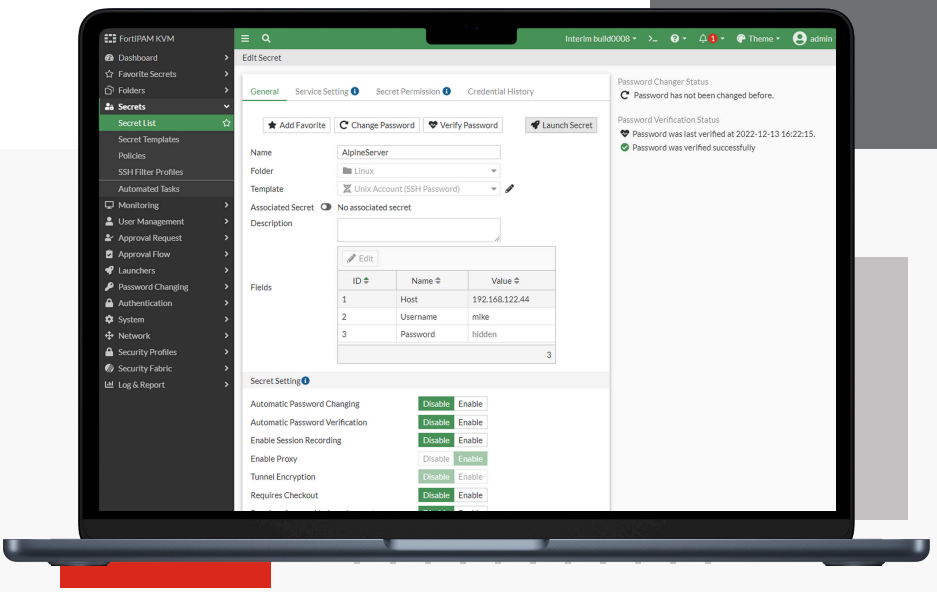
FortiPAM

Privileged Access and Session Management



Highlights

Connects, as part of Fortinet's Security Fabric, with FortiAuthenticator, FortiToken, and FortiClient for a complete IAM solution

Integrates with FortiClient EMS for zero-trust network access (ZTNA) advanced access tagging

Provides high-performance and low-latency for business-critical resources

Includes scheduled credential changing capabilities (LDAPS, Samba, SSH, SSH key)

Enables native program access with PuTTY and RDP (FCT required) along with browser-based access via Chrome, Firefox, and Edge

Account Credentials, User Access, and Activity

Privileged Access and Session Management for managing account credentials, controlling privileged user access, and monitoring activity on privileged accounts. FortiPAM ensures uptime with high availability active/standby HA capabilities.

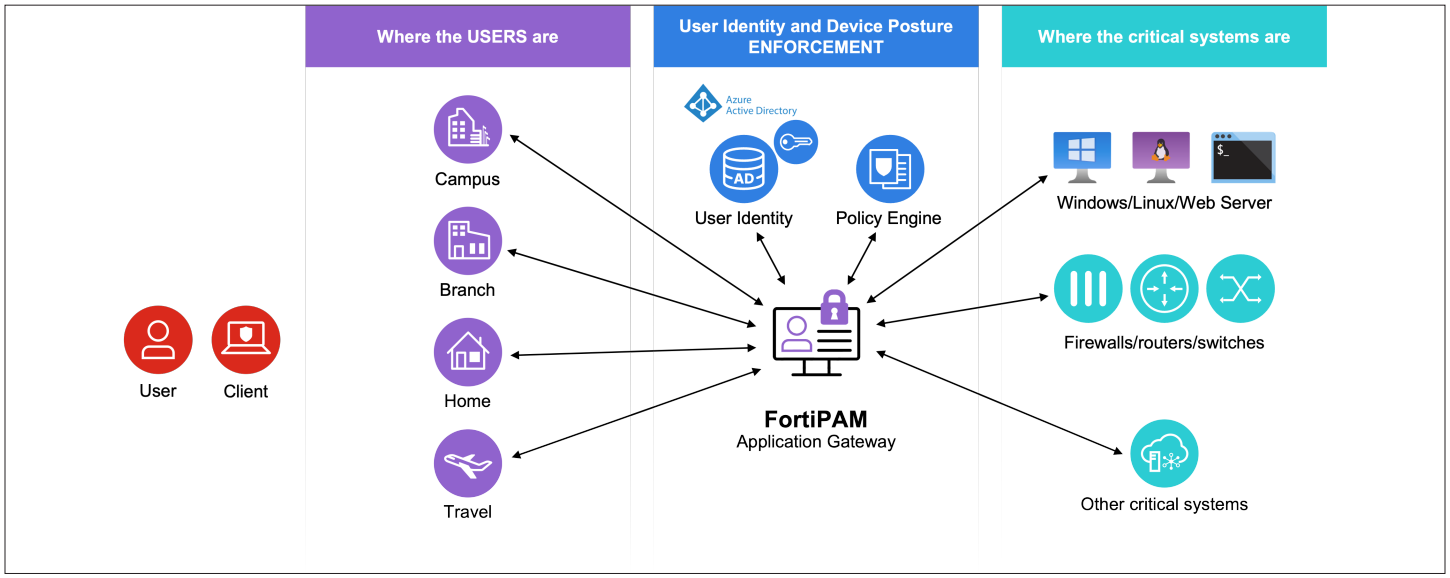
FortiPAM privileged access management provides controls over elevated privileged access and permissions for users, accounts, processes, systems, and sensitive data across the entire IT environment. FortiPAM is an integral component of the Fortinet Identity and Access Management (IAM) solution which allows organizations to provide tight security for privileged accounts and privileged credentials. FortiPAM provides tightly controlled privileged access to the most sensitive resources within an organization. It enables end-to-end management of privileged accounts, control of privileged user access, and visibility of account usage including monitoring and audit capabilities. These features allow FortiPAM to introduce zero-trust principles to privileged accounts and dramatically lower an organizations' overall attack surface.

Organizations looking to modernize IAM capabilities need to look beyond standard user identities and bring in controls for privileged accounts in the form of a PAM solution. These accounts have access to the most sensitive information which necessitates an extra level of security. FortiPAM can assist with three primary use cases when it comes to privileged accounts. These are managing account credentials, controlling privileged user access, and monitoring privileged activity.

Feature Highlights

ZTNA Elements - FortiPAM as Access Proxy

The components of a client-based ZTNA solution.



Available in

Appliance

Virtual

Manage Account Credentials

Managing privileged accounts goes beyond storing privileged credentials. It means fully automating the privileged-accounts lifecycle. Organizations often struggle with orphaned privileged accounts or ensuring these accounts have updated credential policies. FortiPAM can help manage privileged accounts by automatically changing passwords based on policy. FortiPAM owns the privileged-credential vault of specific resources so that users will not need to know the resource's credentials. This reduces the risk of the credentials falling into the wrong hands. FortiPAM also ensures that no sensitive privileged account information will be delivered to the end-user's device in proxy mode.

Control Privileged User Access

Privileged accounts need to use zero-trust principles because of the sensitive company resources they have access to. FortiPAM can bring zero-trust to these privileged accounts by ensuring that end users are only granted access to critical resources based on roles, such as standard user or administrator, and always ensuring least privilege. FortiPAM provides full controls of all resource secrets through administrator-defined central policies. These include options for automatic password changes after check-in. Organizations are also able to use FortiPAM to implement a hierarchical approval system and control risky commands.

Monitor Privileged Access

In addition to managing and controlling privileged accounts, it's just as important to provide monitoring capabilities for users of these highly sensitive resources. FortiPAM can provide reporting of privileged account usage in the case of a security incident. FortiPAM can provide full-session video recordings to provide a view of the users logged into privileged accounts, including monitoring keystrokes and mouse events. When needed for audit purposes, FortiPAM can provide full audit tracking of all privileged account usage.

Specifications

FUNCTION
User Management
Local User
Remote Authentication: LDAP Server
Remote Authentication: Radius Server
SAML
MFA: FortiToken
MFA: Email Token
MFA: SMS Token
Administrator Role Management
User Group
API User
User Trusted Host
FortiToken Cloud
Secret Folder
Public Folder
Personal Folder
Folder Permission Control
Secret Policy Management
Secret Template and Access
Unix SSH (Password or Key)
Windows Domain Account (LDAPS or Samba)
Template - FortiGate
Template - Cisco Device
Template - Web Account
Template - Machine
Custom Template
Secret
Secret Check-out/Check-in
Renew Secret Check-out
Approval Request
Verify Password
Periodical Password Changer
Password Heartbeat
Video Recording
SSH Filter
Auto Password Delivery on Native Launcher
Cisco Device Auto-Enable on Native Launcher
Associated Secret Launcher
Associated Secret Password Changer
SSH Keyboard Interactive Authentication on Native Launcher
RDP Security Level
Block RDP Clipboard
AD Target Restriction
Move/Clone a Secret
Secret Permission Control
Favorite Secrets

FUNCTION
Launcher
PuTTY (FCT required)
Remote Desktop - Windows (FCT required)
Web Launcher
Web RDP
Web SFTP
Web SMB
Web SSH
Web VNC
WinSCP
VNC Viewer (FCT required)
Tight VNC (FCT required)
Custom Launcher
Secret Request Approval
Approval Profile (up to three Tiers)
Request Review and Approve
Request Notification
Multiple Approvals Requirement
Script
Password Changer
Password Policy
Custom Password Changer
Monitor and Record
User Monitor
Active Sessions Monitor
Session Recording
Log and Audit
Events - System
Events - User
Events - HA
Logs - Secrets
Logs - Video (Record and Replay)
System
HA
Glass Breaking
Maintenance Mode
Automatic Configuration Backup
Max Duration for the Launcher Session
vTPM: KVM
vTPM: VMWare
FortiClient: Custom FCT FortiVRS (video recording daemon) Port
High Availability
Disaster Recovery support

FUNCTION
Authentication
Address (Used in AD Target Restriction)
Scheme and Rules
Stability
Long Session
Stress Test (Overload, CPU 70%)
Installation
Upgrade
Installation Doc/ Administration Guide
Security
ZTNA Tag Endpoint Control to target server and/or PAM server
2 Factor Authentication for local PAM users or remote SAML, Radius, LDAP users
Anti-Virus scanning for web-based file transfer (Web SFTP, Web SAMBA) and SCP-based file transfer
Automatic blocking of dangerous commands with SSH filtering profile
User access control based on IP and/or schedule
Secret access request/approval
Secret check-out/check-in protection
Auto password changing after check-in
Scheduled password change
High-strength SSH encryption algorithm
Advanced RDP authentication protocol including CredSSP, TLS
Role-based access control
Policy-based access profile enforcement
Trusted Platform Module to protect user private keys
Data Leak Prevention based on file types, size, or watermarks

Specifications

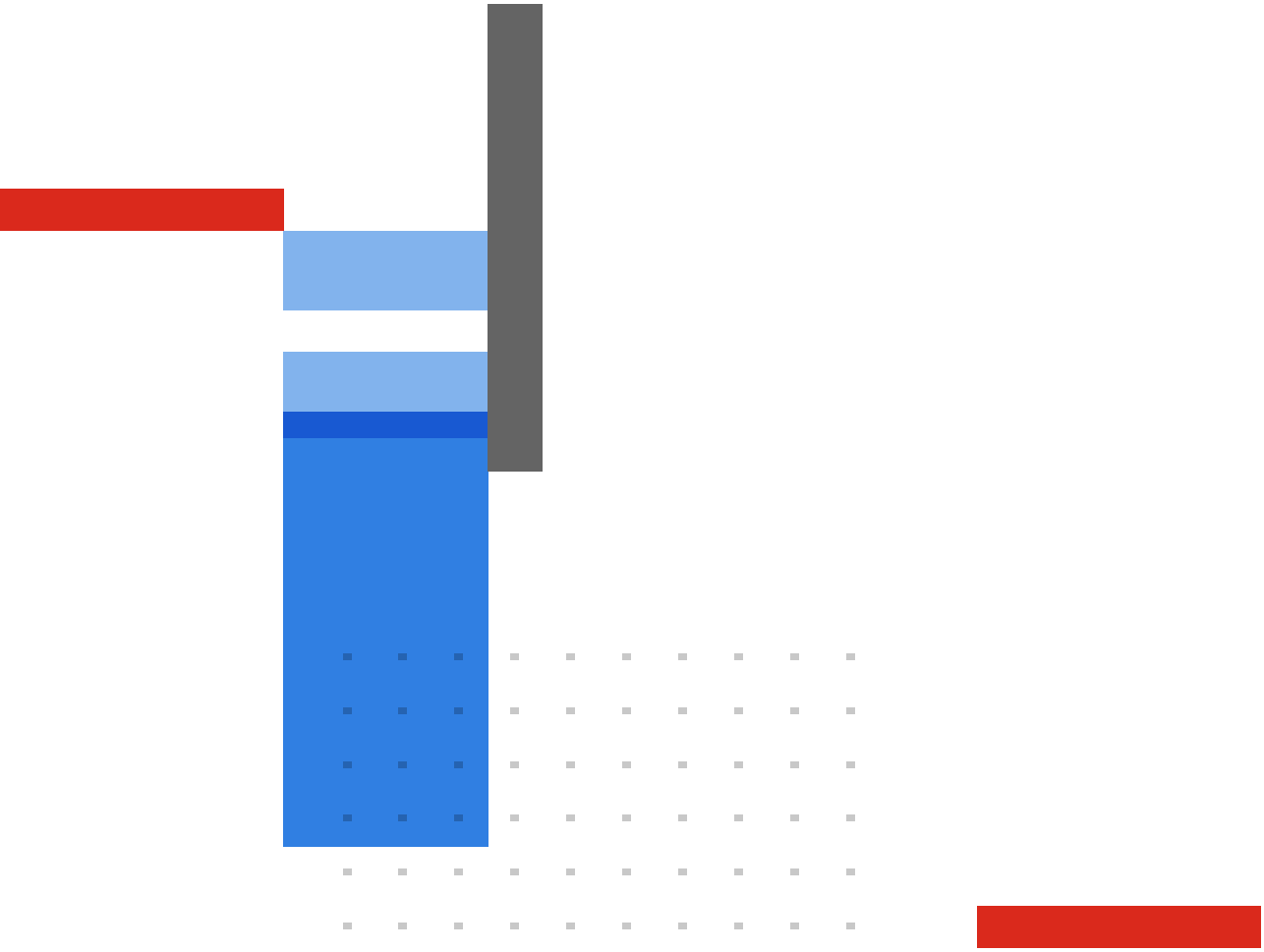
	FPA-1000G	FPA-3000G
Hardware		
10/100/1000 Interfaces (Copper, RJ-45)	4	4
SFP Interfaces	4	6
Local Storage	6× 2 TB Hard Disk Drive	6× 6 TB Hard Disk Drive
Trusted Platform Module (TPM)	Yes	Yes
Power Supply	300W Redundant Auto Ranging (100V-240V), Optional Dual (1+1)	300W Redundant Auto Ranging (100V-240V), Optional Dual (1+1)
System Capacity		
Local + Remote Users (Base)	50	100
Secrets	5000	10 000
Folders	2000	6000
Secret Requests	5000	10 000
Dimensions		
Height x Width x Length (inches)	3.5 × 17.2 × 25.5	3.47 × 17.2 × 31.89
Height x Width x Length (mm)	89 × 437 × 647	88 × 445 × 810
Weight	48.5 lbs (22 kg)	52.91 lbs (24.0 kg)
Environment		
Form Factor	2RU	2RU
Rack Mount Type	Sliding Rail	Sliding Rail
Power Source	100-240 VAC, 60-50 Hz	100-240 VAC, 60-50 Hz
Maximum Current	100-240V / 7.5-3.9A	100-240V / 10-5A
Nominal Current	12V / 45.8A ; 12Vsb / 3A	12V / 70.8A ; 12Vsb / 2.1A
Power Consumption (Average / Maximum)	233.7 W / 285.67 W	461.0 W / 563.42 W
Heat Dissipation	1008.83 BTU/h	1956.51 BTU/h
Joules/h	1064.41 (Joules/h)	2064.31 (Joules/h)
MTBF	90 600 Hours	78 937 Hours
Operating Environment and Certifications		
Operating Temperature	32°–104°F (0°–40°C)	32°–104°F (0°–40°C)
Storage Temperature	-40°–158°F (-40°–70°C)	-13°–158°F (-25°–70°C)
Humidity	5%–90% non-condensing	10%–90% non-condensing
Noise Level		
Forced Airflow		
Operating Altitude		
Compliance		
Certifications		

FPA-1000G

FPA-3000G

Ordering Information

PRODUCT	SKU	DESCRIPTION
Hardware		
FortiPAM 1000G	FPA-1000G	FortiPAM-1000G Privileged Access Management server for up to 50 users.
FortiPAM 3000G	FPA-3000G	FortiPAM-3000G Privileged Access Management for up to 100 users
Virtual Machines		
FortiPAM-VM	FC1-10-PAVUL-591-02-DD	Subscription for one FortiPAM Virtual Machine seat for between 5 to 9 users. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license for an additional unit with the same user seats license on the backup unit.
	FC2-10-PAVUL-591-02-DD	Subscription for one FortiPAM Virtual Machine seat for between 10 to 24 users. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license for an additional unit with the same user seats license on the backup unit.
	FC3-10-PAVUL-591-02-DD	Subscription for one FortiPAM Virtual Machine seat for between 25 to 49 users. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license for an additional unit with the same user seats license on the backup unit.
	FC4-10-PAVUL-591-02-DD	Subscription for one FortiPAM Virtual Machine seat for between 50 to 99 users. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license for an additional unit with the same user seats license on the backup unit.
	FC5-10-PAVUL-591-02-DD	Subscription for one FortiPAM Virtual Machine seat for between 100 to 249 users. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license for an additional unit with the same user seats license on the backup unit.
	FC6-10-PAVUL-591-02-DD	Subscription for one FortiPAM Virtual Machine seat for 250 or more users. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license for an additional unit with the same user seats license on the backup unit.
License Options		
FortiPAM License Options		Licensed FortiClient with PAM function activated. This is the recommended deployment as additional SSL VPN, ZTNA, SSOMA functions can also be activated. This uses the existing EMS licenses - no additional license required.
		Dedicated unlicensed standalone FortiClient with PAM function which does not require EMS. This standalone FortiClient can not be combined with other FCT standalone versions and can only be used for FortiPAM.



FORTINET

www.fortinet.com

June 2, 2023

FPM-DAT-R03-20230602