



# Sender ID Framework

## Improving online trust and confidence

### Implementation Guidelines

E-mail has become an important part of everyday life, enhancing communications, productivity and e-commerce. Unfortunately, spammers and online criminals exploit e-mail, creating threats to security and personal identity. Left unchecked, these dangers undermine customer trust and online confidence.

To address this critical security issue, an industry consortium has jointly developed the Sender ID Framework (SIDF), now approved by the Internet Engineering Task Force (IETF) to help increase the detection of deceptive e-mail and to improve the deliverability of legitimate e-mail. SIDF is an e-mail authentication protocol that is designed to be implemented at no cost, independent of one's e-mail architecture. Today, SIDF is embraced by more than 15 million domains, sending nearly 50 percent of all legitimate e-mail worldwide.

When e-mail-receiving networks include the SIDF results with their existing antispam solutions, SIDF can improve e-mail deliverability while also reducing false positives. Although it will not stop spam completely, SIDF can help improve online trust and confidence when it is used with reputation data and antispam and phishing heuristics. This document provides an overview of how SIDF works, instructions on creating an effective Sender Policy Framework (SPF) record, and implementation tips. If you have suggestions or comments, please send an e-mail message to [senderid@microsoft.com](mailto:senderid@microsoft.com).

### How Sender ID Works

To use Sender ID, e-mail domain owners must publish or declare all of the Internet Protocol (IP) addresses used by their outbound e-mail servers, or the IPs authorized to send e-mail on their behalf, in the Domain Name System (DNS). These IPs are included in an SPF text file. The following diagram and steps outline the SIDF process:

1. A sender or user sends an e-mail message from an e-mail client or Web interface. No interaction or changes to the sender's client or Mail Transfer Agent (MTA) are required.

2. The recipient's inbound e-mail server receives the e-mail message. The server uses SIDF and calls the purported responsible domain's (PRD) DNS for the SPF record.

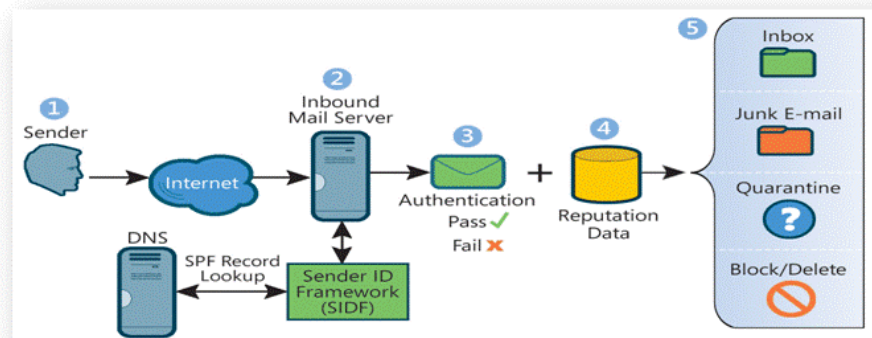


Figure 1 How Sender ID works

3. The receiving MTA determines whether the outbound e-mail server's IP address matches the IP addresses that are authorized to send e-mail for the domain.
4. For most domains and IPs, sender reputation data is applied to the SIDF verdict check.
5. Based on the SPF record syntax, the pass or fail verdict, the reputation data, and the content filtering score, the receiving MTA delivers the e-mail message to the inbox, a junk or bulk folder, or a quarantine folder. If an e-mail message fails, the receiving network may block, delete, or junk the message.

## Authenticating Outbound E-Mail

Domain holders need to complete an inventory and publish all IP addresses of their outbound e-mail servers in the DNS zone file. This is an administrative step that requires no changes to an organization's e-mail or DNS software. Even if your domain has no outbound e-mail servers, you can help protect your domain from spoofing by publishing an SPF record in the DNS that states this. Follow the steps below to create and publish an SPF record for each domain name that your organization owns.

1. Determine the IP addresses of the outbound e-mail servers for the domain.
2. Identify the e-mail servers that transmit outbound e-mail for all of the domains and subdomains in your organization, as well as the IP addresses for these servers. You will need to publish a Sender ID record for each of them. If your organization uses any third parties to send e-mail on its behalf, such as an e-mail service provider or a hoster, you will also need to know their domain names. However, you do not need to know the IP addresses of their outbound e-mail servers. (You may want to encourage them to publish Sender ID records for their own domains.)
3. Create the SPF record. You can use the Sender ID Wizard described in this document to make it easier. (See [www.microsoft.com/senderid/wizard](http://www.microsoft.com/senderid/wizard).)

**Note** You must create a separate SPF record for each domain and subdomain that sends e-mail for you. It is possible for several domains to share the same Sender ID record.

4. After you have created the SPF records for your organization, publish them in DNS TXT records. You may need the assistance of your DNS administrator, Web hoster, or registrar.
5. Ensure that your domain can be correctly identified as the purported responsible domain (PRD) for each message you send. This means that the sender's domain must be shown in certain headers of the e-mail message. Sender ID has been carefully designed to ensure that most legitimate e-mailers, remailers, and mailing list operators already satisfy this requirement. In a few cases, such as mail forwarding services, you may need to add additional headers to e-mail messages.

## Sending Scenarios

Receiving e-mail systems examine each message to determine the PRD—that is, the Internet domain that purports to have sent the message. Therefore, e-mail senders must ensure that their domain is the one that is identified as the PRD. The Sender ID specification describes how the PRD is determined. Basically, receiving systems examine the RFC 2822 headers of each e-mail message in a particular sequence. The following are descriptions of some scenarios and use cases, including which headers will be used to determine the PRD in each.

- **Ordinary Interpersonal E-Mail.** Ordinary e-mail sent from a user in one domain to a recipient in another is typically injected into the Internet mail system by servers that belong to the sending domain. The "From" header of the message will be used by receiving systems to identify the PRD. As long as sending servers use their own domain name in the "From" header of the message and publish an SPF record, they are already compliant with Sender ID.
- **Mailing Lists.** Mailing list servers receive a message from the original sender and then re-send that message to all the members of the intended mailing list. In so doing, the mailing list server itself becomes the new sender of the message. Sender ID will validate that the message originates from an e-mail server that is under the control of the mailing list service. In other words, the PRD of the message is the domain of the mailing list service. Therefore, a mailing list server must add an appropriate header to each message that contains an e-mail address that it is authorized to use. Most of today's mailing list software already adds an appropriate header, usually "Sender," that identifies the owner of the mailing list. This software is already compliant with Sender ID. The Sender ID specification encourages the use of the "Resent-From" header for this purpose. The "Sender" header is also acceptable.

- **Mail Forwarding.** E-mail forwarding services receive mail sent to one address and automatically forward it to a second address. Forwarding is commonly done by retransmitting messages verbatim, preserving exactly both the original Simple Mail Transport Protocol (SMTP)–level envelope information and the entire original message body. Unfortunately, this means that the forwarding service itself is never identified as the re-sender of the message. As a result, a message sent through a forwarding service cannot be distinguished from forged mail. Therefore, Sender ID requires that an e-mail forwarding service add an appropriate header that contains an e-mail address that the service is authorized to use. Sender ID recommends the use of the “Resent-From” header for this purpose.
- **Mobile Users and Third-Party Mailers.** It is increasingly common for users to send e-mail from a variety of devices, including mail-enabled phones and personal digital assistants (PDAs). These devices are commonly connected to the Internet through a third-party network carrier or Internet Service Provider (ISP). Although users typically have accounts on these third-party networks, they often want mail sent over them to appear to originate from their regular corporate or personal e-mail account. However, because the message is injected into the Internet mail system by the third-party network, the PRD of the message is actually the domain of the third-party network. Sender ID requires that an e-mail service that sends mail on behalf of another user in this way add an appropriate header that contains an e-mail address that the service is authorized to use. Typically this address will be the user's address on the third-party network. Such programs should use the “Sender” header for this purpose.

This also applies to other third-party mailing services, including applications such as electronic greeting card and invitation services, “e-mail this article to a friend” services, and similar services that send e-mail on behalf of their users. Third-party mailers that add a “Sender” header to messages today are already compliant with Sender ID.

- **Guest E-Mail Services.** Another common scenario involves users who send e-mail over networks for which they have only temporary or guest access and no permanent account. For example, hotels commonly offer Internet access to their guests. Guests use their regular corporate or personal e-mail addresses to send e-mail, but messages are routed through the hotel's e-mail servers. As in the third-party mailer, Sender ID requires that these third party e-mail servers add an appropriate header that contains an e-mail address that the servers are authorized to use. Sender ID recommends the “Resent-From” header in this case. Because the user does not have an account on the third-party network, a generic service address may be used.

### **Responsible Submitter: An Optimization**

To determine the purported responsible address (PRA) of an e-mail message, the receiving server must examine the headers in the message body. In other words, the message must be transmitted to the receiving server before the PRA can be identified.

To enable receiving servers to identify the PRA before the message is transmitted, an extension to the SMTP protocol, called Responsible Submitter, has been proposed. Using this extension, sending e-mail servers would determine the PRA of their own messages and include this address on a new “SUBMITTER” parameter added to the “SMTP MAIL” command. When the “SUBMITTER” parameter is present, receiving e-mail systems can validate the PRA of the message before the message body is transmitted. MTA software will need to be upgraded to support this proposed extension.

## Sender ID Framework SPF Record Wizard: Overview and Tutorial

The following section provides an overview of the Sender ID Framework SPF Record Wizard<sup>1</sup>, an interactive tool designed to help you create a properly formatted SPF record.

The first step toward a successful deployment of e-mail authentication is the creation of an SPF record. To create a record, e-mail senders need to identify the computers that send e-mail on their domain's behalf and determine the IP addresses of those servers.

For most senders, the computers that send their e-mail fall into one of two categories: servers operated and administered by their organization or servers operated by third parties. The SPF Record Wizard can be used in both of these scenarios.

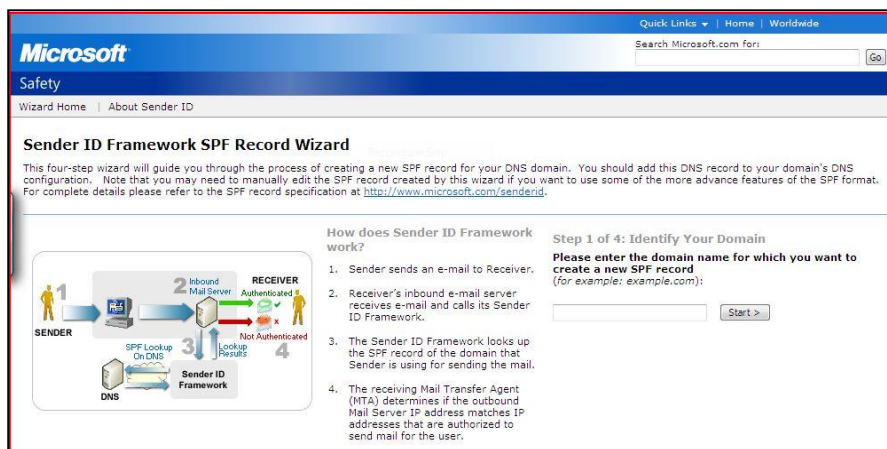


Figure 2 Sender ID Framework SPF Record Wizard

- **Servers operated and administered by the sender's organization.** These are typically the organization's own e-mail servers. They are familiar to the organization's IT department and are usually already identified in the DNS by MX or A records. The Sender ID Framework SPF Record Wizard will display these records; however, additional e-mail servers may be operated by other departments. Particularly in large organizations, it may be necessary to conduct a comprehensive survey 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.

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.

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).

All addresses listed in A records may send mail

207.46.130.108

207.46.250.119

Figure 3 SPF Record Wizard outbound mail server screen

<sup>1</sup> This tool was designed for typical mailing environments. Depending on your environment, you may need to edit the record to be able to make full use of the broad set of SPF record options.

- **Servers operated by third parties to whom sending of e-mail has been outsourced.** E-mail service providers commonly send e-mail on behalf of a domain for a variety of business and marketing functions. After these external senders have been identified, the IP addresses of the additional servers should be included in your SPF record. Additionally, the external providers should be encouraged to publish SPF records of their own. The SPF Record Wizard makes it easy to add references to outsourced domains to an SPF record. Additional information and resources are available on the Authentication and Online Trust Alliance (AOTA) Web site ([www.aotalliance.org](http://www.aotalliance.org)) and the Windows Live Postmaster Services Web site ([www.microsoft.com/postmaster](http://www.microsoft.com/postmaster)).

**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 4 Adding outsourced domains

### ***Creating an Inventory of E-Mail Servers***

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

- Advertising and Public Relations
- Broadcast Mailings
- Corporate E-Mail
- Customer Service
- Customer and Technical Support
- Event Marketing
- Forward to a Friend
- Help Desk
- Human Resources
- Investor Relations
- Newsletters
- Order and Shipping Confirmation

## Testing and Verification

Several tools are available to verify and test records. A list is available on the Microsoft Sender ID Resources Web page ([www.microsoft.com/senderid/resources](http://www.microsoft.com/senderid/resources)). After an SPF record has been created and posted to a DNS, it can be tested by sending e-mail to an automated testing reflector. A reply e-mail message that includes an analysis of the message's authentication status will be sent from multiple e-mail authentication technologies, including the PRA and MAIL FROM checks. (To validate a record completely, an e-mail message must be sent from each of the IP addresses included within the SPF record.)

## Frequently Asked Questions

The following are answers to common questions that arise regarding creating an SPF record. More information can be found in the Sender ID specification (available from [www.microsoft.com/senderid](http://www.microsoft.com/senderid)), and additional information is available from the AOTA Web site (<http://www.aotalliance.org>).

### 1. My domain never sends e-mail. Why do I need to publish a DNS record?

Even if e-mail is never sent from your domain, you can help protect the domain from being spoofed by publishing this simple TXT record in DNS (replace `example.com` with your own domain name):

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

You can publish similar records for sub-domains that do not send e-mail. Suppose `www.example.com` never sends e-mail. You could publish the following record to help protect that sub-domain, even if `example.com`, the parent domain, does send e-mail. In both cases the `-all` record indicates that no mail is sent from the domain.

```
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. What should I do?

Microsoft recommends that you consult broadly within your organization to identify all third-party service providers that may have been engaged to send e-mail on your domain's behalf. Typically these services are used to send things such as newsletters and marketing-related communications. Check with the appropriate departments in your organization and add their IP addresses to your SPF record.

### 3. What happens if I fail to include an IP address of a server?

For some organizations, it can be a challenge to inventory internal and external servers. More importantly, it requires that you have a policy and procedure in place to ensure that your SPF records are maintained. Fortunately, a domain holder can update its SPF record at any time and is limited only by the time it takes the DNS to replicate. By design an e-mail message sent from a server that is not listed may be deleted, blocked, or junked based on the receiving network or ISP's authentication policies. E-mail or domains that are not authenticated are more likely to be subject to greater filtering and not enjoy the benefits of IP reputation.

### 4. 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 up to 48 hours for DNS information to propagate through the Internet, so it's a good idea to wait 48 hours after making a change to your record before you initiate any new e-mail activities. This may be of critical importance to specific e-mail campaigns, and Microsoft recommends that all senders test beforehand.

**5. Some of my employees use mobile devices. How do I accommodate these users?**

Microsoft suggests that the mobile network carrier publish its own SPF record and then insert a header into outbound messages that identifies the user's account on the mobile network. In this way, e-mail can be authenticated as legitimately originating from that network.

**6. Mobile employees frequently send e-mail from hotel or other "guest" e-mail servers. What do I put in my SPF record to cover these situations?**

The best option is for mobile users to send e-mail over a VPN connection or by using a Web-based e-mail client. This way their e-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 e-mail by using a POP or IMAP client, their messages flow through the hotel or guest e-mail server. To deal with this, you could end your SPF record with ~all. The ~all causes a "soft fail" when Sender ID checking is performed. This does not mean that messages will be rejected, but they may be subject to additional spam filtering. Microsoft also suggests that the hotel or other guest e-mail service publish its own SPF record and then insert a header into outbound messages that identifies the guest account. In this way, e-mail can be authenticated as legitimately originating from that service.

**7. 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 that are used in both the MAIL FROM and PRA addresses of messages sent from your domain.

**8. 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 that are used in both the MAIL FROM and PRA addresses of messages sent from your domain.

**9. I am having trouble creating my record. Who can provide assistance?**

Many leading antispam vendors, ISPs, and hosters can provide this service. In addition, you can contact your e-mail marketing service provider. Sender authentication assistance is also available online from the Deliverability.com Web site (<http://www.deliverability.com/>) or by e-mail (contact [senderid@microsoft.com](mailto:senderid@microsoft.com)).

**10. My domain is often used to forward e-mail to other systems. How does Sender ID help me?**

E-mail that is manually forwarded by a user to another user is not affected. However, e-mail that is configured to automatically be forward by a server needs the e-mail forwarder to include an SPF record. The forwarder should insert a header into outbound messages that identifies the user's account. In this way, e-mail can be authenticated as legitimately originating from that network.

**11. Windows Live Hotmail uses a cache of SPF records instead of performing live look-ups in the DNS. How can I include my SPF record in the cache?**

Windows Live Hotmail utilizes a cache to help handle more than 5 billion e-mail messages each day. Although this is not a typical implementation, it provides redundancy and reduces the risk of DNS timeouts. To help ensure that your record is in the cache, after you publish your SPF, you can submit your domain to the cache by using the Web form available at [www.microsoft.com/postmaster](http://www.microsoft.com/postmaster). Please allow 24 hours before you begin your e-mail campaign. The cache is updated several times each day, automatically downloading your most current SPF record.

## 12. Why should I not include a PTR (Pointer Record) or reverse DNS lookup?

Windows Live Hotmail does not support the use of a PTR. As a reference, the Internet Engineering Taskforce (IETF) does not recommend the inclusion of a PTR within an SPF record because it will create unnecessary DNS traffic, will be more prone to errors, and will not function in implementations where SPF records are cached on local servers.

## 13. Why isn't mail that fails SPF deleted or blocked when it is spoofed?

This decision is dependent on the policies of the ISP and the receiving networks. As SIDF has matured, more e-mail that fails the authentication check is expected to be blocked. This change is the result of increasing levels of deceptive and malicious e-mail and the risk of inadvertently clicking links that may be in a user's junk mail folder, independent of user warning. To maximize your brand protection and e-mail deliverability, create your SPF record with the `-all` suffix.

## 14. What else should I do to create and publish an SPF record?

Adoption of e-mail authentication is critical to the entire ecosystem. This document outlines steps to take for outbound authentication. However, organizations of all sizes are encouraged to implement inbound authentication to protect their employees from threats. Most leading e-mail antispam solutions include inbound SIDF validation. Leading solutions are available that support Sendmail and Postfix open source platforms, as well as being fully supported by Microsoft Exchange Server 2003 and Microsoft Exchange Server 2007. A list of third-party solutions providers is available on the Microsoft Sender ID Framework Industry Support and Solutions Web page (<http://www.microsoft.com/senderid/partners>).

## 15. My SPF record was created with an invalid syntax. Why did this happen?

Some third-party tools, including UNIX and Linux shell wrappers, can create and add extra invalid null terminators. The only suffixes permitted are `~all`, `-all`, `?all`, and `+ all`. **Only the `~all` and `-all` should be considered for production purposes; the other record types provide no value to e-mail deliverability or brand protection.**

## 16. What type of SPF records should I not use?

The IETF specification allows for the use of SPF records for testing utilizing a record ending with `?all` as well as provides a syntax declaring anyone can mail from your domain, utilizing `+all`. Neither of these syntaxes should be used. They provide no protection from spoofing and no benefits for enhanced e-mail deliverability. Domain holders should be advised that ISPs may place a negative score on any e-mail associated from such records, as they have been used by spammers who mistakenly think their e-mail would be considered SIDF compliant and obtain a favorable score by doing so.

#####

© 2007 Microsoft Corp. All rights reserved.

This document is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

Microsoft, MSN, Hotmail, and Windows Live are either registered trademarks or trademarks of Microsoft Corp. 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. R11/07