

# FortiManager™ Appliances

Centralized Management for Fortinet Security Networks

## Take Control of Your Security Infrastructure

FortiManager centralized management appliances deliver the essential tools needed to effectively manage your Fortinet-based security infrastructure. Whether deploying a few or thousands of new devices or agents, distributing updates, or installing security policies across managed assets, FortiManager appliances drastically reduce management costs and overhead. Device discovery, group management, auditing facilities, and the ability to manage complex mesh and star VPN environments are just a few of the time-saving features that FortiManager appliances offer. Complemented by the FortiAnalyzer™ centralized logging and reporting appliance, the FortiManager appliance is a comprehensive and powerful centralized management solution for your organization.

## Be The Master of Your Domain

Because FortiManager appliances scale to manage thousands of Fortinet devices and agents, we offer a choice of two management modes for increased flexibility. You may choose to manage all assets centrally, with configuration choices being made from the FortiManager user interface. Alternately, you can enable a distributed network of administrators to manage sets of devices and agents based on your definitions. Groupings of devices and agents, along with their administrators, form the FortiManager concept of Administration Domains (ADOMs). And whether you choose the fully centralized or distributed management model, with one or one hundred ADOMs, FortiManager appliances always allow you to manage your Fortinet assets effectively and efficiently.



## Fortinet's Integrated Management Solution

FortiManager appliances provide you with a secure web-based interface for the command and control of your Fortinet security infrastructure. FortiManager appliances also provide centralized policy-based provisioning, configuration, and update management for FortiGate, FortiWiFi, and FortiMail appliances, as well as FortiClient endpoint security agents. Finally, FortiManager includes real-time monitoring capabilities for added visibility.

To complete your centralized management solution, FortiManager seamlessly integrates with our FortiAnalyzer appliances. These appliances provide in-depth discovery, analysis, prioritization, and reporting of the security events detected within your environment. Together, the FortiManager and FortiAnalyzer systems form a comprehensive and enterprise-class management solution.

Features	Benefits
<b>Global or Elemental Management Modes</b>	Allows for centralized or distributed management where some or all management tasks are performed locally
<b>Global Object Database</b>	Facilitates reuse of common configurations across the organization
<b>Appliance-Based Centralized Management</b>	Simplifies the deployment and maintenance associated with the central management solution by eliminating third-party operating systems and hardware requirements
<b>Automated Device Provisioning / Centralized Policy Configuration</b>	Reduces cost of deploying new FortiGate or FortiClient installations and maintain policies across all managed assets
<b>Role-Based Administration</b>	Enables distributed administration, an important requirement for larger organizations
<b>Policy/Device Auditing</b>	Allows you to prove compliance, and track any deviations to the required security policy



FortiManager-100C



FortiManager-400B



FortiManager-1000C



FortiManager-3000C



FortiManager-5001A

Virtual Machine

FortiManager Virtual Appliance

### Administrative Domains (ADOMs)

Enables the primary administrator (admin) to create groupings of devices for other administrators to monitor and manage

- Administrators can maintain the devices specific to their geographic location or business division
- FortiGate units with multiple configured VDOMs can be divided among multiple administrative domains
- When an administrative user logs in, they see only the devices or VDOMs configured for that administrator
- The primary administrator (admin) can see and maintain all administrative domains and the devices within those domains

### Global Object Database

A centralized repository within FortiManager that houses the configuration details of various assets

- Create device configuration templates to quickly configure a new Fortinet appliance
- Reuse similar configurations among a group of managed assets

### Administrative Web Portals

Designed for multi-tenancy applications within a single management platform

- Provides an administrative web portal for customers who require some degree of control over their network security management
- Enables customers to control their own SSL-VPN user list and Web Filtering settings
- If configured, customers can also view the firewall policies for their unit or VDOM

### Locally Hosted Security Content

Hosting security content locally allows the administrator greater control over security content updates and provides improved response time for rating databases

Includes support for

- Antivirus definition updates
- Intrusion Prevention updates
- Vulnerability and Compliance Management updates
- Web Filtering (select systems)
- Antispam (select systems)

### Global and Elemental Management Modes

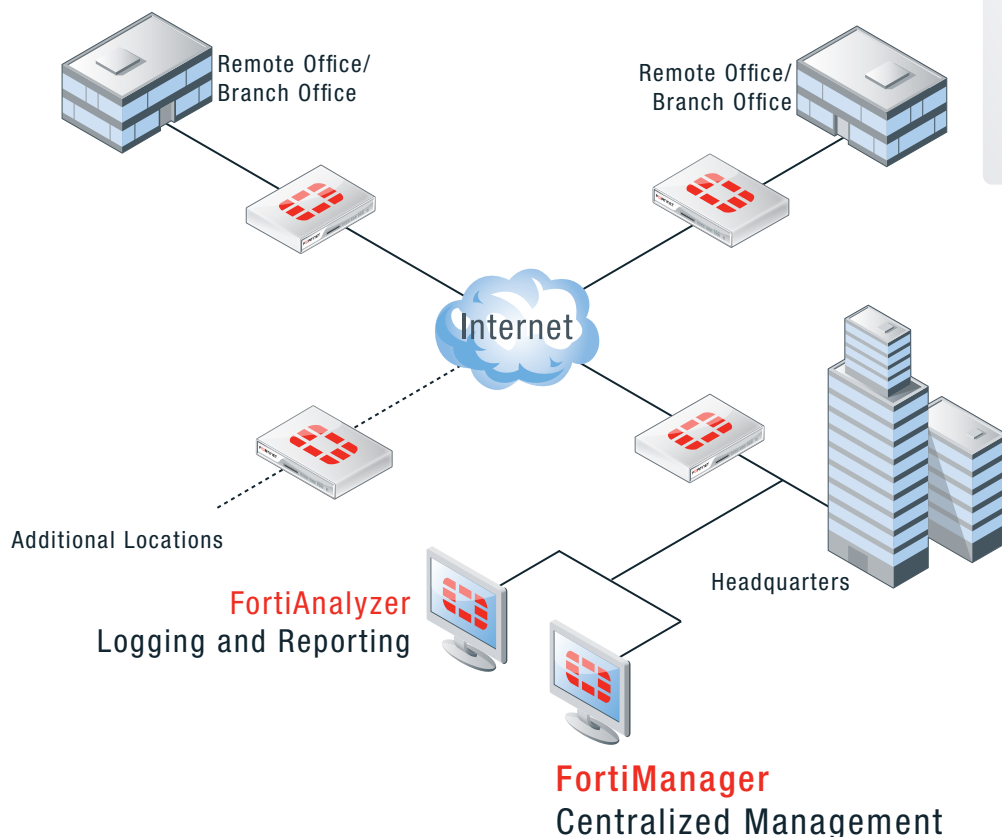
A choice of operating modes adapts to your management model

Global Management System (GMS) mode

- Used to manage multiple devices with a single configuration.
- Each installation has the same policies, groups, VPN configurations and setup
- Configuration is “pushed” to all devices

Element Management System (EMS)

- Enables administrators to manage multiple devices with multiple configurations
- Each installation has a unique or specific configuration, whether its firewall policies, user groups, VPN configurations, etc.



FortiManager	FortiManager-100C	FortiManager-400B	FortiManager-1000C	FortiManager-3000C	FortiManager-5001A
<b>Capacity Specification</b>					
Licensed Network Devices <sup>1</sup> (Max)	20	200	800	5,000	4,000
FortiClient Agents (Max)	2,500	10,000	25,000	120,000	100,000
Administration Domains (ADOMs)	10	10	50	200	100
Administrative Web Portals	10	10	50	100	100
Web Portal Users (Max)	200	200	500	4,000	4,000
Model Restrictions	FortiGate-5000 series hardware	FortiGate-5000 series hardware	FortiGate-5000 series hardware	None	None
Locally Hosted Security Content	Antivirus, Intrusion Prevention, and Vulnerability Management Updates	Antivirus, Intrusion Prevention, and Vulnerability Management Updates	Antivirus, Intrusion Prevention, and Vulnerability Management Updates, Web Filtering and Antispam Databases	Antivirus, Intrusion Prevention, and Vulnerability Management Updates, Web Filtering and Antispam Databases	Antivirus, Intrusion Prevention, and Vulnerability Management Updates, Web Filtering and Antispam Databases
<b>Hardware Specification</b>					
Hardware Form Factor	Desktop	Rack Mount (1-RU)	Rack Mount (1-RU)	Rack Mount (2-RU)	ATCA Blade
10/100 Ethernet (Base-T)	1	–	–	–	–
10/100/1000 Ethernet (Base-T)	2	4	4	4	2
RS-232 Console Port	Yes	Yes	No	Yes	Yes
LCD Display	No	No	Yes	Yes	No
Disk Storage Capacity	1 TB	500 GB	1 TB	2 TB	80 GB
High Availability Support	Yes	Yes	Yes	Yes	Yes
Hot-Swappable Power Supplies	–	–	No	Yes	Yes (Built into chassis)
<b>Dimensions</b>					
Height	1.77 in (4.5 cm)	1.77 in (4.5 cm)	1.69 in (4.30 cm)	3.5 in (8.9 cm)	1.18 in (3.0 cm)
Width	10.79 in (27.4 cm)	17.25 in (43.8 cm)	17.09 in (43.4 cm)	17.5 in (44.5 cm)	14 in (35.5 cm)
Length	6.10 in (15.5 cm)	14.5 in (36.8 cm)	24.69 in (62.71 cm)	29.0 in (73.7 cm)	12.2 in (31.0 cm)
Weight	5.9 lbs (2.66 kg)	10 lbs (4.5 kg)	24.2 lbs (11 kg)	63 lbs (28.6 kg)	8 lbs (3.63 kg)
<b>Environment</b>					
AC Power Required	100 – 240 VAC, 50 – 60 Hz, 0.8 Amp (Max)	100 – 240 VAC, 50 – 60 Hz, 4.0 Amp (Max)	100 – 240 VAC, 50 – 60 Hz, 7.0 Amp (Max)	100 – 240 VAC, 50 – 60 Hz, 9.0 Amp (Max)	N/A (DC powered from system chassis)
Power Consumption (AVG)	56 W	121 W	189 W	200 W	148 W
Heat Dissipation	190.4 BTU	304 BTU	643.6 BTU	868 BTU	505 BTU
Operating Temperature	32 – 104 deg F (0 – 40 deg C)	32 – 104 deg F (0 – 40 deg C)	32 – 104 deg F (0 – 40 deg C)	32 – 104 deg F (0 – 40 deg C)	32 – 104 deg F (0 – 40 deg C)
Storage Temperature	-13 – 158 deg F (-25 – 70 deg C)	-13 – 158 deg F (-25 – 70 deg C)	-13 – 158 deg F (-25 – 70 deg C)	-13 – 158 deg F (-25 – 70 deg C)	-13 – 158 deg F (-25 – 70 deg C)
Humidity	5 to 95% non-condensing	5 to 95% non-condensing	5 to 95% non-condensing	5 to 95% non-condensing	20 to 90% non-condensing
<b>Compliance</b>					
	FCC Class A Part 15, UL/CB/CUL, C Tick, VCCI	FCC Class A Part 15, UL/CB/CUL, C Tick, VCCI	FCC Class A Part 15, UL/CB/CUL, C Tick, VCCI	FCC Class A Part 15, UL/CB/CUL, C Tick, VCCI	FCC Class A Part 15, UL/CB/CUL, C Tick, VCCI

<sup>1</sup> Each Virtual Domain (VDOM) operating on a physical device counts as one licensed network device

### Command and Control

- Manage devices and endpoint agents individually or as logical groups
- Discover new devices automatically
- Create, deploy, and monitor virtual private networks
- Delegate control to other users with distributed administration features
- Audit configuration changes to ensure compliance

### Manage Updates

- Simplify the ongoing maintenance of your Fortinet-based security infrastructure by scheduling device updates

### Monitor, Analyze, and Report

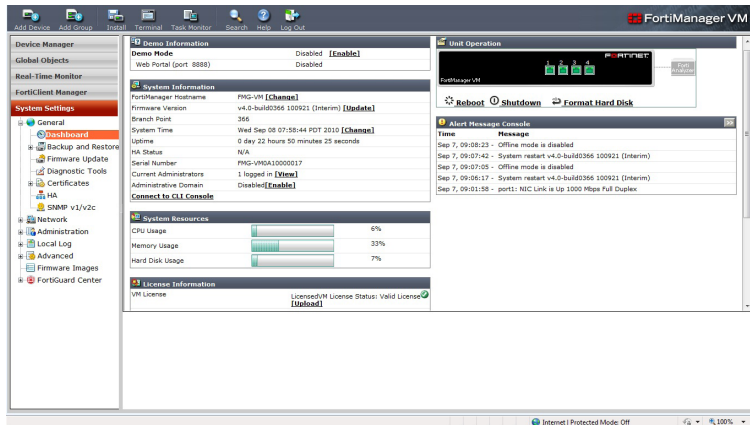
- Access vital security and network statistics
- Combine with a FortiAnalyzer appliance for additional data mining and graphical reporting capabilities.

### Supported Devices & Agents

- FortiGate** Multi-Threat Security Appliances
- FortiClient** Endpoint Security Software
- FortiMail** Messaging Security Appliances
- FortiAnalyzer** Analysis & Reporting Appliances
- FortiSwitch** Security Appliances
- FortiCarrier** Multi-Threat Security Appliances

FortiManager Virtual Appliance	
<b>Capacity Specifications</b>	
Licensed Network Devices <sup>1</sup> (Max)	5,000
FortiClient Agents (Max)	120,000
Administration Domains (ADOMs)	200
Administrative Web Portals	100
Web Portal Users (Max)	4,000
Model Restrictions	None
Locally Hosted Security Content	Antivirus, Intrusion Prevention, and Vulnerability Management updates. Local caching for Web Filtering and Antispam rating databases
<b>Virtual Machine Specifications</b>	
Hypervisors Supported	VMware ESXi/ESX 3.5/4.0/4.1
Virtual Machine Form Factor	Open Virtualization Format (OVF)
Virtual NICs Required	1
Virtual Machine Storage Required (Minimum)	60 GB
Virtual Machine Memory Required (Minimum)	512 MB
High Availability Support	Yes

<sup>1</sup> Each Virtual Domain (VDOM) operating on a physical device counts as one licensed network device



## FortiManager Virtual Appliance

Virtualized infrastructure continues to transform today's IT landscape. From Virtual LANs to servers and user desktops, the IT environment as a whole is increasingly becoming part of a virtualized cloud. To that end, Fortinet offers a virtualized version of our FortiManager appliance. The virtual appliance offers all of the features of our traditional hardware-based FortiManager appliances in a form factor that leverages an existing investment in virtualization technology.

## Fortinet Virtual Appliances

The Fortinet virtual appliance family includes these models:

### FortiGate-VM multi-threat security

- Consolidated security in a virtual form factor

### FortiManager-VM centralized management

- Command and control for Fortinet infrastructure
- Up to 5,000 Fortinet devices
- Up to 120,000 FortiClient endpoint security agents

### FortiAnalyzer-VM centralized analysis and reporting

- Aggregate log data for forensic analysis
- Perform vulnerability assessments of networked hosts
- Generate graphical reports to aid in demonstrating compliance

### FortiMail-VM messaging security

- Block spam and malware from users' inboxes
- Archive mail for compliance and e-discovery purposes

**FortiGuard® Security Subscription Services** deliver dynamic, automated updates for Fortinet products. The Fortinet Global Security Research Team creates these updates to ensure up-to-date protection against sophisticated threats. Subscriptions include antivirus, intrusion prevention, web filtering, antispam, vulnerability and compliance management, application control, and database security services.

**FortiCare™ Support Services** provide global support for all Fortinet products and services. FortiCare support enables your Fortinet products to perform optimally. Support plans start with 8x5 Enhanced Support with "return and replace" hardware replacement or 24x7 Comprehensive Support with advanced replacement. Options include Premium Support, Premium RMA, and Professional Services. All hardware products include a 1-year limited hardware warranty and 90-day limited software warranty.



#### GLOBAL HEADQUARTERS

Fortinet Incorporated  
1090 Kifer Road, Sunnyvale, CA 94086 USA  
Tel +1.408.235.7700  
Fax +1.408.235.7737  
www.fortinet.com/sales

#### EMEA SALES OFFICE – FRANCE

Fortinet Incorporated  
120 rue Albert Caquot  
06560, Sophia Antipolis, France  
Tel +33.4.8987.0510  
Fax +33.4.8987.0501

#### APAC SALES OFFICE – SINGAPORE

Fortinet Incorporated  
300 Beach Road #20-01  
The Concourse  
Singapore 199555  
Tel: +65-6513-3730  
Fax: +65-6223-678

Copyright© 2010 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions. Network variables, different network environments and other conditions may affect performance results, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding contract with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. 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 guarantees. 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. Certain Fortinet products are licensed under U.S. Patent No. 5,623,600.