

FORTINET FortiGate-60E-DSL

Fortinet FortiGate-60E-DSL FortiGuard IPS Service User Manual

1. INTRODUCTION TO FORTIGUARD IPS SERVICE

This manual provides essential information for the Fortinet FortiGuard IPS (Intrusion Prevention System) Service, specifically for the FortiGate-60E-DSL model. The FortiGuard IPS Service is a critical component of network security, designed to protect against various cyber threats.

Fortinet's IPS technology is integrated into its FortiGate firewalls, offering high-performance threat detection and prevention. This service leverages Fortinet's extensive threat intelligence to identify and block malicious activities before they impact your network.

2. SERVICE ACTIVATION AND SETUP

The FortiGuard IPS Service is provided as a license subscription. To activate your service, follow these steps:

- Purchase Confirmation:** Ensure you have purchased the correct license for your FortiGate-60E-DSL device. The manufacturer part number for this service is FC-10-FG60E-108-02-12.
- License Delivery:** The license contract is typically delivered via email within 1-2 business days after purchase. Check your inbox and spam folders for an email from Fortinet or your reseller containing the activation key or instructions.
- Access FortiCare Portal:** Navigate to the FortiCare support portal (support.fortinet.com) and log in with your Fortinet account. If you do not have an account, you will need to register.
- Register Product/Service:** Within the FortiCare portal, locate the option to 'Register Product' or 'Activate Service'. Enter the license key or registration code provided in your email.
- Associate with FortiGate-60E-DSL:** Follow the on-screen prompts to associate the FortiGuard IPS service with your specific FortiGate-60E-DSL appliance. This typically involves entering the serial number of your device.
- Verify Activation:** Once registered, the service status should update in your FortiCare account and on your FortiGate device's management interface.



Image 2.1: Representation of a Fortinet Activation Key box. This image illustrates the typical packaging for a Fortinet service license, which contains the necessary activation key for service registration.

3. OPERATING THE FORTIGUARD IPS SERVICE

The FortiGuard IPS Service operates by continuously monitoring network traffic for known and emerging threats. It uses a comprehensive database of threat signatures and behavioral analysis to detect and prevent intrusions.

Key aspects of the FortiGuard IPS Service include:

- **Real-time Threat Intelligence:** The service receives up-to-the-minute threat intelligence from FortiGuard Labs, ensuring protection against the latest vulnerabilities and attack methods.
- **Signature-Based Detection:** It identifies known attack patterns and exploits using an extensive database of IPS signatures.
- **Anomaly Detection:** Beyond signatures, the IPS can detect unusual network behavior that may indicate a zero-day attack or sophisticated intrusion attempt.
- **Automated Prevention:** Upon detection, the IPS automatically blocks malicious traffic, preventing it from reaching internal systems.
- **Reporting and Logging:** The FortiGate device provides detailed logs and reports on IPS activity, allowing administrators to monitor threats and assess network security posture.

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 3.1: Overview of Fortinet Security Subscriptions. This image highlights the comprehensive nature of Fortinet's security offerings, including the FortiGuard IPS, which benefits from global threat intelligence and proactive countermeasures.

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 3.2: Detailed FortiGuard Subscription Options. This graphic provides a breakdown of various FortiGuard services, including Next Generation Application Control and IPS, Antivirus, Web Application Security, Antispam, Vulnerability Scan, Botnet IP and Domain Reputation, Mobile Security, and Advanced Threat Protection. The FortiGuard IPS service is a core component of these integrated security solutions.

4. MAINTENANCE AND RENEWAL

To ensure continuous protection, it is crucial to maintain an active FortiGuard IPS service subscription. Fortinet designs its support and subscriptions to be continuous.

- **Renewal Process:** You will typically receive notifications prior to your service expiration date. It is recommended to renew your subscription before it expires to avoid any lapse in service.
- **Lapse in Service:** If a subscription is not renewed by its expiration date, a lapse in the service period occurs. During this period, your FortiGate-60E-DSL will not receive the latest IPS signature updates, potentially leaving your network vulnerable to new threats.
- **Reactivation:** If your service lapses, you will need to purchase a new or renewal license and reactivate it through the FortiCare portal, similar to the initial setup process.

5. TROUBLESHOOTING

If you encounter issues with your FortiGuard IPS Service, consider the following troubleshooting steps:

- **Verify License Status:** Log in to your FortiCare account to confirm that your FortiGuard IPS subscription is active and correctly associated with your FortiGate-60E-DSL device.
- **Check FortiGate Configuration:** Ensure that IPS features are enabled and correctly configured on your FortiGate-60E-DSL through its web-based management interface.
- **Network Connectivity:** Confirm that your FortiGate device has stable internet connectivity to reach FortiGuard update servers.
- **Review Logs:** Examine the system and IPS logs on your FortiGate for any error messages or indications of issues.
- **Firmware Updates:** Ensure your FortiGate-60E-DSL is running a supported and up-to-date firmware version.
- **Contact Support:** If problems persist, refer to the Fortinet support section of this manual or visit the Fortinet support website for further assistance.

6. SPECIFICATIONS

The FortiGuard IPS Service is designed for integration with the Fortinet FortiGate-60E-DSL appliance. Key specifications related to the service and its associated hardware include:

Attribute	Detail
Service Type	FortiGuard IPS Subscription
Duration	1 Year
Compatible Model	FortiGate-60E-DSL
Manufacturer Part Number	FC-10-FG60E-108-02-12
Manufacturer	FORTINET
Associated Hardware Weight	Approximately 1 pound (for FortiGate-60E-DSL)

7. FORTICARE SUPPORT SERVICES

Fortinet offers various FortiCare support services to assist users with their products and subscriptions. These services provide access to technical support and hardware replacement options.

- **FortiCare 8x5 Service:** This service provides access to technical support via the web portal, online chat system, and telephone during standard business hours (8 hours a day, 5 days a week). It typically includes return and replace service for hardware failures and written access to technical support requests.
- **FortiCare 24x7 Service:** For mission-critical requirements, the 24x7 service offers round-the-clock access to technical support 365 days a year. This includes advanced replacement service for hardware failures, ensuring minimal downtime.
- **FortiCare 360 Service:** The FortiCare 360 Advanced Services Technical Support is a proactive service combining Fortinet's cloud-based analytics with premium support. It enables organizations to take a more proactive approach to rapid detection and remediation of potential security and performance issues associated with FortiGate and FortiWiFi devices.



Image 7.1: Overview of FortiCare Support Services. This image illustrates the different tiers of FortiCare support available, including 8x5, 24x7, and 360 services, each offering varying levels of technical assistance and hardware support.

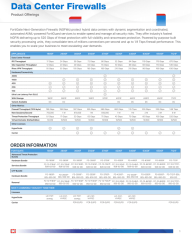

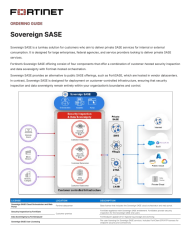


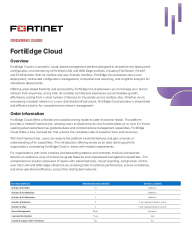
For detailed information on your specific FortiCare contract and to access support resources, please visit the official Fortinet support website: support.fortinet.com.

8. WARRANTY INFORMATION

Specific warranty details for Fortinet services and hardware are subject to Fortinet's official warranty policy. For comprehensive information regarding the warranty terms and conditions applicable to your FortiGate-60E-DSL device and the FortiGuard IPS Service, please refer to the official Fortinet website or your purchase agreement documentation.

Typically, service subscriptions like FortiGuard IPS are covered under the terms of the associated hardware warranty or a separate service agreement. It is recommended to review these documents for full details on coverage, duration, and claims procedures.

Related Documents - FortiGate-60E-DSL

	<p>Fortinet Data Center Firewalls: Ordering Guide and Specifications</p> <p>Comprehensive ordering guide for Fortinet Data Center Firewalls (NGFWs), detailing product offerings, appliance specifications, order information, and frequently asked questions for high-performance network security.</p>
	<p>FortiOS 7.4 IPS Concept Guide: Understanding Intrusion Prevention Systems</p> <p>A comprehensive guide to FortiOS 7.4's Intrusion Prevention System (IPS), covering detection methodologies, types, use cases, and benefits for network security.</p>
	<p>Fortinet Sovereign SASE Ordering Guide: Private SASE Solution</p> <p>Comprehensive ordering guide for Fortinet's Sovereign SASE, a private Secure Access Service Edge solution for enterprises and service providers, detailing components, SKUs, and FAQs.</p>
	<p>FortiOS 7.4.1 Release Notes - Fortinet</p> <p>Official release notes for FortiOS 7.4.1 by Fortinet. Details new features, enhancements, changes in CLI/GUI, resolved issues, known issues, and upgrade information for Fortinet's network security operating system.</p>
	<p>FortiOS 7.4.5 Release Notes: Key Changes, Issues, and Upgrade Guide</p> <p>Comprehensive release notes for FortiOS 7.4.5, detailing new features, resolved issues, known problems, and essential upgrade information for Fortinet's network security operating system.</p>
	<p>FortiEdge Cloud Ordering Guide: Network Management Platform</p> <p>This guide provides detailed ordering information for FortiEdge Cloud, Fortinet's cloud-based management platform for FortiAP, FortiSwitch, and FortiExtender. It covers features, licensing tiers, product SKUs, and frequently asked questions.</p>

