

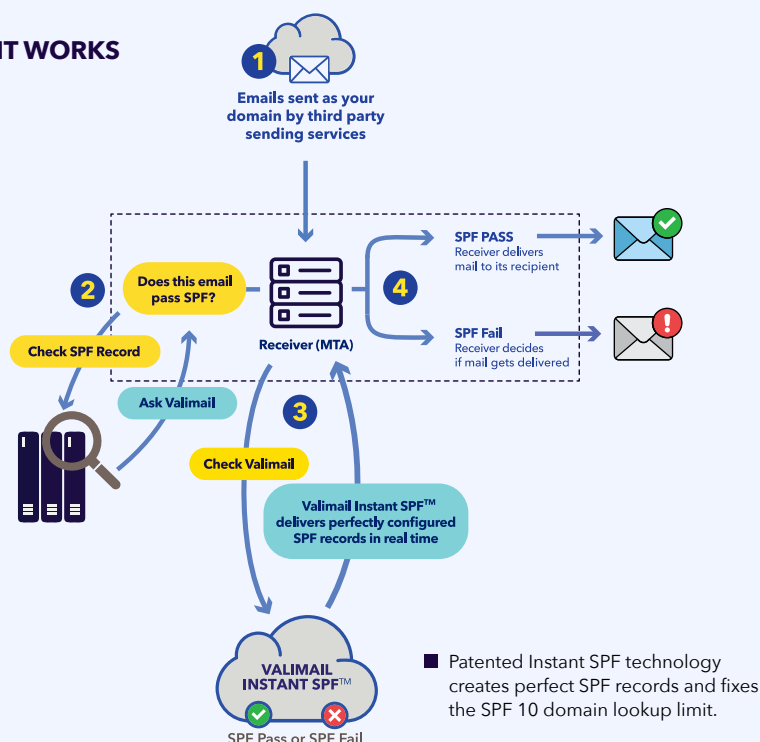
Sender Policy Framework (SPF) is a DNS-based mechanism for defining a whitelist of mail servers that can send email on your domain's behalf. Getting SPF right on your own is hard and some commercial services claim to help, but most offer a mix of incomplete reporting and imprecise workarounds that often fail to do the job properly.

Valimail's patented Instant SPF technology is the industry's gold standard for how to make sure anyone sending as you is approved to send as you. It is the only solution that auto-generates perfectly tailored SPF records, in milliseconds, in response to each mail server request. By responding dynamically with an SPF rule set as specified by the sending service itself, Instant SPF guarantees 100% accuracy for every single email, 24/7, regardless of network changes to services or underlying email service providers.

Instant SPF utilizes advanced macros to solve the 10-domain lookup limit without resorting to substandard approaches like flattening (by listing IP addresses instead of domain names) or subdomains, no matter how many services are sending on your organization's behalf.

Instant SPF™ works in conjunction with Valimail Helios™, which actively maps thousands of third-party sending services. Simply point your SPF record to Valimail, designate the services you want to authorize by selecting them from a list, and you can be certain that your SPF authentication will work seamlessly.

HOW IT WORKS








KEY BENEFITS:

- **Put the 10-domain lookup limit in the past**
Using more than just a few cloud services can easily hit the limit of 10 DNS lookups, meaning SPF can break and good email won't be delivered. Instant SPF is the only solution that elegantly bypasses this hurdle by delivering perfect SPF records in real time for each of your authorized services, no matter how many services you have.
- **No manual DNS management**
Valimail's automated SPF technology makes authentication 100% accurate and maintenance-free. This means no risk of configuration error in live DNS, and no need for ongoing tactical work or coordination with third party sending services to make sure syntax and records are correct and up to date. Instead, it's one click in the Valimail interface to enable or disable services.
- **Avoid flattening and get a true fix**
Flattening (also referred to as SPF compression) is a fragile, management-intensive approach to circumventing the 10-domain lookup limit by replacing lookups with IP addresses and IP blocks. It requires constant monitoring of underlying IP infrastructure changes, which leaves the door open for outdated and broken SPF. Instead of relying on a single static SPF record with a flattened response like all other SPF solutions, Valimail generates dynamic records in real time as needed.
- **Enterprise scale**
Instant SPF works flawlessly at scale to authenticate billions of emails per week for some of the world's largest brands. Instant SPF is fully compliant with the SPF standard, works with all existing mail receivers and gateways, and is built on Valimail's globally distributed cloud-based infrastructure for optimal availability.






WHAT TRUE SPF AUTOMATION LOOKS LIKE:

Other vendors claim to offer automated SPF, and in many cases they do host and manage your SPF in DNS. But in virtually every case, they actually do IP flattening behind the scenes. So what may look like a dynamic response merely masks a "flattened" list of IPs delivered by the hosted service. In reality, flattening – even when delivered dynamically by a vendor – is a non-automated, unscalable, and brittle method. Only Valimail has a truly dynamic, patented method for generating SPF records correctly using include: directives.

OTHER VENDORS

-  Rely on maintaining, monitoring, and parsing lists of IP addresses; less accuracy, longer response times
-  Return large blocks of allowed IPs, potentially allowing other users of that service to also send as your domain; overly permissive
-  Return a static, parameterized SPF record with a flattened list of IPs; requires constant monitoring
-  Brittle fix to the 10 lookup limit; requires manual maintenance without notification; becomes more complex with more services
-  Lag time between updates to IP lists can result in legitimate email failing to authenticate

VALIMAIL

-  Auto-generates SPF records in real time as needed; ensures accuracy and improves response times
-  Leverages EHLO name; ensures only customer-specific IPs from that service are allowed; non permissive
-  Returns the service's own SPF rule that is maintained by the service itself; no need to monitor for changes to the service
-  Dynamic solution to the 10 lookup limit; failsafe SPF authentication at scale with no limit on number of sending services
-  All services stay authorized 100% of the time

THE VALIMAIL DIFFERENCE

OTHER VENDORS

Record published in customer's DNS

```
v=spf1 include:_u.ef.com._spf.smart.vendor.com ~all
```

The record looks dynamic...

Flattened response

```
v=spf1 ip4:52.100.0.0/14 ip4:40.92.0.0/15 ip4:13.111.0.0/16
ip4:40.107.0.0/16 ip4:149.72.0.0/16 ip4:104.47.0.0/17 ip4:167.89.0.0/17
ip4:168.245.0.0/17 ip4:54.240.0.0/18 ip4:77.32.128.0/18 ip4:192.28.128.0/18
ip4:198.2.128.0/18 ip4:212.146.192.0/18 ip4:213."32.128.0/18
ip4:216.198.0.0/18 ip4:23.251.224.0/19 ip4:50.31.32.0/19 ip4:77.32.192.0/19
include:_p.1.jbsg7t._u.ef.com._spf.smart.vendor.com ~all
```

The last include: directive points to another flattened record that then points to four more, all of which contain vast amounts of IPs. This makes accurate maintenance and change detection difficult. It also weakens the organization's security posture by authorizing SPF authentication for every single listed IP.

```
v=spf1 ip4:153.92.224.0/19 ip4:23.249.208.0/20 ip4:66.231.80.0/20
ip4:68.232.192.0/20 ip4:69.169.224.0/20 ip4:76.223.176.0/20
ip4:136.147.128.0/20 ip4:136.147.176.0/20 ip4:188.172.128.0/20
ip4:1
ip4:2
v=spf1 ip4:62.13.144.0/21 ip4:74.112.64.0/21 ip4:94.143.16.0/21
ip4:104.37.32.0/21 ip4:148.105.8.0/21 ip4:161.71.32.0/21
ip4:198.21.0.0/21 ip4:199.122.12.0/21 ip4:208.85.48.0/21
ip4:3
ip4:4
v=spf1 ip4:199.15.212.0/22 ip4:199.127.232.0/22
ip4:199.255.192.0/22 ip4:208.75.120.0/22 ip4:62.13.152.0/23
ip4:64.132.88.0/23 ip4:130.248.172.0/23 ip4:13.111.63.0/24
ip4:5
v=spf1 ip4:65.240.141.0/24 ip4:65.250.141.0/24 ip4:72.3.185.0/24
ip4:72.32.154.0/24 ip4:72.32.217.0/24 ip4:72.32.243.0/24 ip4:91.198.169.0/24
ip4:136.147.182.0/24 ip4:193.202.110.0/24 ip4:195.47.247.0/24 ip4:207.67.38.0/24
ip4:6
v=spf1 ip6:2a01:111:4003::/48 ip6:2a01:4180:4050:400::/64
ip6:2a01:4180:4050:800::/64 ip6:2a01:4180:4051:400::/64
ip6:2a01:4180:4051:800::/64 ip4:3.80.205.151 ip4:3.123.234.69 ip4:3.222.219.88
ip4:5 ip4:15.223.142.138 ip4:18.132.189.127 ip4:18.197.43.76 ip4:34."198.95.97
ip4:34.198.193.174 ip4:34.199.167.230 ip4:34.202.174.188 ip4:34.224.96.251
ip4:3 ip4:35.157.192.122 ip4:35.158.67.243 ip4:35.158.71.15 ip4:35.182.195.41
ip4:7 ip4:51.38.52.224 ip4:52.16.38.44 ip4:52.16.49.62 ip4:52.16.75.109
ip4:2 ip4:52.16.75.118 ip4:52.22.249.6" ip4:52.38.191.241 ip4:52.50.129.119
ip4:5 ip4:52.65.244.27 ip4:52.203.5.138 ip4:54.79.0.4 ip4:54.85.129.207
ip4:3 ip4:54.93.104.220 ip4:54.174.209.165 ip4:74.112.66.161 ip4:74.112.66.162
ip4:94.236.119.5 ip4:123.207.185.116 ip4:129.33.239.44 ip4:129.41.76.62
ip4:12" ip4:172.141.1 ip4:185.28.196.15 ip4:185.28.196.86 ip4:193.201.168.38
ip4:195.143.170.1 ip4:209.235.2.13 ip4:212.203.75.94 ip4:222.73.107.148
ip4:222.73.121.135 ip4:222.73.121.144 exists:%(i)_spf.mta.salesforce.com ~all
```

VALIMAIL

Record published in customer's DNS

```
v=spf1 include:defendmy.email._nsf.vali.email include:%(i)_ip.%(h)_.
ehlo.%(d)_.spf.vali.email -all
```

Instant SPF leverages macros in the SPF record that are based on the specific email being authenticated. This allows Valimail to send only the exact information required to authenticate that email.

Query gathered from the mail receiver

```
209.85.222.48._ip.mail-ua1-f48.google.com._ehlo.defendmy.email._spf.vali.
email
```

Instant SPF response

```
v=spf1 include:_spf.google.com -all
```

Valimail's response is tailored to the specific service as needed, and acts as a pointer to the sender-maintained SPF information. This ensures error-free SPF authentication without ever having to worry about the 10 lookup limit.



**Schedule a
LIVE DEMO**
to see Instant SPF delivering
perfect records in real-time,
per sending service.



Valimail, the global leader in zero-trust email authentication security, invented hosted DMARC in 2015 and DMARC-as-a-service in 2021. The company's full line of cloud-native solutions authenticates sender identity to stop phishing, protect brands, and ensure compliance. From neighborhood shops to some of the world's largest brands, many organizations use these solutions to secure their emails. Valimail holds the most robust portfolio of patents that unlock DMARC for businesses at scale, and is the only DMARC solution to earn FedRAMP certification. The premier DMARC partner for Microsoft 365 environments, Valimail also holds leadership positions on every key industry standards body, driving today's email authentication policies and tomorrow's cybersecurity advancements for everyone. For more information visit www.valimail.com.