



# Domain Spam Filtering

Help Documentation

## Domain Spam Filtering

This settings page is only available to Domain Administrators and System Administrators with the proper permissions.

SmarterMail includes a variety of antispam measures that will help keep a user's inbox free of unwanted mail. In the Spam Filtering section, Domain Administrators can review/configure the spam filtering options and trusted senders for users on their domain. To access the spam filtering configuration, log into SmarterMail as a Domain Administrator and use the Menu icon to navigate to the Domain Settings section. Then click on Spam Filtering in the navigation pane.

Jump To:

- Options - Configure the filtering Actions for spam messages on your domain
- Trusted Senders - Exempt specific email addresses and domains from spam filtering

### Options

In most cases, a System Administrator has already configured the filtering options -- spam weights and Actions -- for spam messages on your domain. However, if the System Administrator allows it, Domain Administrators can override those settings and change the Actions configured for spam messages of varying weights to help further remove potentially unwanted email.

### Options

- Override spam settings - Enable this setting to customize the spam filtering Actions for your domain. If this option is disabled, the system's default spam filtering policy will be displayed.
- Allow users to override spam settings - Enable this setting if, as the Domain Administrator, you want to allow users to be able to further edit and manage the Actions taken on messages of varying weights.

### Editing Actions

Each type of spam check has an associated weight that factors into the spam probability of a message. In addition, a specific Action is set for messages that score the weight set by the System Administrator.

To edit the action, click on the card associated with the weight you want to edit. From there, click the dropdown on the Action to change it and click the OK button to save your change.

### Trusted Senders

Domain Administrators can add specific email addresses (such as `jsmith@example.com`) or domains (such as `example.com`) that will be exempted from spam filtering. This lets the system know that these

messages come from a trusted source and can prevent mail from friends, business associates and mailing lists from being blocked or sent to the Junk Email folder. By default, every contact in a user's Contacts list is considered a trusted sender and bypasses spam filtering.

**Important Note :** If SPF and DKIM spam checks are enabled, SmarterMail will run those checks on ALL emails, including those from trusted senders, whitelisted IP addresses and IP bypasses. Because anyone can write any return path that they want when sending a message, this extra check helps prevent spammers from flooding users with hundreds of messages that aren't truly from a trusted sender. If an SPF or DKIM check fails on an incoming message, the trusted sender status will be bypassed, and the weights of all enabled spam checks will be applied. The specific spam check results that will bypass the trusted sender status are SPF\_Fail, SPF\_Softfail, SPF\_PermError, or DKIM\_Fail.

If the trusted sender status of an email was bypassed due to a failed SPF or DKIM check, the TotalSpamWeight line in the email header would appear in the following format:

```
X-SmarterMail-TotalSpamWeight: {Total Spam Weight} ({Where the trusted sender status originates}, {Reason the trusted sender status was bypassed})
```

For example:

```
X-SmarterMail-TotalSpamWeight: 9 (Trusted Sender - Domain, failed SPF)
```

This example indicates that the sender is in the domain-level Trusted Senders list, but the email received a total spam weight of 9 because the message failed the SPF check.

When entering trusted senders or domains, enter only one item per line break.