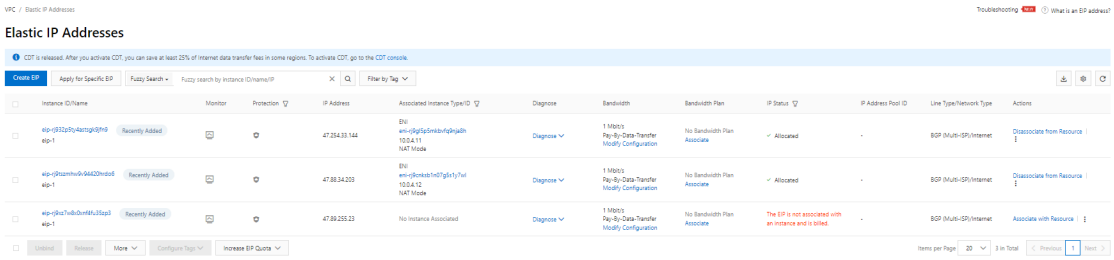
```
            ],
            "Resource": "*"
        }
    ]
}
```

Creating two FortiPAM instances for HA

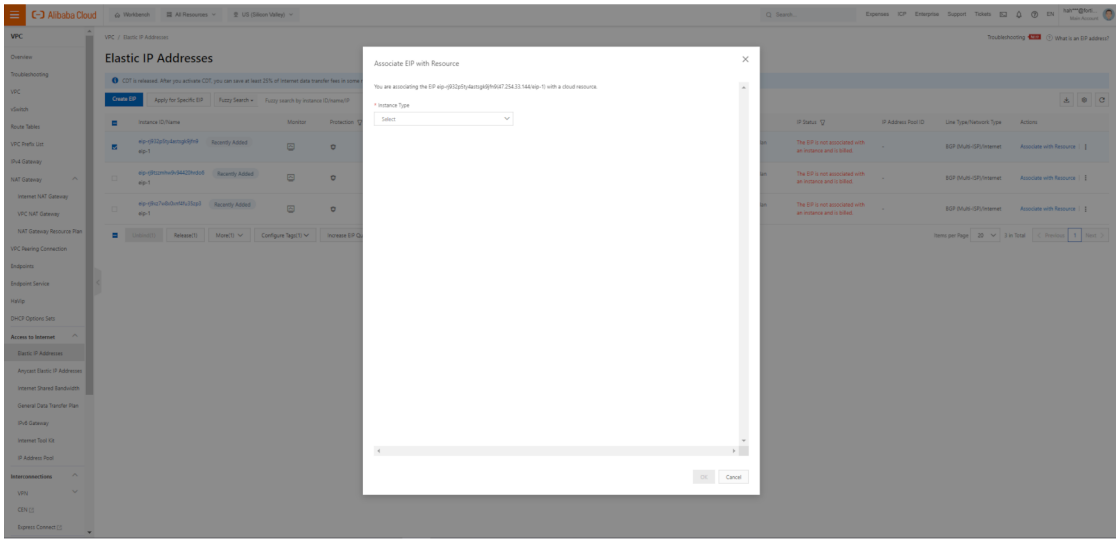
Follow the instructions in Appendix R: FortiPAM HA on Azure on page 598 to create two FortiPAM-VM instances - primary and secondary FortiPAM units.

Pay attention to the following:

1. In both the primary and the secondary instance, it automatically creates the primary ENI.
   Specify the primary private IP address of the primary ENI from the `port1` IP address from table in Creating Elastic Network Interfaces (ENI) on page 650.
   In the example, the primary FortiPAM IP address is `10.0.1.11` and the secondary primary IP is `10.0.1.12`.
2. Do not enable *Assign Public IPv4 Address* for both the FortiPAM instances.
3. Associate the final EIP created in Creating Elastic IP Addresses (EIP) on page 653 with the primary FortiPAM IP address `10.0.1.11`.
   a. In the Alibaba Cloud console, from the search bar, look for *Virtual Private Cloud*.
   b. Go to *Elastic IP Address*.
   There is one unassociated elastic IP address in the list.



   c. Select *Associate with Resource* for the unassociated elastic IP address.
   The *Associate EIP with Resource* window opens.



d. In *Instance Type*, select *ENI*.
e. In *Resource Group*, select the resource group selected in Creating a resource group on page 643.
f. In *Mode*, ensure that *NAT Mode* is selected.
g. In *Select an instance associate*, select the primary FortiPAM unit ENI.
h. Click *OK*.

4. After the two FortiPAM instances are ready, bind the six ENIs as secondary ENI- three for each FortiPAM instance (one each for internal, heartbeat, and the management) in *Associated Resources* in the *Instance Details* page.

Configuring HA settings on the FortiPAM-VMs

After the two FortiPAM VMs are successfully deployed, you must configure Active-Passive HA settings on the two VMs in the CLI console in the GUI or via SSH.

To configure HA settings on the primary FortiPAM in the CLI console:

1. Configure static gateway before setting the system interface:

```
config router static
 edit 1
  set gateway 10.0.1.253
  set device "port1"
 next
end
```

2. Enter the following CLI commands:

```
config system interface
 edit "port1"
  set vdom "root"
  set ip 10.0.1.11 255.255.255.0
  set allowaccess ping ssh ftm
  set type physical
  set snmp-index 1
 next
 edit "port2"
  set vdom "root"
  set ip 10.0.2.11 255.255.255.0
  set allowaccess ping ssh
  set type physical
  set snmp-index 2
 next
 edit "port3"
  set ip 10.0.3.11 255.255.255.0
  set allowaccess ping ssh
  set type physical
  set snmp-index 4
 next
 edit "port4"
  set ip 10.0.4.11 255.255.255.0
  set allowaccess ping ssh
  set type physical
  set snmp-index 5
 next
 edit "ssl.root"
  set vdom "root"
```

```
    set type tunnel
    set alias "SSL VPN interface"
    set snmp-index 3
   next
  end
  config system vdom-exception
   edit 1
    set object firewall.vip
   next
  end
  config system ha
   set group-id 123 #same group id
   set group-name "FPAM-HA" #same group name
   set mode active-passive
   set password 123 #set the same password as the secondary FortiPAM
   set hbdev "port3" 50
   set ha-mgmt-status enable
   config ha-mgmt-interfaces
    edit 1
     set interface "port4"
     set gateway 10.0.4.253
    next
   end
   set override enable
   set priority 128 #ensure the priority level is higher than the settings on the
secondary FortiPAM
   set unicast-status enable
   set unicast-gateway 10.0.3.253
   config unicast-peers
    edit 1
     set peer-ip 10.0.3.12
    next
   end
  end
```

You can now shutdown the primary FortiPAM, disassociate the public EIP from the primary FortiPAM, and associate the public EIP to the secondary FortiPAM.

You can use the same IP address to log in to the secondary FortiPAM and continue to perform configurations.

To configure HA settings on the secondary FortiPAM in the CLI console:

1. Configure the static gateway before setting the system interface:

```
config router static
 edit 1
  set gateway 10.0.1.253
  set device "port1"
 next
end
```

2. Enter the following CLI commands:

```
config system interface
 edit "port1"
  set vdom "root"
  set ip 10.0.1.12 255.255.255.0
  set allowaccess ping ssh ftm
```

```
    set type physical
    set snmp-index 1
   next
   edit "port2"
    set vdom "root"
    set ip 10.0.2.12 255.255.255.0
    set allowaccess ping ssh
    set type physical
    set snmp-index 2
   next
   edit "port3"
    set ip 10.0.3.12 255.255.255.0
    set allowaccess ping ssh snmp
    set type physical
    set snmp-index 4
   next
   edit "port4"
    set ip 10.0.4.12 255.255.255.0
    set allowaccess ping ssh snmp
       set type physical
    set snmp-index 5
   next
   edit "ssl.root"
    set vdom "root"
    set type tunnel
    set alias "SSL VPN interface"
    set snmp-index 3
   next
  end
  config system vdom-exception
   edit 1
    set object firewall.vp
   next
  end
  config system ha
   set group-id 123 #same group id
   set group-name "FPAM-HA" #same group name
   set mode active-passive
   set password 123 #set the same password as on primary FortiPAM
   set hbdev "port3" 50
   set ha-mgmt-status enable
   config ha-mgmt-interfaces
    edit 1
     set interface "port4"
     set gateway 10.0.4.253
    next
   end
   set override enable
   set priority 64
   set unicast-status enable
   set unicast-gateway 10.0.3.253
   config unicast-peers
    edit 1
     set peer-ip 10.0.3.11
    next
```

```
    end
  end
```

a. Reboot the secondary FortiPAM.
b. Disassociate the public EIP from the secondary FortiPAM and associate the public EIP to the primary FortiPAM.
c. Power on the primary FortiPAM.

Verification

1. Reboot the two FortiPAM VM instances.
2. Log in to the primary FortiPAM.

Appendix U: FortiPAM HA on VMware

Prerequisites

- We set up a primary and a secondary FortiPAM node in an HA cluster.
- The two FortiPAM instances must use the same version of the FortiPAM-VM image.
- Each instance must have at least two network interfaces to successfully implement HA.

To deploy and configure FortiPAM HA on VMware:

1. Configuring FortiPAM instances on page 666
2. Configuring network interfaces on page 667
3. Setting up an HA A-P FortiPAM cluster on page 667

Configuring FortiPAM instances

To configure FortiPAM instances:

1. Create two FortiPAM VMs on VMware.
   See Appendix B: Installation on VMware on page 496.

Ensure that the vCPU, RAM and other parameters are sufficiently set.
See System requirements.

Use the CLI command `get system status` to check the FortiPAM-VM instance status.

Wait till the license status changes to valid before configuring the FortiPAM instances for HA.



Configuring network interfaces

We configure two network interfaces:

- One for the external data traffic on the public network side.
- The other for the heartbeat traffic between the two members of the HA cluster.
  This is for the unicast communication and configuration synchronization.
  Since HA is used under the same subnet, no additional gateway is set for the heartbeat traffic.

The following lists the IP address assignments for the HA deployment:

Port	Primary address for the primary FortiPAM	Primary address for the secondary FortiPAM
port1	10.59.112.157/24	10.59.112.158/24
port2	10.1.100.11/24	10.1.100.12/24

To configure network interface:

1. To configure a network interface, see Editing an interface on page 368.

Setting up an HA A-P FortiPAM cluster

To set up an HA A-P FortiPAM cluster:

1. On the primary FortiPAM:
   a. **Change the hostname**:

```
config system global
 set hostname fpam-primary
end
```

   b. **Add static route gateway**:
   On the VMware ESXi host, add gateway information within FortiPAM to access the external traffic.

```
config router static
 edit 1
  set gateway 10.59.112.1 #change based on your local network gateway address
  set device "port1"
 next
end
```

   c. **Set the network interface based on the IP address assignment table in IP address assignments**:

```
config system interface
 edit "port1"
  set ip 10.59.112.157 255.255.255.0
  set allowaccess ping ssh
  set type physical
  set snmp-index 1
 next
 edit "port2"
  set ip 10.1.100.11 255.255.255.0
  set allowaccess ping ssh
```

```
    set type physical
    set snmp-indext 2
   next
  end
```

d. Configure HA:

```
   config system ha
    set group-id 101 #use the same group-id within the cluster
    set group-name "fpam-ha-dr" #use the same group-name within the cluster
    set mode active-passive
    set password 123 #use the same password within cluster
    set hbdev "port2" 0 #set the heartbeat interface and priority; same priority level
within a cluster
    set override enable
    set priority 200 #instance priority; keep the secondary instance priority lower
than the primary instance
    set unicast-status enable
    config unicast-peers
     edit 1
      set peer-ip 10.1.100.12 #The secondary instance heartbeat interface IP address
     next
    end
   end
```

2. On the secondary FortiPAM:

a. Change the hostname:

```
   config system global
    set hostname fpam-secondary
   end
```

b. Add static route gateway:

```
   config router static
    edit 1
     set gateway 10.59.112.1 #change based on the local network gateway address
     set device "port1"
    next
   end
```

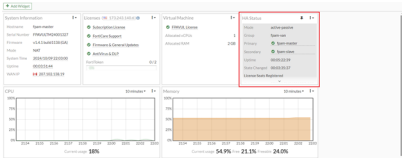
c. Set the network interface based on the IP address assignment table in IP address assignments:

```
  config system interface
   edit "port1"
    set ip 10.59.112.158 255.255.255.0
    set allowaccess ping ssh
    set type physical
    set snmp-index 1
   next
   edit "port2"
    set ip 10.1.100.12 255.255.255.0
    set allowaccess ping ssh
    set type physical
    set snmp-index 2
   next
  end
```

d. Configure HA:

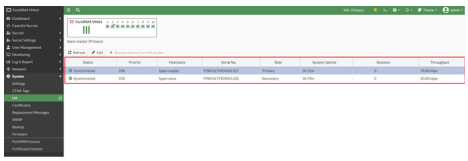
```
config system ha
 set group-id 101 #use the same group-id within the cluster
 set group-name "fpam-ha-dr" #use the same group-name within the cluster
 set mode active-passive
 set password 123 #use the same password within the cluster
 set hbdev "port2"0 #set the heartbeat interface and priority; same priority level
within a cluster
 set override enable
 set priority 200 #instance priority; keep the secondary instance priority lower
than the primary instance
 set unicast-status enable
 config unicast-peers
  edit 1
   set peer-ip 10.1.100.11 #The primary instance heartbeat interface IP address
  next
 end
end
```

3. Check the HA status:
   a. Reboot the two FortiPAM-VM instances.
   The following shows the HA sync status in the *Dashboard*:



   b. On the primary FortiPAM, go to *System* > *HA* to check the HA status is synchronized.

The HA synchronization takes a few minutes.



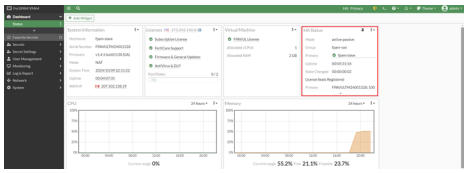
In the CLI console, enter `get system ha status` to check the HA status.

The primary and the secondary instances must display in-sync status in the CLI console.

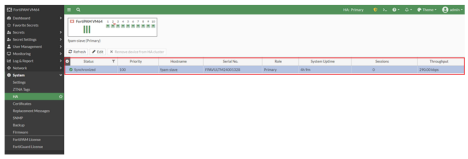
```
get system status
HA Health Status: OK
Model: FortiPAM-VM64
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 5:24:12
Cluster state change time: 2024-10-09 18:27:21
```

```
Primary selected using:
  .
  .
  .
  .
Configuration Status:
  FPAVULTM2024001327 (updated 4 seconds ago): in-sync
  FPAVULTM2024001328 (updated 1 seconds ago): in-sync
  .
  .
  .
```

4. HA failover:
   a. Shutdown the primary FortiPAM instance.
   b. Verify that the secondary FortiPAM instance has become the primary in the secondary FortiPAM GUI *Dashboard*.



   c. In the secondary FortiPAM, go to *System* > *HA*.
   Only one node remains.



   d. Power on the primary FortiPAM.
   e. Wait a few minutes for the HA synchronization to complete.
   The HA status recovers between the primary and the secondary FortiPAM.

Appendix V: Terraform- FortiPAM as a provider

Fortinet's Terraform support provides customers with more ways to efficiently deploy, manage, and automate security across physical FortiPAM appliances and virtual environments. You can use Terraform to automate various IT infrastructure needs, thereby diminishing mistakes from repetitive manual configurations.

The FortiPAM terraform provider offers resource management for secrets and folders on the FortiPAM appliance or VM as a data center target.

For example, if Fortinet is releasing a new FortiPAM version, your organization may require you to test a new functionality to determine how it may impact the environment before globally deploying the new version. In this case, the ability to rapidly stand up environments and test these functions prior to production environment integration provides a resource-efficient and fault-tolerant approach.

The FortiPAM Provider Terraform Registry is available on:

https://registry.terraform.io/providers/fortinetdev/fortipam/latest

The FortiPAM Provider Terraform Source Code is available on:

https://github.com/fortinetdev/terraform-provider-fortipam

FortiPAM terraform provider

The FortiPAM terraform provider offers secret CRUD operations on FortiPAM appliance or VM with secret name.

Requirements

1. FortiPAM 1.5.0 or later.
2. FortiPAM Provider: The example uses `terraform-provider-fortipam 1.0.0`.
3. Terraform: The example uses `Terraform v1.9.6`.
4. A REST API user created on FortiPAM with the API token.

Generating an API token on FortiPAM

The FortiPAM Terraform Provider can use the API token to be authenticated for FortiPAM. An API token is generated by creating a new REST API user.



The steps shown below can be performed from the FortiPAM GUI or the CLI using an administrator account with the *Super Administrator* user role.

To generate an API token in the GUI:

1. Go to *User Management* > *User List*, and select *Create*.
   The *New User* wizard opens.

2. From *User Privilege* pane, select *Standard User*, and click *Next*.
3. From the *User Type* pane, select *API User*, and click *Next*.
4. In the *User Details* pane:
   a. In *Username*, enter a name.
   b. In *Language*, select *English*.
   c. Optionally, enter comments.
   d. Click *Next*.
5. Click *Next*.
6. Review the settings.
7. Click *Submit*.
   The *New API key for test* window opens with the new API key.



Click *Close*.

If the token is not displayed on the GUI, click the recently created API user, and select *Re-generate API Key*.

In the CLI console, use the following commands to create an API user:

```
config system api-user
 edit "api-user"
  set accprofile "pam_standard_user"
 next
end
```

Run `execute api-user generate-key <API_USER_NAME>`, e.g., `execute api-user generate-key api_user` to generate the token for the API user.

Make note of the API token as it is only displayed once and cannot be retrieved.

Terraform task

1. Secret and folder example:

```
...
 terraform {
  required_providers {
   fortipam = {
    source = "fortipam.com/local/fortipam"
    version = "1.0.0"
   }
  }
 }
 provider "fortipam" {
```

```
base_url = "<fortipam host ip>"
access_token = "<api token>"
verify_ssl = false
}
#new secret field value
locals {
 fields = [
   {
    "name" = "Host",
    "value" = "<host value>"
   },
   {
    "name" = "Username",
    "value" = "<user name>"
   },
   {
    "name" = "Password",
    "value" = "<password name>"
   },
  ]
 }
#new folder resource
resource "fortipam_resource_folder" "folder" {
 parent = "<parent_folder_name>"
 name = "<new_folder_name>"
}



#new secret resource
resource "fortipam_resource_secret" "new_secret" {
 provider = fortipam.fpam-vault
 name = "<new secret name>"
 path = "<secret folder path>"
 template = "Unix Account (SSH Password)" # <secret template>
 dynamic "fields" {
  for_each = local.fields
  content {
   name = fields.value.name
   value = fields.value.value
  }
 }
}
output "job_status" {
 value = "secret created successfully"
}

....
```

Performing Terraform Task

1. `terraform init`: Initializes the working directory. Downloading provider plugins and setting up the backend.
2. `terraform plan`: Generates and displays the execution plan detailing the changes that Terraform makes to the secret.

When you intend to update a secret information:

a. Modify any secret field value that needs update.

b. Keep the rest of the fields.

c. Replan the task.

The command output indicates the field value that is updated.

For example, when you update the Host value, the output is: value = "10.59.112.103" -> "10.59.112.104".

```
...
Terraform used the selected providers to generate the following execution plan.
Resource actions are indicated with the following symbols:
~ update in-place
Terraform performs the following actions:
 #fortipam_resource_secret.new_secret will be updated in-place
 ~ resource "fortipam_resource_secret" "new_secret" {
     id = "7"
     name = "terraform_fake_secret"
     # (2 unchaged attributes hidden)
     ~ fields {
        name = "Host"
        ~ value = "10.59.112.103" -> "10.59.112.104"}
        # (2 unchanged blocks hidden)
     }
    Plan: 0 to add, 1 to change, 0 to destroy.
```

3. `terraform apply`: Applies the changes defined in the execution plan to read, create, and update the secret information.

4. `terraform destory`: Delete the secret in the remote target.

Secret import example

```
 ...
 #import resource secret by secret id in the target FortiPAM
resource "fortipam_resource_secret"{
}
...
```

Using command with secret ID to import the secret field value and output it to `terraform.tfstate` file as plain text.

```
 ...
 terraform import fortipam_resource_seret.sec <sec_id>
 ...
```

Secret import example

```
 ...
 import {
  to = fortipam_resource_secret.importSec
  id = "<sec_id>"
}
 ...
```

Using the command to output the secret field value to another `generated.tf` file besides `terraform.tfstate`.

```
  terrfaform plan -generate-config-out=generated.tf
```

Appendix W: Installation on Proxmox

Purpose

This document provides a comprehensive guide for installing FortiPAM on Proxmox, a robust open-source hypervisor platform using KVM virtualization.

Scope

The document covers the complete scope for creating and configuring a FortiPAM.

Prerequisites

System requirements

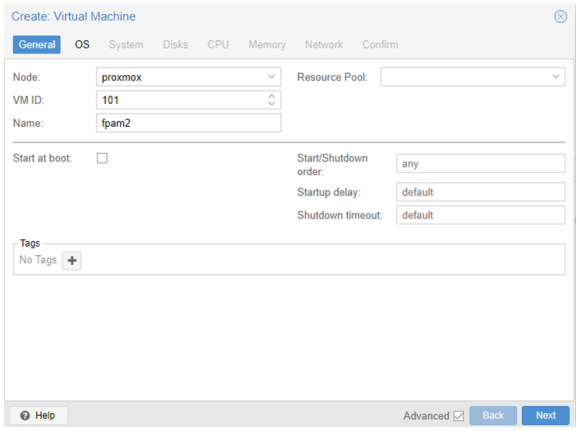
- Proxmox VE (Virtual Environment) installed
- `fortipam.qcow2` disk image
- Administrative access to the Proxmox server
- Stable network configuration

Creating the FortiPAM-VM on Proxmox

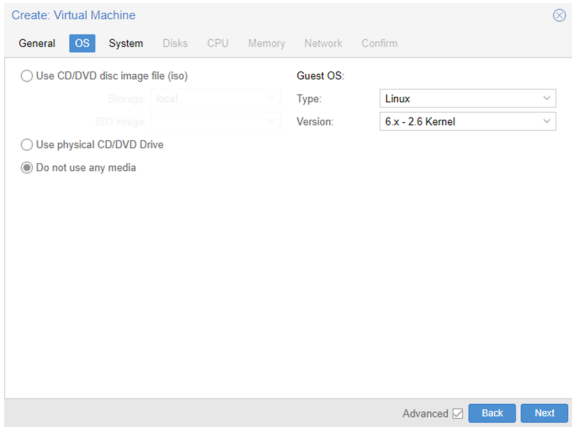
To create the FortiPAM-VM on Proxmox:

1. Log in to the Proxmox web interface.
2. Go to *Datacenter* > *Storage,* and select the storage where you want to store FortiPAM files.
3. Go to *Content*, click *Upload*, and upload the FortiPAM disk image file.
4. Go to the Proxmox node where the VM will be created.

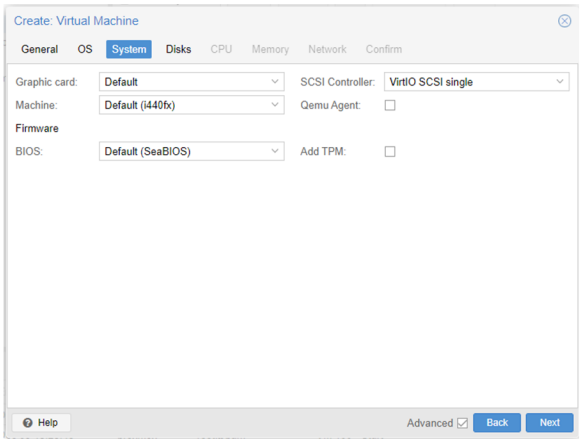
5. Click *Create VM* and configure the following:
   a. In the *General* tab, enter a name for the VM, and click *Next*.



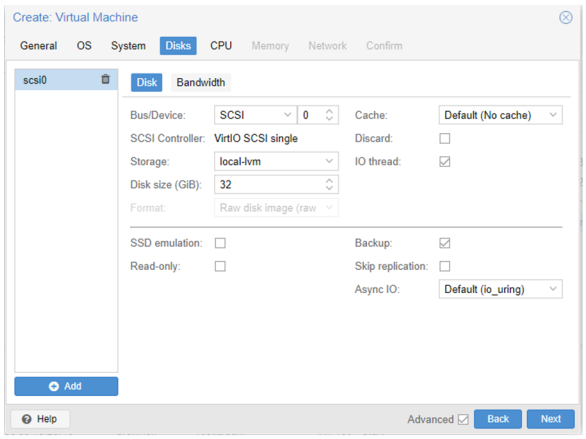
   b. In the *OS* tab, select *Do not use any media*, and select *Next*.



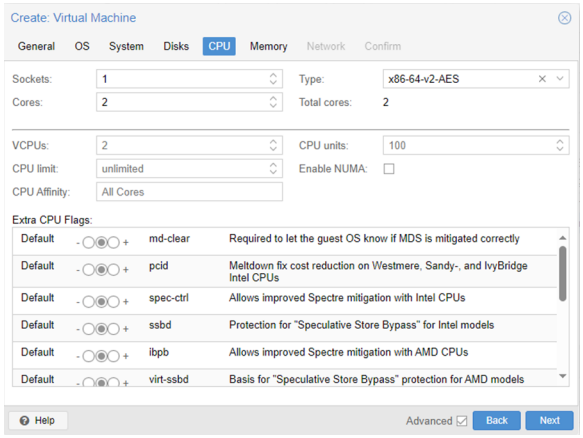
   c. In the *System* tab, keep the default values, and click *Next*.



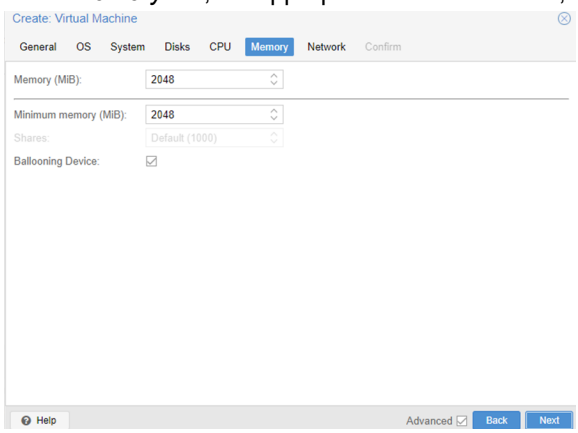
   d. In the *Disks* tab, configure the log disk size, and click *Next*.



e. In the *CPU* tab, assign cores based on the anticipated workload, and click *Next*.



f. In the *Memory* tab, set appropriate RAM allocation, and click *Next*.



g. In the *Network* tab, select *No network device*, and click *Next*.
Alternatively, add a network device if the intended device is already known.

h. Click *Finish* to complete the VM setup.

Disk image transfer

The VM has been created, but there is no operating system yet. We transfer the `fortipam.qcow2` file to the Proxmox machine.

We use SCP to perform the disk image transfer.

```
scp fortipam.qcow2 root@proxmox-server-IP:/root/
```

Importing the disk image

To import the disk image:

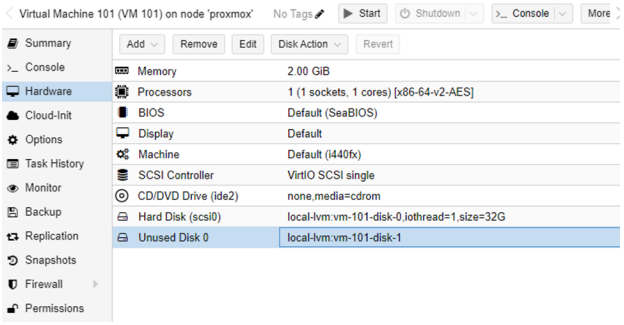
1. Go to the Proxmox Shell and import the disk image to the VM manually.

   ```
   qm importdisk <VMID> fortipam.qcow2 local-lvm
   ```

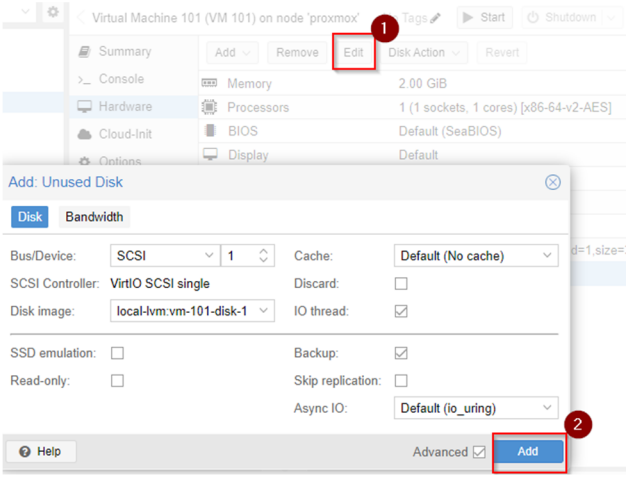
   If the storage `local-lvm` does not exist, import the disk image using the following command:

   ```
   qm importdisk <VMID> fortipam.qcow2 local
   ```

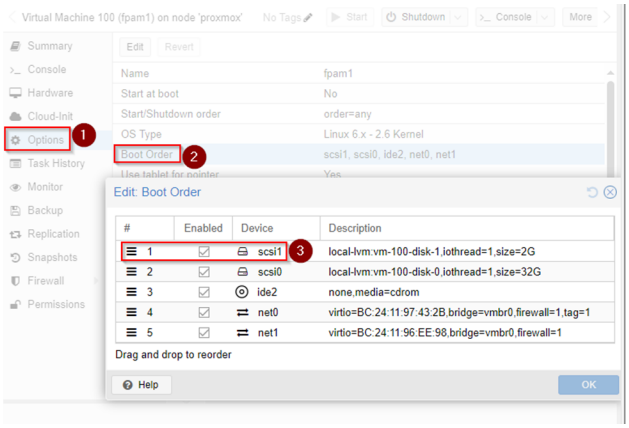
   The disk image is visible when inspecting the FortiPAM-VM.



2. Click the *Unused Disk 0*, click *Edit*, and click *Add*.



3. Change the boot order in *Options* to ensure that the VM is booted from the new disk image.



Network configuration

Attaching Linux bridge interfaces (`vmbrX`)

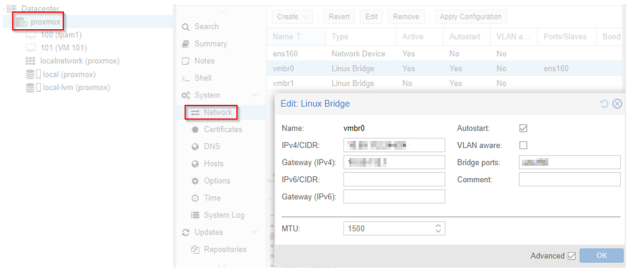
On Proxmox, you can attach Linux bridge `vmbrX` interfaces to the VM.

Each of these bridges are associated with a physical network adapter. Depending on the intended use cases, it is possible to attach the same bridge multiple times onto a VM.

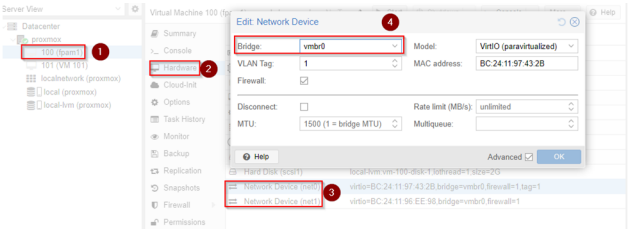
In this example, a bridge is attached to the VM.

To attach the Linux bridge interface:

1. Select the node, go to *Network*, and edit the Linux bridge.



2. Attach the bridge to the VM network.



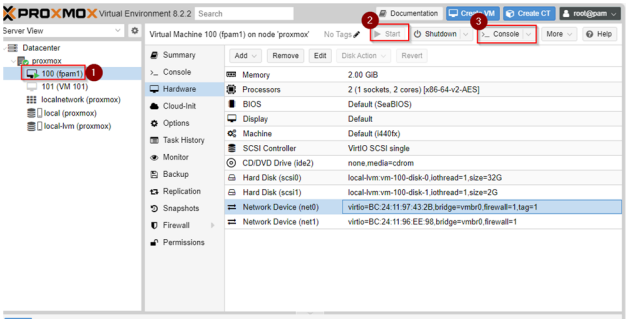
The Linux bridge VLAN can detect all the VLANs on the physical port.

Upon attaching the interface to the VM in Proxmox, it allows all the VLANs on the bridge unless a VLAN ID is specified.

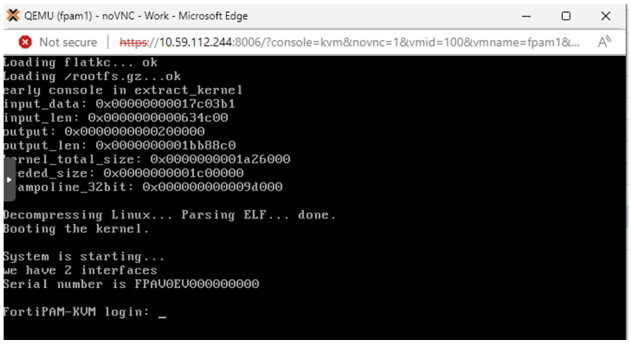
Accessing the FortiPAM-VM

To access the FortiPAM-VM on Proxmox:

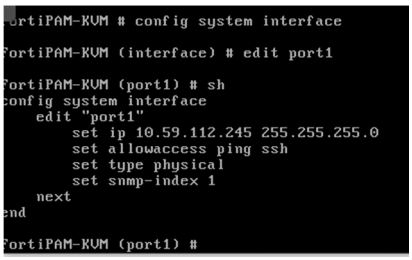
1. On the Proxmox web UI, start the FortiPAM-VM.



2. Go to the console to interact with the VM.
3. Log in to FortiPAM-VM and confirm that the network interfaces show up correctly.



4. Set up the IP address to connect to the FortiPAM GUI using the CLI commands shown below.



5. Use the following CLI commands to set up the gateway.



Appendix X: Deploying FortiPAM-VM HA on AWS between multiple zones

This guide provides sample configuration for Active-Passive FortiPAM-VM High Availability (HA) on AWS between multiple zones.

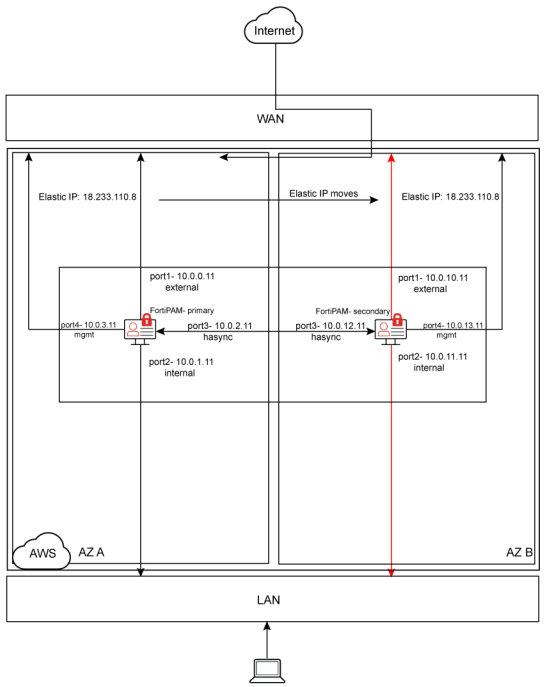
You can configure FortiPAM native HA feature without using an AWS supplementary mechanism with two FortiPAM instances: one acting as the primary node and the other as the secondary node located in two different availability zones (AZs) within a single VPC.

You can configure a pair of FortiPAM 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 with the same Elastic IP address. Endpoints continue to communicate with the external resources over the FortiPAM.

This gives FortiPAM the ability to recover in the event of a catastrophic failure. In the case where both FortiPAM devices are located in the same AZ and that AZ fails, both FortiPAM go down and HA is unusable. Therefore, there is a need to support HA configuration where both FortiPAM devices are in separate AZs.

How to configure FortiPAM HA on the AWS platform

HA deployment topology



FortiPAM- Primary IP addresses

Port	FortiPAM interface IP address	AWS primary address	AWS subnet	Public IP address
Port 1	10.0.0.11(WAN)	10.0.0.11	10.0.0.0/24 (EIP)	FortiPAM GUI VIP
Port 2	10.0.1.11(LAN)	10.0.1.11	10.0.1.0/24	
Port 3	10.0.2.11(HB)	10.0.2.11	10.0.2.0/24	
Port 4	10.0.3.11 (MGMT)	10.0.3.11	10.0.3.0/24 (EIP)	MGMT IP address

FortiPAM- Secondary IP addresses

Port	FortiPAM interface IP address	AWS primary address	AWS subnet	Public IP address
Port 1	10.0.10.11(WAN)	10.0.10.11	10.0.10.0/24 (EIP)	FortiPAM GUI VIP
Port 2	10.0.11.11(LAN)	10.0.11.11	10.0.11.0/24	
Port 3	10.0.12.11(HB)	10.0.12.11	10.0.12.0/24	
Port 4	10.0.13.11 (MGMT)	10.0.13.11	10.0.13.0/24 (EIP)	MGMT IP address

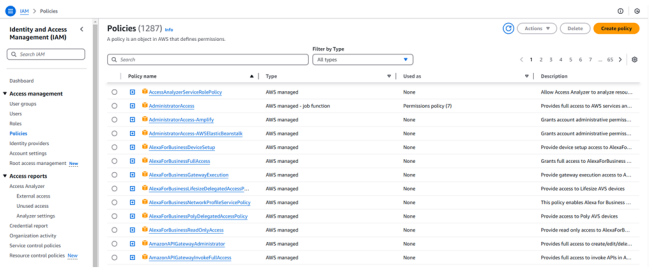
Prerequisites

- Creating a custom permission policy on page 682
- Creating an IAM role on page 683
- Creating a VPC on page 685
- Creating subnets on page 686
- Creating an internet gateway on page 687
- Configuring routing tables on page 688
- Creating network interfaces on page 690
- Creating elastic IP addresses on page 691

Creating a custom permission policy

To create a custom permission policy:

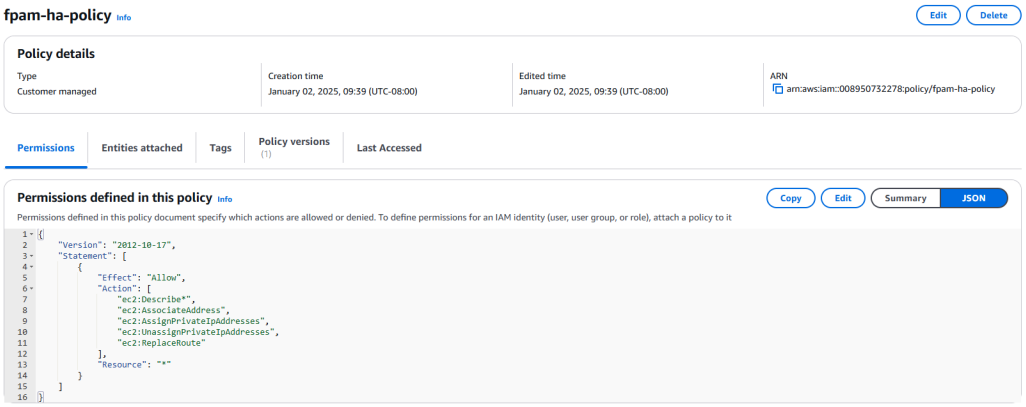
1. In the AWS console, open *IAM*.
2. From the *Dashboard*, go to *Access management* > *Policies*.
   The *Policies* window opens.



3. Select *Create policy*.
4. Select *JSON*.
5. The following shows the minimum sufficient IAM roles required for this deployment.

```
{
 "Version": "2012-10-17",
 "Statement": [
   {
    "Effect": "Allow",
    "Action": [
      "ec2:Describe*",
      "ec2:AssociateAddress",
      "ec2:AssignPrivateIpAddresses",
      "ec2:UnassignPrivateIpAddresses",
      "ec2:ReplaceRoute"
    ],
    "Resource": "*"
  }
 ]
}
```

6. Click *Next*.
7. In *Policy name*, enter a name for the policy.
8. Optionally, enter a description for the policy.
9. Click *Create policy*.



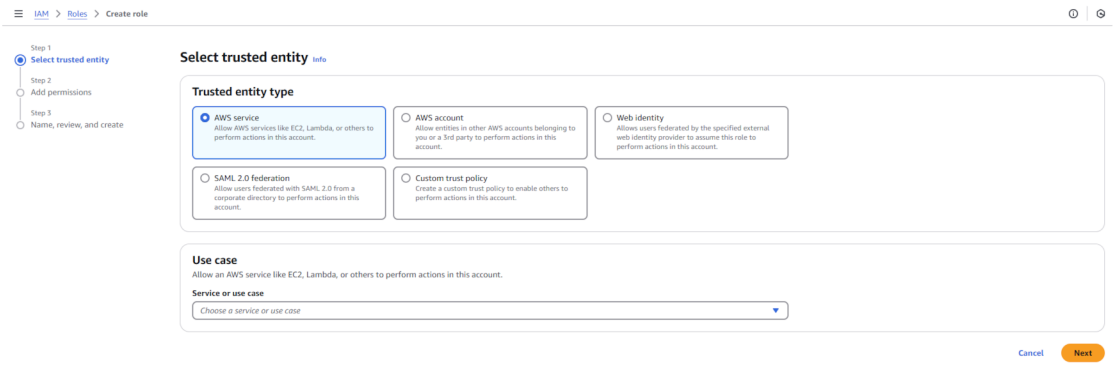
Creating an IAM role

The IAM role is necessary for HA failover.

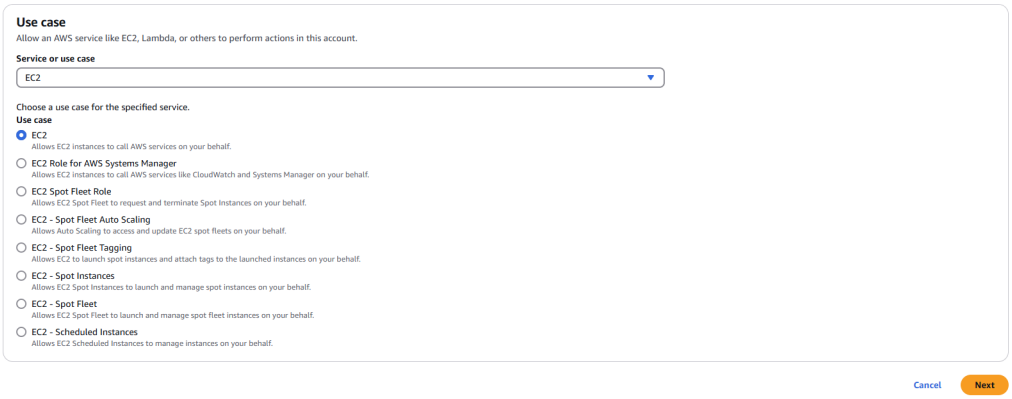
Ensure that the IAM role can read and write EC2 information to read, detach, and reattach network interfaces and edit routing tables.

To create an IAM role:

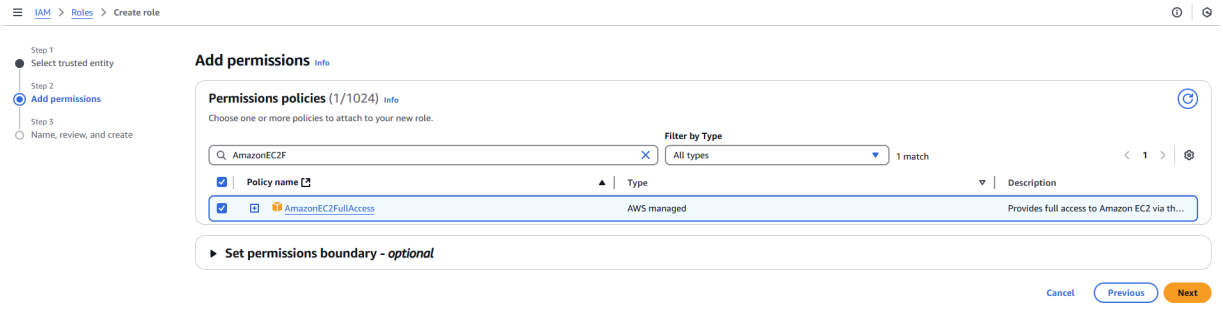
1. In the AWS console, open *IAM*.
2. From the *Dashboard*, go to *Access management* > *Roles*.
3. Select *Create role*.
   The *Select trusted entity* wizard opens.



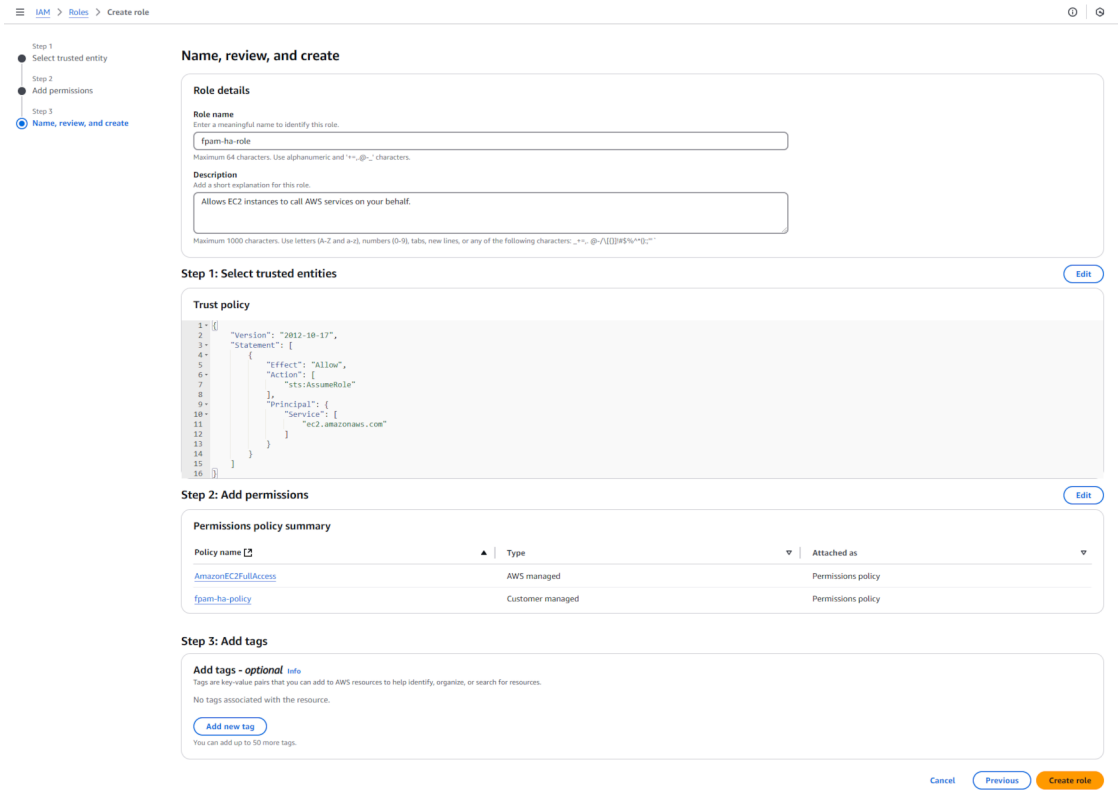
4. From *Trusted entity type*, select *AWS service*.
5. In *Use case*, select *EC2*.



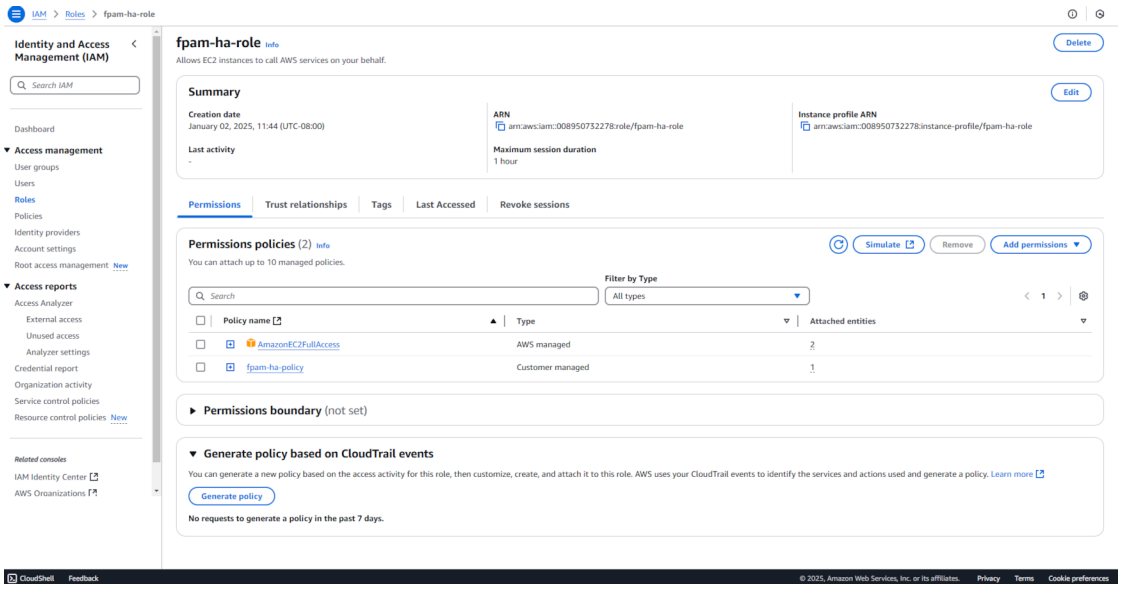
6. Click *Next*.
   The *Add permissions* window opens.
7. From the permission policies list, select *AmazonEC2FullAccess* and the policy created in Creating a custom permission policy on page 682, and click *Next*.



8. In the *Role details* pane, enter a name for the role.



9. Select *Create role*.



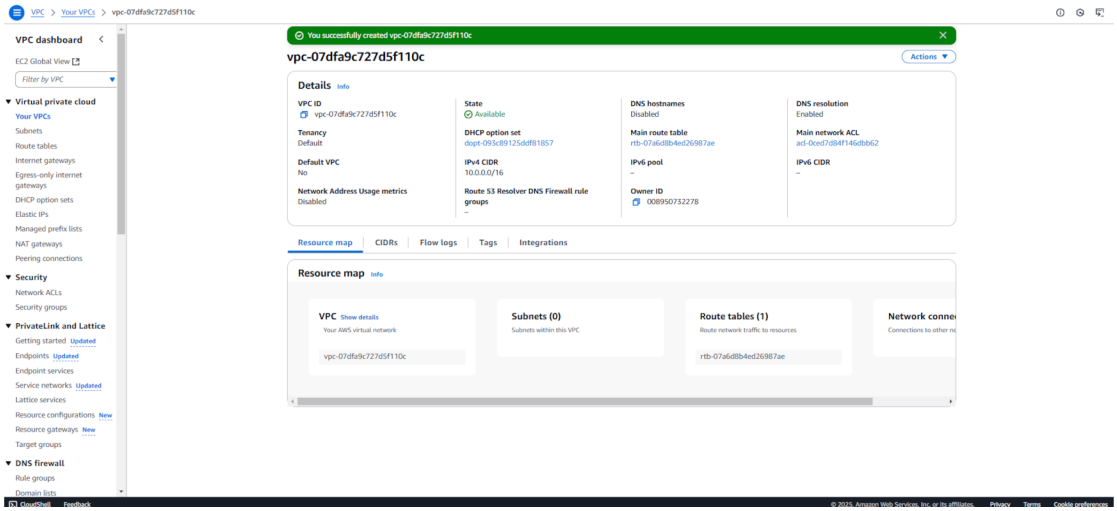
Creating a VPC

We create a VPC with eight 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. In *IPv4 CIDR*, enter `10.0.0.0/16`.
4. Keep the default settings.
5. Select *Create VPC*.



Creating subnets

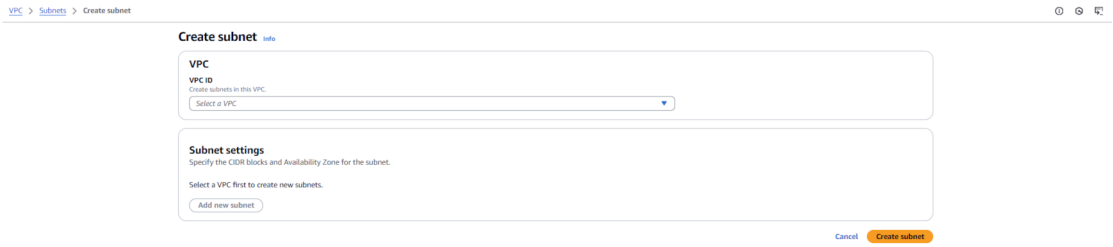
We create eight subnets.

The eight subnets are as follows:

- **Four in AZ A**:
  - Public WAN: `10.0.0.0/24`
  - Internal network: `10.0.1.0/24`
  - Hearbeat network: `10.0.2.0/24`
  - Management network: `10.0.3.0/24`
- **Four AZ B**:
  - Public WAN: `10.0.10.0/24`
  - Internal network: `10.0.11.0/24`
  - Heartbeat network: `10.0.12.0/24`
  - Management: `10.0.13.0/24`

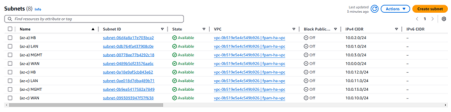
To create a subnet:

1. In the VPC created in Creating a VPC on page 685, go to *Virtual private cloud* > *Subnets*.
2. Select *Create subnet*.
   The *Create subnet* wizard opens.



3. From the *VPC ID* dropdown, select the VPC created in Creating a VPC on page 685.
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.

   The following displays the eight subnets.



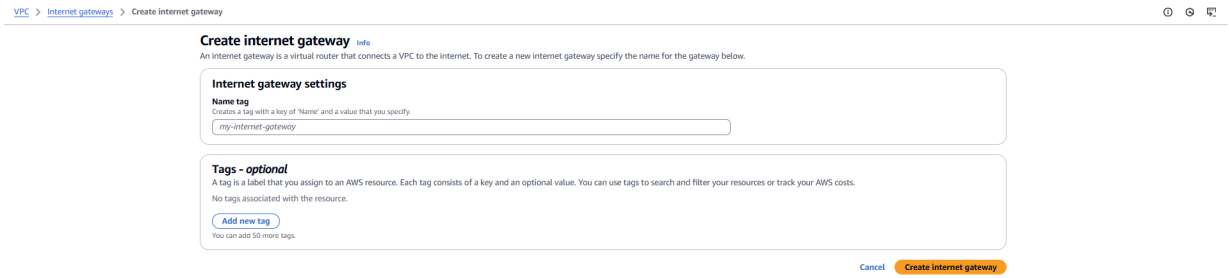
Creating an internet gateway

We create a new gateway and attach it to the newly created VPC in Creating a VPC on page 685.

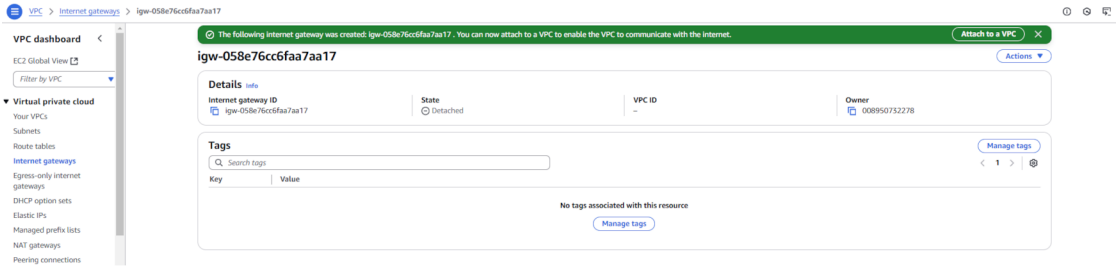
The internet gateway takes charge of the VPC to communicate to the public internet.

To create an internet gateway:

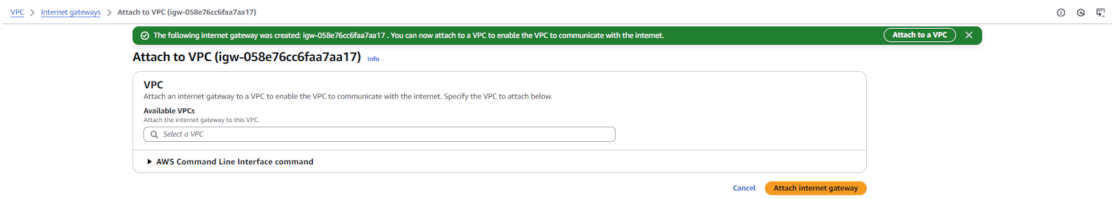
1. In VPC, go to *Virtual private cloud* > *Internet gateways*.
2. From the internet gateways list, select *Create internet gateway*.
   The *Create internet gateway* wizard opens.



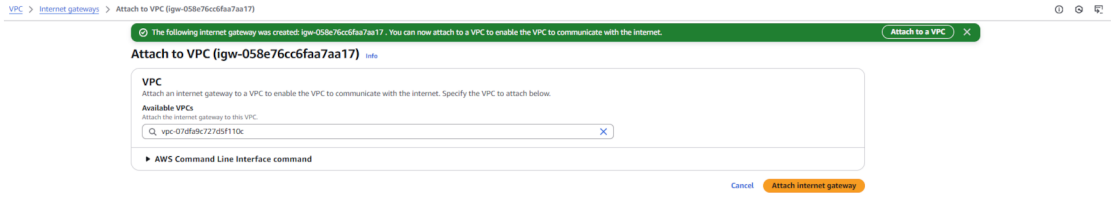
3. Enter a name for the tag.
4. Click *Create internet gateway*.
   The internet gateway is created.



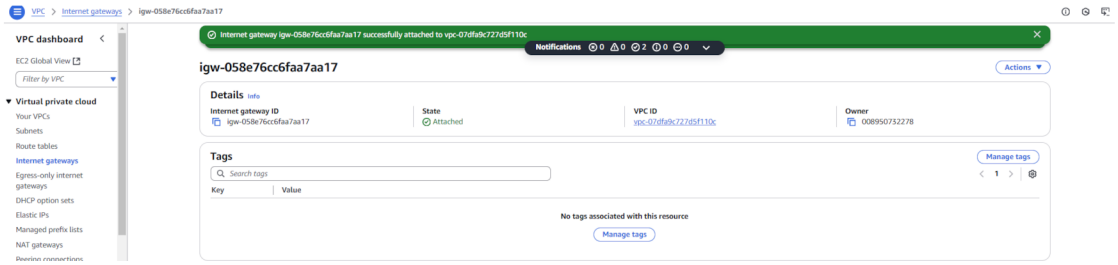
5. From the green banner, select *Attach to a VPC*.
   The *Attach to VPC* window opens.



6. From *Available VPCs*, select the VPC created in Creating a VPC on page 685.



7. Click *Attach internet gateway*.
   The internet gateway is attached to the VPC.

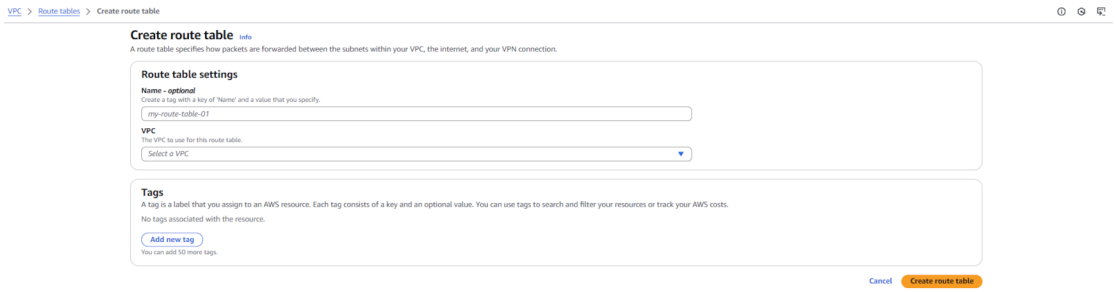


Configuring routing tables

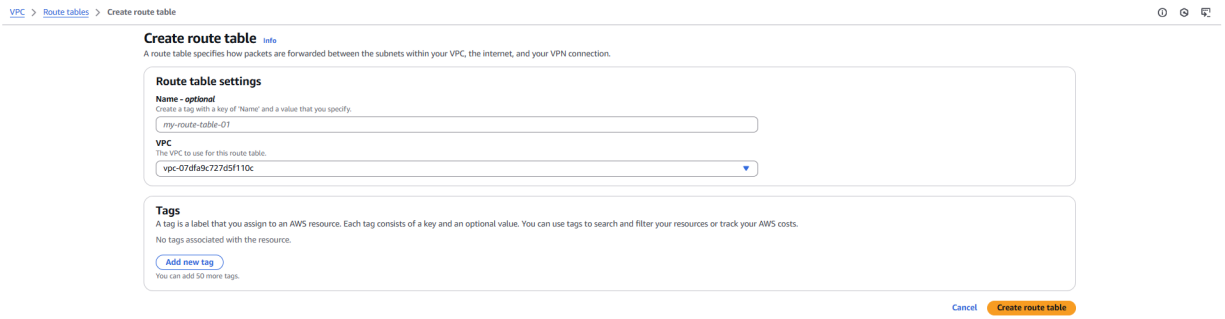
Two routing tables needs to be configured.

To configure a 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.



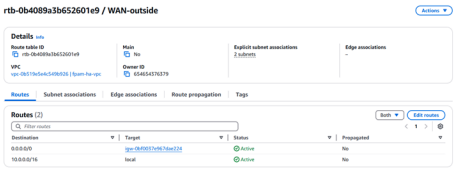
2. From the *VPC* dropdown, select the VPC created in Creating a VPC on page 685.

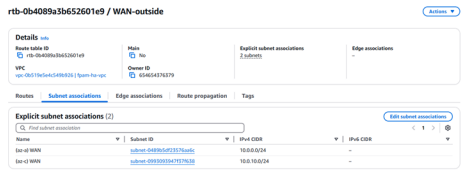


3. Select *Create route table*.

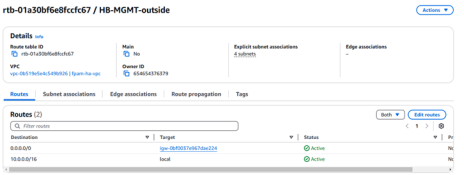
   The routing table is created.

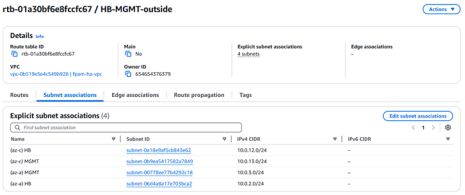
   The following shows the public WAN routing table. Ensure to point `0.0.0.0/0` CIDR to the internet gateway.



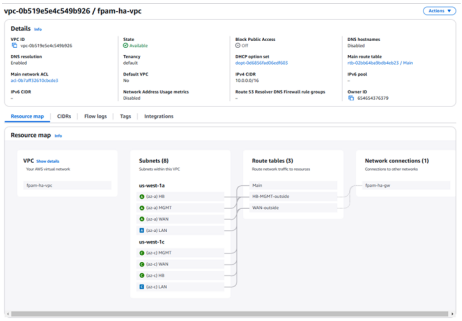


   The following shows the heartbeat and management networks routing table.





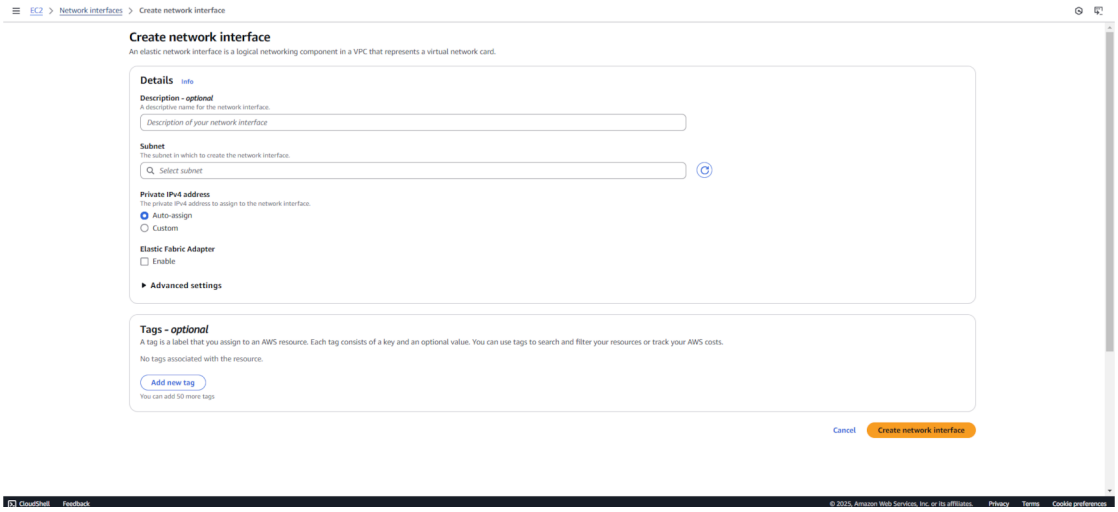
   After all the VPC, subnets, gateways, and routing tables are configured, the VPC configuration looks like the following:



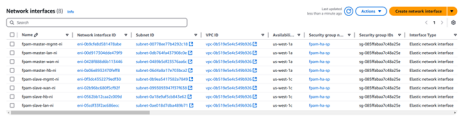
Creating network interfaces

To create network interface:

1. Go to *EC2* > *Network & Security* > *Network Interfaces*.
   The *Network interfaces* window opens.
2. From the right, select *Create network interface*.
   The *Create network interface* wizard opens.



3. Optionally, enter a description.
4. From the *Subnets* dropdown, select one of the subnets created in Creating subnets on page 686.
5. In the *Security groups* pane, select a security group.
   To configure a security group, see *Configuring a security group* in the latest *FortiPAM AWS Administration Guide*.
6. 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.



Creating elastic IP addresses

To create elastic IP address:

1. Go to *EC2* > *Network & Security* > *Elastic IPs*.
   Setting up the environment requires three elastic IP addresses.
   a. One FortiPAM GUI VIP.
   b. One FortiPAM primary management IP address.
   c. One FortiPAM secondary management IP address.
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.
   After successfully created EIPs, you should manually associate the EIP to the network interface private IP address.



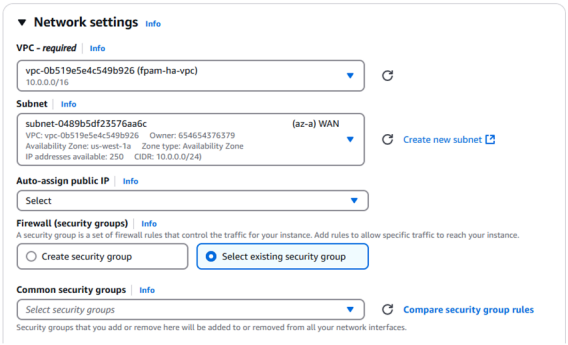
Installing and configuring FortiPAM instances on AWS

- Configuring FortiPAM instance on page 691
- Launching FortiPAM instance on page 692
- Configuring FortiPAM HA on page 693
- Testing and debugging HA failover on page 696

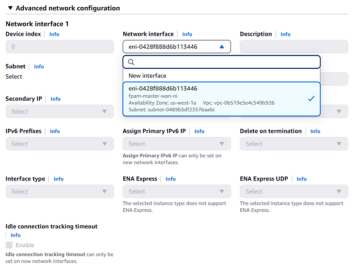
Configuring FortiPAM instance

To configure FortiPAM instance:

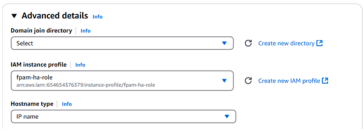
1. Upload FortiPAM image and create the FortiPAM AMI.
   See Appendix J: Installation on AWS on page 534.
   The following shows FortiPAM
2. The following shows the FortiPAM instance network settings with VPC, public WAN subnet, and the security group created beforehand.



3. In *Advanced network configuration*, attach the four network interfaces created in Creating network interfaces on page 690 to the FortiPAM instance.



4. In *Advanced details*, attach HA role to the FortiPAM instance.

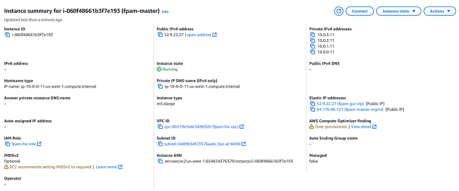


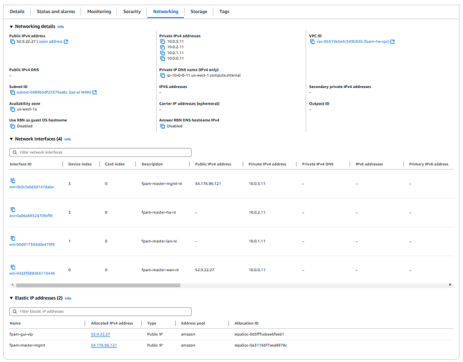
Launching FortiPAM instance

The following shows the main configurations and network settings for the primary and the secondary FortiPAM instances.

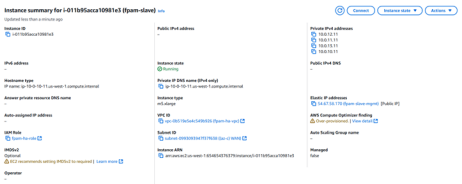
Currently, both the FortiPAM GUI VIP and the `port1` IP address are attached to the main FortiPAM instance.

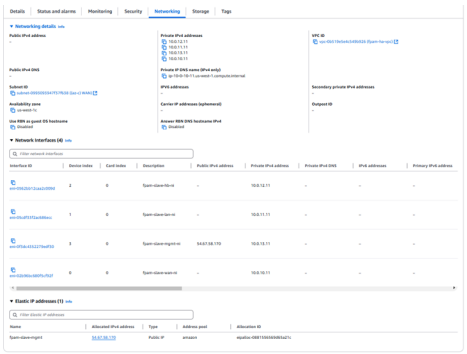
FPAM_MAIN





FPAM_SECONDARY





Configuring FortiPAM HA

After the FortiPAM instance boots up, configure FortiPAM_PRIMARY as below:

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

```
config router static
 edit 1
  set gateway 10.0.0.1
  set device "port1"
 next
end
config system interface
 edit "port1"
 set ip 10.0.0.11 255.255.255.0
 set allowaccess ping ssh
 set type physical
 set alias "WAN"
 set snmp-index 1
 set mtu-override enable
 set mtu 9001
next
edit "port2"
 set ip 10.0.1.11 255.255.255.0
 set allowaccess ping ssh
 set type physical
 set alias "LAN"
 set snmp-index 2
next
edit "port3"
 set ip 10.0.2.11 255.255.255.0
 set allowaccess ping ssh
 set type physical
 set alias "HB"
 set snmp-index 3
next
edit "port4"
 set ip 10.0.3.11 255.255.255.0
 set allowaccess ping ssh
 set type physical
 set alias "MGMT"
 set snmp-index 4
next
```

```
 end
 config system ha
  set group-name "fpam"
  set mode active-passive
  set password XXXXXXX #change into your personal password, primary and secondary should
use the same
  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 255
  set unicast-status enable
  set unicast-gateway 10.0.2.1
  config unicast-peers
   edit 1
    set peer-ip 10.0.12.11
   next
  end
 end
 config system vdom-exception
  edit 1
   set object system.interface
  next
  edit 2
   set object router.static
  next
  edit 3
   set object firewall.vip
  next
  edit 4
   set object user.saml
  next
  edit 5
   set object system.ftm-push
  next
 end
```

Configure FortiPAM_SECONDARY as below:

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

```
 config router static
  edit 1
   set gateway 10.0.10.1
   set device "port1"
  next
 end
 config system interface
  edit "port1"
   set ip 10.0.10.11 255.255.255.0
   set allowaccess ping ssh
   set type physical
```

```
     set alias "WAN"
     set snmp-index 1
     set mtu-override enable
     set mtu 9001
    next
    edit "port2"
     set ip 10.0.11.11 255.255.255.0
     set allowaccess ping ssh
     set type physical
     set alias "LAN"
     set snmp-index 2
    next
    edit "port3"
     set ip 10.0.12.11 255.255.255.0
     set allowaccess ping ssh
     set type physical
     set alias "HB"
     set snmp-index 3
    next
    edit "port4"
     set ip 10.0.13.11 255.255.255.0
     set allowaccess ping ssh
     set type physical
     set alias "MGMT"
     set snmp-indext 4
    next
    edit "ssl.root"
     set type tunnel
     set alias "SSL VPN interface"
     set snmp-index 5
    next
   end
   config system ha
    set group-name "fpam"
    set mode active-passive
    set password XXXXXXX #change into your personal password, primary and secondary
should use the same
    set hbdev "port3" 0
    set ha-mgmt-status enable
    config ha-mgmt-interfaces
     edit 1
      set interface "port4"
      set gateway 10.0.13.1
     next
    end
    set override enable
    set unicast-status enable
    set unicast-gateway 10.0.12.1
    config unicast-peers
     edit 1
      set peer-ip 10.0.2.11
     next
    end
   end
   config system vdom-exception
    edit 1
```

```
    set object system.interface
  next
  edit 2
    set object router.static
  next
  edit 3
    set object firewall.vip
  next
  edit 4
    set object user.saml
  next
  edit 5
    set object system.ftm-push
  next
 end
```

Testing and debugging HA failover



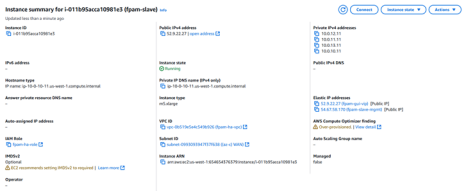
After finishing configuration in the both the primary and secondary instance, manually reboot the two instances.

1. In the CLI console, enter the following command to verify that FortiPAM units are in sync:

   ```
   get system ha
   ```

2. In the FortiPAM GUI, create a secret.
   To create a secret, Creating a secret on page 71.
3. Verify that you can launch the secret.
   See Launching a secret on page 99.
4. Before you power off `FPAM-PRIMARY`, you can see the VIP (`52.9.22.27`) is associated with `FPAM-SECONDARY` WAN (`port1`) interface.
5. Power off `FPAM-PRIMARY`.
6. Wait for five seconds and you can relogin to the FortiPAM GUI successfully.
7. Launch the secret created in step 2.
   You should be able to successfully launch the secret.
8. Check `FPAM-SECONDARY` status on AWS, you can see the VIP (`52.9.22.27`) is re-associated to the secondary instance.

When you SSH to the `FPAM_SECONDARY` and enable the debug command, you can power off `FPAM_PRIMARY` to trigger a failover.

```
diagnose debug en
diagnose debug application awsd -1
```

The following shows HA failover debug information:



```
diagnose de application awsd -1
diagnose de enable
HA state: primary
send_vip_arp: vd root primary 1 intf port1 ip 10.0.10.11
send_vip_arp: vd root primary 1 intf port2 ip 10.0.11.11
send_vip_arp: vd root primary 1 intf port3 ip 10.0.12.11
send_vip_arp: vd root primary 1 intf port4 ip 10.0.13.11
send_vip_arp: vd root primary 1 intf port1 ip 10.0.10.11
awsd get iam role fpam-ha-role
awsd get instance id i-011b95acca10981e3
awsd get region us-west-1
awsd get vpc id vpc-0b519e5e4c549b926
awsd checking ha status for vdom root
awsd checking elastic ip for port1
awsd associate elastic ip 52.9.22.27 to 10.0.10.11 of eni eni-
02b96bc680f5cf92f
awsd associate elastic ip 52.9.22.27 successfully
```



www.fortinet.com

Copyright© 2025 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. 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.