Domain Settings

Help Documentation

Domain Settings

Default User Settings

Default user settings apply to all new email users added in your domain. Editing the default settings does not change users that are already in place in your domain.

The Default User Settings are almost identical to those found when adding a user. For more information about what each one does, please refer to the help topic Adding a User . For information about the new Skin tab please see below.

Domain Content Filtering

Domain content filtering allows you to create the same types of content filters as you can in My Content Filtering, but the filters added will be applied to all members of a domain. The evaluation of domain content filters happens before the evaluation of account-specific content filters. For more information about how to add a content filter, please refer to the topic My Content Filtering .

Note: Be aware that many users will prefer to set their own content filtering. You may want to minimize filtering at the domain level to filter only items that affect the entire domain.

Domain Spam Filtering

SmarterMail includes many advanced Anti-Spam measures that will help protect your users from unwanted email. The system administrator has probably already set up some default spam options which you may accept or override as you feel is best.

Use default spam settings - Choose this option to accept the default spam options provided by your system administrator. The settings will be displayed for your reference.

Override spam settings for this domain - Select this option to customize the way spam is handled. Spam check weights and actions will become overridable by end users. More information about the types of actions allowed can be found below.

Spam check weights

Each type of spam check has an associated weight that factors into the spam probability of a message. When an email comes in, all of the checks listed are run, and for each check that the message fails, the weight is added to the overall score of the email. The thresholds for each spam probability are examined, and the email is placed into the appropriate category.

SPF Filtering Options

Pass - Indicates that the email was sent from the server specified by the SPF record (more likely good mail). The weight you set may be 0 (for no effect) or a negative number, thereby reducing the spam rating.

Fail - Indicates that the email was sent from a server prohibited by the SPF record (highly likely spam). Set this to a relatively high weight, as the probablility that the email was spoofed is very high.

SoftFail - Indicates that the email was sent by a server that is questionable in the SPF record. This should either be set to 0 or a low spam weight.

Neutral - Indicates that the SPF record makes no statement for or against the server that sent the email. Except in very special circumstances, leave this set to 0.

PermError - Indicates that the email sender does not publish an SPF record or there is a syntax error in the record. Since SPF is relatively new, many legitimate domains do not have SPF records. It is recommended that you leave this at 0 until SPF becomes more popular on the internet.

SpamAssassin

The SpamAssassin weights can only be changed at the system administrator level. If you would like to change these weights, we recommend getting together with your system administrator and working out an agreeable anti-spam strategy.

Actions

When you choose to override the spam options set by your system administrator, you get to choose the actions that are taken when email comes in that has a low, medium, or high priority of being spam. For each spam level, choose the action you wish to have taken. If you chose to add text to the subject line of messages, enter in the text in the box below the action drop down.

Trusted Senders - Email addresses (ex: joe@example.com) or domain names (ex: example.com) can be added to the domain list of trusted senders. When email comes in from a trusted sender, all spam filtering for that email is bypassed. Enter one email address or domain name per line.

When all settings are entered, click on the Save link.

Domain Aliases

A Domain Alias is an alias for a secondary domain name that points to an existing email account on the server under an existing primary domain name.

For example, a full email addresses requires a user name and a domain name (ex. user@example.com). If you add a domain alias on a secondary domain like "example-alias.com" then not only will "user@example.com" be valid, but the same mailbox will also work with "user@example-alias.com". If an email was sent to both emails then the "user" mailbox would get two copies of the emails.

A user cannot log into the web interface under a domain alias, just the original domain, nor can a user send an email from the domain alias. Remember, any alias is simply a pointer to an existing email account on the server.

Notes:

- Messages can not be retrieved with a domain alias email address unless the domain is properly registered at a domain registrar.
- The mail exchange (MX) record for the domain being added must already be pointing at the server prior to this process. This prevents users from 'hijacking' mail from valid domains. For example if this check were not in place a user could add a domain alias of example.com. Then, any mail sent from the server to "anything@example.com" would go to the domain with the example.com domain alias, rather than to the actual domain.

Domain Folder Auto-Clean

Domain Folder Auto-Clean is a method for limiting how much of your account disk space is used by the Junk E-Mail, Sent Items, and Deleted Items folders. By placing limits on the size of these folders, you can help ensure that your domain accounts do not fill up unnecessarily. Oldest messages will be deleted from the folders first. If you override the auto-clean settings, the settings you choose will trickle down to your users.

Note: Depending on the policies your administrator has established, you may or may not be able to change the settings on this page.

Note: If auto-clean is active on a folder, messages will get deleted from it eventually, so do not keep messages in that folder if you want to keep them.

Options

Use default auto-clean settings - Choosing this option will let you adopt the policy of your system administrator. If the administrator changes the policy, yours will automatically change with it. You can see the current policy on the Folders tab when this option is active.

Override auto-clean settings for this account - Choose this option to override the settings. Any changes you make will not be affected if the administrator changes the policy, unless they disable overrides.

Folder Settings

If you are using the default auto-clean settings set up by your administrator, you will be shown them on this tab.

In the case that you have chosen to override the settings, the following options appear once for each folder that can be auto-cleaned.

Enable auto-clean for this folder - If this box is checked, then auto-clean will be active for the specified folder.

Folder size BEFORE auto-clean - Once the folder reaches this size (in megabytes), the auto-clean process is started, and older messages are cleaned.

Folder size AFTER auto-clean - This is the goal size for the auto-clean process. It will try to delete older messages until the folder gets to this size. This number should always be lower than the "before" number.