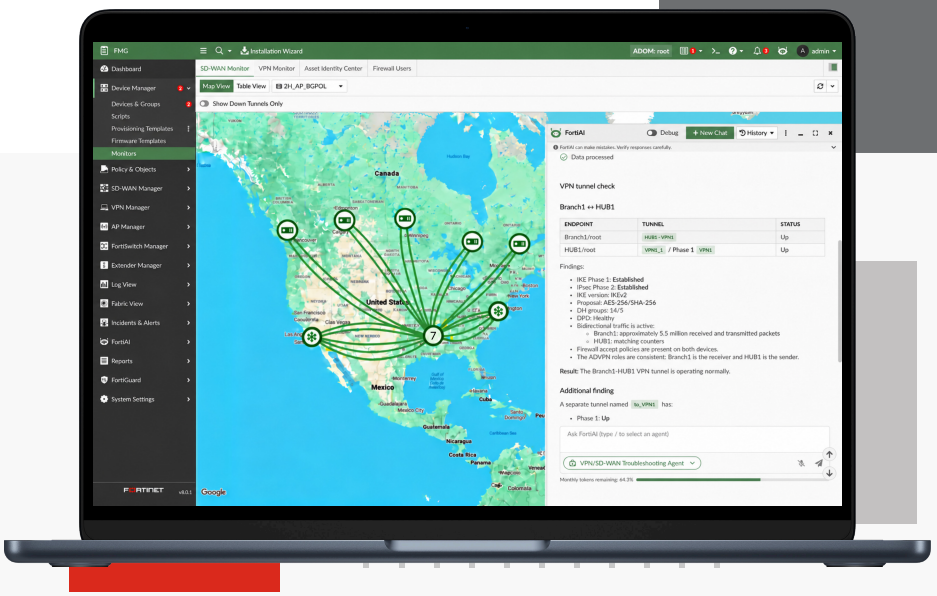
FortiManager



Highlights

- Transform network operation and speed up troubleshooting with add-on FortiAI subscription
- Centrally manage network and security policies
- Centralize distribution of security content, signatures, and firmware images
- Simplify configuration, deployment, and maintenance
- Reduce complexity and costs
- Automate workflows and configurations
- Separate customer data and manage domains
- Automate backups with streamlined software and security updates

FortiAI-powered and automation-driven centralized device management from a single console

FortiManager, integrated with FortiAI, provides automation-driven centralized management of your Fortinet devices from a single console. This process enables full administration and visibility of your network devices through streamlined provisioning and innovative automation tools, enhanced by AI-driven capabilities for configuration, troubleshooting, scripting, validation, and IoT vulnerability analytics.

Integrated with the Fortinet Security Fabric advanced security architecture and automation driven network operations capabilities provide a solid foundation to secure and optimize your network security. Built-in Fortinet factory default templates with best security practice and relevant network configuration for specific use cases.

Highlights

Single-Pane Management

Single-Pane Management and Provisioning simplifies centralized administration of policies and objects, while offering automated revision history and control. It also provides advanced role-based access control (RBAC) capabilities, allowing for distinct user roles in Firewall and Intrusion Prevention System (IPS) management.

Zero-Touch Provisioning

Zero-touch provisioning simplifies the deployment process for SD-Branch (FortiGates and access devices) with powerful templates that directly utilize meta-variables for scalable provisioning to thousands of sites.

Fabric Automation

Our solution leverages automation and tight integration across Fortinet Security Fabric. With built-in FortiGuard update server, FortiManager delivers real-time security updates and protection to managed devices. By integrating ZTNA and SASE capabilities, we can enforce consistent security policy across different network topologies, independent of users' locations. Centralized analytics and logging through FortiAnalyzer provide end-to-end visibility and the APIs and Fabric Connectors enable integration and end-to-end automation, to reduce operational overhead.

FortiManager High Availability (HA) with Automatic Failover (VRRP)

FortiManager high availability (HA) provides enhanced reliability, data protection, redundancy, and operational performance to ensure agreed-upon uptime and availability requirements are met, with option for dedicated interface for management of the individual cluster member. In the event that the operating FortiManager unit fails, a backup FortiManager (one primary and up to four secondary) unit can take the place of the failed unit, for seamless access to devices and business-critical network operations.

Monitoring and Troubleshooting

Central monitoring and visibility for device inventory, applications, SD-WAN, LAN edge, network traffic, public cloud, and more.

Built-in speed tests to troubleshoot branch office connectivity and packet capture to investigate LAN related issues.

Agentic AI-Assisted Operations

FortiManager embeds Agentic AI and MCP frameworks, an AI layer built directly into the management console, to shift network operations from manual, reactive tasks toward AI-assisted workflows. Administrators can automate routine configuration and policy work, get AI-generated recommendations for optimizing network settings, and accelerate diagnostics.

Key Features

Device Manager

Centrally manage thousands of FortiGates, SD-WAN / SD-Branch, FortiProxy, FortiSwitches, FortiAPs, and FortiExtenders.

License Manager

Actively manages, monitors and enforces licenses, support contracts and subscriptions for FortiGates.

Firmware Manager

Schedule automated firmware upgrades for all managed devices, provides detailed upgrade report.

Provisioning Templates

Device blueprint, templates, and template group used for device onboarding and provision configuration. Buit-in factory-default best-practice templates to automate configuration for SD-WAN and LanEdge.

Policy and Objects Manager

Policy packages centrally enforce security on FortiGates and FortiSASE.

Policy Blocks

Group multiple firewall policies that can be reused as needed in Policy Packages.

Workspace / Workflow / Per-Admin Mode

Controls collaborative configuration management by allowing administrators to lock specific resources to prevent conflicts. Workflow mode enforces an approval process model, ensuring changes are reviewed and authorized before deployment. Per-Admin mode allows each administrator to install own changes only, without locking the resource.

FortiGuard Update Server

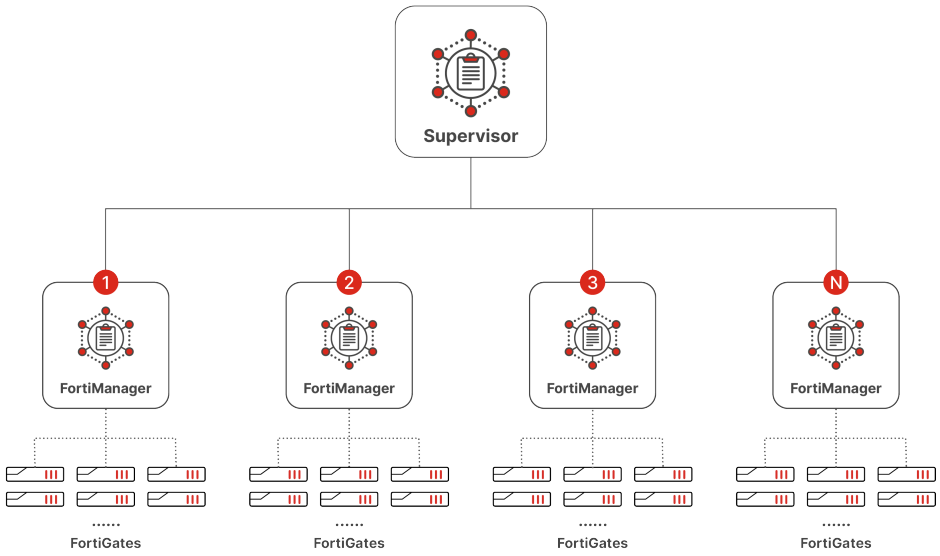
Buit-in module, centralizes real-time distribution of security content and signatures updates.

REST APIs

Built to automate workflows, device onboarding and configuration, and maintain a simplified deployment at scale.

Fabric of FortiManager

Scale As You Go Flexible design of FortiManager Fabric Cluster with Supervisor and up to 32 members to increase performance in very large environments



Fabric Cluster with Supervisor and Members to increase performance

Single-Pane Management

Device Configuration and Provisioning

FortiManager expands the network administrator's capabilities with a rich set of tools to centrally manage up to 100 000 devices including FortiGate NGFWs, FortiExtender, FortiSwitch switches, FortiAP access points, Fortinet Secure SD-WAN, and more.

Central configuration using enhanced templates and device blueprint with variables support, in preparation for zero-touch provision for mass deployments, firmware version enforcement for installs and upgrades, and a Fabric Authorization Template automatically provisions and authorizes LAN Edge devices on the managed FortiGates.

FortiManager includes extended SSL and certificate support for enhanced ssl-ssh-profile configuration, a restricted IPS Admin role to support transitioning and upgrading from dedicated IPS solutions, custom commands on FortiSwitch and configuring MCLAG from the FortiSwitch Manager.

Automated device configuration backups and revision control make daily administrative tasks easy. Track changes with Event Log to review configuration updates for auditing and compliance.

Security Policy and Objects Management

FortiManager Policy and Objects enable admins to centrally manage and configure security policies, including security profiles to control antivirus definitions, intrusion prevention signatures, web filtering, and applications.

The global policy feature allows MSSP and PaaS providers to apply ADOM level header/footer policies for updating all policy packages or select packages. Administrators can also group commonly used policies in a policy block and use in different Policy Packages.

Policy and Objects include a revision history, providing information on admins who have made changes, change date, summary, and a mandatory change notes field to capture change reason.

The per-policy lock feature under workspace mode allows admins to control the policy change by implicitly locking a policy rule when a policy is changed.

Extend security policies across hybrid and multi-cloud environments, with configuration templates for IPSec, BGP, CLI, and SD-WAN rules.

Secure SD-WAN

FortiManager offers powerful SD-WAN management capabilities using intuitive workflows and simplified provisioning at scale. Leverage application centric SD-WAN business policies to fine-tune traffic steering decisions based on performance service level agreement (SLA) targets for each WAN provider.

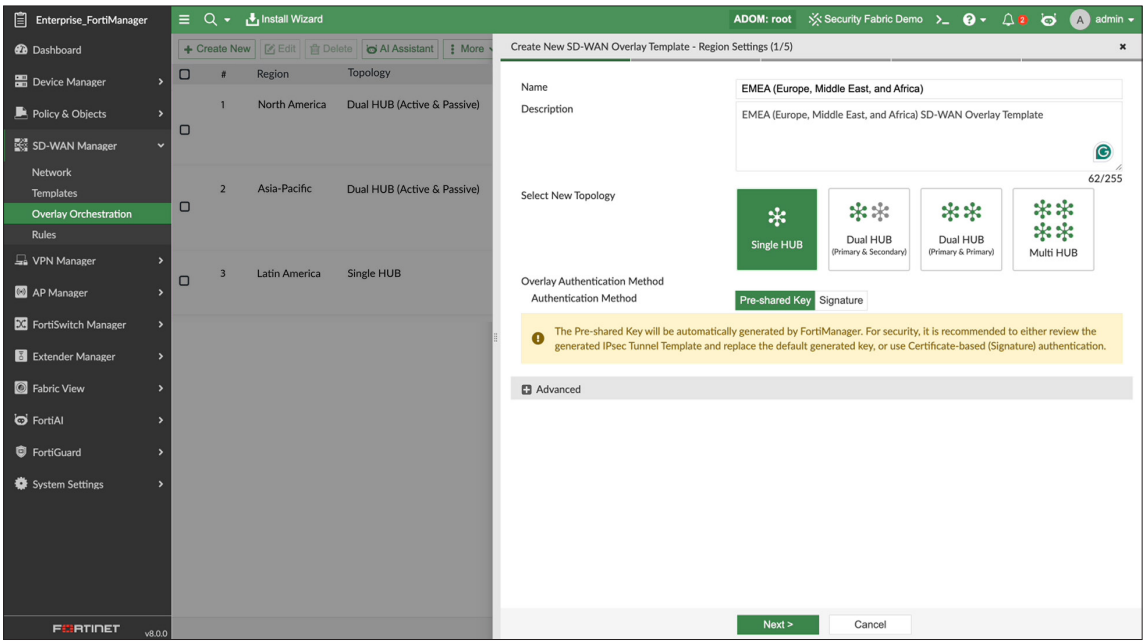
Simplify and accelerate SD-WAN configuration on a global scale with automated SD-WAN overlay provisioning. Utilize device blueprints for large SD-WAN deployments with support for importing new devices from CSV and assign meta-data variables.

Multi-Tenancy and Role-Based Administration

FortiManager offers granular control over device management and user roles, enabling zero-trust multi-tenancy setups for large organizations. It features a hierarchical database of objects that allows for efficient reuse of common configurations across multiple customers.

Administrative Domains (ADOMs) are used to manage independent security environments, with domain-specific policies and dedicated configuration databases. The intuitive GUI makes it easy for admins to view, create, clone, and manage ADOMs, define global Objects, Policies, and Security Profiles across ADOMs, with Health Check to keep ADOMs in sync.

Assign IPS admin restricted user role, for users performing only IPS related object configuration and installations. Use per-admin UI background themes for unique visual associations.



Use the Secure SD-WAN reports and monitoring dashboards to closely monitor application performance including metrics for bandwidth, latency, jitter, and packet loss.

Built-in Automation for Network and Security Operations

Leveraging the Threat Feed connectors and integration with FortiAnalyzer, FortiManager can automatically block the malicious URL, Domains, and IP Addresses based on FortiAnalyzer detections.

The built-in FortiGuard Distribution server can provide license management and security updates for managed devices, even in closed network (air gapped) topology.

APIs and Connectors

Utilize automation and orchestration and optimize network operations with FortiManager through querying of FortiGate NGFWs and the Fortinet Security Fabric via application programming interfaces (APIs). This process will actively collect and share network information and broaden end-to-end visibility and response.

FortiManager reduces complexity and cost by leveraging REST API, scripts, connectors, and FortiGate automation stitches to automate time-intensive processes and accelerate workflows. This method helps NOC and SOC teams by reducing administrative tasks, and addressing talent shortages. Admins can automate common tasks such as provisioning of FortiGate NGFWs and configuring new or existing devices.

Join the Fortinet KYC Network for exclusive access to articles, how-to content for automation and customization, community-built tools, scripts, and sample code.

Zero-Trust Network Access and SASE

Increase operational efficiencies with simplified and automated provisioning and deployment of Fabric devices, using open Fabric APIs for new integrations and workflows.

Utilize ZTNA rules and policies to enforce access control, the EMS connector to retrieve ZTNA tags or tag groups, configure a ZTNA server and use the ZTNA tags in policies to enforce zero trust RBAC (role-based access control).

Centrally managed FortiSASE policies and objects from FortiManager. Changes are created on FortiManager and synchronized to SASE FortiGates.

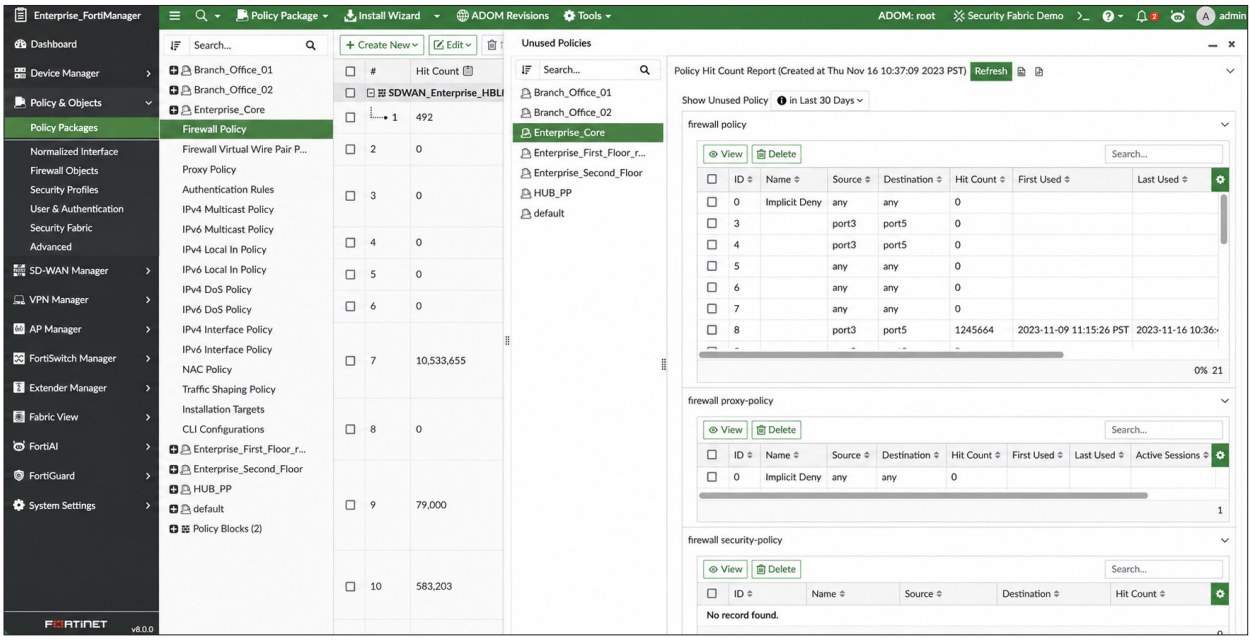
Automate Third Party Integration

FortiManager can enhance security by using External Threat Feeds Connectors, to dynamically upload the external block lists and centrally distribute the block content to all managed FortiGates.

Use Fabric connectors to facilitate connections with third party vendors such as vCenter, pxGrid, ClearPass, OCI, ESXi, AWS, and others to share and exchange data.

FortiManager integrates with ITSM to seamlessly mitigate security incidents and events, apply configuration changes, and update policies. Integration with FortiAnalyzer provides in-depth discovery, analysis, prioritization, and reporting of network security events.

The FortiManager workflow for audit and compliance enables review, approval, and auditing policy changes. These methods include automating processes for policy compliance, policy lifecycle management, and enforced workflow to reduce risk.



Post-Quantum Cryptography

FortiManager protects sensitive data and critical infrastructure against future quantum computing threats with built-in support for Post-Quantum Cryptography (PQC). Powered by an integrated OpenSSL 3.5.x stack with NIST-standardized ML-KEM (Module-Lattice-Based Key-Encapsulation Mechanism) algorithms, FortiManager negotiates hybrid post-quantum key exchange groups - combining classical elliptic-curve cryptography with quantum-resistant ML-KEM—during TLS 1.3 handshakes.

PQC is supported across FortiManager's core communication channels, including the GUI/REST API (HTTPS), FortiGate device management (FGFM), CLI access (SSH), administrator authentication (RADIUS/TACACS+), log forwarding (OFTP), and HA cluster synchronization, ensuring configuration data, policy information, and administrative sessions remain secure against quantum attacks. FortiManager supports both pure PQC groups (ML-KEM-512/768/1024) and hybrid groups (X25519MLKEM768, X448MLKEM1024, SecP256r1MLKEM768, SecP384r1MLKEM1024), and interoperates with modern PQC-enabled browsers and servers.

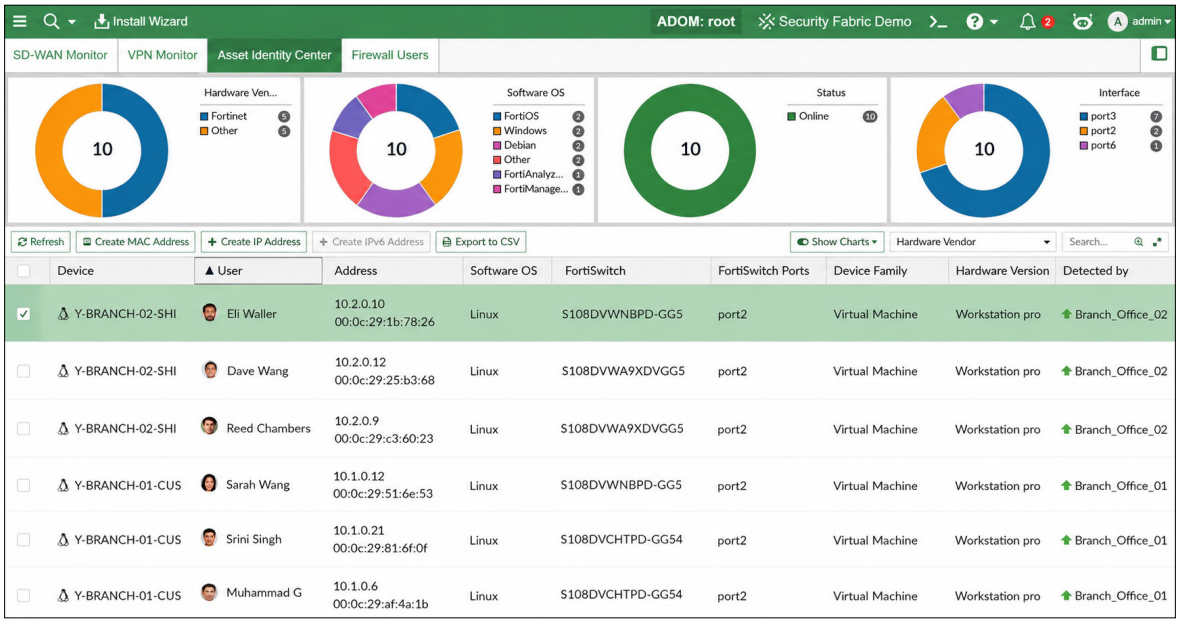
Monitoring and Troubleshooting

Deep Visibility

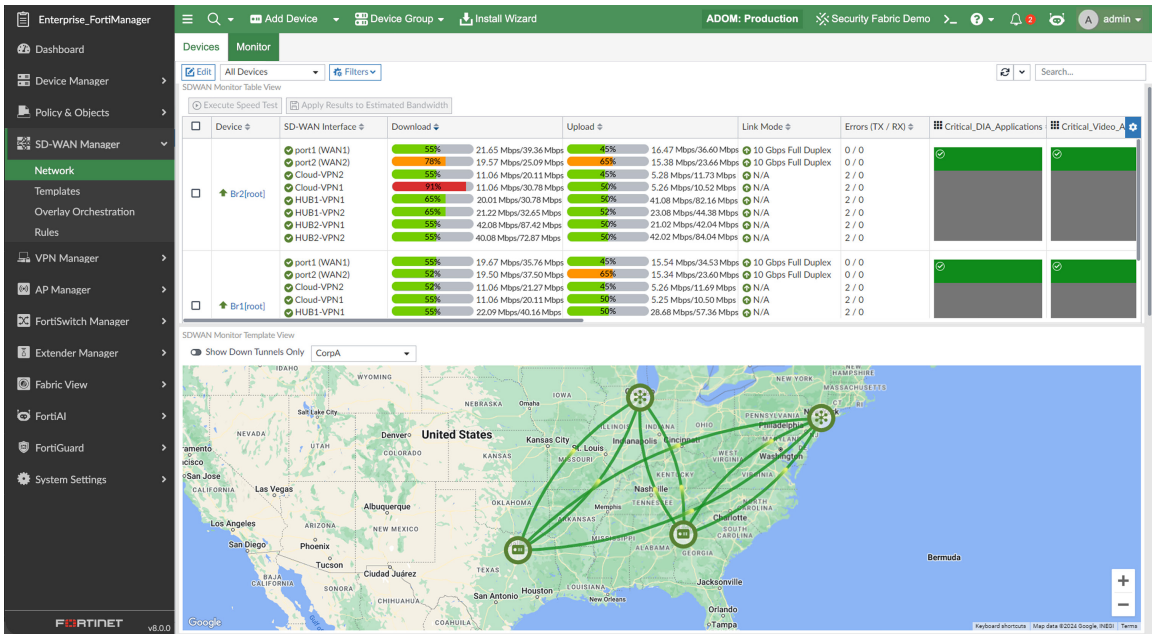
The FortiManager Device Manager provides full visibility, access, and management of Fortinet managed devices, interfaces, scripts, templates, automation, users, settings, and more. Install, edit, and delete policies. Monitor the health of FortiGate devices through customizable dashboards and widgets to see resource usage, network status of DHCP, IPsec and SSL VPN, routing, traffic shapers, and more. Easily navigate the hierarchical tree with categories for managed devices, logging devices, unauthorized devices, and customize to display as a table, folder, or a map view.

Use Fabric View to check Security Fabric ratings and network topology. Access vital security and network statistics, as well as real-time monitoring and topology information to provide visibility into network and user activity. Add a FortiAnalyzer appliance or virtual machine (VM) for powerful analytics and enhanced Fabric view with asset and identity info, additional data mining, statistical analysis, and graphical reporting capabilities.

FortiManager includes a multitude of tools for simple and intuitive analysis of Fortinet firewalls, switches, access points, and more. Gain one-click access to PSIRT information for detected vulnerabilities, and Device Inventory Monitor with device and user, FortiSwitch, FortiAP, and SSID information, and IoT device information gathered from FOS Asset Identity Center.



Built-in speed test for underlay WAN ports used to test Branch Office link performance. For LAN troubleshooting a packet capture can be configured and executed on demand or schedule, directly from FortiManager.



Agentic AI Powered by Model Context Protocol (MCP)

FortiManager's AI capabilities are built on the Model Context Protocol (MCP), the standard that lets FortiAI agents maintain and act on rich, structured context - device state, policy history, configuration intent across multi-step tasks.

Dedicated AI Agents in FortiManager

FortiAI within FortiManager is built around a set of purpose-built agents rather than a single general-purpose assistant. A scripting agent handles Day 0–1 network design and configuration, translating natural-language intent into validated CLI and Jinja scripts and catching errors before they reach production. A device and vulnerability agent handles Day-2 operations, continuously monitoring connected devices, correlating real-time vulnerability data, and generating prioritized remediation guidance.

Each AI Agent is scoped to a specific stage of the network lifecycle, and together they cover configuration, validation, and ongoing risk management.

FortiManager Virtual Machines

FortiManager virtual machines are a virtual version of the hardware appliance and are designed to run on many virtualization platforms, offering all the latest features of the FortiManager appliance. They allow organizations to centrally manage any number of Fortinet network security devices and scale from several to thousands, supporting centralized management, best practices compliance, and automated workflows to deliver superior protection against threats. FortiManager-VMs are available in both a subscription and perpetual offering.

FortiManager-VM-S

The new FortiManager-VM subscription license model consolidates the VM product SKU and the FortiCare Premium Support SKU into a single SKU to simplify the product purchase, upgrade, and renewal.

The FortiManager-VM S Series SKUs come in stackable subscriptions to manage 10, 100, and 1000 devices/ VDOMs. Multiple units of this SKU can be purchased at one time to increase the number of devices/ VDOMs as needed. This SKU can also be purchased with other FortiManager-VM-S SKUs to expand the total number of devices/ VDOMs.

FortiManager-VM

Fortinet offers the FortiManager-VM in a stackable license model. This software-based version of the FortiManager hardware appliance is designed to run on many virtualization platforms, which allows you to expand your virtual solution as your environment expands. The FortiManager virtual appliance family minimizes the effort required to monitor and maintain your network and offers all the features of the FortiManager hardware appliance.

FortiManager Appliances

FortiManager hardware appliances are built to power fast, scalable, and secure network operations for enterprises and service providers. Ranging from entry-level models like the FMG-410G to manage 30-150 devices, to high-end units such as the FMG-1000G, FMG-3100G, and FMG-3750G for up to 100 000 devices — they deliver a single console to manage hyperscale deployments across on-premises, cloud, SD-WAN, and SASE — bringing true end-to-end visibility and control into one unified platform.

Trusted Platform Module (TPM) Encryption

FortiManager G Series features a dedicated micro-controller module that hardens physical networking appliances by generating, storing, and authenticating cryptographic keys in TPM. This hardware-based security mechanism protects users from malicious software and phishing attacks.

FortiManager Cloud Services

FortiManager Cloud

FortiManager Cloud is a cost effective central management solution, easy to deploy, and accessible everywhere 24/7. By integrating with FortiCloud organizational unit (OU) structure, it provides single-pane management of multiple FortiManager-Cloud instances making it a good fit for enterprise customers and service providers.

Specifications

FORTIMANAGER VIRTUAL APPLIANCES	FMG-VM-10-UG	FMG-VM-100-UG	FMG-VM-1000-UG	FMG-VM-5000-UG
Capacity				
Devices/VDOMs (Default) [1, 3]	+10	+100	+1000	+5000
GB/ day of Logs [2]	2	5	10	25
Chassis Management	✓	✓	✓	✓
Virtual Machine				
Hypervisor Support	Up-to-date hypervisor support can be found in the release notes for each FortiManager version. Visit https://docs.fortinet.com/product/fortimanager/ and find the Release Information at the bottom section. Go to "Product Integration and Support" → "FortiManager [version] support" → "Virtualization"			
vCPU Support (Min / Max)	4 / Unlimited			
Network Interface Support (Min / Max) [4]	1 / 12			
Memory Support (Min / Max)	8 GB / Unlimited for 64-bit			
High Availability Support	✓			

1 Each virtual domain (VDOM) operating on a physical or virtual device counts as one (1) licensed network device.

2 GB/ day of logs are not stackable. These values represent the maximum available with purchased license.

3 VM SKUs are stackable up to 100 000 Devices/VDOMs.

4 VM supports up to 12 vNIC interfaces/ports. Applicable to 6.4.3+. Actual consumable numbers vary depending on cloud platforms.

Specifications

FORTIMANAGER APPLIANCES	FMG-410G	FMG-1000G
Capacity and Performance		
Devices/VDOMs (Default) [1]	150	1000
Devices/VDOMs (Maximum) [3]	—	—
Sustained Log Rates	50	50
GB/ day	2	2
Hardware Specifications		
Storage Capacity	32 TB (8 × 4 TB)	32 TB (8× 4TB)
Usable Storage (after RAID)	24 TB	24 TB
RAID Levels Supported	RAID 0/1,1s/5,5s/6,6s/10/50/60	RAID 0/1,1s/5,5s/6,6s/10/50/60
Default RAID Level	50	50
Hardware Form Factor	2 RU Rackmount	2 RU Rackmount
Total Interfaces	4 x GE RJ45, 2 x SFP	2× 2.5GBaseT RJ45 + 2 × 25GbE SFP28
Console Port	RJ45	RJ45
Self-Encrypting Drives (SED)	✓	✓
IPMI Sensors*	—	—
Removable Hard Drives	✓	✓
Redundant Hot Swap Power Supplies	✓**	✓
Trusted Platform Module (TPM) [2]	✓	✓
Dimensions		
Height x Width x Length (inches)	3.5 × 17.5 × 22.2	3.46 × 17.24 × 24.41
Height x Width x Length (cm)	8.8 × 44.5 × 56.5	8.8 × 43.8 × 62.0
Weight	35.27 lbs (16 kg)	49.6 lbs (22.5 kg)
Environment		
AC Power Supply	100–240V AC, 50-60 Hz	100–240V AC, 50–60 Hz
Power Consumption (Average / Maximum)	140 W / 182 W	251.36 W / 302 W
Heat Dissipation	621 BTU/h	857.73 BTU/h
Operating Temperature	32°F to 104°F (0°C to 40°C)	32°F to 104°F (0°C to 40°C)
Storage Temperature	-4°F to 167°F (-20°C to 75°C)	-40°F to 158°F (-40°C to 70°C)
Humidity	5% to 95% non-condensing	8% to 90% non-condensing
Forced Airflow	Front to Back	Front to Back
Operating Altitude	Up to 7400 ft (2250 m)	Up to 16 404.2 ft (5000 m)
Compliance		
Safety Certifications	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB	FCC Part 15 Class A, RCM, VCCI, CE, UL/cUL, CB

1 Each virtual domain (VDOM) operating on a physical or virtual device counts as one licensed network device. Global policies and high availability support available on all models.

2 Gen2 refers to hardware that has been upgraded since initial release.

3 Devices/VDOMs maximum with device add-on license, if supported.

* IPMI Sensors: For FMG-410G, FMG-1000G - no IPMI support, basic sensors information is extracted from motherboard. For FMG-3100G/3750G - sensors information available via OS, no physical port access to IPMI.

** Optional redundant AC power supply, not included.



FortiManager 410G



FortiManager 1000G

Specifications

FORTIMANAGER APPLIANCES	FMG-3100G	FMG-3750G
Capacity and Performance		
Devices/VDOMs (Default) [1]	4000	10 000
Devices/VDOMs (Maximum) [3]	8000	100 000
Sustained Log Rates	150	150
GB/ day	10	10
Hardware Specifications		
Storage Capacity	64 TB (16 × 4TB) SAS SED HDD + 3.84 (2× 1.92TB) NVMe SSD	384 TB (24 × 16TB) SAS SED HDD + 60TB (4 × 15TB) NVMe SED SSD
Usable Storage (after RAID)	56 TB	336TB (RAID 50, group 3 as default)
RAID Levels Supported	RAID 0/1,1s/5,5s/6,6s/10/50/60	RAID 0/1,1s/5,5s/6,6s/10/50/60
Default RAID Level	50	RAID 50
Hardware Form Factor	3 RU Rackmount	4 RU Rackmount
Total Interfaces	2 x GbE RJ45 ports, 2× 25GbE SFP28 ports	2× 10GbE RJ45 and 2× 25GbE SFP28
Console Port	DB9	DB9
Self-Encrypting Drives (SED)	✓	✓
IPMI Sensors*	✓	✓
Removable Hard Drives	✓	✓
Redundant Hot Swap Power Supplies	✓	✓
Trusted Platform Module (TPM) [2]	✓	✓
Dimensions		
Height x Width x Length (inches)	5.2 × 17.2 × 25.5	7 × 17.2 × 27.5
Height x Width x Length (cm)	13.0 × 44.0 × 65.0	17.8 × 43.7 × 69.9
Weight	69.6 lbs (31.57 kg)	70 lbs (31.8 kg)
Environment		
AC Power Supply	100-127V~/10A, 200-240V~/5A Hz	180-240Vac, 11-8A, 50-60Hz
Power Consumption (Average / Maximum)	395 W / 510 W	1134 W / 1474 W
Heat Dissipation	1740.19 BTU/h	5029.5 BTU/h
Operating Temperature	32°F to 104°F (0°C to 40°C)	50°F to 95°F (10°C to 35°C)
Storage Temperature	-40°F to 158°F (-20°C to 70°C)	-40°F to 158°F (-40°C to 70°C)
Humidity	5% to 95% non-condensing	10% to 93% non-condensing
Forced Airflow	Front to Back	Front to Back
Operating Altitude	Up to 13 123 ft (4000 m)	Up to 10 000 ft (3048m)
Compliance		
Safety Certifications	FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST	FCC Part 15 Class A, ISED, CE, RCM, VCCI, BSMI (Class A), UL/cUL, CB

1 Each virtual domain (VDOM) operating on a physical or virtual device counts as one licensed network device. Global policies and high availability support available on all models.

2 Gen2 refers to hardware that has been upgraded since initial release.

3 Devices/VDOMs maximum with device add-on license, if supported.

* IPMI Sensors: For FMG-410G, FMG-1000G - no IPMI support, basic sensors information is extracted from motherboard. For FMG-3100G/3750G - sensors information available via OS, no physical port access to IPMI.



FortiManager 3100G



FortiManager 3750G

Ordering Information

Product	SKU	Description
	FMG-410G	Centralized management appliance — 4x GE RJ45, 2x SFP, 32 TB storage, up to 150 Fortinet devices/VDOMs.
	FMG-1000G	Centralized management appliance — 2× 2.5 GBaseT RJ45 + 2× 25 GbE SFP28, 32 TB storage, up to 1000 Fortinet devices/VDOMs.
	FMG-3100G	Centralized management appliance — 2x GbE RJ45 ports, 2× 25GbE SFP28, 64 TB storage, dual power supplies, manages up to 4000 Fortinet devices/VDOMs.
	FMG-3750G	FMG-3750G Centralized Management appliance — 2× 10GE RJ-45 + 2× 25GE SFP28, 384TB SAS SED HDD + 60TB NVMe SED SSD storage, dual power supplies, manages up to 10 000 Fortinet devices/VDOMs.
FortiManager-VM Subscription License with Support	FC1-10-FMGVS-258-01-DD	Subscription license for 10 devices/VDOMs managed by FortiManager VM S-series, including FortiCare Premium; allows for total of 2 GB/Day of Logs.
	FC2-10-FMGVS-258-01-DD	Subscription license for 100 devices/VDOMs managed by FortiManager VM S-series, including FortiCare Premium; allows for total of 5 GB/Day of Logs.
	FC3-10-FMGVS-258-01-DD	Subscription license for 1000 devices/VDOMs managed by FortiManager VM S-series, including FortiCare Premium; allows for total of 10 GB/Day of Logs.
FortiManager-VM	FMG-VM-10-UG	Upgrade license for adding 10 Fortinet devices/VDOMs; allows for total of 2 GB/Day of Logs.
	FMG-VM-100-UG	Upgrade license for adding 100 Fortinet devices/VDOMs; allows for total of 5 GB/Day of Logs.
	FMG-VM-1000-UG	Upgrade license for adding 1,000 Fortinet devices/VDOMs; allows for total of 10 GB/Day of Logs.
	FMG-VM-5000-UG	Upgrade license for adding 5,000 Fortinet devices/VDOMs; allows for total of 25 GB/Day of Logs.
FortiManager-Cloud	FC0-10-MVCLD-227-01-DD	Subscription for 3 devices/VDOMs managed by FortiManager Cloud. FortiCare Premium support included.
	FC1-10-MVCLD-227-01-DD	Subscription for 10 devices/VDOMs managed by FortiManager Cloud. FortiCare Premium support included.
	FC2-10-MVCLD-227-01-DD	Subscription for 100 devices/VDOMs managed by FortiManager Cloud. FortiCare Premium Support included.
	FC3-10-MVCLD-227-01-DD	Subscription for 1000 devices/VDOMs managed by FortiManager Cloud. FortiCare Premium support included.
FortiManager Device Upgrade License	FMG-DEV-100-UG	FortiManager device upgrade license for adding 100 Fortinet devices/VDOMs. (3000 series and above - hardware only).

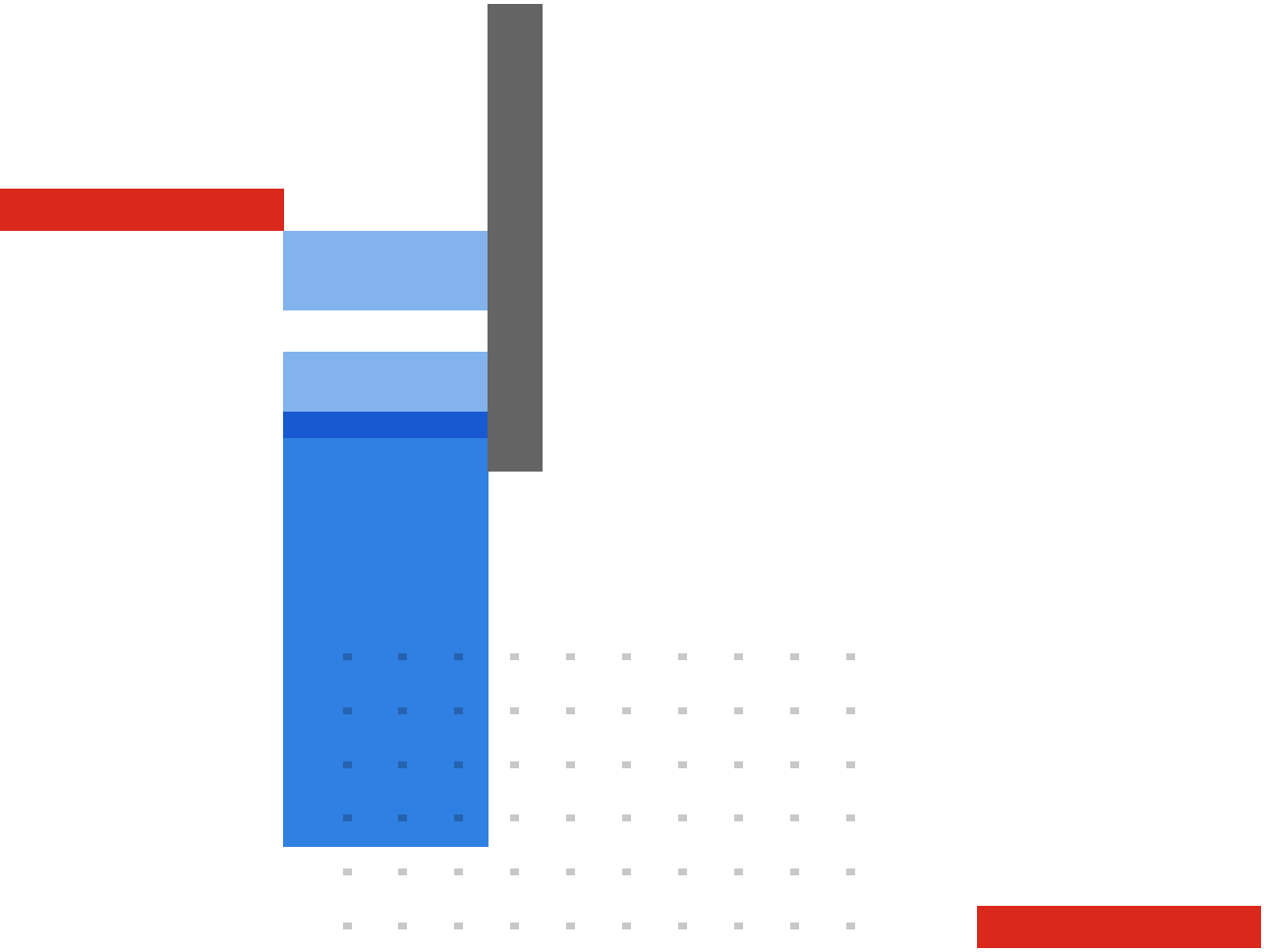
NOTE:

For hardware models, the default number of ADOMs can be found in the Release Notes on docs.fortinet.com

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

Copyright © 2026 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.

October 27, 2026

FMG-DAT-R84-1027