Help for System Administrators

Help Documentation

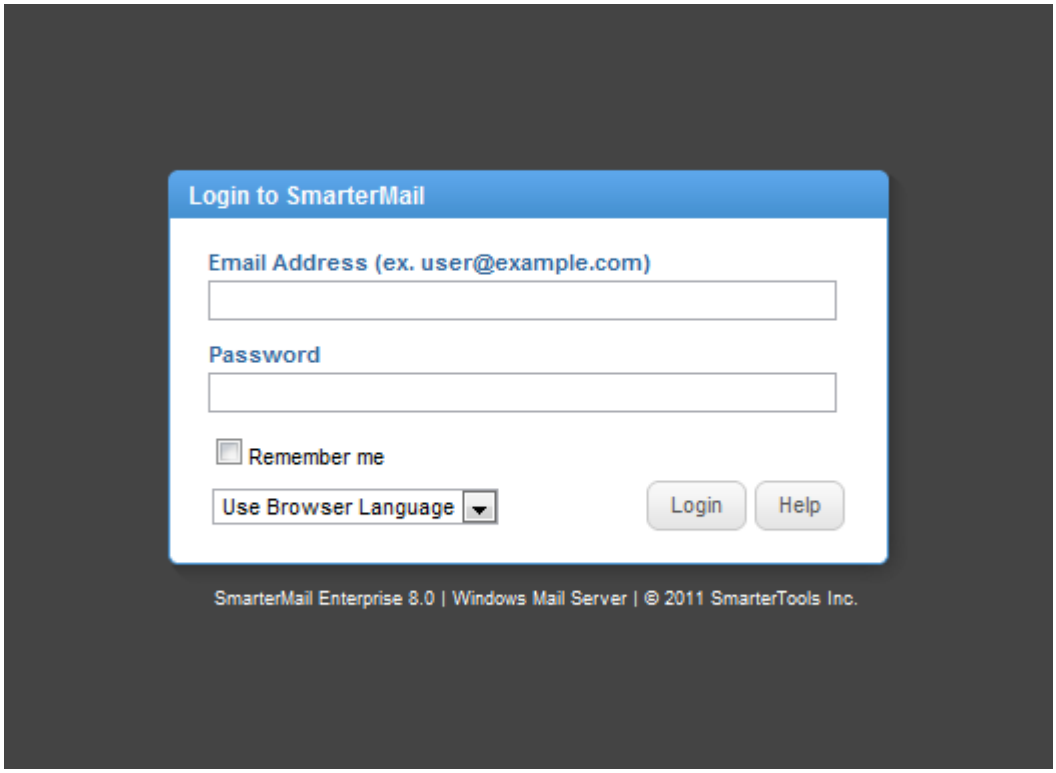
Help for System Administrators

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.



Manage

All Domains

System administrators can use this section to manage all of the domains in SmarterMail. To view all domains, click the manage icon and then click All Domains in the navigation pane. A list of domains will load in the content pane and the following columns will be available:

- Checkbox - Use these boxes to select multiple domains. Domains must be selected before choosing an action from the content pane toolbar.
- Domain Name - The name of the domain. For example, smartermail.com or example.com.
- Size - The amount of disk space used by all mailboxes on the domain.
- File Storage - The amount of disk space used for file storage on the domain.
- Users - The number of users (mailboxes) on the domain.
- Aliases - The number of alias addresses on the domain.
- Mailing Lists - The number of mailing lists on the domain.

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

- Edit - Edits the settings for the selected domain.
- Delete - Permanently deletes the selected domain(s).
- Manage - Impersonates the domain administrator and give the system administrator access to all of the domain settings.

Creating New Domains

To create a new domain, click the manage icon . Then click New in the navigation pane toolbar and click Domain . The domain settings will load in the content pane and the following tabs will be available:

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. IP Address - The IP address for which the domain will check for incoming requests. Note: This setting does not affect Web interface login and is only used to check for SMTP, POP, and IMAP traffic. --%> --%>
- 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.

• Mailing List Username - The email address for which listserv commands are emailed.

• Domain Administrator Username - The identifier the domain administrator uses to login to SmarterMail. 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.

• Domain Administrator Password - The password associated to the domain administrator username.

• Disable Domain - Select this option to disable the domain. Disabled domains cannot send or receive email and users cannot login to the Web interface. This option is a good way to temporarily shut off a domain without deleting it.

Technical

Use this tab to specify the following technical settings:

SMTP Port - The SMTP port used to connect to the email server. By default, the SMTP port is 25. Note: Changing the default port is not recommended unless you are behind a firewall that requires this setting to be changed.

• SMTP Port (Alternate) - The SMTP port used to connect to the email server if an ISP restricts the standard port 25.

• Enabled - Check this box to enable the alternate SMTP port.

• POP Port - The POP port used to connect to the email server. By default, the POP port is 110. Note: Changing the default port is not recommended unless you are behind a firewall that requires this setting to be changed.

• IMAP Port - The IMAP port used to connect to the email server. By default, the IMAP port is 143. Note: Changing the default port is not recommended unless you are behind a firewall that requires this setting to be changed.

• LDAP Port - The LDAP port used to connect to the server. By default, the LDAP port is 389. Note: This is an Enterprise only feature. Changing the default port is not recommended unless you are behind a firewall that requires this setting to be changed. --%>

• Outbound IP - The IP used to connect to external SMTP servers when a message is sent by the domain..

• Logout URL - The URL that the user is redirected to upon logout.

• Auto-responder Exclusions - To prevent the system from sending automated messages 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.

• 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.
• Enable once per day per sender auto-responder restriction - Select this option to limit how frequently an auto-responder is sent.
• Disable greylisting - Select this option to disable greylisting.
• Enable users to opt out of LDAP listings - Select this option to allow users to remove themselves from the Global Address List.
• Enable domains to override mailing list message size - Select this option to allow domain administrators to specify the maximum size for mailing list messages.

Features

Use this tab to enable or disable the following features:

• Enable Active Directory integration - Select this option to enable active directory authentication.
• Enable calendar - Select this option to allow users to use the calendar feature.
• Enable catch-alls - Select this option to allow users to use catch-all email addresses.
• Emable contacts - Select this option to allow users to use the contacts feature.
• Enable content filtering - Select this option to allow users to use content filtering.
• Enable control of service access - Select this option to give users access to POP, IMAP, SMTP and webmail services.
• Enable domain aliases - Select this option to allow domain administrator to create domain aliases.
• Enable domain reports - Select this option to provide additional reports for domain administrators.
• Enable file storage - Select this option to allow users to use the file storage feature.
• Enable email reports - Select this option to provide the ability to email reports.
• Enable IMAP retrieval - Select this option to allow users to download IMAP email from third-party mail servers.
• Enable mail signing - Select this option to enable email verification via mail signing.
• Enable mailing lists Select this option to allow domain administrators to create and use mailing lists to send mass emails.
• Enable notes - Select this option to allow users to use the notes feature.
• Enable POP retrieval - Select this option to allow users to download POP email from third-party mail servers.
• Enable spam filtering - Select this option to allow domain administrators to override the spam

filtering settings.

• Enable SyncML - Select this option to allow users to sync SmarterMail with Outlook, Thunderbird and most smartphones using SyncML.

• Enable tasks - Select this option to allow users to use the tasks feature.

• Enable 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. 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. By default, domains are limited to two 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, this setting will be overridden.

• 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. 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.

Sharing

This tab is only available in SmarterMail Enterprise edition.

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

• Enable 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.
• Enable shared calendars - Select this option to allow calendars to be shared with other users on the domain.
• Enable shared contacts - Select this option to allow contact lists to be shared with other users on the domain.
• Enable shared folders - Select this option to allow email folders to be shared with other users on the domain.
• Enable shared notes - Select this option to allow notes to be shared with other users on the domain.
• Enable shared tasks - Select this option to allow task lists to be shared with other users on the domain.

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.

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

• 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.

• 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.

• 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.
• Event Emails - The priority level for messages reminding users of upcoming 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

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 the message during the SMTP 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 - 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 Eevent - Select this option to enable the User Added event type.
- Enable User Deleted event - Select this option to enable the User Deleted event type.
- Enable User Disk Space Used event - Select this option to enable the User Disk Space event type.

Disabled Domains

System administrators can use this section to manage all of the domains in SmarterMail. To view all domains, click the manage icon and then click All Domains in the navigation pane. A list of domains will load in the content pane and the following columns will be available:

- Checkbox - Use these boxes to select multiple domains. Domains must be selected before choosing an action from the content pane toolbar.
- Domain Name - The name of the domain. For example, smartermail.com or example.com.
- Size - The amount of disk space used by all mailboxes on the domain.
- File Storage - The amount of disk space used for file storage on the domain.
- Users - The number of users (mailboxes) on the domain.
- Aliases - The number of alias addresses on the domain.
- Mailing Lists - The number of mailing lists on the domain.

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

- Edit - Edits the settings for the selected domain.
- Delete - Permanently deletes the selected domain(s).
- Manage - Impersonates the domain administrator and give the system administrator access to all of the domain settings.

Disabling and Enabling Domains

To disable or re-enable a domain, select the desired domain and click Edit in the content pane toolbar. The domain settings will open in a popup window and the option to disable or enable the domain will be in the Options tab.

Spool

The email spool is a list of emails, in order of when they are created, that are available for the server to send or deliver locally. SmarterMail is multi-threaded, which means that if a message cannot process out of the queue, 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 of the messages in the spool, click the manage icon and expand the Spool in the navigation pane. Then click All Messages . To only view the messages waiting to be delivered, click the manage icon and expand the Spool in the navigation pane. Then 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.
- Sender - The email address that initially sent the email.
- Size - The total size of the message on the hard drive, in kilobytes.
- Recipients - The number of delivered/total recipients.
- Time in Spool - The total amount of time the message has been in the spool.
- Attempts - The number of delivery attempts that have been made.
- Next Attempt - The date and time of the next delivery attempt.
- Status - The current status of the message.
- Spool Path - The spool the message resides in. If you have subspools enabled, the message may be placed in one of those locations.
- Priority - The priority level of the message.

The following actions are available from the content pane toolbar:

- Force - Clicking this button will allow the system administrator to push 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 - Clicking this button will allow the system administrator to reset 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.

• View - Clicking this button will allow the system administrator to view selected message in a popup window.

• Recipients - Clicking this button will allow the system administrator to see who the message was sent to and the status of that message (i.e. delivered or pending).

• Priority - Clicking this button will allow the system administrator to change the priority level of a message.

• 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.

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 User - Permanately disables the user from logging in to the system.

• Refresh - Refreshes the list of online users.

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.

Current Connections

SmarterMail will monitor the server and see who is connecting via the different protocals—SMTP, IMAP, and POP. System administrators can then blacklist a certain user if they believe a user is making too many connections.

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

Current Blocks

SmarterMail will monitor the server and keep track of all users who are currently being blocked for SMTP, IMAP, POP, LDAP, or email harvesting.

System adminstrators can then click Delete in the content pane toolbar to remove anyone from the list.

Mass Messaging

SmarterMail gives system administrators the opportunity to send mass emails and reminders to selected groups.

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.
- 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.

Send Reminder

To send a mass email, 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.

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.
- Status Indicator - The status indicator, or the colored ball next to the checkbox, shows the current status of the service.
- Descroption - 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 and saved in a mailbox on the mail server.
- 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 - 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.

View Logs

System administrators can use this section to quickly view the server's log files. 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 date of 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.

• Enable related traffic - Select this option to only display data that occurred within the same sesion.

To search for a specific log, complete the Date, Type, and Search String fields. Then click Search in the content pane. Any matching log files will display in the content pane. Note: SmarterMail will show logs files up to 1MB.

Alternatively, system administrators can download the log file by clicking Download in the content pane toolbar. This page allows administrators to get quick access to a domains log files. Administrators can view log files by utilizing this page, or they can download the selected log file as a .zip file by clicking Download in the content pane toolbar.

Message Archive Search

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

Message archiving is a method of storing all email traffic for a domain 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.

To search the archive, click the manage icon and click 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.

Domain administrators can also search the archive by clicking email icon and clicking Message Archive Search in the navigation pane.

For more information on archiving, see Message Archiving .

Indexing Status

SmarterMail Search Indexing allows users to instantly find any files--including messages, attachments, appointmenst, 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. This method of indexing reduces server utilization while increasing the speed in 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 (or queued for indexing) will load in the content pane.

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 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.

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

- Send Email - Sends an email to the selected user(s).

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.

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.

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:

Use this tab to specify the following settings:

- Username - The system administrator login name.
- Old Password - In order to change the system administrator password, you must type the current password associated with the system administrator account in this field. Passwords are case-sensitive.
- New Password - Type the desired password for the system administrator account in this field. Passwords are case-sensitive.
- Confirm New Password - Verify the desired password for the system administrator account. Passwords are case-sensitive.
- Items per Page - The number of items will display on each page within SmarterMail.

• Enable Login Access by IP Address - Select this checkbox to restricts logins to the system administrator account by IP address.
• Enable Lite Mode - SmarterMail Lite is a specially-developed version of the SmarterMail mail server that provides unlimited email accounts and domains and it is only available with specific product offerings from SmarterTools technology partners. If SmarterMail detects software from a company that has partnered with SmarterTools to make this edition available, SmarterMail Lite will automatically be enabled. Because SmarterMail Lite has a limited feature set, some customers may want to revert to SmarterMail Free edition. To do so, uncheck this box. Note: SmarterMail Free edition has the same functionality as SmarterMail Enterprise, but is limited to one domain with up to 10 users.

Login Access

Use this tab to specify the IP addresses from which the system administrator can login. Note: This tab is only available if the system administrator has enabled login access by IP address in the Administrator tab. --%>

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 - The email address for the postmaster. This is usually the owner or system administrator.
• 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 upon logout.

• Enabled - Select this checkbox to redirect users to the Logout URL after logging out of SmarterMail.
• Enable domain admins to override logout URL - Select this option to allow domain administrators to specify the Logout URL. If this option is not enabled, it will not be visible to domain administrators.
• Enable Lite Mode - SmarterMail Lite is a specially-developed version of the SmarterMail mail server that provides unlimited email accounts and domains and it is only available with specific product offerings from SmarterTools technology partners. If SmarterMail detects software from

a company that has partnered with SmarterTools to make this edition available, SmarterMail Lite will automatically be enabled. Because SmarterMail Lite has a limited feature set, some customers may want to revert to SmarterMail Free edition. To do so, uncheck this box. Note: SmarterMail Free edition has the same functionality as SmarterMail Enterprise, but is limited to one domain with up to 10 users.

• Reset getting started - Select this checkbox to view the Getting Started checklist. This checklist is designed to system administrators set up the mail server and appears automatically after installation. However, system administrators may choose to refer to the checklist at a later time as a reference guide when adding additional domains or users.

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 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 15 seconds.

• 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 attempting to be resent. 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.

• Attempts before bouncing DNS errors - 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 processing unnecessary messages 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.

• 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. In general, a timeout of 5 seconds should suffice.

Reports

Use this tab to specify the following settings:

• Delete Server Stats After - The number of months that the server stats will be deleted. By default, the server stats are deleted after 13 months.

• Enabled - Select this checkbox to delete server stats after the specified time period.
• Delete Domain Stats After - The number of months that the domain stats will be deleted. By default, the domain stats are deleted after 13 months.

• Enabled - Select this checkbox to delete domain stats after the specified time period.
• Delete User Stats After - The number of months that the user stats will be deleted. By default, the user stats are deleted after 13 months.

• Enabled - Select this checkbox to delete user stats after the specified time period.

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 index more users simultaneously.
• 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.
• 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.
• 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.
• 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.
• Deleted Items Before Indexing - 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.

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 navigatione 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 the user uses to login to SmarterMail.
• New Password - The corresponding password used to login to Smartermail.
• Confirm New Password - The corresponding 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.

Login Access

Use this tab to specify the IP address or IP range from which system administrators can login to SmarterMail from. 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 and 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 - The maximum number of threads you want SmarterMail to work on concurrently. 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.

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 and 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 POP messages. By default, the POP retrieval interval is 10 minutes.
• 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, you can set the type of relays you will allow, or completely disallow mail relay completely.

• 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 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.
• 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 - After this many bad recipients, 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. Submission IP:Port - The submission port is a special SMTP port that requires SMTP Authentication in order to be used to deliver any mail whatsoever, regardless of domain-specific settings. This setting is an advanced feature that is typically used when a whitelisted inbound gateway is being used for spam and virus scanning and all other SMTP traffic is blacklisted. Note: This setting will not function until the Enabled checkbox next to the setting is checked. --%>

• 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.

• Disable relay settings when using SMTP authentication - Select this checkbox to disable the "Allow Relay" setting from above.

• 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.

• Disable appending of received line for authenticated messages - Select this checkbox to prevent SmarterMail from appending the received line when a message is received over SMTP and the message is authenticated.

SMTP Out

Use this tab to specify the following outgoing SMTP settings:

• Outbound IP - Select the IP address that is used to deliver outbound messages from the list.
• Enable fallback to Primary IP on failure - Select thsi checkbox to have SmarterMail automatically fallback 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 and 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.
• 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.

ActiveSync Mailboxes

System administrators will use this section to enable and disable the Microsoft Exchange ActiveSync add-on for mailboxes. Note: Before you can configure a mailbox to sync using the ActiveSync technology, you must activate the ActiveSync add-on. For more information, please refer to the KB article How To - Activate Microsoft Exchange ActiveSync .

To access this section, click the settings icon 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.

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.
• Search - Searches for a specific mailbox with Exchange ActiveSync enabled.

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 files that are no longer used from the server when possible.

To manage the file storage settings, click the settings icon 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 in KB of any file uploaded to the server.

- Enabled - Select this option to enable the max file size setting.
- 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.

- Enabled - Select this option to enable the custom base URL setting.

Extension Blacklist

Use this tab to list any file types that cannot be uploaded to the server.

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.

To view hostnames, click the manage icon 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).

Message Footer

System administrators can configure server-wide message footers that SmarterMail will append on all outgoing and incoming 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 and click Message Footer in the navigation pane. 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 the message footer on.
- 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. Note: The message footer does not support the use of variables.

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.

Skins

SmarterMail supports custom skinning, so administrators can create skins that represent their own style or emulate the company's branding and appearance.

To view the skin settings, click the settings icon and click Skins in the navigation pane. The following skinning settings will load in the content pane:

- Default Skin - Select the skin to use as the default from the list.
- Enable ability for domains to override skin - Select this option to allow domain administrators to choose a skin for their domain

Log Settings

System administrators can use this section to manage how logs are written and how much detail is included in 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.
- 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 Level - The log level for Exchange ActiveSync connections.
- Delivery Log Level - The log level for message delivery and spool operations.
- IMAP Log Level - The log level for IMAP sessions.
- IMAP Retrieval Log Level - The log level for IMAP retrieval sessions.
- LDAP Log Level - The log level for LDAP sessions.
- Message-ID Log - The log level for logging Message-ID's of all messages sent to mailing lists.
- Event Log - The log level for event sessions.
- SycnML Log Level - The log level for SyncML sessions.
- POP Log Level - The log level for POP sessions.
- POP Retrieval Log Level - The log level for POP retrieval sessions.
- SMTP Log Level - The log level for SMTP sessions.

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

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 on the IP 111.111.111.11 but not on the IP 222.222.222.22.

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.

Ports

System administrators can use this section to configure the ports that can be assigned to IPs. In addition, this section is used to add Secure Socket Layer (SSL) and Transport Layer Security (TLS) rules.

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 availble 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 (SMTP, IMAP, LDAP, POP or submission port).
- Encryption - If the port requires SSL or TLS encryption, select the appropriate option from the list. SSL always assumes the connnection will be secure and sends the encryption immediately. TSL 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.
• Certificate Path - The path to the certificate file on the server. Typically, named a *.cer file. Note: This option is only available if SSL or TLS encryption is enabled for the port. The certificate you are using must be added to the Certificates Microsoft Management Console within your Windows operating system. In addition, you must associate the Private Key with this same certificate.
• Description - A short description of the port.

Defaults

Domain Defaults

Use this section to create global default settings that will be applied to new domains 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 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.
• SMTP Port - The SMTP port used to connect to the email server. By default, the SMTP port is 25. Note: Changing the default port is not recommended unless you are behind a firewall that requires this setting to be changed.
• SMTP Port (Alternate) - The SMTP port used to connect to the email server if an ISP restricts the standard port 25.

• Enabled - Check this box to enable the alternate SMTP port.
• POP Port - The POP port used to connect to the email server. By default, the POP port is 110. Note: Changing the default port is not recommended unless you are behind a firewall that requires this setting to be changed.
• IMAP Port - The IMAP port used to connect to the email server. By default, the IMAP port is 143. Note: Changing the default port is not recommended unless you are behind a firewall that requires this setting to be changed.
• LDAP Port - The LDAP port used to connect to the server. By default, the LDAP port is 389.

Note: This is an Enterprise only feature. Changing the default port is not recommended unless you are behind a firewall that requires this setting to be changed.

• Auto-responder Exclusions - To prevent the system from sending automated messages 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.

• 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.

• Enable once per day per sender auto-responder - Select this option to limit how frequently an auto-responder is sent.

• Disable greylisting - Select this option to disable greylisting.

• Enable users to opt out of LDAP listings - Select this option to allow users to remove themselves from the Global Address List.

Features

Use this tab to enable or disable the following features:

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

• Enable catch-alls - Select this option to allow users to use catch-all email addresses.

• Emable contacts - Select this option to allow users to use the contacts feature.

• Enable content filtering - Select this option to allow users to use content filtering.

• Enable control of service access - Select this option to allow the domain administrator to restrict access to certain services.

• Enable domain aliases - Select this option to allow the domain administrator to create domain aliases.

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

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

• Enable IMAP retrieval - Select this option to allow users to download IMAP email from third-party mail servers.

• Enable mail signing - Select this option to enable email verification via mail signing.

• Enable mailing lists Select this option to allow the domain administrator to create and use mailing lists to send mass emails.

• Enable notes - Select this option to allow users to use the notes feature.

• Enable POP retrieval - Select this option to allow users to download POP email from third-party mail servers.

• Enable spam filtering - Select this option to allow the domain administrator to override the spam filtering settings.
• Enable SyncML - Select this option to allow users to sync SmarterMail with Outlook, Thunderbird, and most smartphones using SyncML.
• Enable tasks - Select this option to allow users to use the tasks feature.
• Enable 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. 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. By default, domains are limited to two 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, this setting will be overridden.
• 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.
• 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.

Sharing

This tab is only available in SmarterMail Enterprise edition.

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

• Enable 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.

• Enable shared calendars - Select this option to allow calendars to be shared with other users on the domain.
• Enable shared contacts - Select this option to allow contact lists to be shared with other users on the domain.
• Enable shared folders - Select this option to allow email folders to be shared with other users on the domain.
• Enable shared notes - Select this option to allow notes to be shared with other users on the domain.
• Enable shared tasks - Select this option to allow task lists to be shared with other users on the domain.

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.

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

• 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.

• 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.

• 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.
• Event Emails - The priority level for messages reminding users of upcoming events.

• Enabled - Check this box to enable priority settings for event emails.
• Priority After Attempt X - 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 Y - 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 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

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.

• Enabled - Check this box to enable throttling for outgoing messages.
• Outgoing Bandwidth per Hour - The total number of MBs sent by the domain per hour. By default, the outgoing bandwidth is 100.

• Enabled - Check this box to enable throttling for bandwidth.
• 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.

• Enabled - Check this box to enable throttling for bounced messages.

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.

Collaborate

- 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.

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 the User Added event type.
- Enable User Deleted Event - Select this option to enable the User Deleted event type.
- Enable User Disk Space Used Event - Select this option to enable the User Disk Space event type.

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 settins 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 Defaults 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 .

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 Defaults 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:

- Enable domains to override auto-clean settings - Selet this option to allow domain administrators to create their own auto-clean policies.
- Enable users to auto-clean inbox - Select this option to allow users to create their own auto-clean policies.

Folder Settings

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.

Routing

Forwarding Blacklist

Emails cannot be forwarded to the domains in this list. This is to prevent issues with companies that have strict spam policies and blacklist the sending server for forwarded spam.

This feature is commonly used for AOL, which blacklists servers that forward spam to their servers. If this becomes a problem, you may decide to add AOL.com to your forwarding blacklist.

Message Archiving

This feature is only available in SmarterMail Enterprise edition.

Message archiving is a method of storing all email traffic for a domain 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.

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.

To view the message archiving rules for your SmarterMail installation, click the settings icon . Then expand the Routing folder 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, incoming messages, or outgoing messages.

Note: 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.

Outgoing Gateway

Gateway servers allow you to reduce the load on your primary server by using a secondary server to process outgoing mail. Gatway servers can also be used to combat blacklisting. If the 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 incoming 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.
- 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 encription from the list.
- Priority Range - The priority range for this server.
- Enable SmarterMail gateway mode - Select this option to indicate that the outgoing gateway server is another SmarterMail server.

SmarterMail Gateway

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.

Incoming Gateways

prpose is to reduce server load. Generally, spam checks and antivirus scans should be performed on the incoming gateways.

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 - The IP address 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:

- 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

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.
• Message Delivery Priority - The priority level assigned to this user's messages.
• Description - A brief summary why the sender priority override was created.

Activation

Licensing

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 actions toolbar:

- Activate - Activates a new SmarterMail license key.
- Reactivate - Reactivates a SmarterMail license key.
- 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 trial.

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

Antivirus Administration

SmarterMail is equipped with effective and self-updating ClamAV antivirus protection out-of-the-box. In addition, SmarterMail can support additional third-party solutions that include a quarantine directory. 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

- Enable ClamAV - Select this checkbox to enable ClamAV.
- Enable Real-Time AV - Select this checkbox to enable Real-Time AV.
- Enable Command-Line AV - Select this checkbox to enable a command-line virus scanner.
- Enable Commtouch Zero-hour Antivirus - Select this checkbox to enable the Commtouch Zero-hour Antivirus add-on.

ClamAV

Clam AntiVirus is a third-party open source antivirus toolkit, designed especially for scanning email on mail gateways. 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 to wait before moving on. By default, the timeout is 10 seconds.
• Failures Before Disable - The maximum number of timeouts allowed before ClamAV 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. To manually update virus definitions, click Update ClamAV in the actions toolbar.

Real-Time AV

• Quarantine Directory - The full path to the quarantine directory for the server.
• Virus Action - The action taken when an email contains a virus. The available actions are:

• Delete - Deletes any files attached to the message from the spool directory. This does not take any action on the quarantine directory.
• Inform Sender - Informs the "From" address that a message was received by the server, and because a virus was found in the message, it did not reach the intended recipient. Note: With some of the more recent viruses, this action becomes less useful, as many viruses now spoof the "From" email address.

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.

Commtouch Zero-hour Antivirus

The Commtouch Zero-hour Antivirus add-on uses Recurrent Pattern Detection technology to identify identifies 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.

Commtouch 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 Commtouch 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 .

Antispam Administration

SmarterMail's antispam features 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.

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.

In short, when an email comes in, spam checks are run on it. The checks that fail add points to the email, which then put the email into a category of spam probability.

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 checkbox and click Save .

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

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, and all you need to do in SmarterMail is enable the spam check. Declude score will be included on spam line. For more information, visit www.declude.com .

SpamAssassin-based Pattern Matching

SmarterMail includes a proprietary pattern matching engine built upon the SpamAssassin technology.

- 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.

Remote SpamAssassin

SpamAssassin is a powerful, third party open source mail filter used to identify spam. 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 SpamAssasasin 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

Commtouch Premium Antispam

The Commtouch 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 Commtouch 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 .

Custom Headers

Email can be assigned spam weights based on headers in the message. To configure weights for custom headers, complete the following fields:

• Header - The custom header to search for in the email message.

- Value - The value of the custom header.
- Weight - The amount to add to the email message's spam weight.

Custom Body Rules

Email can be assigned spam weights based on the body text 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 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.

Bayesian Filtering

Bayesian filtering uses statistical analysis to identify whether or not an email appears to be spam. Bayesian filtering "learns" from previous spam-marked messages to progressively improve performance. Tying it together with blacklists and SPF allows you to be quite sure that email is or is not spam.

- Weight - The default weight for this spam check. If an email has a high probability of being spam based on its content, this is the value that will be added to the message's total spam weight.
- Max memory to allocate for filtering - Bayesian filtering can be memory intensive. As a result, SmarterMail allows you to configure the maximum resources that will be dedicated to Bayesian filtering. In general, the more memory you reserve for Bayesian filtering, the more accurate the results will be.
- Messages required for filter update - Once this number of messages have been processed as known-good or known-spam email, SmarterMail will reanalyze the filters to help your system protect against new spam threats. In this way, Bayesian filtering can become more tailored to handle the mail of the domains on the server.

DomainKeys

DomainKeys is an email authentication system designed to verify the DNS domain of an email sender and the message integrity. The DomainKeys specification has adopted aspects of Identified Internet Mail to create an enhanced protocol called DomainKeys Identified Mail (DKIM).

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 probablility 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.

Reverse DNS (Domain Name Sever)

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.

RBL Lists (Real-Time Blacklists)

RBL lists (also known as IP4R Lists) are publicly accessible lists of known spammer IP addresses. These lists can be a very important part of spam protection. To attach to a list, click Add List in the actions toolbar.

- 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.

• Hostname - The hostname of the RBL.
• Required Lookup Value - The expected value returned from an RBL if the sender's IP is listed with the RBL provider.
• Enable bitmap checking - Select this checkbox if the RBL supports bitmapping. DNS Server - Spam lists operate through DNS. As a result, each list provider gives out a DNS server that contains the blacklist. Enter it in this box. --%>

Filtering

Emails are filtered into one of four categories based on their total weight. If a weight is equal to or higher than a certain category, then it is assigned that probability of being spam. Use the Actions tab 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.

• 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)

Options

This tab contains options relating to the processing of spam and overridability.

• Auto Responders - Allows you to restrict what types of auto-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 Spam Assassin, Commtouch Premium Antispam, custom rules and Bayesian filtering. Note: Increasing this number will also increase the mail server's memory usage.
• Enable 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 intra-domain email - Check this to disable spam filtering when messages are sent from from within the same domain (e.g. user1@example.com to user2@example.com).
• Disable spam filtering on SMTP whitelisted IP Addresses - Check this to disable spam filtering on IP Addresses which have been added to a whitelist.
• 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.

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.

Greylisting

What is Greylisting and how does it work?

Greylisting is a new tool in the fight against spam. It will temporarily block incoming mail from a sender and then returns the mail to the sender's mail server with a message saying effectively, "try again later." The sending server must then retry sending the mail after the Block Period but before the Pass Period (see below for definitions of these values).

Greylisting is effective because spammers will not usually bother to attempt a second delivery, but legitimate e-mail servers will.

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 which would do automatic retries.

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. Enable Greylisting to SmartHosts - If this feature is enabled, it will determine whether or not SmartHosts are governed by Greylisting. This is determined by evaluating the MX record of the recipient's address and matching it against the IP address of any target server IP address configured in the SmartHost settings area. For more information, see the SmarterHosts section of the online help. --%> 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
- Any IP in the greylistBypass.xml file

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 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 can control which IP addresses are blacklisted (not allowed) from mail services on this machine, or whitelisted (trusted) to access the mail services on this machine.

To manage the blacklist, click the security icon and click Blacklist in the navigation pane.

To manage the whitelist, click the security icon and click Whitelist in the navigation pane.

Note: Whitelisted IP addresses are not subject to relay restrictions which you may have 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 server.

Adding/Editing an Entry

To edit a blacklist or whitelist, click Edit in the content pane toolbar. To create a new entry in the blacklist or whitelist, click New 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).
- Blacklist or Whitelist SMTP / POP / IMAP / Greylisting - Check the boxes for the protocols you wish to include in the blacklist or whitelist entry. The Greylisting checkbox is only available for whitelisted IPs, and if checked, the whitelisted IP will not be greylisted.

Blacklist / Whitelist

System administrators can control which IP addresses are blacklisted (not allowed) from mail services on this machine, or whitelisted (trusted) to access the mail services on this machine.

To manage the blacklist, click the security icon and click Blacklist in the navigation pane.

To manage the whitelist, click the security icon and click Whitelist in the navigation pane.

Note: Whitelisted IP addresses are not subject to relay restrictions which you may have 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 server.

Adding/Editing an Entry

To edit a blacklist or whitelist, click Edit in the content pane toolbar. To create a new entry in the blacklist or whitelist, click New 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).
- Blacklist or Whitelist SMTP / POP / IMAP / Greylisting - Check the boxes for the protocols you wish to include in the blacklist or whitelist entry. The Greylisting checkbox is only available for whitelisted IPs, and if checked, the whitelisted IP will not be greylisted.

SMTP Authentication Bypass

SMTP Authentication is a security measure that can be very beneficial in the fight against spam and unauthorized email. 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 the 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 new IP addresses 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 systemadministrators to list specific email addresses (such as jsmith@example.com) or domains (such as example.com) that will be exempted from 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).

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 Abouse 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).

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) Prevention - 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 Type - Select the service that will be monitored for this type of attack (POP/SMTP/IMAP/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 hits the threshold.

Bad SMTP Sessions (Email 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. 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 targetting, 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 hits the threshold.

Internal Spammer Detection and Notification - Enabling this feature in SmarterMail will alert an administrator whenever a multiple emails are received on the server of the same size.

- Time Frame - The period of time in the past that is examined to determine if an alert should be sent. Too many duplicate emails in this period of time, and an alert will be sent.
- Messages Before Notify - After this many duplicate messages are received within the time period specified, the email notification is sent.
- Email to Notify - The administrator account to which the notification will be sent.

Password Requirements

To ensure the security of the mail server and its mailboxes, system administrators can specify minmum 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.
- Require a number in the password - Select this option to force users to include a number in the password.
- Require a capital in the password - Select this option to force users to include a capital letter in the password.
- Require a lowercase 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.

SMTP Blocked Senders

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.

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

Adding a SpamAssassin Server

To add a SpamAssassin server go to the SpamAssassin page in the Security menu. Here you will be presented with a list of servers currently set up to run SpamAssassin checks. To edit one of these servers simply click on it in the list, see below for a complete list of options. To add a new server simply click the Add SpamAssassin Server button, see below for a complete list of options. When you are finished adding the server click on the save button to add it to the list. For more information on downloading and installing SpamAssassin on your server please check out their website .

Add SpamAssassin Server Form

- Name - The name you wish to call this server
- IP Address - The IP address of the server running SpamAssassin
- Port - The SpamAssassin port on the server running SpamAssassin (783 by default)
- Multithreaded - If the server you have installed SpamAssassin on is a Linux machine it is recommended that you check this. If it is running on a Windows machine you cannot have this selected.

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>

<p><a href= "JavaScript:GoToMail()" > Log into your mail </a></p>

</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.

To receive notifications of every update that SmarterTools releases for SmarterMail, go to the SmarterTools Customer Portal , login, select Account Management, then select Mailing Lists, and

choose the "Updates.SmarterMail" subscription. Whenever a new update for SmarterMail is released, an email is sent to that mailing list. The list is not used for any other purpose.

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.
- Go to the General Settings page under the Settings menu.
- Click on the Security tab.
- Change Catch-Alls to Disabled.
- Click on Save icon.

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.
- Go to the General Settings page under the Settings menu.
- Click on the Security tab.
- Change Auto-Responders to either Disabled or Require SPF.
- Change Bouncing to either Disabled or Require SPF.
- Click on Save icon.

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.
- Go to Manage Domains.
- Click on the Actions menu next to the domain and choose Edit Domain.
- Go to the Technical tab.
- Check the Require SMTP Authentication box.
- Click on Save icon.

It is also recommended that you update this setting in Default Domain Settings so that all new domains will require SMTP Authentication.

To apply this setting to all domains on your server at once, use the Default Domain Settings 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.org/

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 General Settings in the left tree view.
- Click on the Administrator tab.
- Enter the current password for verification.
- Enter a new username and password (avoid using an email address for the username).
- Click on Save icon.

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 manage icon . Then select the desired domain in the content 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.