How to Warm up an IP Address

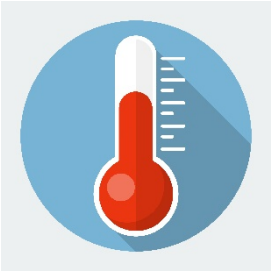
Achieving a good deliverability can be difficult, but possible if you have the right information and tools. Sometimes, the answer is in the details, and many of those details concern your sending IP address. This is more than important if you manage an in-house email system with a dedicated SMTP server and dedicated IP.

Mailbox providers decide whether or not to deliver your email to the Inbox, spam, or Promotions folder based on your sending behavior and your sender reputation score. So, the better your sending practices, the higher your reputation score and the more likely your emails will be delivered.

When you get a new IP address, it doesn't have a reputation score since it has no sending history yet. So how do you successfully send to Inbox from a new IP with zero reputation? You need to start with *warming up*! It involves building the IP reputation gradually starting with a small volume of emails and increasing the volume over time until the desired volume is reached.

Our goal at GlockApps is to ensure that you have all the tools and knowledge available to get your emails delivered to the user's Inbox.

This guide will show you how to start sending emails from a new IP address without experiencing troubles with ISPs, without delays or delivery failures.



Why Warm up a New IP

When you start sending low volumes of emails on your new dedicated IP, and then systematically increase your volume over a period of time, it gives ISPs the time to recognize, evaluate and adjust to your sending practices.

During this period ISPs evaluate your sending behavior, content, and your recipient engagement to see how well you manage your list hygiene and how willing you are to send relevant information to responsive users. They even look at how many users opened your email, replied you, moved your message to other folders or deleted it without opening.

From the ISP perspective, the “warm up” period allows the ISPs to gain trust in you as a sender and learn your usual sending volumes so they can identify any suspicious activity on your IP address. Spammers are known to flood Inboxes with malicious mail by hopping from IP to IP to circumvent ISP’s security checkpoints.

As a sender, you can also use this warm up period to your advantage. You have the opportunity to find out and fix any deliverability issues you may have before you start sending big volumes.

You can determine whether or not ISPs are throttling your emails, check your deliverability rates by campaign, domain, day, time, etc. and adjust accordingly.

Additionally, it’s a perfect time to evaluate your content and recipient engagement and determine which emails are generating the most (or least) response. By sending small volumes, you can identify

trends and then when your IP is warmed up, deliver the winning messages to your entire subscriber database.

So, for you, as a sender, the time when you are warming up your IP is a unique opportunity to test and optimize your entire email campaign. And the good reputation you build during the warm up period will make your life much easier when it comes to deliverability.

Instead of fixing deliverability problems, you'll be able to focus more closely on your business. Every email delivered to the Inbox increases your ROI and teaches you more about your customers and their needs.

How to Warm up a New IP

How many emails you send during your warm up period depends on your total email volume, but, in any case, you must send enough emails at enough frequency so that ISPs can track your email reputation.

NOTE:

The information below is a *suggestion* only. Every sender is different, and you may need advice from email deliverability experts to determine the right volume and frequency for your warm up period.

As a general rule, to warm up your new IP address, you should send at least 50,000 emails at least twice per month (for 100,000 emails total). Thus, if you are a small sender, you don't need to worry about warming up the IP at all!

As most reputation systems store data for the last 30 days, you should not interrupt your sending activity on that IP address for 30 days or more. If you do, then you will need to start from scratch.

The biggest challenge is where to *start*. First, decide on a segment of your email program. The idea is to select a mail stream that has *strong permission* from recipients. This will help build your reputation and "cement" your legitimacy as a sender in the eyes of the ISPs.

Once you've decided on a segment, determine the amount of emails you will send (see the sample scheduler on Page 5). Send that volume of emails for several days in a row and then gradually increase your volume. This process can last up to 60 days.

To determine speed, analyze your results. If you have good email deliverability with high engagement rates, then you can try to speed up the process. But if you get throttled, slow it down.

IMPORTANT!

You must warm up your IP at EACH ISP. Make sure that each ISP is receiving a comparable amount of emails each day. Don't warm up Gmail on Monday, Yahoo! on Tuesday, Hotmail on Wednesday etc., but evenly disperse your mail stream to each ISP on each day of the warm up period. If you don't do it, your sending activity will look sporadic and you won't be able to build a solid reputation with ISPs.

Sample Newsletter Warm Up Scheduler

Regular Approach	Speedy Approach
Divide your total monthly email volume by 30. Then, spread your emails evenly over the first 30 days, based on that calculation. *Example: if you will send 150,000 emails/month, start by sending 5,000 per day over the first month.*	Divide your total monthly email volume by 15. Then, spread your emails evenly over the first 15 days, based on that calculation. *Example: if you will send 150,000 emails/month, start by sending 10,000 for the first 15 days. If you experience throttling, slow down the sending.*

Sample Transactional Email Warm Up Scheduler

Established Business	New Business
If you're already sending a ton of emails, and decide to switch to a new ESP or delivery vendor, you should migrate your campaigns a little bit at a time. Split your email traffic and move small portions of it to the new IP over time. If you are maintaining multiple mail servers, move your servers over to your new IP one at a time.	Typically, the growth of your business will organically create an ideal increase. Since transactional emails depend on the number of customers you have, the growth in your customer base will create a comfortable growth in your email volume.

Questions to Ask Your ESP

As we told above, each sender is different, and the provided scheduler may not suit everyone. Therefore, you are advised to consult email deliverability experts to help you determine the right volume and frequency to get your email messages delivered as soon as possible.

Here are some questions you should ask your email service provider:

1. Do I have a dedicated IP or a shared IP?

This is important because warming up an IP is only required for a dedicated IP.

2. Do I need to think about IP warming up at all?

A dedicated IP has no reputation. But if your ESP tells you that you don't need to warm up your IP, then follow their direction.

3. Will you help me monitor my progress?

Make sure that your email service provider tracks the critical metrics that will help you determine the status of your warm up process: bounce, delivered, clicked, opened, unsubscribed and complaint rates.

4. How will I know whether it works or not?

You should be able to rely on your email service provider. They should be able to help analyze your reports, give recommendations for warming up your IP and preventing problems that can cause poor reputation and long-term delivery failures. They should also be able to contact ISPs on your behalf if you are having major deliverability issues.

How to Maintain a Good Reputation

Reputation is essential for high email deliverability. Therefore, before you change an email service provider or move from a shared IP to a dedicated IP, you should remember that restoring a bad reputation can be more costly and time-consuming than building a good one. You also have to have the tools to regularly check and monitor your IP reputation and email deliverability.

Here are a few things to consider before getting started:

1. Patience is the key.

Often times, senders are so eager to get their emails out of the door that they are ready to put their reputation at risk. However, it's very hard to repair a bad reputation. Since sending reputation is evaluated during 30 days, it could take 4 or more weeks to repair it, and every day you get email delivery failures can cost you.

2. IP rotation is a bad thing.

You don't need dozens of IPs. ISPs see the IP rotation as a spammer tactic and will block the entire IP range. You can send lots of marketing messages per day from a single IP if you warm it up and continue to follow best email marketing practices to keep its reputation in order.

3. It's time for optimization.

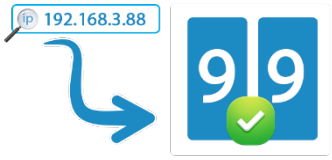
Consider your warm up period as a great opportunity to optimize your email program, determine deliverability issues and solve them. ISPs like to see that you are responsive. Doing the right thing will always work in your favor.

4. Marketing and transactional emails are not the same.

Differentiate IPs for your marketing email and transactional email streams. Transactional emails are more important and are treated as "wanted" email by the ISPs. They are generally granted a little more "indulgence". Marketing emails typically have more "chances" to be filtered or blocked. Therefore, you'll want to use two dedicated IPs - one for marketing emails and the other for transactional emails – to be sure that your transactional emails are delivered in case your marketing activity leads to the IP block.

5. Best email practices open all doors.

You'll want to follow best email marketing practices and handle your bounce and unsubscribe emails, monitor user engagement and remove inactive users, while you are warming up your IP and after the warm up period.



How to Monitor IP Reputation

Having the right tools for checking the IP reputation is half way to success. Here are some tools and services you can use:

- Senderscore.org by Return Path. The score ranks from 0 to 100, 100 being the best. It tells you how you're performing. Typically it's recommended that you maintain your sender score of 90 or better.

- Senderbase.com by Cisco. It tells you how your reputation is across all the network providers Cisco manages. The reputation score is grouped into Good, Neutral, and Poor.

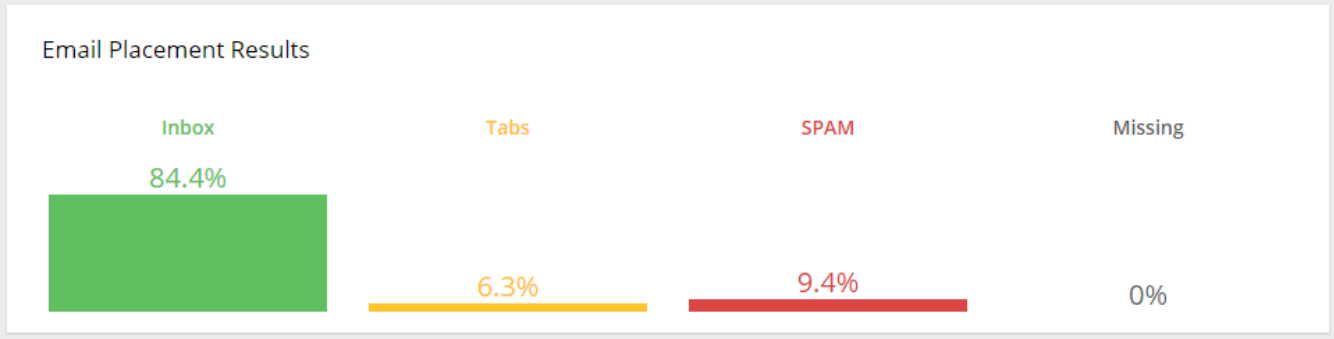
- Postmaster.live.com. Microsoft's Smart Network Data Services give you the information about the traffic originating from your IP address such as the volume of sent emails, complaint rates, and spam trap hits.

- Postmaster.google.com. Gives access to your domain's data on Google Search Console.

- Postmaster.aol.com. Check your IP reputation and rates it as “bad”, “neutral”, and “good”. If your IP reputation is “bad” with AOL, you’ll see your emails filtered out as junk mail or blocked altogether. A “neutral” reputation is generally OK.

- GlockApps.com is a good place for testing and monitoring sender reputation and email deliverability. It shows your sender score and email spam score, tests your authentication records and email placement at different mailbox providers.

  Plus, GlockApps can test your sending IP against 50+ of the most common industry blacklists including Spamhaus, SURBL, SORBS, and others and help you diagnose and solve deliverability issues for continuous deliverability. You can setup an automated process of checking your IPs against blacklists and be alerted via email when the IP got listed.



The Bottom Line

Warming up your new IP is an essential part of creating a successful email program. With the right tools and knowledge, you can ensure your emails get Inboxed with each mailbox provider.

At GlockApps, we provide users the information and advice to help them test and monitor their IP reputation and email placement. We have detailed reports which give our customers an inside look at how their emails are being treated by major mailbox providers and spam filters. We also provide all available information we can scratch from email headers to help our customers determine deliverability issues and solve them.

Try GlockApps for FREE Now