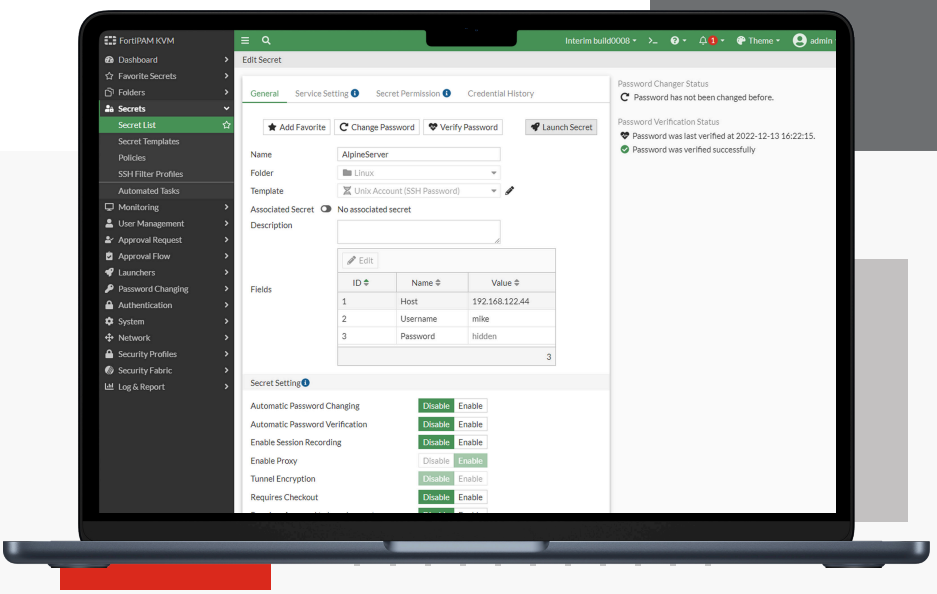
FortiPAM

Available in

Appliance

Virtual



Highlights

- Credential security
- Certificate storage
- Zero Trust Network Access (ZTNA) integration
- Privileged session monitoring
- Service account management
- Secure access with MFA, SSO and SAML, RADIUS, and LDAP support
- Comprehensive reporting
- Fortinet ecosystem integration

Privileged Access and Session Management

Privileged Access is defined as access to an account with privileges beyond those of regular accounts, typically in keeping with roles such as IT Managers and System Administrators. Examples of privileged access include Firewall and Network Administrators, Windows Domain and Enterprise administrators.

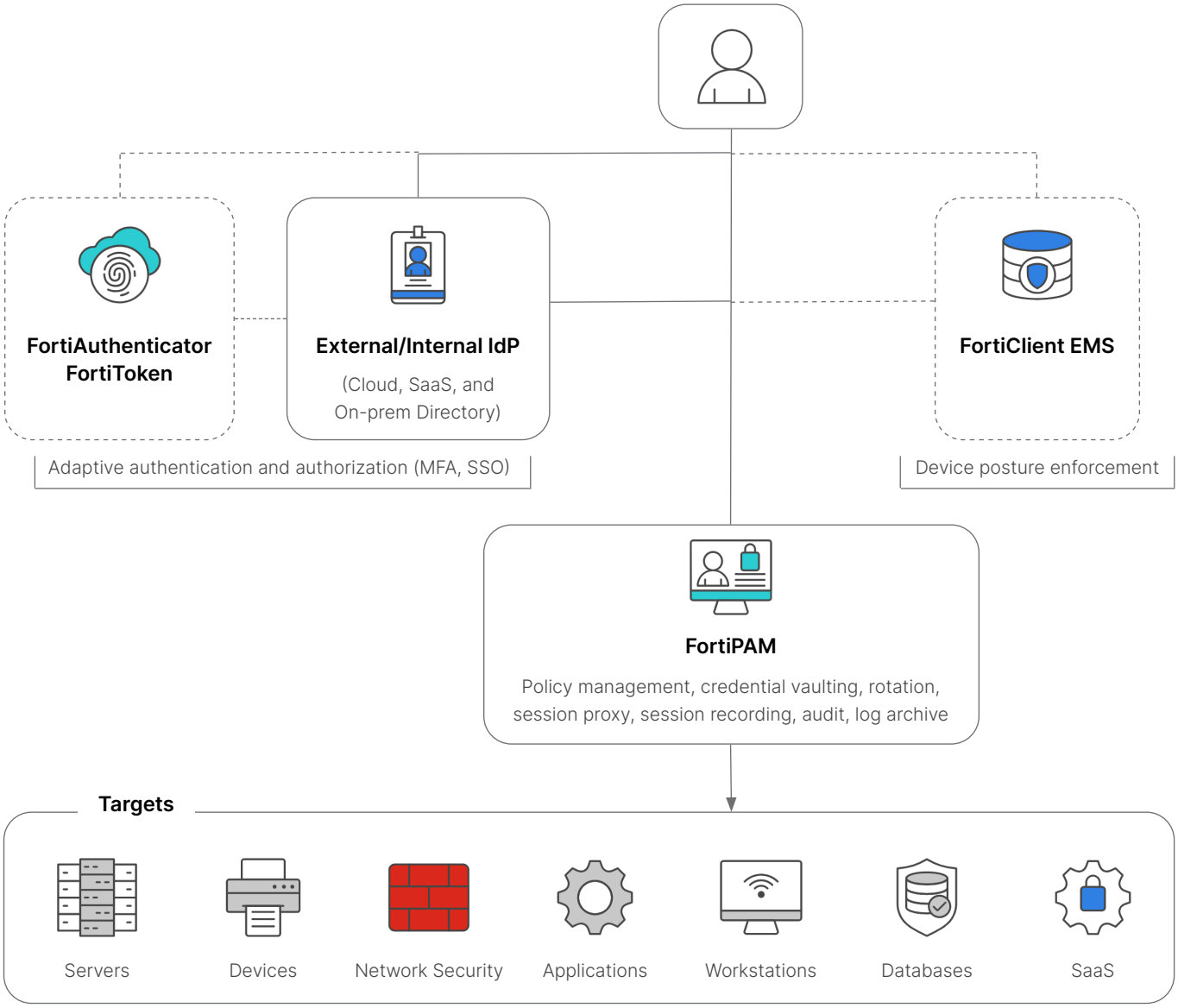
Importantly Privileged Account attacks remain a high-profile attack vector, and in many instances, detection alone is measured in hundreds of days, with recovery taking significantly longer.

Built on the firm foundations of FortiOS, FortiPAM provides robust privileged account management, session monitoring and management, and strict role-based access control to secure access to sensitive assets and mitigate data breaches.

With capabilities such as account discovery, secure password and certificate storage, password rotation, identity authentication, session monitoring and recording, and reporting, FortiPAM provides security teams with full visibility and control of privileged credential usage.

FortiPAM is incredibly straightforward to deploy and maintain. Whilst FortiPAM is fully capable of running in stand-alone mode, it also offers deep integrations with several Fortinet products.

Solution Deployment



Denotes optional component

FortiPAM Privileged Access and Session Management—Key Features

Scalable, market-proven, enterprise-ready solution. Flexible solution with high availability and redundancy, as well as 'break-glass' to help ensure business continuity. Distributed network gateway support enables secret and session management across multiple networks and geographies, and the native REST API enables integration with third-party tools (e.g., Ansible, Terraform) for secret retrieval.

Comprehensive session controls. With built in SSH command and Windows application filtering in place, FortiPAM administrators can block harmful or unwanted actions on their connected assets.

Fully secure credentials. When a secret is saved in FortiPAM, that data is encrypted using advance AES256 encryption. When a FortiPAM session is launched to an asset, the credentials are completely obfuscated from the user. With this approach, regardless of what assets are being connected, credentials can never be captured or leaked by the user.

Zero Trust Network Access (ZTNA). When integrated with FortiClient EMS, FortiPAM performs continuous ZTNA endpoint validation, ensuring connecting user devices are policy compliant before granting access to sensitive systems or data. ZTNA controls offer highly granular, robust, real-time controls over connecting machines, thus ensuring only trusted users and devices are able to connect to targets.

Privileged session monitoring. Provides granular control of user activities by monitoring, recording, and auditing privileged user activity (e.g., login, keystrokes, and mouse events). Authorized admins can restrict privileged user activities with command filtering or SSH filter controls. Admins can also monitor and terminate active sessions. Session video recording and playback are available for further analysis.

Built-in DLP and Antivirus capabilities. Powered by FortiGuard Labs, FortiPAM provides built-in DLP and Antivirus capabilities, ensuring comprehensive protection for File Transfer traffic and alerting on data misuse or leakage. Prevents data exfiltration and blocks unwanted data downloads.

Connectivity. FortiPAM supports a broad range of access protocols for connectivity to target assets, including out-of-the-box and high-profile protocols, such as RDP, SSH, VNC, Telnet, MSSQL, SMB, SCP, HeidiSQL, and others. Further, should a protocol requirement exist which has not been pre-defined, FortiPAM users are able to design a custom protocol launcher.

Automated service account discovery, and management of privileged accounts and credentials. Automatically discover, import, and rotate service account credentials based on policies, mitigating manual, and error-prone processes. Admins can define granular policies (e.g., rotation frequency or password complexity) and hierarchical access approval processes, ensuring compliance and security requirements are met.

Certificate storage. In addition to target and secret storage, FortiPAM also securely stores certificates and keys for future deployment and logs all certificate-related activities.

Comprehensive reports. Centralized audit and reporting to meet required compliance mandates. Full tamper-resistant audit trail tracks all user activity and provides enhanced visibility and security.

Secure privileged access with Multifactor Authentication (MFA) and Single Sign-On (SSO). FortiPAM offers extensive support for authentication protocols, including OOTB support for SAML, RADIUS, and LDAP, with Active Directory integration for assigning user roles and permissions. FortiPAM integrates seamlessly with FortiToken Cloud, enabling contextualized user authentication and a streamlined user access experience.

Secure remote user for third-party privileged access. FortiPAM can easily be configured to enable visitor/guest access. With robust OOTB authentication, FortiPAM is the ideal solution to authenticate external, remote employees/vendors. Adopting a least privileged approach, external visitors may only access the resources explicitly declared by the administrator. In addition, admins can set up an auto-onboarding rule for users in FortiPAM. This process is triggered by the user's first successful login, during which FortiPAM automatically syncs permissions via LDAP, RADIUS, or SAML based on group membership and user role.

Integrations. FortiPAM supports seamless integration with several Fortinet products; FortiClient EMS integration provides continuous ZTNA endpoint validation to ensure privileged user devices are secured before allowing access to sensitive data. FortiToken and FortiAuthenticator integrations provide orchestrated user authentication and authorization workflows to enable MFA, SSO, passwordless access, and more. Customers can even integrate with FortiSandbox for file transfer operations for deep inspection and threat analysis.

Reduce your Identity Attack Surface and Streamline Secure Access Across the Hybrid Network with FortiPAM

FortiPAM helps organizations mitigate their identity-related exposure and secure human privileged access and credentials, ensuring consistent enforcement of least privilege. The solution, part of Fortinet Security Fabric, provides built-in integration with FortiAuthenticator, FortiToken (Mobile, Cloud, or HW) for a simple unified authentication method and user experience. FortiPAM enables organizations to:

- Reduce the risk of compromised privileged credentials —Automatically discover, add, and manage privileged accounts and credentials based on predefined policies, to mitigate the risk of unauthorized access. Privileged session monitoring allows admins to monitor user activity in real-time and terminate suspicious active session.
- Control and manage service accounts—Simplify service accounts discovery, credentials onboarding, and management.
- Ensure secure third-party privileged access—Leverage FortiPAM and FortiToken Cloud integration to enable passwordless and adaptive MFA for fast user validation.
- Prevent the spread of malware—FortiPAM leverages built-in DLP and Antivirus capabilities powered by FortiGuard Labs, providing robust protection for session traffic, and alerting on, for example, data misuse, leakage, or file transfer. It is also possible to integrate FortiPAM with FortiSandbox, enabling real time sandboxing of suspicious files and traffic.
- Drive operational efficiencies and reduce complexity—With automated privileged-account lifecycle management, from onboarding to secret rotation, auditing and reporting, FortiPAM eliminates human errors, achieving simplicity and enabling scalability.
- Satisfy audit and compliance requirements—Provides policy-based privileged access controls, session recording, and detailed audit trails of access activity for retrospective analysis, ensuring compliance with security mandates and industry regulations.

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/SFP+ Interfaces	2× 1GbE SFP 2× 10GbE SFP+	2× 1GbE SFP 4× 10GbE SFP+
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
Interfaces and Modules		
CPU	Single AMD EPYC 7402, 24C48T, 2.80GHz	Dual AMD EPYC 7402, 24C48T, 2.80GHz
RAM	128GB (DDR4)	256GB (DDR4)
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

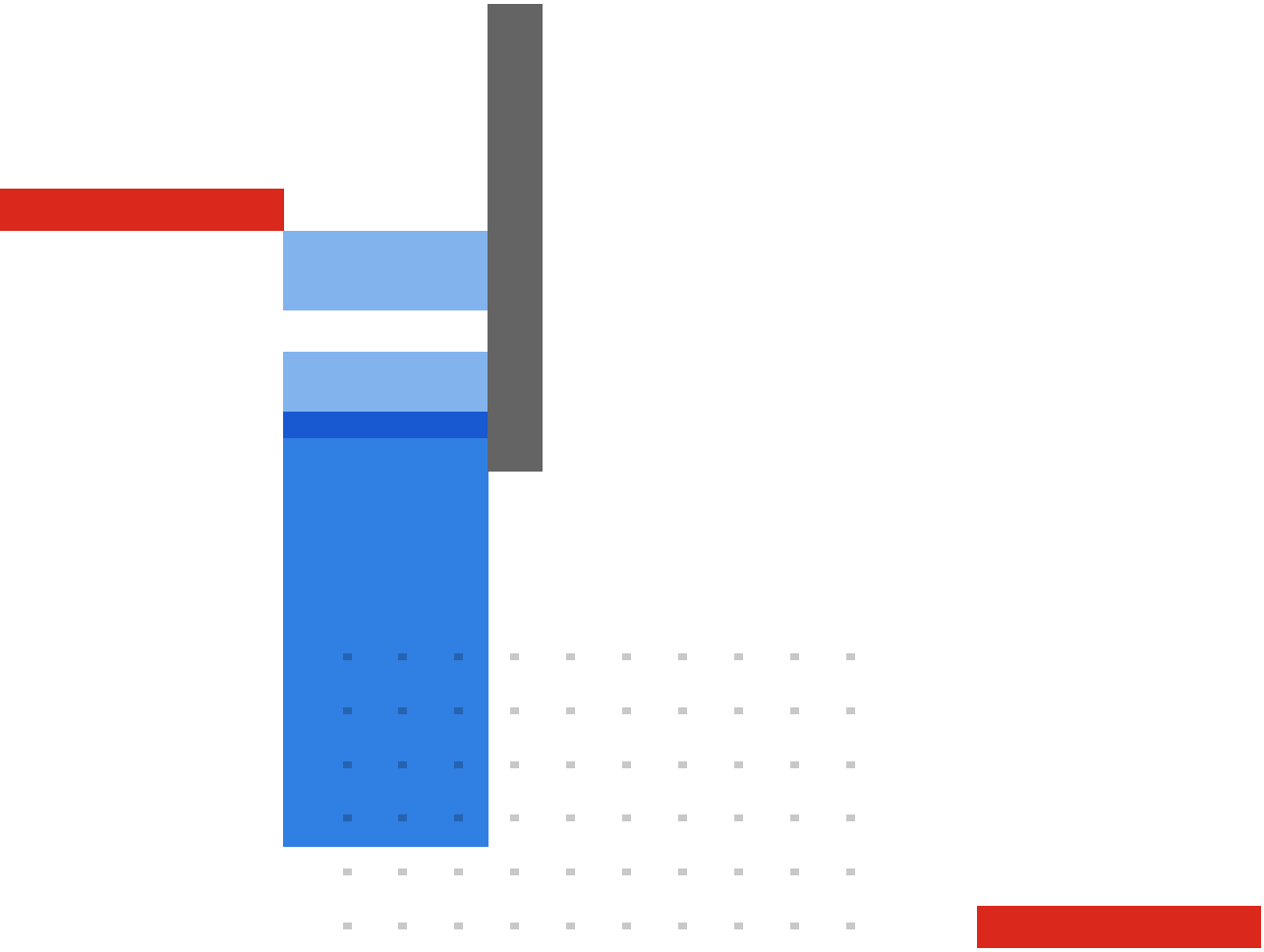
Ordering Information

PRODUCT	SKU	DESCRIPTION
Hardware		
FortiPAM 1000G	FPA-1000G	FortiPAM-1000G Privileged Access Management server for up to 50 users.
	FC-10-PA1KG-681-02-DD	Antivirus and Data Leak Prevention protection.
	FC-10-PA1KG-247-02-DD	FortiCare Premium Support.
FortiPAM 3000G	FPA-3000G	FortiPAM-3000G Privileged Access Management for up to 100 users.
	FC-10-PA3KG-681-02-DD	Antivirus and Data Leak Prevention protection.
	FC-10-PA3KG-247-02-DD	FortiCare Premium Support.
Hardware UG		
FPM-HW-UG	FPM-HW-25UG	Adds 25 users to FPAM HW models' user limit.Stackable license.Support included.
	FPM-HW-50UG	Adds 50 users to FPAM HW models' user limit.Stackable license.Support included.
	FPM-HW-100UG	Adds 100 users to FPAM HW models' user limit.Stackable license.Support included.
	FPM-HW-200UG	Adds 200 users to FPAM HW models' user limit.Stackable license.Support included.
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 Advanced Malware Protection. Includes FortiCare Premium support. HA requires additional license.
	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 Advanced Malware Protection. Includes FortiCare Premium support. HA requires additional license.
	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 Advanced Malware Protection. Includes FortiCare Premium support. HA requires additional license.
	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 Advanced Malware Protection. Includes FortiCare Premium support. HA requires additional license.
	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 Advanced Malware Protection. Includes FortiCare Premium support. HA requires additional license.
	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 Advanced Malware Protection. Includes FortiCare Premium support. HA requires additional license.
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.

Visit https://www.fortinet.com/resources/ordering-guides for related ordering guides.

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainability for all through cybersecurity, with respect for human rights and ethical business practices, making possible a digital world you can always trust. You represent and warrant to Fortinet that you will not use Fortinet's products and services to engage in, or support in any way, violations or abuses of human rights, including those involving illegal censorship, surveillance, detention, or excessive use of force. Users of Fortinet products are required to comply with the Fortinet EULA and report any suspected violations of the EULA via the procedures outlined in the Fortinet Whistleblower Policy.



FORTINET

www.fortinet.com

December 30, 2024

FPM-DAT-R06-20241230