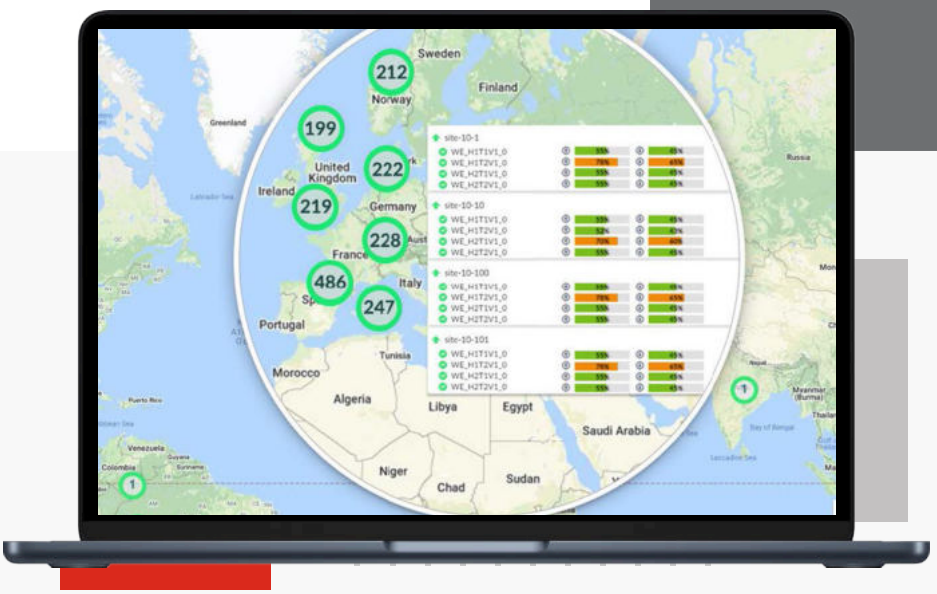
FortiManager



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 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.

Available in

Appliance

Virtual

Cloud

Highlights

Single-Pane Management and Provisioning

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.

Fabric Automation

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

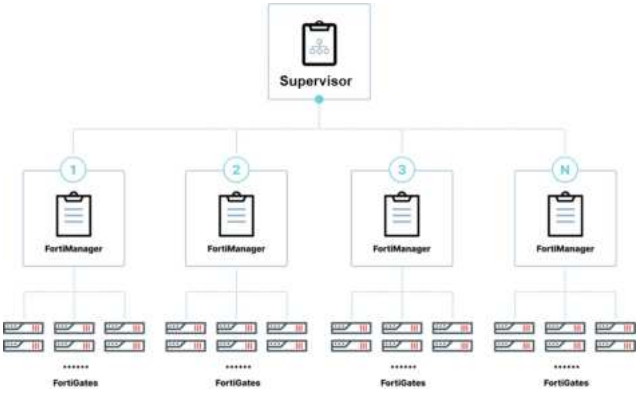
Monitoring, Visibility, and Troubleshooting

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.

Key Features

- Centrally manage network and security policies for thousands of FortiGate NGFWs and Secure SD-WAN plus FortiSwitches, FortiAP, and FortiExtender. Provide updates to FortiGate, FortiMail, FortiSandbox, FortiClient, FortiNDR, as well as SIEM and SOAR content packages for FortiAnalyzer
- License management, centralized distribution of security content and signatures through the use of the built-in FortiGuard module which are designed to work in air-gapped networks
- Simplify configuration, deployment, and maintenance for Secure SD-WAN at scale
- Reduce complexity and costs by leveraging REST API, scripts, CLI and Jinja templates, connectors, and automation stitches
- Automate workflows and configurations for Fortinet firewalls, switches, and wireless infrastructure
- Separate customer data and manage domains leveraging ADOMs to be compliant and operationally effective
- 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 and Provisioning

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.

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

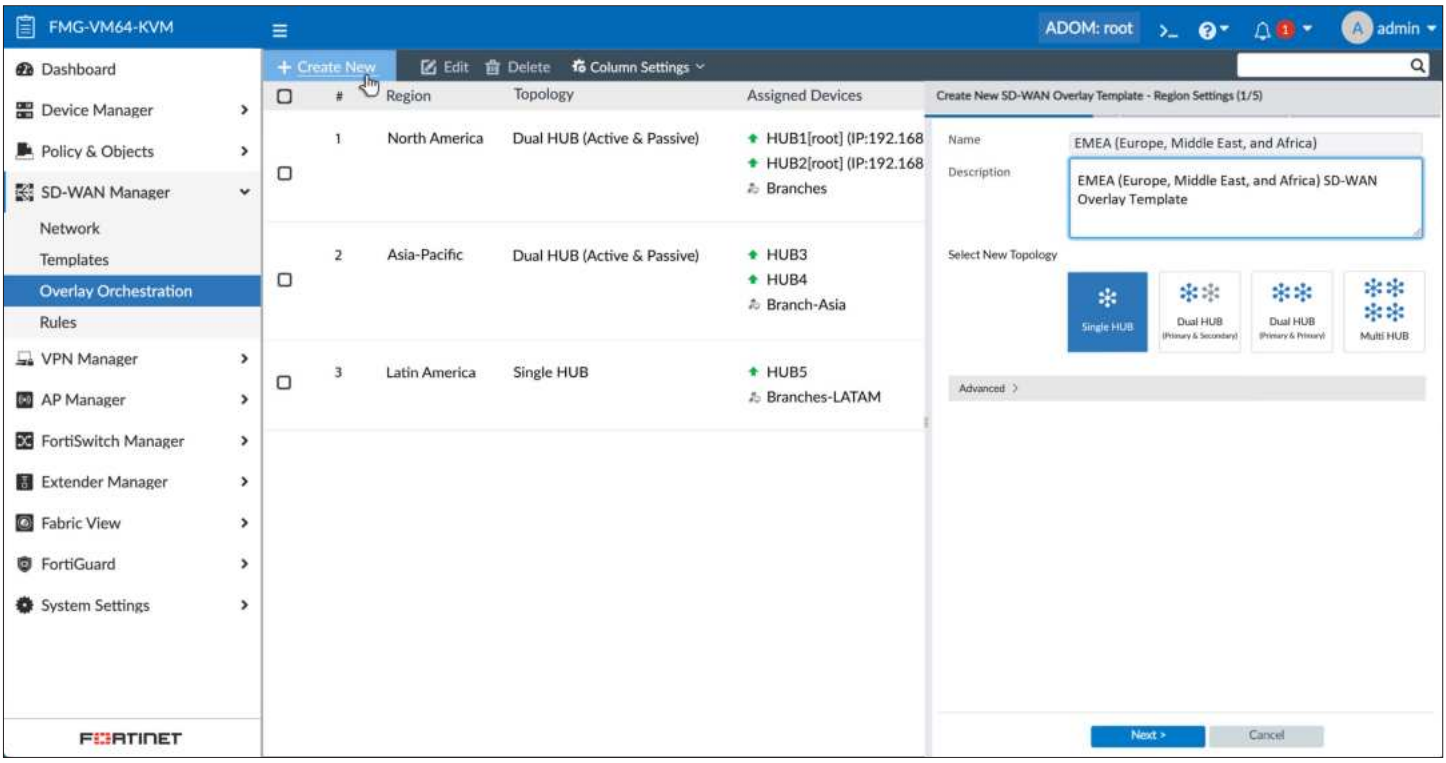
FortiManager high availability (HA) provides enhanced reliability, data protection, redundancy, and operational performance to ensure agreed-upon uptime and availability requirements are met, with option for dedicated interface for management of the individual cluster member. In the event that the operating 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.

Single-Pane Management and Provisioning (continued)

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.



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

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.

Fabric Automation

Network and Security Operations Visibility (NOC/SOC)

FortiManager supports NOC-SOC workflows to assist network teams in maintaining optimal performance. Automated data exchanges between security (SOC) workflows and operational (NOC) workflows, create a single, complete workflow that not only saves time, but also provides the capacity to complete additional incident response activities.

Integration with FortiAnalyzer magnifies visibility with advanced data visualization and analytics. This insight helps analysts quickly connect the dots, identify threats, and simplify the expeditious configuration and security of managed devices.

Automation 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 Developer Network (FNDN) for exclusive access to articles, how-to content for automation and customization, community-built tools, scripts, and sample code.

Expanded Operations Capabilities

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).

Make use of FortiSwitch multiple port selection configuration templates for effortless configuration of native and allowed vlans, security policies, QoS policies, and LLDP Profiles for simplified LAN edge management.

Use the IPS templates for quick and easy creation and installation of IPS profiles. Admins can use the IPS Signatures on-hold monitor for a centralized view of all on-hold signatures, including severity, OS, application, on-hold dates, and more.

FortiManager can also act as the management update server to managed FortiGates for IoT query device identification service.

FortiManager can serve as a centralized update server for managed FortiGate devices, providing IoT device identification services and updates.

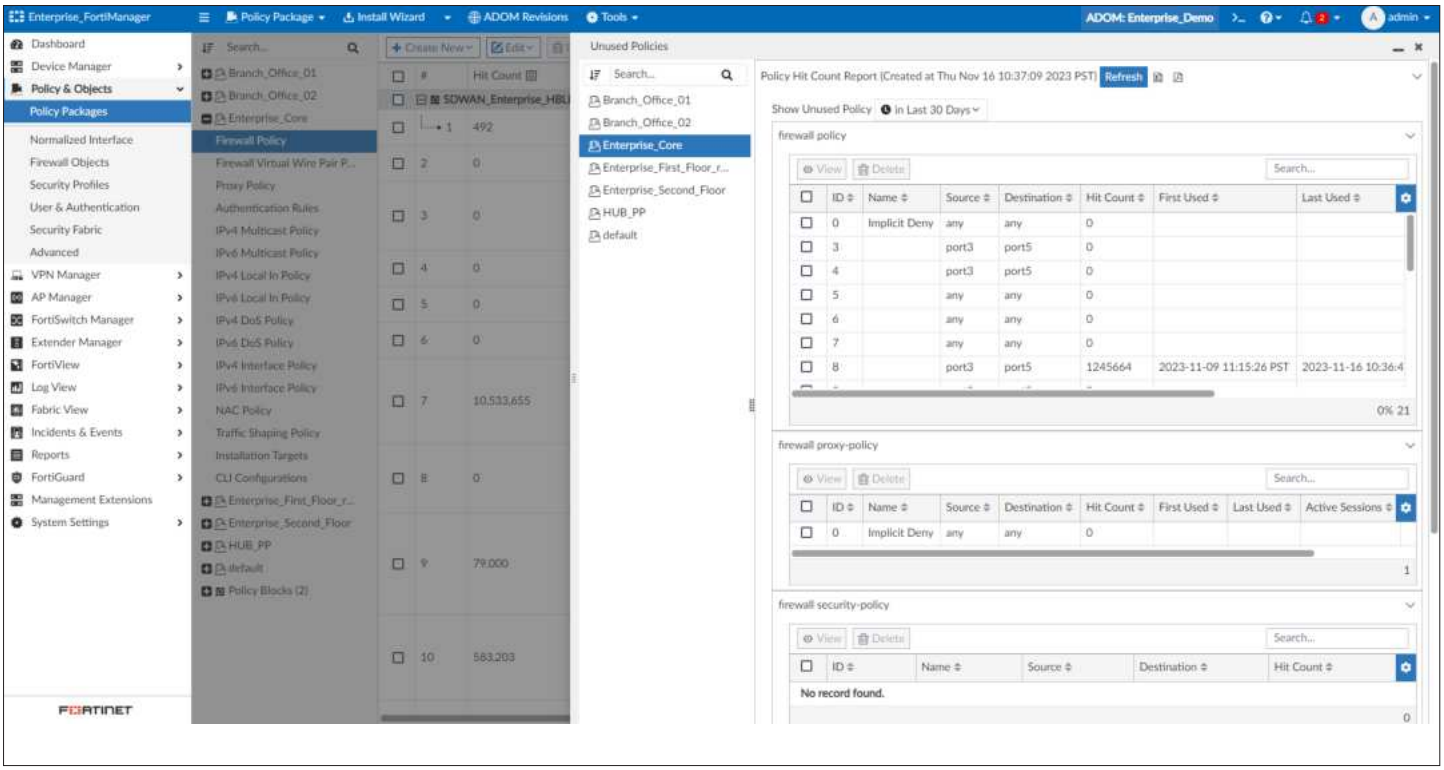
Fabric Automation (continued)

Security Fabric and Third Party Integration

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.

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.

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.



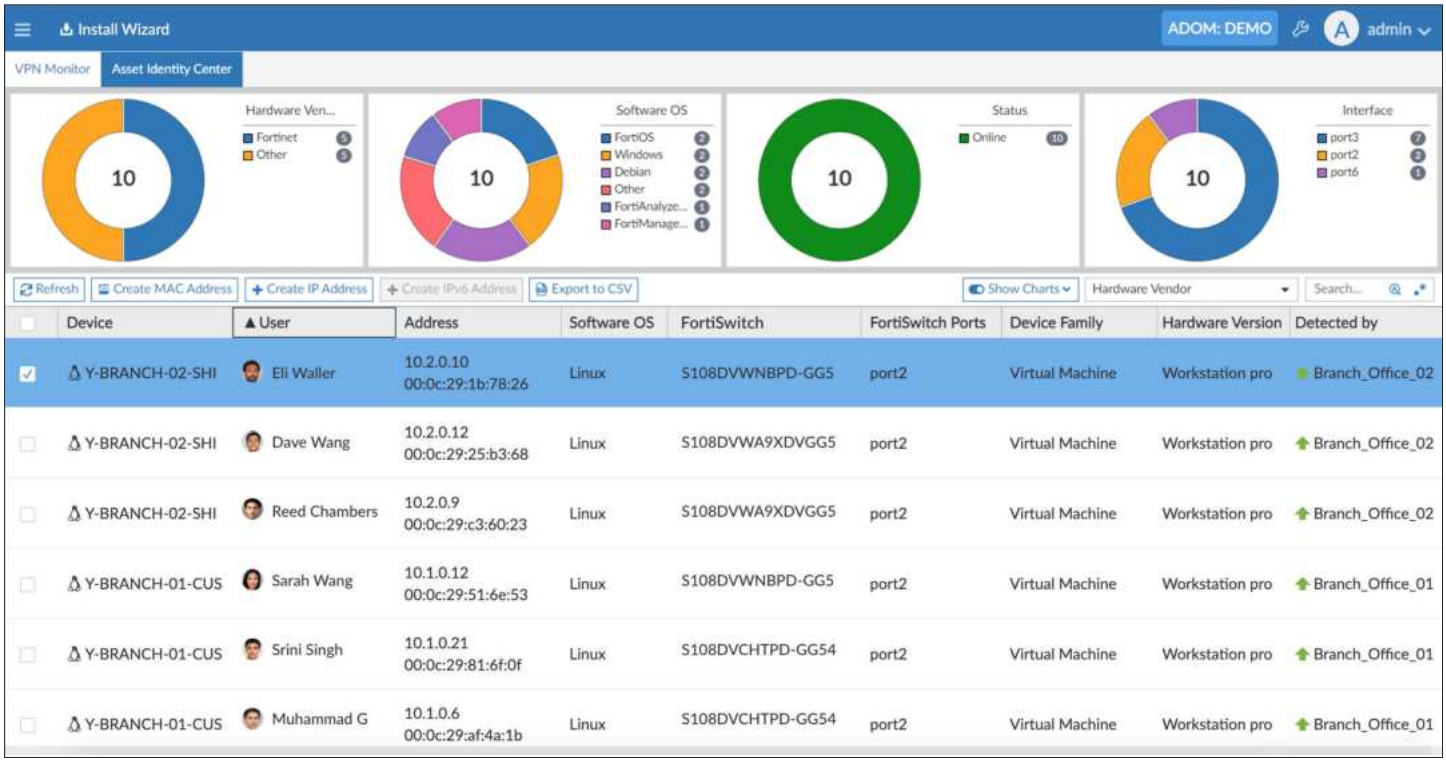
Monitoring, Visibility, and Troubleshooting

Manage and Monitor with 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.

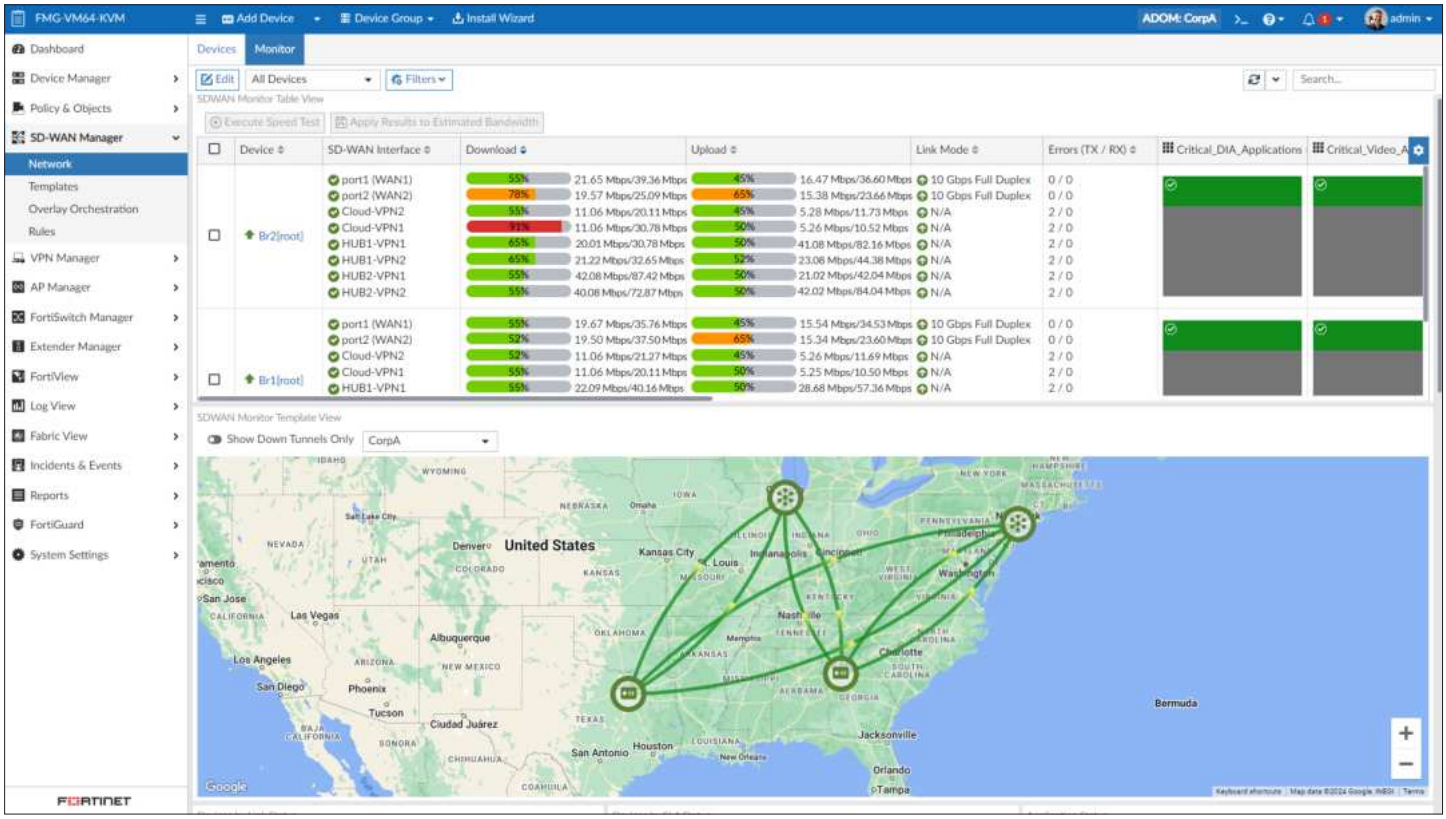
Use Fabric View to check Security Fabric ratings and network topology. Access vital security and network statistics, as well as real-time monitoring and topology information to provide visibility into network and user activity. Add a FortiAnalyzer appliance or virtual machine (VM) for powerful analytics 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 MEAs like the FortiAIOps extension, access 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.



Monitoring, Visibility, and Troubleshooting (continued)

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.



Harness AI to Elevate Network Operation

Scripting Generation and Validation on CLI and Jinja for Day 0-1 Network Design and Configuration

FortiAI within FortiManager streamlines network configuration by offering advanced scripting generation and validation. Using CLI and Jinja, FortiAI assists in creating accurate scripts based on conversational commands, making it accessible for users with varying levels of programming expertise. The validation feature scrutinizes the code for errors and suggests edits, enhancing the reliability and accuracy of configuration scripts.

IoT Device Assistant and Vulnerability Analytics for Day-2 ongoing network maintenance

FortiAI-powered FortiManager includes a robust IoT device assistant that enhances the management of connected devices. It offers real-time vulnerability analytics, helping identify and address potential security risks associated with IoT devices. This feature enables network administrators to proactively monitor, analyze, and mitigate vulnerabilities. It can also generate tailored vulnerability analytics and detailed reports. With continuously updated data and AI-driven recommendations, network teams can make informed decisions to maintain optimal security and performance.

NOC Cloud Services

Management Extensions

The Management Extensions pane allows rapid expansion of the single pane to manage more Security Fabric products. The built-in engine runs containerized management extension applications (MEAs) pulled from FortiGuard Labs Threat Intelligence. FortiManager's MEAs include one-click access to modules for FortiAIOps, Universal Connector, FortiWLM, FortiSigConverter, FortiSOAR, and others.

Dynamic Cloud Security

Fortinet cloud security and management solutions offer organizations a PaaS-based delivery option for central management of FortiGate devices from a cloud-based FortiManager.

FortiManager Cloud provides an automation-driven and single pane-of-glass management capability that is easy-to-implement, easy-to-manage, flexible, and scalable.

Use the single sign-on portal to manage Fortinet NGFW and SD-WAN. The built-in cloud-init service allows admins to easily customize a prepared image of a virtual installation for KVM, AZURE, support for Azure Virtual WAN of the Network Virtual Appliance (NVA), and AWS. FortiManager cloud-based network management helps organizations streamline FortiGate provisioning with automation-enabled management of Fortinet devices.

FortiManager-VM has been added to the FortiFlex offering to provide flex license management for FortiGates and to allow scaling up/down managed FortiGates or number of ADOMs.

Automatic configuration synchronization for the members of the Auto Scaling Group in Public Cloud in case of scale-out/scale-in events. Visibility improvement for auto scaling clusters with auto scale status, cluster type, HA status and mode and elastic IP information of the cluster members.

FortiManager can orchestrate the deployment of FortiGate autoscaling groups (ASG) on Amazon Web Services (AWS). This function allows administrators to use FortiManager as a single-pane to deploy all resources required to implement FortiGate ASG in the public cloud.

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 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.

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	Yes			

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-200G	FMG-410G	FMG-1000G
Capacity and Performance			
Devices/VDOMs (Default) [1]	30	150	1000
Devices/VDOMs (Maximum) [3]	—	—	—
Sustained Log Rates	50	50	50
GB/ day	2	2	2
Hardware Specifications			
Storage Capacity	8 TB (2 × 4 TB)	32 TB (8 × 4 TB)	32 TB (8× 4TB)
Usable Storage (after RAID)	4 TB	24 TB	24 TB
RAID Levels Supported	RAID 0/1	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	1	50	50
Hardware Form Factor	1 RU Rackmount	2 RU Rackmount	2 RU Rackmount
Total Interfaces	4xRJ45 GE	4 x GE RJ45, 2 x SFP	2× 2.5GBaseT RJ45 + 2 × 25GbE SFP28
Console Port	RJ45	RJ45	RJ45
Removable Hard Drives	No	✓	✓
Redundant Hot Swap Power Supplies	✓*	✓*	✓
Trusted Platform Module (TPM) [2]	Gen2	✓	✓
Dimensions			
Height x Width x Length (inches)	1.73 × 17.24 × 16.38	3.5 × 17.5 × 22.2	3.46 × 17.24 × 24.41
Height x Width x Length (cm)	4.4 × 43.8 × 41.6	8.8 × 44.5 × 56.5	8.8 × 43.8 × 62.0
Weight	22.5 lbs (10.2 kg)	35.27 lbs (16 kg)	49.6 lbs (22.5 kg)
Environment			
AC Power Supply	100-240V 50-60 Hz	100–240V AC, 50-60 Hz	100–240V AC, 50–60 Hz
Power Consumption (Average / Maximum)	90.1 W / 99 W	140 W / 182 W	251.36 W / 302 W
Heat Dissipation	337.8 BTU/h	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)	32°F to 104°F (0°C to 40°C)
Storage Temperature	-13°F to 167°F (-25°C to 75°C)	-4°F to 167°F (-20°C to 75°C)	-40°F to 158°F (-40°C to 70°C)
Humidity	20% to 90% non-condensing	5% to 95% non-condensing	8% to 90% non-condensing
Forced Airflow	Front to Back	Front to Back	Front to Back
Operating Altitude	Up to 7400 ft (2250 m)	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	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.

* Optional redundant AC power supply, not included.

FortiManager 200G

FortiManager 410G

FortiManager 1000G

Specifications

FORTIMANAGER APPLIANCES	FMG-3100G	FMG-3700G
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)	240TB (60× 4TB) HDD + 19.2TB (6× 3.2TB) NVMe SSD
Usable Storage (after RAID)	56 TB	224 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	3 RU Rackmount	4 RU Rackmount
Total Interfaces	2 x GbE RJ45 ports, 2× 25GbE SFP28 ports	2× 25GE SFP28, 2× 10GE RJ-45
Console Port	DB-9	DB-9
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	7.0 × 17.2 × 30.2
Height x Width x Length (cm)	13.0 × 44.0 × 65.0	17.8 × 43.7 × 76.7
Weight	69.6 lbs (31.57 kg)	120 lbs (54.6 kg)
Environment		
AC Power Supply	100-127V~/10A, 200-240V~/5A Hz	2000W AC 4
Power Consumption (Average / Maximum)	395 W / 510 W	850 W / 1423.4 W
Heat Dissipation	1740.19 BTU/h	4858 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	5% to 95% non-condensing
Forced Airflow	Front to Back	Front to Back
Operating Altitude	Up to 13 123 ft (4000 m)	Up to 7400 ft (2250 m)
Compliance		
Safety Certifications	FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST	FCC Part 15 Class A, RCM, VCCI, CE, BSMI, KC, UL/cUL, CB, GOST

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.

4. The 3700G must connect to a 200V-240V power source.

FortiManager 3100G

FortiManager 3700G

Ordering Information

Product	SKU	Description
FortiManager	FMG-200G	Centralized management appliance — 4x RJ45 GE, 8 TB storage, up to 30x Fortinet devices/VDOMs.
	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-3700G	Centralized management appliance — 2× 25GE SFP28, 2× 10GE RJ-45, 240 TB + 19.2 TB 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.
	FC2-10-FMGVS-258-01-DD	Subscription license for 100 devices/VDOMs managed by FortiManager VM S-series, including FortiCare Premium.
	FC3-10-FMGVS-258-01-DD	Subscription license for 1000 devices/VDOMs managed by FortiManager VM S-series, including FortiCare Premium.
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).

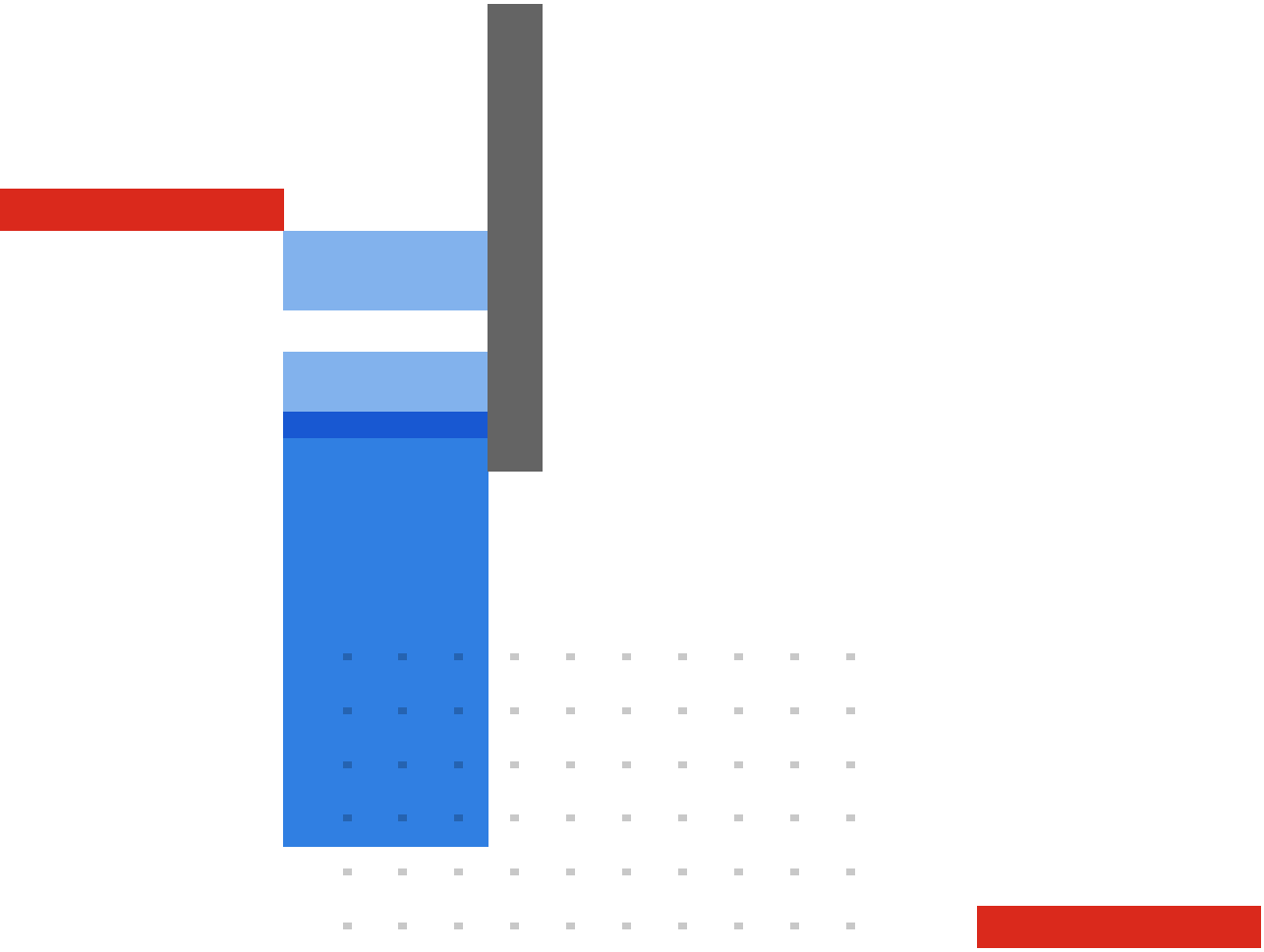
NOTE:

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

For FortiManager-VM Subscription licenses for five ADOMs are included. Additional ADOMs can be purchased.

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

July 10, 2024

FMG-DAT-R80-20240710