Controller | Datasheet

Omada Software Controller

Highlights

- **Centralized Management:** Up to 10,000 Omada access points, switches, and gateways/routers.*
- **Cloud Access:** Manage and monitor with the Omada app or Web UI from anywhere, anytime.
- **Free of Charge:** Download and use locally or from the cloud without additional expense.
- **Easy and Intelligent Network Monitoring:** The easy-to-use dashboard makes it simple to see the real-time network status and traffic distribution.
- **Real-Time Network Topology:** Helps IT admins quickly see and troubleshoot connections at a glance.
- **Easier Network Maintenance:** WiFi heatmap simulator, visualizable network report, and batch & multi-site management benefit network maintenance.

Omada Solution

Omada's Software Defined Networking (SDN) platform integrates network devices, including access points, switches, and gateways, providing 100% centralized cloud management. Omada creates a highly scalable network—all controlled from a single interface.

Specifications

Model		Omada Software Controller
System Management	Multi-Site Management	√
	Multi-tenant Management (Role/Site/Device Privileges)	√
	Cloud Access	√
	Migration (Site Migration/Controller Migration)	√
	Account Management	√
	Maximum Number of Sites	1000
	Maximum Number of Accounts	1000
	Maximum Number of Local Accounts	500
	Maximum Number of Cloud Accounts	500
	Maximum Number of Vouchers	50,000
	Maximum Number of Local Users	50,000
	Maximum Simultaneously Used VLANs	4,090 per site*
	Maximum Number of WLAN Groups	5000
	Maximum Number of SSIDs	16 in each site
	Maximum Number of ACL	For each site: Gateway/Router: 64 Switch: 32** EAP: 16
	Maximum Number of Free Authentication	32 in each site
	Maximum Number of Pre-Authentication Access	32 in each site
	Maximum Number of Authentication Free Policy	96 in each site
	Maximum Number of Reboot Schedule	8 in each site
	Maximum Number of PoE Schedule	8 in each site
	Maximum Number of MAC Filter Groups	8 in each site
	Maximum Number of MAC Addresses in Each MAC Filter Group	500 (4,000 in total per controller)
	Maximum Number of VPN	64 in each site
	Maximum Number of Static Routing	64 in each site
	Maximum Number of Policy Routing	64 in each site
	Backup & Restore	√
	Auto Backup	√
	Customized UI Interface	√

* The actual number of VLANs depends on the switch capacity and it may be less than 4090.

** The actual number of ACL depends on the configuration and it may be less than 32.

Model		OC200 V2
Network Management	Wired Network	√
	Wireless Network	√
	Network Security (ACL/URL Fitering/Attack Defense)	√
	Transmission (Routing/NAT/Session Limit/Bandwidth Control)	√
	VPN (IPSec/L2TP/PPTP/OpenVPN)	√
	Portal (Voucher/Local User/SMS/RADIUS/Facebook/ External Portal Server)	√
	802.1x	√
	RADIUS (Authentication/MAC Auth/Accounting)	√
Device Management	Management Device Type	Omada EAP, Omada Switch*, Omada Gateway/Router*
	Management Scale*	≤ 10,000 Devices**
	Device Automatic Discovery	√
	Batch configuration	√
	Online upgrade	√
	Reboot Schedule	√
	PoE Schedule	√
	WLAN Scheduler	√
	DDNS	√
	SNMP	√
	SSH	√
Monitoring	Dashboard (Custom Dashboard)	√
	Statistics (Performance/Switch Stats/Speed Test Stats)	√
	Network topology	√
	Network Map	√
	Devices List (Custom Table)	√
	Clients List (Custom Table)	√
	Insights (Known Clients/Past Connections/Past Portal Authorizations/Rogue APs)	√
	Logs (Alerts/Events/Custom Notifications)	√

*The actual management scale will vary as a result of network environment, bandwidth and different settings.

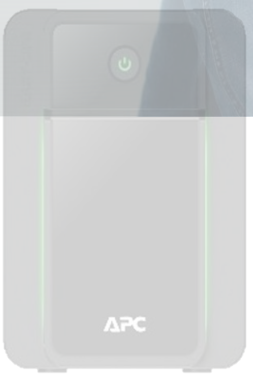
**Omada Software Controller can manage up to 10,000 EAPs if the Controller Host has enough hardware resources. To guarantee operational stability for managing 10,000 EAPs, we recommend that you use the hardware which meets or exceeds the following specifications:

-CPU: Intel Core i3-8100, i5-6500, or i7-4700 with 2 or more cores and 4 or more threads.

-Memory: 6 GB RAM or more.

Advanced Power Protection

APC Back-UPS BX Series 750VA – 2200kVA



APC™ Back-UPS™ BX series is a cost effective power protection solution for home and home office environments.

The series comprehensive VA range with premium features further enables single UPS capabilities

Ideal Power Protection for the following environments and devices:

Home Office

Work from home & remote learning devices

- Modem / Router
- PC Desktop Computer
- PC Monitor
- Network-attached Storage

Home Entertainment

Living room essentials

- Modem / Router
- TV Box
- Television
- Music Speaker

Smart Home

IoT electronics

- Modem / Router
- Smart Speaker
- Home Security / Surveillance Camera

www.apc.com

Life Is On

APC by Schneider Electric

Protect your devices from power surges and outages

How does a UPS protect my uptime?

Power Surge Protection

Stabilizes the main electrical line voltage to your devices

Refined Power Supply

Protects computer and connected devices from dips and spikes caused by lightning

Instant Power

Instant power to your equipment the exact moment the power goes out

Battery backup is key to home continuity

The electronic devices you rely on for communication, security and entertainment depend on a stable network connection,

Ensure reliable uptime and clean power for your critical devices.

Comprehensive Power Capacity Range

Models ranging from 750VA-2200VA; choose a solution aligned with your specific application and runtime needs

Visibility and Manageability Software

In the event of an extended power outage, prevent potential data loss or corruption with PowerChute Personal Edition Software

Form Factor:
Compact for office and business spaces
(BX750MI-FR: 160 x 120 x 355) mm.

Outlets
3-4 battery backup with surge protection outlets

Functional ease-of-use
Front panel LED green lights to easily tell the functional status

1Gb Network Protection
Safeguards your equipment and valuable files from “back door” surges traveling along data lines without sacrificing internet speed

Automatic Voltage Regulation (AVR)
Instantly corrects incoming utility power without utilizing the battery, saving the battery for when it is needed most

Life Is On | APC by Schneider Electric

APC Back-UPS technical specifications

BX Series

	BX750MI-FR	BX950MI-FR	BX1200MI-FR	BX1600MI-FR	BX2200MI-FR
Output					
Power Rating	750VA/410W	950VA/520W	1200VA/650W	1600VA900W	2200VA/1200W
Nominal Output Voltage	230V				
Output Voltage (On Battery)	230+/-10%@ 100% load				
Output Frequency (Hz)	50/60HZ +/-0.5Hz				
Topology	Line Interactive				
Waveform Type	Stepped approximation to a sinewave				
Output Connections (Battery Backup)	3 French	4 French	4 French	4 French	4 French
Input					
Nominal Input Voltage	230V				
Input Connections	CEE7				
Input Cord	1.3 m				
Input Frequency	50 Hz or 60 Hz				
USB Charging	No				
Batteries & runtime					
Battery Type	Maintenance-free sealed Lead-Acid battery with suspended electrolyte :				
Typical Backup Time at ½ Load	8.5 min	6.5 min	5 min	6.5 min	8.5 min
Typical Backup Time at Full Load	1 min	1 min	1 min	1 min	1 min
Typical Recharge Time	6 hours	6-8 hours	8 hours	8 hours	8 hours
Communications & Management					
LED Indicators	Visual LED indicators				
Data Line Protection	RJ 45 Gigabit				
Interface Ports	273				
Software	PowerChute Personal Edition				
Physical					
Dimensions (HxWxD) mm	160 x 120 x 355		190 x 140 x 390		
Weight (kg)	5.4	6.1	7.6	10.3	12.3
Environmental					
Operating Environment	0 - 40 °C				
Operating Relative Humidity	0 - 95 %				
Operating Elevation	0-3000 meters				
Storage Temperature	15 - 40 °C				
Storage Relative Humidity	0-95%				
Conformance					
Approvals	CB Meet EN62040-1 / CE / IEC-62040-1 / IEC-62040-2				
Standard Warranty	2 years repair or replace				
RoHS Compliant	Yes				

Life Is On

APC by Schneider Electric

DIGITUS Charging Trolley for 30 Notebooks / Tablets up to 15.6 inch, USB- C

DN-45006
EAN 4016032494546

Charging trolley, 15.6", USB-C 30 charge bases, PDU, fan, 1260 x 824 x 650 mm

The mobile charging cabinet from DIGITUS® is the ideal and compact solution for storing and charging your portable devices such as notebooks and tablets. Mobile charging cabinets are frequently used in public facilities such as schools in order to store devices securely at a central location while charging them at the same time. The cabinet includes 3 rows with 10 charging stations each, all of which have their own USB connection on the front. The devices can also be connected with installed socket strips (3 x 10 safety sockets) at the back. Thanks to ample cable feedthroughs and excess cable storage, optimal cable management is guaranteed. Installed ventilators (3 x 24 V) combined with ventilation slits ensure active cooling of the cabinet.

The ideal solution for storing and charging your portable devices.

- Double Folding Front and Back Door
- Pressure lock system with swiveling lever handle on the front and back door, lockable
- 180° door opening angle
- 2-point locking (rod lock)
- Incl. 4 rollers (2 lockable)
- Casters can be dismantled if necessary
- Including handles for better mobility (enclosed)
- Product dimensions (H x W x D) in mm: 1260 x 824 x 650 mm
- Safety plug socket (AC) with switch on the side
- C20 connection on the side
- Incl. RCD 30 mA (residual current operated device)
- Delivery is completely assembled
- Depth of inner tray: 415 mm (suitable for up to 15,6" devices)
- USB-C Port Output: 18W (5 V 3A) per port; 540W max.
- Temperature control: Fans start automatically when the internal temperature exceeds 40 °C
- Blue plastic holders can be dismantled if necessary

Attributes

- Color: black, RAL 9005
- Suitable for display size: 39,6 cm (15,6")
- Number of Devices: 30
- USB connection (charging): USB C
- Additional connection (charging): Safety outlets
- UV-C disinfection: no
- Data synchronisation function: no
- Type: Trolley
- Locking type: mechanical

Package contents

- Mobile charging cabinet
- 2 x handle (for installation on outside) including mounting material
- Power cable, 2 m
- User manual
- 4 x keys

Logistics						
	Number (pcs)	Weight (kg)	Depth (cm)	Width (cm)	Height (cm)	cm³
Packaging Unit Carton	1	128.00	69.00	77.00	126.00	669,438.00
Packaging Unit Inside	1	128.00	69.00	77.00	126.00	669,438.00
Packaging Unit Single	1	128.00	69.00	77.00	126.00	669,438.00
Net single without Packaging	1	96.00	65.00	82.40	126.00	0.00

More images:



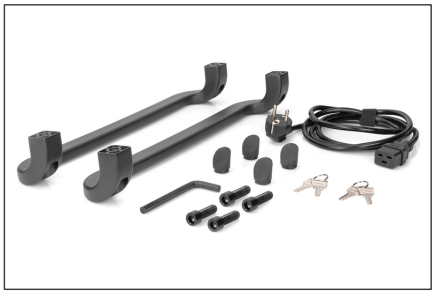












Safety notes

- The product may only be operated on sockets that are protected by a residual current circuit breaker.
- The electrical connection of the product must be made directly to a permanently installed socket.
- The use of multiple sockets or extension cables is not permitted.
- The connection cable must be undamaged. A cable with kinks, crushing or cracks must be replaced immediately.
- Before connecting electrical devices to the product, ensure that the device to be connected, including its connection cable, is in a fault-free and damage-free condition.
- Always insert the plug fully into the socket. It may only be disconnected by pulling on the plug itself - never pull on the cable.
- When operating doors or flaps, care must be taken to ensure that the connecting cables of electrical devices are not crushed or damaged
- Use only in dust and moisture-protected indoor areas
- Prevent higher humidity or temperatures than those specified in the data sheet - Avoid moisture, dust or vapors, solvents, flammable gases.

- Avoid moisture, dust or vapors, solvents, flammable gases.
- The appliance may only be dismantled and transported if the mains plug has been disconnected beforehand.
- Only connect the charging system to an earthed and easily accessible socket.
- Safety must be assessed by a qualified electrician.
- The sockets may only be used with the devices intended for this purpose, for example:
- Chargers for rechargeable batteries and hand-held devices
- Smartphones or tablets (mobile devices)
- Laptops / Notebooks / UltraBooks (mobile computers)
- Mobile batteries / PowerBanks
- Please ensure that the maximum total output specified on the rating plate is not exceeded.
- Please also ensure that no liquids enter the electrical equipment of the cabinet.

EU responsible person

EU based economic operator ensuring the product complies with the required regulations.

ASSMANN Electronic GmbH
Auf dem Schüffel 3
Lüdenscheid, Germany
https://www.assmann.com
info@assmann.com

EAP653

Přístupový bod AX3000 WiFi 6 pro montáž na strop

HARDWARE FEATURES

Interface	1× Gigabit Ethernet (RJ-45) Port (supports IEEE802.3at PoE)
Button	Reset
Power Supply	Power Supply • 802.3at PoE • 12V DC (EU Version: 12 V / 1.0 A DC. US Version: 12 V / 1.5 A DC). Note: DC adapter is not included in the package, and is sold separately • 48V Passive PoE
Power Consumption	• EU: 13.5 W • US: 14.7 W
Dimensions (W x D x H)	6.3 × 6.3 × 1.3 in (160 × 160 × 33.6 mm)
Antenna Type	Internal Omni • 2.4 GHz: 2× 4 dBi • 5 GHz: 2× 5 dBi

HARDWARE FEATURES

Mounting	• Ceiling /Wall Mounting (Kits included) • Junction Box Mounting

WIRELESS FEATURES

Wireless Standards	IEEE 802.11ax/ac/n/g/b/a
Frequency	2.4 GHz and 5 GHz
Signal Rate	• 5 GHz: Up to 2402 Mbps† • 2.4 GHz: Up to 574 Mbps†
Wireless Functions	• 1024-QAM • 4× Longer OFDM Symbol • OFDMA • Multiple SSIDs (Up to 16 SSIDs, 8 for each band) • Enable/Disable Wireless Radio • Automatic Channel Assignment • Transmit Power Control (Adjust Transmit Power on dBm) • QoS(WMM) • MU-MIMO • HE160 (160 MHz Bandwidth)‡ • Seamless Roaming § • Omada Mesh§ • Band Steering • Load Balance • Airtime Fairness • Beamforming • Rate Limit • Reboot Schedule • Wireless Schedule • Wireless Statistics based on SSID/AP/Client
Wireless Security	• Captive Portal Authentication§ • Access Control • Wireless Mac Address Filtering • Wireless Isolation Between Clients • SSID to VLAN Mapping • Rogue AP Detection • 802.1X Support • WPA-Personal/Enterprise, WPA2-Personal/Enterprise, WPA3-Personal/Enterprise
Transmission Power	• CE: <20 dBm(2.4 GHz, EIRP) <23 dBm(5 GHz, Band1 & Band2, EIRP) <30 dBm(5 GHz, Band3, EIRP) • FCC: <25 dBm (2.4 GHz) <25 dBm (5 GHz)

MANAGEMENT

MANAGEMENT

Omada App	Yes
Centralized Management	• Omada Hardware Controller (OC300) • Omada Hardware Controller (OC200) • Omada Software Controller • Omada Cloud-Based Controller
Cloud Access	Yes. Requiring the use of OC300, OC200, Omada Cloud-Based Controller, or Omada Software Controller.
Email Alerts	Yes
LED ON/OFF Control	Yes
Management MAC Access Control	Yes
SNMP	v1, v2c, v3
System Logging Local/ Remote Syslog	Local/Remote Syslog
SSH	Yes
Web-based Management	HTTP/HTTPS
L3 Management	Yes
Multi-site Management	Yes
Management VLAN	Yes
Zero-Touch Provisioning	Yes. Requiring the use of Omada Cloud-Based Controller.

OTHERS

Certification	CE, FCC, RoHS
Package Contents	• EAP653 • Ceiling/Wall Mounting Kits • Installation Guide Note: DC adapter is not included in the package, and is sold separately.
System Requirements	Microsoft Windows XP, Vista, Windows 7, Windows 8, Windows10, Windows 11, Linux
Environment	• Operating Temperature: 0–40 ŷ (32–104 Ø) • Storage Temperature: -40–70 ŷ (-40–158 Ø) • Operating Humidity: 10–90% RH non-condensing • Storage Humidity: 5–90% RH non-condensing

†Maximální rychlosti bezdrátového připojení jsou fyzické rychlosti odvozené ze specifikace standardu IEEE 802.11. Skutečná propustnost dat v bezdrátové síti a její pokrytí garantovány a budou se lišit na základě 1) faktorů okolního prostředí včetně stavebních materiálů, fyzických objektů a překážek, 2) síťových podmínek včetně místního rušen hustoty datových přenosů, umístění produktu, složitosti a režie sítě a 3) omezení klientů včetně jmenovitého výkonu, umístění, připojení, kvality a stavu klienta.

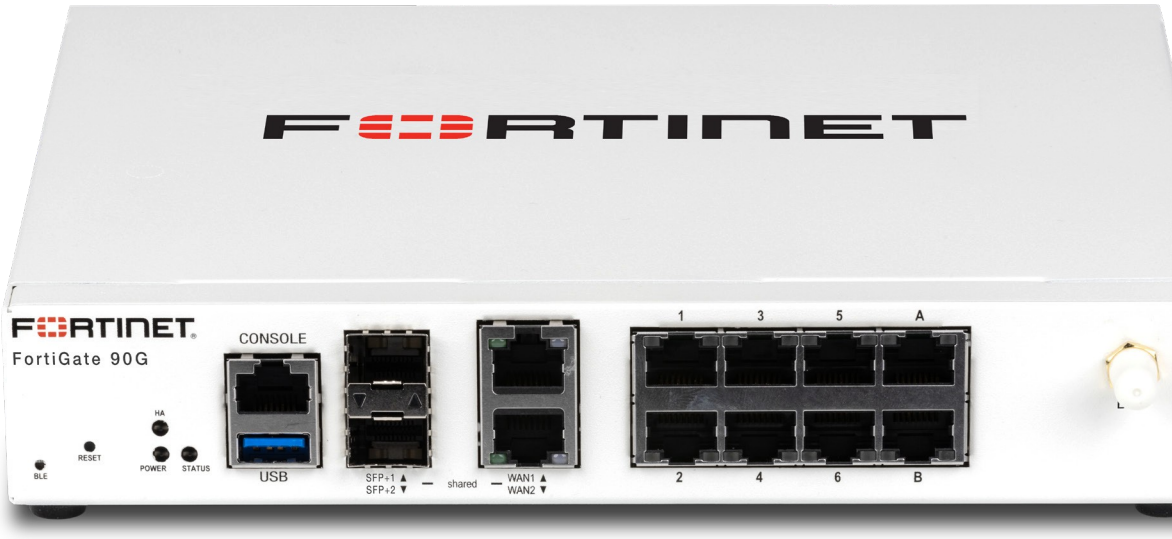
‡ Použití standardu WIFI 6 (802.11ax) a jeho funkcí, včetně OFDMA, HE160 a 1024-QAM, vyžaduje, aby klienty rovněž podporovaly odpovídající funkce. 160MHz šířka pásma je dostupná pouze v pásmu 5 GHz. V některých regionech/zemích může být nedostupná v důsledku regulačních omezení. Dvojnásobná šířka pásma odkazuje na 160 MHz ve srovnání s 80 MHz u přístupových bodů podporujících standard WIFI 6.

§ Omada Mesh, plynulé přepínání mezi připojenými zařízeními a přihlašovací portál vyžadují použití kontrolerů Omada SDN. Na stránce https://www.tp-link.com/en/omada-mesh/product-list/ najdete všechny modely, které podporují technologii Omada Mesh. Možnosti konfigurace kontrolerů Omada SDN jsou uvedeny v příslušných uživatelských příručkách.

* Funkce ZTP (Zero-Touch Provisioning), automatický výběr kanálu a nastavení spotřeby energie vyžadují použití cloudového kontroleru Omada. Na stránce https://www.tp-link.com/en/omada-cloud-based-controller/product-list/ si můžete ověřit, které modely podporují cloudové kontrolery Omada.

Sledujte nás

FortiGate 90G Series



Highlights

Gartner® Magic Quadrant™ Leaders for both Network Firewalls and SD-WAN

Unparalleled performance enabled by Fortinet's patented ASIC and the FortiOS operating system

Enterprise-grade protection with FortiGuard AI-Powered Security Services

Simplified operations with centralized management for networking and security, automated workflows, deep analytics, and self-healing

Inclusive SD-WAN and wireless controller in every FortiGate appliance at no extra cost

Rich portfolio for any business budget and need

Converged Next-Generation Firewall and SD-WAN

The FortiGate 90G series integrate firewalling, SD-WAN, and security in one appliance, making them perfect for building secure networks at distributed enterprise sites and transforming WAN architecture at any scale.

The 90G series runs on FortiOS, the industry's first converged networking and security operating system. This single OS approach enables businesses to gain benefits of operational efficiency and unified protection from the seamless integration of Fortinet Solutions within a Hybrid Mesh Firewall architecture.

As a cornerstone of the Fortinet Security Fabric platform, the FortiGate NGFW works seamlessly with FortiGuard AI-Powered Security Services to deliver coordinated, automated, end-to-end threat protection in real time.

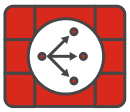
The 90G family is built on the patented SD-WAN-based ASIC, which delivers unmatched performance over traditional CPUs with lower cost and reduced power consumption. This application-specific design and embedded multi-core processor further accelerate the convergence of networking and security functions in the 90G family to optimize secure connections and deiver a robust user experience at branch locations.

IPS	NGFW	Threat Protection	Interfaces
4.5 Gbps	2.5 Gbps	2.2 Gbps	Multiple GE RJ45, 10 GE RJ45, and SFP+ Share Media Slots | Variants with internal storage

Use Cases

Perimeter Protection

- Protect networks from malicious traffic, guard against file-based threats, block web-based attacks, and secure applications and data with natively integrated FortiGuard AI-Powered Security Services
- Inspect and control incoming and outgoing traffic based on defined security policies
- Perform real-time SSL inspection (including TLS 1.3) with full visibility into users, devices, and applications across the attack surface
- Accelerate performance, protection, and energy efficiency with Fortinet's patented SPU with converged security and networking technologies



Secure SD-WAN

- FortiGate enables best-of-breed WAN edge with integrated SD-WAN, WAN optimization, security, and unified management from a single FortiOS operating system
- FortiGate, built on a patented SD-WAN-based ASIC, delivers faster application identification to avoid delays in accessing applications and acceerates overlay performance regardless of location
- Enhances hybrid working with a comprehensive SASE solution by integrating cloud-delivered SD-WAN with security service edge (SSE)
- Achieves operational efficiencies at any scale through automation, deep analytics, and self-healing

Secure Branch

- The Fortinet Security Fabric platform enables FortiGate NGFWs to automatically discover and secure IoT devices for faster branch onboarding
- Fully integrated with FortiSwitch secure Ethernet switches and FortiAP access points, FortiGate easily extends security to WAN, LAN, and WLAN at branch offices for unified protection and reliable connectivity
- FortiGate and Fortinet products work seamlessly with FortiManager to centralize visibility and simplify management across locations for IT teams
- FortiGate HA support ensures continuous network protection and minimizes downtime in the event of hardware failures or network disruptions

Universal ZTNA

Control access to applications no matter where the user is and no matter where the application is hosted for universal application of access policies.

- Provide extensive authentications, checks, and enforce policy prior to granting application access every time
- Agent-based access with FortiClient or agentless access via proxy portal for guest or BYOD

FortiGuard AI-Powered Security Services

FortiGuard AI-Powered Security Services is part of Fortinet's layered defense and tightly integrated into our FortiGate NGFWs and other products. Infused with the latest threat intelligence from FortiGuard Labs, these services protect organizations against modern attack vectors and threats, including zero-day and sophisticated AI-powered attacks.

Network and file security

Network and file security services protect against network and file-based threats. With over 18,000 signatures, our industry-leading intrusion prevention system (IPS) uses AI/ML models for deep packet/SSL inspection, detecting and blocking malicious content, and applying virtual patches for newly discovered vulnerabilities. Anti-malware protection defends against both known and unknown file-based threats, combining antivirus and sandboxing for multi-layered security. Application control improves security compliance and provides real-time visibility into applications and usage.

Web/DNS security

Web/DNS security services protect against DNS-based attacks, malicious URLs (including those in emails), and botnet communications. DNS filtering blocks the full spectrum of DNS-based attacks while URL filtering uses a database of over 300 million URLs to identify and block malicious links. Meanwhile, IP reputation and anti-botnet services guard against botnet activity and DDoS attacks. FortiGuard Labs blocks over 500 million malicious/phishing/spam URLs weekly, and blocks 32,000 botnet command-and-control attempts every minute, demonstrating the robust protection offered through Fortinet.

SaaS and data security

SaaS and data security services cover key security needs for application use and data protection. This includes data loss prevention to ensure visibility, management, and protection (blocking exfiltration) of data in motion across networks, clouds, and users. Our inline cloud access security broker service protects data in motion, at rest, and in the cloud, enforcing compliance standards and managing account, user, and cloud app usage. Services also assess infrastructure, validate configurations, and highlight risks and vulnerabilities, including IoT device detection and vulnerability correlation.

Zero-Day threat prevention

Zero-day threat prevention is achieved through AI-powered inline malware prevention to analyze file content to identify and block unknown malware in real time, delivering sub-second protection across all NGFWs. The service also integrates the MITRE ATT&CK matrix to speed up investigations. Integrated into FortiGate NGFWs, the service provides comprehensive defense by blocking unknown threats, streamlining incident response, and reducing security overhead.

OT security

With over 1000 virtual patches, 1100+ OT applications, and 3300+ protocol rules, integrated OT security capabilities detect threats targeting OT infrastructure, perform vulnerability correlation, apply virtual patching, and utilize industry-specific protocol decoders for robust defense of OT environments and devices.

Available in

Appliance

Virtual

Hosted

Cloud

Container

FortiOS Everywhere

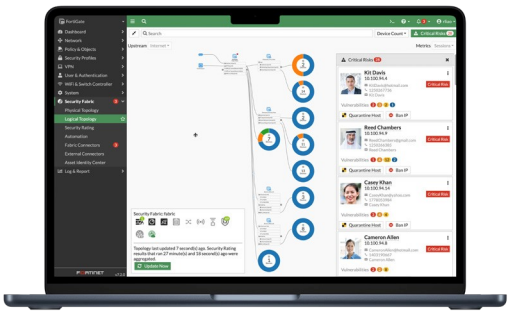
FortiOS, Fortinet's Real-Time Network Security Operating System

FortiOS is the operating system that powers Fortinet Security Fabric platform, enabling enforcement of security policies and holistic visibility across the entire attack surface. FortiOS provides a unified framework for managing and securing networks, cloud-based, hybrid, or a convergence of IT, OT, and IoT. FortiOS enables seamless and efficient interoperation across Fortinet products with consistent and consolidated AI-powered protection across today's hybrid environments.

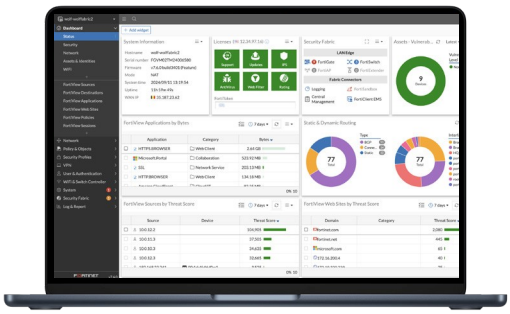
Unlike traditional point solutions, Fortinet adopts a holistic approach to cybersecurity, aiming to reduce complexities, eliminate security silos, and improve operational efficiencies. By consolidating security functions into a single platform, FortiOS simplifies management, reduces costs, and enhances overall security posture. Together, FortiGate and FortiOS create intelligent, adaptive protection to help organizations reduce complexity, eliminate security silos, and optimize user experience.

By integrating generative AI (GenAI), FortiOS further enhances the ability to analyze network traffic and threat intelligence, detects deviations or anomalies more effectively, and provides more precise remediation recommendations, ensuring minimum performance impact without compromising security.

Learn more about what's new in FortiOS. https://www.fortinet.com/products/fortigate/fortios

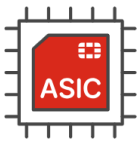


Intuitive easy to use view into the network and endpoint vulnerabilities



Comprehensive view of network performance, security, and system status

Fortinet ASICs: Unrivaled Security, Unprecedented Performance



Powered by the only purpose-built SPU

Traditional firewalls cannot protect against today's content and connection-based threats because they rely on off-the-shelf general-purpose central processing units (CPUs), leaving a dangerous security gap. Fortinet's custom SPUs deliver the power you need to radically increase speed, scale, and efficiency while greatly improving user experience and reducing footprint and power requirements. Fortinet's SPUs deliver up to 520 Gbps of protected throughput to detect emerging threats and block malicious content while ensuring your network security solution does not become a performance bottleneck.

Fortinet ASICs are designed to be energy-efficient, leading to lower power consumption and improved TCO. They deliver industry-leading throughput, handle more traffic and perform security inspections faster, reduce latency for quicker packet processing and minimize network delays.

Fortinet SPUs are designed with integrated security functions like zero trust, SSL, IPS, and VXLAN to name but a few, dramatically improving the performance of these functions that competitors traditionally implement in software.

Secure SD-WAN ASIC SP5

- Combines a RISC-based CPU with Fortinet's proprietary SPU content and network processors for unmatched performance
- Delivers the industry's fastest application identification and steering for efficient business operations
- Accelerates IPsec VPN performance for the best user experience on direct internet access
- Enables best-of-breed NGFW security and deep SSL inspection with high performance
- Extends security to the access layer to enable SD-Branch transformation with accelerated and integrated switch and access point connectivity

Unified Management for Optimal Security and Efficiency

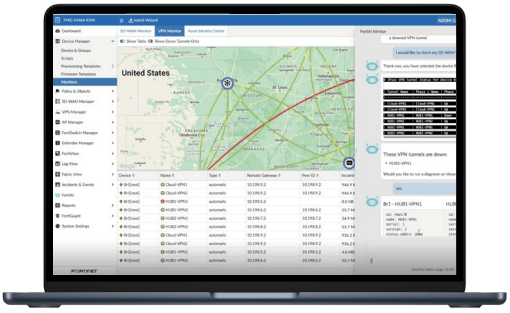
Whether you are a small business or a large enterprise, Fortinet provides centralized control, visibility, and automation for your security infrastructure.

FortiManager: Centralized management at scale for distributed enterprises

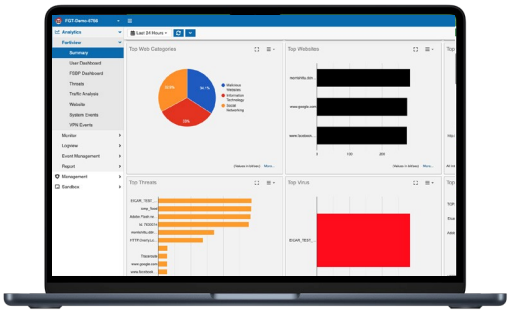
FortiManager, powered by FortiAI, is a centralized management solution for the Fortinet Security Fabric. It streamlines mass provisioning and policy management for FortiGate, FortiGate VM, cloud security, SD-WAN, SD-Branch, FortiSASE, and ZTNA in hybrid environments. Additionally, FortiManager provides real-time monitoring of the entire managed infrastructure and automates network operation workflows. Leveraging GenAI in FortiAI, it further enhances Day 0–1 configurations and provisioning, and Day N troubleshooting and maintenance, unlocking the full potential of the Fortinet Security Fabric and significantly boosting operational efficiency.

FortiGate Cloud: Simplified management for small and mid-size businesses

FortiGate Cloud is a SaaS service offering simplified management, security analytics, and reporting for Fortinet FortiGate NGFWs to help you more efficiently manage your devices and reduce cyber risk. It simplifies the initial deployment, setup, and ongoing management of FortiGates and downstream connected devices such as FortiAP, FortiSwitch, and FortiExtender, with zero-touch provisioning. It provides real-time and historical visibility into traffic analytics and security threats to reduce risks and improve security posture. View various threats, web traffic, and system events stored in the cloud for up to a year, with predefined reports to meet compliance and deliver actionable insights.



GenAI in FortiManager helps manage networks effortlessly—generate configuration and policy scripts, troubleshoot issues, and execute recommended actions.



FortiGate Cloud provides intuitive management and analytics solution with end-to-end visibility, logging and reporting for SMB.

FortiConverter Service

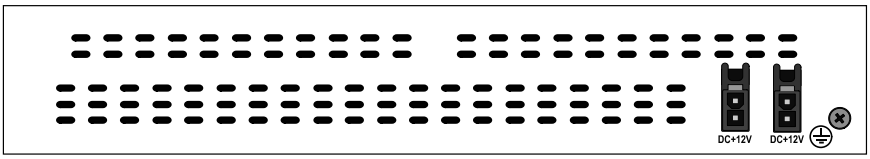
Migration to FortiGate NGFW made easy

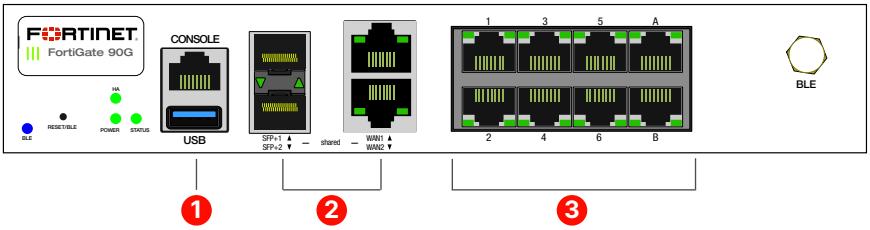
The FortiConverter Service provides hassle-free migration to help organizations transition quickly and easily from a wide range of legacy firewalls to FortiGate NGFWs. The service eliminates errors and redundancy by employing best practices with advanced methodologies and automated processes. Organizations can accelerate their network protection with the latest FortiOS technology.

Hardware

FortiGate 90G/91G

SP5 DESKTOP 120GB





Interfaces

1. 1x RJ45 Console and 1x USB Management Port
2. 2× 10/5/2.5/ GE RJ45 or 10GE/GE SFP+/SFP Shared Media Ports
3. 8x GE RJ45 Ports

Hardware Features

Trusted Platform Module (TPM)

The FortiGate 90G series features a dedicated module that hardens physical networking appliances by generating, storing, and authenticating cryptographic keys. Hardware-based security mechanisms protect against malicious software and phishing attacks.

Compact and reliable form factor

Designed for small environments, the FortiGate can be on a desktop or wall-mounted. It is small, lightweight, yet highly reliable with superior meantime between failures, minimizing the chance of network disruption.

Specifications

	FORTIGATE 90G	FORTIGATE 91G
Hardware Specifications		
10/5/2.5/GE RJ45 or 10GE/GE SFP+/ SFP Shared Media pairs	2	2
GE RJ45 Internal Ports	8	8
Wireless Interface	—	—
USB Ports	1	1
Console (RJ45)	1	1
Internal Storage	–	1 × 120 GB SSD
Trusted Platform Module (TPM)	✓	✓
Bluetooth Low Energy (BLE)	✓	✓
Signed Firmware Hardware Switch	—	—
System Performance* — Enterprise Traffic Mix		
IPS Throughput [2]	4.5 Gbps	
NGFW Throughput [2, 4]	2.5 Gbps	
Threat Protection Throughput [2, 5]	2.2 Gbps	
System Performance and Capacity		
Firewall Throughput (1518 / 512 / 64 byte UDP packets)	28 / 28 / 27.9 Gbps	
Firewall Latency (64 byte UDP packets)	3.23 µs	
Firewall Throughput (Packets Per Second)	41.85 Mpps	
Concurrent Sessions (TCP)	3 M	
New Sessions/Second (TCP)	124 000	
Firewall Policies	5000	
IPsec VPN Throughput (512 byte) [1]	25 Gbps	
Gateway-to-Gateway IPsec VPN Tunnels	200	
Client-to-Gateway IPsec VPN Tunnels	2500	
SSL-VPN Throughput [6]	1.4 Gbps	
Concurrent SSL-VPN Users (Recommended Maximum, Tunnel Mode)	200	
SSL Inspection Throughput (IPS, avg. HTTPS) [3]	2.6 Gbps	
SSL Inspection CPS (IPS, avg. HTTPS) [3]	1400	
SSL Inspection Concurrent Session (IPS, avg. HTTPS) [3]	300 000	
Application Control Throughput (HTTP 64K) [2]	6.7 Gbps	
CAPWAP Throughput (HTTP 64K)	23.6 Gbps	
Virtual Domains (Default / Maximum)	10 / 10	
Maximum Number of FortiSwitches Supported	24	
Maximum Number of FortiAPs (Total / Tunnel Mode)	128 / 64	
Maximum Number of FortiTokens	500	
High Availability Configurations	Active-Active, Active-Passive, Clustering	

	FORTIGATE 90G	FORTIGATE 91G
Dimensions		
Height x Width x Length (inches)	1.65 × 8.5 × 7.0	
Height x Width x Length (mm)	42 × 216 × 178	
Weight	2.47 lbs (1.12 kg)	
Form Factor	Desktop	
Operating Environment and Certifications		
Input Rating	12V DC, 3A (dual redundancy optional)	
Power Required (Redundancy Optional)	Powered by up to 2 External DC Power Adapters (1 adapter included), 100–240V AC, 50/60 Hz	
Power Supply Efficiency Rating	80Plus Compliant	
Power Required (Redundancy Optional)	Powered by up to 2 External DC Power Adapters (1 adapter included), 100–240V AC, 50/60 Hz	
Maximum Current	115Vac/0.4A, 230Vac/0.2A	
Power Consumption (Average / Maximum)	19.9 W / 20.53 W	22.4 W / 23.5 W
Heat Dissipation	70.0 BTU/hr	80.1 BTU/hr
Operating Temperature	32°F to 104°F (0°C to 40°C)	
Storage Temperature	-31°F to 158°F (-35°C to 70°C)	
Humidity	10% to 90% non-condensing	
Noise Level	21.73 dBA	
Operating Altitude	Up to 10 000 ft (3048 m)	
Compliance	FCC, ICES, CE, RCM, VCCI, BSMI, UL/cUL, CB	
Certifications	USGv6/IPv6	

Note: All performance values are “up to” and vary depending on system configuration.

[1] IPsec VPN performance test uses AES256-SHA256.

[2] IPS (Enterprise Mix), Application Control, NGFW and Threat Protection are measured with Logging enabled.

[3] SSL Inspection performance values use an average of HTTPS sessions of different cipher suites.

[4] NGFW performance is measured with Firewall, IPS and Application Control enabled.

[5] Threat Protection performance is measured with Firewall, IPS, Application Control and Malware Protection enabled.

[6] SSL VPN only supported between 7.0.12 and 7.0.15

Subscriptions

Service Category	Service Offering	A-la-carte	Bundles		
			Enterprise Protection	Unified Threat Protection	Advanced Threat Protection
FortiGuard Security Services	IPS — IPS, Malicious/Botnet URLs	•	•	•	•
	Anti-Malware Protection (AMP)—AV, Botnet Domains, Mobile Malware, Virus Outbreak Protection, Content Disarm and Reconstruct [3], AI-based Heurestic AV, FortiGate Cloud Sandbox	•	•	•	•
	URL, DNS and Video Filtering — URL, DNS and Video [3] Filtering, Malicious Certificate	•	•	•	
	Anti-Spam		•	•	
	AI-based Inline Malare Prevention [3]	•	•		
	Data Loss Prevention (DLP) [1]	•	•		
	Attack Surface Security — IoT Device Detection, IoT Vulnerability Correlation and Virtual Patching, Security Rating, Outbreak Check	•	•		
	OT Security—OT Device Detection, OT vulnerability correlation and Virtual Patching, OT Application Control and IPS [1]	•			
	Application Control		----------included with FortiCare Subscription----------		
	Inline CASB [3]		----------included with FortiCare Subscription----------		
SD-WAN and SASE Services	SD-WAN Underlay Bandwidth and Quality Monitoring	•			
	SD-WAN Overlay-as-a-Service	•			
	SD-WAN Connector for FortiSASE Secure Private Access	•			
	SASE connector for FortiSASE Secure Edge Management (with 10Mbps Bandwidth) [2]	•			
NOC and SOC Services	FortiConverter Service for one time configuration conversion	•	•		
	Managed FortiGate Service—available 24×7, with Fortinet NOC experts performing device setup, network, and policy change management	•			
	FortiGate Cloud—Management, Analysis, and One Year Log Retention	•			
	FortiManager Cloud	•			
	FortiAnalyzer Cloud	•			
	FortiGuard SOCaaS—24×7 cloud-based managed log monitoring, incident triage, and SOC escalation service	•			
Hardware and Software Support	FortiCare Essentials [2]	•			
	FortiCare Premium	•	•	•	•
	FortiCare Elite	•			
Base Services	Device/OS Detection, GeoIPs, Trusted CA Certificates, Internet Services and Botnet IPs, DDNS (v4/v6), Local Protection, PSIRT Check, Anti-Phishing		----------included with FortiCare Subscription----------		

1. Full features available when running FortiOS 7.4.1.
2. Desktop Models only.
3. Not available for FortiGate/FortiWiFi 40F, 60E, 60F, 80E, and 90E series from 7.4.4 onwards.

FortiGuard AI-Powered Security Bundles for FortiGate

FortiGuard AI-Powered Security Bundles provide a comprehensive and meticulously curated selection of security services to combat known, unknown, zero-day, and emerging AI-based threats. These services are designed to prevent malicious content from breaching your defenses, protect against web-based threats, secure devices throughout IT/OT/IoT environments, and ensure the safety of applications, users, and data. All bundles include FortiCare Premium Services featuring 24×7×365 availability, one-hour response for critical issues, and next-business-day response for noncritical matters.

FortiCare Services

Fortinet prioritizes customer success through FortiCare Services, optimizing the Fortinet Security Fabric solution. Our comprehensive life-cycle services include Design, Deploy, Operate, Optimize, and Evolve. The FortiCare Elite, one of the service offerings, provides heightened SLAs and swift issue resolution with a dedicated support team. This advanced support option includes an extended end-of-engineering support of 18 months, providing flexibility and access to the intuitive FortiCare Elite portal for a unified view of device and security health, streamlining operational efficiency and maximizing Fortinet deployment performance.

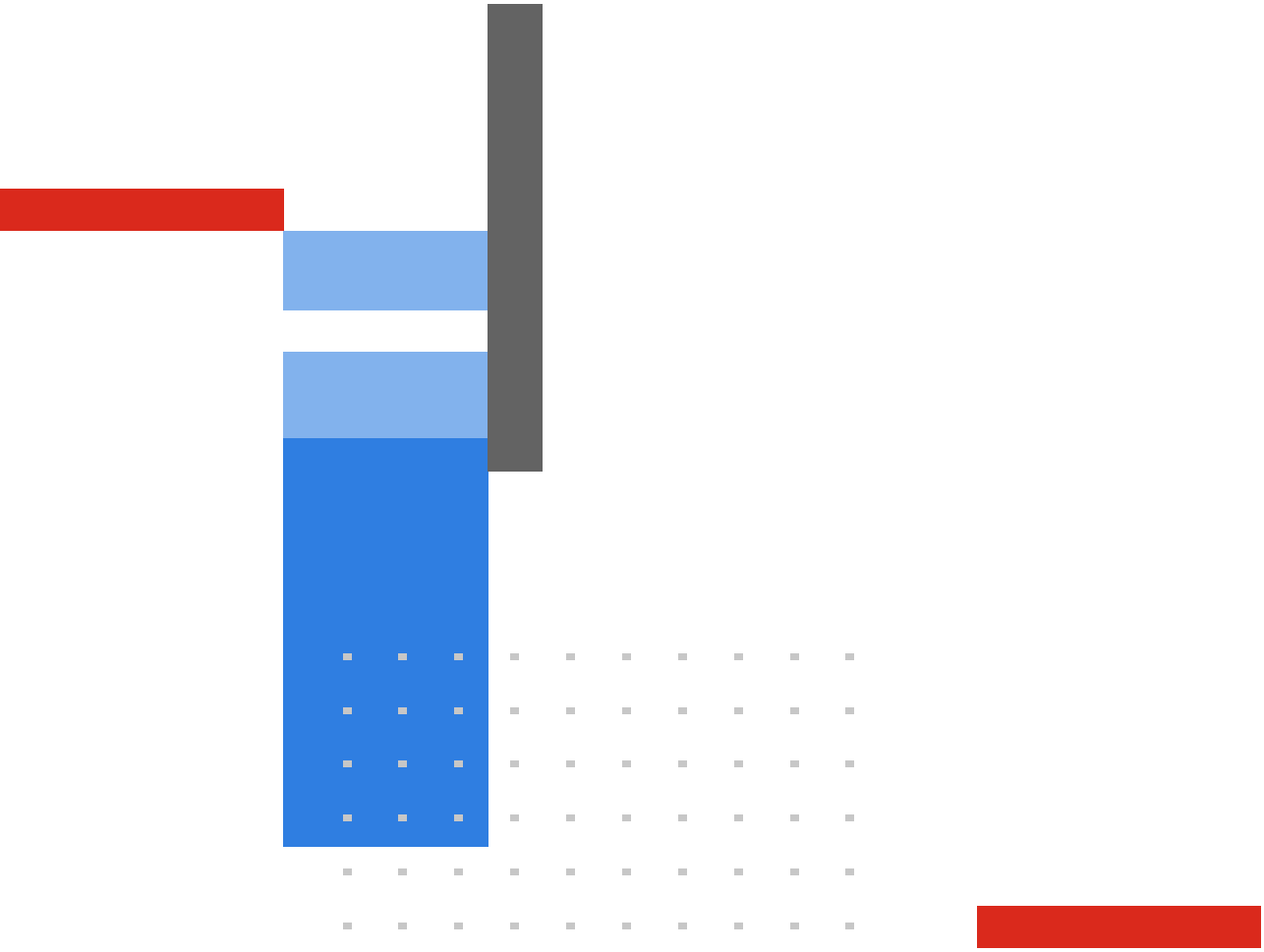
Ordering Information

Product	SKU	Description
FortiGate 90G	FG-90G	8x GE RJ45 ports, 2× 10GE RJ45/SFP+ shared media WAN ports.
FortiGate 91G	FG-91G	8x GE RJ45 ports, 2× 10GE RJ45/SFP+ shared media WAN ports with 120GB SSD.
Optional Accessories		
AC Power Adaptor	SP-FG60E-PDC-5	Pack of 5 AC power adaptors for FG/FWF 60E/61E, 60F/61F, 70/71F, 70/71G, 80E/81E, 80/81F, 90/91G and FDC-100G. Power cable SP-FG60CPCOR-XX sold separately
Wall Mount Kit	SP-FG60F-MOUNT-20	Pack of 20 wall mount kits for FG/FWF-60F, FG-90G/91G and FG/FWF-80F series.
Rack Mount Tray	SP-RACKTRAY-02	Rack mount tray for all FortiGate E, F, and G series desktop models.
Mounting Ear Bracket	SP-EAR-FG90G-10	Mounting Ear brackets for FG-90/91G 10 pairs pack.
Transceivers		
1 GE SFP RJ45 Transceiver Module	FN-TRAN-GC	1 GE SFP RJ45 transceiver module for all systems with SFP and SFP/SFP+slots.
1 GE SFP SX Transceiver Module	FN-TRAN-SX	1 GE SFP SX transceiver module for all systems with SFP and SFP/SFP+ slots.
1 GE SFP LX Transceiver Module	FN-TRAN-LX	1 GE SFP LX transceiver module for all systems with SFP and SFP/SFP+ slots.
10 GE SFP+ RJ45 Transceiver Module	FN-TRAN-SFP+GC	10 GE SFP+ RJ45 transceiver module for systems with SFP+ slots.
10 GE SFP+ Transceiver Module, Short Range	FN-TRAN-SFP+SR	10 GE SFP+ transceiver module, short range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Long Range	FN-TRAN-SFP+LR	10 GE SFP+ transceiver module, long range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, Extended Range	FN-TRAN-SFP+ER	10 GE SFP+ transceiver module, extended range for all systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Transceiver Module, 30km Long Range	FN-TRAN-SFP+BD27	10 GE SFP+ transceiver module, 30km long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD33, ordered separately).
10 GE SFP+ Transceiver Module, (connects to FN-TRAN-SFP+BD27, ordered separately)	FN-TRAN-SFP+BD33	10 GE SFP+ transceiver module, 30km long range single BiDi for systems with SFP+ and SFP/SFP+ slots (connects to FN-TRAN-SFP+BD27, ordered separately).
Cables		
10 GE SFP+ Passive Direct Attach Cable, 1m	FN-CABLE-SFP+1	10 GE SFP+ passive direct attach cable, 1m for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Passive Direct Attach Cable, 3m	FN-CABLE-SFP+3	10 GE SFP+ passive direct attach cable, 3m for systems with SFP+ and SFP/SFP+ slots.
10 GE SFP+ Passive Direct Attach Cable, 5m	FN-CABLE-SFP+5	10 GE SFP+ passive direct attach cable, 5m for systems with SFP+ and SFP/SFP+ slots.

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

Fortinet Corporate Social Responsibility Policy

Fortinet is committed to driving progress and sustainabiity 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

February 25, 2025

FG-90G-DAT-R11-20250225