



# Domain Settings

Help Documentation

# Domain Settings

## General Domain Settings

This settings page is only available to Domain Administrators.

Below are the options available for managing and configuring a domain. To access the domain settings, log into SmarterMail as a Domain Administrator and use the Menu icon to navigate to the Domain Settings section. Then click on General in the navigation pane. The following options will be available:

Jump To:

- Domain Aliases - Add an alternate domain name for users on the domain
- User Options - Adjust settings that apply to users on the domain
- Custom Help - Add a button to the Help menu
- Login Display - Customize the login page for your domain
- 2-Step Authentication - Turn 2-Step on or off for the domain
- Logout URL - Set a special page to load on logout
- Footer - Add a message footer that appends all outgoing messages
- Email Signing - Protect users from phishing schemes and spam attacks
- Attachments - Manage the incoming and outgoing extension blacklist
- Mailing Lists - Set the Bounces Before Removal threshold for mailing lists

## Domain Aliases

A domain alias is basically an alternate domain name for one that already exists in SmarterMail. Domain aliases are useful, as they allow companies with multiple domain name extensions to receive any email sent to one of their domains directly within SmarterMail. For example, imagine you have a domain, 'example.com' with a user configured under 'user@example.com'. By adding a domain alias for 'example.net', any email sent to 'user@example.net' will be delivered to 'user@example.com'.

Note: You must own the domain name in order to create a domain alias. In addition, messages cannot be retrieved with a domain alias email address unless the domain is properly registered at a domain registrar.

### Creating a Domain Alias

To create a new domain alias, click New Domain Alias . Then enter the name of the alternate domain. The name will be used to create the domain alias email address. For example, if the name of the alias is "example2.com", the domain alias email address will be user@example2.com.

Note: By default, before a Domain Administrator can save a domain alias, SmarterMail will check that the mail exchange record for the domain is pointing to the server. This prevents Domain Admins from "hijacking" mail from valid domains. For example, if this check were not in place, a Domain Admin 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. Alternatively, System Administrators who impersonate a domain will see an option when adding a domain alias on whether to verify the MX record before saving.

## User Options

This feature is only available when using SmarterMail Enterprise.

- Include mailing lists in the Global Address List - The Global Address List (GAL) is basically a listing of all users who have accounts for your particular email domain. By toggling the slider to the right, any mailing lists that have been created will appear as a contact in the Global Address List. In turn, that means anyone with access to the GAL will be able to see and/or possibly send emails to the list.
- Include aliases in the Global Address List - The Global Address List (GAL) is basically a listing of all users who have accounts for your particular email domain. By toggling the slider to the right, any aliases that have been created will appear as a contact in the Global Address List. By default, this is enabled, but Domain Administrators may want to exclude aliases from appearing in the GAL, as they could be used to send emails to customers or to important contacts.
- Show calendar availability for all users in domain - This setting is enabled by default and allows SmarterMail to alert users of any scheduling conflicts when adding a member of the Global Address List as an attendee on a calendar appointment. In addition, this allows users to view an Availability window to review the times that their attendee is free/busy. When disabled, domain users' scheduling information will not be displayed in the appointment window.

## Custom Help

Note: This section will only be visible if the System Administrator has enabled Login Display Customization for the domain.

- Custom Help URL - Entering a full URL in this field will add a custom button to the Help menu that users can access in the SmarterMail interface. Administrators can link to a variety of things, including server-specific instructions for syncing, help resources, contact information, etc.
- Custom Help Text - The hyperlink text for the custom URL in the Help menu. Note: If no text is entered in this field, the hyperlink text in the Help menu will default to "External Help".

## Login Display

Domain Administrators can customize the SmarterMail login page for their domain to add a company logo, provide additional branding text, or simply adjust the default “Login to SmarterMail” text to be more in line with an overall brand message.

Note: This section will only be visible if the System Administrator has enabled Login Display Customization for the domain. Furthermore, if the System Administrator allows a domain to override the custom login display and the Domain Administrator does not enable customization for their domain, users will see the default SmarterMail login screen, regardless of whether the System Administrator has enabled a custom login display for the server.

- **Image for Login Screen** - Upload an image, like a company logo, by dragging and dropping a file in the highlighted area or clicking to browse for a file (max file size of 3mb). Uploading an image using this upload control will host the image publicly on the server and enter the `` tag in the HTML section. Note: Uploading an image here alone will NOT display the image on the login screen. The HTML must remain in the Login Page HTML section. This upload control can be used by those who don't have their logo publicly hosted or who wish the image source to point back to their mail server. Furthermore, regardless of the image uploaded, the image's source URL will remain the same; only one image may be hosted at a time.
- **Custom Login Text** - Use this setting to customize the login page header to something more in line with an overall brand message. If Custom Login Text is left blank, SmarterMail's login page will show the default text "Welcome to SmarterMail".
- **Custom Title Text** - Use this setting to customize the title of the login page to something more in line with an overall brand message. If Custom Title Text is left blank, SmarterMail's login page will show the default text of "SmarterMail" in the browser tab title. Note: Users will see this text on the login page only, with their email address displayed as the browser title for all other pages.
- **Login Page Language** - Use this setting to set the default language of login page as well as the default language if "Login Display Customization" is enabled for a domain. NOTE: This setting will only go into effect for a new user who is visiting the SmarterMail login page for the first time, or if a user's local storage is cleared. This will NOT change the default language for users who return to the login page after already visiting it under a different language.
- **Enable custom login page HTML** - Toggle the slider to the right to enable the ability to use HTML to further modify the login screen to add additional text or adjust the layout.
- **Login Page HTML** - Enter the custom HTML that will be used to further modify the login screen (in-line custom CSS can be used as well). Note: To include white space around the Image for Login Screen, the div id "companyinfo" must be included. In addition, Domain

Administrators cannot enter scripts as this is considered to be unsafe code; however, System Administrators do not have this limitation.

## 2-Step Authentication

2-Step Authentication is a method of providing a second verification of account ownership before a user can log into their account or connect to third-party clients and/or devices. For example, when a user has set up 2-Step Authentication for their account, the SmarterMail login page will require their primary account password and a secondary verification of account ownership before the user can log into webmail. The second method of verification will be provided to the user through popular authentication apps, like Google or Microsoft Authenticator, or through a recovery email address. When this feature is enabled for a domain, the Domain Administrator can choose whether to enable or force 2-Step Authentication for their users.

## Logout URL

In most cases, when a user logs out of SmarterMail, they are taken back to the standard login screen. However, Administrators can enforce a logout redirect for all users on the system (like to an Intranet page or company site) or allow Domain Administrators to enforce their own policies. In this section, the system policy will be displayed.

If the Administrator has allowed it, you can toggle the slider to the right to Override System Settings , then enter a unique logout URL for the domain in the Logout URL text box.

## Footer

If the system administrator has enabled footer customization for the domain, Domain Administrators can configure server-wide message footers that SmarterMail will append on all outgoing messages, forwards that do not already have a footer, replies to messages and emails sent to a mailing list from SmarterMail, if enabled. Although similar to signatures, message footers are typically used to convey disclaimers or provide additional information. For example, a domain administrator may want every message to include a notice that the message was scanned for viruses or the text "Sent by SmarterMail." NOTE: If the system administrator has a footer configured and enabled for all messages, incoming messages will use that footer. If the domain footer is the only one being used, it is only appended to outgoing messages.

The following options will be available:

- Override footer settings for this domain - Toggle the slider to the right to customize the footer for your domain.
- Enable footer for all messages - When toggled to the left, only outgoing messages will have the footer appended. When toggled to the right, new messages as well as replies and forwards

will have the footer appended.

- Apply to mailing lists - By default, footers are not applied to emails posted to mailing lists. To add the footer to mailing list emails, toggle the slider to the right. Note: Mailing lists have their own configurable footers. If a custom mailing list footer is already configured, enabling this option will append a second footer at the end of each message posted to the mailing list subscribers. Because this may be confusing for mailing list moderators and recipients, most administrators will choose to keep this option disabled.
- Footer - Use this section to create the message footer text. Clicking the edit icon will open a modal that includes an HTML-based editor, allowing admins to create footers that seamlessly fit into any email message. Note: The message footer does not support the use of variables.

## Email Signing

Email signing protocols can be used to protect users from phishing schemes or spam attacks. For example, DKIM signing uses cryptography to verify the authenticity of a message, ensuring the message came from your server and was not changed in transit. To enable DKIM Signing, click the Enable button. SmarterMail will display a unique Text Record Name and Text Record Value. You will need to contact your DNS provider and add the TXT record to your DNS server. After the TXT record has been added to DNS, click on the Enable button once again. SmarterMail will attempt to verify the DNS settings and DKIM Signing will be enabled.

To view the Text Record Name and Value, click on View Record . To adjust the mail signing settings, click the Settings button. Note: In most cases, these settings do not need to be altered. However, in the event that you would like to specify how closely you want the system to monitor messages in transit, please refer to the DKIM documentation linked below.

- Body Canonicalization - The method used to monitor in-transit changes to the body of a message. Two canonicalization algorithms are defined for the body: a "simple" algorithm that tolerates almost no modification and a "relaxed" algorithm that tolerates common modifications such as whitespace replacement and header field line rewrapping. For more information, please visit <http://dkim.org/specs/rfc4871-dkimbase.html#canonicalization> .
- Header Canonicalization - The method used to monitor in-transit changes to the header of a message. Two canonicalization algorithms are defined for the header: a "simple" algorithm that tolerates almost no modification and a "relaxed" algorithm that tolerates common modifications such as whitespace replacement and header field line rewrapping. For more information, please visit <http://dkim.org/specs/rfc4871-dkimbase.html#canonicalization> .
- Header Field to Use - The header fields included in the hash algorithm. This is further defined by header fields. For assistance in determining the header fields to sign, please visit <http://dkim.org/specs/rfc4871-dkimbase.html#canonicalization> .

- Header Fields - The header fields included in the hash algorithm. Note: List only one header field per line break.

## Attachments

- Incoming Extension Blacklist - This list allows you to limit the file types that can be attached to emails sent to users on your domain. For example, many email administrators won't allow executable files (EXE) as they can cause issues on the mail server, and possibly across an entire network. To add a blacklisted file type, simply type in the file extension, one per line. (E.g., .exe or EXE)
- Outgoing Extension Blacklist - This list allows you to limit the file types that are users on your domain are allowed to send out of the mail server. For example, many email administrators won't allow batch files (BAT) as they can cause issues on the recipients' mail server, and possibly across their entire network. To add a blacklisted file type, simply type in the file extension, one per line. (E.g., .bat or BAT)

## Mailing Lists

Mailing Lists are a great way to allow users to communicate with a number of different individuals via a single email address. Unlike an Alias, a mailing list allows people to subscribe to, or unsubscribe from, email communications. In addition, mailing lists can be public or private, be replied to by all users or managed by a single list administrator and more. Use this card to specify the following mailing list setting:

- Bounces Before Removal - The number of times a message to a specific subscriber may bounce before the subscriber is automatically removed from the mailing list.

## Accounts

### Users Overview

This settings page is only available to Domain Administrators.

The Users section is where a Domain Administrator can manage the user accounts on their domain. This document explains the actions that can be taken on user accounts, including the ability to set the default user settings and propagate those settings to specific users, import users, improve the search functionality for a user by reindexing their account, and more.

For information on how to add, edit or delete a user account, and for an explanation of the configuration options available for user accounts, please refer to the Managing Users page.

To access the Users section, log in to SmarterMail as a Domain Administrator and click on the Domain Settings icon . Then click on Accounts in the navigation pane. The Users tab will load by default.

Jump To:

- User Defaults and Propagation - Set the default configuration of new users and propagate settings to all or specific users.
- Reindex a User - Improve the search functionality for a user by reindexing their account.
- Refresh Disk Usage - Recalculate the disk usage for one or more user accounts.
- Expire Password - Force a user to change their password on their next webmail login.
- Import from CSV - Import new user accounts from a CSV file.
- Import from LDAP - Import new user accounts from Microsoft's Active Directory.
- Export All CSV - Export a CSV file of all users on the domain.

## User Defaults and Propagation

For domains that have a large number of users, it can be time consuming to make a change to user permissions and then ensure the right users have the same change applied to their mailboxes. With User Defaults, however, Domain Administrators can create a template for the default user settings so that they only have to make the change in one location, and then propagate those settings to a select few users or each user on the domain. This makes changing settings quick and easy and ensures each user has the exact same permissions and settings applied.

To review the default configuration for new users, click on the User Defaults button. (The default user settings are identical to those found when adding or editing a user. For more information on these settings, refer to the Managing Users page.) Modify and save these settings as desired.

To apply some or all of the default user settings to some or all of the existing users on the domain, click on Propagation . Checkmark the settings to propagate, then select whether to push these settings to specific users or all users on the domain. Then click Propagate.

Simply making a change to the User Defaults doesn't automatically propagate, so a change to default settings does not change users that are already in place for the domain. In order for changes to take effect, they must be propagated.

NOTE: If a System Administrator is impersonating a domain administrator and wants to propagate settings changes -- and, specifically, Exchange Synchronization changes -- User Administration for those settings MUST be enabled for the domain. Otherwise, changes will not be saved for users.



## Reindex a User

If a user reports errors or a lack of results when performing a search, it may be necessary to reindex their user account, which will regenerate the mailbox index file. To reindex one or multiple users, checkmark the desired user accounts, click on the Actions (...) button, then click on Reindex .

## Refresh Disk Usage

This option can be used to recalculate the disk usage for the selected user(s). If you find discrepancies in the user's disk usage display throughout the various areas of the interface (in the email section, reports, or Users grid), use this option to recalculate and correct that display. Please note that there may be no visual effect if the disk usage numbers shown were already correct. To refresh the disk usage for one or multiple users, checkmark the desired user accounts, click on the Actions (...) button, then click on Refresh Disk Usage .

## Expire Password

This option can be used to expire the password of one or more users, forcing the user(s) to change their account password the next time they log into the webmail interface. To expire the password of one or multiple users, checkmark the desired user accounts, click on the Actions (...) button, then click on Expire Password .

Note: If password changes were disabled for a user, expiring the user's password will automatically enable password changes and expire their password. They will be required to set a new password next time they log in. In addition, accounts set to Active Directory authentication cannot be expired.

## Import Users From CSV

To add new SmarterMail users via a CSV spreadsheet, click on the Actions (...) button then click on Import from CSV . Upload the CSV file that contains the user information and click Next . The first page of the import modal will allow you to map the CSV column headers to the appropriate configuration option within SmarterMail. For example, if your CSV contained a column header for "user name", you can select the "Username" mapping.

At minimum, the CSV file must contain a "Username" column header. All remaining account configuration options will mimic the domain's User Defaults template. If no "Password" column header is provided in the CSV, the import modal will prompt you to create a temporary password for the user(s) being imported. Those users will be prompted to change their password the next time they log into the webmail interface.

## Import Users From LDAP

This feature is only available to Domain Administrators using SmarterMail Enterprise.
---

The Lightweight Directory Access Protocol (LDAP) is an Internet protocol that email servers and other programs use to connect to, and look up information from, a server. In SmarterMail, LDAP is most commonly used for integrating SmarterMail with Microsoft's Active Directory.

To add new SmarterMail users via the LDAP protocol, click on the Actions (...) button then click on Import from LDAP . Type in the LDAP Binding String . Enable Use LDAP email as username if you would like the LDAP email to be used as the account username. Click List Users to preview the users that will be imported. Then click Import .

Note: LDAP integration will only function if SmarterMail is on the same domain as the LDAP server you are trying to connect to.

## Export All CSV

To export a list of all user accounts on the domain, click on the Actions (...) button then click on Export All CSV . The CSV file will continue a variety of details about the user accounts, including their username, display name, authentication method, home and work address, disk usage, and more.

## Managing Users

This settings page is only available to Domain Administrators.

The Users section is where a Domain Administrator can add, view and modify the user accounts on their domain, where each account represents a person's actual mailbox and email address (ex: `jdoe@example.com`). Domain Administrators can modify basic configuration options for a user, including their password method, features they can access, reply-to addresses, webmail preferences and more.

For a better understanding of the actions that can be performed in the Users section, see the Users Overview page.

To access the list of users on your domain, log in to SmarterMail as a Domain Administrator and click on the Domain Settings icon . Then click on Accounts in the navigation pane. The Users tab will load by default.

## Adding Users

Adding a new user and editing an existing user both deal with the same settings. To create a new user, simply click on the New button. The following initial options will be available:

- Username - The identifier the user uses to login to SmarterMail. This is the portion of the email address that comes before the domain name. For example, the "jdoe" part of `jdoe@example.com`.

- **Authentication Mode** - The authentication method used to login to SmarterMail. By default, SmarterMail will use its included username/password authentication. However, SmarterMail can also be integrated with customers using Microsoft Windows Active Directory for their corporate logins. For information on Active Directory integration, visit the SmarterTools Knowledge Base .
- **Active Directory Username** - If Active Directory is selected for the Authentication Mode, this field will appear. Enter the Active Directory username to authenticate against for Active Directory authentication.
- **Domain** - If Active Directory is selected for the Authentication Mode, this field will appear. Enter the Domain to authenticate against for Active Directory authentication.
- **Password** - If SmarterMail is selected for the Authentication mode, this field will appear. Enter the password this user will use to log into their account.
- **Confirm Password** - If SmarterMail is selected for the Authentication mode, this field will appear. Confirm the password this user will use to log into their account.
- **Force password change at next login** - Enable this setting to require the user to set a new password the first time they log in to the SmarterMail web interface.

After the initial creation of a new user, and when editing an existing user, the following options will be available:

## Account

- **Username** - The identifier the user uses to login to SmarterMail. To change an account's username, click on the Actions (...) button and then Rename .
- **User Status** - Domain administrators can change the status on a mailbox to limit a user's access as needed. For example, if a user leaves the company, either voluntarily or not, a domain administrator can suspend the account pending further review by company management. Options include:
  - **Enabled** - The mailbox is in use by the user.
  - **Disabled and allow mail** - The mailbox continues to receive email but the user is unable to access their mailbox.
  - **Disabled and don't allow mail** - The mailbox no longer accepts incoming messages and the user is unable to access their mailbox.
- **Display Name** - The friendly name that is displayed on outgoing messages.
- **Authentication Mode** - The authentication method used to login: SmarterMail or Active Directory. To change a user's password when using SmarterMail verification, click on the Actions (...) button and then Change Password . When using Active Directory, changes to a user's password must be done in the directory itself.

- **Active Directory Username** - If Active Directory is selected for the Authentication Mode, this field will appear. Enter or adjust the Active Directory username to authenticate against for Active Directory authentication.
- **Domain** - If Active Directory is selected for the Authentication Mode, this field will appear. Enter or adjust the Domain to authenticate against for Active Directory authentication.
- **Mailbox Size Limit** - The maximum size of the mailbox. By default, the maximum mailbox size is 100 MBs. However, domain administrators can change this to whatever they like to correspond to company limits. For unlimited disk space, type in 0.
- **Domain Administrator** - Toggle the slider to the right to make this user one of the Domain Administrators for the domain, which allows the user to create new users and edit domain-wide settings.

## Exchange Synchronization

This feature is only available when using SmarterMail Enterprise.

- **Enable EAS** - Toggle the slider if EAS is enabled for the domain and if you want the User to be able to connect a mobile client using EAS.
- **Enable MAPI/EWS** - Toggle the slider if MAPI/EWS is enabled for the domain and if you want the User to be able to connect to Microsoft Outlook and other email clients using MAPI and/or EWS. (NOTE: if ONLY MAPI or EWS is needed for a domain, both protocols will still be available once the slider is active.)

## User

- **Time Zone** - The time zone to use for marking the sending and receiving date and time.
- **Reply-to Email Address** - The email address used in the reply-to header of messages sent through webmail. This address will be used by receiving email clients when replying to a message.
- **Recovery Email Address** - The email address to which password reset instructions will be sent if the user forgets their account password. This address should be separate from the SmarterMail account, such as a Gmail or Yahoo! address, or even the default email address of a Domain Administrator. Note: The backup email address can only be used if the System Administrator has enabled password retrieval for the login page. If the account is protected by 2-Step Authentication, this address may also be used to retrieve the 2-Step verification code.
- **Plus Addressing** - Plus addressing allows users to automatically sort incoming email without creating content filtering rules first. A major benefit of plus addressing is that it allows users to generate special email addresses if they do not want to give out their real address. For example, if user@example.com needs to provide a valid email address to sign up for a newsletter, he can sign up for the newsletter using the following address: user+technewsletter@example.com.

When the newsletter is delivered, it can automatically be routed to the Technewsletter folder. If the folder does not already exist, it can be created automatically. Note: For plus addressing to work, the plus (+) sign is required AFTER the username but BEFORE the domain name. For example, username+foldername@domain.com).

- Disabled - Select this option to turn off plus addressing for the account.
- Move to Folder - If the target folder already exists, the incoming message will be placed into it. If the folder does not exist, it will be created automatically. Note: To prevent abuse, no more than 10 folders can be auto-created in this method during a six hour period.
- Move to Folder (If Exists) - If the target folder already exists, the incoming message will be placed into it. If the folder does not exist, the email will be placed in the Inbox.
- Leave in Inbox - The incoming message will be placed in the Inbox.
- Calendar Auto-Clean - SmarterMail allows domain administrators to keep users' past calendar events from cluttering up calendar views. By default, this is set to Domain Default, which follows the policy set by the Administrator for the domain. However, you can adjust this policy per user, as needed.
- Disable password changes - Select this option to prevent the user from changing the login password. This setting overrides the password expiration found in Security settings. A user's password will not expire or be required to be changed if this setting is enabled.
- Show in Global Address List - This setting is enabled by default and allows the user account to be displayed in the Global Address List, which is found in the Contact section. This option is useful for only displaying accounts that are tied to real people as opposed to addresses used by departments, such as support@example.com. Note: This option is only available when using SmarterMail Enterprise.
- Enable External SMTP Accounts - Enable this option to allow users to send email from a third-party mail server account right from within SmarterMail. For example, if a user has a second email address that they regularly use, enabling this option would allow the user to set up an SMTP Account for that address and choose which account to send from when composing new messages.
- Disable greylisting - Greylisting is a spam prevention method that temporarily rejects any email from an unrecognized sender. Though effective, greylisting can lead to a delay in email delivery for a user. Domain administrators can disable greylisting on a user-by-user basis as needed, while allowing it for other mailboxes. Note: This setting will only be visible if greylisting has been enabled for the server. --%>

## Temporary Password

This feature is only available to System Administrators.
--

This feature allows System Administrators who are managing/impersonating the domain to create an additional, temporary user password in order to troubleshoot account issues. Creating a temporary password, rather than impersonating the account, may be required when it's necessary to log into a user's email or IM client where impersonation is not available. In addition, administrators will find that some behavior in webmail may be slightly different depending if an account is impersonated or logged in directly. For example, when you impersonate a user, the Domain Admin's settings always show, even if you're impersonating a user that isn't a Domain Admin. For a clear idea of the options available to the user, an administrator may wish to log in directly instead.

- **Generate** - Click on Generate to create a temporary password. Only one temporary password may be created at a time, and on creation, will be available for 24 hours. Extend the time remaining or revoke the password by clicking on the corresponding button. Choosing to extend the password will add 24 more hours to the remaining time. Note: Creating and using a temporary password does not disable the user's standard account password or impact their ability to log in or access webmail.

## Webmail

- **Delete Action** - To specify the action performed on deleted messages, select the appropriate action from the list.
- **Move to Deleted Items folder** - Deleted items will appear in the deleted items folder, which will need to be regularly emptied.
- **Auto Purge Folder** - Permanently deletes the message. Note: When deleted messages are purged, the action is final. You will not be able to retrieve these messages later.
- **Mark as Deleted** - Flags the message for deletion, but it does not move messages to the Deleted Items folder and messages remain until the folder is purged.
- **Mark as Deleted and Hide** - Flags the messages for deletion and hides them from view, but they will not be removed until the folder is purged. Note: Be careful to monitor your disk space usage when using this option, as it may fill up with what appears to be a small number of messages.
- **Text Encoding** - To specify the character set used in messages composed through the Web interface, select the appropriate option from the list. By default, SmarterMails sets the encoding to Western European (ISO). However, SmarterMail supports encoding for over 35 different text formats, thereby supporting encoding for most parts of the world.
- **Compose Font** - Specify the default font for emails by selecting an option from the list.
- **Compose Size** - Specify the default font size for emails by selecting an option from the list.
- **Preview Pane** - To specify where the preview pane displays in the webmail interface, select the appropriate option from the list: Right, Bottom or None. By default, the preview pane appears to

the right of the messages list. Disabling the Preview Pane means only a list of messages appears in the content pane and each message will need to be opened separately in order to view their contents.

- Search Language Indexer - The language that the Lucene indexer will index against. In most cases, Generic Indexer is the best selection as it incorporates English and common umlauts. However, if the user views the interface in certain languages, such as Chinese, Japanese, or Korean, this setting should specify the language for better indexing results.
- Request read receipts by default - Select this option to automatically request read receipts for all outgoing messages sent via webmail. When this setting is enabled, all outgoing messages that are sent via webmail will request that the recipient(s) send a read receipt when the message has been read. If the read receipt is sent by the recipient(s), the user will receive a message from the system administrator confirming that the message has been read. Note: Users should be careful when enabling this feature and should only do so if required for business or compliance or regulatory requirements.
- Request delivery receipts by default - Select this option to automatically receive delivery receipts for all outgoing messages sent via webmail and email clients. When this setting is enabled, the user will receive a message from the system administrator stating the status of their outgoing message. Note: Users should be careful when enabling this feature and should only do so if required for business or compliance or regulatory requirements.
- Use sent items for autocomplete (webmail only) - SmarterMail's auto-complete feature allows users to quickly select an email address from a dropdown list when filling in the To, Cc and Bcc fields while composing an email or when adding Attendees to a calendar appointment. Select this option to automatically add the To, Cc and Bcc addresses of all outgoing messages delivered via webmail to the autocomplete list.
- Mark messages downloaded by POP as read - Select this option to mark all messages that are downloaded via a POP3 connection as read.
- Allow Inline Images - Enable this option to automatically display all in-line remote content when an email is viewed. (Remote content is considered to be any image, video, animated gif, etc. that has an external source and is contained in the message.) When this is enabled, the user will not have to manually display the remote content on emails they receive; it will be visible automatically. Note: Emails from trusted domains and senders will always display remote content automatically.

## Forwarding

If this card is not displayed, your domain has not been permitted to utilize automated forwarding. To display these options, a system administrator must enable the Automated Forwarding feature for your domain.

- **Enable Automated Forwarding** - Select this option to allow the user to utilize the automated forwarding feature and to display the forwarding settings. If this setting is disabled, the Forwarding card will not be displayed in the user's Account settings.
- **Forwarding Address** - The email address to which messages sent to the mailbox will be automatically forwarded. Note: Messages routed to other email folders via content filters or plus addressing will also be forwarded to this address.
- **Forward Method** - To specify the method by which messages are forwarded, select the appropriate option from the list.
  - **Normal** - Includes original content, including font styles from original message, as part of the new message.
  - **Text** - Inserts the plain text version of the original message into the new message. This is useful if you want to exclude links, fonts or other formatting.
  - **Embed as Attachment** - Attaches the original message to the new message as an attachment. The message will not appear in the body of your message.
  - **Delete messages when forwarded** - Select this option to delete messages from the SmarterMail mailbox after they are forwarded.

## User Groups

This feature is only available when using SmarterMail Enterprise.

User Groups are used to give a specific subset of users on the domain permission to access shared resources. Use this card to add the user to any existing Groups that have been configured for the domain.

## Throttling

Throttling limits the number of messages sent per hour and/or the amount of bandwidth used per hour to send messages. Domain administrators can use this feature on a per user basis to either delay or reject messages that exceed their desired limits, thereby ensuring users don't send out massive amounts of email throughout the day that can possibly get the domain blacklisted.

Note: For each threshold and action, you'll see "(Default = X)" which indicates the throttling policy that's put in place by the system administrator for the ENTIRE domain. It's important to consider the domain's throttling limits when modifying a specific user's limits. For example, if you set the user's throttling limit to the domain max, and that user sends that many messages in an hour, the WHOLE domain would be throttled. This means that outgoing messages from all users on the domain would either be delayed or rejected, depending on the domain's throttling action.



- **Outgoing Messages per Hour (0 = Unlimited) (Default = 5000)** - The number of messages sent by the user per hour.
- **Message Throttling Action (Default = None)** - Select an action for SmarterMail to take once the particular throttling level is reached. Of course, administrators can elect to do nothing at all, or they can either Delay or Reject messages until the amount of mail being sent falls beneath the throttling limit that is set.
- **Outgoing Bandwidth per Hour (0 = Unlimited) (Default = 100)** - The total number of MBs sent by the user per hour.
- **Bandwidth Throttling Action (Default = None)** - Select an action for SmarterMail to take once the particular throttling level is reached. Of course, administrators can elect to do nothing at all, or they can either Delay or Reject messages until the amount of bandwidth being used falls beneath the throttling limit that is set.

## Service Access

This card can be used to adjust a user's access to the standard protocols that SmarterMail utilizes. For example, you can limit services like POP, IMAP and SMTP so that specific users are not able to connect their email accounts to external email clients. The following services can be managed for each user:

- **Webmail** - Enable this option to allow users to log into SmarterMail from the webmail interface.
- **POP** - Enable this option to allow the user to download mail to an email client using POP3.
- **IMAP** - Enable this option to allow the user to create a two-way email sync between SmarterMail and an email client using IMAP.
- **Incoming SMTP** - Enable this option to allow users to receive email from external domains.
- **Outgoing SMTP** - Enable this option to allow users to send email to external domains.
- **Chat (XMPP) (Enterprise Only)** - Enable this option to allow users to set up third-party chat clients like Adium, Pidgin and Windows Live Messenger for use with SmarterMail's live chat features. This setting is only available when using SmarterMail Enterprise.

## Aliases

This settings page is only available to Domain Administrators.

An email alias is essentially a forwarding email address that can be used to forward messages to a single address or multiple email addresses. Aliases are most commonly used for departments or groups of individuals, like a small team of people working on a project or task. For example, in a working environment with multiple email addresses, the office may want to make a central email address that

distributes messages to all personnel. The alias, `workplace@example.com`, can be made for messages to be sent and then distributed to all of the employees.

Note: Even though an alias acts as an email address, users cannot login to an alias like they do a standard email address; there is not a mailbox associated with the alias and no email is ever actually stored for the alias itself. Instead, emails are simply sent to the list of addresses provided for the alias and are stored in the mailboxes of the individual users.

To access the email aliases for the domain, log in as a Domain Administrator and click on the Domain Settings icon. Then click on Accounts in the navigation pane and navigate to the Aliases tab .

To create a new email alias, click New . Whether creating a new alias or editing an existing one, the following options will be available:

- Name - The name of the alias. This name will be used to create the email alias address. For example, if you want to use the email alias address "`info@example.com`", you'd simply use "info" for the Name. (You do NOT need to add the domain to the end of the name -- that's supplied automatically.)
- Display Name -- This is the friendly name used for the Alias. When used in conjunction with "Allow alias users to send from this alias", this is the display name that appears as the sender in the recipient's inbox.
- Email Addresses (one per line) - Type the full email address(es) of the user(s) who should receive emails sent to this alias.
- Internal use only - Enable this option to only allow emails to be received from addresses within the alias's domain.
- Include all domain users - Enable this option to include all domain users automatically in the alias. Note: This option does not override the email addresses listed in the Email Address box. If selected, all domain users will be included in addition to the users entered in the Email Addresses text box.
- Allow alias users to send from this alias - Enable this option to allow alias users (those users/accounts that are part of the alias) to manually change their Send From address to the alias email address on new emails and replies. When a user sends mail as an alias, the recipient will see the alias's Display Name as the email friendly from address. If the Display Name for the alias is blank, the user's Display Name shows.
- Show in Global Address List - Enable this option to display the alias in the Global Address List. Note: This feature is only available when using SmarterMail Enterprise.
- Show as a room in chat - Enable this option to allow the alias to appear as a room in chat. Enabling aliases for chat means that instant messages can be sent to the alias from within webmail as well as when using third-party chat clients.

- Use as domain catch-all - Enable this option to use the alias address as a catch-all account for the domain. A catch-all alias is an email address that will catch any incoming email sent to an invalid address on a domain. Instead of bouncing the message back to the sender, the message will be stored in the mailbox that is assigned as the catch-all account. Note: This option will only be visible if the System Administrator has enabled catch-all as a feature for the domain. In addition, only one email alias can be assigned as the domain catch-all at a time. Enabling a different alias as the catch-all will override any assignment already in place.

## A Note About Catch-All Aliases

A catch-all alias is simply that: an alias that catches all email sent to a domain that doesn't correspond to an actual account. Catch-all aliases can be useful as long as they are monitored and kept clear of unwanted email. However, due to the nature of email and the amount of spam that is sent every day, a catch-all can become a burden to email systems and to domain administrators. Therefore, it is suggested that they be used sparingly, or not at all if it can be avoided. Furthermore, it is important to never set an autoresponder on an email account that the catch-all forwards to, as it may result in backscatter, causing additional bandwidth usage and potentially causing your domain to be blacklisted.

## Administrators

This settings page is only available to Domain Administrators.

The Administrators section is where Domain Administrators can review all of the users on their domain who have Domain Administrator access and can make changes to domain-wide settings. To access the Administrators section, log into SmarterMail as a Domain Administrator and use the Menu icon to navigate to the Domain Settings section. Then click on Accounts in the navigation pane and navigate to the Administrators tab .

At a quick glance, you can see every user on the domain who has Domain Administrator access enabled for their account. You can determine the Primary Administrator (the user account chosen by the System Administrator as the Administrator for this domain), see the last date the administrators logged in and review their disk usage status. Using the New button or clicking on an administrator in this list will open the configuration options for that user account. For more information on the settings available, please refer to the Managing Users page.

It is also important to note that using the Delete button on this page does NOT remove the Domain Administrator access from the user account. Instead, deleting a user from this list will permanently delete the entire user account. To simply remove the Domain Administrator privileges, click on a user to open the account configuration options and and disable the setting for 'Domain Administrator.'

## EAS

This settings page is only available to Domain Administrators.

EAS is the industry standard for synchronizing mobile devices to SmarterMail, in addition to some desktop email clients. It uses direct push technology to sync email and collaboration items to variety of mobile devices, including smartphones and tablets, as well as Windows Mail, which ships as part of Windows 10.

If a Domain Administrator is given the ability to manage EAS mailboxes -- that is, add and remove EAS functionality for Accounts -- then this tab allows that Domain Administrator to do that. In addition, any mailbox with EAS added will appear here.

### Details

Once the tab loads, all Accounts that have EAS enabled are displayed. Domain Administrators can either Enable EAS for an Account, or, by selecting one or more accounts in the list, Disable EAS. Columns displayed include:

- Account - The Account username.
- Name - The friendly name of the Account.
- Last Login - The most recent login date for the account using the EAS protocol.

### Add EAS to an Account

To add EAS functionality to an account, click Enable . A small modal window will open and you simply need to add the Username for the account requiring EAS. Then click Save .

## MAPI/EWS

This settings page is only available to Domain Administrators.

MAPI is Microsoft's "Outlook protocol". That means it is the foundation by which Outlook on Windows does things like share tasks, calendars and email folders; set up meetings; create contact groups and much more. EWS is a similar protocol, but one that was developed specifically for integration with the Apple ecosystem. While other, non-Mac email clients have adopted EWS (e.g., eM Client), it primarily works with Apple Mail on the Mac.

What makes SmarterMail's use of MAPI different than its competitors is that SmarterMail has native, server-level integration of MAPI, just like Microsoft Exchange. Other products use separate pieces of software that are installed on client machines to "emulate" Exchange functionality. These "Outlook

Connectors" don't provide the full suite of Exchange features to Outlook. In addition, they're another piece of software that a client has to install, and that mail administrators or IT staff have to manage.

If a Domain Administrator is given the ability to manage MAPI/EWS mailboxes -- that is, add and remove MAPI/EWS functionality for Accounts -- then this tab allows that Domain Administrator to do that. In addition, any mailbox with MAPI/EWS added will appear here.

## Details

Once the tab loads, all Accounts that have MAPI/EWS enabled are displayed. Domain Administrators can either Enable MAPI/EWS for an Account, or, by selecting one or more accounts in the list, Disable MAPI/EWS. Columns displayed include:

- Account - The Account username.
- Name - The friendly name of the Account.
- Last Login - The most recent login date for the account using either protocol.

## Add MAPI/EWS to an Account

To add MAPI/EWS functionality to an account, click Enable . A small modal window will open and you simply need to add the Username for the account requiring either MAPI or EWS. Then click Save

NOTE: Both MAPI and EWS are enabled for the account. That means that a user can use either EWS OR MAPI, so they can connect clients that use either protocol, or connect multiple different clients across different computers.

## Mailing Lists

### Mailing Lists | Overview

This settings page is only available to domain administrators.
--

Mailing Lists are a great way to allow users to communicate with a number of different individuals via a single email address. For example, many companies use mailing lists to email newsletters, promotional offers, or information about product updates to subscribers. Unlike an Alias , a mailing list allows people to subscribe to, or unsubscribe from, email communications. In addition, mailing lists can be public or private, be replied to by all users or managed by a single list administrator and more. NOTE: SmarterMail can accommodate mailing lists of up to 75,000 subscribers. Anything greater than that should be managed by a third-party mailing list service provider such as Constant Contact or MailChimp.

Using a mailing list is as simple as sending a standard email: the allowed posters simply send an email to the list address, which takes the form of the list name appended to the domain name. For example, if you create a mailing list called "newsletter" you send a message to newsletter@example.com. If there are other requirements, such as a password, etc. those need to be taken into account as well.

By default, when a subscriber reads a mailing list message, the From field in the subscriber's inbox will display the email address of the individual that sent the mailing list message; the To field will display the list name or mailing list email address; and the Reply To field will display the mailing list email address or the email address of the individual that sent the message, depending on the list settings. Note: Domain administrators and mailing list moderators can customize the From, To, and Reply To fields by editing the mailing list settings.

To view the mailing lists for your domain, log into SmarterMail as a Domain Administrator and use the Menu icon to navigate to the Domain Settings section. Then click on Mailing Lists in the navigation pane. Whether creating a new mailing list or modifying an existing one, the following options will be available:

- Options - Configure the mailing list options and permissions
- Subscribers and Digest Subscribers - Add subscribers who will receive the standard mailing list postings or digest emails.
- Posters - Whitelist email addresses or domains who can post to the mailing list
- Banned Users - Prevent specific email addresses or domains from posting to the mailing list
- Messages - Configure the header and footer for postings as well as the replies sent to listserv commands
- Custom Fields - Customize list postings with subscriber custom fields

## **Variables**

Emails that are posted to a mailing list support the use of the following variables. These variables can be used in the body or subject line of emails that are sent to the mailing list subscribers and also in the footer, header and subscriber Messages . Though similar to Custom Fields in format, these variables need no additional configuration. Simply enter the variable below to display its associated information. Variables will always follow this format: #Variable#

- #UnsubscribeLink# - An unsubscribe variable is included to allow users to unsubscribe from the mailing list with a URL. Note: This URL can also be given friendly hyperlink text (rather than linking the URL) by modifying the Friendly Unsubscribe setting when configuring or modifying a mailing list. For more information, see Mailing List | Options .
- #Recipient# - The email address of the subscriber who was sent the message.
- #Sender# - The email address of the user sending the message.

- #DomainDateNow# - The current date (in shorthand) according to the domain's new user time zone defaults found in User Defaults. Ex: 07/13/2015.
- #DomainTimeNow# - The current time according to the domain's new user time zone defaults found in User Defaults. Displayed in 24-hour format.
- #DomainDateTimeNow# - The current date and time according to the domain's new user time zone defaults found in User Defaults. Displayed in shorthand and 24-hour format.
- #DomainDayNow# - The current date (date alone, without month and year) according to the domain's new user time zone defaults found in User Defaults. Ex: 13.
- #DomainMonthNow# - The current month (in numeric value) according to the domain's new user time zone defaults found in User Defaults. Ex: 07.
- #DomainYearNow# - The current year according to the domain's new user time zone defaults found in User Defaults. Ex: 2015.
- #DomainDayNameNow# - The current day of the week according to the domain's new user time zone defaults found in User Defaults. Ex: Monday.
- #DomainMonthNameNow# - The current month (by its name) according to the domain's new user time zone defaults found in User Defaults. Ex: July.
- #ModeratorDateNow# - The current date (in shorthand) according to the Moderator's time zone. Ex: 07/13/2015.
- #ModeratorTimeNow# - The current time according to the Moderator's time zone. Displayed in 24-hour format.
- #ModeratorDateTimeNow# - The current date and time according to the Moderator's time zone. Displayed in shorthand and 24-hour format.
- #ModeratorDayNow# - The current date (date alone, without month and year) according to the Moderator's time zone. Ex: 13.
- #ModeratorMonthNow# - The current month (in numeric value) according to the Moderator's time zone. Ex: 07.
- #ModeratorYearNow# - The current year according to the Moderator's time zone. Ex: 2015.
- #ModeratorDayNameNow# - The current day of the week according to the Moderator's time zone. Ex: Monday.
- #ModeratorMonthNameNow# - The current month (by its name) according to the Moderator's time zone. Ex: July.
- #ServerDateNow# - The current date (in shorthand) according to the server's system time zone. Ex: 07/13/2015.
- #ServerTimeNow# - The current time according to the server's system time zone. Displayed in 24-hour format.
- #ServerDateTimeNow# - The current date and time according to the server's system time zone. Displayed in shorthand and 24-hour format.

- #ServerDayNow# - The current date (date alone, without month and year) according to the server's system time zone. Ex: 13.
- #ServerMonthNow# - The current month (in numeric value) according to the server's system time zone. Ex: 07.
- #ServerYearNow# - The current year according to the server's system time zone. Ex: 2015.
- #ServerDayNameNow# - The current day of the week according to the server's system time zone. Ex: Monday.
- #ServerMonthNameNow# - The current month (by its name) according to the server's system time zone. Ex: July.

## Mailing Lists | Options

This settings page is only available to domain administrators.

To view the mailing lists for a specific domain, click the settings icon . Then expand the Domain Settings and Mailing Lists folders and click Mailing Lists in the navigation pane. To create a new mailing list, click the New button in the content pane toolbar. You can also edit an existing mailing list by selecting the desired mailing list and clicking the Edit button in the content pane toolbar.

### Options

- Name - Essentially, the "username" for the mailing list. SmarterMail will use the name to create the actual email address that will be associated with the mailing list.
- Status - New mailing lists default to a status of Enabled. To temporarily prevent postings to this list, change the status to Disabled.
- Moderator - The "owner" of the mailing list. This person will actively manage the mailing list, posts to the list and any replies. The moderator must be an active email user for the domain.
- Description - A brief summary of the mailing list.

### List Settings

- List To Address - The email address that will display in the To field when a subscriber receives a mailing list message. Setting this to List Address means that the email address associated with the list will display as the To: address when recipients receive the message.
- List From Address - The email address that will display in the From field when a subscriber receives a mailing list message. By default this is set to List Address.
- List Reply To Address - The email address that will display in the Reply To field when a subscriber receives a mailing list message. When a subscriber hits 'Reply' to the message, this address will receive the reply. If a subscriber hits 'Reply All' all list recipients will receive the reply. By default this is set to List Address
- Webmail URL - The URL for the SmarterMail login page. This setting can be used to override



the server's configured hostname for mailing list communications. Note: URLs should include the https:// prefix. For example: https://mail.example.com/

## Posting

- Password - To restrict people from sending emails to a mailing list, type a password in this field. Note: To send emails to a mailing list that is password protected, you must add the password to the beginning of the subject line of the email, enclosed by brackets and colons. For example, if "password" is entered into this field, the subject line of the email would need to begin with [:password:].
- Allowed Posters - An email that is sent to the mailing list (and therefore to its subscribers) is considered to be "posted." Use this field to specify who has access to post to the list. Note: Email addresses specified on the Posters tab will override this field.
- Anyone - Setting the list to "anyone" means that anyone can email the list, regardless of whether they are subscribed to the list or not. In turn, this sends an email to all members. Note: This setting can cause abuse if it is not closely monitored. Therefore, it is recommended to restrict the allowed posters to 'subscribers only', at the very least. For larger lists, allowing Moderator Only is a better idea and will cause less issues.
- Subscribers Only - Setting the list to "subscribers only" allows only the list subscribers, and only the list subscribers, to send and receive posts. The moderator will still be permitted to post. This can cause abuse issues as well if you have an active list, so using Subscribers Only should only be used for smaller lists or for digest mode only.
- Moderators Only - If the moderator is set as the post option, the moderator is the only one who can post to the list. This means that no one else, not even list subscribers, will be able to post.
- Max Message Size - The maximum number of KBs a message can be. If the message exceeds this size, it will not be posted. By default, the max message size is unlimited.
- Subject Prefix - The optional text that will appear in the subject line. SmarterTools recommends using a subject prefix for discussion lists to help subscribers easily filter through posts. For example, add a "List- " or "Discussion -" prefix so that users know that the message is posted to an email list. Recipients can then create filters to move those messages to a specific folder or manage them in some other way.

## Commands

- Enable SUBSCRIBE Command - Select this option to allow people to subscribe to the mailing list by emailing a listserv command to the command address. For more information, refer to Listserv Commands . Note: If this option is disabled, only list administrators can add new subscribers to the mailing list.
- Enable LIST Command - Select this option to allow people to receive a list of the mailing list

subscribers by emailing a listerv command to the command address. For more information, refer to Listserv Commands . Note: It is recommended that you leave this option disabled, as people or automated systems could use the user list for malicious purposes.

- Friendly Unsubscribe - The text entered here will be hyperlinked when using the Unsubscribe variable . If this field is left blank, the unsubscribe link will hyperlink the full URL.

## Throttling

Throttling limits the number of messages sent per hour and/or the amount of bandwidth used per hour to send messages. Domain Administrators can use this feature to ensure a mailing list does not send out massive amounts of email through out the day, thereby possibly getting the domain blacklisted.

- Outgoing Messages per Hour - The number of messages sent by the mailing list per hour. By default, the number of outgoing messages is 500.
- Outgoing Bandwidth per Hour - The total number of MBs sent by the mailing list per hour. By default, the outgoing bandwidth is 50MB.
- Throttling Action - When using either message or bandwidth throttling, administrators can select an action for SmarterMail to take once the particular throttling level is reached. Domain Administrators can elect to do nothing at all, or they can either Delay or Reject messages until the amount of mail being sent falls beneath the throttling limit that is set. By default, mailing lists are set to Delay messages once the threshold has been reached.

## Message Options

- Send Subscribe Email - Select this option to automatically send an email to new subscribers confirming their subscription to the list. Note: This is not an opt-in message, only a confirmation email.
- Send Unsubscribe Email - Select this option to automatically send an email response to unsubscribe requests.
- Enable Double Opt-In - Select this option to automatically send an email to new subscribers that requires them to confirm that they are subscribing to the list by clicking on an activation link. Using double opt-in is a good way to confirm subscriptions to the list and to help reduce abuse complaints.
- Disable List Error Replies - Select this option to prevent the system from automatically replying to incorrect listserv commands.

## Digest Settings

To reduce the number of emails mailing list subscribers receive, domain administrators can allow subscribers to sign up for digest mode or normal mode. Essentially, digest mode condenses all the messages sent to the list into a single email that is sent to subscribers on a monthly, biweekly, weekly,

daily, or other defined basis. This is especially useful for very active lists or lists with a larger number of subscribers.

- Enable digest mode - To enable digest mode, toggle the slider to the right. The remaining settings will become available.
- Subject - The subject line for the digest email.
- Trigger Type - The frequency of the digest emails: Daily, Weekly, Biweekly, Monthly or Manual. If Manual is selected, digest emails will only be sent when using the Send Digest button.
- Digest Format - The format (HTML, text, etc.) in which digest emails are sent.
- Disable non-text attachments in digest - Select this option to remove non-text attachments from the digest email.

## Mailing Lists | Subscribers and Digest Subscribers

This settings page is only available to Domain Administrators.

Mailing Lists are a great way to allow users to communicate with a number of different individuals via a single email address. For a complete understanding of how mailing lists work, please see [Mailing Lists Overview](#) .

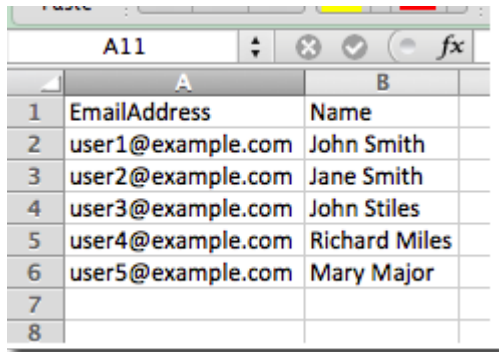
Individuals that sign up to receive messages from the mailing lists are called subscribers. To view a list of the mailing list subscribers, log into SmarterMail as a Domain Administrator and use the Menu icon to navigate to the Domain Settings section. Then click on Mailing Lists in the navigation pane and open a mailing list's configuration options.

Subscribers are categorized into two sections: the Subscribers tab stores the subscribers for standard mailing list postings and the Digest Subscribers tab stores subscribers for condensed digest emails.

### Adding Subscribers

To add a new subscriber, click on [New](#) . Email addresses can be added individually or in bulk, with one email address per line break. Note: When uploading email addresses from Gmail.com, be sure to enter the From address of the email account. If the address contains periods, they must be included in these fields.

To upload a list of subscribers to the mailing list, click on the [Actions \(...\)](#) button, then [Import CSV File](#) . Only .csv files can be uploaded. At a bare minimum, the .csv file must contain a column named "EmailAddress". Any additional columns in the .csv file will be added to the Custom Fields for the corresponding subscriber/email address. See example below:



	A	B
1	EmailAddress	Name
2	user1@example.com	John Smith
3	user2@example.com	Jane Smith
4	user3@example.com	John Stiles
5	user4@example.com	Richard Miles
6	user5@example.com	Mary Major
7		
8		

## Managing Subscribers

Once a subscriber has been added to the list, you can modify their custom field values, review the other mailing lists to which they are subscribed, see the history of bounce messages they've received and reviewed the history of messages they've received.

To download the list of subscribers as a text file, click on the Actions (...), then Export CSV File .

## Mailing Lists | Posters

This settings page is only available to Domain Administrators.

Mailing Lists are a great way to allow users to communicate with a number of different individuals via a single email address. For a complete understanding of how mailing lists work, please see Mailing Lists Overview .

Domain Administrators can restrict the posting privileges for a mailing list to Anyone, Subscribers Only or Moderators Only. In addition, they can use the Posters section to specify additional whitelisted posters.

To add additional posters to a mailing list, log into SmarterMail as a Domain Administrator and use the Menu icon to navigate to the Domain Settings section. Then click on Mailing Lists in the navigation pane and open a mailing list's configuration options. Then click on the Posters tab .

To add a new poster, click New . Enter the email address(es) of the people who can post messages to the mailing list.

### Uploading/Downloading Subscribers

In addition to manually adding new subscribers, it's possible to upload a text file that contains subscriber emails and any Custom Fields assigned to your subscribers. Text files should be in Comma Separated Value (.CSV) format.

Of course, since you can upload a subscriber list, you can also download one. This is especially convenient if the subscribers for one list -- or a subset of those subscribers -- is interested in another

list you start up. Downloading your list subscribers, then editing it if needed, makes it simple to add subscribers to a new list.

### **Banned Users**

It's also possible to keep a list of users who are banned from posting to your mailing list. You can import subscribers to this list as well as download that list to use in others you've created. For more information, see the section on Banned Users .

## **Mailing Lists | Banned Users**

This settings page is only available to Domain Administrators.

Mailing Lists are a great way to allow users to communicate with a number of different individuals via a single email address. For a complete understanding of how mailing lists work, please see Mailing Lists Overview .

Domain Administrators can restrict the posting privileges for a mailing list to Anyone, Subscribers Only or Moderators Only. In addition, they can use the Banned Users section to specify additional blacklisted posters.

To prevent users from posting to a mailing list, log into SmarterMail as a Domain Administrator and use the Menu icon to navigate to the Domain Settings section. Then click on Mailing Lists in the navigation pane and open a mailing list's configuration options. Click on the Banned Users tab .

To add a new banned user, click New . Enter the email address(es) of the people who cannot post messages to the mailing list.

## **Mailing Lists | Messages**

This settings page is only available to Domain Administrators.

Mailing Lists are a great way to allow users to communicate with a number of different individuals via a single email address. For a complete understanding of how mailing lists work, please see Mailing Lists Overview .

Domain Administrators can customize the system messages used for mailing lists. Some system messages, such as headers and footers, are viewable by list subscribers. Other messages are only viewable when emailing listserv commands to the mailing list username. For more information, please see Listserv Commands .

Note: Variables can be used in the footer, header and subscribe system messages. For more information on variables, see Mailing Lists Overview .

To edit a particular message, simply click on it from the list. When you do, a modal opens that will allow you to fully customize the message, as well as how that message is presented using a complete HTML editor. Once you've made your changes, be sure to save them.

- `digestfooter` - This is the footer that is displayed when digest emails are sent to digest list subscribers.
- `digestheader` - This is the header that is displayed when digest emails are sent to digests list subscribers.
- `digestseparator` - This is the character set (e.g., dashes) that will be used to separate messages within digest emails.
- `disabledlistemail` - This message is returned when a user attempts to post to a list that is no longer active.
- `doubleoptin` - This message is sent to subscribers to verify their subscription request when your mailing list utilized a double opt-in subscription model (recommended).
- `doubleopinreply` - This message is sent to subscribers notifying them that they were successfully subscribed to the list when the double opt-in subscription model is used.
- `faildsetdigestmode` - `LISTSERV COMMAND ONLY`. This message is returned when the list command attempts to set digest mode but digest mode is not enabled for the specific list.
- `failedtosetstandardmode` - `LISTSERV COMMAND ONLY`. This message is returned when the list command tries to set the mode for a subscriber that is not actually subscribed to the list.
- `footer` - This is the footer (information at the very bottom of the message) that is displayed on messages that are sent to list subscribers.
- `header` - This is the header (informatin at the very top of the message) that is displayed on messages that are sent to list subscribers.
- `help` - `LISTSERV COMMAND ONLY`. This can be used to return information about the list, such as its creation date, last updated date, etc. or any other information the domain or list owner wants returned.
- `helpmessage` - `LISTSERV COMMAND ONLY`. This is the default message that is returned when a listserv command is sent to the mailing list username but the command is not recognized. By default it returns information on how to properly format commands.
- `insufficientpostingpermissionemail` - This email is sent to posters that do not have the proper permission to post to the list. For example, this is returned to list subscribers who reply to the list but only moderators are allowed to post.
- `invalidlistpasswordemail` - When a list is password-protected, this message is returned when a person posting to the list provides the incorrect information.
- `listcommandresponse` - `LISTSERV COMMAND ONLY`. This returns a list of subscribers for a particular list. This requires the `LIST` command to be set.

- listoflists - LISTSERV COMMAND ONLY. This returns a list of the mailing lists for a particular domain. This requires the LIST command to be set.
- maxmessagesizeexceededemail - This is returned when a message posted to a list is larger than the maximum size set for messages.
- nolistcommand - LISTSERV COMMAND ONLY. This is returned when a particular list is set to not allow a list of subscribers to be returned. That is, the LIST command is not enabled for that list.
- privatelist - This is returned when anyone tries to subscribe to the list but the list doesn't allow for automatic subscriptions. Instead, the list owner will need to add the subscriber manually.
- setdigestmode - LISTSERV COMMAND ONLY. This is returned when the list command sets the digest mode for a subscriber.
- setstandardmode - LISTSERV COMMAND ONLY. This is returned when the list command sets the standard mode (one email per list post) for a subscriber.
- subscribe - This is sent to a list subscriber when they subscribe to a specific list.
- unsubscribeemail - This is sent to a user when they unsubscribe from a specific list.

## Mailing Lists | Custom Fields

This settings page is only available to Domain Administrators.

Mailing Lists are a great way to allow users to communicate with a number of different individuals via a single email address. For a complete understanding of how mailing lists work, please see [Mailing Lists Overview](#) .

Mailing lists can utilize Custom Fields in order to manage information about subscribers. When a custom field has been created, a value can be applied to a specific subscriber. Then, the custom field is used as a variable in a mailing list message in order to display that custom information about the subscriber. For example, if you'd like your messages to be sent out with the subscriber's first name in the message greeting (ex. "Hello John,"), you'd first create the Custom Field then add a value for each subscriber.

To create or manage Custom Fields, log into SmarterMail as a Domain Administrator and use the Menu icon to navigate to the Domain Settings section. Then click on Mailing Lists in the navigation pane. Open a mailing list's configuration options and click on the Custom Fields tab .

### Adding a New Subscriber Field

To add a new Subscriber Field, click the New button. A modal window will display the following options:

- Name - The name of the Subscriber Field. Note: The text entered here is used as the variable when sending subscriber fields in mailing list messages. For example, if you enter "First Name"

in this field, you will need to enter #First Name# as the variable in the mailing list message.

- **Default Value** - Enter the text that should be automatically entered for current and new subscribers. Once the field is created, subscribers can be individually modified to change the value. Note: If a default value is not included, and the subscriber does not have their field configured, the variable will be removed from the message, leaving a blank space in its location.

## Using Custom Fields in Messages

A Custom Field can be used in mailing list messages as a type of custom variable. To enter Custom Fields as variables, the name of the field must be enclosed with a #. For example, if a Subscriber Field was created for "Customer Name", you would enter #Customer Name# in your message.

## Listserv commands

Listserv commands allow you to control the list through commands sent in email messages to the listserv command address. By default, the command address for a domain is "STServ@example.com", where example is the name of your domain. However, your system administrator may change this command address.

To send a command, compose an email to the command address with the command in the body of the message. The subject of the message is ignored.

### Available Commands

Note: Any references to listname should be replaced with the list you are trying to use.

Help listname - Replies to the email with the contents of the Help system message for that list.

List - Replies to the email with a list of all available lists.

List listname - Replies to the email with a list of all subscribers for a particular list. Note: This command can be disabled by the domain administrator.

Subscribe listname - Adds your email address to the subscribers list of the mailing list. Note: This command can be disabled by the domain administrator.

Unsubscribe listname - Removes your email address from the subscribers list for the mailing list referenced by listname.

Set mode digest listname - Sets your email address to receive emails in digest mode, which will send all messages for the list combined into one email at regular intervals.

Set mode standard listname - Sets your email address to receive emails in standard mode (the default), which will send messages one at a time to your email account.



## Domain Events

This settings page is only available to Domain Administrators.

The Event system in SmarterMail is an incredibly powerful and flexible tool that allows Domain Administrators to automatically perform actions based on specific criteria and remain up-to-date with what is going on with the SmarterMail server and user accounts. SmarterMail can detect events as they occur, generate messages for those events, and deliver the messages to users that need the information. For example, Domain Administrators can automatically add an additional recipient on messages sent or received by users on the or receive notifications when a task is due or their domain disk space has met a certain threshold.

To create or view events for the domain, log into SmarterMail as a Domain Administrator and use the Menu icon to navigate to the Domain Settings section. Then click on Events in the navigation pane. To create a new event, click New . The following options will be available:

### General

- Event Name - The friendly name of the event.
- Event Status - New events default to a status of Enabled. However, to temporarily stop an event from triggering, you can change the status to Disabled.
- Event Category - The feature to which the event pertains: User, Mailing List, Alias, Throttling, Email or Collaboration.
- Event Type - The occurrence that triggers the event. Each category has several specific event types that can trigger the action.

### Conditions

Each event type has its own corresponding conditions. The global conditions that are seen across all event types are listed below.

- Time of Day - The time frame during which the event occurs.
- Day of Week - The day(s) of the week during which the event occurs.

### Actions

Each event type has its own corresponding actions. The global actions that are seen across all event types are listed below.

- Send a notification - This option will send a notification to the Notifications window. It can also send a popup browser notification and an email.
- Send an email - This option will send an email to the specified address.

## Folder Auto-clean

This settings page is only available to domain administrators.

Setting up auto-clean rules for email folders is a simple, yet effective, way to limit how much of the domain's disk space is taken up by users' Junk Email, Sent Items, and Deleted Items folders. By placing limits on the size of these folders, or by automatically deleting mail older than X number of days, you can help ensure that your domain disk space does not fill up unnecessarily. In addition, if you want to set a size limit on a folder for users, their messages are deleted in the order that they were received so that older messages get deleted first.

To access the folder auto-clean settings for a domain, log into SmarterMail as a Domain Administrator and click on the Settings icon . Then, in the Domain Settings section, click on Folder Auto-Clean . The following options will be available:

Note: Depending on the policies the System Administrator has established, you may or may not be able to adjust the auto-clean settings for a domain.

### Options

- Override auto-clean settings for this domain - Toggle the slider to the right to override the settings established by the System Administrator, allowing you to create your own rules. Any changes you make will not be affected if the administrator changes their policy, unless they disable domain overrides.
- Enable users to override auto-clean settings - Toggle the slider to the right to allow users to override the domain policy and create their own auto-clean rules.

### Rules

If you are using the default auto-clean settings set up by your administrator, they will appear on this tab. If you override the auto-clean rules, this section will allow you to view/create your personal auto-clean policy.

To create a new auto-clean rule, click on New Rule .

### Auto-clean by Size

These options will be visible if you set up the rule by folder Size :

- Folder - This dropdown will show the default email folders that every user has: Deleted Items, Junk Email and Sent Items.
- Type - This allows you to create rules based on folder Size or by Age.
- When size is great than (MB) - The size the folder needs to reach BEFORE the auto-clean rule

will run.

- Reduce to (MB) - The size the folder will be reduced to once the auto-clean rule finishes.

### **Auto-clean by Age**

These options will be visible if you set up the rule by folder Age :

- Folder - This dropdown will show the default email folders that every user has: Deleted Items, Junk Email and Sent Items.
- Type - This allows you to create rules based on folder Size or by Age.
- Days - The number of days old an email can be before it is automatically deleted from the folder.

## **Sharing**

This settings page is only available to Domain Administrators.

In the Sharing section, Domain Administrators have the ability to create a few resources for all users of the domain:

- Domain Calendars - Domain Calendars can be used for company-wide events such as company holidays, payroll or PTO schedules. Domain calendars show up as "subscribed" calendars for users and can be displayed/hidden in a user's Calendars area just like other calendars.
- Conference Rooms - Conference Rooms are used in conjunction with meetings/events that are created. When creating a new event in a calendar, a shared conference room can be selected for the location of that meeting/discussion/event.
- User Groups - User Groups are used to give permissions to specific subsets of users on the domain to access shared resources. For example, if a business wanted to make it easy for members of its Sales Department to share their calendars with other team members, the Domain Administrator would create a User Group for all the Sales Department employees.

The Sharing page is separated into 2 different cards:

### **Sharing**

The Sharing card is where Domain Administrators create shared calendars and/or conference rooms. When clicking the New Shared Resource button on the Sharing card, the Domain Administrator is presented with a modal window that contains the following information to be filled out:

- Name - The name of the resource. It's always a best practice to name the shared resource something that will be easily identified by users. For example, if the resource will be a conference room name the resource the same as the room designation. For example, South

Conference Room or Main Hall. For calendars, something like "PTO Calender" or simlilar.

- Type - The type of resource being added: Calendar or Conference Room.
- Users - Here, you'll enter individual users that will receive the share. Enter only the username of the account. (For example, for user account, "jdoe@example.com", you would enter "jdoe".) Once you begin typing the username, you'll notice a second line appears below where you're typing. This allows you to share the resource with any number of individual users.
- User Groups - User Groups can be selected to give permissions to specific subsets of users on the domain. By default, two groups are always available: Everyone and Admins. If other User Groups have been created, they'll appear in this dropdown list.
- Access Permissions - Next to the usernames you've added, or the User Groups selected, you'll want to set the type of access for each:
  - None - This option can act as a negator for permission settings. For example, if you provide access to the Admin user group, you can omit one or multiple of those Admins by entering their name in the Users field and selecting None for their access.
  - Read-Only - This option allows Users or User Groups to see the shared data but they do not have the ability to edit the item.
  - Full Control - This option allows Users or User Groups to fully edit the shared data.

## User Groups

To create a User Group, click the New User Group button on the User Groups card. To edit an existing user group, simply click on the corresponding group name. A modal window will pop up with the following options:

- Name - The friendly name of the user group. For example, "Sales Team".
- User - The individual Users you want to add to the user group. Start typing the username and it will be displayed. Simply select it to add it to the User Group. Note: Alisases can not be added to a User Group.

Regardless of whether you're creating shared Calendars or Conference Rooms, or setting up User Groups, be sure to save your information after you've finished your edits.

## Signatures

This settings page is only available to domain Administrators.

An email signature is a block of text automatically appended at the bottom of an email message. Signatures may contain the sender's name, address, phone number, disclaimer, or other contact information.

Businesses that want to ensure a consistent company appearance may require employees to follow a specific signature format. Instead of allowing the users to define their own signatures, the domain administrator can create a domain-wide signature that all employees must use. Depending on the signature configurations set up by the domain administrator, users may or may not be able to override the default signature.

To access the domain signature settings, log into SmarterMail as a Domain Administrator and use the Menu icon to navigate to the Domain Settings section. Then click on Signatures in the navigation pane.

## Signatures

To create a new signature, click on New . To edit an existing signature, click on its Signatures card.

Whether you add or edit a signature, the signature creation window appears. Here, you can create signatures using a full HTML editor that allows domain administrators to add in stylized text, links to websites, images and even icons linked to social media outlets. In addition, the signature can incorporate variables so that a generic template can be created for all users of the domain. The available variables are listed by clicking the Custom Variables dropdown in the text box's toolbar, which looks like a settings cog. (If the cog icon doesn't appear in the toolbar, you may need to click the + sign to "Show More" tools.)

## Mapped Field

Use this card to assign a domain-wide signature for all users on your domain and any email or domain aliases that have been configured. To allow users to create and use their own signatures, toggle the slider to the right to Enable users to override . Note: If this setting is disabled, users must use the domain-wide signature. To assign a signature to your domain, select the signature from the dropdown menu and enable the mapping by moving the slider to the right.

## Message Archive Search

Setting up Archiving for All Domains only, and not including per-domain rules, limits the ability to search the Archive to system administrators only. Message Archiving is only available in SmarterMail Enterprise.

Message archiving is a method of storing all email and live chat traffic for a domain -- either incoming messages, outgoing messages or both -- in a separate location on the mail server. Typically, this feature is used for companies that need mail servers in compliance with the Sarbanes-Oxley Act of 2002 or other regulatory compliance.

It is important to note that message archive search is available to domain administrators only when rules are set up individually for their specific domains. If archiving is set up for "all domains" on a server, then only the system administrator will be able to search the message archive. Therefore, if a domain admin needs access to the email archive for the domain "example.com", then a Message Archiving rule specifically for example.com needs to be set by the system admin.

System administrators can perform a message archive search by going to the Settings area and clicking on the Manage icon, then selecting Message Archive Search . System administrators can search for a message by domain, date range, the sender's address, the recipient's address, or the subject.

When message archiving is set up for a specific domain, that domain's administrator can find a Message Archive Search option by clicking on the Settings icon . Domain administrators can search for a message by date range, the sender's address, the recipient's address, or the subject.

For more information on archiving, see Message Archiving .

## Domain Spam Filtering

This settings page is only available to Domain Administrators.

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 actions for this domain - Toggle the slider to the right to customize the spam filtering Actions for your domain. If this option is disabled, the system's default spam filtering policy will be displayed.

- Users can override domain actions - Toggle this to the right 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 My Contacts list is considered a trusted sender and bypasses spam filtering.

Note: If SPF and DKIM spam checks are enabled, SmarterMail will run those checks on ALL emails, including those from trusted senders. 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 the SPF and DKIM weights on a message from a trusted sender meet the Low, Medium or High spam filtering threshold, the corresponding spam filtering action (Move to Junk Email Folder, Delete Message, Add Text to Subject) will be performed on that email, despite the email coming from a trusted sender.

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

## Domain Content Filtering

This settings page is only available to Domain Administrators.

Content Filtering at the domain level is a great way to perform actions that meet specific criteria for all users on the domain. For example, you can use content filters to delete messages with certain attachments (e.g., attachments with a `.exe` extension), forward messages from a specific email address to another account, or even alter the subject of specific types of email. Content filters are most commonly used to organize email by moving messages to specific folders. However, content filtering is extremely flexible and allows you to filter messages for users the way you want to.

Note: The evaluation of domain content filters happens before the evaluation of account-specific content filters.

To access the content filtering settings for the domain, log into SmarterMail as a Domain Administrator and click on the Settings icon . Then click on Content Filtering .

To add a new content filter, click New . The following options will be available:

## General

- Name - The friendly name chosen to describe the rule.
- Order - Content filters are executed in the order in which they appear. In addition, when a content filter gets triggered and performs an action on a message, no other content filtering is performed on that message. In this field, enter the position number for your filter. If a filter already exists in the position number that was entered, the filter currently being edited will override that position and existing filters will adjust accordingly.
- Match Type - Because multiple conditions can be configured per content filter, SmarterMail provides the option to require ALL conditions to be met or only ONE of the conditions to be met in order for the rule's action to be triggered. Select the appropriate option from this list.
- Enable wildcards in search strings (\* and ?) - Toggle the slider to the right to enable wildcard functionality. Wildcards can be used to replace a specific word, phrase or character, where a question mark (?) represents a single character and an asterisk (\*) represents any text. For example, if you wanted to block sales01@domain.com, sales02@domain.com and sales03@domain.com, you could enter sales??@domain.com . If you wanted to block all sales addresses, you could enter sales\* instead.

## Conditions

Click on New Condition to specify the criteria that triggers the rule's action(s). For each condition selected, you will be able to add specifications and enter any necessary details, as required. For example, if you choose to filter on 'From Address', you can enter one or multiple email addresses. If you choose to filter on 'Contains specific words or phrases', you can enter the specific text and choose to look for that text in an email's subject, message body, header, etc.

On many conditions, you also have the ability to reverse the logic of the criteria item by changing the Comparison selection. For example, imagine you only want to accept email from specific domains. You would choose the 'From specific domains' condition and set the Comparison field to 'Does Not Match'. Any messages sent from domains that do not match what you've entered in the text box can be deleted.



Note: If you select a condition that requires a value to be entered, and the field is left blank, SmarterMail will ignore this rule.

The following conditions are available, separated by Condition Type:

#### From Address

- From specific addresses
- From specific domains
- From trusted senders

#### Contains Specific Words or Phrases

- Subject
- Body
- Subject or Body
- From Address
- To Address
- Email header
- Anywhere in message

#### To Address

- To specific addresses
- To specific domains
- Only to me
- My address in to field
- My address not in to field
- My address in to or cc field

#### Attachments

- Has any attachment
- Specific filenames
- Specific extensions
- Over specific size

#### Other

- Flagged as high priority
- Flagged as normal priority
- Flagged as low priority

- Message automated (no return address)
- Sender authenticated
- Message over size
- Message under size
- Received in date range
- Sent through a specific server (by IP address)
- Spam probability

## Actions

Click on New Action to specify what should occur when an email triggers the content filter condition(s). Note: If you select an action that requires a value to be entered, and the field is left blank, SmarterMail will ignore this rule.

The following actions are available:

- Delete message - Deletes the message so that it will never arrive at your Inbox. Note: Messages deleted through content filtering cannot be recovered.
- Reroute message - Forwards the message to another email address. Unlike 'Forward message', this option will not store a copy of the email in your own account.
- Bounce message - Sends a message back to the sender of the email saying that the message was bounced. Note that the message is still delivered to you unless you choose to delete it as well. Note: If the system administrator has disabled bouncing, this option will function the same as the delete action.
- Move message - Delivers the incoming message to the folder you choose from the dropdown list. Note: If you later delete that folder and leave the content filter active, the filter will automatically create the folder when the action is triggered.
- Add Header - Adds an email header within the incoming message, which can be useful when performing additional filtering through Outlook or another email clients. Headers should be formatted like "X-someheadername: value"
- Add text to subject - Appends a prefix to the subject line of the email. This is useful for categorizing emails as the subject line will be altered to include the text you specify in the text box.
- Forward message - Forwards a copy of the message to another email address and leaves a copy of the message in your account as well.
- Mark as read - Automatically marks the messages as read, which means it will not show up in your inbox, or any other folder, as unread.
- Set Priority - Automatically elevates the priority of a message. For example, if you create a content filter that flags a message from a VIP, you may want to set the priority of the message

to High as well to denote its importance.

- Flag message - Automatically flags the message for follow-up. This makes it easy to find messages that have been acted upon by your content filter.

## Chat History Search

This settings page is only available to domain administrators.

A major advantage of SmarterMail is that it stores all chats, regardless of whether the chats occur within the webmail interface, using a third-party client or a combination of both. Domain administrators have the ability to perform custom searches by date range, by the users involved in the chat conversations, by specific keywords or phrases used during a chat or a combination of all of these variables. The results can then be downloaded to a desktop or laptop (search results cannot be downloaded to a mobile device due to storage limitations) and reviewed as needed. Note: Chat history search is configured by the system administrator. For more information, see the Features area of the All Domains page of SmarterMail Help.

The options available when performing a chat history search are as follows:

- Date Range - The date range you want to use for your search. You can either type in the date or click on the calendar icon and use SmarterMail's calendar control to select your start and end date.
- User 1 - The username or email address of the person who originated the chat.
- User 2 - The username or email address of the person who was the recipient of the chat.
- Text - Any word or phrase that was used during a chat. For example, "2012 sales numbers" or "product ID 33489".

## Chat Clients and Encryption

Many XMPP chat clients out these days encrypt the chats that happen between 2 or more users. Unfortunately, this encrypted chat traffic occurs between the client and SmarterMail itself. (Or fortunately, depending on where you fall on the topic of personal encryption.) Therefore, while SmarterMail will see chats occur, it doesn't have the ability to capture and archive the unencrypted text. Therefore, some results returned when you do a Chat History search will appear garbled or show generic text, like this from the XMPP client Gajim:

[This is part of an encrypted session. If you see this message, something went wrong.] ([This is part of an encrypted session. If you see this message, something went wrong.])