Help for System Administrators

Help Documentation

Help for System Administrators

How to Login - System Admin

You will need to open a web browser to the location of your 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 admin username and password on the login screen. 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).

By checking the "Remember Me" box SmarterMail encrypts your login and password. You can then close the browser window and not have to re-log in when you return. This function works as long as you do not "log out" of SmarterMail prior to closing your browser window. If you do log out, you will have to log back in upon your return, regardless of whether the "Remember Me" box was checked or not. You will need cookies enabled on your browser for this feature to work.

Manage

Create a New Domain

To create a new domain, click the Manage button on the main toolbar and click the New Domain in the left tree view. 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 loginand is only used to check for SMTP, POP, and IMAP traffic. This IP address should match at least one MX record on your DNS server.

• Folder Path - The directory in which all information (XML files, mail statistics, alias information, etc.) pertaining to the domain is saved. Note: If the directory does not already exist, it will be created. This directory should be soley dedicated to SmarterMail.
• Mailing List Username - The email address for which listserv commands are emailed.
• Domain Administrator Username - The identifier the domain administrator uses to log in to SmarterMail. The domain administrator is responsible for adding and deleting email accounts, and setting specific configurations for the domain.
• 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 log in 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:

• 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 our 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 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 Email Reports - Select this option to provide the ability to email reports.
• Enable IMAP Retrieval - Select this option to allow users to download POP 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 IMAP 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.
- 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 X Threshold - The number of retry attempts the system should make before the priority set in Priority After Attempt X is assigned to the message.
• Priority After Attempt Y - 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 Y Threshold - The number of retry attempts the system should make before the priority set in Priority After Attempt Y 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 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.

View Logs

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 the Download icon from the Actions toolbar.

Log file settings can be configured by clicking the Settings button from the main toolbar, and then selecting Log Settings from the left tree view.

Date - Enter the date which you would like to view log files from.

Type - Select the delivery method from the drop down box that you would like to analyze.

Search String - Enter a string of words that you would like to search.

Enable Related Traffic - Enable this box if you would only like data shown that occurred within the same session.

Note: SmarterMail will show logs files up to 1MB.

Enabling and Disabling Services

Arrive at this page by clicking the Manage button on the main toolbar, then selecting Services from the left tree view. This page allows system administrators 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 Manage in the main toolbar and then click Services in the left tree view. 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 actions 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.

Create a New Domain

To create a new domain, click the Manage button on the main toolbar and click the New Domain in the left tree view. 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 loginand is only used to check for SMTP, POP, and

IMAP traffic. This IP address should match at least one MX record on your DNS server.
• Folder Path - The directory in which all information (XML files, mail statistics, alias information, etc.) pertaining to the domain is saved. Note: If the directory does not already exist, it will be created. This directory should be soley dedicated to SmarterMail.
• Mailing List Username - The email address for which listserv commands are emailed.
• Domain Administrator Username - The identifier the domain administrator uses to log in to SmarterMail. The domain administrator is responsible for adding and deleting email accounts, and setting specific configurations for the domain.
• 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 log in 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:

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

• Enable IMAP Retrieval - Select this option to allow users to download POP 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 IMAP 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.
• 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 X Threshold - The number of retry attempts the system should make before the priority set in Priority After Attempt X is assigned to the message.
• Priority After Attempt Y - 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 Y Threshold - The number of retry attempts the system should make before the priority set in Priority After Attempt Y 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 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.

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 button in the main toolbar and expand the Spool in the left tree view. Then click All Messages . To only view the messages waiting to be delivered, click the Manage button in the main toolbar and expand the Spool in the left tree view. 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 actions 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 actions 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 have the ability to monitor the activity of all users on their server. Each user will be listed individually who is logged into the system. To get started with User Activity, click the Manage button from the main tool bar and then select Online Users from the User Activity tree view on the left side. They can monitor each user by the following variables:

Type - This will tell the System Admin whether they are connected with IMAP or Web mail.

IP Address - This will tell the IP Address of the user.

Start Date - This will tell the Start Date the user made the connection.

Duration - This will tell the total duration of the connection.

The System Administrator also have 3 actions he can perform from the actions tool bar&mdash: End Session , Disable User , and Search .

End Session - This will end the current session of any particular user.

Disable User - This will permanately disable the user from the system.

Search - This gives the System Admin the ability to search users on the system.

Inactive Users

System Administrators have the ability to search and find users who have been inactive from the

system. To perform this search, click the Manage button from the main toolbar, and then select Inactive Users from the left tree view.

System Administrators have four options to choose from for the search&mdash: Inactive for 30 Days, Inactive for 90 Days, Inactive for 6 months, and Inactive for 12 months.

Current Connections

SmarterMail will monitor the server and see who is connecting via the different protocals&mdash: SMTP, IMAP, and POP. System Administrators can then blacklist a certain user by clicking the Blacklist icon on the actions toolbar if they believe a user is making too many connections.

Users can be viewed by All Connections from the left tree view, or by each protcol individually.

Current Blocks

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

Email harvesting can also be monitored, which is the process of obtaining lists of e-mail addresses using various methods for use in bulk e-mail or other purposes usually grouped as spam.

System Adminstrators can then click the Delete icon from the actions 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 get started with a mass email, click the Manage button on the main toolbar, then select Send Email from the Mass Messaging tree view. After clicking Send Email you will be asked to populate the following fields:

From - Enter here who the email is from. "System Administrator" will be entered as a default.

To - Choose from the drop down menu who you want to receive the email. (All Users, All Users on Domain, All Domain Administrators, Specific User) 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 - Enter the subject of the email in this field.

Message - Enter the message you would like to send.

Once you complete all the fields, click the Send icon in the actions toolbar to send the message.

Send Reminder

To get started with a mass email, click the Manage button on the main toolbar, then select Send Reminder from the Mass Messaging tree view. After clicking Send Email you will be asked to populate the following fields:

To - Choose from the drop down menu who you want to receive the email. (All Users, All Users on Domain, All Domain Administrators, Specific User) 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 - Enter the subject of the email in this field.

Message - Enter the message you would like to send.

Once you complete all the fields, click the Send icon in the actions toolbar to send the message.

Message Archive Search

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.

To search the archive, click the Manage button in the main toolbar and click Message Archive Search in the left tree view. 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 the Email button in the main toolbar and clicking Message Archive Search in the left tree view.

For more information on archiving, see Message Archiving .

Reports

Reports Overview

System administrators, domain administrators, and individual users can use real-time mail server statistics, historical summary reporting, and detailed trend analysis at the system, domain, and user

levels to understand the performance of their systems. With dozens of pre-defined reports, SmarterMail provides critical statistics that help system and domain administrators monitor their systems.

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

Settings

General Settings

To access the general settings for SmarterMail server, click the Settings button on the main toolbar, then click the Settings navigation pane and click General Settings in the left tree view. The general settings will load and the following tabs will be available:

Administrator

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 log in. 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.

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 to Run on New Mail - 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.

Protocol Settings

To access the settings for standard email protocols, click the Settings button on the main toolbar, then click the Settings navigation pane and click Protocol Settings in the left tree view. 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.

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 button on the main toolbar and click the Settings control bar. Then click ActiveSync Mailboxes in the left tree view. 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.

Hostnames

To get started with Hostnames, click the Manage button on the main toolbar, then select Hostnames from the left tree view.

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. Prior to this addition, SmarterMail could only specify one hostname for all IPs.

Notification Profiles

Customize notification profiles for any group on your account. Assign events to your profiles which can utilize any number of notifications such as reminders, SMS, or Email.

To set your profile, click the Settings button on the main toolbar, then select Notification Profiles from the Settings folder tree view.

Adding a Profile - To add a new profile, click the New icon from the actions toolbar.

- Name - This can be any name that will help you recognize this profile.
- Email Address - If you would like a reminder sent to an email, enter it here and check the enable box.
- SMS Email - If you would like a reminder sent as a text message, enter it here and check the enable box.
- Enable Reminders - Check this box if you would like a popup window reminder for Tasks and Appointments.

Once you have completed all boxes to your satisfaction, click the Save icon from the actions toolbar.

Edit a Profile - Editing a profile can be done in three different ways:

- Select the profile that you would like to edit and then click the Edit icon from the actions toolbar, or
- Move your mouse over the profile you want to edit and right-click, then select Edit from the drop down menu, or
- Double-click the profile that you would like to edit

Deleting a Profile - Deleting a profile can be done two different ways:

- Select the profile that you would like to delete and then click the Delete icon from the action toolbar, or

- Move your mouse over the profile you want to delete and right-click, then select Delete from the drop down menu

Searching a Profile - To search your profiles, first click the Search icon from the actions toolbar. Another toolbar will appear under the actions toolbar with two boxes to populate. The first box asks for the search criteria that you would like to search for. The second box is a drop down list looking for what fields you want to search through—All Fields, Name, and Type.

Skins

The SmarterMail Web interface contains built-in skins for your convenience.

The various skins can be found by clicking the Settings button on the main toolbar, then selecting Skins from the Interface folder tree view. Users can also create custom skins to emulate their own style or that of their company.

Default Skin - These are the available skins provided by SmarterMail.

Enable ability for domains to override skin - Enable this to allow Domain Admins to choose a skin for their domain.

Log Settings

In order for you to know what activity is happening on your server, SmarterMail has multiple logging options for various parts of the mail server. Use this page to manage how logs are written and how much detail is written.

To get started, click the Settings button on the main toolbar, then select Log Settings from the Settings tree view. Settings will not be applied to any tab until you click the Save icon from the actions toolbar.

Log Files

Log Path - This is 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 - Log files older than the number of days specified in this field will be automatically deleted when enabled.

Log Detail Levels

These settings change the amount of detail that is stored in the protocol logs. Possible values for each are shown below:

- 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.

Delivery Log Level - The log level for message delivery and spool operations.

IMAP Log Level - The log level for IMAP 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.

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 button on the main toolbar and click the Settings navigation pane. Then expand the Defaults folder and click Domain Defaults in the left tree view. 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 X Threshold - The number of retry attempts the system should make before the priority set in Priority After Attempt X 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 Y Threshold - The number of retry attempts the system should make before the priority set in Priority After Attempt Y 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 button on the main toolbar and click the Settings navigation pane. Then expand the Defaults folder and click Domain Propagation in the left tree view. 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 button on the main toolbar and click the Settings navigation pane. Then expand the Defaults folder and click User Defaults in the left tree view. 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 button on the main toolbar and click the Settings navigation pane. Then expand the Defaults folder and click User Propagation in the left tree view. The default domain settings will load in the content pane. For more information on these settings, refer to Users .

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

Routing

Forwarding Blacklist

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 button on the main toolbar and click the Settings navigation pane. Then expand the Routing folder and click Message Archiving in the left tree view. A list of archiving rules will load in the content pane.

To create a new archiving rule, click New in the actions toolbar. To edit an existing rule, select the appropriate rule and click Edit in the actions 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.

Options

Server Address - Enable this and add the IP address of the Gateway Server.

Auth Username - Enable this and enter the username of the gateway server given to you by your ISP.

Auth Password - Enter a password for your gateway server.

Priority Range - Set 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

SmarterMail URL - The Webmail URL for the SmarterMail server being used an an outgoing gateway. This will allow the use of web services to find out how many messages are in the spool in order to do an intelligent round robin distribution.

Admin Username - The identifier used to log in to the gateway server.

Admin Password - The corresponding password used to log in to the gateway 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 button in the main toolbar and click the Settings navigation pane. Then expand the Routing folder and click Incoming Gateways in the left tree view. A list of incoming gateways will load in the content pane.

To add a new incoming gateway, click New in the actions 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 XXX

- 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 log in to the primary mail server.

• SmarterMail Password - The corresponding password used to log in 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 button in the main toolbar and click the Settings navigation pane. Then expand the Routing folder and click Sender Priority Overrides in the left tree view.

To create a new sender priority override, click New in the actions 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 button on the main toolbar and click the Settings navigation pane. Then expand the Activation folder and click Licensing from the left tree view. 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 button in the main toolbar and then click the Settings navigation pane. Then expand the Activation folder and click SmarterMail Self Diagnostic from the left tree view. 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 button in the main toolbar and then click Antivirus Administration in the left tree view. 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.

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 button in the main toolbar and then click Antispam Administration in the left tree view. 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 typs 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 - XXX
• 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.

• 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 button on the main toolbar, then select Greylisting from the Email Protection folder tree view.

- 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).
- Enable Greylisting - If this is enabled it will allow Greylisting to happen.
- Enable Users to Override Greylisting - Enable this to allow users to selectively turn off Greylisting (useful if you have an account that receives time sensitive mail).

• 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

From this page you 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 get started with Blacklists, click the Security button on the main tool bar, then select Blacklist from the Security folder tree view.

To get started with Whitelist, click the Security button on the main tool bar, then select Whitelist from the Security folder tree view.

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.

New icon - Click on this button to add an IP address or an IP address range to the list.

Edit icon - Click on a row to edit the whitelist or blacklist settings for the entry.

Delete icon - Click on this link to remove an entry from the list.

Adding / Editing an Entry

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

From this page you 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 get started with Blacklists, click the Security button on the main tool bar, then select Blacklist from the Security folder tree view.

To get started with Whitelist, click the Security button on the main tool bar, then select Whitelist from the Security folder tree view.

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.

New icon - Click on this button to add an IP address or an IP address range to the list.

Edit icon - Click on a row to edit the whitelist or blacklist settings for the entry.

Delete icon - Click on this link to remove an entry from the list.

Adding / Editing an Entry

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 button on the main toolbar, then select SMTP Authentication Bypass from the Security folder tree view.

New Icon - Click on this button to add additional IP addresses to the bypass. More information can be found below.

Edit Icon - Editing and item can be done three ways:

- Select the item and then choose the Edit icon from the actions toolbar, or
- Right-click the item and choose Edit from the drop down list, or
- Double-click the item you would like to edit

Delete Icon - Deleting an item can be done two ways:

- Select the item and click the Delete icon from the actions toolbar, or
- Right-click the time and select Delete from the drop down list

Adding a Bypass

IP Address - Enter a single IP address in dotted quad notation (X.X.X.X) in this box if you want to bypass 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 bypassed (ex: 192.168.1.1 - 192.168.1.255).

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 get started, click the Security button on the main toolbar, then select Abuse Detection from the Security folder tree view.

Once you arrive on the Abuse Detection screen, you will see three icons on the actions toolbar— New , Edit , and Delete .

When clicking the New icon on the actions toolbar you will have these options:

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.

Edit Icon - Editing and item can be done three ways:

- Select the item and then choose the Edit icon from the actions toolbar, or
- Right-click the item and choose Edit from the drop down list, or
- Double-click the item you would like to edit

Delete Icon - Deleting an item can be done two ways:

- Select the item and click the Delete icon from the actions toolbar, or
- Right-click the time and select Delete from the drop down list

Password Requirements

Minimum Password Length - This will allow System Administrators to designate the minimum numbers of characters a password requires.

Password Strength Requirements - The System Administrator is able to set the requirements for passwords and, as a result, all users must adhere to those standards. The password options available to the System Administrator are: Number, Capital Letter, Lower Case Letter, Symbol, Not User Name.

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 get started, click on the Security button on the main toolbar, then select SMTP Blocked Senders from the Security folder tree view.

Blocked Senders - Enter the email addresses or domain names you want to block, one per line. The asterisk (*) wildcard symbol is permitted in the list.

SSL

This page is available in Enterprise Edition only

SmarterMail allows System Administrators to add Secure Socket Layer (SSL) and Transport Layer Security (TLS) rules.

To get started click the Security button on the main toolbar, then select SSL from the Security folder tree view.

When adding a new rule there are several fields that need to be addressed. These fields are:

IP Address - This is the IP address where SmarterMail will listen.

SMTP, POP, IMAP - Determines on which port SmarterMail will listen for the respective protocol.

Type - Sets the type of rule you would like to add, SSL or TLS. SSL always assumes the connnection will be secure, and therefore, sends the encryption immediately. TSL connects normally, and then looks to see if the connection is secure before sending the encryption.

Certificate Path - The path to the certificate file on the server. Typically, named a *.cer file.

- 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.

Please Note: When removing a SSL rule, the System Administrator will need to perform a service restart.

Edit Icon - Editing and item can be done three ways:

- Select the item and then choose the Edit icon from the actions toolbar, or
- Right-click the item and choose Edit from the drop down list, or
- Double-click the item you would like to edit

Delete Icon - Deleting an item can be done two ways:

- Select the item and click the Delete icon from the actions toolbar, or
- Right-click the time and select Delete from the drop down 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 Topics

Automating LogIn to SmarterMail

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

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

altered to reflect this change. This example demonstrates how easy and powerful the Smartermail application is in allowing companies to automate entry into the mail application.

<html>

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

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

<body>

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

 Log into your mail

</body>

</html>

Gateways and Other Server Roles

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

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

Primary mail server

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

- Follow instructions in online help

Backup MX Server

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

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

Incoming Gateway server

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

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

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

Outgoing Gateway server

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

- Use as a delivery mechanism to reduce load on your primary servers.
- Also use as a method to combat blacklisting. If the server gets blacklisted, rotate the primary

IP on the network card to a different one to send out on the new IP.

• To configure:

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

SmartGateway server

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

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

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

Backup MX Servers

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

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

Case 1 - No Backup MX

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

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

Case 2 - With a Backup MX

How Email works when a Backup MX Server is involved:

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

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

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

Configuring a Backup MX Server

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

Locking Down Your Server

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

What is Security for a Mail Server?

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

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

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

- Update SmarterMail regularly
- Disable catch-all accounts
- Restrict bounces and auto-responders
- Require SMTP authentication
- Encourage the adoption of SPF

Update SmarterMail Regularly

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

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

- Log in 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 on Resetting an Administrator Login .

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 log in 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 button on the main toolbar and then click the Impersonate icon on the actions 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.

Glossary

Below is an alphabetized list of the various terms and phrases used in the SmarterMail Product.

SMARTERTOOLS END USER LICENSE AGREEMENT

SmarterTools, Inc. Software License Terms

This End User License Agreement ("EULA") is between SmarterTools, Inc. ("SmarterTools") and the License holder ("You") of the software product this EULA accompanies ("Software"). It is important to read and understand all of the terms, limitations, and conditions contained in this EULA prior to installing and using the Software because they affect how You may use the Software and Your rights under this License. By explicitly accepting this EULA, or by installing, copying, downloading, accessing, or otherwise using the Software, You agree to be bound by the terms of this EULA. If, prior to using or installing the Software, You decide that You are unable or unwilling to agree to the terms of this EULA, promptly and completely uninstall and destroy any electronic copies of the Software and accompanying items in your possession.

This EULA shall apply to:

* This Software

* Future Versions of this Software

* Updates, add-ons, and plug-ins to this Software, as may be made available by SmarterTools from time to time, including but not limited to language packs, dictionaries, and skins (collectively "Updates")

* Features selection(s), including, but not limited to, "Professional," "Enterprise", and "Free" editions of the Software, and maximum allowed numbers of users, profiles, devices, email addresses domains, web sites, or agents ("level");

* Services, support, advice, and recommendations related to this Software that may be made available by SmarterTools on the Internet, in the Software documentation, or by telephone

* Any and all Technical Support Services offered in connection with the Software

DEFINITIONS

The following definitions shall apply for the purposes of this EULA:

* "Dedicated Hosting" shall refer to an individual, group, or organization ("Dedicated Host") that maintains a physical server device that is wholly or, in the case of Virtual Private Servers ("VPS"), a dedicated portion of a physical server device that is sold, leased, or otherwise made available to a third party; whether or not a fee or other compensation is exchanged; and in which the third party has authorization and/or access to the activation areas of the software and/or to system administration functions.

* "Effective Date" shall be the date upon which this EULA was accepted by You.

* "Elastic Computing" shall refer to a user's ability to install software, create websites or instantiate a database on one or more Workers that can then be given incremental CPU cycles or percentages, memory (RAM) allocations, and/or physical disk space and bandwidth allocations that can all, then, be managed (increased or decreased) separately and on an as needed basis.

* "Failover" is the ability of a system to automatically switch to a second, standby system should the primary system fail or is temporarily shut down.

* "License" shall refer to the revocable, non-exclusive, non-transferable license to use the Software ("License") in accordance with the terms and conditions of this EULA. The term License applies to purchased and non-purchased Licenses, including but not limited to the object code, source code, and any accompanying alphanumeric combinations used to enable and/or activate the software or certain Features Selection(s) in the Software (collectively, "License Keys").

* "License Key" shall apply to the alphanumeric combination entered/applied upon installation and used to access Feature Selections. License Keys are delivered to the owners of purchased (paid for) Licenses and to those who may receive authorized promotional or trial Licenses, if applicable (pursuant to this EULA). SmarterTools may create and provide certain Levels, Editions, and/or Versions of the Software that do not require entry or use of a License Key for promotional or other purposes. This EULA remains in full force and effect whether or not a License Key is required or provided by SmarterTools.

* "Load Balancing" is a networking methodology whereby processing and workload is distributed evenly among a group of independent machines (e.g., servers) so that no single device is overwhelmed and so that there is no single point of failure.

"Multi-tenancy" and "Multi-tenant license(s)" shall refer to the ability of any single license to support multiple separate and unique client organizations, particularly when offering a single license in a Software as a Service (SaaS) capacity. For the purposes of this EULA, only SmarterStats and SmarterMail are multi-tenant licenses.

* "Periodic License" shall be a License with a defined temporal component (start and end date) whether or not such License is subject to renewal, automatically renews, effectively terminates, or is extended (e.g., Monthly/Lease Licenses, Trial Licenses, Development Licenses). Periodic Licenses may be governed by additional terms and conditions in a separate written agreement.

* "Third Party Providers" shall be any other software, application, plug-in, add-on, utility, tool, device, or methodology by any individual, group, organization, affiliation, company, or other entity that connects, modifies, links, and/or integrates to/with the Software for any purpose whatsoever.

* "Shared Hosting" shall refer to an individual, group, or organization ("Shared Host") that maintains a physical server device upon which software and/or tools are owned and installed by the Shared Host and made available to third parties for access or use; whether or not a fee or other compensation is exchanged; and in which the third parties do not have authorization or access to the activation areas of the Software and/or do not have authorization or access to system administration functions.

* "Worker(s)" shall be the location where software, websites or databases are installed in an Elastic Computing environment. A Worker can then have CPU cycles, disk space and RAM allocations and bandwidth modified (i.e., increased or decreased) on an as needed basis to accommodate shifts in traffic and usage. Also known as a worker process.

1. License.

A. Grant of License.

Upon the the Effective Date, SmarterTools hereby grants You a revocable, non-exclusive, non-transferable license to use the Software ("License") in accordance with the terms and conditions of this EULA. This License shall commence on the Effective Date of this EULA and shall remain in effect until terminated in accordance with the terms of this EULA or superseded by another end user license agreement pursuant to installation of an Update or changes in Features Selection. SmarterTools, together with any third party content providers whose software code is incorporated in the Software or distributed with it, retains all right, title, and interest to the Software, including, but not limited to, copyrights, trademarks, proprietary methods, and trade secrets incorporated into the Software.

This License is subject to any restrictions SmarterTools, in its sole discretion, may impose in this EULA or imposed as a condition of purchase, including but not limited to the particular Features Selection You chose at the time of purchase. Updates and Features Selection are subject to the terms

and conditions of this EULA, or any other end user license agreement provided with such Update or Features Selection at the time of receipt or purchase, which shall supersede this EULA.

This License to use the Software is conditioned upon You paying all related charges and fees imposed by SmarterTools for purchase of the Software, monthly-license of the Software, or for the authorized delivery of the Software as a service (SaaS). SmarterTools may, in its sole discretion, terminate this License if You fail to pay such charges or fees within the time allowed by SmarterTools.

B. Use of the Software.

You shall use the Software for Your own personal or internal business purposes. Personal or internal business purposes shall include the installation of the Software and activation of only one License on any single personal computer or server; one instance of a Virtual Private Server; or in the case of Elastic Computing, on any single Worker for Your own use or use by Your Customer(s) pursuant to the terms of section 1.C. below. Should SmarterTools designate that a specific license can be used for Failover, then You may install that license on a second machine that matches the exact specifications of the initial installation machine, and use that second machine as a Hot Standby. Should SmarterTools designate that a license can be used for Load Balancing, then You may install that license on as many similarly-configured machines as necessary to meet any Load Balancing requirements.

C. Sublicense, Resale, Lease, Sub-lease ,or Transfer

You may sublicense this License to a third party(ies) ("Customer") only pursuant to a Shared Hosting agreement and the terms and conditions of this EULA, if applicable. You represent and warrant that each Customer has accepted this EULA prior to allowing the Customer access to or utilization of the Software and You shall promptly provide confirmation of each Customer(s)'s acceptance of the EULA upon request by SmarterTools. You shall indemnify, defend, and hold SmarterTools harmless against any claims asserted by or against You by any of Your Customer(s) or by any third party related to Your Customer(s)'s use of the Software, including but not limited to claims of infringement of the intellectual property rights of any third party and the additional warrantee, liability, and indemnification provisions found in Sections 3 and 5.

Certain authorized parties ("SmarterTools Authorized Reseller") may Resell, Lease, Sub-lease, or Transfer this License (collectively, "Transfer") to any third party subject and pursuant to a separate authorizing agreement in writing with SmarterTools (e.g., Master Partner Agreement). For the purposes of this EULA, Transfer shall refer to any transaction whereby sole use, management, ownership, and/or control of the software is assigned to any third-party for that party's benefit, pursuant to the terms and conditions of this EULA, whether or not a fee or other compensation is charged and whether or not such Transfer is permanent or temporary. Transfers by or between any

party(ies) other than SmarterTools or a SmarterTools Authorized Reseller must be approved by SmarterTools in advance and in writing.

You may install and maintain the Software on behalf of a third party; however, all SmarterTools Licenses in such circumstances must be purchased by the third party directly through SmarterTools or through a SmarterTools Authorized Reseller and the Software must be activated under the name of the related third party; thereby, the related third party assumes full ownership of the License subject to the terms and conditions of this EULA.

D. Limitations on Use of the Software and License Keys

You shall not modify, reverse engineer, reverse assemble, decompile, disassemble, decrypt, reflect, or use reflection on the Software, or otherwise attempt to discover or obtain the source code or structure, sequence, or organization of the software in whole or in part, except as provided in Section 9 of this EULA. You may distribute copies of the software code in the same format that you received it, pursuant to the terms of this EULA, so long as You do not modify the Software in any way and so long as all copyright, trademark, and other notices contained in the Software remain intact.

The Software may periodically and automatically contact SmarterTools pursuant to Section 10 of this EULA. This contact may occur without any notice to You of such contact, and You hereby consent to such contact with SmarterTools. You shall not disable, delay, dismantle, disrupt, or otherwise interfere with the ability of the Software to contact or communicate with SmarterTools or the authentication of License Keys. Further, You shall not attempt to bypass, circumvent, disable, design around, or obviate the License Keys for any reason, including but not limited to attempts to access features, capacity, or capabilities in the Software not included in your Features Selection. Further, other than pursuant to Section 1.C. of this EULA, You shall not disclose or disseminate any License Keys associated or distributed with the Software, publicly or to any third party, nor shall You allow anyone else to use any such License Keys.

You may reassign/migrate this Software to a different device owned, leased, or rented by You subject to SmarterTools' approval in its sole discretion, provided that You completely uninstall or delete the Software from any personal computer, server, Virtual Private Server, Elastic Computing Worker or other device on which the Software was previously installed. SmarterTools reserves the right to require, in its sole discretion, reauthorization, re-registration, or another form of authentication at no additional charge to enable reassignment of the Software, and may disable the related License Key and/or access to the Software at any time if it determines, in its sole discretion, that such reassignment is prohibited by the terms of this EULA or constitutes fraud.

You shall not use the Software to harm third parties, disseminate unsolicited communications (emails, etc.), requests, or harmful data or programs including but not limited to malicious scripts and viruses.

You shall not use the Software to disseminate pornography, child pornography, or other harmful or illegal materials, or in any way that may disparage or bring disrepute to SmarterTools.

2. Term and Termination.

This EULA is effective as of the date You install or use the Software, or as of the date You accept this EULA, whichever is sooner. You may terminate this EULA by completely deleting and wholly destroying any copies of the Software and documentation in Your possession or control. SmarterTools may terminate and/or disable the License or EULA if, in its sole discretion, SmarterTools determines that You have breached any of the terms and conditions of this EULA, with or without notice to You of such termination.

Sections 1.B., 1.C., 1.D., 3, 5, 6, 7, 8, 9, 10, 11, 12, and 13 shall survive termination of this EULA.

3. Limited Warranty and Limitation of Liability.

A. No Warranties

SmarterTools does not warrant that the Software will meet Your requirements, that the operation of the Software will be uninterrupted or error-free; that any data supplied by the Software will be accurate; or that the Software will work with any 3rd-party or supplemental software or hardware furnished with or accompanying the Software. Further, SmarterTools does not warrant the efficacy, functionality, or operation of such Accompanying Software or Hardware. ALL HARDWARE, SOFTWARE, OR OTHER PRODUCTS OR SERVICES PROVIDED BY SMARTERTOOLS UNDER THIS EULA ARE PROVIDE AS-IS, AND SMARTERTOOLS EXPRESSLY DISCLAIMS ALL WARRANTIES, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

B. No Liability for Damages

SmarterTools shall not be liable for any damages under this EULA, including but not limited to consequential, statutory, punitive, incidental, or indirect damages, including but not limited to any loss of data, loss of profits, loss of savings, loss of time or convenience, or additional cost arising out of the use of or inability to use the Software, documentation, support, or any 3rd-party or accompanying software or hardware; even if SmarterTools has been advised of the possibility of such damages. Further, SmarterTools shall not be liable for nor bound by any claims, representations, promises, assertions, or other statements made by anyone other than SmarterTools employees or officers, including but not limited to resellers and sales representatives. SmarterTools shall not be liable for any damages or inconvenience resulting from errant data or misreporting of data, nor failures to relay information that may be deemed important by the user, any errant or substantial mistranslation of language or information, and/or for any damages arising from events listed in Section 5 of this EULA.

C. Third Party Providers and Web Services

The Software is designed to integrate and/or to be used in conjunction with Third Party Providers through Web services. SmarterTools assumes no liability and makes no warranty or guarantee regarding the applicability of effectiveness of this Software when used in conjunction with these products or whether or not such integration or use might interfere with the operation therein. You agree to hold SmarterTools harmless in all matters resulting from the integration or use with Third Party Providers.

D. Limitation of Liability

Your sole remedy under this Agreement shall be limited to replacement of the Software.

4. Technical Support

Currently, SmarterTools provides technical support for the Software via SmarterTools personnel, documentation, and Internet resources. Depending on Your Features Selection, including but not limited to pricing, volume, Software version, and the number of licenses You purchased, a certain amount of technical support may be included at no additional charge. Otherwise, technical support may be available for an additional charge on a per incident, per call, or per time-frame basis or in other support packages. The amount of these charges may vary from time to time. Technical support is provided AS-IS, and the provisions of section 3.A., 3.B., and 3.C. apply to technical support.

SmarterTools provides no guarantee, expressed or implied, regarding the efficacy or continuation of technical or other support for this Software or particular version of this Software for any length of time and SmarterTools may choose to discontinue such support at any time and for any reason.

5. Indemnification.

You shall defend, indemnify, and hold harmless SmarterTools and its suppliers, licensors, successors, affiliates, agents, employees, executives, and assigns (hereafter "SmarterTools Indemnified Parties") from any claims, damages, losses, or expenses (including without limitation attorney fees and costs) incurred in connection with any and all damages, losses, claims, suits, judgments, or causes of action asserted against SmarterTools Indemnified Parties by third parties or Your Customers related to:

* Any claims arising from or related to Your use of the Software or use of the Software by Your Customers or any portion thereof, including but not limited to claims of infringement of patents, copyrights, or other intellectual property or proprietary rights arising from your use of the Software or from use of the Software or any portion thereof in combination with any other software, hardware, device, system, or service;

* Damages arising from Your breach or Your Customer's breach of this EULA;

* Any loss, misdirection, or inaccuracy of any and all data, message, and/or information (partial or complete) by or directed to You, Your Affiliates, Your Customers, Your vendors, Your assignees, or any related third party and from any action, inaction, or consequence arising out of such loss, misdirection, or inaccuracy of any data, message, or information;

* Any misuse, abuse, hostile transmission, fraud, or unlawful action arising from or related to the use of the Software or any portion thereof by or directed at You, Your affiliates, Your Customers, Your vendors, Your assignees, and/or any related third party;

* Any claim, damage, loss, or expense related to the installation, quality, use, operation, functionality, transfer, or de-installation of the Software to You, Your Customer(s), or third parties.

* Any charges imposed by You or third parties on You or Your Customers related to Your or Your Customer(s)'s use of the Software, including but not limited to charges for data transmission and bandwidth, regardless of whether you have followed any recommendations provided with the Software or Software documentation.

6. Transfers

The rights under the License may be sublicensed under the terms of Section 1.C. or transferred to any of Your successors, heirs, or assigns. Any other attempt to sublicense, assign, or transfer any of the rights, duties, or obligations hereunder is void unless You have a separate written agreement with SmarterTools allowing for such transfer(s).

7. Jurisdiction.

This Agreement shall be governed in all respects by the laws of the United States and the State of Arizona, except for conflict of law's provisions. The parties agree that for any dispute, controversy, or claim arising out of or in connection with this Agreement, venue and personal jurisdiction shall be in the federal, state, or local court with competent jurisdiction located in Maricopa County, Arizona. The prevailing party will be entitled to an award of reasonable attorney's fees.

In the case that You are an agency or entity of the United States Government, the following additional terms apply:

* The Software qualifies as Restricted Computer Software, as defined in the Rights in Data-General clause at Federal Acquisition Regulations 52.227-14.

* Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

8. Payments.

You shall pay the total fee(s) for the Software imposed by SmarterTools at the time of purchase. You shall pay all invoices rendered by SmarterTools within thirty (30) calendar days after the invoice date, or within another time frame set forth by SmarterTools in writing in a separate agreement. All payments shall be made in United States Dollars ($). If You fail to pay any amount due within the above timeframe, SmarterTools may impose late charges equal to the lesser of 1.5% per month or the highest interest rate allowable by applicable law, together with all related expenses and collection costs, including reasonable attorneys' fees, incurred by SmarterTools collecting any amounts owed under this EULA. Further, You shall reimburse SmarterTools for any out-of-pocket expenses incurred in connection with duties performed by SmarterTools hereunder. Upon request by You, SmarterTools shall provide You with reasonable documentation evidencing the out-of-pocket expenses incurred by SmarterTools.

SmarterTools may disable License Keys for invoices that are not paid within a reasonable timeframe as determined by SmarterTools in its sole discretion. Licenses purchases that are made fraudulently, deceptively, or that result in a charge-back or disputed charge are considered to be not paid and are subject to disablement at the sole discretion of SmarterTools.

9. Limitations to Customization.

Should You choose to alter the appearance and/or user interface of the Software (the "Skin") by using the custom style or Skin options included in certain versions of the Software or by using a third-party process to alter the appearance or interface of the Software, the following requirements must be met:

* You shall maintain and not remove or obscure any proprietary notices in the Software. The SmarterTools name may be displayed in any font type or style, but it must be displayed in no smaller than 8-point font. The name of the Software shall remain visible to the naked eye and free from any clutter or similar color scheme (e.g. black font on a black or similarly dark background that would preclude the user from easily identifying the Software). Use of the qualifiers "powered by" and "provided by" is permitted (e.g. "Powered by SmarterMail"). Any deviation from these limitations must be approved in writing by SmarterTools in advance of implementation and may result in additional license fees, if applicable.

* All applicable copyright and trademark information shall not be removed, remain visible to the naked eye, free from any clutter or similar color scheme, and can be displayed in any font type or style but shall be displayed in no smaller than 8-point font.

10. Transmission of Information and Communication.

At purchase of the Software and at other times during the term of this EULA You will be required to supply certain information including, but not limited to, email address(es), password(s), personal and/or company information, payment information (e.g. credit card information), and/or other personally identifiable and potentially valuable information. Acceptance of this Agreement indicates Your willingness to provide this information and have it transmitted to SmarterTools via internet, phone, facsimile, verbally, or otherwise and Your assumption of the incumbent risks associated with such transfers. SmarterTools takes the privacy and security of data very seriously and will make efforts to protect data in accordance with our privacy policy. A copy of the SmarterTools privacy policy is available by request. In any event, SmarterTools and its suppliers, licensors, successors, affiliates, agents, employees, executives, and assigns shall not be liable for any stolen, misdirected, or otherwise mishandled information pursuant to this EULA.

From time to time SmarterTools may contact You at any address, including any email address(es), You have provided to SmarterTools regarding the Software, available Updates or Features Selection for the Software, or for promotional purposes. You hereby expressly consent to such communications. If you do not wish to receive further notices, you may notify SmarterTools of your preferences.

From time to time the Software may cause computers, servers, and/or other electronic devices on which You install and operate this Software to use the internet or other means to exchange data with computers, servers, or other electronic devices owned by SmarterTools in order to maintain licenses, communicate updates or instructions, track the location and install base of the Software, gauge performance, enforce SmarterTools' rights with regard to licensing and this EULA, or other information as is needed to properly maintain, protect, or update the Software. Acceptance of this Agreement indicates Your acceptance of this communication and Your assumption of the incumbent risks associated with such communication. Any attempt to prevent, preclude, disrupt, or modify this communication is not allowed under this EULA and may result in the disablement of the Software and license key.

11. Third-party Correspondence, Interaction, Purchase, Service, or Promotion

During use of the Software, You may enter into correspondence with, purchase goods and/or services from, or participate in promotions of third party advertisers or sponsors displaying goods and/or services through the Software. Any such activity, and any terms, conditions, warranties, or representations associated with such activity, is solely between You and the applicable third party. SmarterTools shall have no liability, obligation, or responsibility for any such correspondence, interaction, purchase, service or promotion between You and any such third-party including, but not limited to, translations, mapping, sharing, or any other service or transfer, even if such third-party correspondence, interaction, purchase, service, or promotion is listed as a benefit or feature of the Software. SmarterTools explicitly disclaims any liability, obligation or responsibility for the

continuation, viability, quality, reliability, or availability of any such third party provided correspondence, interaction, purchase, service, or promotion.

SmarterTools does not endorse any sites on the Internet that are linked through the Software. SmarterTools provides these links to You only as a matter of convenience, and in no event shall SmarterTools or its licensors be responsible for any content, products, or other materials on or available from such sites. SmarterTools provides the Software to You pursuant to the terms and conditions of this Agreement. You recognize, however, that certain third-party providers of ancillary software, hardware, or services may require Your agreement to additional or different licenses agreements or other terms prior to Your use of or access to such software, hardware, or services.

In all events, conditions, and circumstances the provisions and limitations of Sections 3, 5, and 7 shall apply.

12. Severability.

The provisions of this Agreement will be deemed severable and the invalidity or unenforceability of any provision(s) will not affect the validity or enforceability of any other provision(s) herein.

13. Entire Agreement.

This EULA constitutes and expresses the entire agreement and understanding between the parties hereto with respect to the subject matter, all revisions discussions, promises, representation, and understanding relative thereto, if any, being herein merged. This Agreement replaces and supersedes any prior agreement entered into between the parties hereto with respect to the subject matter herein.

Thank You for choosing SmarterTools Software.

Rev. 20120524