



## ANSWERS TO FREQUENTLY ASKED QUESTIONS

Welcome to the SendGrid FAQ. In this document, you will find answers to important questions regarding SendGrid products, APIs, services, security, and infrastructure policies.

While this document contains answers to our most frequently answered questions, should you have any additional questions, please contact your sales representative or our [24x7 support team](#).

### TABLE OF CONTENTS (please click the chapter headings for easy navigation)

- [2 PRODUCT FAQs](#)
- [3 API FAQs](#)
- [4 SUPPORT AND SERVICES FAQs](#)
- [4 SECURITY FAQs](#)
- [7 INFRASTRUCTURE FAQs](#)

With unmatched deliverability, scalability, and support, SendGrid makes email easy.



#### Proven Deliverability

30+ deliverability experts, ISP monitoring and outreach, and rigorous compliance standards protecting our high quality senders.



#### Scale with Confidence

Sending 20 billion+ emails per month via our proprietary MTA and distributed infrastructure with built-in redundancy to deliver excellent uptime.



#### 24/7 Global Support

24/7 customer and compliance support, dedicated technical account managers for Premier accounts, and robust documentation.

## PRODUCT FAQs

**Q: Does your system have the ability to do throttling/rate limiting by IP to a specific ISP?**

**A:** Yes. We facilitate automatic rate throttling for optimization in reaction to ISP responses. However, rate throttling cannot be controlled by a customer or for individual IPs and ISP destinations.

**Q: Does your infrastructure support dedicated IPs for each business unit for sending?**

**A:** Yes. We support the ability to purchase dedicated IPs for customers on our Pro plans (Note: Pro plan customers receive 1 dedicated IP as part of their package. Additional IPs can be purchased for \$20.00 mo.) Customers with dedicated IPs can segment email traffic by business unit or by email use case (transactional, marketing, etc.).

**Q: Does your system support message queue prioritization (message sending with multiple priority queues for newsletter sending and RTM mail sending)? For example, if a higher priority message is loaded into the system, lower priority mail sending should pause and then continue when higher priority mail finishes?**

**A:** SendGrid's products do not currently support this.

**Q: Does your system have the ability to write a custom cookie at click time?**

**A:** No.

**Q: Does your system have the ability to append custom tracking tags to the end of URLs that are tracked at send time? Example: tag=nl.e100.**

**A:** No, but an alternative would be to use our [Google Analytics app](#) or our [Event Webhook](#) using unique arguments.

**Q: Does your system have the ability to segment emails that have "web inserts" in them to a separate queue so mail sending is not impacted (do this automatically based on if the "web insert" exists in the template)?**

**A:** No, SendGrid's products do not currently support this.

**Q: Does your infrastructure support the ability to automate exports of campaign information for integration with data warehouse systems?**

**A:** Yes. Using our Event Webhook, you can receive event data in real-time.

**Q: Does your infrastructure support the ability to automate exports of click, open, and bounce information for data warehouse integration?**

**A:** Yes. Using our Event Webhook you can receive real-time data posts of these event types.

**Q: Does your infrastructure support "web insert" capabilities (the ability to have part of a template be an HTTP call to a 3rd party service to pull in content). If so, do you have the ability to collapse the unit if HTTP call times out, or "bounce" the message as a soft content error if the content fetch fails?**

**A:** SendGrid's products do not currently support Web Insert capabilities.

## PRODUCT FAQs *continued*

**Q: Does your platform have mobile integration capabilities/APIs to push mobile notifications via an APP type notification?**

**A:** No, SendGrid's products do not currently support this.

**Q: Does your system provide the ability to integrate RSS/XML feeds from site into an automated newsletter production tool?**

**A:** No, SendGrid's products do not currently support this feature however we do work with [Zapier](#) who provides this functionality.

**Q: Does SendGrid provide the ability to create, preview, and save email template functionality within a graphical interface?**

**A:** Yes.

---

## API FAQs

**Q: What are the main integration methods that SendGrid supports?**

**A:** SendGrid supports multiple ways for you to integrate your application environment with our cloud-based email platform, including our SMTP API and our Web API. Information on these APIs is included below. For additional information on all our integration methods, please reference our [Integration Documentation](#) page.

**SMTP API:** SendGrid's SMTP API allows developers to deliver custom handling instructions for email. This is accomplished through a header, X-SMTPAPI, that is inserted into the message. The header is a JSON encoded list of instructions and options for that email. For more information, please reference the [SMTP API Documentation](#) page.

**Web API:** SendGrid's Web API allows an additional way to send mail. This option is mostly likely used if:

1. You do not control the environment that your application runs in, and it is difficult to install/configure an SMTP library.
2. You are developing a library from scratch to send email—developing against a Web API is much easier than developing an SMTP library.

For more information on SendGrid's Web API, please reference the [Web API Documentation](#) page.

**Q: Does SendGrid provide webhook functionality to access and customize real-time event data?**

**A:** Yes. SendGrid's Event Webhook allows developers to customize their integration with SendGrid and receive powerful event data in real-time. Please visit the [Event Webhook Documentation](#) page for more information.

**Q: Does SendGrid provide inbound email parsing capabilities?**

**A:** Yes, SendGrid's Inbound Parse Webhook allows customers the ability to parse attachments and content from inbound emails. The Inbound Parse Webhook will POST the parsed email to a URL configured in your account. Please visit the [Inbound Parse Webhook Documentation](#) page for more information.

## SUPPORT AND SERVICES FAQs

**Q: Is customer onboarding training included with the purchase of a paid SendGrid account?**

**A:** Customized onboarding training is not included as part of a typical paid package. Our customer support team, however, is available 24x7 to help with any technical related questions that a customer may encounter as part of their account setup. For those customers who might need additional onboarding and account setup assistance, SendGrid does offer paid onboarding assistance. Please speak with your sales representative for additional information and pricing.

**Q: Are consulting services required for integration with SendGrid products and are these services included in the monthly subscription fees?**

**A:** No, consulting services are not required to integrate with SendGrid. Integration is straightforward and we offer a host of integration methods and libraries to use. Additionally, 24/7 support is available from our customer support team to help answer any integration related questions. For more information, please visit our [Integration Documentation](#) page.

---

## SECURITY FAQs

**Q: Does SendGrid have a security policy?**

**A:** Yes, SendGrid has a security policy that covers a wide array of security controls that governs how we implement information security to protect information stored, processed, and transmitted by SendGrid products and services.

**Q: What areas do those policies cover?**

**A:** SendGrid takes security very seriously, and its policy covers areas such as physical security, access control and account management, people security, system development, incident management and response, business continuity, and system development.

**Q: How can I get a copy of these policies?**

**A:** You can request a copy of our policy by emailing support, your technical account manager, or your sales point of contact.

### **Q: How do you protect my data?**

**A:** Our customers rely on us to protect the information they send through our systems. This includes email addresses, email content, and deliverability data. SendGrid has a number of ways to ensure this data is protected:

- Data backups are encrypted at rest. Data in transit is encrypted.
- Documents and electronic media that contain customer data are destroyed using a leading document destruction service to ensure everything is disposed of securely.
- We have a lot of physical security measures in place at our data centers and our business facilities that we go into below.

### **Q: What kind of security do you provide for my emails?**

**A:** SendGrid utilizes opportunistic TLS to transmit your emails—that means that your email is encrypted end-to-end “on the wire,” provided the recipients’ ESP supports TLS. We also use SSL for click tracking so when your recipients click on a link, their browser uses SSL to track their clicks.

### **Q: Do you support encrypted transmission of email messages to your servers?**

**A:** Yes.

### **Q: Do you encrypt email messages from your servers (aka opportunistic TLS)?**

**A:** Yes. SendGrid utilizes opportunistic TLS to transmit your email as well as SSL for click tracking so when your recipients click on a link, their browser uses SSL to track their clicks.

### **Q: How do you secure your data centers and facilities?**

**A:** SendGrid utilizes data center co-locations all around the world, in nondescript facilities. Physical access is strictly controlled both at the perimeter and at the building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff. SendGrid only provides data center access and information to employees who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked. All physical and electronic access to SendGrid data centers is logged and audited.

SendGrid’s data centers also have environmental controls in place, including fire detection and suppression, climate and environmental control, and short- and long-term alternative power sources to ensure redundant power 24/7/365.

Your data is stored and processed in data centers located in the United States, while we use other data centers around the world to receive your mail quickly. Mail is not processed or stored at these locations, however.

### **Q: How do you manage application security?**

**A:** SendGrid's InfoSec team is involved in every software development project within the company. Security requirements are identified for each project at inception, and are tracked throughout the lifecycle of the project. Security testing is performed prior to release, and issues remediated as part of the software development lifecycle.

SendGrid also performs internal and third party application layer assessment of our applications on a continuous basis. We use the OWASP Testing Guide as the basis for our application layer vulnerability testing. This structured methodology ensures that our applications are free of the OWASP Top 10 most critical vulnerabilities, which include injection attacks, cross site scripting, security misconfiguration and sensitive data exposure.

SendGrid uses a "Graybox" testing methodology, which combines selective "whitebox" code review with interactive "blackbox" testing of the running application to maximize effectiveness.

### **Q: What other methods of security do you employ?**

**A:** SendGrid monitors its systems and services for security vulnerabilities with a variety of methods, including:

**Third party vulnerability testing**—We hire reputable security consulting agencies to perform testing, including application, network, and infrastructure vulnerability testing, selected penetration testing and code review, and selected security control review.

**Regular vulnerability scans**—We conduct weekly scans of our offices and production network to identify and remediate known vulnerabilities on our infrastructure and application platform.

**System monitoring**—Network based and host based Intrusion Detection (IDS) / Intrusion Prevention (IPS) systems to detect anomalous and/or malicious traffic on our networks and systems.

**Firewall infrastructure**—Next generation firewalls and/or ACLs are utilized to restrict access to systems from external networks and between systems internally. By default, all access is denied and only explicitly allowed ports and protocols are permitted based on business need.

**DDoS mitigation**—Our infrastructure incorporates multiple DDoS mitigation techniques in addition to maintaining multiple backbone connections. We work closely with our providers to quickly respond to events and enable advanced DDoS mitigation controls when needed.

### **Q: What kind of regulatory compliance do you meet?**

**A:** SendGrid is PCI-DSS compliant (Level 4 merchant), and its data centers are SSAE-16 compliant. SendGrid is currently working toward SSAE-16 attestation (SOC2 Type 2 report). SendGrid uses PCI compliant payment provider Zuora for encrypting and processing credit card payments. SendGrid's infrastructure providers are PCI Level 1 compliant. Our PCI Merchant Certificate of Compliance is available upon request. Zuora's certificate may be requested directly from their security department.

## SECURITY FAQs *continued*

### **Q: Is SendGrid HIPAA compliant?**

**A:** SendGrid is a general purpose email transport platform, and while it could be part of a HIPAA-compliant solution, SendGrid by itself is not HIPAA compliant. A HIPAA compliant email solution requires meeting a variety of security, training, policy, and procedure requirements that extend beyond the secure transmission of a message itself. These policies and procedures ensure that medical office staff sends protected information with appropriate levels of security to the right person. These checks would need to be done by systems before the email message was submitted to SendGrid for delivery.

As far as security goes, HIPAA requires private health information (PHI) to be secure while in transit and while at rest. SendGrid's built-in "over the wire" TLS encryption helps protect messages while they are being delivered to our servers or from our servers. We cannot however ensure that these messages were secure before we received them, while they are temporarily stored on our servers, or after they have been delivered to the recipient's downstream mail server. For that reason, an end-to-end encryption mechanism must be added to the service that we offer.

---

## INFRASTRUCTURE FAQs

### **Q: Where are SendGrid data centers located?**

**A:** Las Vegas, NV; Chicago, IL; and Dallas, TX.

### **Q: Does SendGrid use other data centers?**

**A:** Yes. When you send mail, it will go to the inbound data center that is closest to you in order to transfer mail to our pipeline quickly. Mail is not processed or stored at these locations, but is forwarded to our US-based data centers for processing and sending. We utilize data centers for geo-forwarding in Washington D.C., Amsterdam, London, and Singapore.

### **Q: What is SendGrid's published uptime?**

**A:** The service will be deemed "available" at all times that the service is available for access by users from the public Internet to create email messages to send via the service ("service availability" will refer to the times during which the service is available). Monthly uptimes are typically in the 99.95% range.

### **Q: What level of redundancy does SendGrid have?**

**A:** SendGrid has redundancy inside each datacenter for primary mail flow. All databases, load balancers, mail servers, etc. are set up in clustered and redundant modes. We have multiple datacenters and we are able to migrate primary mail flow (inbound and outbound) between datacenters. We have BGP and DNS based datacenter failover for primary mail flow.

### **Q: For customers with a dedicated IP, does that mean a single point of failure?**

**A:** Having a dedicated IP does not mean a single point of failure. These IPs are clustered inside a datacenter and can also be migrated via BGP routing to machines in another datacenter, all without the IP address or DNS changing at all.

## INFRASTRUCTURE FAQs *continued*

**Q: What additional means have you implemented to make this more robust, making customers' IP addresses continually available?**

**A:** Customers can have several IP addresses, which further protects from failure. If a customer has multiple IP addresses, the traffic is load-balanced and if there is a complete failure of one of the IPs, it is no longer used and the other IPs will take the remaining traffic.

**Q: Is SendGrid monitoring the reputation of our IP and delivery issues with ISPs?**

**A:** Yes. We have several internal tools we utilize to monitor customer sending reputation. And, for high volume accounts, our account management team takes a proactive approach to help monitor your account. Account managers receive reports of what is happening within your account and anything out of the ordinary (larger than normal queue, blocking by an ISP, etc.) can be mitigated.

Examples of some tools we use are ReturnPath tools, our own reputation monitoring algorithms, ISP reports (ex: SNDS), blacklist reports, etc. Monitoring is a partnership and therefore you have tools you can use as well. One of these is "alerts." We also have [documentation](#) about our alert settings.

**Q: Are sending software instances shared or dedicated? How does this affect performance and SLA commitments?**

**A:** The SendGrid platform is a multi-tenant application as it relates to our servers and infrastructure. We generalize performance and SLA across all customers equally.

**Q: What disaster recovery measures do you have in place?**

**A:** Current disaster recovery measures include:

- Multiple cross-functional offices
- Majority of business systems are hosted and are accessible externally via a secured connection
- Critical business systems can be run from multiple locations
- Data backups are securely stored off-site