Domain Settings

Help Documentation

Domain Settings

Accounts

Users

This settings page is only available to Domain Administrators.

The Users section is where a Domain Administator can manage the user accounts on their domain. This document explains the actions that can be taken on user accounts, incuding the ability to import users, improve the search functionality for a user by reindexing their account, enabling or disabling the MAPI/EWS and/or EAS synchronization add-ons, and more.

More information is availble for adding new users as well as Managing Users .

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:

- Adding new users
- Import from CSV - Import new user accounts from a CSV file.
- Import from LDAP - When enabled, this allows a Domain Administrator to import new user accounts from Microsoft's Active Directory.
- Export All to CSV - Export a CSV file of all users on the domain.
- Reindex - Reindexes users/accounts to 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.
- Enable EAS - This will give the selected User(s) the ability to set up Exchange accounts on mobile email clients, contacts and calendar apps, etc.
- Disable EAS - This removes the EAS capabilities for the account(s).
- Enable MAPI/EWS - This will give the selected User(s) the ability to set up Exchange accounts in Microsoft Outlook for Windows, Outlook for Mac, Apple Mail and will sync the account to eM Client.
- Disable MAPI/EWS - This removes the MAPI/EWS capabilities for the account(s).

Users

The Users tab lists all users created on the domain, as well as some basic information about each user. This information includes:

- Account - The username, or name that appears to the left of the "@" symbol in the email address.
- Name - The Display Name set for the User.
- Type - The "Role" of the User: User, Domain Admin or Primary Admin.
- EAS - Whether or not the EAS add-on is enabled for the User. If there is a checkmark here, this add-on is enabled.
- MAPI/EWS - Whether or not the MAPI/EWS add-on is enabled for the User. If there is a checkmark here, this add-on is enabled.
- Enabled - Whether the User is allowed to send/receive email (Enabled) or not.
- Last Login - The last date and time the User logged in to webmail.
- Disk Usage - The total amount of disk space being used versus their limit.

In addition, each User has a series of actions that can be performed. This are available by clicking on the Actions (...) button and include:

Import 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 only available to Domain Administrators using SmarterMail Enterprise.

The Lightweight Directory Access Protocol (LDAP) is, as the name implies, a lightweight client-server protocol that email servers, software and network appliances can use to connect to, and look up information from, a directory service. For example, LDAP can be used to look up information from Microsoft Active Directory.

For its part, SmarterMail acts as an LDAP client. That means LDAP can be used to integrate SmarterMail with Microsoft Active Directory for lookup and authentication services. The LDAP integration between SmarterMail and AD via LDAP is, therefore, one-way: SmarterMail can look up information within Active Directory but it can't send information TO Active Directory. So, when Active Directory is used as an authentication method for users, if the user changes their password, display name or other information in SmarterMail, that change is NOT synced back to Active Directory. However, if that same information is changed in AD, it will sync back to SmarterMail.

Follow these steps to import new users using LDAP:

- Log into SmarterMail as the domain administrator.
- Click on the Domain Settings icon.
- When the domain settings load, click on Accounts in the navigation pane. All existing accounts will load in the content pane.
- Click the Actions (...) button.
- From the dropdown menu, click Import from LDAP . A modal will appear.
- Input the location of your active directory users via the LDAP binding string. An example LDAP string might look like this:

```
LDAP://testdomain.local/CN=Users,OU=Company,DC=testdomain,DC=local
• If you want to use the LDAP email address as the username for the
imported accounts, enable it.
• Click List Users .
• Select the users you wish to import into the domain. NOTE: If any users,
aliases or mailing lists already exist in SmarterMail they will not show up
in the LDAP list.
• Click Import to begin the import process.
```

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 to 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.

Reindex

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.

Enable/Disable EAS

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 these options will be available once a account, or several accounts, are selected.

Enable/Disable MAPI/EWS

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 Outlook for Mac and Apple Mail.

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 these options will be available once a account, or several accounts, are selected.

Managing Users

This settings page is only available to System Administrators and Domain Administrators.

The Users section is where System and Domain Administators can add, view and modify the user accounts on a domain, where each account represents a person's actual mailbox and email address (ex: jdoe@example.com). 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.

Jump to:

- Account
- Service Access
- User
- Webmail
- Forwarding
- User Groups
- Throttling

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 Diretory 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 Diretory 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 - Enable this setting 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.

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.

• Inbound SMTP - Enable this option to allow users to receive email from external domains.

• Outbound SMTP - Enable this option to allow users to send email to external domains.

• Chat (XMPP) (Enterprise Only) - Enable this option to activate SmarterMail's included Group Chat feature for Users.

• 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.

• EAS (Enterprise Only) - This will give the users the ability to set up Exchange accounts on mobile email clients, contacts and calendar apps, etc.

• MAPI/EWS (Enterprise Only) - This will give the User the ability to set up Exchange accounts in Microsoft Outlook for Windows, Outlook for Mac, Apple Mail and will sync the account to eM Client.

User

• Language - The language selected for Users in SmarterMail is EXTREMELY important. That's because it's much more than simply what is seen in the webmail client when that User logs in. SmarterMail's language selection is the basis for everything: the things seen in the webmail interface as well as what's returned to an email client when connecting using Outlook, eM Client, iOS Mail and more. That includes things like settings labels, folder names, calendars and calendar appointment, contact groups, email message content, log files and essentially everything within SmarterMail. Therefore, it is extremely critical select the proper language for a User. For more information, see Languages, Protocols and Clients

• Changing Language Settings : When a user tries to update their language, SmarterMail checks for potential conflicts prior to changing the language. For example, if a user is set to English and they have a folder named "Bandeja de entrada", if they try to change their language to Spanish, the change will not be saved and they will see a warning letting them know that the language wasn't updated to prevent an email folder name conflict. This is because "Bandeja de entrada" is the Spanish name for Inbox used in the default Spanish language translation file. If the change was saved, there would be 2 folders with the same name, which would cause issues.

• 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. While it's possible to set the Reply-to address or a user, that user can change the Reply-to when composing a message or reply in an email client, such as Microsoft Outlook. Should they do this, that address will take precedence over what's set in the user's settings.

• 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.

Webmail

• Delete Email Action - To specify the action performed on deleted messages, select the appropriate action from the list. NOTE: This action only affects messages. If folders are deleted, the folder and its contents will always go to the Deleted Items folder.

• Move to Deleted Items folder - Deleted items will appear in the deleted items folder, which will need to be regularly emptied.

• Permanently Delete - 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.

• 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.

• Font Size - Specify the default font size for emails by selecting an option from the list.

• 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.

• Use To: address for replies - When enabled, replying to a message via webmail will use that email's To: field as the Send From address of a reply, regardless of whether the message was sent to a specific SmarterMail email address or a domain alias, email alias, SMTP account, disposable address or plus address. For example, if an email is sent an alias, replies to that email via webmail will automatically use the email alias address of the Alias member as the Send From address. (This setting does not prevent a user from manually changing the Send From address when composing a message.)

• 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 receipient(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.

• Mark messages downloaded by POP as read - Select this option to mark all messages that are downloaded via a POP3 connection as read.

• Show images from external websites - 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. NOTE: These settings only affect webmail. If it's been disabled for your domain, forwarding may still occur when using Events and/or content filters, or when using an email client.

• Forward all email to another address - 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

User Groups are used to give a specific subset of users on the domain permission 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.

If any User Groups have been created, they'll be listed here and can be set to On or Off for specific users.

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.

- Outbound 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 thorttling 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.
- Outbound 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 thorttling 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.

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. Click on Accounts in the navigation pane, then 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 delivered to accounts that are hosted within the same SmarterMail server.

• 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.

• Alias can be used as from address in webmail - Enable this option to allow alias users (those users/accounts that are part of the alias) to manually change their 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 (Enterprise Only) - Enable this option to allow the alias to appear as a room in Group Chat. Enabling aliases for chat means that instant messages can be sent to the alias, and everyone in that 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.

General Domain Settings

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

Below are the options available for managing and configuring a domain. To access the domain settings, log into SmarterMail as a Domain Administrator and click the Domain Settings icon. 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
- Folder Auto-Clean - Add settings that affect the auto-clean rules set for the domain on default folders.
- Team Workspace Video / WebRTC - Set up alternate STUN/TURN server(s) for Team Workspaces
- Custom Help - Add a custom Help link to the Logout menu
- Webmail Login - Customize the login page for your 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
- 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.

- Two-Step Authentication - Two-Step Authentication is a method of providing a second way to verify 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 Two-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 Two-Step Authentication for their users - With Enable, users can choose whether to implement Two-Step for their accounts whereas with Force, users MUST use Two-Step for their accounts.
- 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.

• Allow users to opt out of Global Address List - The Global Address List (GAL) is basically a listing of all users who have accounts for your particular email domain. However, not all accounts would necessarily need to be listed in the GAL. For example, generic addresses like info@ or support@ may not need to be listed as they're used for specific purposes (e.g., support@ being imported into a ticketing system.)

Folder Auto-Clean

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' Inbox, 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.

• Allow users to override auto-clean settings - Enable this setting to allow users to override the domain policy and create their own auto-clean rules.
• Override auto-clean settings - Enable this setting 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 System Administrator changes their policy, unless they disable domain overrides.

If "Override auto-clean settings" is off, the auto-clean rules created by the System Administrator will be displayed at the bottom of this card. (If no rules were created by the System Administrator, a note saying such will be displayed.

However, if "Override auto-clean settings is turned on, you're presented with a New rule button that will allow you to create your own rule(s) for domain users. Auto-clean rules can be created for any default mail folder, and can be created based on a message's age, the length of time a message has been in a folder, or a particular folder's size.

Size of Folder vs. Age Rules

It's possible to either set an auto-clean rule based on the size of a folder, or the age of a message (or messages) within a folder. Size-based auto-clean rules are run whenever an action is performed on a particular folder. For example, moving a message into the folder. Once that action occurs, the auto-clean rule is run, and it runs each time an action is performed. Age-based rules, however, run once per day, on the FIRST folder action for that day. For example, deleting an email first thing in the morning. When you delete an email, it's moved to the Deleted Items folder, which is a folder action. At that point, if there's an age-based auto-clean rule for the Deleted Items folder, the rule is run, and then is silent until an action is performed on the next day.

When using a folder's size, it's possible to set upper and lower limits for the space used for the folder. For example, you can create an auto-clean rule so that when a folder gets larger than 50MB in size, the rule automatically deletes messages to reduce the folder's size to 5MB. When freeing up space, the total size of each message is used, which includes any message attachments.

When using Age as a guideline, there are two types of age: Message Age and Age in the Folder.

- Message Date: This is based on the initial receipt date of the message. So if you received a message on January 1st, and the number of days is set to 14, on January 15 the message is automatically deleted.
- Time in Folder: This is based on when a message is actually moved to the folder that has the auto-clean rule configured. The age of the message itself is not used. That means, if the Age in Folder is set to 14 days, it doesn't matter when the message was received. Instead, the message is deleted 14 days after it's been moved into the folder.

Team Workspace Video / WebRTC

This feature is only available when using SmarterMail Enterprise.

SmarterMail's Team Workspaces uses Web RealTime Communication (WebRTC) for peer-to-peer audio and video chat. WebRTC is an open standard that uses plugin-free APIs to connect web browsers (WebRTC compatible web browsers, that is) for the transfer of voice, video and general data.

For most people, using Team Workspaces as it's implemented in SmarterMail is perfectly fine. It uses a default STUN service to assist with the transfer of the data from user-to-user. However, larger or more complex networks may have restictions that limit, if not fully deny, a Workspace's WebRTC requests. For example, the use of firewalls or the use of Network Address Translation (NAT) on their routers. In these cases, using a standalone STUN or TURN server may be necessary.

To add a separate STUN/TURN server for a domain, simply click the New STUN/TURN Server button. Once you do so, you'll be presented with the following:

- Type - Whether you're adding a STUN or TURN server.
- URI Paths - These are the paths to the STUN or TURN server you're setting up.
- Username - When setting up a TURN server, this is the username used to connect to that server.
- CREDENTIAL - When setting up a TURN server, this is the "password" for connecting to that server.

While STUN servers are very inexpensive for a company to operate (they're basically a glorified "What's My IP" service), TURN servers can consume a significant amount of bandwidth. Therefore, a TURN server may require you to use a paid service to host it for you. Companies like Twilio or Xirsys

offer such services. If you want to host your own TURN server, one of the most popular options is Coturn , a Linux-based TURN server. Note: These are simply examples, and are NOT endorsements of any product or service mentioned.

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".

Webmail Login

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.

• Logo Image - 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 - This is the language to use on the SmarterMail login page if the user's browser language isn't supported by SmarterMail. For example, if French is set as the Login Page Language, and a user's browser language is set to Galician, which is not currently supported by SmarterMail, when the user goes to log in to SmarterMail, the login page will appear in French. However, the user's Getting Started wizard, which appears on a user's first log in to SmarterMail, allows the user to change their language preference so that subsequent log ins will appear in the language they choose.

• Enable custom login page HTML - Enable this setting 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.

• Preview Login - This button will open a small preview in a pop-up window of the login customizations you've made without you having to save your changes and test it yourself.

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 enable the ability 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 - Enable this setting to customize the footer for your domain.
- Enable footer for all messages - When enabled, all messages -- new messages as well as replies and forwards -- will have the footer appended. When disabled, only outgoing messages 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, enable the setting. 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.

- Key Size - The length of encryption key to use. 2048 is recommended.
- Max message size to sign (MB) - This is the largest message size you want to sign using DKIM. DKIM generates a "hash" on the email up to the size limit. Generating the "hash" could be an expensive operation, especially if the domain sends large messages all the time. Limiting it means not having to process the whole message -- It would only grab the bytes up to the size
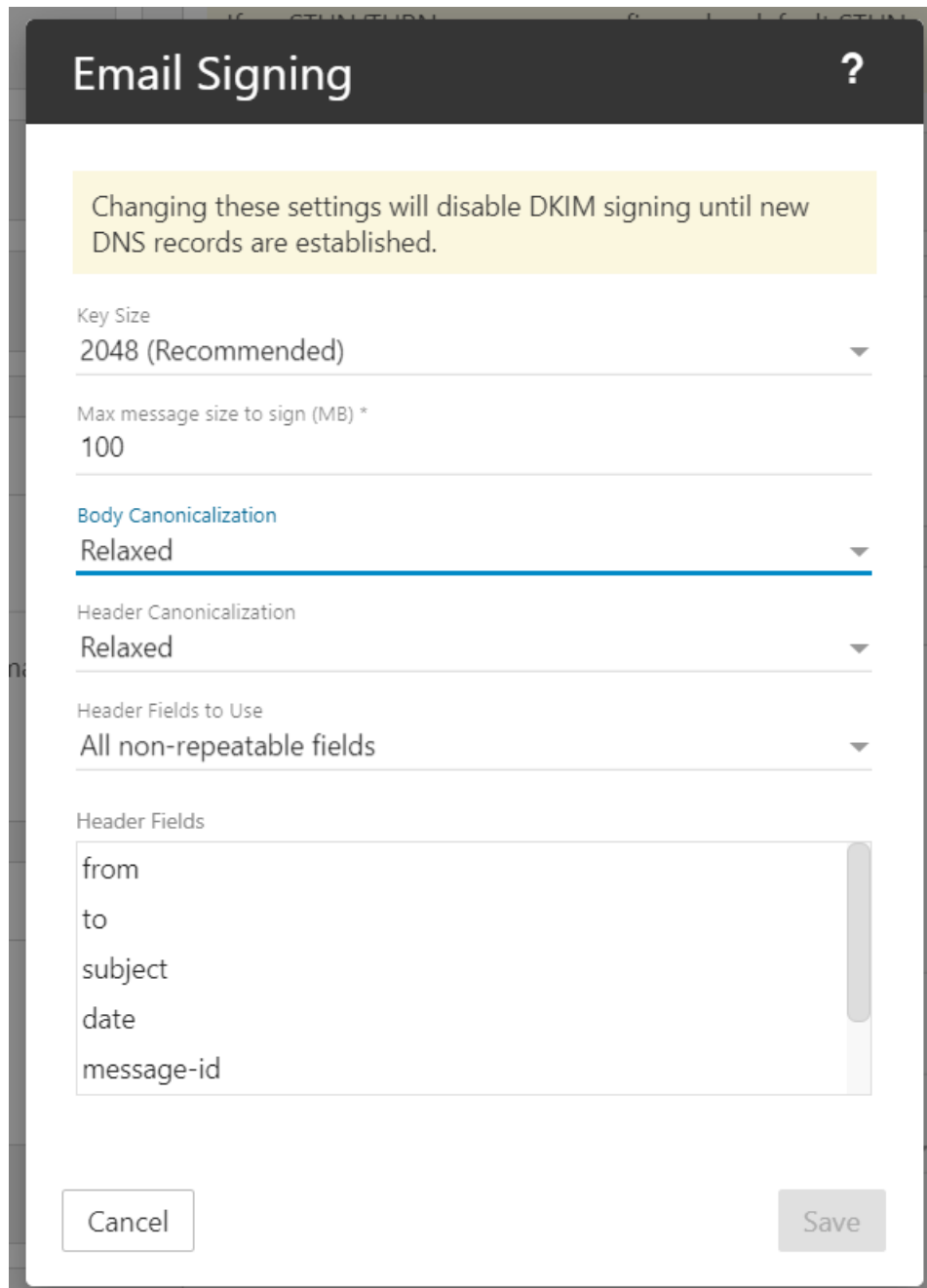
limit and sign that.

• 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.

Setting Up Email Signing

Setting up email signing and creating the fields necessary to add DKIM to a domain's DNS record is simple within SmarterMail.

> • Log in as a Domain Administrator
> • Click on the Domain Settings icon
> • Navigate to the domain's General settings
> • Find the Email Signing card
> • Click on the Settings button
> • A modal window opens, like the one below. Here, all of the DKIM settings are displayed. SmarterMail defaults all of these to a set of general recommendations, but they can be adjusted as needed.• Make any changes you want and save them. If no changes are made, simply click the Cancel button.
> • Next, click the Enable button on the Email Signing card. A modal window will open, and it will contain the text necessary for adding the DNS record. This window contains two important pieces of information: the "Text Record Name" and the "Text Record Value". The Text Record Name contains the "DKIM selector", which is the value that precedes "._domainkey". For example, "2B8U4DAB93D58YR". The selector can be used to verify that your DKIM record is set up correctly. (When the Text Record Name is added to DNS, the ".domain" should automatically be appended by DNS.) The Text Record Value is also the public key that's created by the SmarterMail server. Therefore, it's the encrypted key that pairs to the private key
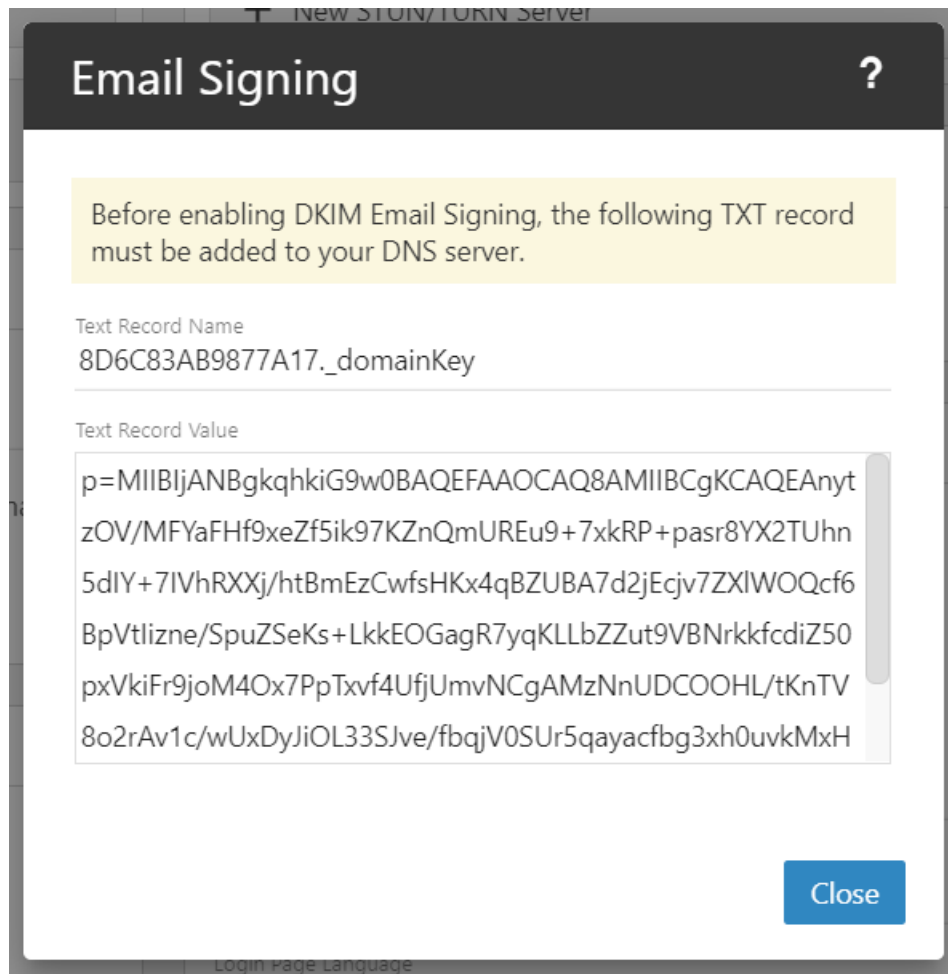
that's stored on the mail server. This is why it looks like a random series of characters.• Now that you have the Name and Value for the TXT record, you will want to log in to your DNS provider and create the actual DNS record. How you do this depends on who your provider is. In general, the DNS TXT record format will be as follows:

- NAME = Text Record Name, which will be something like
  2B8U4DAB93D58YR._DomainKey
- TYPE = TXT
- VALUE = Text Record Value, which contains the public key created by SmarterMail

NOTE: As this is a change to DNS, it may take a few hours for the record to propagate for the domain. Generally that propagation is pretty fast, but it could take 24 hours or more.

Validating Your DKIM Record

Once you've made the changes to your domain's DNS, it can take a few hours for those changes to take effect. To test whether you're set it up properly, you can do a search for "DKIM record validation" or use a site such as MXToolbox . MXToolbox makes DKIM validation simple; you just need your domain name and the selector. (The "selector" is what comes before the "." in your Text Record Name. So if your Text Record Name was 2B8U4DAB93D58YR._domainKey, the selector is 2B8U4DAB93D58YR). Enter those into their form, and they'll let you know a) if the record can be found, and b) if it's valid.

Attachments

> • Inbound 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)
>
> • Outbound 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:

> • Mailing List Command Address - This is, essentially, the "To" address for your listserv. If someone wants to subscribe to a list, for example, they'd email listserv@your-domain.com with the listname and the word "subscribe" in the body of their message. They'd then be subscribed to that mailing list.
>
> • 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. By default, this number is 2.

Chat 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 adminstrators 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 cannnot 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 - The username or email address of the person who participated in a chat.
> • Name - The Display Name of the person who participated in a 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.])

Domain Content Filtering

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

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: Some content filtering actions, such as a Forward action, do not work in conjunction with Plus Addressing as content filters are run BEFORE any plus addressing commands. Using both could lead to duplicate messages or other unwanted/unnecessary behavior.

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 Domain Settings icon. Then click on Content Filtering in the navigation pane.

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

General

- Name - The friendly name chosen to describe the rule.
- 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 ?) - Enable this setting to allow 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 a 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.

Domain Events

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

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 recepient 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 click on the Domain Settings icon. 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 occurence 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.

A Practical Example: Receive an Email When a New There's a New Subscriber to a Mailing List

This practical example of setting up an Event is the result of an old knowledge base article we had. It details how to set up an event that sends an email to the List Admininstrator when a new persons subscribes to that List Administrator's mailing list. As an aside, while this is an exmaple of setting the Event up as a Domain Admininstrator, the process for setting it up as the List Administrator is very similar.

- Log into SmarterMail as the Domain Administrator.
- Click the Domain Settings icon.
- Click Events in the navigation pane. A list of existing events will load.
- Click the New button.
- On the General card, do the following:.

- In the Event Name field, type a descriptive friendly name for the event.
- In the Event Status drop down, select Enabled.
- In the Event Category field, select Mailing.
- In the Event Type field, select Mailing List Subscribe.
- On the Conditions card, a new Condition is possibly already there. This is perfectly fine. However, since we want to be notified when a new person subscribes to a specific mailing list, you'll want to click the New Condition button. Then do the following

- On the Condition modal, select Mailing List Address from the dropdown, then enter the full address for the list. (E.g., testlist@example.com)
- Click the Save button to add the new Condition.
- On the Actions card, click the New Action button. Then do the following:

- On the Actions modal, select Send and email from the dropdown.
- The modal will change, allowing you to select your Frequency, From Address, To Address, Subject, etc. then add the email contents that will be sent. Your To Address should be the List Admininstrator. You can leave the email's content the default that's filled out or edit it how you see fit.
- Click the Save button.
- Your new Event is pretty much finished. Just click the Save button to actually save the Event so that it can run.

Message Archive Search

Message archiving is a method of storing all email and live chat traffic for a domain -- either inbound messages, outbound 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 availalbe 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 Admininstrators will be able to search the message archive. Therefore, if a Domain Admininstrator 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 clicking on the Settings icon, selecting Message Archive in the navigation pane, and clicking the Archive Search tab. 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(s) can find a Message Archive Search option by clicking on the Domain Settings icon then clicking on Message Archive Search in the navigation pane. Domain adminstrators 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 .

Sharing

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

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 Admininstrators create shared calendars and/or conference rooms. When clicking the New Shared Resource button on the Sharing card, the Domain Admininstrator 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.

As an example, here are the steps to set up domain calendar:

• Login as the domain administrator
• Click on the Domain Settings icon.
• When the Domain Settings menu loads, click on Shared Resources.
• Click the New Shared Resources button.
• Enter name of the Calendar you're creating.

• For Type , select Calendar to create a domain shared calendar. Otherwise, select Conference Room to allow for conference room scheduling.

• Next, you'll want to set up the Permissions for sharing the calendar or conference room with Users or User Groups for the domain.

• Once all settings have been added, click Save.

• Once saved, the domain calendar will be automatically mapped to all users and available for them to start using on any new calendar items they create.

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 and System Admininstrators with the proper permissions.

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.)

Default Signatures

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, activate the setting 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.

Domain Spam Filtering

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

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

Jump To:

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

Options

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

Options

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

Editing Actions

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

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

Trusted Senders

Domain Administrators can add specific email addresses (such as jsmith@example.com) or domains (such as example.com) that will be exempted from spam filtering. This lets the system know that these messages come from a trusted source and can prevent mail from friends, business associates and mailing lists from being blocked or sent to the Junk Email folder. By default, every contact in a user's Contacts list is considered a trusted sender and bypasses spam filtering.

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

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

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

For example:

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

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

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

User Defaults

For domains that have a large number of users, it can be time consuming to make a change to user settings -- increase the Mailbox Size Limit or disabling the ability to change passwords, for example -- and then ensure the changes are applied to all users. 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.

User Defaults

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.).

You can make whatever changes you want to these settings, and any NEW accounts that are added will use these defaults. However, it's also possible to change these settings, then push those settings to one or more users individually, or to all users. In the case of pushing changes to individual users, say you have a set Mailbox Size Limit set for all users of 2000MB (2GB). However, the C-Level execs need more. It's possible to change that limit to something higher -- 8000MB (8GB), for example -- and then push that change to all of the accounts set up for the C-Level executives.

Propagation

To apply some or all of the default user settings to some or all of the existing users on the domain, do the following:

- First, make any changes you want on this page, then click the Save button.
- Next, click on the Propagate button. A modal window opens up.
- Scroll down the list of settings, placing a check mark next to the settings you want to push to your user(s).
- Once all items have been selected, you can pick who you want to propagate the changes to:

- Specific Users - Selecting this allows you to start entering the users you want to propagate the changes to. These changes will only propagate to the users you enter.
- All Users - This will propagate the changes to all users of the domain.

> • Once you've selected your changes, and added the specific users you want to propagate the changes to, click the Propagate button.

NOTE: 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. They only affect any new users that are created. In order for changes to take effect, they must be propagated. In addition, if you're making changes to individual users, you may need to go back and change the propagated settings back to what they were originally. Otherwise, any new users created will use those new settings.

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.

Mailing Lists

Mailing Lists Overview

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

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.

Mailing Lists can be managed by System Admininstrators with Manage Domains permissions, Domain Admininstrators and the List Admininstrators themselves. Accessing Mailing Lists is dependent on the role you possess:

List Admininstrators

To view your mailing lists, log in with your username and navigate to your Settings . Then click on Mailing Lists in the navigation pane. The Mailing Lists you administer will be listed here.

Domain Admininstrators

To view the mailing lists for a domain, log into SmarterMail as a Domain Administrator and navigate to the Domain Settings . Then click on Accounts in the navigation pane. If mailing lists are enabled for the domain, they'll be listed here.

System Administrators

To view the mailing lists for a domain, log in to SmarterMail as a System Admininstrator and click on the Manage icon, then click on Domains in the navigation pane. Select the domain from the list to edit it. If you have domain management permissions, you'll see a number of tabs displayed. Click on the Accounts tab, then the Mailing Lists sub-tab. The mailing lists for the domain will be listed here.

Regardless of your role, 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#

• Unsubscribe Link (#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 (#Recipient#) - The email address of the subscriber who was sent the message.

• Sender (#Sender#) - The email address of the user sending the message.

• Domain Date Now (#DomainDateNow#) - The current date (in shorthand) according to the domain's new user time zone defaults found in User Defaults. Ex: 07/13/2015.

• Domain Time Now (#DomainTimeNow#) - The current time according to the domain's new user time zone defaults found in User Defaults. Displayed in 24-hour format.

• Domain Date Time Now (#DomainDateTimeNow#) - The current date and time according to the domain's new user time zone defaults found in User Defaults. Disaplyed in shorthand and 24-hour format.

• Domain Day Now (#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.

• Domain Month Now (#DomainMonthNow#) - The current month (in numeric value) according to the domain's new user time zone defaults found in User Defaults. Ex: 07.

• Domain Year Now (#DomainYearNow#) - The current year according to the domain's new user time zone defaults found in User Defaults. Ex: 2015.

• Domain Day Name Now (#DomainDayNameNow#) - The current day of the week according to the domain's new user time zone defaults found in User Defaults. Ex: Monday.

• Domain Month Name Now (#DomainMonthNameNow#) - The current month (by its name) according to the domain's new user time zone defaults found in User Defaults. Ex: July.

• Moderator Date Now (#ModeratorDateNow#) - The current date (in shorthand) according to the Moderator's time zone. Ex: 07/13/2015.

• Moderator Time Now (#ModeratorTimeNow#) - The current time according to the Moderator's time zone. Displayed in 24-hour format.

• Moderator Date Time Now (#ModeratorDateTimeNow#) - The current date and time according to the Moderator's time zone. Disaplyed in shorthand and 24-hour format.

• Moderator Day Now (#ModeratorDayNow#) - The current date (date alone, without month and year) according to the Moderator's time zone. Ex: 13.

• Moderator Month Now (#ModeratorMonthNow#) - The current month (in numeric value) according to the Moderator's time zone. Ex: 07.

• Moderator Year Now (#ModeratorYearNow#) - The current year according to the Moderator's time zone. Ex: 2015.

• Moderator Day Name Now (#ModeratorDayNameNow#) - The current day of the week

according to the Moderator's time zone. Ex: Monday.

• Moderator Month Name Now (#ModeratorMonthNameNow#) - The current month (by its name) according to the Moderator's time zone. Ex: July.

• Server Date Now (#ServerDateNow#) - The current date (in shorthand) according to the server's system time zone. Ex: 07/13/2015.

• Server Time Now (#ServerTimeNow#) - The current time according to the server's system time zone. Displayed in 24-hour format.

• Server Date Time Now (#ServerDateTimeNow#) - The current date and time according to the server's system time zone. Disaplyed in shorthand and 24-hour format.

• Server Day Now (#ServerDayNow#) - The current date (date alone, without month and year) according to the server's system time zone. Ex: 13.

• Server Month Now (#ServerMonthNow#) - The current month (in numeric value) according to the server's system time zone. Ex: 07.

• Server Year Now (#ServerYearNow#) - The current year according to the server's system time zone. Ex: 2015.

• Server Day Name Now (#ServerDayNameNow#) - The current day of the week according to the server's system time zone. Ex: Monday.

• Server Month Name Now (#ServerMonthNameNow#) - The current month (by its name) according to the server's system time zone. Ex: July.

Options

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

To view the mailing lists for a specific domain, click the Settings tab, then click Mailing Lists in the navigation pane.

This page consists of a number of tabs, and each tab has its own page:

• Options - The configuration options for an individual mailing list.

• 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

Creating a New Mailing List

To create a new mailing list, click the New button in the content pane toolbar. You can also edit an existing mailing list by clicking on it. When you click the New button, a modal window opens with the following fields:

> • List Address - This is the "email address" that will be used for the list. A List Address is simliar to a new Account address: it simply needs to be whatever will be appended to the left of the domain name. For example, "MarketingNewsletter". Posters, then, send messages to "MarketingNewsletter@domain.com". Therefore, just as with accounts, list names should not include spaces, special characters, etc.
> • List Administrator - This is the existing Account that will act as the administrator of the list. Select a user from the drop down.

Once the new list is created, its options will open, where you can edit the list as needed. These cards and options are discussed below.

Options Tab

Options

> • Name - This matches the List Address that's set when the mailing list is created. Essentially, it's the "username" for the mailing list. Posters, then, send messages to "name@domain.com" to post messages to the list. Therefore, just as with accounts, list names should not include spaces, special characters, etc.
> • Status - New mailing lists default to a status of Enabled. To temporarily prevent postings to this list, change the status to Disabled.
> • List Admininstrator - The "owner" of the mailing list. This person will actively manage the mailing list, posts to the list and any replies. The administrator must be an active email user for the domain.
> • Show in Global Address List - There are times when you may want a mailing list to show up in the Global Address List so that all of your subscribers can send to it. If that's the case, enable this setting.
> • Description - A brief summary of the mailing list.

Message Options

> • 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

• Text to show in unsubscribe link - 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.

• 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/

• 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. This email is only sent when subscribe is intitiated by the listserv command. If an administrator manually adds a subscriber to a list via the web interface, via the API or by importing via CSV, this email is not sent to the subscriber(s).

• Send Unsubscribe Email - Select this option to automatically send an email response to unsubscribe requests. This email is only sent when unsubscribe is intitiated by the listserv command. If an administrator manually removes a subscriber from a list via the web interface, via the API or by importing via CSV, this email is not sent to the subscriber(s).

• 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. This email is only sent when double opt-in is intitiated by the listserv command. If an administrator manually adds or removes a subscriber from a list via the web interface, via the API or by importing via CSV, this email is not sent to the subscriber(s). NOTE: If Double Opt-in is disabled for a list, any unverified subscribers will be removed from the list. A warning appears noting this for list administrators prior to making this change.

• Disable List Error Replies - Select this option to prevent the system from automatically replying to incorrect listserv commands.

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 - 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 'subcribers only', at the very least. For larger lists, allowing Moderator Only is a better idea and will cause less issues.

• Subscribers Only - Allows 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.

• List Administrators Only - The List Administrator(s) is/are the only one(s) who can post to the list. This means that no one else, not even list subscribers, will be able to post.

• 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.

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.

• Outbound Messages per Hour - The number of messages sent by the mailing list per hour. By default, the number of outgoing messages is 500.

• Message Throttling Action - When using either message or bandwidth throttling, adminstrators

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.

• Outbound Bandwidth MB per Hour - The total number of MBs sent by the mailing list per hour. By default, the outgoing bandwidth is 50MB.

• Bandwidth Throttling

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 - Enable this setting to view and modify the remaining Digest settings.

• 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.

• Send Digest - Allows an administrator the ability to send the Digest manually. 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. --%>

Subscribers and Digest Subscribers

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

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 an Administrator (List, Domain or System) and go to the Settings area based on your role. Then click on Mailing Lists in the navigation pane. Then click on the Subscribers tab.

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

Manually Adding Subscribers

There are two primary methods for manually adding subscribers -- either regular list subscribers or digest subscribers -- to a mailing list:

• If there are only a few emails to add to the mailing list, List Administrators, Domain Administrators or System Administrators with the proper domain management permissions can manually add subscribers.
• If there are a large number of emails to add to a mailing list, Domain Administrators or System Administrators with the proper domain management permissions can upload a .CSV file containing all of the subscriber emails.

Adding individual subscribers to a mailing list:

• Log in to SmarterMail as a List Administrator, Domain Administrator or System Administrator.
• List Administrators access their mailing list(s) by clicking on Mailing Lists in the navigation pane; Domain Administrators access mailing lists in the Accounts area for their domain -- there is a Mailing Lists tab; System Administrators first have to select the Domain that has the mailing list they want to manage, then click the Accounts tab for that domain where they will see the Mailing Lists tab, just as Domain Administrators do.
• Regardless of how you get there, click on the desired mailing list. The mailing list settings will load in the content pane.
• Click the Subscribers tab. A list of subscribers to this mailing list will load in the content pane.

• Click New .
• In the Email Address field, type the subscriber(s) email address(es), one per line.
• Once all addresses have been added, click Save .

Adding multiple subscribers to a mailing list at once:

It's also possible to add multiple users to a list at one time by uploading a list of users using a .CSV file. 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 Subscriber Fields for the corresponding subscriber/email address. The Import from CSV option can be used to:

• Add new Subscribers, with our without Custom Field data.

- Update/overwrite the Custom Field values for existing Subscribers.
- Add new Custom Fields to existing Subscribers.

NOTE: If you import a CSV that contains existing Subscribers, their Custom Field data will be overwritten with the contents of the CSV.

- Log in to SmarterMail as a List Administrator, Domain Administrator or System Administrator.
- List Administrators access their mailing list(s) by clicking on Mailing Lists in the navigation pane; Domain Administrators access mailing lists in the Accounts area for their domain -- there is a Mailing Lists tab; System Administrators first have to select the Domain that has the mailing list they want to manage, then click the Accounts tab for that domain where they will see the Mailing Lists tab, just as Domain Administrators do.
- Regardless of how you got there, click on the desired mailing list.
- When the list's Options open, click on the Subscribers tab. A list of current subscribers to this mailing list will load in the content pane, if there are any.
- Click on the Actions (...) button.
- From the dropdown menu, select Import CSV File . the Upload Subscribers modal window opens.
- You can either drag-and-drop a CSV file into the modal window, or click inside the window to open File Explorer to find and "open" the file. Click Upload in the content pane toolbar.

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 .

Posters

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

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 .

List Administrators, Domain Administrators and System Administrators (with the proper Manage Domains permissions) 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 list

subscribers who can post messages to the list -- these special subscribers are considered "Whitelisted" as they've been given special permission to post messages, in addition to, say, Moderators Only.

To add additional posters to a mailing list, log into SmarterMail as an Administrator (List, Domain or System) and go to the Settings area based on your role. 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 subsribers, 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 .

Banned Users

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

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 .

Administrators (List, Domain or System) 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 an Administrator (List, Domain or System) and go to the Settings area based on your role. 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.

Messages

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

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 .

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.

- Command help email -- 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.
- Digest footer - This is the footer that is displayed when digest emails are sent to digest list subscribers.
- Digest header - This is the header that is displayed when digest emails are sent to digets list subscribers.
- Digest separator - This is the character set (e.g., dashes) that will be used to separate messages within digest emails.
- Double op-in successful email - 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.
- HELP response - 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.
- LIST members response - disabled - 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.

• LIST members response - enabled - LISTSERV COMMAND ONLY. This returns a list of subscribers for a partiular list. This requires the LIST command to be set.

• LIST response - LISTSERV COMMAND ONLY. This reutrns a list of the mailing lists for a particular domain. This requires the LIST command to be set.

• Post failure - insufficient permissions - 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.

• Post failure - invalid list password - When a list is password-protected, this message is returned when a person posting to the list provides the incorrect information.

• Post failure - list disabled - This message is returned when a user attempts to post to a list that is no longer active.

• Post failure - message too big - This is returned when a message posted to a list is larger than the maximum size set for messages.

• Posted message footer - This is the footer (information at the very bottom of the message) that is displayed on messages that are sent to list subscribers.

• Posted message header - This is the header (informatin at the very top of the message) that is displayed on messages that are sent to list subscribers.

• SET MODE DIGEST response - failed - LISTSERV COMMAND ONLY. This is returned when the list command that sets the disget mode for a subscriber fails.

• SET MODE DIGEST response - ok - LISTSERV COMMAND ONLY. This is returned when the list command sets the disget mode for a subscriber.

• SET MODE STANDARD response - failed - 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.

• SET MODE STANDARD response - ok - LISTSERV COMMAND ONLY. This is returned when the list command sets the standard mode (one email per list post) for a subscriber.

• SUBSCRIBE response - double opt-in required - This message is sent to subcribers to verify their subscription request when your mailing list utilized a double opt-in subscription model (recommended).

• SUBSCRIBE response - list is private - 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.

• SUBSCRIBE response - subscribed - This is sent to a list subscriber when they subscribe to a specific list.

• UNSUBSCRIBE response - 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 List Administrators and System Admininstrators with the proper permissions.

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 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 an Administrator (List, Domain or System) and go to the Settings area based on your role. 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 "listserv@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.