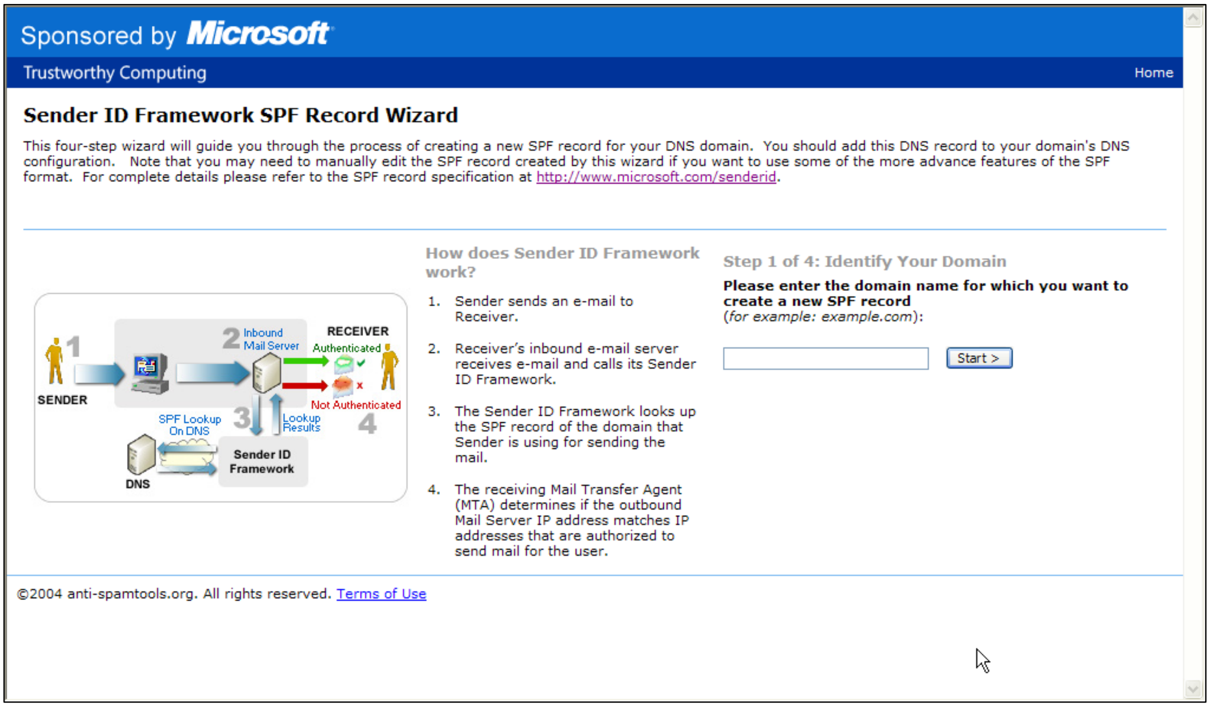
Sender ID Framework
Implementation Tips for the Sender ID Framework - Creating Your SPF Record

E-mail authentication is a critical technology and industry initiative that is helping to stem the tide of spam, e-mail spoofing, and phishing. Left unchecked these online dangers threaten customer trust and online confidence, as well as the ability to communicate.

For e-mail senders, the Sender ID Framework (SIDF) is a valuable e-mail authentication solution to help defend e-mail against spoofing, Web sites from phishing, and protecting online brands and reputations. When e-mail receivers include the SIDF Purported Responsible Address (PRA) or “Mail From” check results with your organization’s existing anti-spam heuristics, you can realize improved e-mail deliverability with reduced false positives and false negatives.

Today, over 1 million domains and 300 million users worldwide are realizing the benefits of SIDF authenticated e-mail. While this alone will not stop spam, collectively with complementary e-mail authentication techniques, e-mail reputation services, anti-spam heuristics, customer education, industry collaboration and strong legislation and enforcement, we can help ensure online trust and confidence for all users.

The first step towards a successful deployment of e-mail authentication is the creation of a Sender Policy Framework (SPF) record. To create a record, e-mail senders need to identify the computers that send e-mail on their domain's behalf, and to determine those computers IP addresses. You can use the Sender ID Framework SPF Record Wizard to help collect this information and create your SPF record. The wizard can be found at http://www.microsoft.com/senderid.



Sender ID Framework SPF Record Wizard

This four-step wizard will guide you through the process of creating a new SPF record for your DNS domain. You should add this DNS record to your domain's DNS configuration. Note that you may need to manually edit the SPF record created by this wizard if you want to use some of the more advance features of the SPF format. For complete details please refer to the SPF record specification at http://www.microsoft.com/senderid.

How does Sender ID Framework work?

1. Sender sends an e-mail to Receiver.
2. Receiver’s inbound e-mail server receives e-mail and calls its Sender ID Framework.
3. The Sender ID Framework looks up the SPF record of the domain that Sender is using for sending the mail.
4. The receiving Mail Transfer Agent (MTA) determines if the outbound Mail Server IP address matches IP addresses that are authorized to send mail for the user.

Step 1 of 4: Identify Your Domain

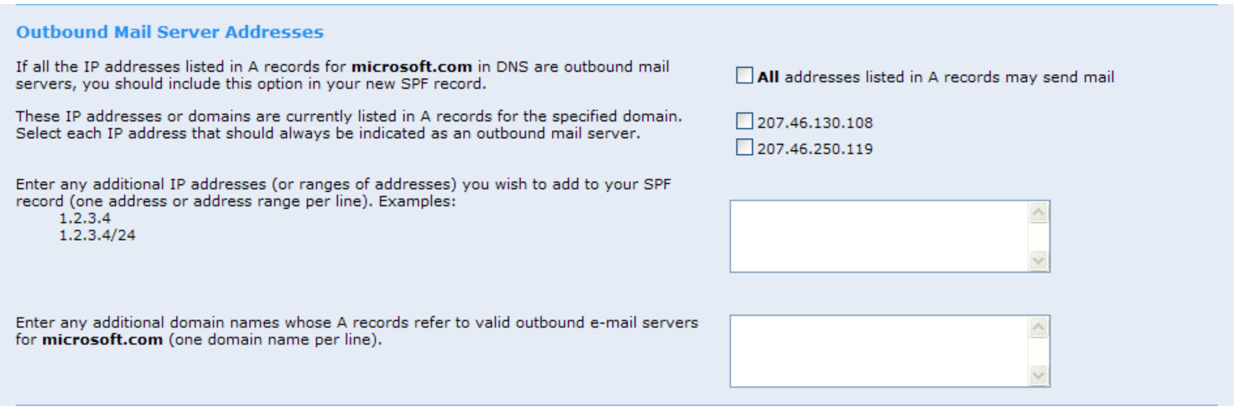
Please enter the domain name for which you want to create a new SPF record
(*for example: example.com*):

©2004 anti-spamtools.org. All rights reserved. Terms of Use

Figure 1 - Sender ID SPF Record Wizard

For most organizations, the computers that send their e-mail fall into one of two categories: 1) those with servers operated and administered by their organization, or 2) those with servers operated by third parties. The following provides an overview of how you can use the SPF Record Wizards in both of these scenarios.

1. Servers operated and administered by the organization. These are typically the organization's own mail servers. These servers are usually well known to an organization's IT department, and are often already identified in the Domain Name System (DNS) by MX or A records. The Sender ID Framework SPF Record Wizard will display these records for you. However, additional mail servers may be operated by other departments. Particularly in large organizations, it may be necessary to conduct a comprehensive survey in order to identify all outbound e-mail servers.



Outbound Mail Server Addresses

If all the IP addresses listed in A records for **microsoft.com** in DNS are outbound mail servers, you should include this option in your new SPF record.

□ **All** addresses listed in A records may send mail

These IP addresses or domains are currently listed in A records for the specified domain. Select each IP address that should always be indicated as an outbound mail server.

□ 207.46.130.108

□ 207.46.250.119

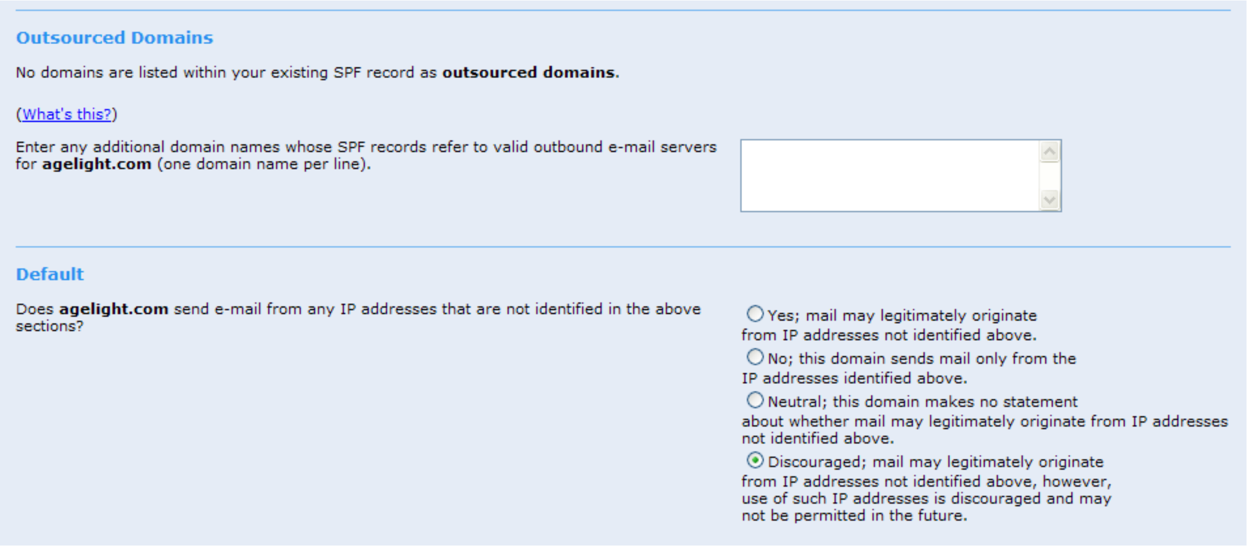
Enter any additional IP addresses (or ranges of addresses) you wish to add to your SPF record (one address or address range per line). Examples:

1.2.3.4
1.2.3.4/24

Enter any additional domain names whose A records refer to valid outbound e-mail servers for **microsoft.com** (one domain name per line).

Figure 2 - SPF Wizard Outbound Mail Server Screen

2. Servers operated by third parties to whom sending of e-mail has been outsourced. E-mail service providers often send mail on behalf of a domain for a variety of business and marketing functions. Once you identify these senders, you need to include a reference to their SPF records in your own. (You may need to encourage them to publish an SPF record if they have not already done so.) The Sender ID Wizard makes it easy to add references to outsourced domains to your SPF record. For additional information, please contact your e-mail service provider or the E-mail Service Provider Coalition at www.espcoalition.org.



Outsourced Domains

No domains are listed within your existing SPF record as **outsourced domains**.

(What's this?)

Enter any additional domain names whose SPF records refer to valid outbound e-mail servers for **agelight.com** (one domain name per line).

Default

Does **agelight.com** send e-mail from any IP addresses that are not identified in the above sections?

○ Yes; mail may legitimately originate from IP addresses not identified above.

○ No; this domain sends mail only from the IP addresses identified above.

○ Neutral; this domain makes no statement about whether mail may legitimately originate from IP addresses not identified above.

● Discouraged; mail may legitimately originate from IP addresses not identified above, however, use of such IP addresses is discouraged and may not be permitted in the future.

Figure 3 - Adding Outsourced Domains

One approach to identifying the internal and external mail servers that send mail on your domain's behalf is to identify the various categories of mail your organization sends, and to then determine, in consultation with the appropriate functional groups within your organization, how each category of e-mail is sent. Typical categories of e-mail include:

.

- Advertising & Public Relations
- Broadcast mailings
- Corporate E-mail
- Customer Service
- Customer / Technical Support
- Event Marketing
- Forward To A Friend
- Helpdesk
- Human Resources
- Investor Relations
- Newsletters
- Order and Shipping Confirmation

Several tools are available to verify and test your record including tools from Port25, Microsoft, and other industry leaders. Once you have created and posted your SPF record to your DNS, you can test it by simply sending an e-mail to Port25’s automated testing reflector tool check-auth@verifier.port25.com. A reply e-mail will be sent to you with an analysis of the message's authentication status from multiple e-mail authentication technologies including the PRA and Mail From checks. (Note: To completely validate your record, an e-mail needs to be sent from each of the IP addresses included within your SPF record.) You can also visit http://senderid.espcoalition.org/ for an interactive, web-based testing tool.

The following are answers to some specific questions or situations you may wish to consider with when creating your SPF record. For complete information, please refer to the SPF and Sender ID specification posted at www.microsoft.com/senderid or at the IETF’s web site, http://www.ietf.org/.

.

1. My domain never sends e-mail. To protect this domain from being spoofed, you should publish this very simple TXT record in DNS:

```
example.com IN TXT "v=spf1 -all"
```

   Replace `example.com` with your own domain name. You can also publish similar records for sub domains that do not send mail. Suppose www.example.com never sends mail. You could publish the following record to protect that domain, even if example.com, the parent domain, does send mail.

```
www.example.com IN TXT "v=spf1 -all"
```

2. I know my internal servers, but I am concerned that I may miss one of our third-party e-mail service providers. We recommend that you consult broadly within your organization to identify any third-party e-mail service providers who may have been engaged to send mail on your domain's behalf. Typically, these services are used to send newsletters, marketing-related communications, etc. Check with the appropriate departments in your organization.

3. I made changes to my SPF record and posted it into my DNS today. How soon can I expect this record to be used to authenticate e-mail sent from my domain? It can take roughly 24 to 48 hours for DNS information to propagate completely through the Internet. However, only a few hours are usually required for updated DNS information to become available in well-connected parts of the Internet. We suggest you wait 48 hours after making a change to your record before initiating any new e-mail activities.

4. Some of my employees use mobile devices. How do I accommodate these users? We suggest that the mobile network carrier publish its own SPF record, and then insert a header into outbound messages identifying the user's account on the mobile network. In this way, e-mail can be authenticated as legitimately originating from that network.

5. Mobile employees often send mail from hotel or other “guest” e-mail servers. What do I put in my SPF record to cover these situations?   The best option, if possible, is for mobile users to send mail over a VPN connection or by using a Web-based e-mail client. This way their mail flows through your regular e-mail servers and you don’t need to make any changes to your SPF record. If mobile users submit mail using a POP or IMAP client then their messages flow through the hotel or guest e-mail server.   To deal with this, you could terminate your SPF record with “~all”. The “~all” causes a “soft fail” when Sender ID checking is performed. This does not mean messages will be rejected, but they may be subject to additional spam filtering. We also suggest that the hotel or other guest e-mail service publish its own SPF record, and then insert a header into outbound messages identifying the guest account. In this way, e-mail can be authenticated as legitimately originating from that service.

6. I have SPF1 or SPF classic records already posted in my DNS. Do I need to make a change? Typically, no. The same SPF record can generally be used to authenticate both the MAIL FROM and PRA domains. Sometimes, however, different domain names are used in the MAIL FROM (or “envelope” address) and the addresses used in the message body. You need to ensure that SPF records are published for all the domains used in both the MAIL FROM and PRA addresses of messages sent from your domain.

7. Do I need to create separate records for receivers who have implemented the “Mail From” or the PRA check? Typically, no. The SIDF specification has been designed to use the same SPF record for both. Sometimes, however, different domain names are used in the MAIL FROM (or “envelope” address) and the addresses used in the message body. You need to ensure that SPF records are published for all the domains used in both the MAIL FROM and PRA addresses of messages sent from your domain.

8. I still am experiencing difficulty in creating my record. Who can provide assistance? Many leading anti-spam vendors, ISPs, and Hosters provide this service for their customers. Additionally, you may contact your e-mail marketing service provider for assistance. Sender authentication assistance is also available online at http://www.deliverability.com/email-auth.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY. Microsoft and the Microsoft logo are registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.