Saved from manuals.plus.
Open the live page for links to other documents and user manuals.

FORTINET FortiSandbox Cloud Service

Fortinet FortiWeb-400D FortiSandbox Cloud Service User Manual

Model: FortiSandbox Cloud Service (FC-10-V0404-123-02-12)

1. Introduction

This manual provides essential information for the activation, operation, and maintenance of your Fortinet FortiWeb-400D 1 Year FortiSandbox Cloud Service. This service is designed to provide advanced threat protection by analyzing suspicious files and URLs in a secure, isolated environment to identify zero-day threats and advanced persistent threats.

The FortiSandbox Cloud Service integrates with Fortinet security products to enhance your organization's security posture against evolving cyber threats.

2. Service Activation and Setup

The FortiSandbox Cloud Service is activated using a unique activation key. Upon purchase, you will receive an activation key that is essential for initiating your 1-year service subscription.



Image: Fortinet Activation Key Box. This image displays the packaging for the Fortinet Activation Key, which is required to activate the FortiSandbox Cloud Service.

2.1. Activation Steps

1. **Locate Your Activation Key:** The activation key is typically provided on a physical card or via email upon purchase.
2. **Access Fortinet Support Portal:** Navigate to the official Fortinet Support Portal (support.fortinet.com). If you do not have an account, you will need to register.
3. **Register the Product:** Within the portal, locate the "Product Registration" section. Enter your activation key and follow the on-screen prompts to register your FortiSandbox Cloud Service.
4. **Link to FortiWeb-400D:** Ensure your FortiWeb-400D appliance is properly configured and connected to the internet. The FortiSandbox Cloud Service will be linked to your FortiWeb-400D appliance through the Fortinet management interface.
5. **Verify Service Status:** After registration, verify the service status within your FortiWeb-400D management interface to confirm that the FortiSandbox Cloud Service is active and operational.

For detailed configuration instructions specific to your FortiWeb-400D appliance, refer to the FortiWeb Administration Guide available on the Fortinet documentation website.

3. Operating the FortiSandbox Cloud Service

The FortiSandbox Cloud Service operates by providing advanced threat protection capabilities, primarily through dynamic analysis of suspicious content. It is an integral part of Fortinet's comprehensive security ecosystem, leveraging FortiGuard Security Subscriptions.

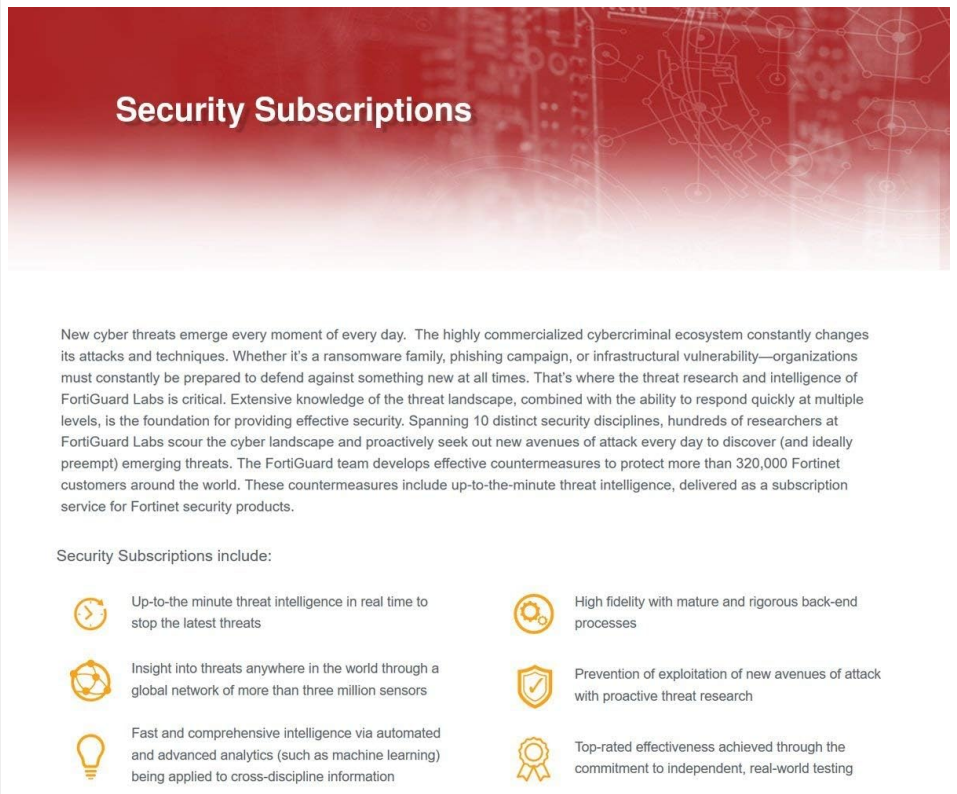

Image: Fortinet Security Subscriptions Overview. This image illustrates the various security subscriptions offered by Fortinet, including up-to-the-minute threat intelligence, insight into threats, fast and comprehensive intelligence, high fidelity processes, prevention of exploitation, and top-rated effectiveness.

3.1. Key Features and Functionality

- **Advanced Threat Protection (ATP):** The FortiSandbox Cloud Service provides a secure environment to execute and analyze suspicious files and URLs, identifying malicious behavior that might bypass traditional security measures.

- **Zero-Day Threat Detection:** By observing the actual behavior of unknown files, the service can detect previously unseen (zero-day) threats.
- **Integration with FortiWeb-400D:** The service seamlessly integrates with your FortiWeb-400D appliance, allowing it to send suspicious content for analysis and receive threat intelligence updates.
- **Threat Intelligence Updates:** Leveraging FortiGuard Labs, the service continuously updates its threat intelligence, ensuring protection against the latest cyber threats.

3.2. FortiGuard Subscription Options

The FortiSandbox Cloud Service is part of a broader suite of FortiGuard Subscription Options that enhance the security capabilities of Fortinet products. These include:

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: FortiGuard Subscription Options. This image details various FortiGuard services including Next-Generation Application Control and IPS, Web Filtering, Antivirus, Web Application Security Service, Antispam, Vulnerability Scan, Botnet IP and Domain Reputation, Database Security Control, Mobile Security Service, and Advanced Threat Protection (FortiSandbox Cloud).

- **Advanced Threat Protection (FortiSandbox Cloud):** Utilizes FortiSandbox Cloud for dynamic analysis of suspicious files and URLs to identify zero-day threats.
- **Next-Generation Application Control and IPS:** Provides application control and intrusion prevention.
- **Web Filtering:** Filters malicious and inappropriate web content.
- **Antivirus:** Detects and neutralizes malware.
- **Web Application Security Service:** Protects web applications from various attacks.
- **Antispam:** Filters unwanted and malicious email.
- **Vulnerability Scan:** Helps identify vulnerabilities on endpoints.
- **Botnet IP and Domain Reputation:** Blocks communication with known botnet command and control servers.
- **Database Security Control:** Provides database security and compliance.
- **Mobile Security Service:** Protects mobile platforms.

For detailed information on configuring and utilizing these features with your FortiWeb-400D, consult the FortiWeb Administration Guide.

4. Maintenance

Maintaining your FortiSandbox Cloud Service ensures continuous and effective threat protection. As a cloud-based service, much of the maintenance is handled by Fortinet, but user responsibilities include monitoring and ensuring active subscriptions.

4.1. Subscription Management

- **Monitor Expiry:** Keep track of your 1-year service subscription expiry date to ensure timely renewal and uninterrupted protection.
- **Renewal:** Renew your FortiSandbox Cloud Service subscription through your Fortinet partner or the Fortinet Support Portal before it expires.

4.2. Monitoring and Reporting

- **Review Logs and Reports:** Regularly review the logs and reports generated by your FortiWeb-400D appliance regarding the FortiSandbox Cloud Service. This provides insights into detected threats and service performance.
- **FortiCloud Access:** Utilize your FortiCloud account to access detailed analytics and reports related to your FortiSandbox Cloud Service.

5. Troubleshooting

Should you encounter issues with your FortiSandbox Cloud Service, consider the following troubleshooting steps:

- **Verify Subscription Status:** Ensure your FortiSandbox Cloud Service subscription is active and has not expired. Check this on the Fortinet Support Portal.
- **Check Network Connectivity:** Confirm that your FortiWeb-400D appliance has stable internet connectivity and can reach Fortinet's cloud services.
- **Review FortiWeb Logs:** Examine the system logs on your FortiWeb-400D for any error messages related to the FortiSandbox Cloud Service.
- **Firewall Rules:** Ensure that any firewalls between your FortiWeb-400D and the internet are not blocking necessary communication ports for Fortinet cloud services.

- **Firmware Updates:** Ensure your FortiWeb-400D appliance is running the latest recommended firmware version.
- **Contact Fortinet Support:** If issues persist, gather relevant logs and information and contact Fortinet Technical Support for assistance.

6. Specifications

The following specifications pertain to the FortiSandbox Cloud Service and its associated product information:

Attribute	Value
Manufacturer	FORTINET
Item Model Number	FortiSandbox Cloud Service
Associated Product	FortiWeb-400D
Service Duration	1 Year
ASIN	B01FRBM068
Date First Available	August 3, 2017
Item Weight (Packaging)	1 Pounds

7. FortiCare Support Services

Fortinet offers comprehensive FortiCare Support Services to ensure the optimal performance and reliability of your Fortinet products and services, including the FortiSandbox Cloud Service. These services provide technical assistance, hardware replacement, and advanced support options.

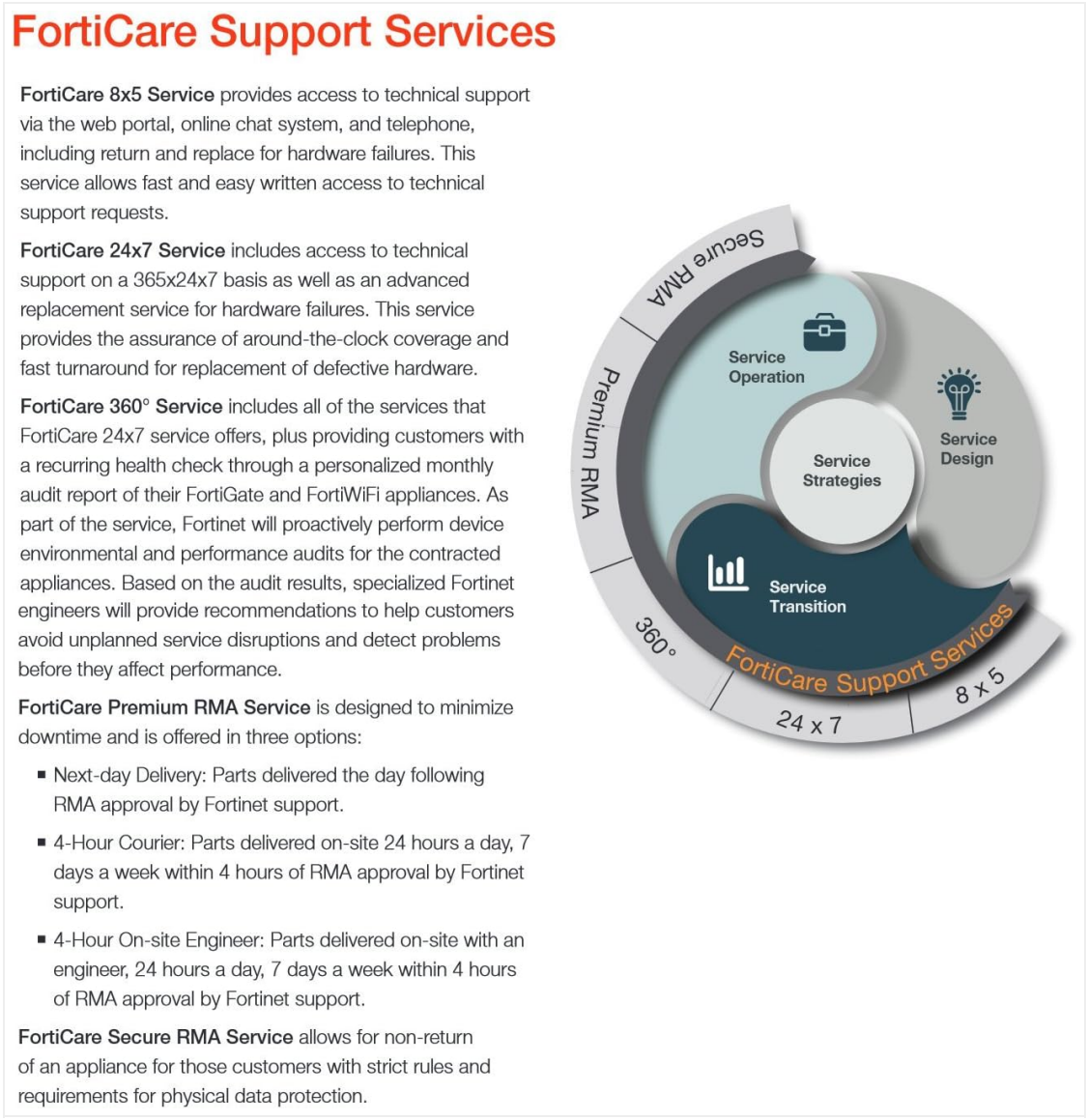

Image: FortiCare Support Services Details. This image provides a detailed breakdown of FortiCare services, including 8x5, 24x7, and 360 support, along with information on FortiCare Premium RMA Service options (Next-day, 4-Hour Courier, 4-Hour On-site Engineer) and FortiCare Secure RMA Service.

7.1. FortiCare Service Tiers

- **FortiCare 8x5 Service:** Provides access to technical support via web portal, online chat, and telephone during business hours (8 hours a day, 5 days a week). Includes return and replace for hardware failures and access to technical support requests.
- **FortiCare 24x7 Service:** Offers round-the-clock access to mission-critical support (24 hours a day, 7 days a week, 365 days a year). Includes advanced replacement service for hardware failures.
- **FortiCare 360° Service:** An advanced services technical support offering combining cloud-based analytics with premium support. It enables organizations to proactively detect and remediate current and potential security and performance issues.

7.2. FortiCare Premium RMA Service

Designed to minimize downtime, the Premium RMA Service offers expedited hardware replacement options:

- **Next-day Delivery:** Parts delivered the day following RMA approval by Fortinet support.
- **4-Hour Courier:** Parts delivered on-site within 4 hours of RMA approval by Fortinet support.
- **4-Hour On-site Engineer:** An engineer delivers parts on-site within 4 hours of RMA approval by Fortinet support.

7.3. FortiCare Secure RMA Service

This service allows for non-return of an appliance, providing enhanced physical data protection for customers with strict security requirements.
For more information on FortiCare services and to determine the best support plan for your needs, please visit the official Fortinet website or contact your Fortinet representative.

© 2024 FORTINET. All rights reserved. Information subject to change without notice.

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/B01FRBM068

More documents and user manuals: **https://manuals.plus/**