Help for System Administrators

Help Documentation

Help for System Administrators

Logging in to SmarterMail

To access the login page, SmarterMail system administrations will need to navigate their Web browser to the location of the SmarterMail installation. By default, this URL is http://127.0.0.1:9998 (if running the browser on the server itself, otherwise use the IP address of the server instead of 127.0.0.1), but it may be different if you have changed the location of SmarterMail.

To login to SmarterMail, type in the system administrator username and password in the appropriate fields and click Login . Note: By default, the username and password are both "admin" (without the quotes). If everything matches up, you will be presented with the manage domains page or the activation wizard (if you have yet to activate SmarterMail).

To stay logged in to SmarterMail even after closing the browser, be sure to select the Remember Me checkbox. This will allow SmarterMail to encrypt the email address and password. Note: Browser cookies must be enabled for this feature to work. In addition, SmarterTools does not recommend selecting this option if you use a public or shared computer.

Domains

All Domains

System administrators can use this section to manage all of the domains in SmarterMail. To access this section, click the Domains icon . A list of configured domains will load in the navigation pane, while the selected domain□sdetails will load in the content pane. These details include information about the basic setup of the domain: statistics, such as the number of users and aliases for the domain; throttling and priority settings; as well as the various features enabled for the domain, including file storage, IMAP retrieval and more.

In general, the following options are available in the navigation pane toolbar:

- New - Creates a new domain.
- Actions - Click this button and select the appropriate option to select all domains, delete the selected domain(s), manage or edit the selected domain, or export a list of the domains to CSV. Please note you can only manage or edit one domain at a time, though you can delete multiple domains.

In general, the following options are available in the content pane toolbar:

• Edit - Edits the settings for the selected domain.
• Manage - Impersonates the domain administrator and give the system administrator access to all of the domain settings.

Creating New Domains

Adding a new domain and editing an existing domain are essentially the same process, and they both deal with the same settings. To create a new domain, click New in the navigation pane toolbar.

To edit a domain□ssettings, select the desired domain and choose Edit from the Actions menu found in the navigation pane toolbar. You can also double-click on a domain or right-click and choose Edit to open the settings. Regardless of the method used, the domain settings will load in a new window and the tabs below will be available. NOTE: When editing a domain□ssettings, use the Rename button in the window□stoolbar to change the domain name.

Options

Use this tab to specify the following domain options:

• Name - The name of the domain. For example, smartermail.com or example.com. Note: To send or receive mail, the domain name must match the domain name registered with the DNS server.
• Folder Path - The directory in which all information (XML files, mail statistics, alias information, etc.) pertaining to the domain is saved. Note: If the directory does not already exist, it will be created. This directory should be soley dedicated to SmarterMail. By default, SmarterMail saves domain information to C:\SmarterMail\Domains.
• Mailing List Username - The email address for which listserv commands are emailed for the domain. By default, SmarterMail sets this as stServ.
• Disable Domain - Select this option to disable the domain. Disabled domains cannot send email and users cannot login to the Web interface. However, the domain will still receive email to prevent email loss. This option is a good way to temporarily shut off a domain without deleting it.
• Domain Location - Administrators can specify the domain location for email delivery. This allows you to specificy whether the domain is hosted locally or partially/entirely on an external server. The following options are available:

• Local - Select this option if the mail server is hosted locally.
• External (use MX record) - Select this option if the mail server is hosted partially or entirely externally. Messages will be delivered based on an MX lookup. Note: Select the option "Deliver locally if user exists" to perform a local delivery instead of external if the user exists locally.

• External (use host address) - Select this option if the mail server is hosted partially or entirely externally. Messages will be delivered to the specified host address. The host address can either be entered as an IP address or the Fully Qualified Domain Name (FQDN), such as mail.yourdomain.com. Note: Select the option "Deliver locally if user exists" to perform a local delivery instead of external if the user exists locally.
• Domain Administrator - The domain administrator is responsible for adding and deleting email accounts and setting specific configurations for the domain. Domain administrator accounts also have the ability to send and receive email, manage contacts, etc., just like a user account. Select an existing user from the dropdown menu or enter new user credentials.

• Domain Administrator Username - The identifier the domain administrator uses to login to SmarterMail.
• Domain Administrator Password - The password associated to the domain administrator username. Enter the password twice to confirm it is entered correctly.

Technical

Use this tab to specify the following technical settings:

• Outbound IPv4 - The IPv4 address used to connect to external SMTP servers when a message is sent by the domain. If multiple IPv4 IPs are on the server, they will be listed in the dropdown.

• Outbound IPv6 - The IPv6 address used to connect to external SMTP servers when a message is sent by the domain. If multiple IPv6 IPs are on the server, they will be listed in the dropdown.

• Logout URL - By default, when users log out the are presented with the screen to log back into SmarterMail's Web interface. This feature allows for a seprate URL that the user is redirected to upon logout. Check the Enabled box to enable the logout URL. This setting can also be managed by domain administrators.
• Auto-responder Exclusions - To prevent SmarterMail from sending automated messages, such as out-of-office replies, to addresses based on the spam level of the original message, select the appropriate option from the list.
• Forwarding Exclusions - To prevent the system from forwarding messages based on the spam level of the message, select the appropriate option from the list.
• TLS - To enable or disable TLS (SSL encryption) for outgoing mail, select the appropriate option from the list.
• SRS - To enable or disable SRS (the ability for the mail server to re-write the senders email address so that forwarded messages pass SPF checks) for mail, select the appropriate option from the list.

• Calendar Auto Clean - Use this to set a time frame that SmarterMail will use to automatically remove legacy calendar items from users' calendars. This setting can also be managed by domain administrators.
• Require SMTP Authentication - Select this option to require SMTP authentication when sending email. Note: If this option is enabled, users must provide an email address and password to send email from their account. SmarterMail supports cram-md5 and login authentication methods.
• Restrict auto-responders to once per day per sender - Select this option to limit how frequently an auto-responder is sent. Continually sending somethign like an out-of-office reply to the same address every time an email comes in can cause abuse issues. Therefore, it is recommended that this be set for all domains.
• Disable greylisting - Select this option to disable the greylisting anti-spam option for the domain. Greylisting, though effective, can lead to a delay in email delivery for a domain.
• Allow users to opt out of LDAP listings - Select this option to allow users to remove themselves from the Global Address List.
• Allow domains to override mailing list message size - Select this option to allow domain administrators to specify the maximum size for mailing list messages.
• Exclude IP from received line - Select this option to remove the client's IP address from the received header on messages received through SMTP. Note: Removing the IP address from the received header is not recommended because it violates RFC.
• Allow users to override personalization settings - Select this option to allow users to modify the way their user interface appears in webmail.

Features

Use this tab to enable or disable the following features:

• Active Directory Integration - Select this option to enable active directory authentication. By enabling this, domain administrators will be able to add in the necessary LDAP binding string to import LDAP users.
• ActiveSync Remote Wipe - Select this to allow users with the Exchange ActiveSync add-on to have access to SmarterMail's remote wipe functionality.
• ActiveSync User Management - Select this to allow domain administrators to add and delete mailboxes that can use the Exchange ActiveSync add-on. Note: The option to limit the number of ActiveSync mailboxes allotted for the domain can be found on the Limits tab.
• Calendar - Select this option to allow users to use the calendar feature.
• Catch-All Alias - Select this option to allow users to create catch-all email addresses. When enabled, this setting can be managed by domain administrators as well.
• Connected Services - Select this option to allow users to connect different services to their

SmarterMail accounts to facilitate actions like attaching links to shared files.

• Contacts - Select this option to allow users to use the contacts feature. When enabled, this setting can be managed by domain administrators as well.

• Content Filtering - Select this option to allow users to use content filtering. When enabled, this setting can be managed by domain administrators as well.

• Control of Service Access - Select this option to give domain administrators the ability to manage access to POP, IMAP, SMTP and webmail services for users.

• Disposable Addresses - Select this option to allow users to create a temporary, disposable address independent of their email address.

• Domain Aliases - Select this option to allow domain administrator to create domain aliases. When enabled, this setting can be managed by domain administrators as well.

• Domain Chat History View - Select this option to allow domain administrators to be able to search through all chat history for any and all users of a domain.

• Domain Reports - Select this option to provide additional reports for domain administrators.

• Domain Spam Options - Select this option to show or hide the spam filter settings for domain administrators. Hiding the spam filter settings will prevent domain administrators from changing the weights set by the system administrator for spam checks.

• Email Reports - Select this option to provide the ability to email reports.

• Exchange Web Services (EWS) - Select this option to enable users on the domain to synchronize SmarterMail with supported email clients using Exchange Web Services (EWS). Note: For domains that will support inboxes with large volumes of email, IMAP is encouraged as the primary protocol as EWS does not perform well with large amounts of email.

• File Storage - Select this option to allow users to use the file storage feature. When enabled, this setting can be managed by domain administrators as well.

• IMAP Retrieval - Select this option to allow users to download IMAP email from third-party mail servers. When enabled, this setting can be managed by domain administrators as well.

• Live Chat (XMPP) - Select this option to allow users on the domain to chat with each other via the Web interface or any XMPP-compatible chat client. When enabled, this setting can be managed by domain administrators as well.

• Login Display Customization - Select this option to allow domain administrators to customize the login screen to add a company logo, provide additional branding text, or adjust the default □Login to SmarterMail□ text.

• Mail Signing - Select this option to enable email verification via mail signing. When enabled, this setting can be managed by domain administrators as well.

• Mailing Lists Select this option to allow domain administrators to create and use mailing lists to send mass emails. When enabled, this setting can be managed by domain administrators as well.

• Notes - Select this option to allow users to use the notes feature. When enabled, this setting can be managed by domain administrators as well.
• POP Retrieval - Select this option to allow users to download POP email from third-party mail servers. When enabled, this setting can be managed by domain administrators as well.
• SMTP Accounts - Select this option to allow users to send email from a third-party mail server account right from within SmarterMail. When enabled, this setting can be managed by domain administrators as well.
• SyncML - Select this option to allow users to sync SmarterMail with Outlook, Thunderbird and most smartphones using SyncML.
• Tasks - Select this option to allow users to use the tasks feature. When enabled, this setting can be managed by domain administrators as well.
• User Reports - Select this option to provide reports for users.

Limits

Use this tab to specify the following limits:

• Disk Space - The maximum number of megabytes allocated for the domain. By default, the domain is allocated 500 MB of disk space. This disk space limit also includes file storage for users. Note: When this limit is reached, SmarterMail will send a warning to the domain administrator and mailboxes on the domain will not be able to receive new mail.
• Domain Aliases - The maximum number of domain aliases allowed for the domain. A domain alias acts as a secondary domain that users can user for sending and receiving emails. By default, domains are limited to two domain aliases.
• Users - The maximum number of mailboxes allowed for the domain. By default, domains are limited to 100 users. Note: If your SmarterMail license limits the number of mailboxes allowed on the domain, your license level will override this setting.
• User Aliases - The maximum number of alias email accounts (forwarded to a true email account) allowed for the domain. By default, domains are limited to 1,000 user aliases.
• Mailing Lists - The maximum number of mailing lists allowed for the domain. By default, this setting is unlimited.
• Mailing List Max Message Size - The maximum size message that can be sent to a mailing list. By default, the maximum message size is unlimited.
• POP Retrieval Accounts - The maximum number of POP email accounts a user can set up in SmarterMail. By default, users can receive download messages for 10 POP email accounts.
• IMAP Retrieval Accounts - The maximum number of IMAP email accounts a user can set up in SmarterMail. By default, users can receive download messages for 10 IMAP email accounts.
• Max Message Size - The maximum size email a user can send. By default, the max message size is 10,000 KB. This number includes text, HTML, images and attachments. Note: Base64

encoding of attachments increases the size of attachments by approximately 50%. This can impact the overall size of the message and can lead to confusion on the part of senders. For example, if Max Message Size is set to 12MB and a sender adds a 9MB attachment to a message it will essentially be 13MB due to the Base64 encoding. This means that the 9MB attachment will still exceed the message size limit due to this increase.

• Recipients per Message - The maximum number of recipients a message can have. By default, users can send messages to 200 email addresses.

• ActiveSync Accounts - The maximum number of MIcrosoft Exchange ActiveSync accounts that can be set up for the domain. Note: This setting is used in conjunction with the ActiveSync User Management setting on the Features tab.

Sharing

This tab is only available in SmarterMail Enterprise edition.

Use this tab to enable sharing of the following collaboration features:

• Global Address List - Select this option to allow users on a domain to see all user profiles on the domain and participate in LDAP queries against the domain. When enabled, domain administrators can manage this feature as well.

• Shared Calendars - Select this option to allow calendars to be shared with other users on the domain. When enabled, domain administrators can manage this feature as well.

• Shared Contacts - Select this option to allow contact lists to be shared with other users on the domain. When enabled, domain administrators can manage this feature as well.

• Shared Folders - Select this option to allow email folders to be shared with other users on the domain. When enabled, domain administrators can manage this feature as well.

• Shared Notes - Select this option to allow notes to be shared with other users on the domain. When enabled, domain administrators can manage this feature as well.

• Shared Tasks - Select this option to allow task lists to be shared with other users on the domain. When enabled, domain administrators can manage this feature as well.

Priority

Use this tab to prioritize the remote delivery of certain messages. All messages default to a priority of 5 with a range of 1 to 10. Messages assigned a priority of 10 will have the highest priority and will be delivered first, while messages assigned a priority of 1 will have the lowest priority and will be delivered last.

The use of message delivery priorities also gives system administrators the ability to create automated actions based upon that priority. A common use would be to set up a separate specific outbound gateway to handle all mailing lists to avoid potential blacklisting of the primary IP and to efficiently

deliver all messages. The system administrator could then assign all mailing lists a priority of 1, and would set up a gateway to handle only messages with a priority range of 1 to 1.

• Standard Messages - The priority level for messages that don't have another priority affecting it, as detailed below.

• Enabled - Check this box to enable priority settings for standard messages.
• Mailing Lists - The priority level for messages sent to a mailing list.

• Enabled - Check this box to enable priority settings for mailing list messages.
• Priority When Over Size - The priority level for messages that exceed the message size threshold. For example, system administrators may want to lower the priority of large messages to avoid slowing down the spool.

• Enabled - Check this box to enable priority settings for messages that exceed the message size threshold.
• Message Size Threshold - The maximum size a message can be without triggering the Priority When Over Size rule.
• Auto-Responders - The priority level for auto-responder messages, such as out-of-office responses.

• Enabled - Check this box to enable priority settings for auto-responders.
• Bounces - The priority level for non-delivery receipts.

• Enabled - Check this box to enable priority settings for bounced messages.
• Email Reports - The priority level for email reports.

• Enabled - Check this box to enable priority settings for email reports.
• Appointment Reminders - The priority level for messages reminding users of upcoming appointments, meetings or events.

• Enabled - Check this box to enable priority settings for event emails.
• Priority After Attempt 1 - The priority level for messages that were not successfully sent after the specified number of tries.

• Enabled - Check this box to enable priority settings for subsequent delivery attempts.
• Attempt 1 Threshold - The number of retry attempts the system should make before the priority set in Priority After Attempt 1 is assigned to the message.
• Priority After Attempt 2 - The priority level for messages that were not successfully after the specified number of tries.

- Enabled - Check this box to enable priority settings for subsequent delivery attempts.
- Attempt 2 Threshold - The number of retry attempts the system should make before the priority set in Priority After Attempt 2 is assigned to the message.

Throttling

This tab is only available in SmarterMail Enterprise edition.

Throttling allows system administrators to limit the number of messages per hour and/or the amount of bandwidth used per hour to send messages. If the throttling action is set to Reject, SmarterMail will bounce any messages attempting to be sent after the threshold is met, until the next session. If the throttling action is set to Delay, SmarterMail will allow the message into the spool and trickle delivery.

Use this tab to edit the following throttling settings:

- Outgoing Messages per Hour - The number of messages sent by the domain per hour. By default, the number of outgoing messages is 5,000.
- Message Throttling Action - The action SmarterMail should take when the message throttling threshold is reached.
- Outgoing Bandwidth per Hour - The total number of MBs sent by the domain per hour. By default, the outgoing bandwidth is 100.
- Bandwidth Throttling Action - The action SmarterMail should take when the bandwidth throttling threshold is reached.
- Bounces Received per Hour - As bounce messages are received from null senders per RFCs, this setting dictates the number of messages from null senders a domain can receive over SMTP before any further messages from null senders will be rejected. By default, a domain can receive 1,000 bounces per hour.
- Bounces Throttling Action - The action SmarterMail should take when the bounces throttling threshold is reached.

Event Restrictions

Use this tab to enable the following event types and categories:

Alias

- Enable Alias Added event - Select this option to enable the Alias Added event type.
- Enable Alias Deleted event - Select this option to enable the Alias Deleted event type.

Collaboration

- Enable Calendar Reminder Occured event - Select this option to enable the Calendar Reminder event type.
- Enable Task Reminder Occured event - Select this option to enable the Task Reminder event type.

Email

- Enable Message Received event - Select this option to enable the Message Received event type.
- Enable Message Sent event - Select this option to enable the Message Sent event type.

Mailing List

- Enable Mailing List Added event - Select this option to enable the Mailing List Added event type.
- Enable Mailing List Deleted event - Select this option to enable the Mailing List Deleted event type.
- Enable Message Sent to Mailing List event - Select this option to enable the Message Sent to Mailing List event type.
- Enable Mailing List Bounce Removal event - Select this option to enable the Mailing List Bounce Removal event type.
- Enable Mailing List Subscribe event - Select this option to enable the Mailing List Subscribe event type.
- Enable Mailing List Unsubscribe event - Select this option to enable the Mailing List Unsubscribe event type.

Throttling

- Enable User Throttled event - Select this option to enable the User Throttled event type.
- Enable Domain Throttled event - Select this option to enable the Domain Throttled event type.

User

- Enable User Added Event - Select this option to enable an event type for when a new user is added to a domain.
- Enable User Deleted event - Select this option to enable an event type for when a new user is deleted from a domain.
- Enable User Changed Password event - Select this option to enable an event type for instances where users change their passwords.
- Enable User Changed Forward event - Select this option to enable an event type for instances where users change the forwarding address they have set up for their account.

• Enable User Disk Space Used event - Select this option to enable and event to fire when a user approaches a certain amount of disk space usage.

Manage

Spool

The email spool is a list of emails, in order of when they are created, that are available for the server to send out to other mail servers or to deliver locally. SmarterMail is multi-threaded, which means that if a message cannot process out of the spool, SmarterMail simply moves on to the next message until the maximum number of threads that are designated in the administrative configurations are in use. Administrators can use the information here to adjust threads and resources to allocate for concurrent messages.

Messages enter and leave the spool fairly quickly. In fact, some pass through so quickly that they will not display in the spool. Most messages in the spool are displayed because they are large, have many recipients, or are having trouble being sent to their final destination.

To view all messages in the spool, click the Manage icon and expand the Spool in the navigation pane. To view all messages in the spool, both incoming and outgoing, click All Messages . To only view the messages waiting to be delivered, click Waiting to Deliver .

In general the following columns are available:

• Checkbox - Use these boxes to select multiple messages. Messages must be selected before choosing an action from the content pane toolbar.
• File Name - The filename on the hard disk.
• Spool Path - The spool the message resides in. If you have subspools enabled, the message may be placed in one of those locations.
• Sender - The email address that initially sent the email.
• Recipients - The number of delivered/total recipients.
• Size - The total size of the message on the hard drive, in kilobytes.
• Attempts - The number of delivery attempts that have been made.
• Time in Spool - The total amount of time the message has been in the spool.
• Priority - The priority level of the message.
• Status - The current status of the message.
• Next Attempt - The date and time of the next delivery attempt.

The following actions are available from the content pane toolbar:

• Actions - Click this button and select the appropriate option to force the message, reset retries or change the priority of a message in the spool.

• Force - Pushes the message to the top of the spool. Note: The status of forced messages will not update until the server passes through the spool.
• Reset Retries - Resets the retry counts on all messages in the spool, effectively starting the delivery process over. This can be useful if a DNS or firewall problem has been recently resolved, or if you are using SmartHosting and the target server was down.
• Set Priority - Changes the priority level of a message.
• View - Click this button and select the appropriate option to view the text of a selected message or to see the list of recipents for the selected message.

• Message - Displays the text of the selected message in a new window.
• Recipients - Allows the system administrator to see who the message was sent to and the status of that message (i.e. delivered or pending).
• Delete - Clicking this button will allow the system administrator to delete messages from the spool. Note: No confirmation dialog will display, so use caution when deleting from the spool.
• Refresh - Clicking this button will allow the system administrator to update the page with the most recent contents of the spool.

Searching the Spool

Domain administrators can search for messages from particular senders in the spool. To do so, use the Search bar at the top of the content pane. Simply type in the email address of the sender and click the magnifying glass to search for any messages from that sender that are in the spool.

Spool Dashboard

The Spool Dashboard takes the headache out of spool management by allowing administrators to monitor common aspects of the email spool, including message activity, top outbound senders, top inbound domains and more. In addition to reviewing the spool activity, administrators can take action on any messages that are currently being held in the spool. For example, a sending IP address that is inundating the mail server with unwanted messages can be blocked, thereby preventing issues from becoming problems for email users.

And while monitoring the spool regularly is good practice, the dashboard is extremely helpful should the mail server become compromised. Easily spot a compromised account, block the sender and delete the unnecessary messages. The dashboard provides a real-time look at a mail server's activity, refreshing every 20 seconds, so admins always know what's going on.

To access this section, click the Manage icon and expand the Spool folder in the navigation pane. Then click on Spool Dashboard . The dashboard will load in the content pane, and the total number of messages held in the spool will be displayed in the title bar. The following sections are available:

Note: All tables, with the exception of Message Activity, sort entries based on the message count for the last 24 hours. For example, if an entry is the top sender/receiver within the last 5 minutes or hour, but 12th in the last 24 hours, they would not appear on the table.

Message Activity

This section displays the total number of messages that have been delivered by all users, including local and remote deliveries. From this table, see how many messages were sent in the last 5 minutes, last hour, last 24 hours and from the start of the installation.

Top Outbound Senders

This section displays the top 10 users with the highest number of outbound remote deliveries (for the specified time intervals). Note: The message count does not include local deliveries sent to user-to-user. The following actions can be performed on each user included in the table:

- Manage User - Select this option to impersonate the primary domain administrator that manages the user's email account. When clicked, a new window will load (logged in as the domain admin) and the user's settings will be displayed.
- Disable User - Select this option to immediately disable the user's account. This action utilizes the User Status setting found when editing a user . When a user is disabled within the Spool Dashboard, their User Status will be set to 'Disable and Allow Mail'. This prevents the user from sending outbound messages or accessing webmail; however, the mailbox will continue to receive incoming email. Enabling a user in the Spool Dashboard will adjust the setting in the user's account settings and vice versa.
- Delete Messages - Select this option to permanently delete the messages sent by the user that are currently in the spool. Note: This will only delete messages that are CURRENTLY being held in the spool.
- Move Messages - Select this option to move the messages sent by the user that are currently held in the spool to another folder on the server. Use the default path provided or enter any folder path on the server. Moving the .eml files to their own folder on the server is useful by allowing an administrator to review the messages before taking actions against them.

Note: In general, this table will display SmarterMail user accounts only. However, there may be cases where remote email addresses appear, including if: the email address is authenticated with a local account, the sending IP address is listed in the SMTP Authentication Bypass list, SmarterMail is

acting as an incoming gateway, or messages were manually dropped into the spool with sender addresses that don't exist locally. In these instances, the Manage User and Disable User actions cannot be performed.

Top Inbound Recipients

This section displays the top 10 users (local user accounts) who have received the highest number of incoming messages (for the time intervals specified). Both local and remote deliveries are included in the message count. This allows administrators to know which accounts on the server are receiving the most mail. The following actions can be performed on each user included in the table:

- Manage User - Select this option to impersonate the primary domain administrator that manages the user's email account. When clicked, a new window will load (logged in as the domain admin) and the user's settings will be displayed.
- Delete Messages - Select this option to permanently delete all of the inbound messages sent to the user that are currently in the spool. Note: This will only delete messages that are CURRENTLY being held in the spool.
- Move Messages - Select this option to move a user's inbound messages that are currently held in the spool to another folder on the server. Use the default path provided or enter any folder path on the server. Moving the .eml files to their own folder on the server is useful by allowing an administrator to review the messages before taking actions against them.

Top Inbound Senders

This section displays the top 10 email addresses that have sent the highest number of messages to users on the server (for the time intervals specified). The following actions can be performed on each email address included in the table:

- Block Inbound SMTP - Select this option to block all incoming mail sent from the email address. This action utilizes SMTP Blocking found in the Advanced Settings of the Security section. When an email address is blocked within the Spool Dashboard, an entry will be added to the SMTP Blocked list for incoming email and the entry will be denoted as having been blocked from the spool dashboard. Unblocking an email address in the Spool Dashboard will remove the SMTP Blocked entry and vice versa.
- Delete Messages - Select this option to permanently delete all inbound messages sent from the email address that are currently in the spool. Note: This will only delete messages that are CURRENTLY being held in the spool.
- Move Messages - Select this option to move all the inbound messages sent from the email address that are currently held in the spool to another folder on the server. Use the default path provided or enter any folder path on the server. Moving the .eml files to their own folder on the

server is useful by allowing an administrator to review the messages before taking actions against them.

Top Inbound IP Addresses

This section displays the top 10 IP addresses that have sent the highest number of messages to users on the server (for the time intervals specified). The following actions can be performed on each IP address included in the table:

• Blacklist IP - Select this option to block the IP address from sending messages to the server. When an IP address is blacklisted within the Spool Dashboard, an entry will be added to the Blacklist found in the Security section. The IP address will be blocked on SMTP only, and the entry will be denoted as having been blocked from the spool dashboard. Unblocking an IP address in the Spool Dashboard will remove the Blacklist entry in Security settings and vice versa.
• Delete Messages - Select this option to permanently delete all inbound messages sent from the IP address that are currently in the spool. Note: This will only delete messages that are CURRENTLY being held in the spool.
• Move Messages - Select this option to move all the inbound messages sent from the IP address that are currently held in the spool to another folder on the server. Use the default path provided or enter any folder path on the server. Moving the .eml files to their own folder on the server is useful by allowing an administrator to review the messages before taking actions against them.

Top Outbound IP Addresses

This section displays the top 10 IP addresses that have sent the highest number of outbound, remote deliveries (for the time intervals specified). The following actions can be performed on each IP address included in the table:

• Blacklist IP - Select this option to block the IP address from sending messages to the server. When an IP address is blacklisted within the Spool Dashboard, an entry will be added to the Blacklist found in the Security section. The IP address will be blocked on SMTP only, and the entry will be denoted as having been blocked from the spool dashboard. Unblocking an IP address in the Spool Dashboard will remove the Blacklist entry in Security settings and vice versa.
• Delete Messages - Select this option to permanently delete all outbound messages sent from the IP address that are currently in the spool. Note: This will only delete messages that are CURRENTLY being held in the spool.
• Move Messages - Select this option to move all the outbound messages sent from the IP address that are currently held in the spool to another folder on the server. Use the default path

provided or enter any folder path on the server. Moving the .eml files to their own folder on the server is useful by allowing an administrator to review the messages before taking actions against them.

Top Inbound Domains

This section displays the top 10 domains that have sent the highest number of messages to users on the server (for the time intervals specified). The following actions can be performed on each domain included in the table:

- Block Inbound SMTP - Select this option to block all incoming mail sent from the domain. This action utilizes SMTP Blocking found in the Advanced Settings of the Security section. When an domain is blocked within the Spool Dashboard, an entry will be added to the SMTP Blocked list for incoming email, and the entry will be denoted as having been blocked from the spool dashboard. Note: This action does not block on the EHLO Domain. Instead, it uses the Email Address field and enters only the domain. Unblocking a domain in the Spool Dashboard will remove the SMTP Blocked entry and vice versa.
- Delete Messages - Select this option to permanently delete all inbound messages sent from the domain that are currently in the spool. Note: This will only delete messages that are CURRENTLY being held in the spool.
- Move Messages - Select this option to move all the inbound messages sent from the domain that are currently held in the spool to another folder on the server. Use the default path provided or enter any folder path on the server. Moving the .eml files to their own folder on the server is useful by allowing an administrator to review the messages before taking actions against them.

Spam Quarantine

System administrators can quarantine outgoing messages that have been flagged as spam by SmarterMail's spam checks for a maximum of 30 days. Quarantining such messages allows administrators to investigate why certain messages are blocked as spam and make appropriate adjustments, if necessary. In addition, system administrators can easily resend any outgoing messages that should not have been quarantined.

To view a list of quarantined spam messages, click the Manage icon and expand the Spool folder in the navigation pane. Then click Spam Quarantine . A list of messages currently under quarantine because they were flagged as spam by SmarterMail's antispam measures (including the Message Sniffer or Cyren Premium Antispam add-ons, if enabled) will load in the content pane and the following columns will be available:

- Checkbox - Use these boxes to select multiple messages. Messages must be selected before choosing an action from the content pane toolbar.
- File Name - The filename on the hard disk.
- Date - The date the message was flagged for quarantine.
- Sender - The email address that initially sent the email.
- Recipients - The total number of recipients.
- Size - The total size of the message on the hard drive, in kilobytes.
- Time In Quarantine - The amount of time the message has been quarantined.
- Time of Removal - The amount of time until the message is automatically removed from quarantine and permanently deleted.

The following actions are available from the content pane toolbar:

- Actions - Click this button and select the appropriate option to resend a quarantined message.
- Resend - Moves the selected message(s) to the spool for delivery to its intended recipients.
- View - Click this button and select the appropriate option to view the text of a selected message or to see the list of recipents for the selected message.
- Message - Displays the text of the selected message in a new window.
- Recipients - Allows the system administrator to see who the message was sent to.
- Delete - Clicking this button will allow the system administrator to delete messages from quarantine.
- Refresh - Clicking this button will allow the system administrator to update the page with the most recent quarantined spam messages.

Note: Spam quarantine settings can be managed from the Antispam Administration page. To access this page, click the security icon and click Antispam Administration . The quarantine settings are on the SMTP Blocking tab.

Virus Quarantine

System administrators can quarantine outgoing messages that have been flagged as containing viruses by SmarterMail's ClamAV or the Cyren Zero-hour Antivirus add-on for a maximum of 30 days. Quarantining such messages allows administrators to investigate false positives and make appropriate adjustments or notify the developer of the virus scanner, if necessary.

To view a list of quarantined virus messages, click the manage icon and expand the Spool folder in the navigation pane. Then click Virus Quarantine . A list of messages currently under quarantine because

they were flagged for a virus by SmarterMail antivirus measures will load in the content pane and the following columns will be available:

- Checkbox - Use these boxes to select multiple messages. Messages must be selected before choosing an action from the content pane toolbar.
- File Name - The filename on the hard disk.
- Date - The date the message was flagged for quarantine.
- Sender - The email address that initially sent the email.
- Recipients - The total number of recipients.
- Size - The total size of the message on the hard drive, in kilobytes.
- Time In Quarantine - The amount of time the message has been quarantined.
- Time of Removal - The amount of time until the message is automatically removed from quarantine and permanently deleted.

The following actions are available from the content pane toolbar:

- View - Click this button and select the appropriate option to view the text of a selected message or to see the list of recipents for the selected message.

- Message - Displays the text of the selected message in a new window.
- Recipients - Allows the system administrator to see who the message was sent to.
- Delete - Clicking this button will allow the system administrator to delete messages from quarantine.
- Refresh - Clicking this button will allow the system administrator to update the page with the most recent quarantined virus messages.

Note: Spam quarantine settings can be managed from the Antivirus Administration page. To access this page, click the security icon and click Antivirus Administration . The quarantine settings are on the Options tab.

User Activity

System administrators can use this section to monitor the activity of users on the server.

To view a list of users currently logged in to SmarterMail, click the Manage icon . Then expand User Activity and click Online Users in the navigation pane. A list of users that are online will load in the content pane.

In general, system administrators can view the following attributes of online users:

- User - The name of the user.
- Type - The connection type. For example, IMAP or webmail.

- IP Address - This will tell the IP address of the user.
- Start Date - The start date and time of the connection.
- Duration - The length of the connection.

In general, the following options are available in the content pane toolbar:

- End Session - End the selected user's session.
- Disable - Permanately disables the user from logging in to the system.
- Refresh - Refreshes the list of online users.

If you seen any anonymous users, there could be a number of reasons why. For example, these could be people who have the login page open in a browswer but they're not logged in or perhaps there is a monitoring app or service that is monitoring whether a login page responds to ping, etc.

Inactive Users

To view a list of inactive users, click the Manage icon . Then expand User Activity and click Inactive Users in the navigation pane. Then select whether you want to view users that have been inactive for 30 days, 90 days, 6 months, or 12 months.

Viewing inactive users is a good way to clean out users for a domain that are no longer needed. Perhaps these users and their mailboxes can be archived or copied and moved to another location to recover some disk space.

Current Migrations

Use this section to manage the mailbox migrations currently taking place.

Current Migrations

SmarterMail's Mailbox Migration tool makes it easy for users to switch email providers by giving them the ability to import emails, contacts, calendars, tasks, and notes to SmarterMail from most third-party mail servers.

That being said, users can do this on their own, with little input from a SmarterMail system administrator. While this normally is not an issue, there are times when a system administrator may need to help a migration along - or even stop it altogether. That's where the Current Migrations page comes in.

To view any current mailbox migrations occurring on a server, click the Manage icon . Then expand User Activity and click Current Migrations in the navigation pane. A list of all current mailbox migrations will load in the content pane.

In general, system administrators can view the following attributes of current migrations:

- User - The name of the user performing the migration.
- Status - The status of the migration being performed. The status displayed will be one of the following:

- Queued - The migration was intitiated and is waiting to start.
- In Progress - The migration was started and is currently processing.
- Completed - The migration is finished for that user.

In general, the following options are available in the content pane toolbar:

- End Session - End the selected user's migration. The migration will be stopped, regardless of where it is in process. As mailbox migrations are an "all or nothing" proposition, if a migration is stopped in the middle, none of the migration steps will be finalized unless the migration shows as "Completed."
- Refresh - Refreshes the list of current mailbox migrations and their status.

Current Connections

SmarterMail will monitor the server and see who is connecting via the different syncing protocols, including SMTP, IMAP, POP, XMPP and ActiveSync. System administrators can then use this section to blacklist a certain user if they believe too many connections are being made. Current connections can be viewed all at once or separated by protocol.

To view the current connections, click the Manage icon and expand Current Connections in the navigation pane. Then click the appropriate connection type.

Regarding connections that appear to last longer than they should, this could be due to a number of reasons. For example, SMTP connections that stay active for hours could be due to multiple people connecting from behind a firewall. These people all appear to connect from a single IP, but they're actually individual connections, one for each user. The firewall simply portrays the connections as being from a single source. Another thing to note is an "anonymous" connection. An "anonymous" user is someone who has created a session without logging in. For instance, if they hit the login page and don't actually log in, that will create a new session marked as anonymous. You can get a large number of these if a search engine attempts to index your site or if you have an uptime service monitoring your login page.

Current IDS Blocks

This report displays all IPs that have been blocked by the mail server as a result of any abuse detection rules a system admin set up in SmarterMail's Security management area. As a result of these rules, SmarterMail will monitor the server and keep track of all users who are currently being blocked for

SMTP, IMAP, POP, LDAP, XMPP, Webmail or for potential email harvesting abuse. System admins can view a list of blocked IPs by abuse type or view all blocked connections at one time.

System adminstrators can select an IP and click Delete in the content pane toolbar to remove an IP from the list. However, this does not affect the abuse detection rule that blocked the IP in the first place, it just removes the block from the IP.

Mass Messaging

SmarterMail gives system administrators the opportunity to send mass emails and reminders to selected groups. This can be extremely beneficial for notifying users of a specific domain about any policy changes or work being done that may impact their access to the mail server, for sending warnings to specific users about any potential mail server abuse, for sending emails to all domain administrators regarding settings changes and much more. It's a simple way for system admins to keep mail server users up-to-date and current about a variety of topics.

Send Email

To send a mass email, click the manage icon . Then expand Mass Messaging in the navigation pane and click Send Email . The mass messaging options will load in the content pane and the following fields should be completed:

- From - The individual sending the email message. "System Administrator" will be entered as a default.
- To - Select the message recipients from the list. Note: If All Users on a Domain is chosen, you will then be asked to enter the domain name. If you choose Specific User you will be asked to enter a Specific User's email address.
- To Friendly Name - This is a friendly name or description for the recipients that will appear in conjunction with their email address in the To field. For example, if you're sending an email to all users of the domain example.com you could use something like "Example.com User - "
- Subject - The subject of the email.
- Message - Type the text of the message in this field. Messages can be in plain text or stylized with HTML formatting.

Once you complete all the fields, click the Send in the content pane toolbar to send the message.

Send Reminder

Reminders are a quick and easy way to send a follow-up to a previous, more detailed and stylized mass message. For example, if you send a message to all users of a domain about some upcoming

maintenance work on the mail server, you can use use Send Reminder to do a quick follow up reminding the users of the scheduled work.

To send a reminder, click the manage icon . Then expand Mass Messaging in the navigation pane and click Send Reminder . The mass messaging options will load in the content pane and the following fields should be completed:

- To - Select the message recipients from the list. Note: If All Users on a Domain is chosen, you will then be asked to enter the domain name. If you choose Specific User you will be asked to enter a Specific User's email address.
- Subject - The subject of the email.
- Message - Type the text of the message in this field.

Once you complete all the fields, click the Send in the content pane toolbar to send the message.

Services

System administrators can use this section to enable and/or disable specific services on the mail server. Generally, all of these services should be enabled. However, there are cases where a system administrator will want to disable one or more. For example, a web host or ISP may want to limit users' access to incoming mail to POP only when they connect with an email client in order to conserve disk space on the mail server. In this case, the system administrator would want to stop the IMAP services. Another example would be a mail administrator for a large corporation who doesn't want users to add multiple email accounts and therefore read and reply to email from personal accounts as well as their corporate accounts. In this case, the administrator would want to disable the IMAP Retrieval and POP Retrival services.

To view the status of the services, click the manage icon and then click Services in the navigation pane. The list of available services will load in the content pane and the following columns will be available:

- Checkbox - Use these boxes to select multiple services. Services must be selected before choosing an action from the actions toolbar.
- Service - The name of the servivce.
- Status - The current status of the service, either Active or Inactive.
- Description - A brief summary of the service.

The following options will be available in the content pane toolbar:

- Start - Enables the service.
- Stop - Disables the service.

Services

In general, system administrators can enable/disable the following services:

- IMAP - A client/server protocol in which email is received and held by the mail server. IMAP requires continual access to the client during the time that it is working with the mail server.
- IMAP Retrieval - With IMAP retrieval, mail is retrieved from external IMAP servers (e.g., another mail server like GMail) and saved in a mailbox on the mail server.
- Indexing - Indexes messages, contacts, calendars, tasks and notes so that users can search for specific mailbox items via the Web interface.
- LDAP (Enterprise Edition Only) - A communication protocol for accessing online directory services. Programs like Outlook and Thunderbird use LDAP to retrieve contact lists from SmarterMail. SmarterMail will validate email addresses for user accounts, aliases, and mailing lists.
- POP - An email protocol in which mail is saved in a mailbox on the mail server. When the end user reads the mail, it is immediately downloaded to the client computer and is no longer maintained on the mail server.
- POP Retrieval - Similar to IMAP Retrieval, with POP retrieval, mail is retrieved from external POP3 servers and saved in a mailbox on the mail server.
- SMTP - A TCP/IP (Internet) protocol used for sending and receiving e-mail. However, since it's limited in its ability to queue messages at the receiving end, it's usually used with one of two other protocols, POP or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP or IMAP for receiving messages from their local server.
- Spool - The internal message queue used to deliver messages locally and to remote services.
- SyncML - An open synchronization techology that is most commonly used to synchronize mail account data (calendars, contacts, etc.) between a mail server and a mobile device.
- XMPP (Enterprise Edition Only) - An open-source IM protocol designed to allow interoperability between different IM client programs. SmarterMail uses this protocol to power its chat functionality in the Web interface and/or third-party chat clients.

View Logs

System administrators can use this section to quickly view the server's log files. Viewing a server's log files, especially when it's possible to narrow down the type of server action or protocol that is being viewed, allows system administrators to look for any specific errors that could cause reliablity issues on the server or narrow down reasons why a specific behavior is being seen. For example, system

administrators can review SMTP logs to see if an email was delivered or check ActiveSync logs to see if they can narrow down synchronization issues between a specific user's mailbox and their mobile device.

To view logs, click the manage icon and click View Logs in the navigation pane. The following options will be available in the content pane:

- Date - The start and end dates for the log files you want to view.
- Type - Select the type of log file (or the delivery method of the files) that you would like to view.
- Search String - Type the words or phrases to that should be contained in the log files.
- Display related traffic - Select this option to only display data that occurred within the same sesion.

To search for a specific log, complete the date range, select the log type, and enter a search string. Then click Search in the content pane. Any matching log files will display in the content pane. Note: SmarterMail will only display up to 1MB of any specific log.

Alternatively, system administrators can download the log file in a .zip format by clicking Download in the content pane toolbar. This page allows administrators to get quick access to a domain's entire log file so that they can review them more thoroughly on their local machine.

Message Archive Search

This feature is available to domain administrators and/or system administrators using SmarterMail Enterprise.

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

It is important to note that message archive search is 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 admininstrator will be able to search the message archive. Therefore, if a domain admin needs access to the email archive for the domain "example.com", then a new Message Archiving rule for example.com needs to be set by the system admin.

When message archiving is set up for a specific domain, that domain's administrator will see a Message Archive Search option in the navigation pane when they click on the Email icon. It will generally appear under My Today Page . Domain adminstrators can search for a message by date range, the sender's address, the recipient's address, or the subject.

System administrators can perform a message archive search by clicking on the manage icon and then clicking Message Archive Search in the navigation pane. System administrators can search for a message by date range, the sender's address, the recipient's address, or the subject.

For more information on archiving, see Message Archiving .

Impersonate

There are times when you will need to access domain or user specific information. SmarterMail uses impersonation to accomplish this goal, causing a separate window to login automatically as the domain administrator or a user. This can be a useful method to examine settings or diagnose a problem.

To impersonate a user, click the Manage icon and then click Impersonate in the navigation pane. A modal window will display asking for the email address that you would like to impersonate. Clicking OK will open a new tab in which you will be impersonating the user. From there, you may edit user settings, content filters, or whatever other part of the account that needs to be changed. Closing the tab will end the impersonation. In addition, when managing/impersonating a domain, an Impersonate button is available within the Users grid for quick impersonation. (To impersonate a domain, enter the domain administrator's email address. Alternatively, you can impersonate a domain by clicking the Domains icon, selecting the domain in the navigation pane and choosing to Manage the domain.)

Indexing Status

SmarterMail Search Indexing allows users to instantly find any files -- including messages, attachments, appointments, contacts, tasks, or notes -- in their mailbox. Following the initial scan of the server, SmarterMail continually monitors each user's mailbox for changes and updates the index accordingly. This method of indexing reduces server utilization while increasing the speed with which search results are returned.

System administrators can use this section to view the status of SmarterMail Search Indexing. Viewing the status of indexing can be beneficial when troubleshooting a problem. For example, if the mail service seems to be using a large amount of CPU, the system administrator can check to see if the cause of the temporary increase in CPU usage is due to indexing.

To view the indexing status, click the manage icon and click Indexing Status in the navigation pane. A list of users being indexed (Processing) or users awaiting indexing (Queued) can be viewed.

Password Policy Compliance

System administrators can use the Password Policy Compliance page to find users whose passwords do not meet the configured password requirements. Non-compliant users can then be notified via email that they need to change their passwords in accordance with the password requirements to maintain the security and integrity of the mail server.

To view a list of non-compliant users, click the Manage icon . Then click Password Policy Compliance in the navigation pane. A list of non-compliant users will load in the content pane and the following columns will be available:

- Checkbox - Use these boxes to select multiple users. Users must be selected before choosing an action from the content pane toolbar.
- User - The username that is non-compliant.
- Domain - The domain on which the user exists.
- Name - The display name of the user that is non-compliant.
- Violations - The number of password requirements that are not being met.
- Auto Block SMTP Status - This column is used to display the SMTP status of the user. It will show “Blocked” if the user’s SMTP has already been blocked or a date of when the user will be blocked. At times, “N/A” may appear if the block has not yet been determined as this is processed once per day. Note: This column will only display if the “Disable outgoing SMTP when auto-block grace period ends” setting is enabled.

In general, the following options are available in the content pane toolbar:

- Send Email - Allows the system administrator to compose a message to send to the selected user(s), informing the user(s) of their non-compliance and advising the user(s) of how to remedy the situation and become compliant with the password policy for the domain.
- Export to CSV - Export the entire list of non-compliant users in CSV format.

Restore

System administrators can use the Restore page to restore a user’s emails, email folders or their entire user account. This can be extremely useful if a folder or email is mistakenly deleted or if there is corruption within the mailbox.

To restore user data, click the Manage icon then Restore in the navigation pane. The following options will be available in the content pane:

- Type - Select the type of restore that you would like to perform:

• Attach User - Select this option to attach a user that is on disk but not in the domain. In other words, to restore an entire user's account. Note: The user's folder needs to be correctly placed in the domain folder on the server prior to performing this action.
• Attach Folder - Select this option to to attach a folder that is on disk but not in the account. In other words, to restore a user's email folder.
• Rebuild Folder - Select this option to copy .grp files or .eml files into an existing user's folder and have SmarterMail re-build that folder to include the new .grp and .eml files. In other words, to restore a user's emails.
• Email Address - The full email address of the user account being restored.
• Folder Path - The path of the folder within the Web interface that will be used to rebuild or restore an email folder. For example, if you're restoring a subfolder that was created under the Inbox, the folder path would look like: Inbox\Example Folder.
• Recursive - Check this box to attach any subfolders that are found within a folder that is being attached or rebuilt.

Note: There could be a UID conflict issue if you restore .grp files into an existing folder with existing .grp files. If you are only restoring email messages, it is recommended that you create a new folder within the SmarterMail interface and copy the .grp and/or .eml files to that new folder. Then use the Rebuild Folder function. This issue would not occur when restoring .eml files into an existing folder with existing email.

Reports

Reports Overview

System administrators, domain administrators, and individual users can use real-time mail server statistics, historical summary reporting, and detailed trend analysis at the system, domain, and user levels to understand the performance of their systems. With dozens of pre-defined reports, SmarterMail provides critical statistics that help system and domain administrators monitor their systems.

For more information, see the Reports folder of the Help for Users section of the online help.

Settings

General Settings

To access the general settings for SmarterMail server, click the settings icon and click General Settings in the navigation pane. The general settings will load and the following tabs will be available:

Server Info

Use this tab to specify the following server settings:

- Hostname - The hostname of the server. Note: Hostnames should be in the format computername.domain.com.
- Postmaster Mailbox - This is usually the mail server system administrator's email address as this is where errors in e-mail processing are generally directed.
- IP of Primary DNS - The IP address of the primary DNS server. If left blank, the DNS server information will be pulled from the the Windows Networking settings (recommended).
- IP of Secondary DNS - Enter the IP address of the secondary DNS server. If left blank, the DNS server information will be pulled from the the Windows Networking settings (recommended).
- Logout URL - The URL to which users are redirected when they log out of SmarterMail. By default, users are presented with the log in page for the mail server. If this should be different, a new URL can be added.
- Allow domain admins to override logout URL - Select this option to allow domain administrators to specify a Logout URL for their domain. If this option is not enabled, the option will not be visible to domain administrators.

Login Display

Small businesses using SmarterMail on their own servers, or even companies using SmarterMail from their hosting provider, will benefit from the ability to customize the SmarterMail login page 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: System Administrators can allow Domain Administrators to override the custom login screen by editing the Domain, clicking on the Features tab and checking Login Display Customization.

Use this tab to adjust the SmarterMail login display settings:

- 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.

- Enabled - Check this box to enable the custom help URL in the Help menu.
- Custom Help Text - The hyperlink text for the custom URL in the Help menu.
- Custom Login Text - Use this field to adjust the default "Log into SmarterMail" text with something more in line with an overall brand message.

• Enabled - Check this box to enable the Custom Login Text.
• Company Logo - Upload 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 a logo 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.
• Favicon - A favicon is an icon that is associated with a URL and displayed in a browser□s address bar or next the site name in a bookmark list. Upload a favicon by dragging and dropping a file in the highlighted area or clicking to browse for a file. Click Save and refresh the page to view the favicon that has been uploaded. Note: Recommend sizes for a favicon are 32x32, 64x64 or 128x128 pixels. On upload, the image will be converted to a 32x32 .ico image.
• Enable custom login page HTML - Check this box to enable the ability to use HTML to further modify the login screen to add additional text or adjust the layout. This is used in conjunction with the Login Page HTML section below.
• 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 company logo, the div id "companyinfo" must be included.

The following options are available in the content pane toolbar:

• Save - Saves the custom login display settings.
• Preview - Opens a new popup window displaying what the current settings render on the login screen. If this window remains open, live changes can be seen as settings are adjusted.

Spool

Use this tab to specify the following spool settings:

• Spool Path - The full path in which messages are stored prior to delivery. If you are using a real-time virus scanner, this is the path that must be scanned in order to properly handle viruses.
• SubSpools - SubSpools are within the spool path and allow SmarterMail to work around the NTFS limitation of 30,000 objects in an individual folder. SmarterMail will utilize subspools by allocating up to 10,000 messages per subspool. (Default value is 10)
• Delivery Delay - This number of seconds mail will be held in the spool before it is delivered. A delivery delay is beneficial when you are running a secondary service (such as a virus checker) that needs access to messages prior to delivery, as it provides ample time for the

secondary service to interact with the message. By default, the delivery delay is 1 second.

• Retry Intervals - When the mail server is unable to contact the receiving server, the email attempting to be sent is held for a period of time before the mail server attempts to resend it. This is the time between retries. Users can specify multiple retry attempts to resend emails before it is bounced. By default, this is set to 4 attempts - at 15 min, 30 min, 60 min, and 90 min intervals.

• Bounce DNS errors after - The maximum number of attempts SmarterMail should make before the message is bounced due to a DNS error. The most common cause of a DNS error is a misspelled domain. Limiting the number of attempts before DNS errors are bounced is beneficial because messages will not sit in the queue for long periods of time taking up processing on the mail server and possibly slowing the system down. This will be helpful to users because messages will be bounced sooner and will give users the opportunity to fix any mistakes and get a message resent. By default, the server will make 2 attempts. Note: Setting this at 1 retry can be dangerous if the DNS server fails or if there is a loss of Internet connectivity. To disable this feature, set the number of bounces equal to the number of retry intervals.

• Notify senders of delay after - Sets the number of delivery attempts before the sender is notified that the email delivery is delayed. This can be beneficial as it lets the sender know that the mail server is still attempting to deliver the message but that the recipient has not received it yet. (Default value is 0.)

• Command-Line File - Enable this and enter the full path to an executable you wish to use to process incoming messages. Use %filepath as an argument to pass the path of the email file to the executable. It is allowable for the executable to delete the message to prevent delivery. Example: If you set this field to "c:\program files\myexe.exe %filepath", the program myexe.exe will be launched with the full path to the spool file as its first argument. Note: The command will not be executed if the Enabled box is not checked.

• Command-Line Timeout - The number of seconds that the server will wait for information from the remote server. By default, the timeout is set to 5 seconds.

Reports

Use this tab to specify the following settings:

• Delete Server Stats After - The length of time server stats should be kept before being deleted. By default, server stats are deleted after 13 months.

• Delete Domain Stats After - The length of time domain stats should be kept before being deleted. By default, the domain stats are deleted after 13 months.

• Delete User Stats After - The length of time user stats should be kept before being deleted. By default, the user stats are deleted after 13 months.

Indexing

Use this tab to specify the following settings:

- Max Threads - The maximum number of threads to use for search indexing. Increasing this value will cause SmarterMail to use more CPU, but will allow the system to simultaneously index more users. (Default value is 1.)
- Segment Count Before Optimizing - The number of segment counts in an index before the index is reorganized. Increasing this number will increase file counts per mailbox, but will use less CPU. (Default value is 20.)
- Items Before Garbage Collection - The number of indexed items across the server before freeing as much memory as possible. Increasing this number will increase memory usage and lower CPU usage. (Default value is 5000.)
- Items to Index Per Pass - The number of items to index per user per index attempt. Increasing this number will increase memory usage and decrease the time it takes to index one user. However, it will increase the length of time it takes to index many small users if there are a few large users. (Default value is 2500.)
- Seconds In Queue Before Indexing - The amount of time a user must be in the indexing queue before being indexed. This setting provides a buffer for many changes to a mailbox to ensure the same user is not indexed multiple times. Increasing this number will cause search results to be delayed further, but will result in indexing heavier users less frequently. (Default value is 5.)
- Deleted Items Before Optimizing - The number of items that will be removed from the index before an optimization will occur. Increasing this number will slow search results. Decreasing this number will increase CPU and disk usage, but will increase search result speed. (Default value is 1000.)

System Administrators

SmarterMail allows a single installation to have multiple system administrator logins, each with their own unique login and password. To view a list of system administrator accounts, click the settings icon and click System Administrators in the navigation pane. A list of users with system administrator access will load in the content pane and the following options will be available in the content pane toolbar:

- New - Creates a new system administrator account.
- Edit - Edits the selected system administrator account.
- Delete - Permanently deletes the selected system administrator account(s).

Creating New System Administrators

To create a new system administrator account, click New in the content pane toolbar. The system administrator settings will load in a popup window and the following tabs will be available:

Options

Use this tab to specify the following settings:

- Username - The identifier used to login to SmarterMail.
- New Password - The password used to login to Smartermail.
- Confirm Password - Re-type the password used to login to Smartermail.
- Description - A brief description of the administrator. For example, "for support department".
- Enable login access by IP address - Select this option to only allow system administrators to login from certain IP addresses.
- Allow Impersonation and Domain Management - There are times when an administrator may need to access domain or user specific information. SmarterMail uses impersonation to accomplish this goal, causing a separate window to login automatically as the domain administrator or user. Select this option to allow secondary system administrators the ability to impersonate user accounts and domains.

Login Access

Use this tab to specify the IP address or IP range from which system administrators can login to SmarterMail. Note: This tab is only accessible if the option to enable login access by IP address was selected in the Options tab.

Protocol Settings

To access the settings for standard email protocols, click the settings icon and click Protocol Settings in the navigation pane. The protocol settings will load and the following tabs will be available:

POP

Use this tab to specify the following POP settings:

- POP Banner - The text that is displayed when initially connecting to the port. The banner supports the use of the following variables, which will be replaced with their corresponding values:

- #HostName# - The hostname of the IP address to which the connection is made.
- #ConnectedIP# - The IP address of the remote computer.
- #Time# - The system's local time.

• #TimeUTC# - The time in UTC.
• #UnixTime# - The number of seconds since January 1, 1970.
• Command Timeout - If the server receives a command that sends large amounts of data but the data stops coming in for this number of minutes, the command will be aborted. By default, the command times out after 5 minutes.
• Max Bad Commands - After this many unrecognized or improper commands, a connection will be automatically terminated. By default, the maximum number of bad commands is 8.
• Max Connections - Some protocols in SmarterMail allow you to specify the maximum number of connections. Increasing this value allows SmarterMail to handle more connections of that type at once, but results in higher CPU and memory utilization. By default, the maximum number of connections is 500.
• POP Retrieval Download Path - The path in which mail is stored from POP accounts until it is read.
• Max POP Retrieval Threads - SmarterMail is multi-threaded, meaning it can do more than one thing at a time. This setting is for the maximum number of threads you want SmarterMail to work on concurrently for retrieving mail using the POP protocol. By default, the maximum number of POP retrieval threads is 10.
• POP Retrieval Interval - The frequency by which SmarterMail checks for new POP messages. By default, the POP retrieval interval is 1 minute.
• Autodiscover Host - The URL of the mail server (e.g., mail.domain.com) to be returned by an auto discover query.
• Autodiscover Port - The port to autodiscover uses to communicate with the mail server.
• SSL - Check this box to enable autodiscover to use SSL. NOTE: Autodiscover generally requires the use of SSL, especially when used with Microsoft Outlook.

IMAP

Use this tab to specify the following IMAP settings:

• IMAP Banner - The text that is displayed when initially connecting to the port. The banner supports the use of the following variables, which will be replaced with their corresponding values:

• #HostName# - The hostname of the IP address to which the connection is made.
• #ConnectedIP# - The IP address of the remote computer.
• #Time# - The system's local time.
• #TimeUTC# - The time in UTC.
• #UnixTime# - The number of seconds since January 1, 1970.
• Command Timeout - If the server receives a command that sends large amounts of data but the

data stops coming in for this number of minutes, the command will be aborted. By default, the command times out after 15 minutes.

• Max Bad Commands - After this many unrecognized or improper commands, a connection will be automatically terminated. By default, the maximum number of bad commands is 8.

• Max Connections - Some protocols in SmarterMail allow you to specify the maximum number of connections. Increasing this value allows SmarterMail to handle more connections of that type at once, but results in higher CPU and memory utilization. By default, the maximum number of connections is 1000.

• IMAP Retrieval Download Path - The path in which mail is stored from IMAP accounts until it is read.

• Max IMAP Retrieval Threads - The maximum number of threads you want SmarterMail to work on concurrently. By default, the maximum number of POP retrieval threads is 10.

• IMAP Retrieval Interval - The frequency by which SmarterMail checks for new IMAP messages. By default, the IMAP retrieval interval is 10 minutes.

• Autodiscover Host - The URL of the mail server (e.g., mail.domain.com) to be returned by an auto discover query.

• Autodiscover Port - The IMAP port returned when autodiscover communicates with the mail server. System administrators can modify this port as needed to accommodate firewall settings, etc.

• SSL - Check this box to enable autodiscover to use SSL. NOTE: Autodiscover generally requires the use of SSL

• Enable IDLE Command - Select this checkbox to enable IMAP IDLE. IMAP idle is an extension of the IMAP protocol that allows a mail server to send status updates in real time. Through IMAP IDLE, users can maintain a connection with the mail server via any mail client that supports IMAP IDLE, allowing them to be instantly aware of any changes or updates. When enabled, SmarterMail will inform any connecting IMAP client that it accepts the IDLE command. Note: IMAP clients that do not fully support IMAP IDLE, like Microsoft Outlook, may use the command in such a way that it actually hinders performance.

LDAP

Use this tab to specify the following LDAP settings:

• Session Timeout - After a connection fails to respond or issue new commands for this number of seconds, the connection will be closed. By default, the session times out after 300 seconds.

• Command Timeout - If the server receives a command that sends large amounts of data and the data stops coming in for this number of seconds, the command will be aborted. By default, the command times out after 120 seconds.

SMTP In

Use this tab to specify the following incoming SMTP settings:

• SMTP Banner - The text that is displayed when initially connecting to the port. The banner supports the use of the following variables, which will be replaced with their corresponding values:

• #HostName# - The hostname of the IP address to which the connection is made.
• #ConnectedIP# - The IP address of the remote computer.
• #Time# - The system's local time.
• #TimeUTC# - The time in UTC.
• #UnixTime# - The number of seconds since January 1, 1970.
• Allow Relay - If you are concerned about spam mailers using the relay function to send mail through your server or do not want any other mail server to use your SMTP server as a gateway, set this to Nobody (recommended). However, you can set the type of relays you will allow, should you so desire.

• Nobody - Restricts sent mail to only work via SMTP authentication and with accounts on the local SmarterMail Server (except for IPs on the White List).
• Only Local Users - Limits relay access to users (email accounts) for a valid domain on your SmarterMail Server.
• Only Local Domains - Limits relay access only to mail hosts (domains) on your SmarterMail Server.
• Anyone - Allows any other mail server to pass messages through your mail server, increasing the chances of your mail server being used for sending large volumes of messages with domains not associated with your local mail server. Selecting this option turns off statistics for all domains, due to the high amount of messages that are passed through the mail server with an open relay.
• Session Timeout - After a connection fails to respond or issue new commands for this number of seconds, the connection will be closed. By default, the session times out after 15 minutes.
• Enabled - Select this checkbox to enable the session timeout setting.
• Command Timeout - If the server receives a command that sends large amounts of data but the data stops coming in for this number of seconds, the command will be aborted. By default, the command times out after 120 seconds.
• Max Bad Commands - After this many unrecognized or improper commands, a connection will be automatically terminated. By default, the maximum number of bad commands is 8.
• Max Connections - Some protocols in SmarterMail allow you to specify the maximum number of connections. Increasing this value allows SmarterMail to handle more connections of that

type at once, but results in higher CPU and memory utilization. By default, the maximum number of connections is 1000.

• Max Hop Count - After a message gets delivered through this many mail servers, it is aborted by the software. This prevents looping due to DNS problems or misconfigurations. By default the max hop count is 20.

• Max Message Size - Messages greater than this size will be rejected by the mail server. By default, the max message size is 0 (unlimited).

• Max Bad Recipients - At times, spammers will hammer a domain with a dictionary harvesting attack. This means that software is used to send messages to many of the most common mailbox addresses (e.g., admin, user, contact, etc.) or username variations (e.g., alan@, alana@, alanb@, etc.) in order to find valid email addresses. Setting the max bad recipients means that after this many bad recipients (those that don't exist for the domain), the SMTP session will be terminated. This setting allows you to better protect yourself against email harvesting attacks. A value of 20 is recommended in most cases.

• Append Received Line - Select the option for appending the received line for all messages, only for SMTP Authenticated messages or for no messages at all.

• Require Auth Match - Select this to force a user's From: address to match their SMTP authenticated address, either by matching the entire email address or by matching just the domain - or not requiring it at all. This setting helps keep senders from spoofing email addresses through email clients.

• Max Messages Per Session - The maximum number of messages that can be sent in one session. This is useful in handling cases where spammers will make one connection and then send a large amount of messages with that connection.

• Autodiscover Host - The URL of the mail server (e.g., mail.domain.com) to be returned by an auto discover query.

• Autodiscover Port - The SMTP In port returned when autodiscover communicates with the mail server. System administrators can modify this port as needed to accommodate firewall settings, SMTP restrictions by ISPs, etc.

• SSL - Check this box to enable autodiscover to use SSL. Note: Autodiscover generally requires the use of SSL.

• Enable VRFY command - Select this checkbox to allow others (including other mail servers) to verify an email address on the server. Note: Some people believe enabling VRFY commands is a security risk, so be sure to research the possible ramifications before enabling this feature.

• Enable EXPN command - Select this checkbox to allow others to list all users associated with an alias or list. Note: Some people believe enabling EXPN commands is a security risk, so be sure to research the possible ramifications before enabling this feature.

• Allow relay for authenticated users - Select this checkbox to enable the "Allow Relay" setting

from above when users are required to use SMTP Authentication for sending messages.
• Enable Domain's SMTP auth setting for local deliveries - Select this checkbox to enforce SMTP authentication for all local deliveries. For example, mail from user1@example.com to user2@example.com must be authenticated even though the message is bound for local delivery.
• Disable AUTH LOGIN method for SMTP authentication - Select this checkbox to disable plain text authentication.

SMTP Out

Use this tab to specify the following outgoing SMTP settings:

• Outbound IPv4 - The IPv4 address used to connect to external SMTP servers when a message is sent by the domain. If multiple IPv4 IPs are on the server, they will be listed in the dropdown.

• Outbound IPv6 - The IPv6 address used to connect to external SMTP servers when a message is sent by the domain. If multiple IPv6 IPs are on the server, they will be listed in the dropdown.

• Enable Primary IP on failure - Select this checkbox to have SmarterMail automatically fall back to the primary IP when a failure has occurred. SmarterMail will only attempt to connect once if this option is enabled.
• Command Timeout - If the server receives a command that sends large amounts of data but the data stops coming in for this number of seconds, the command will be aborted. By default, the command times out after 60 seconds.
• Max Spam Check Threads - The maximum number of messages that can be spam checked at one time. By default, the maximum spam check threads is 30.
• Max Delivery Threads - The maximum number of messages that can be sent at one time to email addresses that are not on the local server. If a message cannot be sent, the SmarterMail server's multi-threading capabilities will move on to the next message and eventually get back to the one it skipped. This action can save tremendous amounts of time when compared to some other mail servers that stall the spool if a message cannot be sent right away. By default, the max delivery threads is 50.
• Enable DNS Caching - Select this checkbox to cache the results of DNS calls in SmarterMail. This can help speed up delivery of messages.
• Enable TLS if supported by the remote server - Select this checkbox to use TLS (SSL encryption) if the server you are connected to supports it.
• Append authenticated as header for outgoing messages - Checking this box means that outgoing messages will have a new line item in the message header called "x-smartermail-authenticatedas" that demonstrates that the message sender was verified using SMTP

authentication. This header can then be used by anti-spam services for validation.

• Enable Remote Bounces - Select this checkbox to enable bounce messages from all senders. When unchecked, bounce messages are restricted to only internal senders. Note: This setting is enabled by default.

XMPP

Use this tab to specify the following XMPP settings:

• Max Connections - Some protocols in SmarterMail allow you to specify the maximum number of connections. Increasing this value allows SmarterMail to handle more connections of that type at once, but results in higher CPU and memory utilization. By default, the maximum number of connections is 1000.

• Web Chat URL Listeners - The URLs that XMPP services should listen to in order to ensure live chat connections are made. Examples include "http://+:80/http-bind/" or "https://+:443/http-bind"

EWS

• Modification Auto Clean - SmarterMail records when an account syncs using Exchange Web Services and stores those sync sessions in a file. This setting tells SmarterMail how long to keep those sync sessions before they are automatically purged from the file.

• Autodiscover Host - The URL of the mail server (e.g., mail.domain.com) to be returned by an auto discover query when Exchange Web Services are enabled.

EAS

• Autodiscover Host - The URL of the mail server (e.g., mail.domain.com) to be returned by an auto discover query when Exchange ActiveSync is enabled.

Log Settings

System administrators can use this section to manage how logs are written and how much detail is included in SmarterMail's logs.

To access the log settings, click the Settings icon and click Log Settings in the navigation pane. The log settings will load in the content pane and the following tabs will be available:

Log Files

Use this tab to specify the following settings:

• Log Path - The default location for the Logs that email messages in SmarterMail produce. If you would like to change the default location, enter a new path here.

• Compress Log Files After - The number of days after which log files are automatically compressed. This preserves existing log files but also saves server space.

• Enabled - Select this option to allow log files to be compressed after a specific number of days.
• Delete Log Files After - The number of days after which log files are automatically deleted.

• Enabled - Select this option to allow log files to be deleted after a specific number of days.

Log Detail Levels

Use this tab to specify how detailed the logs should be:

• Exceptions Only - Small size logs that record only errors.
• Normal - Medium size logs that record most activity taken on the mail server.
• Detailed - Very detailed logs that can get very large. Only enable this option when asked to by SmarterTools Support, or when troubleshooting server operations.

Note: More detailed logs require more disk space. If you choose a detailed log, you may want to enable the auto-delete setting on the Log Files tab.

System administrators can apply these settings to the following log file types:

• ActiveSync - The log level for Exchange ActiveSync connections.
• Administrative - The log level for for any changes and/or modifications made by system administrator accounts.
• Delivery - The log level for message delivery and spool operations.
• Events - The log level for event sessions.
• EWS - The log level for Exchange Web Services sessions.
• IMAP - The log level for IMAP sessions.
• IMAP Retrieval - The log level for IMAP retrieval sessions.
• Indexing - The log level for SmarterMail indexing.
• LDAP - The log level for LDAP sessions.
• Mailbox Importing - The log level for data imported during mailbox migrations.
• Maintenance - The log level for maintenance tasks performed by SmarterMail.
• Message-ID - The log level for logging Message-ID's of all messages sent to mailing lists.
• POP - The log level for POP sessions.
• POP Retrieval - The log level for POP retrieval sessions.
• SMTP - The log level for SMTP sessions.
• SycnML - The log level for SyncML sessions.
• WebDAV - The log level for CalDav and CardDav sessions.

Note: By default, SmarterMail sets all log detail levels to exceptions only.

ActiveSync Mailboxes

This feature is only available in SmarterMail Enterprise.

Microsoft Exchange ActiveSync (EAS) is the industry standard for synchronizing email clients and mobile devices with email servers such as SmarterMail. Using EAS you can synchronize email, contacts and calendars with a number of email clients such as Microsoft Outlook 2013 as well as with smartphones, tablets and "phablets" from Apple, HTC, Samsung and others.

System administrators will use this section to enable and disable the EAS add-on for mailboxes across all domains on the SmarterMail server. Domain administrators will use this page to manage the EAS add-on for their particular domain. Note: Before an administrator can configure a mailbox to sync using ActiveSync, the add-on needs to be activated and available for users of the domain. For more information, please refer to the KB article Activate Microsoft Exchange ActiveSync . Furthermore, domain administrators will only see this section available when the system administrator has enabled ActiveSync User Management for their domain.

To access this section as the System Administrator, click the Settings icon and click ActiveSync Mailboxes in the navigation pane. To access this section as the Domain Administrator, click the Settings icon , expand the Domain Settings folder and click ActiveSync Mailboxes in the navigation pane. A list of accounts for which the Exchange ActiveSync add-on is enabled will load in the content pane.

In general, the following columns are available:

- Checkbox - Use these boxes to select multiple mailboxes. Mailboxes must be selected before choosing an action from the actions toolbar.
- Email Address - The email address of the SmarterMail user.
- Display Name - The display name of the SmarterMail user.

The following options are available from the actions toolbar:

- Add - Adds Exchange ActiveSync to a mailbox on the domain.
- Delete - Removes Exchange ActiveSync from the selected mailbox.

Personalization

SmarterMail supports the ability to personalize the webmail interface so that administrators, or even users, can create skins that represent their own style or emulate the company's branding and appearance.

To view the personalization settings, click the settings icon and open either My Settings for user personalization, or Domain Settings and then click Personalization in the navigation pane. The following tabs will load in the content pane:

Settings

The Settings tab will be where users select whether to use the default settings for the domain or whether to customize the general color scheme and overall CSS of the SmarterMail interface. The following options are available, depending on the default domain settings:

- Use default settings - Selecting this will use as the default personalization settings.
- Override Settings - Selecting this activates the Colors and Custom CSS tabs and allows users to customize those settings.
- Enable users to override - This is a domain administrator only setting. Selecting this option will allow end users to modify the custom CSS and general color scheme for their webmail login.
- Skin - This dropdown will list any skins developed for SmarterMail. In general, the Default skin will always be available, but others may appear in this list as well.

Colors

The Colors tab allows users to modify the Primary, Secondary and Link colors for the SmarterMail interface.

- Primary Color - This is the color for the title bar in SmarterMail, the numbered notifications (e.g., for new messages), highlight colors for input boxes, calendar items, etc. The default is #519CDE
- Secondary Color - This is the color of the button bar. The default is #D1E8FC
- Link Color - This is the color of hyperlinks that appear in messages, calendar items, etc. The default is #1677C2

Custom CSS

The Custom CSS tab allows users to take the existing styles used in the SmarterMail interface and modify them based on branding or personal preference. As noted on the page, however, errors in custom CSS may cause the interface to have issues, so modifications should only be made if the person making the changes is extremely proficient with styles and stylesheets.

To modify a style, you should first use a Web browser like Chrome to inspect the element that you want to modify. (Using FireFox's Firebug plug-in will work as well). By inspecting the element you will see the class used and any styles associated with the class. You can then create a version of that

style yourself, and then paste it in the box to override the default. Realize this will happen wherever that style is used, so changing one style can affect several pages within the interface. To enable the custom styles, simply check the Enabled box on the Custom CSS tab.

To remove any customization and personalization of the interface, simply remove the custom style and save the changes. This will reset the interface back to its original default settings.

System Messages

SmarterMail sends a variety of automated email messages for certain actions within SmarterMail. For example, system messages are sent to users when their password has expired or is in violation. Administrators can modify certain messages sent out from the server to make them match a company's voice and style, add extra information or add a standard From address.

To access this section, click the Settings icon and click System Messages in the navigation pane. A list of adjustable system messages will load in the content pane.

In general, the following columns are available:

- Name - The friendly name of the system message.
- Subject - The subject of the email.
- Display Name - The friendly name or description of the sender that will appear in conjunction with the From address (if included) in the From field of the email.
- From Address - By default, system messages send from "System Administrator" without a From address. Administrators can add a From address to allow users to respond to system messages or to decrease the likelihood a message will be caught by spam filters.

The following option is available from the actions toolbar:

- Edit - Select this option to edit the selected system message.

Events

Events Overview

SmarterMail can detect events as they occur, generate messages for those events, and deliver the messages to system administrators and agents that need the information. For more information, see the Events folder of the Help for Users section of the online help.

Notification Profiles

SmarterMail can detect events as they occur, generate messages for those events, and deliver the messages to system administrators and agents that need the information. For example, users can receive notifications when a task is due or system administrators can receive notifications when the disk space for a domain reaches a certain percentage. Notification profiles determine how those messages are sent.

Although users can set up their own notification profiles, some organizations may find it beneficial to create a notification profile that applies to all system administrators. You can use this page to do so.

To view a list of notification profiles, click the settings icon and click Notification Profiles in the navigation pane. Your notification profiles will load in the content pane.

The following columns are available:

- Checkbox - Use these boxes to select multiple profiles. Notification profiles must be selected before choosing an action from the content pane toolbar.
- Notification Profile Name - The name of the profile.
- Type - The types of notification enabled for the selected profile.

The following options are available from the content pane toolbar:

- New - Creates a new notification profile.
- Edit - Edits an existing notification profile.
- Delete - Permanently deletes the selected notification profile(s).

To view a specific notification profile, simply double-click the appropriate profile. The profile will load in the content pane and the following fields will be available:

- Notification Profile Name - The name of the profile.
- Email Address(es) - The email address(es) to which notifications are sent.
- Enable - Select this option to enable email notifications.
- SMS Email Address(es) - The mobile device email address to which notifications are sent.
- Enable - Select this option to enable SMS notifications.
- Enable Reminders for all domain administrators - Select this option to send a reminder to all domain administrators when the event is triggered.

Bindings

IP Addresses

System administrators can use this section to specify on which ports the IPs on the server should listen. All ports being used should be assigned to at least one IP. However, SmarterMail provides system administrators with some flexibility when configuring IP bindings. This means, for example, that the system administrator can allow POP (port 110) on the IP 111.111.111.11 but not on the IP 222.222.222.22. In addition, some servers may have other programs installed that need to listen on mail ports. To accommodate this, the system administrator can configure SmarterMail to listen on a subset of IP addresses, leaving the remaining IP addresses available for other programs.

Another benefit to binding IPs to your mail server is that you can limit the possibility of your entire mail server being blacklisted by assigning IPs on a per domain basis. That means that spammers sending messages on your mail server will only get their domain and their specific IP blacklisted rather than getting the entire mail server blocked.

To access the IP address settings, click the Settings icon and expand the Bindings folder in the navigation pane. Then click IP Addresses . A list of IP addresses on the server will load in the content pane and the following options will be availble in the content pane toolbar:

- Edit - Edits the ports assigned to the selected IP.

Note: The IP Addresses listed in this section are pulled from the server and can only be removed from SmarterMail by removing the IP Address from the Network Interface Card (NIC).

Ports

System administrators can use this section to assign protocols to ports that can then be assigned to IP Addresses . In addition, this section is used to add Secure Socket Layer (SSL) and Transport Layer Security (TLS) rules to any ports and protocols.

To access the port settings, click the settings icon and expand the Bindings folder in the navigation pane. Then click Ports . A list of ports will load in the content pane and the following options will be available in the content pane toolbar:

- New - Creates a new port.
- Edit - Edits the selected port options.
- Delete - Permanently deletes the selected port(s).

Creating New Ports

When adding a new port there are several fields that need to be completed. These fields are:

- Protocol - The type of communications protocol that should be used (IMAP, LDAP, POP, SMTP, XMPP, or Submission Port).
- Encryption - If the port requires SSL or TLS encryption, check the appropriate option. SSL always assumes the connection will be secure and sends the encryption immediately. TLS connects normally and then looks to see if the connection is secure before sending the encryption.
- Name - The friendly name for the port.
- Port - The port number on which to listen for the selected protocol.
- Description - A simple description of the port and/or the port name.

Hostnames

This feature allows administrators to assign a hostname for each IP address. For example: IP 1.1.1.1 can assigned to mail.domain1.com and IP 1.1.1.2 can be for mail.domain2.com. The benefit of assigning hostnames to IPs is that every domain on the server can be assigned its own IP address, thereby limiting the chances of the entire mail server becoming blacklisted should a user on one domain send out unwanted emails.

To view hostnames, click the Settings icon , expand the Bindings folder and click Hostnames in the navigation pane. A list of hostnames will load in the content pane and the following options will be available from the content pane toolbar:

- New - Creates a new hostname.
- Edit - Edits the selected hostname.
- Delete - Deletes the selected hostname(s).

Defaults

Domain Defaults

Use this section to create global default settings that will be applied to new domains created through the Web interface or via SmarterMail's extensive Web services. These default settings can be overwritten and are only intended to avoid needless data entry. Note: Modifications to these settings will not affect existing domains.

To access the domain default settings, click the Settings icon . Then expand the Defaults folder and click Domain Defaults in the navigation pane. The domain default settings will load in the content pane and the following tabs will be available:

Technical

Use this tab to specify the following technical settings:

- Folder Path - The directory in which all information (XML files, mail statistics, alias information, etc.) pertaining to the domain is saved. By default this is C:\SmarterMail. However, it can be modified as needed.
- Auto-Responder Exclusions - To prevent SmarterMail from sending automated messages, such as out-of-office replies, to addresses based on the spam level of the original message, select the appropriate option from the list.
- Forwarding Exclusions - To prevent the system from forwarding messages based on the spam level of the message, select the appropriate option from the list.
- TLS - To enable or disable TLS (SSL encryption) for outgoing mail, select the appropriate option from the list.
- SRS - To enable or disable SRS (the ability for the mail server to re-write the senders email address so that forwarded messages pass SPF checks) for mail, select the appropriate option from the list.
- Calendar Auto Clean - Use this to set a time frame that SmarterMail will use to automatically remove legacy calendar items from users' calendars. This setting can also be managed by domain administrators.
- Require SMTP Authentication - Select this option to require SMTP authentication when sending email. Note: If this option is enabled, users must provide an email address and password to send email from their account. SmarterMail supports cram-md5 and login authentication methods.
- Restrict auto-responders to once per day per sender - Select this option to limit how frequently an auto-responder is sent. Continually sending somethign like an out-of-office reply to the same address every time an email comes in can cause abuse issues. Therefore, it is recommended that this be set for all domains.
- Disable greylisting - Select this option to disable the greylisting anti-spam option for the domain. Greylisting, though effective, can lead to a delay in email delivery for a domain.
- Allow users to opt out of LDAP listings - Select this option to allow users to remove themselves from the Global Address List.
- Exclude IP from received line - Select this option to remove the client's IP address from the received header on messages received through SMTP. Note: Removing the IP address from the

received header is not recommended because it violates RFC.

• Allow users to override personalization settings - Select this option to allow users to modify the look and feel of their webmail experience with custom colors and/or use of custom CSS.

Features

Use this tab to enable or disable the following features:

• ActiveSync Remote Wipe - Select this to allow users with the Exchange ActiveSync add-on to have access to SmarterMail's remote wipe functionality.

• ActiveSync User Management - Select this to allow domain administrators add and delete mailboxes that can use the Exchange ActiveSync add-on. Note: The option to limit the number of ActiveSync mailboxes allotted for the domain can be found on the Limits tab.

• Calendar - Select this option to allow users to use the calendar feature.

• Catch-All Alias - Select this option to allow users to create catch-all email addresses. When enabled, this setting can be managed by domain administrators as well.

• Connected Services - Select this option to allow users to connect different services to their SmarterMail accounts to facilitate actions like attaching links to shared files.

• Contacts - Select this option to allow users to use the contacts feature. When enabled, this setting can be managed by domain administrators as well.

• Content Filtering - Select this option to allow users to use content filtering. When enabled, this setting can be managed by domain administrators as well.

• Control of Service Access - Select this option to give domain administrators the ability to manage access to POP, IMAP, SMTP and webmail services for users.

• Disposable Addresses - Select this option to allow users to create a temporary, disposable address independent of their email address.

• Domain Aliases - Select this option to allow domain administrator to create domain aliases. When enabled, this setting can be managed by domain administrators as well.

• Domain Chat History View - Select this option to allow domain administrators to be able to search through all chat history for any and all users of a domain.

• Domain Reports - Select this option to provide additional reports for domain administrators.

• Enable spam filtering - Select this option to show or hide the spam filter settings for domain administrators. Hiding the spam filter settings will prevent domain administrators from changing the weights set by the system administrator for spam checks.

• Email Reports - Select this option to provide the ability to email reports.

• Exchange Web Services (EWS) - Select this option to enable users on the domain to synchronize SmarterMail with supported email clients using Exchange Web Services. Note: For domains that will support inboxes with large volumes of email, IMAP is encouraged as the primary protocol as EWS does not perform well with large amounts of email.

• File Storage - Select this option to allow users to use the file storage feature. When enabled, this setting can be managed by domain administrators as well.
• IMAP Retrieval - Select this option to allow users to download IMAP email from third-party mail servers. When enabled, this setting can be managed by domain administrators as well.
• Live Chat (XMPP) - Select this option to allow users on the domain to chat with each other via the Web interface or any XMPP-compatible chat client. When enabled, this setting can be managed by domain administrators as well.
• Login Display Customization - Select this option to allow domain administrators to customize the login screen to add a company logo, provide additional branding text, or adjust the default "Login to SmarterMail" text.
• Mailing Lists Select this option to allow domain administrators to create and use mailing lists to send mass emails. When enabled, this setting can be managed by domain administrators as well.
• Mail Signing - Select this option to enable email verification via mail signing using DKIM. When enabled, this setting can be managed by domain administrators as well.
• Notes - Select this option to allow users to use the notes feature. When enabled, this setting can be managed by domain administrators as well.
• POP Retrieval - Select this option to allow users to download POP email from third-party mail servers. When enabled, this setting can be managed by domain administrators as well.
• SMTP Accounts - Select this option to allow users to send email from a third-party mail server account right from within SmarterMail. When enabled, this setting can be managed by domain administrators as well.
• SyncML - Select this option to allow users to sync SmarterMail with Outlook, Thunderbird and most smartphones using SyncML.
• Tasks - Select this option to allow users to use the tasks feature. When enabled, this setting can be managed by domain administrators as well.
• User Reports - Select this option to provide reports for users.

Limits

Use this tab to specify the following limits:

• Disk Space - The maximum number of megabytes allocated for the domain. By default, the domain is allocated 500 MB of disk space. This disk space limit also includes file storage for users. Note: When this limit is reached, SmarterMail will send a warning to the domain administrator and mailboxes on the domain will not be able to receive new mail.
• Domain Aliases - The maximum number of domain aliases allowed for the domain. A domain alias acts as a secondary domain that users can user for sending and receiving emails. By default, domains are limited to two domain aliases.

• Users - The maximum number of mailboxes allowed for the domain. By default, domains are limited to 100 users. Note: If your SmarterMail license limits the number of mailboxes allowed on the domain, your license level will override this setting.
• User Aliases - The maximum number of alias email accounts (forwarded to a true email account) allowed for the domain. By default, domains are limited to 1,000 user aliases.
• Mailing Lists - The maximum number of mailing lists allowed for the domain. By default, this setting is unlimited.
• Mailing List Max Message Size - The maximum size message that can be sent to a mailing list. By default, the maximum message size is unlimited.

• Enable domain to override - Check this option to allow domain administrators to specify the maximum size for mailing list messages.
• POP Retrieval Accounts - The maximum number of POP email accounts a user can set up in SmarterMail. By default, users can receive download messages for 10 POP email accounts.
• IMAP Retrieval Accounts - The maximum number of IMAP email accounts a user can set up in SmarterMail. By default, users can receive download messages for 10 IMAP email accounts.
• Max Message Size - The maximum size email a user can send. By default, the max message size is 10,000 KB. Note: This number includes text, HTML, images and attachments.
• Recipients per Message - The maximum number of recipients a message can have. By default, users can send messages to 200 email addresses.
• ActiveSync Accounts - Sets the maximum number of Microsoft Exchange ActiveSync accoutns a domain can have set up. Note: This setting is used in conjunction with the ActiveSync User Management setting on the Features tab.

Sharing

This tab is only available in SmarterMail Enterprise edition.

Use this tab to enable sharing of the following collaboration features:

• Global Address List - Select this option to allow users on a domain to see all user profiles on the domain and participate in LDAP queries against the domain. When enabled, domain administrators can manage this feature as well.
• Shared Calendars - Select this option to allow calendars to be shared with other users on the domain. When enabled, domain administrators can manage this feature as well.
• Shared Contacts - Select this option to allow contact lists to be shared with other users on the domain. When enabled, domain administrators can manage this feature as well.
• Shared Folders - Select this option to allow email folders to be shared with other users on the domain. When enabled, domain administrators can manage this feature as well.
• Shared Notes - Select this option to allow notes to be shared with other users on the domain.

When enabled, domain administrators can manage this feature as well.

• Shared Tasks - Select this option to allow task lists to be shared with other users on the domain. When enabled, domain administrators can manage this feature as well.

Priority

Use this tab to prioritize the remote delivery of certain messages. All messages default to a priority of 5 with a range of 1 to 10. Messages assigned a priority of 10 will have the highest priority and will be delivered first, while messages assigned a priority of 1 will have the lowest priority and will be delivered last.

The use of message delivery priorities also gives system administrators the ability to create automated actions based upon that priority. A common use would be to set up a separate specific outbound gateway to handle all mailing lists to avoid potential blacklisting of the primary IP and to efficiently deliver all messages. The system administrator could then assign all mailing lists a priority of 1, and would set up a gateway to handle only messages with a priority range of 1 to 1.

• Standard Messages - The priority level for messages that don't have another priority affecting it, as detailed below.

• Mailing Lists - The priority level for messages sent to a mailing list.

• Priority When Over Size - The priority level for messages that exceed the message size threshold. For example, system administrators may want to lower the priority of large messages to avoid slowing down the spool.

• Message Size Threshold - The maximum size a message can be without triggering the Priority When Over Size rule.

• Auto-Responders - The priority level for auto-responder messages, such as out-of-office responses.

• Bounces - The priority level for non-delivery receipts.

• Email Reports - The priority level for email reports.

• Appointment Reminders - The priority level for messages reminding users of upcoming appointments, meetings or events.

• Priority After Attempt 1 - The priority level for messages that were not successfully sent after the specified number of tries.

• Attempt 1 Threshold - The number of retry attempts the system should make before the priority set in Priority After Attempt 1 is assigned to the message.

• Priority After Attempt 2 - The priority level for messages that were not successfully after the specified number of tries.

• Attempt 2 Threshold - The number of retry attempts the system should make before the priority set in Priority After Attempt 2 is assigned to the message.

Throttling

This tab is only available in SmarterMail Enterprise edition.

Throttling allows system administrators to limit the number of messages sent per hour and/or the amount of bandwidth used per hour to send messages. If the throttling threshold is reached, messages will stop sending for the remainder of the hour. Then the system will resume sending messages.

Use this tab to edit the following throttling settings:

- Outgoing Messages per Hour - The number of messages sent by the domain per hour. By default, the number of outgoing messages is 5,000.
- Message Throttling Action - The action SmarterMail should take when the message throttling threshold is reached.
- Outgoing Bandwidth per Hour - The total number of MBs sent by the domain per hour. By default, the outgoing bandwidth is 100.
- Bandwidth Throttling Action - The action SmarterMail should take when the bandwidth throttling threshold is reached.
- Bounces Received per Hour - The number of non-delivery receipts a domain can receive per hour. By default, a domain can receive 1,000 bounces per hour.
- Bounces Throttling Action - The action SmarterMail should take when the bounces throttling threshold is reached.

Event Restrictions

Use this tab to enable the following event types and categories:

Alias

- Enable Alias Added Event - Select this option to enable the Alias Added event type.
- Enable Alias Deleted Event - Select this option to enable the Alias Deleted event type.

Collaboration

- Enable Calendar Reminder Occured Event - Select this option to enable the Calendar Reminder event type.
- Enable Task Reminder Occured Event - Select this option to enable the Task Reminder event type.

Email

- Enable Message Received Event - Select this option to enable the Message Received event

type.

• Enable Message Sent Event - Select this option to enable the Message Sent event type.

Mailing List

• Enable Mailing List Added event - Select this option to enable the Mailing List Added event type.

• Enable Mailing List Deleted event - Select this option to enable the Mailing List Deleted event type.

• Enable Message Sent to Mailing List event - Select this option to enable the Message Sent to Mailing List event type.

• Enable Mailing List Bounce Removal event - Select this option to enable the Mailing List Bounce Removal event type.

• Enable Mailing List Subscribe event - Select this option to enable the Mailing List Subscribe event type.

• Enable Mailing List Unsubscribe event - Select this option to enable the Mailing List Unsubscribe event type.

Throttling

• Enable User Throttled Event - Select this option to enable the User Throttled event type.

• Enable Domain Throttled Event - Select this option to enable the Domain Throttled event type.

User

• Enable User Added Event - Select this option to enable an event type for when a new user is added to a domain.

• Enable User Deleted event - Select this option to enable an event type for when a new user is deleted from a domain.

• Enable User Changed Password event - Select this option to enable an event type for instances where users change their passwords.

• Enable User Changed Forward event - Select this option to enable an event type for instances where users change the forwarding address they have set up for their account.

• Enable User Disk Space Used event - Select this option to enable and event to fire when a user approaches a certain amount of disk space usage.

Domain Propagation

Use this section to apply global default settings to all of the domains on the server. These default settings can be overwritten and are only intended to avoid needless data entry.

To access domain propagation, click the Settings icon . Then expand the Defaults folder and click Domain Propagation in the navigation pane. The default domain settings will load in the content pane. For more information on these settings, refer to Domain Defaults .

To apply some or all of the default settings to all of the domains on your server, select the appropriate settings and click Propagate Now .

User Defaults

Use this section to create global default settings that will be applied to new users created through the Web interface or Web services. These default settings can be overwritten and are only intended to avoid needless data entry. Note: Modifications to these settings will not affect existing users.

To access the user default settings, click the Settings icon . Then expand the Defaults folder and click User Defaults in the navigation pane. The domain default settings will load in the content pane. For more information on these settings, refer to Users .

User Propagation

Use this section to apply global default settings to all of the users on the domain. These default settings can be overwritten and are only intended to avoid needless data entry.

To access user propagation, click the settings icon . Then expand the Advanced Settings folder and click User Propagation in the navigation pane. The default domain settings will load in the content pane. For more information on these settings, refer to Users .

To apply some or all of the default settings to all of the users on the domain, select the appropriate settings and click Propagate Now .

Routing

Forwarding Blacklist

The Forwarding Blacklist is a useful tool for preventing issues with companies that have extremely strict spam policies. For example, AOL and Comcast do not differentiate between the sending server and the server that forwarded a spam message, and as such, they commonly blacklist legitimate domains for forwarding spam. Because it's impossible to prevent ALL spam messages from being forwarded when a user has automated forwarding enabled, administrators may prefer to blacklist email forwarding to those strict domains.

Note: The Forwarding Blacklist only prevents the automated forwarding of email, which is configured in the user's general settings. Any messages that are manually forwarded from the Email section itself will bypass this blacklist.

To access the Forwarding Blacklist, click the Settings Icon . Then expand the Routing folder and click Forwarding Blacklist in the navigation pane. A list of blacklists will load in the content pane.

To add a new forwarding blacklist, click New in the content toolbar. To edit an existing blacklist, select the desired entry and click Edit . The blacklist settings will load in the content pane and the following option will be available:

- Domain Name - Enter the name of the domain that should be blocked from automated email forwarding. When a domain is included in this list, users will see the following notification when they attempt to save a forwarding address with that domain: "Forwards to the following address(es) are not allowed: _____." Note: Users will still be able to manually forward emails to users on that domain.

Outgoing Gateway

Gateway servers allow you to reduce the load on your primary server by using a secondary server to process outgoing mail. Gateway servers can also be used to combat blacklisting. If the gateway server gets blacklisted, simply rotate the primary IP on the network card to a different one to send out on the new IP.

To access the outgoing gateway settings, click the settings icon . Then expand the Routing folder and click Outgoing Gateways in the navigation pane. A list of outgoing gateways will load in the content pane.

To add a new outgoing gateway, click New in the content pane toolbar. To edit an existing gateway, select the desired gateway and click Edit . The outgoing gateway settings will load in the content pane and the following tabs will be available:

Options

Use this tab to specify the following settings:

- Server Address - The IP address of the gateway server.
- Port - The port used to connect to the gateway server. By default, the port is 25.
- Auth Username - The username of the gateway server given to you by your ISP.
- Auth Password - The password for your gateway server.
- Encryption - Select the type of encryption from the list.
- Priority Range - The priority range for this server. System administrators can use gateway

servers to only send mails with a certain priority level. For example, gateways can be used only for lower priority messages, such as newsletters or messages over a certain size, to reduce load and free up processing on the primary mail server. Note: This feature is only avaiable in SmarterMail Enterprise.

• Enable SmarterMail gateway mode - Select this option to indicate that the outgoing gateway server is another SmarterMail server.

• Description - A friendly name or brief description of the gateway.

SmarterMail Gateway

This tab is only available if the SmarterMail gateway mode is enabled in the Options tab. Use this tab to specify the following settings:

• SmarterMail URL - The Webmail URL for the SmarterMail server being used an an outgoing gateway. This will allow the use of Web services to verify the users and domains.

• SmarterMail Username - The identifier used to login to the primary mail server.

• SmarterMail Password - The corresponding password used to login to the primary mail server.

Incoming Gateways

The purpose of an incoming gateway is to reduce server load. Generally, spam checks and antivirus scans should be performed on the incoming gateway, freeing up the primary server processing for the delivery of messages.

To access the incoming gateway settings, click the settings icon . Then expand the Routing folder and click Incoming Gateways in the navigation pane. A list of incoming gateways will load in the content pane.

To add a new incoming gateway, click New in the content pane toolbar. To edit an existing gateway, select the desired gateway and click Edit . The incoming gateway settings will load in the content pane and the following tabs will be available:

Options

Use this tab to specify the following settings:

• Gateway Mode - The function that the incoming gateway will perform. If the incoming gateway is set to backup MX, it will only receive messages when your primary server is down. If the incoming gateway server is set to domain forwarding, it will received all message and forward them to your primary server.

• IP Address / IP Range - The IP address, or range of IP addresses, of the primary mail server.

• User Verification - The method used by the incoming gateway to determine if a user is valid or

not. Note: If none is selected, the incoming gateway server will accept all email addresses for the domain. If Web service is selected, the incoming gateway will check with the primary mail server for a list of valid email addresses.

• Enable SmarterMail Gateway Mode - Select this option to indicate that the incoming gateway server is another SmarterMail server.

• Disable Greylisting - Select this option to disable greylisting for the domain.

Domains

This tab is only available if the gateway mode is set to domain forwarding. Domain forwarding allows you to easily send mail through one server to another. This will allow your server to act as an incoming gateway to your network, and permit you to have a single point of entry for incoming SMTP traffic.

When messages come in to a forwarded domain, they are run through the command-line exe referenced in Protocol Settings. If a delivery delay has been established for the server, messages are also delayed accordingly. This allows you to establish an incoming server that can run external virus or spam scanners, which can reduce the load on your existing network servers.

Use this tab to specify for which domains the incoming gateway will accept mail:

• Domain Verification - The method used by the incoming gateway to determine if a domain is valid or not.

• Specified Domains - The specific domains for which the gateway will accept mail.

Spam

Use this tab to specify the following spam checks:

• Not Spam Action - The action the incoming gateway will perform on messages NOT marked as spam.

• Spam Low Action - The action the incoming gateway will perform on messages with a low probability of being spam.

• Spam Medium Action - The action the incoming gateway will perform on messages with a medium probability of being spam.

• Spam High Action - The action the incoming gateway will perform on messages with a high probability of being spam.

SmarterMail Gateway

This tab is only available if the SmarterMail gateway mode is enabled in the Options tab. Use this tab to specify the following settings:

- SmarterMail URL - The Webmail URL for the SmarterMail server being used an an incoming gateway. This will allow the use of Web services to verify the users and domains.
- SmarterMail Username - The identifier used to login to the primary mail server.
- SmarterMail Password - The corresponding password used to login to the primary mail server.

Sender Priority Overrides

This feature is only available in SmarterMail Enterprise.

Sender priority overrides allows the system administrator to assign priority levels to specific email addresses. For example, a company may want the mail server to send emails from its support team (support@example.com) before sending emails to mailing lists.

To view the sender priority overrides, click the Settings icon . Then expand the Routing folder and click Sender Priority Overrides in the navigation pane.

To create a new sender priority override, click New in the content pane toolbar. The following options will be available:

- Email Address - The email address of the user or group.
- Message Delivery Priority - The priority level assigned to this user's messages.
- Description - A brief summary why the sender priority override was created.

Storage

File Storage

SmarterMail's file storage feature allows users to upload files to the server and share them via public links. One benefit of using file storage is that it reduces the stress on the server by keeping large files out of the spool. Note: Files uploaded to the server are counted toward the user's disk space allocation, so system administrators should encourage users to delete any unused files whenever possible.

To manage the file storage settings, click the settings icon , expand the Storage folder and click File Storage in the navigation pane. The file storage settings will load in the content pane and the following tabs will be available:

Options

Use this tab to specify the folowing settings:

- Max File Size - The maximum size a file can be in order to be uploaded to the server.
- Root URL - The base URL of any file stored and shared in file storage. By default, the base

URL corresponds to the domain the mail server is set up on (i.e., http://mail.example.com). If SmarterMail is configured on an external IP that allows a network address translation (NAT) to an external IP, the system administrator may need to modify the root URL.

Extension Blacklist

Use this tab to select and list any file types that cannot be uploaded to the server. System administrators may want to limit the capabilites of users to upload certain file types, such as executables (.exe) or other file types that can possibly be used to cause problems on the server.

Folder Auto-clean

Folder Auto-clean is a method for limiting how much of a user's disk space is used by the Junk E-Mail, Sent Items, and Deleted Items folders. By placing limits on the size of these folders, domain administrators can help ensure that user accounts do not fill up unnecessarily. Messages are deleted from the folders in the order that they were received so that older messages get deleted first.

To access the folder auto-clean settings, click the Settings icon . Then expand the Storage folder and click Folder Auto-Clean in the navigation pane.

The folder auto-clean settings will load in the content pane and the following tabs will be available:

Options

Use this tab to specify the following options:

- Allow domains to override auto-clean settings - Selet this option to allow domain administrators to create their own auto-clean policies.
- Allow users to auto-clean inbox - Select this option to allow users to create auto-clean policies on the Inbox folder.

Rules

If you are using the default auto-clean settings set up by your administrator, they will appear on this tab. If you chose to override the settings, you can click Add Rule in the content pane toolbar to create your own auto-clean policies based upon size or date.

These options will be visible if size is chosen:

- Folder Size Before Auto-clean - The maximum size of the folder. Once the folder reaches this size, the auto-clean process is started and older messages (messages that were received the longest time ago) are deleted.
- Folder Size After Auto-clean - The goal size of the folder. When auto-cleaning, SmarterMail will delete older messages until the folder reaches this size. Note: This number should aways be

lower than the "before" number.

• Enable auto-clean for this folder - Select this box to activate auto-cleaning of the selected folder.

These options will be visible if date is chosen:

• Mail Age - The maximum number of days mail will stay in the selected folder before deletion.

• Enable auto-clean for this folder - Select this box to activate auto-cleaning of the selected folder.

Message Archiving

This feature is only available in SmarterMail Enterprise edition.

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

By default, SmarterMail does not archive any messages. To specify which domains on the SmarterMail are archived, the system administrator will need to create archiving rules. In addition, if the system administrator wants to allow individual domain administrators to search their domain's message archive then individual rules need to be set up for each domain. Setting the message archiving rules to "all domains" means only the system admin will be able to access message archive and search for messages on the mail server.

When archiving is set up, messages are automatically archived as soon as they hit the spool and before they are handled by any spam and/or content filters. This means that all messages are archived, not simply those that are delivered to a user's mailbox. (The exception to this rule is messages rejected due to SMTP Blocking. If a message is rejected due SMTP Spam blocking, it will never hit the spool and, therefore, will not be archived.) On a nightly basis, SmarterMail zips up archived messages and stores them to conserve disk space on the mail server. However, zipped messages are still searchable.

To view the message archiving rules for your SmarterMail installation, click the settings icon . Then expand Storage and click Message Archiving in the navigation pane. A list of archiving rules will load in the content pane.

To create a new archiving rule, click New in the content pane toolbar. To edit an existing rule, select the appropriate rule and click Edit in the content pane toolbar. The following options will be available:

• Domain - The domain on the SmarterMail server to be archived.

• Archive Path - The directory on the hard drive in which archived messages are saved.

- Rule - Choose to save none of your messages, all messages, only incoming messages or only outgoing messages.

Once email archiving is set up, both system administrators and domain administrators can search the archives. System administrators can only search across all domains whereas domain adminsitrators can search only within their own domain. NOTE: Please note that domain administrator search requires individual domain archiving rules to be set up, as noted above.

It is also important to know that archives are not deleted by SmarterMail and, as a result, they can get very large. Be sure to check your archive folders regularly to see if they should be backed up and removed from the hard drive.

Advanced Settings

Configuring SmarterMail for Failover

Who Should Use This

This document is intended for use by administrators deploying SmarterMail in high-volume environments and/or for organizations that want to ensure maximum uptime. It provides minimal system requirements and considerations for deploying SmarterMail in a failover environment. Note: Failover requires activation of SmarterMail Enterprise. For licensing information for this product, contact the SmarterTools Sales Department .

Failover Overview

SmarterMail Enterprise allows organizations to decrease the likelihood of service interruptions and virtually eliminate downtime by installing SmarterMail on a hot standby that is available should the primary mail server suffer a service interruption. For businesses that use their mail server as a mission-critical part of their operations, failover functionality ensures that the business continues to communicate and that productivity remains at the highest levels possible, even if there is a primary server failure.

Understanding How Failover Works

The main components of failover functionality are a primary server that acts as the default SmarterMail server and manages the licensing of the server cluster and a secondary server that remains connected and available in a “hot standby” mode until the primary server experiences problems with network access or system hardware.

If the primary server fails, SmarterMail can be configured to automatically enable the secondary server. When this occurs, the secondary server takes over responsibility for processing background

threads and supporting all email functionality. This server will remain in active status until another failure occurs or the primary mail server comes back online.

The initial set up of SmarterMail's failover functionality entails system administrators manually disabling both the node and SmarterMail service on the primary server and then starting the node and SmarterMail service on the hot standby. However, system administrators can easily use third-party monitoring systems and script an automated failover and recovery strategy as needed. An example of this is provided at the end of this document.

Minimal System Requirements

- A minimum of two servers running Microsoft Windows Server 2008 R2 or higher. (Windows Server Core is not currently supported).
- Three IP addresses
- Both servers must have their server times synchronized
- NFS/SMB share for mail and system files. We recommend that the share is running on a NAS/SAN that is configured as RAID 10

Adding Network Load Balancing to Your Servers

Note: This needs to be performed on each server that will be used in the failover environment.

- Open the server manager console
- Right click on Features in the tree view and select Add Features
- Check the box next to Network Load Balancing and select Next
- Click Install
- Once the installation finishes, click Close

Configuring the Load Balanced Cluster for Use with Failover

- Navigate to Start -> Administrative Tools -> Network Load Balancing Manager
- Click the Cluster menu item and select New
- In the New Cluster: Connect window, type the IP of your primary server in the Host: text box and select New
- When the Interface Name and Interface IP appear, select the Interface Name and click Next
- Since this is the primary node, ensure the host Priority is set to 1
- In the New Cluster: Host Parameters window, confirm the IP address and Subnet mask are correct and change the initial host state to Stopped . This is to prevent any issues with connectivity if a machine randomly reboots or suffers from a hardware failure. If all nodes are set to Started for their initial host state, traffic will be split between the two (or more) machines. Note: Monitoring software can be used to execute scripts that will start and stop hot standbys in

the event of a failure and recovery. If you are not executing scripts via monitoring software then all failover will need to be handled manually.

• Click Next

• In the New Cluster: Cluster IP Addresses window, click Add and enter in your cluster IP address and the same subnet mask as in Step 6

• Select Next

• In the New Cluster: Cluster Parameters window, confirm the IP address and subnet mask, then enter a Full Internet Name , though this is optional

• Ensure the cluster operation mode is set to Multicast

• Click Next

• In the New Cluster: Port Rules window, click Edit

• If you want you can restrict the cluster IP to work on an individual port or across a port range. You can also simply allow the cluster IP to work across all ports on the server

• Ensure your port rules are set to Single Host in the Filtering Mode section

• Click OK

• Verify your settings and click Finish to complete the setup

Joining Additional Nodes to the Cluster

• From the secondary server navigate to Start -> Administrative Tools -> Network Load Balancing Manager

• Click the Cluster menu item and select Connect to Existing . Note: the existing cluster will need to be running before a secondary node can be added

• In the Connect to Existing: Connect window, enter the IP address of your existing cluster as the Host and click Connect

• Select the existing cluster that appears in the Clusters section and click Finish

• In the main Network Load Balancing Manager , expand Network Load Balancing Clusters and right click on your Cluster (it may be the IP address of your cluster) and select Add Host to Cluster

• In the Add Host to Cluster: Connect window, enter the IP address of the secondary server in the Host: section and click Connect

• When the Interface Name and Interface IP appear, select the Interface Name and click Next

• In the Add Host to Cluster: Host Parameters window, confirm the IP address and subnet mask and ensure the Initial Host State is set to Stopped . As this is the second node you’re adding to your cluster, the Priority should be set at 2

• Click Next

• Just as with the primary node, in the Add Host to Cluster: Port Rules window you have the ability to set this node to respond via specific ports or a port range. If you wish to set these

rules, click Edit . Otherwise, click Finish to complete the setup

• Wait for the nodes to converge and, if necessary, stop the secondary sever by right clicking the second server's name, select Control Host -> Stop

Configure a Shared Service Directory

• Using Network File Sharing (NFS) or Samba (SMB), create a shared directory named SmarterMail , preferably on a NAS or SAN. NOTE: We recommend that this shared directory be hosted on a server that utilizes a RAID 10 configuration for the data.

• Inside that new SmarterMail folder, create a Service folder

• Configure your permissions accordingly. If special permissions are required, configure the SmarterMail service to run with the proper credentials within the Windows Services console. Note: When performing updates to the software, the credentials will need to be re-applied to the service

Configuring a Fresh Installation of SmarterMail for Failover

• Install SmarterMail Enterprise on a server. This will be your hot standby. Leave all setup information as the default settings and after setup is complete, configure SmarterMail as an IIS site.

• Stop the SmarterMail service on the hot standby

• Edit the failoverConfig.xml file in the primary server's Service folder as follows:

• SharedSystemFilesPath - Set to the shared network shared system folder

• FailoverIPAddress - Set this to the IP address of the Network Load Balancer

• IsEnabled - Set this to True

• Save this file, then copy it to the hot standby's Service folder and replace the existing failoverConfig.xm l

• Copy over all folders, DAT and XML files from C:\Program Files (x86)\SmarterTools\SmarterMail\Service to the Service folder in the shared service directory you created

• Start the service on the hot standby server and verify that the paths are pointing to the network shared paths

• Activate your Enterprise key on the hot standby by logging into SmarterMail's management interface as the system admin and going to Settings -> Activation -> Licensing , then stop the SmarterMail service on the server

• Start the service on the primary server, then reactivate your Enterprise license key in the SmarterMail management interface

• After re-activating the license, go to Settings -> Bindings -> IP Address and bind all the ports to the load balancer's IP address and make sure no other IPs have any ports bound to them

• Both servers are now set up for failover. To verify this, when logged into the primary server as the system admin, go to Settings -> Failover Servers to view the servers that are part of the failover cluster

Adding Failover to an Existing Installation of SmarterMail

Note: You will need to configure both servers for Network Load Balancing and set up a shared service directory. See the steps outlined in the Adding Network Load Balancing to Your Servers , Configuring the Load Balanced Cluster for Use with Failover , Joining Additional Nodes to the Cluster and Configure a Shared Service Directory sections earlier in this document for more information.

• Ensure the primary server is running the latest version of SmarterMail and that it is also configured as an IIS site. Ensure the IIS binding is pointing to your cluster IP address
• Install SmarterMail on a hot standby and configure it as an IIS site. Ensure the cluster node is stopped on the hot standby and ensure the IIS binding is also pointing to the cluster IP
• Stop the SmarterMail service on the hot standby
• Copy all of your mail data (located in C:\SmarterMail\ by default) to your shared service directory. If possible, use robocopy to do this because it will not result in any downtime for the mail service
• Once robocopy finishes, run it one more time. This second pass will only copy any new data
• Stop the SmarterMail service on the primary server
• Edit the failoverConfig.xml file in the primary server's Service folder as follows:

• SharedSystemFilesPath - Set to the shared network shared system folder
• FailoverIPAddress - Set this to the IP address of the Network Load Balancer
• IsEnabled - Set this to True
• Run the robocopy one more time to copy over any modified files and remaining spool e-mails
• Copy over all folders, DAT and XML files from C:\Program Files (x86)\SmarterTools\SmarterMail\Service to the Service folder in the shared service directory you created
• Edit the domainlist.xml file in the shared Service folder and change the path of your domains to match the new NFS\SMB path. (For example, \\NAS01\SmarterMail\Domains\mydomain.com)
• Edit the mailconfig.xml file and replace any instances of the old physical path's with your new network location for SmarterMail. (For example, if all of your data was hosted on E:\Smartermail, you would then perform a find and replace for all instances of E:\Smartermail to \\NAS01\Smartermail).
• On the primary server, go to Start -> Administrative Tools -> Network Load Balancing Manager and stop the cluster node, then start the NLB on the secondary node

- Start the SmarterMail service on the hot standby
- Access SmarterMail's web interface at the cluster IP and sign in as the system admin
- Activate your Enterprise key on the hot standby by going to Settings -> Activation -> Licensing
- Verify that the data and settings are being picked up from the shared Service directory
- Stop the SmarterMail service on the hot standby and stop the secondary cluster node
- Start the cluster node and the SmarterMail service on the primary server
- Sign into the web interface on the primary server and re-activate the Enterprise license key by going to Settings -> Activation -> Licensing
- Verify mail data and settings are being accessed from the shared service directory

Scripting Failover

Below is an example of a PowerShell script that can be created to automate the SmarterMail failover process. You can utilize a third party monitoring product such as PRTG or SolarWinds (though there are many others) to execute this script when a failure is detected.

Prepping PowerShell on the Servers

The servers will need to be configured to run remote scripts and accept remote PowerShell sessions. Therefore, on each server, run the following commands within an elevated PowerShell console:

- Set-ExecutionPolicy RemoteSigned - Press Y to accept
- Enable-PSRemoting -force

Sample Script - Stop a Primary Server and Start the Hot Standby

In the scripts below, replace the "WAN" variable called in the –hostname parameter with the name of your interface. This can be obtained by opening a PowerShell console on the server and typing Get-NlbClusterNodeNetworkInterface . Also replace Server01 and Server02 with the NetBIOS names of your servers.

```
$StopPrimary = New-PSSession -ComputerName Server01 Invoke-Command -Session $StopPrimary -ScriptBlock { Import-Module NetworkLoadBalancingClusters ; Stop-nlbclusternode -HostName Server01 -InterfaceName "WAN" ; import-module WebAdministration ; stop-webapppool SmarterMail; set-service -computerName Server01 -name mailservice -status stopped ; remove-pssession Server01}
```

```
$StartSecondary = New-PSSession -ComputerName Server02 Invoke-Command -Session $StartSecondary -ScriptBlock { Import-Module NetworkLoadBalancingClusters ; Start-nlbclusternode -HostName Server02 -InterfaceName "WAN" ; set-service -computerName Server02 -name mailservice
```

```
-status running ; import-module WebAdministration ; start-webapppool
SmarterMail ; remove-pssession Server02 }
```

Sample Script - Stop the Hot Standby and Re-start the Primary Server

These scripts can be used to bring the primary server back online and stop the hot standby after your monitoring software issues an all-clear.

```
$StopSecondary = New-PSSession -ComputerName Server02 Invoke-Command -
Session $StopSecondary -ScriptBlock { Import-Module
NetworkLoadBalancingClusters ; Stop-nlbclusternode -HostName Server02 -
InterfaceName "WAN" ; import-module WebAdministration ; stop-webapppool
SmarterMail; set-service -computerName Server02 -name mailservice -status
stopped ; remove-pssession Server02}
```

```
$StartPrimary = New-PSSession -ComputerName Server01 Invoke-Command -
Session $StartPrimary -ScriptBlock { Import-Module
NetworkLoadBalancingClusters ; Start-nlbclusternode -HostName Server01 -
InterfaceName "WAN" ; set-service -computerName Server01 -name mailservice
-status running ; import-module WebAdministration ; start-webapppool
SmarterMail ; remove-pssession Server01 }
```

Message Footer

System administrators can configure server-wide message footers that SmarterMail will append on all incoming and outgoing messages. Although similar to signatures, message footers are typically used to convey disclaimers or provide additional information. For example, a system administrator may want every message to include a notice that the message was scanned for viruses or the text "Sent by SmarterMail."

To access the message footer options, click the Settings icon , expand the Advanced Settings folder in the navigation pane and click on Message Footer . The message footer settings will load in the content pane and the following tabs will be available:

Options

Use this tab to specify the following settings:

- Enable footer for all messages - Select this option to turn on the message footer for all incoming and outgoing messages.
- Apply to mailing lists - Select this option to append the message footer to mailinglist messages. Note: Mailing lists have their own configurable footers, so enabling this option will append a second footer at the end of each message. Because this may be confusing for mailing

list moderators and recipients, most administrators will choose to keep this option disabled.

• Enable domains to override footer settings - Select this option to allow domain administrators to configure their own message footer for the domain.

Footer

Use this tab to create the message footer text. Admins can use the HTML-based editor to create footers that seamlessly fit into any email message. Note: The message footer does not support the use of variables.

Automation with Web Services

SmarterMail was built with custom configuration in mind. In addition to being able to customize the look and feel of SmarterMail, developers and/or system administrators have the ability to code to the SmarterMail application using several different Web services. These Web services allow developers and/or system administrators to automate a variety of different things: add domains to SmarterMail on the fly, grab domain-specific bandwidth usage for billing purposes, set details on a specific domain or server, update domain information, test servers added to the Web interface, and more.

The Automation with Web Services documentation may include services that have not been released to the public yet or are not available in the version you are using. For the most accurate Web services information, log into SmarterMail as the system administrator and click the settings icon . Then click Web Services in the navigation pane.

Note: Web services are intended for use by high-volume and automated businesses environments and hosting companies as they develop procedures tmanage their SmarterMail system and work flow. In addition, this document assumes a basic understanding of Web service technologies and ASP.NET programming.

Activation

Licensing

System administrators can use this area to view licensing information,

To access view licensing information for SmarterMail or any add-ons, click the settings icon . Then expand the Activation folder and click Licensing in the navigation pane. The edition, version, and license level information for the version of SmarterMail currently being used will load in the content pane. The licensing information for any add-ons will also display in the content pane.

The following options are available from the content pane toolbar:

- Activate - Activates a new SmarterMail license key.
- Reactivate - Reactivates a SmarterMail license key. License keys should be reactivated if you purchase add-ons or change the product edition or level.
- Details - Displays details about the license, including feature, status, expiration, limits and available trials.
- Buy Now - Allows the system administrator to purchase a new license key or add-on.
- Start Trial - Allows the system administrator to begin an available add-on trial. Trials for add-ons are limited to 30 days, after which the add-on needs to be purchased or it will no longer function.

Note: If you are running a trial version of SmarterMail, it will automatically revert to SmarterMail Free when the trial expires. This will be reflected in the licensing details.

SmarterMail Self Diagnostic

Use the SmarterMail Self Diagnostic to test your SmarterMail server for errors. To access this feature, click the settings icon . Then expand the Activation folder and click SmarterMail Self Diagnostic in the navigation pane. SmarterMail will perform a test and display the results in a popup window.

Security

Antispam Administration

SmarterMail comes equipped with a number of antispam features and functions that allow you to be as aggressive as you want when combatting spam. Initial antispam settings were configured during installation, but these settings can be modified at any time. Without having to add any third-party measures, SmarterMail's antispam features can rid mail servers of up to 97% of all spam just using the standard configuration when it's installed.

Due to the flexible nature of SmarterMail's antispam setup, spam checks can influence the spam decision as much or little as you want. When spam protection runs on a particular email, all enabled spam checks are performed on the email. The total weight of all failed tests is what comprises the spam weight for the email. A spam probability level is then assigned to the email using the settings in the Filtering tab and an action is taken on that message based on its total spam weight.

An added benefit to SmarterMail's Antispam Administration is the ability to combat both incoming and outgoing spam messages. Most mail servers only allow system administrators to keep spam from entering the mail server. SmarterMail helps protect mail users from incoming spam but also includes

the added benefit of keeping mail servers from actually sending spam, thereby helping to protect the mail servers from being blacklisted.

To view the antispam settings for your server, click the Security icon and then click Antispam Administration in the navigation pane. The antispam settings will load in the content pane and the following tabs will be available:

Spam Checks

Use this tab to select the spam options that you want to enable for filtering (a point-based weighting system for filtering spam) and for blocking at the SMTP level. Weights can also be edited for the various checks from this tab. Note: Only enabled spam checks are used when calculating spam weight. To enable or disable a check, select the appropriate spam check by checking the box next to it and click Save .

The following options will be available from the content pane toolbar:

- Save - Select this option to preserve any changes made to the spam check.
- Actions - Select an appropriate action from the list:

- Wizard - Select this option to open the Getting Started Wizard in a new tab for quick spam setting adjustments. Note: Only the Spam Profiles and Security options will be displayed.
- Import Spam Settings - Select this option to import the spamConfig.xml file for quick spam setting adjustments. This option allows administrators to easily share spam configurations across all installations within their infrastructure. Note that when importing spam configurations, all existing rules will be replaced with the rules in the imported XML.
- Export Spam Settings - Select this option to export the spamConfig.xml file from the server files. This option allows administrators to easily share spam configurations across all installations within their infrastructure.
- Add RBL - Select this option to create an RBL spam check.
- Add URIBL - Select this option to create a URIBL spam check.
- Edit - Checkmark a spam check from the list and select this option to adjust its settings.
- Delete - Select this option to permanently remove the spam check.

The following columns are available for each spam check:

- Spam Check - The name of the spam check available.
- Avg. Time - The average time, in milliseconds, that the spam check takes to process.
- Weight - The weight range available for the spam check.
- Enable for Filtering - When checked, the weight assigned for the spam check is added to the message and used as part of its overall spam score. SmarterMail then handles the message based

on the spam settings created for a domain.

• Enable for Incoming SMTP blocking - Checking this box enables the spam check for SMTP blocking of incoming emails. If N/A is listed, then that particular spam check relies on content filtering and does not offer SMTP blocking. As SMTP blocks are done at the IP level and not based on message content, some spam checks do not offer SMTP blocking.

• Enable for Outgoing SMTP blocking - Checking this box enables the spam check for SMTP blocking of outgoing emails. If N/A is listed, then that particular spam check relies on content filtering and does not offer SMTP blocking. As SMTP blocks are done at the IP level and not based on message content, some spam checks do not offer SMTP blocking.

The following types of spam checks are available by default. In most cases, selecting the desired spam check and clicking Edit will allow you to set any properties associated with the check.

Custom Rules

Email can be assigned spam weights based on the header, body text or raw content of a message. For example, the system administrator can create a rule that assigns a specific spam weight to all messages containing the word "viagra" in the body text. To configure weights for custom body rules, complete the following fields:

• Rule Name - The name of the rule.

• Rule Source - What you want the rule to be based on: a message's header, body text or raw content. Note: If you select Header you will need to supply header details separately from the Rule Text .

• Rule Type - The type of rule you use to evaluate the text for a match. Rule types are contains, wildcard or regular expression.

• Weight - The amount to add to the email message's spam weight.

• Rule Text - The text that triggers the custom body rule.

Cyren Premium Antispam

The Cyren Premium Antispam add-on uses Recurrent Pattern Detection technology to protect against spam outbreaks in real time as messages are mass-distributed over the Internet. Rather than evaluating the content of messages, the Cyren Detection Center analyzes large volumes of Internet traffic in real time, recognizing and protecting against new spam outbreaks the moment they emerge. For more information, or to purchase this add-on, visit the SmarterTools website .

• Confirmed Weight - The weight that will be assigned if the Cyren Detection Center determines the message as coming from known spam sources.

• Bulk Weight - The weight that will be assigned if the Cyren Detection Center determines the message as sent in bulk. Note: Newsletters or mailing list messages may be included in this

classification.

• Suspect Weight - The weight that will be assigned if the Cyren Detection Center suspects the message may be spam because it was sent to a slightly larger than average distribution.

• Unknown Weight - The weight that will be assigned if the Cyren Detection Center is unable to determine the spam probability of a message. This should be treated similarly to a None Weight.

• None Weight - The weight that will be assigned if the Cyren Detection Center deems the message as not spam.

Declude

Declude integration allows you to use Declude products in conjunction with the SmarterMail weighting system. Declude addresses the major threats facing networks, and are handled by a multi-layered defense. Configuration of Declude is done through the Declude product, so all you need to do in SmarterMail is enable the spam check and the Declude score will be included when calculating the total spam weight of a message. For more information, visit www.declude.com .

• Low Spam Weight - The weight that will be assigned if Declude determines a low probability of spam.

• Medium Spam Weight - The weight that will be assigned if Declude determines a medium probability of spam.

• High Spam Weight - The weight that will be assigned if Declude determines a high probability of spam.

DomainKeys and DKIM

DomainKeys and DKIM are an email authentication system designed to verify the DNS domain of an email sender and the authenticity of a message. While a possible source for determining whether an email is spam or not, neither is universally adopted so any weights assigned for failing these checks should be minimal. In addition, because the DomainKey method has become obsolete; we recommend utilizing DKIM instead.

• Pass Weight - Indicates that the email sender and message integrity were successfully verified (less likely spam). The weight you set may be 0 (for no effect) or a negative number, thereby reducing the spam rating.

• Fail Weight - Indicates that the email sender and message integrity verifications failed (most likely spam). Set this to a relatively high weight, as the probability that the email was spoofed is very high.

• None Weight - Indicates that there was not a valid DomainKey/DKIM signature found to validate the sender and message integrity. Except in very special circumstances, leave this set to 0.

• Max message size to sign - The maximum outgoing message size you want the mail server to sign. By default this is set to 0, meaning all outgoing messages are signed.
• Max message size to verify - The maximum incoming message size you want the mail server to verify.
• Max key size allowed - Select the level of security you want used to sign each message. Default is set to 1024 bits. Setting this value higher may increase the CPU load on your mail server.

Message Sniffer

The Message Sniffer add-on is an intelligent antispam scanner that uses advanced pattern recognition and collaborative learning technologies to accurately identify spam, scams, viruses, and other email borne malware before it gets to a user□s mailbox. For more information, or to purchase this add-on, visit the SmarterTools website .

• Confirmed Weight - The weight that will be assigned if Message Sniffer determines the message as coming from known spam sources.
• None Weight - The weight that will be assigned if Message Sniffer deems the message is not spam.

RBL Lists (Real-Time Blacklists)

RBL lists (also known as IP4R Lists) and URIBL lists are publicly accessible lists of known spammer IP addresses. These lists can be a very important part of spam protection. To attach a list click either Add RBL or Add URIBL in the content pane toolbar. Dependent on the list you□re adding, the following settings are available:

• Name - A friendly name for the list that will help you and your customers identify it.
• Description - This field allows you to store additional information about the list.
• Weight - The default weight for this spam check. If an email sender is listed with the spam list, this is the value that will be added to the message's total spam weight.
• Max Weight - The maximum weight that a single URIBL check can add to the message.
• Hostname - The hostname of the RBL.
• Required Lookup Value(s) - The expected value(s) returned from an RBL if the sender's IP is listed with the RBL provider. Note: Multiple lookup values may be entered, separated by a comma.
• Enable bitmap checking - Select this checkbox if the RBL supports bitmapping. Bitmap checking can be used for RBL□s and URIBL□s that support this kind of spam check. For example, SURBL utilizes a multi-blacklist check. For more information and documentation on the appropriate usage, please visit www.surbl.org/lists .

Remote SpamAssassin

SpamAssassin itself is a powerful, third party open source mail filter used to identify spam that can be easily used alongside SmarterMail. It utilizes a wide array of tools to identify and report spam. By default, SpamAssassin will run on 127.0.0.1:783. For more information, or to download SpamAssassin, visit spamassassin.apache.org .

SmarterMail can use SpamAssassin with its weighting system:

- Low Spam Weight - The weight that will be assigned if SpamAssassin determines a low probability of spam.
- Medium Spam Weight - The weight that will be assigned if SpamAssassin determines a medium probability of spam.
- High Spam Weight - The weight that will be assigned if SpamAssassin determines a high probability of spam.
- Client Timeout - The timeout that SmarterMail will impose on a server if it cannot connect.
- Max Attempts per Message - The number of times SmarterMail will attempt to acquire a SpamAssasassin score for an email.
- Failures Before Disable - The number of times a remote SpamAssassin server can fail before it is disabled.
- Disable Time - The length of time before the SpamAssassin server is re-enabled.
- Header Log Level - The amount of information SpamAssassin inserts into the header of the message

Reverse DNS (Domain Name Server)

Reverse DNS checks to make sure that the IP address used to send the email has a friendly name associated with it.

- Weight - The default weight for this spam check. If an email sender does not have a reverse DNS entry, this is the value that will be added to the message's total spam weight.

SmarterMail's SpamAssassin-Based Pattern Matching

SmarterMail includes a proprietary pattern matching engine built upon the SpamAssassin technology as part of the default installation of the product. It includes a number of spam detection techniques, including DNS-based and fuzzy-checksum-based spam detection, Bayesian filtering and more.

- Low Spam Weight - The weight that will be assigned if the pattern matching engine determines a low probability of spam.
- Medium Spam Weight - The weight that will be assigned if the pattern matching engine determines a medium probability of spam.

• High Spam Weight - The weight that will be assigned if the pattern matching engine determines a high probability of spam.
• Header Log Level - The amount of information the pattern matching engine inserts into the header of the message.

SPF (Sender Policy Framework)

SPF is a method of verifying that the sender of an email message went through the appropriate email server when sending. As more and more companies add SPF information to their domain DNS records, this check will prevent spoofing at an increasing rate.

• Pass Weight - Indicates that the email was sent from the server specified by the SPF record (more likely good mail). The weight you set may be 0 (for no effect) or a negative number, thereby reducing the spam rating.
• Fail Weight - Indicates that the email was sent from a server prohibited by the SPF record (highly likely spam). Set this to a relatively high weight, as the probability that the email was spoofed is very high.
• SoftFail Weight - Indicates that the email was sent by a server that is questionable in the SPF record. This should either be set to 0 or a low spam weight.
• Neutral Weight - Indicates that the SPF record makes no statement for or against the server that sent the email. Except in very special circumstances, leave this set to 0.
• PermError Weight - Indicates that there is a syntax error in the SPF record. Since SPF is relatively new, some domains have published improperly formatted SPF records. It is recommended that you leave this at 0 until SPF becomes more widely adopted.
• None Weight - Indicates that the domain has no published SPF record. Since SPF is relatively new, many legitimate domains do not have SPF records. It is recommended that you leave this at 0 until SPF becomes more widely adopted.

Filtering

Emails are filtered into one of three categories based on their total weight: Low Probability, Medium Probability and High Probability. If a weight is equal to or higher than a certain category, then it is assigned that probability of being spam. Use the Default Action option to define the weight thresholds and the default actions at each level. Note: Users can override these settings if you permit them to.

• Weight Threshold - The email is sorted into probability levels based on the weight threshold values.
• Default Action - The action to take when a message ends up with this probability.
• Text to Add - This is the text that will be displayed when a message reaches a particular level of spam.

SMTP Blocking

This tab allows you to set up extra spam checks that block emails at delivery if a certain amount of spam checks fail. Use the Enabled checkbox to enable a particular SMTP block. Note: Messages rejected due to SMTP blocking do not hit the spool and, therefore, will not be included in the message archive, if enabled.

- Incoming Weight Threshold - Enable this and an incoming email must score this value or higher in order to be blocked. The score is established by the settings on the Spam Checks tab. (Default is 30)
- Greylist Weight Threshold - Enable this and an incoming email must score this value or higher to be greylisted. (Default is 30)
- Outgoing Weight Threshold - Enable this and an outgoing email must score this value or higher in order to be blocked. The score is established by the settings on the Spam Checks tab. (Default is 30)
- Outgoing Quarantine - The amount of time to quarantine blocked SMTP messages.

Options

This tab contains options relating to the processing of spam and the ability for individual domains to override system-level settings.

- Auto Responders - Allows you to restrict what types of automated responses are permitted for the system. Certain anti-spam organizations are starting to block those servers that auto-respond to spam traps. To reduce the possibility of this occurring, set the auto-respond option to be as restrictive as your clients will permit.
- Content Filter Bouncing - As with auto-responses, certain anti-spam organizations also blacklist those servers that send bounce messages back to spam trap accounts. SmarterTools recommends setting this option to be as restrictive as your clients will allow.
- Max message size to content scan - The maximum message size for which content-based spam checks will run. Content-based spam checks include the SpamAssassin-based Pattern Matching Engine, remote SpamAssassin, Cyren Premium Antispam, and custom rules. Note: Increasing this number will also increase the mail server's memory usage.
- Allow domains to override filter weights and actions - Many domain administrators have their own opinions on what spam checks work best for their domain. Enable this to allow them to override the spam options if they wish.
- Enable bounces for outgoing SMTP blocking - Enable this to give a user a notification when a mail message has not been sent due to spam.
- Enable spool proc folder - Enable this to have SmarterMail place messages into this folder to

be analyzed in the background. While the messages are in the Spool Proc folder, .hdr can manipulate elements of the message, such as edit, write, and add headers. Once the scan has been completed, the message will be placed back into the spool and handled by SmarterMail from that point on.

• Disable spam filtering on SMTP whitelisted IP addresses - Disables antispam processing and zeroes the spam weight on whitelisted IPs.

• Enable catch-all accounts to send auto-responders and bounce messages - Enable this if you rely on auto-responders being sent when a message comes in through a catch-all. In general, this is a bad idea, so it should be left unchecked unless your situation specifically requires it.

• Enable SRS when forwarding messages - Enable this to allow the mail server to re-email (as opposed to "forward") an email message so that it passes any SPF checks on the recipient's end.

• Enable DMARC policy compliance check - Enable this to allow the mail server to check messages against the DMARC policy standard. For more information, see the DMARC website .

Bypass Gateways

This tab gives administrators the ability to enter an IP Address or an IP Range of an incoming gateway. SmarterMail will analyze the .EML file and pull the most recent IP Address from the header which will usually be an organizations incoming gateway. By inputting that IP Address on this page will allow SmarterMail to analyze the IP of the originating server rather than focusing on the gateway that SmarterMail received the message from. This is important because the majority of the time an organizations incoming gateway will not be listed on any RBL lists, but the originating server may be.

To add an IP Address or IP Range, click the Add IP icon from the Actions toolbar.

Antivirus Administration

SmarterMail's default installation includes, at no additional cost, effective and self-updating antivirus protection with ClamAV. In addition, SmarterMail can support additional third-party solutions that include a quarantine directory as well as support for command-line antivirus solutions. SmarterMail has the ability to check the quarantine directory and respond to users that attempted to send an email containing a virus.

To view the antivirus settings for your server, click the security icon and then click Antivirus Administration in the navigation pane The antivirus settings will load in the content pane and the following tabs will be available:

Options

- Virus Quarantine - Allows you to specify the amount of time you want to quarantine any detected viruses.
- Enable ClamAV - Select this checkbox to enable ClamAV.
- Enable real-time AV - Select this checkbox to enable virus checking in real-time.
- Enable command-line AV - Select this checkbox to enable a command-line virus scanner.
- Enable Cyren zero-hour antivirus - Select this checkbox to enable the Cyren Zero-hour Antivirus add-on.

ClamAV

Clam AntiVirus is a third-party open source antivirus toolkit, designed especially for scanning email on mail gateways. ClamAV is included at no additional cost in the default installation of SmarterMail. For more information on ClamAV, visit: www.clamav.com

- IP Address - The IP address of the ClamAV server to use.
- Port - The port that the ClamAV server is listening on.
- Remote Server - Select this checkbox if the server is a remote server.
- Timeout - The maximum number of seconds SmarterMail should wait for ClamAV to respond before moving on to the next message. By default, the timeout is 10 seconds.
- Failures Before Disable - The maximum number of ClamAV timeouts allowed before it is disabled. By default, ClamAv is limited to 5 failures.
- Virus Definitions - The date and time the virus definitions were last updated. The definitions are updated whenever the service starts and every 6 hours thereafter.

Command-line AV

- Command Line - The command that you want to execute. %FILEPATH will be replaced with the path to the file to be scanned.

Cyren Zero-hour Antivirus

The Cyren Zero-hour Antivirus add-on uses Recurrent Pattern Detection technology to identify viruses based on their unique distribution patterns and provides a complementary shield to conventional AV technology, protecting in the earliest moments of malware outbreaks and continuing protection as each new variant emerges.

Cyren evaluates each message and determines the probability that the message contains a virus. System administrators can choose the default action taken on a message when Cyren determines the it

has a medium, high, or definite probability of containing a virus. For more information, or to purchase this add-on, visit the SmarterTools website .

Greylisting

What is Greylisting and how does it work?

Greylisting has proven itself to be an effective method of spam prevention. When enabled, the system will keep track of the sending IP address, sending email address and recipient's email address for every message received. If an incoming message has a combination of a sending IP, sending address and recipient address that has not previously been seen, it will return a temporary failure to the sending server, effectively saying, "Try again later." Valid servers will retry the email a short time later, which would be permitted. Spammers, on the other hand, typically create scripts that bombard your server with emails, and they rarely retry on temporary failures. When these messages are bounced back because of greylisting, they are typically not retried, therefore reducing the amount of spam that your customers receive. (Emails sent from whitelisted and authenticated senders will automatically bypass greylisting and are delivered directly to the spool.)

For those messages that are sent from valid email servers, the sending server should retry at least four times. If the first retry is beyond the block period (default 15 minutes) and within the pass period (default 6 hours), the message is passed to the spool and it goes through its normal processing without a delay. A record is also created that says this is a valid email address from that server to the given recipient and keeps it for 36 days (default). If another email from the same email address is received from the same server to the same recipient within the 36 days, the clock is reset for an additional 36 days and delivered directly to the spool.

Why use Greylisting?

Greylisting is a very effective method of spam blocking that comes at a minimal price in terms of performance. Most of the actual processing that needs to be done for Greylisting takes place on the sender's server. It has been shown to block upwards of 95% of incoming spam simply because so many spammers don't use a standard mail server. As such, spam servers generally only attempt a single delivery of a spam message and don't reply to the "try again later" request.

How do I set up Greylisting?

Note: You must be a system administrator to change greylisting settings.

In order to set up Greylisting, click the security icon and click Greylisting in the navigation pane. The greylisting settings will load in the content pane and the following tabs will be available:

Options

Use this tab to specify the following settings:

- Block Period - The period of time (in minutes) that mail will not be accepted (default 15 minutes).
- Pass Period - The period of time (in minutes) in which the sender's mail server has to retry sending the message (default 360 minutes).
- Record Expiration - The period of time(in days) that the sender will remain immune from greylisting once it has passed (default 36 days).
- Apply To - Select who greylisting applies to.
- Enable greylisting - Select this option to enable greylisting.
- Enable users to override greylisting - Select this option to allow users to selectively turn off greylisting (useful if you have an account that receives time sensitive mail).
- Greylist if the country for the IP address is unknown - Select this option to greylist messages when the country cannot be identified for the IP address. System administrators should note that the following cases are exempt from greylisting:

- Whitelisted IPs for SMTP or Greylisting
- Anyone who authenticates (includes SMTP Auth Bypass list)
- Trusted senders
- Anyone who has already sent you an email. Note: This list generates only after greylisting has been enabled.
- Any IP in the greylistBypass.xml file

Filters

If you set the grelisting "Apply To" setting to "Everyone except specified coutries / IP addresses" then you are able to add filters based on the countries or IP addresses you want to exclude from being greylisted.

Disadvantages of Greylisting

The biggest disadvantage of Greylisting is the delay of legitimate e-mail from servers not yet verified. This is especially apparent when a server attempts to verify a new user's identity by sending them a confirmation email.

Some e-mail servers will not attempt to re-deliver email or the re-delivery window is too short. Whitelisting can help resolve this.

Blacklist / Whitelist

System administrators are able to control the IP addresses that are blacklisted or whitelisted from accessing mail services. Blacklisting an IP address prevents it from making incoming connections, while whitelisting an IP address adds the IP as a trusted source, allowing connections to bypass relay restrictions that may be imposed. Exercise caution when granting whitelist status to a server, and be sure that you know what services on that server may send mail through your own.

To manage the blacklist or whitelist, click the Security icon and then click Blacklist or Whitelist in the navigation pane.

To create a new entry in the blacklist or whitelist, click New in the content pane toolbar. To edit an entry, click Edit in the content pane toolbar. The blacklist or whitelist settings will load in a popup window and the following options will be available:

- IP Address - Enter a single IP address in dotted quad notation (X.X.X.X) in this box if you want to add only a single IP (ex: 192.168.1.26).
- IP Range - Enter a range of IP addresses in the two boxes, and all IP addresses that are contained in the range will be added (ex: 192.168.1.1 - 192.168.1.255).
- Protocol - Check the boxes for the protocols you wish to include in the blacklist or whitelist entry. The available options are: SMTP, POP, IMAP, XMPP and Disable greylisting. (Disabling greylisting is only available when whitelisting an IP address, and, if checked, the whitelisted IP will not be greylisted.
- Description - Use this field to enter optional notes for understanding the various whitelist / blacklist entries.

Note: SmarterMail runs a check against the IPs listed in whitelist, blacklist and authentication bypass settings. This check looks at the number of IPs listed and will display a warning if the IPs listed represent a significant number. (E.g., a range greater than a /24.) While the warning does not affect the ability to save the settings, it is an indication that the administrator may want to review the settings prior to adding the IP range.

Blacklist / Whitelist

System administrators are able to control the IP addresses that are blacklisted or whitelisted from accessing mail services. Blacklisting an IP address prevents it from making incoming connections, while whitelisting an IP address adds the IP as a trusted source, allowing connections to bypass relay restrictions that may be imposed. Exercise caution when granting whitelist status to a server, and be sure that you know what services on that server may send mail through your own.

To manage the blacklist or whitelist, click the Security icon and then click Blacklist or Whitelist in the navigation pane.

To create a new entry in the blacklist or whitelist, click New in the content pane toolbar. To edit an entry, click Edit in the content pane toolbar. The blacklist or whitelist settings will load in a popup window and the following options will be available:

- IP Address - Enter a single IP address in dotted quad notation (X.X.X.X) in this box if you want to add only a single IP (ex: 192.168.1.26).
- IP Range - Enter a range of IP addresses in the two boxes, and all IP addresses that are contained in the range will be added (ex: 192.168.1.1 - 192.168.1.255).
- Protocol - Check the boxes for the protocols you wish to include in the blacklist or whitelist entry. The available options are: SMTP, POP, IMAP, XMPP and Disable greylisting. (Disabling greylisting is only available when whitelisting an IP address, and, if checked, the whitelisted IP will not be greylisted.
- Description - Use this field to enter optional notes for understanding the various whitelist / blacklist entries.

Note: SmarterMail runs a check against the IPs listed in whitelist, blacklist and authentication bypass settings. This check looks at the number of IPs listed and will display a warning if the IPs listed represent a significant number. (E.g., a range greater than a /24.) While the warning does not affect the ability to save the settings, it is an indication that the administrator may want to review the settings prior to adding the IP range.

SMTP Authentication Bypass

SMTP Authentication is a security measure that can be very beneficial in the fight against spam and unauthorized email as it forces the sender to authenticate their username and password before an email is sent through the mail server.

Unfortunately, some applications do not have support for SMTP authentication when sending mail. Most often, these are web sites that have automated mail sending mechanisms. The solution is to add the IP addresses of these servers/sites to SmarterMail's SMTP Authentication Bypass. Any IP address entered into this page will not be asked to provide an SMTP Authentication login. In this list you can see all IP addresses that are bypassing SMTP Authentication.

To get started, click the security icon and click SMTP Authentication Bypass in the navigation pane. A list of bypasses IP addresses will load in the content pane and the following options will be available in the content pane toolbar:

- New - Adds a new IP address or IP Address Range to bypass.
- Edit - Edits the selected IP address.
- Delete - Permanently removes the IP address from the SMTP authentication bypass list.

Trusted Senders

This section allows system administrators to exempt specific email addresses (such as jsmith@example.com) or domains (such as example.com) from SmarterMail's spam filtering. This can prevent mail from friends, business associates and mailing lists from being blocked and lets the system know that these messages come from a trusted source.

To view the trusted senders list for the server, click the security icon and click Trusted Senders in the navigation pane. A list of trusted senders will load in the content pane and the following options will be available in the content pane toolbar:

- New - Creates a new trusted sender.
- Edit - Edits an existing trusted sender.
- Delete - Permanently deletes the selected trusted sender(s).

Server Blacklist Checker

Knowing when a mail server is listed by one of the realtime black lists (RBL) SmarterMail incorporates into its various spam checks used to mean system administrators would have to log in to various websites and perform manual checks of their domains and/or IP addresses. However, with the Server Blacklist Check, these checks are performed automatically for all IP addresses added to a SmarterMail server so system administrators know if a server is actively blacklisted. Once a day, SmarterMail checks all of the RBLs available by default for any server IP addresses (besides localhost), regardless of whether the RBL is actively being used as a spam check. If the RBLs come back showing an IP as blacklisted, it changes that IPs blacklist status from False to True on the Server Blacklist page. System administrators are advised to set up Blacklist Status Changed system events that will immediately notify them if a server becomes listed by a RBL.

To access the Server Blacklist Check, click the Security icon and then click Server Blacklist Check . A list of IP addresses on the server will load in the content pane and the following columns will appear in the content pane:

- IP Address - The IP address used for a domain, or for several domains, on that mail server.
- Spam Check - The name of the RBL or URIBL that is being used.
- Blocked - If the IP is blocked by the specific spam check, this column will say True . If the IP

address is NOT blocked, this will say False .

• Change - The last date and time the IP was checked against the specific list.

Advanced Settings

Abuse Detection

SmarterMail has several methods of preventing abuse and denial of service (DoS) attacks. The ones that can be configured are explained below. Any number of detection methods can be added.

To view the configurable abuse detection settings, click the security icon . Then expand the Advanced Settings folder and click Abuse Detection in the navigation pane. A list of abuse detection rules will load in the content pane and the following options will be available in the content pane toolbar:

• New - Creates a new abuse detection rule.

• Edit - Edits the selected abuse detection rule.

• Delete - Permanently deletes the selected abuse detection rule(s).

• Wizard - Displays the Abuse Detection section of the SmarterMail setup wizard, which offers the following preset security options:

• Do not change abuse detection settings

• Relaxed abuse detection (Includes: DoS, SMTP Brute Force)

• Strict abuse detection (Includes: DoS, SMTP Brute Force, Email Harvesting, Internal Spammer Notifications, Bounces Indicate Spammer)

To create a new abuse detection rule, click New in the content pane toolbar. The abuse detection settings will load in the content pane and the following options will be available:

Denial of Service (DoS) - Too many connections from a single IP address can indicate a Denial of Service (DoS) attack. Enable this option to block IPs that are connecting too often to the server. It is recommended that you whitelist any trusted IP addresses that may send out large mailing lists or make many connections if you enable this option.

• Service - Select the service that will be monitored for this type of attack (SMTP/IMAP/POP/XMPP/LDAP).

• Time Frame - The period of time in the past that is examined to determine if an IP address should be blocked. Too many connections in this period of time, and a block will be initiated.

• Connections Before Block - The number of connections before a block is placed. It is common for several connections to be open at once from an IP address. Set this to a relatively high value so that you can catch DoS attacks while not impacting legitimate customers.

• Time to Block - The number of minutes that a block will be placed once an IP address hits the

threshold.

• Description - A friendly name or brief description of the rule.

Bad SMTP Sessions (Harvesting) - A bad session is any connection that ends without successfully sending a message. Many bad sessions usually indicate spamming or email harvesting. Leaving all of these options set to 0 (zero) will disable this type of abuse detection. Note: It is recommended that you whitelist any trusted IP addresses that may send out large mailing lists if you enable this option.

• Time Frame - The period of time in the past that is examined to determine if an IP address should be blocked. Too many bad sessions in this period of time, and a block will be initiated.

• Bad Sessions Before Block - The number of bad sessions before a block is placed. A few bad sessions happen once in a while, for instance when a person sends an email to an email account that does not exist. It is not these people that you are targeting, but rather those that are attempting to compromise or harass your customers.

• Time to Block - The number of minutes that a block will be placed once an IP address hits the threshold.

• Description - A friendly name or brief description of the rule.

Internal Spammer - Enabling this rule in SmarterMail will block or quarantine an account from sending mail, as well as alert an administrator, whenever multiple emails from a single sender are received on the server during a specified time frame.

• Action - Choose whether to send a notification email only, block messages from the sender or quarantine messages from the sender.

• Time Frame - The period of time in the past that is examined to determine if the rule triggers. Too many emails from a single sender in this period of time, and the email notification is sent and the Action chosen is performed.

• Messages Before Notify - After this many messages are received within the time period specified, the email notification is sent and the Action chosen is performed.

• Time to Block - The number of minutes that a block will be placed once an IP address hits the threshold.

• Email to Notify - The email address of the administrator account to which the notification will be sent.

• Description - A friendly name or brief description of the rule.

Password Brute Force by Protocol - A common ploy by spammers and hackers is attempting to guess passwords for users. Many times this entails continual log in attempts to an account using different passwords, each a bit different than the one before it. This thereby brute forcing the password.

- Service - Select the service that will be monitored for this type of attack (SMTP/IMAP/POP/XMPP/LDAP).
- Time Frame - The period of time in the past that is examined to determine if an login attempt is a brute force attempt. Too many connections in this period of time, and a block will be initiated.
- Connections Before Block - The number of failed login attempts before the IP is blocked.
- Time to Block - The number of minutes that a block will be placed once an IP address hits the threshold.
- Description - A friendly name or brief description of the rule.

Bounces Indicate Spammer - Enabling this rule in SmarterMail will block or quarantine an account from sending out mail, as well as alert an administrator, after receiving a certain number of bounce messages in the specified time frame.

- Action - Choose whether to send a notification email only, block messages from the sender or quarantine messages from the sender.
- Time Frame - The period of time in the past that is examined to determine if the rule triggers. Too many emails from a single sender in this period of time, and the email notification is sent and the Action chosen is performed.
- Bounce Threshold - After this many bounce messages are received within the time period specified, the email notification is sent and the Action chosen is performed.
- Time to Block - The number of minutes that a block will be placed once an IP address hits the threshold.
- Email to Notify - The email address of the administrator account to which the notification will be sent.
- Description - A friendly name or brief description of the rule.

Password Requirements

To ensure the security of the mail server and its mailboxes, system administrators can specify minimum requirements for user passwords. To access the password requirements settings, click the security icon . Then expand the Advanced Settings folder and click Password Requirements in the navigation pane. The password requirement settings will load in the content pane and the following options will be available:

- Minimum Password Length - The minimum number of characters the password must have.
- Password Expiration - The number of months that a password is valid. After the specified time, a user□soutgoing SMTP will be disabled and a password change will be forced upon Web interface login. Check the Enabled box to enable this setting. Note: If a user's 'Disable password

changes' setting is enabled, their password will not expire.

• Auto-block Grace Period - The number of days a user can wait to update their account password before outgoing SMTP is disabled due to password policy violation. Note: This setting only applies if the "Disable outgoing SMTP when auto-block grace period ends" setting is checked.

• User Notification Timing - The interval(s) used to notify users of when their password will expire or when their auto-block grace period will end and, subsequently, their outgoing SMTP will be disabled. The default values are 28, 14, 7, 3, 2, 1 days. This means SmarterMail will send out warning messages to the user to change their password 28 days, 14 days, 7 days, 3 days, 2 days and 1 day before their password officially expires or the grace period ends if their password violates the requirements. Note: SmarterMail will send one, single notification for all missed intervals. For example, imagine "Auto-block Grace Period" is set for 30 days and the "User Notification Timing" is set at 60, 45, 25, 10, 2, 1. When a user is in violation, SmarterMail will send a single notification for the 60 and 45 day intervals then continue as normal at the 25 day interval.

• Require a number in the password - Select this option to force users to include a number in the password.

• Require a capital letter in the password - Select this option to force users to include a capital letter in the password.

• Require a lower case letter in the password - Select this option to force users to include a lowercase letter in the password.

• Require a symbol in the password - Select this option to force users to include a symbol in the password.

• Require password does not match username - Select this option to ensure that the username and password do not match.

• Disable password strength for existing passwords - Select this option to allow changes to the password requirements to only affect new users or new passwords.

• Enable password retrieval - Select this option to allow users to reset their password if they forget it. Note: In order for users to utilize password retrieval, they must have a backup email address configured in their account settings.

• Prevent commonly used passwords - Select this option to prevent users from configuring passwords that are included in the list of commonly used, insecure passwords. Note: The default location of the list of commonly used passwords is: C:\Program Files (x86)\SmarterTools\SmarterMail\Service\Common_Passwords.xml.

• Prevent user□sprevious passwords from being used - Select this option to prevent users from using previously used passwords when changing their account password. Note: This setting prohibits old passwords from being used indefinitely. It is not based on a time interval.

• Disable outgoing SMTP when auto-block grace period ends - Select this option to disable outgoing SMTP after the auto-block grace period ends when a user□spassword does not meet the password requirements.

SMTP Blocking

The SMTP Blocked Sender list is an effective method for temporarily canceling a domain or indiviual user's ability to send email on the server. For example, if a particular account is sending an abnormal amount of email, you can add their address to Blocked Senders and they will be unable to send email until you remove them from the Blocked Senders list. Users and/or domains can be left on the list for whatever time you deem appropriate, and can be an effective stop-gap versus actually deleting the user and/or domain from the server.

To view blocked senders, click on the security icon . Then expand the Advanced Settings folder and click SMTP Blocked Senders in the navigation pane. A list of blocked senders will load in the content pane and the following options will be available from the content pane toolbar:

• New - Adds a new SMTP blocked sender.
• Edit - Edits the selected blocked sender.
• Delete - Permanently removes the email or domain from the blocked senders list.

Adding a New SMTP Blocking Rule

To add a new SMTP blocking rule, simply click the New button. You are presented with the following options:

• Block Type - Options are set as either Email Address or EHLO Domain.

• Email Address - The complete email address to set up for the block.
• EHLO Domain - This is the return value given when SmarterMail sends the EHLO or HELO command. A standard EHLO domain is the fully qualified domain name set up for the mail server you're wanting to block. (E.g., mail.smartertools.com). However, it IS possible that it will be something differnt based on whether the command is sent by the SmarterMail Web interface or an email client. For example, it may be the local IP address of the sending machine. Therefore, there is no well-established rule for what should be entered until some testing is done by the system administrator.
• Blocked Address - Enter either the full email address or the EHLO Domain, based on the Block Type that was selected.
• Direction - Specify whether to block either incoming SMTP, outgoing SMTP or both.
• Description - Friendly description for the block.

NOTE: SMTP blocking does NOT occur immediately when the EHLO command is given. Instead, a "soft" block is used and SmarterMail will fail any authentication attempts or RCPT TO commands. This is because if the failure occurs right after the EHLO commaned, any person attempting to spam from a mail server could figure out what the problem is and change the domain given with the command on each send. A "soft" failure should, instead, make the spammer believe he is using an incorrect password.

SpamAssassin

SpamAssassin is a powerful, free mail filter used to identify spam. It utilizes a wide array of tools to identify and report spam. These include:

- Header and text analysis
- Bayesian filtering
- DNS blocklists
- Collaborative filtering databases

To view a list of servers currently set up to run SpamAssassin checks, click the security icon / Then expand the Advanced Settings folder and click SpamAssassin Servers . A list of SpamAssassin servers will load in the content pane and the following columns will be available:

- Name - The name of the SpamAssassin server.
- Status - The status of the SpamAssassin server.
- IP Address - The IP address of the server running SpamAssassin. By default, the port is 783.
- Port - The port on which the SpamAssassin server should listen.

In general, the following options will be available in the content pane toolbar:

- New - Adds a new SpamAssassin server. Administrators will need to provide the server's IP address and the port on which SpamAssassin should listen.
- Edit - Modifies the SpamAssassin server settings.
- Delete - Permanently deletes the SpamAssassin server.

For more information on SpamAssassin, please visit http://spamassassin.apache.org .

Reserved Domain Names

System administrators can prevent certain domains names from being added to SmarterMail. For example, domains that are already used for free email services, like gmail.com or yahoo.com, are ideal additions to the reserve list as allowing administrators to add such domains to SmarterMail could

affect message delivery. Similarly, domains that are traditionally reserved for testing and documentation, such as test.com or example.com are also ideal candidates for the reserve list.

To view a list of reserved domains, click the security icon and expand the Advanced Settings folder in the navigation pane. Then click Reserved Domain Names . A list of reserved domains will load in the content pane and the following options will be available from the content pane toolbar:

- New - Adds a domain to the reserve list.
- Edit - Edits the selected domain.
- Delete - Deletes the selected domain(s) from the reserve list.

Additional Help Topics

Automating LogIn to SmarterMail

The HTML code below demonstrates how you can make a text link (e.g. "Log into your mail") that automatically logs a user in to the SmarterMail application. By putting a hidden form on a simple web page, you can fill in the "Email Address", and "Password" information either via hard coding the data or through a scripting language like ASP, ASP.Net, or ColdFusion.

For the example code listed below, we have the form values set to generic text (e.g. "Actual_Email_Address_Here") to show where you would hard code values that are submitted to the login.aspx page. You could also dynamically generate these values using a scripting language like ASP or ColdFusion (a sample ASP script would substitute value="Actual_Email_Address_Here" with value=<% =email %>). The form action shown (http://127.0.0.1:9998/smartermail/login.aspx) uses the default location of the Smartermail Web Interface. If you have created a separate web site for Smartermail, or assign a different IP address for Smartermail within IIS, this action would have to be altered to reflect this change. This example demonstrates how easy and powerful the Smartermail application is in allowing companies to automate entry into the mail application.

<html>

<head> <meta http-equiv= "Content-Language" content= "en-us" > <meta http-equiv= "Content-Type" content= "text/html; charset=windows-1252 "> <title>Smartermail Login</title> </head>

<SCRIPT LANGUAGE= "JavaScript" > function GoToMail() { document.mailform.submit(); } </SCRIPT>

<body>

<form name= "mailform" action= "http://127.0.0.1:9998/Login.aspx" method= "post" > <input type= "hidden" name= "shortcutLink" value= "autologin" id= "shortcutLink" > <input type= "hidden" name= "email" id= "email" value= "Actual_Email_Address_Here" > <input type= "hidden" name= "password" id= "password" value= "Actual_Password_Here" > </form>

 Log into your mail

</body>

</html>

Gateways and Other Server Roles

Please note that SmarterMail was designed to support one server in several of these roles. For instance, one server could act as an Incoming Gateway, Outgoing Gateway, or Backup MX.

SmarterMail can also take on one of these roles when placed together with a competing mail server product. For example, using SmarterMail as an outgoing gateway on a server other than your primary mail server may help to resolve problems with stability of other mail server software products.

Primary mail server

- Use for storing email for defined users.
- Accessible through POP, SMTP, IMAP, and over the web.
- To configure:

- Follow instructions in online help

Backup MX Server

- Use as a backup for mail delivery in case of short amounts of downtime or delivery problems on your primary mail server.
- To configure:

- Add a placeholder domain (called "example.com") to open up the port to listen on.
- Configure SmartHosting by adding the IP addresses to which delivery should be allowed.
- In general settings, change the delivery retry times to 10, 10, 10, and 1440.

• In DNS, add secondary MX records pointing to the new server's IP. Set the preference value higher than the main MX record.

Incoming Gateway server

The FREE, one-domain version will suffice for virtually all environments.

• Use to host third party anti-virus and/or anti-spam software products in order to reduce load on primary server.
• Reduces load on primary server by managing all incoming sessions and performing abuse/intrusion detection.
• To configure:

• Enable domain forwarding and add all destination IPs and domain names that will be forwarded.
• Add a placeholder domain (called "example.com") to open up the port to listen on.
• In DNS, change the MX records of your domains to reference the new gateway server.
• Install and configure any third-party anti-virus or anti-spam products, such as Declude JunkMail or Declude Virus.

Outgoing Gateway server

The FREE, one-domain version will suffice for virtually all environments.

• Use as a delivery mechanism to reduce load on your primary servers.
• Also use as a method to combat blacklisting. If the server gets blacklisted, rotate the primary IP on the network card to a different one to send out on the new IP.
• To configure:

• Add a placeholder domain (called "example.com") to open up the port to listen on.
• Set relay option in General Settings to "nobody".
• Add the primary mail server's IP addresses to the IP Whitelist for SMTP.
• In your primary mail server's General Settings page, set the IP address of the gateway server and enable gatewaying.

SmartGateway server

The FREE, one-domain version will suffice for virtually all environments.

• Use as a delivery mechanism to balance the load on your gateway servers.
• To configure:

• Add a placeholder domain (called "example.com") to open up the port to listen on.
• Set relay option in General Settings to "nobody".

- Add the primary mail server's IP addresses to the IP Whitelist for SMTP.
- In your primary mail server's General Settings page, set the IP address of the gateway server and enable gatewaying.

Backup MX Servers

A Backup MX Server is a mail server that will store (spool) your incoming email if your primary mail server becomes unavailable. A mail server can become unavailable to receive incoming mail for a number of reasons. For example:

- Hardware or software failure
- Very busy and unable to receive new incoming connections, or emails
- Network connection is down or saturated
- Network routing issues can also cause your mail server to become unavailable

Case 1 - No Backup MX

If you do not have a Backup MX Server, the following conditions may occur:

- Email will be bounced (Returned to Sender).
- Your (inbound) email will cause a backup in the originating mail server's spool.
- Service Timeout. Depending on the Retry attempts by the originating mail server, your mailboxes may never receive their incoming email.
- Users do not understand bounce messages. To most users, bounce messages are unreadable, so when they can't send an email, they do not try to resend.

Case 2 - With a Backup MX

How Email works when a Backup MX Server is involved:

- User sends an email to 'user@example.com' (a mailbox hosted by your SmarterMail Server)
- Their mail server looks up the MX Records for 'example.com' and finds two:

- IP: x.x.x.x Weight: 10
- IP: y.y.y.y Weight: 20
- Their mail server first attempts to connect to: x.x.x.x
- Connection fails, which could be caused by any of the above conditions
- They try to connect to the secondary MX record: y.y.y.y
- They successfully connect to this server.
- Email transmission begins, and the Backup MX Server receives the email into its spool.
- Since there are no existing local domains on this server, SmarterMail stores this email in its spool.

• Based off of the Retry Attempts, SmarterMail will continue to try and make connections to your Primary Mail Server.

• SmarterMail will only make 4 retry attempts. It is recommended that you set the last attempt to a longer timeframe, i.e., 24 hours (1440 minutes)
• This way SmarterMail does not send a Bounce Message to the originator saying that it could not deliver the message, before your Primary Server is back online.
• If your Primary Mail Server comes back online before the final Retry Attempt, you can reset the Retry Counts on all messages in the spool. This will force the Backup MX Server to try forwarding all existing mail in the spool back to your Primary Mail Server.

Configuring a Backup MX Server

• Add a placeholder domain (called "example.com") to open up the port to listen on.
• Configure SmartHosting by adding the IP addresses to which delivery should be allowed.
• In general settings, change the delivery retry times to 10, 10, 10, and 1440.
• In DNS, add secondary MX records pointing to the new server's IP. Set the preference value higher than the main MX record.

Locking Down Your Server

Security is an ever-growing concern to business small and large. Because email servers are constantly under attack, SmarterMail has many features built into it to protect you. This topic explains steps you can take to protect yourself, your users, and your investment.

What is Security for a Mail Server?

The word security has many meanings. SmarterTools' opinion is that mail server security is comprised of several types of protection:

• Protecting your data
• Protecting your users
• Protecting your service availability
• Protecting others on the internet

Below are some "Best Practices" for maintaining a locked-down server, one that can withstand the constant abuse that mail servers are subject to.

• Update SmarterMail regularly
• Disable catch-all accounts
• Restrict bounces and auto-responders

- Require SMTP authentication
- Encourage the adoption of SPF

Update SmarterMail Regularly

SmarterTools is constantly working to improve SmarterMail and make it even more resistant to attacks. It is recommended that you keep your copy of SmarterMail up to date in order to stay protected.

Major and minor SmarterMail version releases are announced on our social media pages as well as the News items on the Support Portal . Email notices are sent to SmarterMail customers who are subscribed to receive these notifications. You can manage your mailing list subscriptions at My Account .

Disable Catch-All Accounts

Catch-all accounts were popular in the past because of the flexibility they offer to a domain administrator. All an administrator had to do was add a catch-all account, and any mail that was mis-delivered would drop right into his mailbox. When catch-alls were most popular, spamming methods were not as sophisticated, and email harvesting attacks were not so prevalent.

Today, however, mail servers get attacked every minute of every day. Spammers assault email domains with thousands of spam messages sent to different email accounts in the hope that they will strike a hit to verify that the email account exists and to deliver another spam email.

In addition, if the catch-all user has an auto-responder enabled, the problem can be doubly harmful. Spammers rarely use their real email address, so if your user auto-responds to each of the thousands of messages above, and they happen to go to a large email provider, you will likely end up getting blacklisted as a spammer yourself.

As you can see, allowing the use of catch-all accounts exposes you to many types of abuse. SmarterMail allows catch-alls because it is expected in a mail server, but to lock down your server, we recommend the following procedure that will disable catch-alls:

- Alert your users that catch-alls are being disabled.
- Click on the Domains icon and edit the desired domain.
- Click on the Features tab.
- Uncheck Catch-All Alias .
- Click Save .

Restrict Bounces and Auto-Responders

Email Bouncing occurs when delivery failures occur or a mailbox is full. A brief explanation of the error is sent back to the original sender of the message. Before spam became such a problem, this was usually not an issue. Today, however, spammers will sometimes spoof known spam trap accounts at places like SpamCop as the sender of the message. Thus, when your mail server bounces the message, the bounce ends up in the spam trap. Enough of these, and you'll be blacklisted.

The exact same is true for auto-responders that reply back to spoofed spam email.

SmarterMail allows you to restrict bounces and auto-responders to only those accounts that pass SPF checks, or to disable them entirely. SPF verifies that an email is not spoofed, and most of the serious spam trap accounts out there have SPF set up. To require SPF for bounces and auto-responders, do the following:

- Alert your users of the new policies being put into place.
- Click on the Security icon .
- Click on Antispam Administration in the navigation pane and then the Options tab.
- Change Auto-Responders to either Disabled or Require message passed SPF .
- Change Content Filter Bouncing to either Disabled or Require message passed SPF .
- Click Save in the content pane toolbar.

Require SMTP Authentication

SMTP Authentication is an unspoken requirement of domains on modern mail servers. Any domain that does not have Authentication enabled is at a serious risk of being a relay for spam. Spammers will try thousands of email accounts until they find one to send through, and if Authentication is not enabled, they will be able to use up your bandwidth and system resources to send mail.

Enabling SMTP Authentication ensures that users must supply credentials to send email from your server. This requires a change in their email clients so that the account information gets passed in SMTP, so there is often a bit of a learning curve. This process is necessary and important to protect your server, however, and without you are open for abuse.

To require SMTP Authentication for a domain, do the following:

- Alert your users of the change they will need to make to their email client. Due to the nature of this change, it is wise to give them a fair amount of warning.
- Click on the Domains icon and edit the desired domain.
- Click on the Technical tab.

- Check Require SMTP Authentication .
- Click Save .

It is also recommended that you update this setting in the default domain settings so that all new domains will require SMTP Authentication. In addition, to further secure the use of SMTP Authentication, you should ensure that "Require Auth Match" is set to Domain or Email Address for all domains. This means that a sender's "From" address much match the SMTP authentication address or domain, making it more difficult for users to spoof addresses. This can be done under the SMTP In tab of the Protocol Settings.

To apply this setting to all domains on your server at once, use the Domain Propagation page in the Settings menu.

Encourage the Adoption of SPF

SPF is an excellent method of preventing email spoofing, protecting your users from having their domain show up on spam throughout the world. SPF, however, is only as effective as you make it, as it requires changes to your DNS servers for each domain you host email for.

It is in the best interest of all email users everywhere that domain administrators add SPF records to their domain that indicate what servers are authorized to send email for their domain. Encouraging your domain administrators to adopt SPF protects them from being the victims of spoofing, and reduces the spam threat on not only your server, but others throughout the world as well.

More information can be found at: http://www.openspf.net/

Proper DNS Settings for Email

There are several major things to set up on your DNS server for each site you add to SmarterMail. How you set these up is dependent upon both who hosts your DNS and what DNS software is used. Check your DNS server documentation for instructions on how to set up the following records (replace example.com with the proper domain name).

Also, please bear in mind that your DNS may need to be set up differently. This is only a guideline that is recommended for most installations.

- WebMail URL - Add an A or CNAME record for mail.example.com that points to the IP address of the webmail interface. This will allow users of that domain to access the webmail by typing in http://mail.example.com or http://mail.example.com:9998 in their web browser (depending on whether you use the included web server or IIS).
- Mail Pointer (MX) - Add an MX record for the domain that points to mail.example.com. This will allow other email servers to locate your mail server.

• Reverse DNS Record - Add a reverse DNS record for IP addresses assigned on the server to provide extra assurance to other mail servers. Also, it is recommended that the primary IP address of the server also have a reverse DNS record.
• Sender Policy Framework - Some large email providers like Hotmail and AOL are starting to require specially formatted TXT records to be added to your DNS. This special format is known as SPF (Sender Policy Framework). Information about how these records should be formatted can be found at http://spf.pobox.com . Please keep in mind that the owners of the domains may have significant input on what goes into these records.

Changing the System Administrator Login

By default, the login for the system administrator for SmarterMail is admin/admin . While this is easy to remember, it is also fairly easy to guess. When installing SmarterMail for the first time, you will be required to change this password during the setup wizard. Here are instructions in the manner you would want to change the system administrator password again.

Instructions

• Login as the administrator with the current login.
• Click the Settings icon .
• Choose System Administrators in the navigation pane.
• Click on the Options tab and double-click on the Primary Administrator or right-click and choose Edit.
• Enter the current password for verification.
• Enter a new and password (If changing the username as well, avoid using an email address for the username).
• Click on Save .

Resetting an Unknown Login

For instructions on how to reset an administrator login when the current login is unknown, please see the KB article How To Reset an Administrator Username and Password .

Troubleshooting a Domain

There are times when you will need to access domain specific information. SmarterMail uses impersonation to accomplish this goal, causing a separate window to login automatically as the domain administrator. This can be a useful method to examine domain settings or configure settings.

To impersonate a domain, click the Domains icon . Then select the desired domain in the navigation pane, right-click and choose Manage . Alternatively, you can select the domain in the navigation pane

and click Manage in the content pane toolbar. A new window will pop up, and you will be logged in as the domain administrator. From there, you may edit user accounts, content filters, or whatever other part of the domain that needs to be changed.

For instructions on troubleshooting specific user accounts on a domain, please see the topic Troubleshooting an Email Account .

Modifying Scoring for the SpamAssassin-based Pattern Matching Engine

System administrators can modify the scoring for the SpamAssassin-based pattern matching engine using the local.cf file. However, this feature is only recommended for experienced system administrators.

The local.cf file is placed in the service's SAData folder. It is used to override existing tests or to create new tests supported by SmarterMail. Note: Any modifications to the local.cf file will not be overwritten when installing a new version.

Overriding an Existing Test's Score

The most common modification to the local.cf file will be to override an existing test's score. For example, if a system administrator he notices a lot of spam messages getting into his users' mailboxes that are failing a particular test, he may want to override a that test's score.

To do so, the server administrator would add something like:

score TEST_I_WANT_TO_OVERRIDE 1.3

Here score is the keyword used by the engine, TEST_I_WANT_TO_OVERRIDE corresponds to the existing test they want to override and 1.3 is the new score.

Creating a New Test

If a system administrator notices a noticed a new pattern appearing in spam messages that isn't covered by the default files, he may want to create a new test. This would look something like this:

body NEW_TEST /test/ #look for the word test in the body of the email score NEW_TEST 10.3

Here body is the keyword for determining the type of test, NEW_TEST is the name of the new test, /test/ is the perl style regular expression that will be used while scanning the email, and everything after the pound-sign is a comment.

The system administrator will also need to score thenew rule so that it has some affect on the final weight.