

# SPF Record Construction

At the beginning of the record, `v=spf1` identifies this as an SPF record. At the end of the record, `-all` defines the policy. Dash - for hard-fail, tilde ~ for soft-fail. In between the identity and policy, each `include:` defines the server domain names that are authorized to send as this domain. Each `+ip4:` defines the IP addresses that are authorized to send as this domain.

## Example

```
v=spf1 +ip4:<IP Address> include:<FQDN> ~all
```

## Microsoft 365

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

## Google Workspace

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

| Prefix | Type    | Value                      | PrefixDesc | Description                                      |
|--------|---------|----------------------------|------------|--|
|        | v       | spf1                       |            | The SPF record version                           |
| +      | include | spf.protection.outlook.com | Pass       | The specified domain is searched for an 'allow'. |
| +      | include | emailus.freshservice.com   | Pass       | The specified domain is searched for an 'allow'. |

| Prefix | Type    | Value                  | PrefixDesc | Description  |
|--------|---------|------------------------|------------|--|
| +      | include | relay.mailchannels.net | Pass       | The specified domain is searched for an 'allow'.   |
| ~      | all     |                        | Fail       | Always matches. It goes at the end of your record. |

Further reading: [a great explanation of SPF](#).

# NEXT STEPS

Configure [DKIM](#) Signature

Configure [DMARC](#) Reports