

[Manuals.plus](#) /

› [FORTINET](#) /

› Fortinet FortiGate-900D 1 Year SD-WAN Cloud Assisted Monitoring Service User Manual

FORTINET FortiGate-900D

Fortinet FortiGate-900D SD-WAN Cloud Assisted Monitoring Service User Manual

Model: FortiGate-900D | Part Number: FC-10-00900-288-02-12

INTRODUCTION

This manual provides essential instructions for the Fortinet FortiGate-900D 1 Year SD-WAN Cloud Assisted Monitoring Service. It covers the service overview, setup, operational guidelines, and support information to ensure optimal performance and utilization of your Fortinet SD-WAN monitoring solution.

The FortiGate-900D SD-WAN Cloud Assisted Monitoring Service offers cloud-based bandwidth and quality monitoring for your SD-WAN infrastructure, enhancing visibility and control over network performance.



Image: Fortinet Activation Key box, representing the software license for the monitoring service.

SERVICE OVERVIEW

The Fortinet FortiGate-900D SD-WAN Cloud Assisted Monitoring Service is designed to provide comprehensive visibility into your SD-WAN network's performance. This cloud-based service assists in monitoring bandwidth utilization and network quality, crucial for maintaining efficient and reliable network operations.

Key Features

- Cloud-based SD-WAN Bandwidth Monitoring
- Cloud-based SD-WAN Quality Monitoring

- Integration with FortiGate-900D appliances
- 1-Year Service Duration

FortiGuard Subscription Options

Here is a brief overview of the FortiGuard subscription feeds available for your organizations:

Next-Generation Application Control and IPS

Application control and intrusion prevention (IPS) are foundational security technologies for a Next-Generation Firewall like FortiGate. FortiGuard IPS blocks approximately 470,000 network intrusions, and new IPS signatures are being created and uploaded to deployed devices every single day.



Web Filtering

On any given day, FortiGuard Labs processes nearly 50 million URL categorization requests and blocks over 160,000 malicious websites. The FortiGuard Web Filtering service rates over 250 million websites and delivers nearly 1.5 million new URL ratings every week. Websites are categorized into six major categories for fast control, and nearly 80 micro-categories for fine-tuned control.



Antivirus

FortiGuard Labs has identified and neutralized nearly 100,000 malware programs targeting traditional, mobile, and IoT platforms. Patented technologies such as the Fortinet Content Pattern Recognition Language (CPRL) enable FortiGuard antivirus to identify thousands of current and future malware variants with a single signature – optimizing your deployment's security effectiveness and performance.



Web Application Security Service

The FortiWeb Security subscription service provides fully automated updates to protect your sensitive data and content from the latest application-layer threats. FortiGuard Labs provides updates on the latest advanced application vulnerabilities, bots, suspicious URL patterns, data-type patterns, and heuristic detection engines to enable FortiWeb Security-enabled appliances to prevent both new and evolving-application threats from gaining access to your web applications.



Antispam

Email is still the #1 vector for the start of an advanced attack on an organization, so a highly effective antispam solution should be a key part of any security strategy. FortiGuard Antispam detects unwanted and often malicious email with global spam filtering that uses sender IP reputation and spam signatures. To keep your antispam solution optimized, FortiGuard Labs delivers nearly 46 million new and updated spam rules every single week. The FortiGuard Antispam feed is available for both the FortiMail and FortiGate solutions.



Vulnerability Scan

The FortiGuard Vulnerability Scan service helps the FortiClient solution accurately identify and manage the latest software vulnerabilities on endpoint devices. It identifies the OS and applications, and discovers known vulnerabilities in versions of software currently running on the endpoints in your organization. It also provides timely remediation intelligence to help you remediate systems that have been identified as vulnerable.



Botnet IP and Domain Reputation

Every minute of every day, FortiGuard Labs blocks approximately 32,000 botnet command & control communication attempts. A key part of a botnet's attack kill chain requires an infected device to communicate with a command & control server – either to download additional threats or to exfiltrate stolen data. FortiGuard's IP and domain address reputation tools block this communication, thereby neutralizing these threats.



Database Security Control

FortiGuard's Database Security service offers centrally managed, enterprise-scale database protection for Fortinet's FortiDB product line. Automated content updates provide the latest pre-configured policies that cover known exploits, configuration weaknesses, OS issues, operational risks, data access privileges, and industry/regulatory best practices.



Mobile Security Service

Protect your organization against attacks targeting your mobile platforms. Fortinet's Mobile Security Service gives you the ability to create effective protection against the latest threats targeting mobile devices. It employs industry-leading advanced detection engines to prevent both new and evolving threats from gaining a foothold inside your network and its invaluable content.



Advanced Threat Protection (FortiSandbox Cloud)

Thousands of organizations leverage FortiSandbox to identify advanced threats. FortiSandbox utilizes the full FortiGuard antivirus database, along with community reputation lookups, platform-independent code emulation, and virtual sandboxing to identify zero-day threats and attacks using new evasion tactics. The FortiSandbox Cloud service leverages this same FortiSandbox technology, and is integrated with the FortiGate platform.



Image: Overview of Fortinet Security Subscriptions, highlighting various threat intelligence and protection services that complement the monitoring service.

SETUP AND ACTIVATION

Prerequisites

- An active FortiGate-900D appliance.
- Internet connectivity for cloud service access.
- A FortiCloud account.
- The provided activation key (FC-10-00900-288-02-12).

Activation Steps

1. Log in to your FortiCloud account at support.fortinet.com.
2. Navigate to the "Asset Management" section.
3. Select "Register Product" and enter your activation key (FC-10-00900-288-02-12).
4. Follow the on-screen prompts to link the service to your FortiGate-900D device.
5. Once activated, the monitoring service will begin collecting data from your FortiGate appliance.

OPERATING THE MONITORING SERVICE

After activation, the SD-WAN Cloud Assisted Monitoring Service operates in the background, continuously collecting and analyzing data from your FortiGate-900D.

Accessing Monitoring Data

1. Log in to your FortiCloud account.
2. Access the FortiGate Cloud portal.
3. Navigate to the SD-WAN monitoring dashboard.
4. View real-time and historical data on bandwidth usage, latency, jitter, and packet loss for your SD-WAN links.

Interpreting Metrics

- **Bandwidth Utilization:** Indicates the amount of data transmitted over your SD-WAN links. High utilization may suggest network congestion.
- **Latency:** The time delay for data packets to travel across the network. Lower values are generally better for performance.
- **Jitter:** Variation in packet delay. High jitter can negatively impact real-time applications like VoIP and video conferencing.
- **Packet Loss:** Percentage of data packets that fail to reach their destination. High packet loss severely degrades network performance and reliability.

MAINTENANCE AND BEST PRACTICES

- Regularly review your SD-WAN monitoring dashboards to identify potential issues and performance trends early.
- Ensure your FortiGate-900D firmware is kept up to date to benefit from the latest features, security enhancements, and bug fixes.
- Verify continuous internet connectivity for your FortiGate appliance to ensure uninterrupted data transmission to the cloud monitoring service.
- Periodically back up your FortiGate configuration to facilitate quick recovery in case of unforeseen issues.

TROUBLESHOOTING COMMON ISSUES

Service Not Reporting Data

- **Check FortiGate Connectivity:** Ensure the FortiGate-900D has active and stable internet access.
- **Verify Service Activation:** Confirm the monitoring service is correctly activated and linked to your device within your FortiCloud account.
- **Firewall Rules:** Ensure no firewall rules on your network are inadvertently blocking communication between the FortiGate and FortiCloud services.

Inaccurate Data Readings

- **Firmware Update:** Ensure your FortiGate-900D is running the latest stable firmware version.
- **Service Status:** Check the operational status of the monitoring service within your FortiCloud account for any reported issues.

SPECIFICATIONS

- **Product:** Fortinet FortiGate-900D 1 Year SD-WAN Cloud Assisted Monitoring Service
- **Model:** FortiGate-900D
- **Part Number:** FC-10-00900-288-02-12
- **Service Duration:** 1 Year
- **Service Type:** Cloud-based SD-WAN Bandwidth & Quality Monitoring
- **Manufacturer:** FORTINET
- **ASIN:** B07WCD5YZK

SUPPORT AND WARRANTY

For technical assistance, product support, or warranty inquiries, please refer to the official Fortinet support channels.

FortiCare Support Services

Fortinet offers various FortiCare support services to assist with product operation and troubleshooting, ensuring you have access to expert help when needed.

FortiCare Support Services



FortiCare 8x5 Service

Get access to technical support via the web portal, online chat system, and telephone, including return and replace for hardware failures. You'll also have fast and easy written access to technical support requests.



FortiCare 24x7 Service

If you need 'round-the-clock access to mission-critical support services, the 24x7 Service will meet your requirements. You'll get access to technical support 365x24x7 as well as advanced replacement service for hardware failures.



FortiCare 360 Service

FortiCare 360 Advanced Services Technical Support is a "pound of prevention," combining Fortinet's cloud-based analytics with premium support to enable organizations to take a more proactive approach to the rapid detection and remediation of current and potential security and performance issues associated with the FortiGate and FortiWifi devices to avoid breaches and downtime.

Image: Overview of FortiCare Support Services, detailing 8x5, 24x7, and 360 support options for Fortinet products.

- **Online Resources:** Visit the Fortinet Support website at support.fortinet.com for comprehensive documentation, knowledge base articles, and community forums.
- **Technical Support:** Contact Fortinet technical support directly for assistance with service activation, configuration, or advanced troubleshooting.
- **Warranty Information:** Details regarding the service warranty are available on the official Fortinet website or through your authorized reseller.

Manufacturer: FORTINET.

Date First Available: February 26, 2021.

FORTIGUARD SUBSCRIPTION OPTIONS (RELATED SERVICES)

While the FortiGate-900D SD-WAN Cloud Assisted Monitoring Service focuses on performance, Fortinet also offers a suite of FortiGuard subscriptions that enhance security and network intelligence. These are separate services but often complement a robust network infrastructure by providing additional layers of protection.

Security Subscriptions

New cyber threats emerge every moment of every day. The highly commercialized cybercriminal ecosystem constantly changes its attacks and techniques. Whether it's a ransomware family, phishing campaign, or infrastructural vulnerability—organizations must constantly be prepared to defend against something new at all times. That's where the threat research and intelligence of FortiGuard Labs is critical. Extensive knowledge of the threat landscape, combined with the ability to respond quickly at multiple levels, is the foundation for providing effective security. Spanning 10 distinct security disciplines, hundreds of researchers at FortiGuard Labs scour the cyber landscape and proactively seek out new avenues of attack every day to discover (and ideally preempt) emerging threats. The FortiGuard team develops effective countermeasures to protect more than 320,000 Fortinet customers around the world. These countermeasures include up-to-the-minute threat intelligence, delivered as a subscription service for Fortinet security products.

Security Subscriptions include:



Up-to-the minute threat intelligence in real time to stop the latest threats



High fidelity with mature and rigorous back-end processes



Insight into threats anywhere in the world through a global network of more than three million sensors



Prevention of exploitation of new avenues of attack with proactive threat research



Fast and comprehensive intelligence via automated and advanced analytics (such as machine learning) being applied to cross-discipline information



Top-rated effectiveness achieved through the commitment to independent, real-world testing

Image: Detailed overview of various FortiGuard subscription options, including Next Generation Application Control, Antivirus, Antispam, Botnet IP & Domain Reputation, Mobile Security Service, Web Filtering, Web Application Security Service, Vulnerability Scan, Database Security Control, and Advanced Threat Protection.

This image illustrates additional security and intelligence services offered by Fortinet, which can be integrated with FortiGate devices to provide comprehensive network protection beyond basic monitoring.

ASK A QUESTION ABOUT THIS MANUAL

Ask about setup, troubleshooting, compatibility, parts, safety, or missing instructions. Manuals+ will review the question and use this page's manual context to help answer it.

Name

Anonymous

Email

you@example.com

After a successful submission, we securely hash the supplied account or form email before sending it to Microsoft Advertising for conversion attribution. [Privacy details](#).

Question

Example: How do I reset this device or fix this error?

Details

Model number, symptoms, what you tried, or the section of the manual you are using.

Submit question

Open the live page

<https://manuals.plus/asin/B07WCD5YZK>

More documents and user manuals: <https://manuals.plus/>