# SPF Records

The Sender Policy Framework (SPF) is an email authentication method designed to detect forging sender addresses during the delivery of the email. SPF allows the receiving mail server to check during mail delivery that a mail claiming to come from a specific domain is submitted by an IP address authorized by that domain's administrators. Adding an SPF record to your DNS configuration can help to reduce spam and improve email deliverability.

**Step-by-Step Guide:**

1. **Log In to Your DNS Provider's Control Panel:**
   - Access your DNS provider's website.
   - Enter your login credentials to access the DNS management console.
2. **Navigate to DNS Management Section:**
   - Look for sections like 'DNS Settings', 'Name Server Management', 'DNS Configuration', or similar.
   - Select the domain you wish to add an SPF record for if you have multiple domains.
3. **Access the DNS Records Section:**
   - Once in the DNS management area, locate the option to view or edit DNS records.
   - This area might be called 'DNS Records', 'Zone File Settings', 'Advanced DNS'.
4. **Check for Existing SPF Records:**
   - Before adding a new SPF record, ensure there are no existing SPF records for your domain to avoid conflicts.
   - An SPF record will start with "v=spf1". If one exists, you should edit this record instead of creating a new one.
5. **Add a New SPF Record:**
   - Look for an option to 'Add Record' or 'Create New Record'.
   - Select the type 'TXT' from the dropdown menu or record type options.
6. **Fill in the SPF Record Details:**
   - In the Host/Name field, you might enter "@" or your domain name to indicate the record is for the root domain.
   - In the Value/Text field, enter your SPF record, which starts with "v=spf1". Here is a simple example:

     ```
     v=spf1 ip4:123.45.67.89 include:_spf.example.com ~all
     ```

   - "**ip4**" defines the IP address authorized to send emails from your domain.
   - "**include**" is used to authorize emails from the domain specified (necessary if you're using a third-party service to send emails on behalf of your domain).
   - "**~all**" indicates that emails from your domain should only come from the specified sources, but it allows for soft failures (used for transitioning and troubleshooting).
7. **Set the TTL (Time to Live):**

- TTL determines how long the record is cached by resolvers. The standard is 3600 seconds (1 hour), but you can set this according to your preferences and needs.

8. **Save the Record:**
   - Click 'Save', 'Add Record', or 'Update' to save the new SPF record.
   - It might take some time for the changes to propagate across the internet, typically from a few minutes to 48 hours.
9. **Verify the SPF Record:**
   - Use online tools like **MXToolBox** to verify that your SPF record is published correctly.
   - Enter your domain and run the test. The tool should show your new SPF record.

**Conclusion:**

You have now added an SPF record to your domain's DNS settings. This should improve your email deliverability and protect against email spoofing. Remember to update your SPF record if you change your email service provider or add new services that send emails on your behalf.

---

Revision #1
Created 9 November 2023 09:09:12 by Admin
Updated 9 November 2023 09:19:49 by Admin