

Adding DNS Records for SPF & DKIM

Enhance email security and deliverability by adding DNS records for SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail). SPF specifies authorized email servers, while DKIM provides email authentication. These records help validate your emails and reduce the risk of them being marked as spam.

- [How to Add SPF and DKIM Records to CloudFlare](#)
- [How to Add SPF and DKIM Records to GoDaddy](#)
- [How to Add SPF and DKIM Records to NameCheap](#)
- [How to Add SPF and DKIM Records to Siteground](#)
- [How to Add SPF and DKIM Records to Dreamhost](#)
- [How to Add SPF and DKIM Records to In-motion](#)
- [How to Add SPF and DKIM Records to HostGator](#)
- [How to Add SPF and DKIM Records to Amazon Route 53](#)
- [How to Add SPF and DKIM Records to Bluehost](#)
- [How to Merge Multiple SPF Records](#)
- [Setting Up DMARC](#)

How to Add SPF and DKIM Records to CloudFlare

Adding your TXT based SPF Record

- From within your Cloudflare account, click on the domain you wish to connect with SmartEngage.
- Along the top menu, select "**DNS**."
- In the top left area is a blue button to "+Add record". Please click on that.
- Then select **TXT**.
- Enter @ as the **Name**.
- Paste the text you copied from your Manage/Integrate page under SPF settings as the **Value**.
- Leave it as **Automatic TTL**.
- Click "**Add Record**."

Adding your TXT based DKIM Record


- The top left dropdown should still show it is selected for **TXT**.
- Paste the text you copied from your Manage/Integrate page under DKIM settings as the **Name**
- Paste the text you copied from your Manage/Integrate page under DKIM settings as the **Value**.
- Leave it as **Automatic TTL**.
- Click "**Add Record**."

How to Add SPF and DKIM Records to GoDaddy

Adding your TXT based SPF Record

- Sign into your GoDaddy Account.
- Select your Domain's **DNS** settings.
- Click **Add** at the bottom right.
- Select **TXT**
- Enter @ as the **Name**.
- Paste the text you copied from your Manage/Integrate page under SPF settings as the **Value**.
- Leave **TTL** to its default setting or enter 14400 if a number is required.
- Click "**Save**"

Adding your TXT based DKIM Record

- Click **Add** at the bottom right.
- Select **TXT**
- Paste the text you copied from your Manage/Integrate page under DKIM settings as the **Name**
 - **IMPORTANT: For GoDaddy You MUST adjust the Name Field you copy and remove the .yourdomainname.com at the end of the name field.**
 - **Example:**
 image not found or type unknown
So the actual record to be added for GoDaddy DKIM is: **the value you see before the dot (.)**
- Paste the text you copied from your Manage/Integrate page under DKIM settings as the **Value**.
- Leave **TTL** to its default setting or enter 14400 if a number is required.
- Click "**Save**"

How to Add SPF and DKIM Records to NameCheap

Adding your TXT based SPF Record

- From within your Namecheap account, click "**Domain List**" on the left navigation.
- Select the box next to your desired domain.
- Click "**Actions.**"
- Select **DNS / Host Records.**
- Select "**I understand this change may impact...**"
- Select "**I want to Update Host Records**" then click "**NEXT.**"
- Click **TXT**
- Enter @ as the **Host.**
- Paste the text you copied from your Manage/Integrate page under SPF settings as the **Target**
- Select **TTL** to and select **Automatic.**
- Click "**Save Changes**"

Adding your TXT based DKIM Record

- From within your Namecheap account, click "**Domain List**" on the left navigation.
- Select the box next to your desired domain.
- Click "**Actions.**"
- Select **DNS / Host Records.**
- Select "**I understand this change may impact...**"
- Select "**I want to Update Host Records**" then click "**NEXT.**"
- Click **TXT**
- Paste the text you copied from your Manage/Integrate page under DKIM settings as the **Host**
 - **IMPORTANT: For NameCheap You MUST adjust the Host Field you copy and remove the `yourdomainname.com` at the end of the name field.**



- **Example:** So the actual record to be added

is: smartengage1._domainkey

- Paste the text you copied from your Manage/Integrate page under DKIM settings as the **Target.**
- Select **TTL** to and select **Automatic.**

- Click "**Save Changes**"

How to Add SPF and DKIM Records to Siteground

Adding your TXT based SPF Record

- From within your Siteground account, click the "**My Accounts**" Menu.
- Select **Access cPanel**.
- Click "**Advanced DNS Zone Editor**."
- Under Add a Record Enter **your domain name** as the **Name** input
- Select **TXT**
- Paste the text you copied from your Manage/Integrate page under SPF settings as the **Address**.
- Enter **14400** for **TTL**.
- Click "**Add Record**."

Adding your TXT based DKIM Record

- Under Add a Record, Paste the text you copied from your Manage/Integrate page under DKIM settings as the **Name**
- Select **TXT**
- Paste the text you copied from your Manage/Integrate page under DKIM settings as the **Address**.
- Enter **14400** for **TTL**.
- Click "**Add Record**."

How to Add SPF and DKIM Records to Dreamhost

Adding your TXT based SPF Record

- From within your Dreamhost account, navigate to your account Menu.
- Click "**Domains.**"
- Click "**Manage Domains.**"
- Click "DNS."
- Scroll to **Add a Custom DNS Record.**
- Enter @ as the **Name.**
- Select **TXT** from the type dropdown menu
- Paste the text you copied from your Manage/Integrate page under SPF settings as the **Value.**
- Click "**Add Record Now.**"

Adding your TXT based DKIM Record

- Scroll to **Add a Custom DNS Record.**
- Paste the text you copied from your Manage/Integrate page under DKIM settings as the **Name**
- Select **TXT** from the type dropdown menu
- Paste the text you copied from your Manage/Integrate page under DKIM settings as the **Value.**
- Click "**Add Record Now.**"

How to Add SPF and DKIM Records to In-motion

Adding your TXT based SPF Record

- Log into your cPanel. Be sure to log in with the cPanel user that owns the domain you are creating the DNS record for.
- Locate the Domains section of cPanel and click on the Zone Editor icon.
- Find your domain in the list under the Domain heading. Under the Actions heading, click on the Manage link that corresponds with the domain you want to create the record for.
- Click the +Add Record drop-down menu button and select the option for the record you would like to add.
- Notice the page now includes fields to enter the details for the new record at the top of the list.
- Enter your domain name as the **Name**
- Leave **TTL** to its default setting or enter 14400 if a number is required
- Set **Type** as **TXT**
- Paste the text you copied from your Manage/Integrate page under SPF settings as the **Record**.
- Finalize by clicking to **Add Record**

Adding your TXT based DKIM Record

- Click the +Add Record drop-down menu button and select the option for the record you would like to add.
- Notice the page now includes fields to enter the details for the new record at the top of the list.
- Paste the text you copied from your Manage/Integrate page under DKIM settings as the **Name**
- Leave **TTL** to its default setting or enter 14400 if a number is required
- Set **Type** as **TXT**
- Paste the text you copied from your Manage/Integrate page under DKIM settings as the **Record**.
- Finalize by clicking to Add Record

How to Add SPF and DKIM Records to HostGator

Adding your TXT based SPF Record

Before continuing, remember that the ability to make these changes yourself is not available without a hosting package with HostGator. However, you may still call HostGator Customer Support to request these changes.

- From within your HostGator account, select “Hosting” from the HostGator dashboard, then “Domains” from the menu.
- Scroll down and select “**Advanced DNS Zone Editor.**”
- Under Add a Record Enter **your domain name** as the **Name** input
- Select **TXT**
- Paste the text you copied from your Manage/Integrate page under SPF settings as the **Address.**
- Enter **14400** for **TTL.**
- Click “**Add Record.**”

Adding your TXT based DKIM Record

- Under Add a Record, Paste the text you copied from your Manage/Integrate page under DKIM settings as the **Name**
- Select **TXT**
- Paste the text you copied from your Manage/Integrate page under DKIM settings as the **Address.**
- Enter **14400** for **TTL.**
- Click “**Add Record.**”

How to Add SPF and DKIM Records to Amazon Route 53

Adding SPF (Sender Policy Framework) and DKIM (Domain Keys Identified Mail) records to your Route 53 hosted domain is an essential step to improve email deliverability and security. These records help verify the authenticity of your email messages, reducing the chances of your emails being marked as spam. Here's a step-by-step guide on how to add SPF and DKIM records for a domain hosted on Route 53:

1. Log in to your AWS Route 53 Console:


- Go to the AWS Management Console (<https://aws.amazon.com/>).
- Sign in to your AWS account.
- Navigate to the Route 53 service.

2. Select Your Domain:

- In the Route 53 dashboard, select the domain for which you want to add SPF and DKIM records.

3. Add SPF Record:

a. SPF records specify which servers are authorized to send email on behalf of your domain. To add an SPF record:

- In the Route 53 dashboard for your domain, click on "Create Record Set" or "Add Record Set."
- Leave the "Name" field blank to create the SPF record for the root domain (e.g., example.com).
- Set the "Type" to "TXT."
- In the "Value" field, enter your SPF record. Here's an example of an SPF record:
arduino 

```
"v=spf1 include:amazonses.com ~all"
```
- Click "Save Record Set" or the equivalent option to save your SPF record.

4. Add DKIM Record:

a. DKIM records provide a signature for your outgoing emails to verify their authenticity. To set up DKIM:

- In your AWS SES (Simple Email Service) dashboard (if you're using SES), navigate to "Email Sending Domains" and select your domain.
- Follow the instructions provided by SES to create DKIM records. This typically involves adding CNAME records in Route 53 with specific values provided by SES.
- In Route 53, create a CNAME record set with the appropriate DKIM values provided by SES.
- Ensure that the "Name" field matches the DKIM record name provided by SES (e.g., "ses1._domainkey.example.com").
- Set the "Type" to "CNAME."
- In the "Value" field, enter the DKIM value provided by SES.
- Click "Save Record Set" to save your DKIM record.

5. Verify Records:

- After adding SPF and DKIM records, it might take some time for DNS propagation. You can use online DNS checking tools to verify that your records are correctly set up.

6. Test Your Email Configuration:

- Send test emails to various email providers to ensure that your SPF and DKIM records are working correctly. Check the email headers to confirm that SPF and DKIM authentication passed.

7. Monitor and Update:

- Regularly monitor your email deliverability and reputation. Make updates to your SPF and DKIM records as needed, especially if you change email providers or sending servers.

That's it! Adding SPF and DKIM records to your Route 53 hosted domain helps improve email deliverability and security by verifying the authenticity of your email messages.

How to Add SPF and DKIM Records to Bluehost

Adding your TXT based SPF Record

- From within your BlueHost Account, navigate to your **Domain** Menu.
- Click "**Zone Editor**."
- Enter @ into the **Host** Input
- Select **TXT** as the type.
- Paste the text you copied from your Manage/Integrate page under SPF settings as the **Value**.
- Leave TTL as **14400**.
- Click "**Add Record**."
- Save your changes.

Adding your TXT based DKIM Record

- Enter ext you copied from your Manage/Integrate page as the **Host** Input
- Select **TXT** as the type.
- Paste the text you copied from your Manage/Integrate page under DKIM settings as the **Value**.
- Leave TTL as **14400**.
- Click "**Add Record**."
- Save your changes.

How to Merge Multiple SPF Records

Merging SPF records

If you use several services to send emails, then you may need to modify an existing SPF record in order to avoid ending up in the recipients' spam filters. This is done through the DNS widget in the Dashboard.

Dissecting the default SPF record

First, let's have a look at the default SPF record:

```
v=spf1 include:spf.smartengage.com -all
```

The first part, "v=spf1", is used to specify that the record in question is an SPF record.

The second, "include:smartengage.com" tells the recipients to include the SPF setup on the domain spf.surf-town.net. We use this domain to list our various email services so that you won't have to worry about which servers that are used to send email.

The third part, "-all", specifies that unauthorized emails should be discarded. One can also use "~all", a less strict variant of "-all", or "?all" if one wants to let the recipients decide what to do with unauthorized emails. We recommend you use "-all" unless you have a specific reason for not doing so.

Now, assume we have the following records:

```
v=spf1 ip4:144.217.88.91 include:nfye.smartengage.com -all
```

And

```
v=spf1 include:spf.protection.outlook.com -all
```

The first, is SmartEngage's default SPF record, the second is the SPF record for another provider such as outlook. If you use another provider for things like receiving email and sending via their interface; this is why this record exists.

In the example above, the first and last parts of the two records are identical. Thus, we simply need to add the middle part of the second record, to the default record:

```
v=spf1 ip4:144.217.88.91 include:nfye.smartengage.com  
include:spf.protection.outlook.com -all
```

Please note, that if the last part, "-all", differ, then you can only select one of them. You cannot have two declarations for all in one SPF record.

Adding the new SPF record

-Remember that only 1 SPF record should exist in your DNS settings so delete the old one and ensure you have just 1 master SPF record which follows the above example.

Due to the way DNS records are cached, it may take somewhere between one 1-24 hours before the new record is visible to the recipients.

Setting Up DMARC

Setting up DMARC (Domain-based Message Authentication, Reporting, and Conformance) can help improve email security and prevent domain spoofing. DMARC can be configured with different levels of strictness, including relaxed (`p=none`) and strict (`p=quarantine` or `p=reject`) policies. Here's a tutorial on how to set up both relaxed and strict DMARC policies:

Setting Up Relaxed DMARC (`p=none`)

Relaxed DMARC allows you to monitor email traffic without taking immediate action on failed messages. This is a good starting point to gain insights into your email authentication status.

1. **Access Your DNS Records:** DMARC records are published in your domain's DNS records. Log in to your domain registrar or DNS hosting provider's dashboard.
2. **Create a DMARC Record:** Add a DMARC TXT record to your domain's DNS. The record should have a `p=none` policy to indicate that you're not taking immediate action on failed messages. Here's an example:

```
v=DMARC1; p=none; rua=mailto:dmarc@example.com;
```

- `v=DMARC1`: This indicates that it's a DMARC record.
 - `p=none`: Specifies that no action should be taken on failed messages.
 - `rua=mailto:dmarc@example.com`: This is the email address where DMARC aggregate reports will be sent.
3. **Publish the Record:** Save the DNS record. It might take some time for DNS changes to propagate across the internet.
 4. **Monitor Reports:** As DMARC reports start coming in, review them to gain insights into email sources and authentication status. Make adjustments to your email infrastructure as needed to improve authentication.

Setting Up Strict DMARC (`p=quarantine` or `p=reject`)

Strict DMARC policies are more secure but can potentially impact legitimate email delivery. Use strict policies when you're confident in your email authentication setup.

1. **Access Your DNS Records:** Access your domain's DNS records as described in the previous section.
2. **Create a DMARC Record:** Add a DMARC TXT record to your domain's DNS. Set the policy to `p=quarantine` or `p=reject` to specify stricter actions for failed messages:
 - `p=quarantine`: Suspicious emails will be delivered to the recipient's spam or quarantine folder.
 - `p=reject`: Fails suspicious emails entirely.

Example for `p=quarantine`:

```
v=DMARC1; p=quarantine; rua=mailto:dmarc@example.com;
```

3. **Publish the Record:** Save and publish the DMARC record in your DNS settings.
4. **Gradual Implementation:** When moving to strict DMARC policies, consider implementing it gradually. Start with `p=none` or `p=quarantine`, monitor reports, and gradually move to `p=reject` as you become confident in your email authentication setup.
5. **Monitor and Adjust:** Continuously monitor DMARC reports and adjust your email infrastructure to ensure legitimate emails aren't affected while blocking suspicious ones.

Remember that strict DMARC policies can affect email delivery, so be cautious when implementing them. Regularly review DMARC reports and refine your DMARC policy based on your organization's needs and email authentication progress.