

# FortiPAM

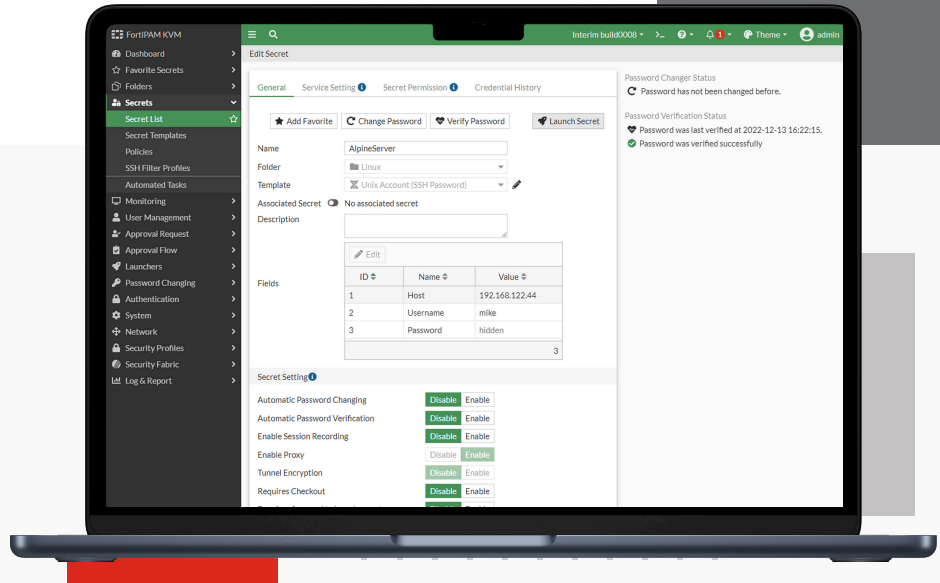
Available in



Appliance



Virtual



## Highlights

Simplifies operations and enhance user experience with unified identity access management. Natively combines Single Sign-On (SSO), adaptive Multi-factor Authentication (MFA), Privileged Access Management (PAM), and DLP and Antivirus, and ZTNA

Part of the Fortinet Security Fabric and integrates with FortiAuthenticator, FortiToken, FortiClient EMS, and FortiAnalyzer for enhanced security

Built-in DLP and Antivirus protection powered by FortiGaurd Labs. Prevent data exfiltration and blocks unwanted data downloads by scanning files for malicious content

Zero Trust Network Access (ZTNA). FortiClient EMS integration enables continuous ZTNA endpoint validation, ensuring only trusted users and devices are able to connect to FortiPAM

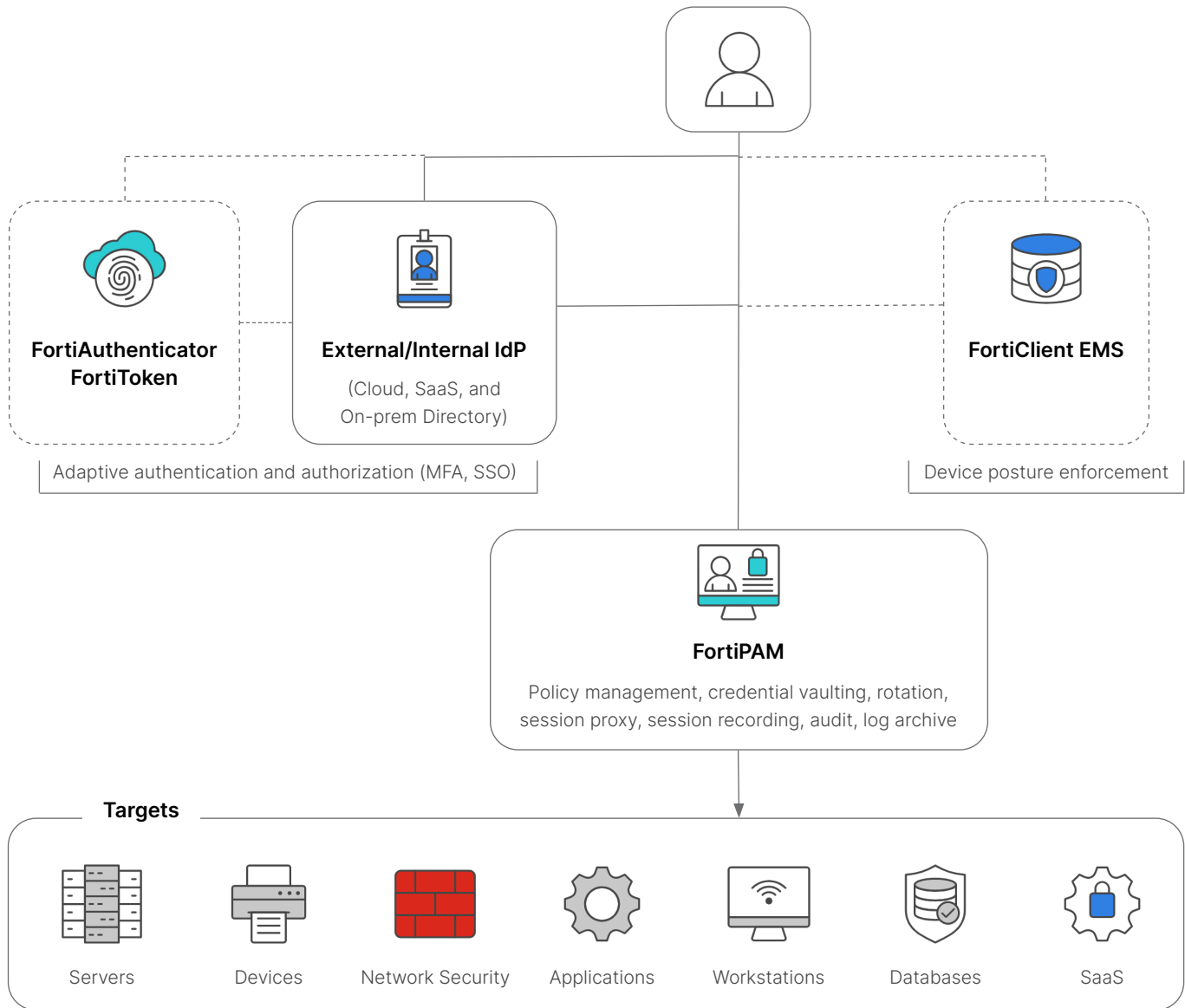
## Privileged Access and Session Management

Privileged credentials grant access to an organization's most sensitive data—posing significant risks if compromised.

FortiPAM is Fortinet's privileged access and session management solution. An integral part of the Fortinet IAM solution, FortiPAM provides privileged account and password management and session monitoring to secure access to sensitive assets and help prevent data breaches. With capabilities, such as credential discovery and onboarding, 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.

Simple to deploy and maintain, FortiPAM is integrated with several Fortinet products, providing automation and governance workflows for identity and credential lifecycle management, such as FortiAnalyzer and FortiClient EMS, enabling an additional detection and protection layer. 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, all to ensure a seamless user access experience while also supporting compliance requirements.

# Solution Deployment



----- Denotes optional component



## FortiPAM Privileged Access and Session Management—Key Features

**Automated discovery, onboarding, and management of privileged accounts and credentials.** Automatically discover, onboard, and rotate user credentials based on policies, to help eliminate manual, error-prone processes. Admins can define granular policies (e.g., rotation frequency, password complexity) and hierarchical access approval processes, ensuring compliance and security requirements are met.

**Secure privileged access with adaptive Multifactor Authentication (MFA) and Single Sign-On (SSO).** FortiPAM integrates seamlessly with FortiToken Cloud, enabling risk-based, contextualized user authentication (e.g., grants access based on device, IP, location), and a streamlined user access experience.

**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.

**Fully secure credentials.** When a FortiPAM user launches a session to an asset, the credentials are completely obfuscated from the user. With this approach, regardless of what assets are being connected to, credentials can never be captured by the attacker.

**Built-in DLP and Antivirus capabilities.** Powered by FortiGuard Labs, FortiPAM provides built-in DLP and Antivirus capabilities, ensuring comprehensive protection for session traffic and alerting on data misuse or leakage. Prevents data exfiltration and blocks unwanted data downloads, in addition to archiving content that passes through FortiPAM.

**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.

**Secure remote user/third-party privileged access.**

Leverages FortiToken Cloud and FortiPAM integration to authenticate external, remote employees/vendors using passwordless, adaptive MFA. In addition, admins can set up an auto-onboarding rule for remote users in FortiPAM, to automate the onboarding of new users. 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 (access profile). This determines whether the user can log in to FortiPAM and what permissions they are granted. Once logged in, the user is automatically created in FortiPAM with time-bound and least privileged access.

**Certificate storage.** Securely stores certificates and keys, reports on soon to be expired/expired certificates, and logs all certificate-related activities.

**Connectivity.** FortiPAM supports a broad range of access protocols for connectivity to target assets, including out-of-the-box and high-impact 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.

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

**Integrations.** FortiPAM offers extensive support for authentication protocols, including SAML, RADIUS, and LDAP, with Active Directory integration for assigning user roles and permissions. FortiPAM also supports seamless integration with FortiClient EMS and FortiAnalyzer, enabling ZTNA, and seamless reporting, respectively.

**Scalable, market-proven, enterprise-ready solution.**

Flexible solution with high availability and redundancy, as well as break glass to help mitigate risks and ensure business continuity. Distributed network gateway support enables secret and session management across multiple networks, and rest API enables integration with third-party tools (e.g., Ansible, Terraform) for secret retrieval/management.



## 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 minimize 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 via facial/fingerprint recognition and time-based password. Combined with full session monitoring, vendor access is granted for a predefined time only, to ensure secure remote access.

**Prevent the spread of malware** — Users do not connect directly to the target, whereby communication with the target is done via FortiPAM, minimizing the risk of malware spread. In addition, 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.

### **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. Integration with Fortinet Identity and Access Management (IAM) solutions, such as FortiAuthenticator and FortiToken Cloud/Mobile/HW, provides a seamless, unified user experience for all identities, simplifying overall policy management.

**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	FUNCTION	FUNCTION
<b>User Management</b>	<b>Launcher</b>	<b>Authentication</b>
Local User	PuTTY (FCT required)	Address (Used in AD Target Restriction)
Remote Authentication: LDAP Server	Remote Desktop - Windows (FCT required)	Scheme and Rules
Remote Authentication: Radius Server	Web Launcher	<b>Stability</b>
SAML	Web RDP	Long Session
MFA: FortiToken	Web SFTP	Stress Test (Overload, CPU 70%)
MFA: Email Token	Web SMB	<b>Installation</b>
MFA: SMS Token	Web SSH	Upgrade
Administrator Role Management	Web VNC	Installation Doc/ Administration Guide
User Group	WinSCP	<b>Security</b>
API User	VNC Viewer (FCT required)	ZTNA Tag Endpoint Control to target server and/or PAM server
User Trusted Host	Tight VNC (FCT required)	2 Factor Authentication for local PAM users or remote SAML, Radius, LDAP users
FortiToken Cloud	Custom Launcher	Anti-Virus scanning for web-based file transfer (Web SFTP, Web SAMBA) and SCP-based file transfer
<b>Secret Folder</b>	<b>Secret Request Approval</b>	Automatic blocking of dangerous commands with SSH filtering profile
Public Folder	Approval Profile (up to three Tiers)	User access control based on IP and/or schedule
Personal Folder	Request Review and Approve	Secret access request/approval
Folder Permission Control	Request Notification	Secret check-out/check-in protection
Secret Policy Management	Multiple Approvals Requirement	Auto password changing after check-in
<b>Secret Template and Access</b>	Script	Scheduled password change
Unix SSH (Password or Key)	<b>Password Changer</b>	High-strength SSH encryption algorithm
Windows Domain Account (LDAPS or Samba)	Password Policy	Advanced RDP authentication protocol including CredSSP, TLS
Template - FortiGate	Custom Password Changer	Role-based access control
Template - Cisco Device	<b>Monitor and Record</b>	Policy-based access profile enforcement
Template - Web Account	User Monitor	Trusted Platform Module to protect user private keys
Template - Machine	Active Sessions Monitor	Data Leak Prevention based on file types, size, or watermarks
Custom Template	Session Recording	
<b>Secret</b>	<b>Log and Audit</b>	
Secret Check-out/Check-in	Events - System	
Renew Secret Check-out	Events - User	
Approval Request	Events - HA	
Verify Password	Logs - Secrets	
Periodical Password Changer	Logs - Video (Record and Replay)	
Password Heartbeat	<b>System</b>	
Video Recording	HA	
SSH Filter	Glass Breaking	
Auto Password Delivery on Native Launcher	Maintenance Mode	
Cisco Device Auto-Enable on Native Launcher	Automatic Configuration Backup	
Associated Secret Launcher	Max Duration for the Launcher Session	
Associated Secret Password Changer	vTPM: KVM	
SSH Keyboard Interactive Authentication on Native Launcher	vTPM: VMWare	
RDP Security Level	FortiClient: Custom FCT FortiVRS (video recording daemon) Port	
Block RDP Clipboard	High Availability	
AD Target Restriction	Disaster Recovery support	
Move/Clone a Secret		
Secret Permission Control		
Favorite Secrets		



## Specifications

	FPA-1000G	FPA-3000G
<b>Hardware</b>		
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)
<b>System Capacity</b>		
Local + Remote Users (Base)	50	100
Secrets	5000	10 000
Folders	2000	6000
Secret Requests	5000	10 000
<b>Interfaces and Modules</b>		
CPU	Single AMD EPYC 7402, 24C48T, 2.80GHz	Dual AMD EPYC 7402, 24C48T, 2.80GHz
RAM	128GB (DDR4)	256GB (DDR4)
<b>Dimensions</b>		
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)
<b>Environment</b>		
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
<b>Operating Environment and Certifications</b>		
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
<b>Hardware</b>		
<b>FortiPAM 1000G</b>	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.
<b>FortiPAM 3000G</b>	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.
<b>Hardware UG</b>		
<b>FPM-HW-UG</b>	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.
<b>Virtual Machines</b>		
<b>FortiPAM-VM</b>	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.
<b>License Options</b>		
<b>FortiPAM License Options</b>	<p>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.</p> <p>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.</p>	

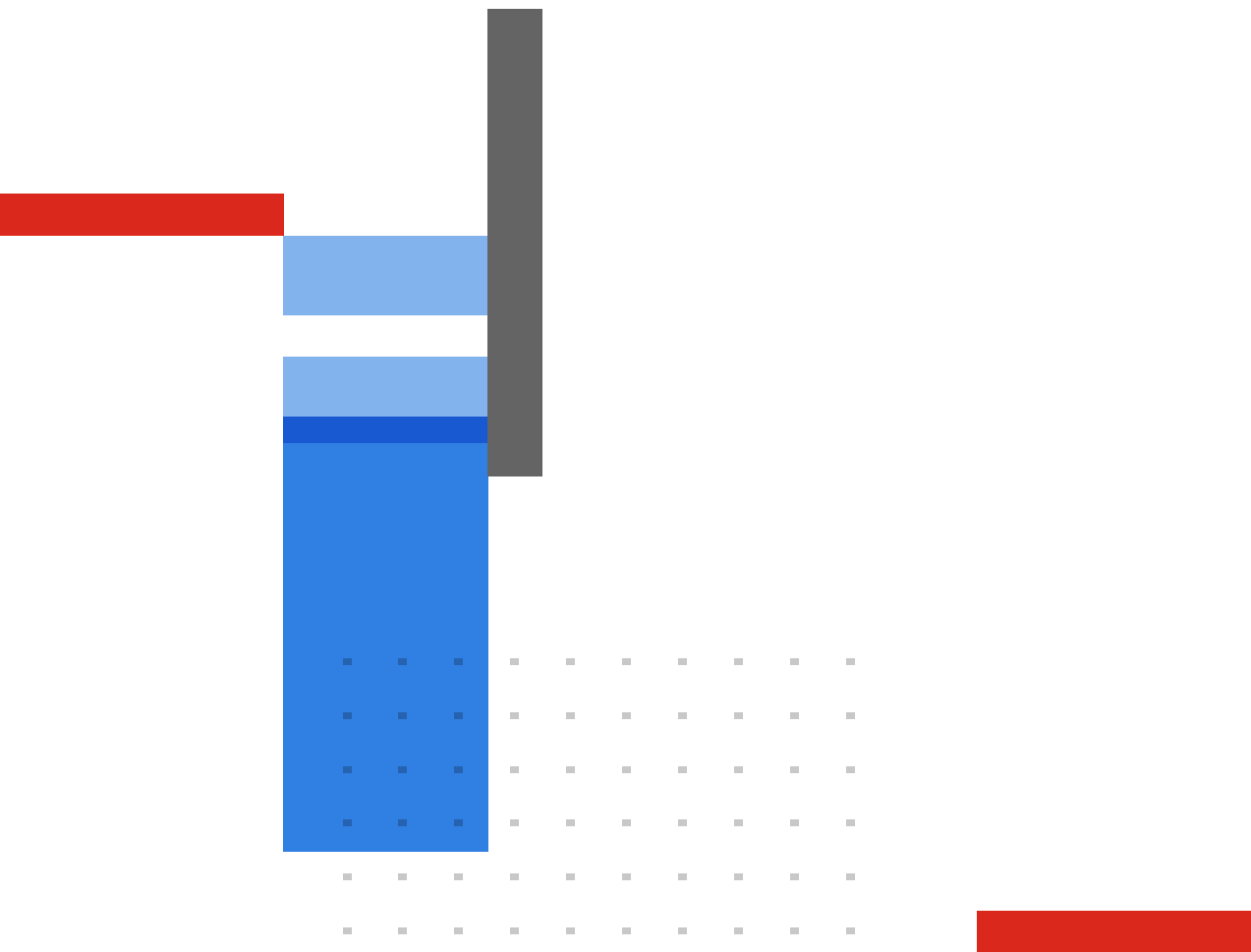
Visit <https://www.fortinet.com/resources/ordering-guides> for related ordering guides.



---

## 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](#).



[www.fortinet.com](http://www.fortinet.com)

Copyright © 2024 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's SVP Legal and above, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.