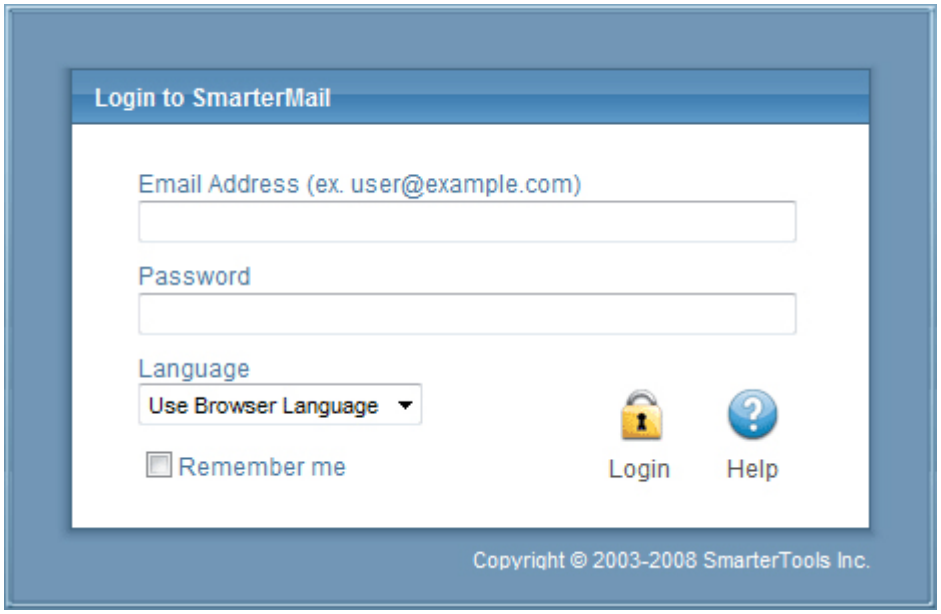
Help for System Administrators

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

Managing Domains

A single, centralized page lets you do most of the management of your domains.

Arrive at this screen by clicking the Manage button on the main toolbar. The parts of this multi-use screen are described in detail below.

Common Tasks

New Domain Icon - Click the New Domain icon on the actions toolbar, or in the tree view on the left side to begin the New Domain Wizard. more info

Edit Icon - You can edit a domain three different ways—Using the Edit icon on the actions toolbar, right-clicking a selecting domain and selecting Edit from the drop down list, or double-clicking a selected domain. more info

Settings Icon - This will allow you to quickly make changes to certain fields, such as—Email Users, Email Aliases, Mailing Lists, Default User Settings, Spam Filtering, Content Filtering, Folder Auto-Clean, and Domain Aliases.

Delete Icon - You can delete a domain two different ways Selecta domain and then click the Delete icon on the actions toolbar or right-click on a selected domain and choose Delete from the drop down list. A confirmation dialog will appear to ensure that a domain does not get accidentally deleted. Please note that once a domain is deleted, the process cannot be reversed.

Impersonate Icon - This will allow System Admins to log in as a Domain Administrator or a user within their server.

Settings Icon list

Users - This choice lets you manage users in the domain.

Aliases - This choice lets you manage aliases that map to email accounts in the domain.

Mailing Lists - Administrate mailing lists for the domain with this item.

Default User Settings - This allows you to set the general settings for a domain.

Spam Filtering - Click on this item to change the spam filtering options for the domain.

Content Filtering - Clicking here will allow you to manipulate the domain level content filters for the domain.

Folder Auto-Clean - This will allow you to set the guidelines for the auto-clean feature at that Domain Administrator level.

Domain Aliases - Manage the domain aliases with this item.

Adding a Domain

Add a domain by clicking the Manage button on the main toolbar and then selecting New Domain in the tree view or by clicking the New icon on the action toolbar.

No changes will be applied on any page until the Save button is clicked.

Options

Name - Enter the full name of the domain (ex. smartertools.com). This domain name must match one that is registered with a DNS server in order to send or receive email.

IP Address - From the drop down list, choose the IP address on which the domain will listen for incoming requests. This setting does not affect the login to the web interface, only to the IP used to listen for SMTP, POP, and IMAP traffic. This IP address should match at least one MX record on your DNS server.

Folder Path - This is the path to the directory where all information pertaining to the domain resides (XML files, mail statistics, alias information, etc.). If the directory does not already exist, it will be created. This path should be under a directory solely dedicated to SmarterMail.

Mail List Username - This is the email address that List Serv commands can be sent to via email.

Domain Administrator Username - Enter the login name for the domain administrator (AKA "domain admin"). The domain administrator is usually the owner of the domain or the technical administrator. The domain administrator is responsible for adding and deleting email accounts, and setting specific configurations for the domain.

Domain Administrator Password - Enter the domain administrator's password for SmarterMail

Disable Domain - Checking this box disables the domain. The domain will be unable to send or receive mail, and no users of the domain will be able to log into the web interface for this domain. This option is a good way to temporarily shut off a domain without deleting it.

Technical Information

SMTP Port - Simple Mail Transfer Protocol (SMTP) uses port 25 on the server as a default. If you would like to use a different port for SMTP on your server, enter it in this box. It is not recommended that you change the default port unless you utilize a firewall that requires this setting to be changed.

SMTP Port (Alternate) - Enable alternate SMTP port which is recommended if your email users access their email through ISPs that restrict the standard port 25, which is becoming more common. Users will be able to access their mail through both the SMTP port and the alternate SMTP port, as both will be available simultaneously.

POP Port - Post Office Protocol (POP3) uses port 110 on the server as a default. If you would like to use a different port for POP on your server, enter it in this box. It is not recommended that you change the default port unless you are behind a firewall that requires this setting to be changed.

IMAP Port - Internet Message Access Protocol (IMAP4) uses port 143 on the server as a default. If you would like to use a different port for IMAP on your server, enter it in this box. It is not recommended that you change the default port unless you are behind a firewall that requires this setting to be changed.

LDAP Port Enterprise Edition Only - Lightweight Directory Access Protocol (LDAP) uses port 389 on the server as a default. If you would like to use a different port for LDAP on your server, enter it in this box. It is not recommended that you change the default port unless you utilize a firewall that requires this setting to be changed.

Logout URL - - Enable logout URL and you can enter any site which you would like your users redirected to when logging off.

Auto-Responder Exclusions - This allows you to choose who will receive an auto-responder based on the spam level of the original message.

Forwarding Exclusions - This allows you to choose what mail can be forwarded based on the spam level of the message.

Require SMTP Authentication - Check this box if you want SMTP Authentication to be used by the end users of the domain. Each user must then supply an email address and password in order to send email from their account. SmarterMail supports two authentication methods, Cram-md5 and Login .

Enable once per day per sender auto-responder restriction - Enable this if you want to put a restriction on the autoresponder frequency.

Disable Greylisting - Check this box if you wish to disable greylisting spam filtering for your mailbox. Greylisting is an effective anti-spam method but does have possible disadvantages.

Features

Enable Active Directory Integration - Domains with this option enabled can add users that are bound to an Active Directory server, and authenticate against a domain.

Enable Calendar - Enable this to allow users to use the calendar feature.

Enable Contacts - Enable this to allow users to use the contacts feature.

Enable Domain Aliases - Enable this to show the "Domain Aliases" option in the Config menu for domain administrators. This will allow domain administrators to combine email addresses with different domain names into one mailbox. more info

Enable Content Filtering - Enable "Domain Content Filtering" in the Config menu for the domain admin. Content filtering is inherited by all end users within the domain. more info

Enable DomainKey Signing - Enable this to have you mail checked against a key to verify the mail is coming from who it says it is. Domain Administrators will configure this option once enabled.

Enable Domain Reports - Enable this to provide additional reports for domain administrators.

Enable Email Reports - Enable this to provide the ability to email reports

Enable Mailing Lists - Enable this to show the "Mailing Lists" page in the Config menu for domain administrators. This will allow domain administrators to use the list serv features for sending emails via lists to many users. more info

Enable Notes - Enable this to allow users to use the notes feature.

Enable POP Retrieval - Enable this to allow users to pull their email from exterior accounts (yahoo, Gmail, etc.).

Enable Tasks - Enable this to allow users to use the tasks feature.

Enable Catch-Alls - Enable this to allow users to use catch-alls.

Limits

Note: Limits on total number of domains and users may be imposed by your SmarterMail license, which may override some options below.

Disk Space - Enter the total amount of space, in megabytes, that the Mail Server will allow the domain to use. Note: Once this limit is reached, SmarterMail will refuse to accept any new mail for the domain, and will send a warning to the domain administrator. (Default is 500 MB)(Use 0 for unlimited)

Domain Aliases - Enter the maximum amount of Domain Aliases allowed for this domain. (Default is 2)(Use 0 for unlimited)

Users - Enter the maximum number of user email accounts that can be added to this domain. (Default is 100)(Use 0 for unlimited)

User Aliases - Enter the maximum number of alias email accounts (forwarded to a true email account) that are allowed per domain. (Default is 1000)(Use 0 for unlimited)

Mailing Lists - Enter the maximum amount of mailing lists allowed for the domain. (Default is 0)(Use 0 for unlimited)

POP Retrieval Accounts - Enter the number of exterior accounts a user is allowed to have.(Default is 10)(Use 0 for unlimited)

Max Message Size - Enter the maximum total size of an email in kilobytes that an end user can send at one time. This number includes text, html, images and attachments. (Default is 10,000 KB)(Use 0 for unlimited)

Recipients per Message - Enter the number of email addresses a user can send a message to at one time. (Default is 200)(Use 0 for unlimited)

Sharing

This page is available in Enterprise Edition only

Enable Global Address List - Enable this to allow users on a domain to see all other user profiles on the domain, and participate in LDAP queries against the domain.

Enable Shared Calendars - Enable this to allow calendars to be shared with other users of the same domain.

Enable Shared Contacts - Enable this to allow contact lists to be shared with other users of the same domain.

Enable Shared Folders - Enable this to allow email folders to be shared with other users of the same domain.

Enable Shared Notes - Enable this to allow note lists to be shared with other users of the same domain.

Enable Shared Tasks - Enable this to allow task lists to be shared with other users of the same domain.

Priority

This tab allows System Administrators to prioritize or deprioritize 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. (For more information on setting up a Gateway Server, see the Gateway Servers help page in the Settings folder.)

Standard Messages - Enable this and set a priority for any message sent by a domain that doesn't have another priority already affecting it.

Mailing Lists - Enable this and set a priority for a message being sent by a mailing list.

Priority When Over size - Enable thisand set a priority for messages that exceed the "Message Size Threshold".

Message Size Threshold - Enter the size in MB that you want to set as your Maximum Threshold. Default is set at 2 MB.

Auto-Responders - Enable this and set a priority for auto-responder messages being sent.

Email Reports - Enable this and set a priority for reports being emailed.

Event Emails - Enable this and set a priority for emails being set to remind users of upcoming events.

Second Delivery Attempt - Enable this and set a priority for emails that were not successfully sent on the first try.

Third Delivery Attempt - Enable this and set a priority for emails that were not successfully sent on the first and second tries.

Throttling

Throttling allows System Administrators to limit the number of messages and/or how much bandwidth a domain, user, or mailing list can use for sending email per hour. Once the throttling threshold is reached, messages will stop sending until that hour expired. At that time, the system will resume sending messages.

Messages per Hour - Enable this and enter the number of messages a domain is allowed to send per hour. (Default is set at 5000)

Bandwidth per Hour - Enable this and enter the maximum size in MB a domain is allowed to send per hour. (Default is set at 100)

Bounces Received per Hour - Enable this and enter the maximum number of bounces a domain can receive in an hour. (Default is set at 1000)

Events

System Administrators can choose which categories and event types they would like enabled for their events system. The categories are as follows: Alias, Collaborate, Email, Mailing List, Throttling, and User.

Alias

Enable Alias Added Event - Enable this to have "Alias Added" added as an event type.

Enable Alias Deleted Event - Enable this to have "Alias Deleted" added as an event type.

Collaborate

Enable Calendar Reminder Occurred Event - Enable this to have "Calendar Reminder Occurred" added as an event type.

Enable Task Reminder Occurred Event - Enable this to have "Task Reminder Occurred" added as an event type.

Email

Enable Message Received Event - Enable this to have "Message Received" added as an event type.

Enable Message Sent Event - Enable this to have "Message Sent" added as an event type.

Mailing List

Enable Mailing List Added Event - Enable this to have "Mailing List Added" added as an event type.

Enable Mailing List Deleted Event - Enable this to have "Mailing List Deleted" added as an event type.

Enable Message Sent to Mailing List Event - Enable this to have "Message Sent to Mailing List" added as an event type.

Throttling

Enable User Throttled Event - Enable this to have "User Throttled" added as an event type.

Enable Domain Throttled Event - Enable this to have "Domain Throttled" added as an event type.

User

Enable User Added Event - Enable this to have "User Added" added as an event type.

Enable User Deleted Event - Enable this to have "User Deleted" added as an event type.

Enable User Disk Space Used Event - Enable this to have "User Disk Space Used" added an event type.

Note: Setup DNS for the Domain

Return to Getting Started

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 you to control which services are running for your mail server. Generally, all of these should be enabled.

On the actions toolbar, you will see two icons—Start and Stop. All services can be started and/or stopped two different ways.

Start - To start a service that is currently stopped, you can select the service(s) and click the Start icon on the actions toolbar, or right-click on the service(s) and select Start from the drop down menu.

Stop - To stop a service that is currently started, you can select the service(s) and click the Stop icon on the actions toolbar, or right-click on the service(s) and select Stop from the drop down menu. Any current threads will continue to run and will finish properly, but no new threads will be started.

Protocols - A green indicator next to a service indicates that it is running, while a red indicator means a service is currently stopped.

Protocol Types

IMAP - Internet Message Access Protocol is a standard service used for accessing e-mail from a mail server. IMAP (the latest version is IMAP4) is a client/server protocol in which e-mail 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. LDAP (Enterprise Edition Only) - Lightweight Directory Access Protocol is 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 - With Post Office Protocol, mail is saved in a mail box on the mail server. When the end user reads the mail, all of it is immediately downloaded to the client computer and no longer maintained on the mail server.

POP Retrieval - With POP Retrieval, mail is retrieved from external POP3 servers and saved in a mail box on the mail server.

SMTP - Simple Mail Transfer Protocol is 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 Spool service is the internal message queue used to deliver messages locally and to remote services.

Editing Domains

Editing a domain can be initiated in three different ways. To get started, click the Manage button on the main toolbar. Then select the domain that you would like to edit and do one of three things: 1) Click the Edit icon on the action toolbar, 2) Right-click the selected domain and select Edit from the drop-down list, or 3) Double click the selected domain.

Editing a site is very similar to adding a new site. No changes will be applied on any page until the Save icon is clicked.

Options

Domain Name - Enter the full name of the domain (ex. smartertools.com). This domain name must match one that is registered with a DNS server in order to send or receive email.

IP Address - From the drop down list, choose the IP address on which the domain will listen for incoming requests. This setting does not affect the login to the web interface, only to the IP used to listen for SMTP, POP, and IMAP traffic. This IP address should match at least one MX record on your DNS server.

Folder Path - This is the path to the directory where all information pertaining to the domain resides (XML files, mail statistics, alias information, etc.). If the directory does not already exist, it will be created. This path should be under a directory solely dedicated to SmarterMail.

Mail List Username - This is the email address that List Serv commands can be sent to via email.

Username - Enter the login name for the domain administrator (AKA "domain admin"). The domain administrator is usually the owner of the domain or the technical administrator. The domain

administrator is responsible for adding and deleting email accounts, and setting specific configurations for the domain.

Password - Enter the domain administrator's password for SmarterMail

Disable Domain - Checking this box disables the domain. The domain will be unable to send or receive mail, and no users of the domain will be able to log into the web interface for this domain. This option is a good way to temporarily shut off a domain without deleting it.

Technical Information

SMTP Port - Simple Mail Transfer Protocol (SMTP) uses a port 25 on the server as a default. If you would like to use a different port for SMTP on your server, enter it in this box. It is not recommended that you change the default port unless you are behind a firewall that requires this setting to be changed.

SMTP Port (Alternate) - Enable alternate SMTP port which is recommended if your email users access their email through ISPs that restrict the standard port 25, which is becoming more common. Users will be able to access their mail through both the SMTP port and the alternate SMTP port, as both will be available simultaneously.

POP Port - Post Office Protocol (POP3) uses port 110 on the server as a default. If you would like to use a different port for POP on your server, enter it in this box. It is not recommended that you change the default port unless you are behind a firewall that requires this setting to be changed.

IMAP Port - Internet Message Access Protocol (IMAP4) uses port 143 on the server as a default. If you would like to use a different port for IMAP on your server, enter it in this box. It is not recommended that you change the default port unless you are behind a firewall that requires this setting to be changed.

LDAP Port Enterprise Edition Only - Lightweight Directory Access Protocol (LDAP) uses port 389 on the server as a default. If you would like to use a different port for LDAP on your server, enter it in this box. It is not recommended that you change the default port unless you are behind a firewall that requires this setting to be changed.

Logout URL - - Enable logout URL and you can enter any site which you would like users redirected to when logging off.

Auto-Responder Exclusions - This allows you to choose who will receive an auto-responder based on the spam level of the original message.

Forwarding Exclusions - This allows you to choose what mail can be forwarded based on the spam level of the message.

Require SMTP Authentication - Check this box if you want SMTP Authentication to be used by the end users of the domain. Each user must then supply an email address and password in order to send email from their account. SmarterMail supports two authentication methods, Cram-md5 and Login .

Enable once per day per sender auto-responder restriction - Enable this if you want to put a restriction on the auto-responder frequency.

Disable Greylisting - Check this box if you wish to disable greylisting spam filtering for your mailbox. Greylisting is an effective anti-spam method but does have possible disadvantages.

Features

Enable Active Directory Integration - Domains with this option enabled can add users that are bound to an Active Directory server, and authenticate against a domain.

Enable Calendar - Enable this to allow users to use the calendar feature.

Enable Contacts - Enable this to allow users to use the contacts feature.

Enable Domain Aliases - Enable this to show the "Domain Aliases" option in the Config menu for domain administrators. This will allow domain administrators to combine email addresses with different domain names into one mailbox.

Enable Content Filtering - Enable "Domain Content Filtering" in the Config menu for the domain admin. Content filtering is inherited by all end users within the domain.

Enable DomainKey Signing - Enable this to have you mail checked against a key to verify the mail is coming from who it says it is. Domain Administrators will configure this option once enabled.

Enable Domain Reports - Enable this to provide additional reports for domain administrators.

Enable Email Reports - Enable this to provide the ability to email reports

Enable Mailing Lists - Enable this to show the "Mailing Lists" page in the Config menu for domain administrators. This will allow domain administrators to use the list serv features for sending emails via lists to many users.

Enable Notes - Enable this to allow users to use the notes feature.

Enable POP Retrieval - Enable this to allow users to pull their email from exterior accounts (yahoo, Gmail, etc.).

Enable Tasks - Enable this to allow users to use the tasks feature.

Enable Catch-Alls - Enable this to allow users to use catch-alls.

Limits

Note: Limits on total number of domains and users may be imposed by your SmarterMail license, which may override some options below.

Disk Space - Enter the total amount of space, in megabytes, that the Mail Server will allow the domain to use. Note: Once this limit is reached, SmarterMail will refuse to accept any new mail for the domain, and will send a warning to the domain administrator. (Default is 500)(Use 0 for unlimited)

Domain Aliases - Enter the maximum amount of Domain Aliases allowed for this domain. (Default is 2)(Use 0 for unlimited)

Users - Enter the maximum number of user email accounts that can be added to this domain. (Default is 100)(Use 0 for unlimited)

User Aliases - Enter the maximum number of alias email accounts (forwarded to a true email account) that are allowed per domain. (Default is 1000)(Use 0 for unlimited)

Mailing Lists - Enter the maximum amount of mailing lists allowed for the domain. (Default is 0)(Use 0 for unlimited)

POP Retrieval Accounts - Enter the number of exterior accounts a user is allowed to have. (Default is 10) (Use 0 for unlimited)

Max Message Size - Enter the maximum total size of an email in kilobytes that an end user can send at one time. This number includes text, html, images and attachments. (Default is 10,000 KB)(Use 0 for unlimited)

Recipients per Message - Enter the number of email addresses a user can send a message to at one time. (Default is 200)(Use 0 for unlimited)

Sharing

This page is available in Enterprise Edition only

Enable Global Address List - Enable this to allow users on a domain to see all other user profiles on the domain, and participate in LDAP queries against the domain.

Enable Shared Calendars - Enable this to allow calendars to be shared with other users of the same domain.

Enable Shared Contacts - Enable this to allow contact lists to be shared with other users of the same domain.

Enable Shared Folders - Enable this to allow email folders to be shared with other users of the same domain.

Enable Shared Notes - Enable this to allow note lists to be shared with other users of the same domain.

Enable Shared Tasks - Enable this to allow task lists to be shared with other users of the same domain.

Priority

This tab allows System Administrators to prioritize or deprioritize 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. (For more information on setting up a Gateway Server, see the Gateway Servers help page in the Settings folder.)

Standard Messages - Enable this and set a priority for any message sent by a domain that doesn't have another priority already affecting it.

Mailing Lists - Enable this and set a priority for a message being sent by a mailing list.

Priority When Over size - Enable thisand set a priority for messages that exceed the "Message Size Threshold".

Message Size Threshold - Enter the size in MB that you want to set as your Maximum Threshold. Default is set at 2 MB.

Auto-Responders - Enable this and set a priority for auto-responder messages being sent.

Email Reports - Enable this and set a priority for reports being emailed.

Event Emails - Enable this and set a priority for emails being set to remind users of upcoming events.

Second Delivery Attempt - Enable this and set a priority for emails that were not successfully sent on the first try.

Third Delivery Attempt - Enable this and set a priority for emails that were not successfully sent on the first and second tries.

Throttling

Throttling allows System Administrators to limit the number of messages and/or how much bandwidth a domain, user, or mailing list can use for sending email per hour. Once the throttling threshold is reached, messages will stop sending until that that hour expired. At that time, the system will resume sending messages.

Messages per Hour - Enable this and enter the number of messages a domain is allowed to send per hour. (Default is set at 5000)

Bandwidth per Hour - Enable this and enter the maximum size in MB a domain is allowed to send per hour. (Default is set at 100)

Bounces Received per Hour - Enable this and enter the maximum number of bounces a domain can receive in an hour. (Default is set at 1000)

Events

System Administrators can choose which categories and event types they would like enabled for their events system. The categories are as follows: Alias, Collaborate, Email, Mailing List, Throttling, and User.

Alias

Enable Alias Added Event - Enable this to have "Alias Added" added as an event type.

Enable Alias Deleted Event - Enable this to have "Alias Deleted" added as an event type.

Collaborate

Enable Calendar Reminder Occurred Event - Enable this to have "Calendar Reminder Occurred" added as an event type.

Enable Task Reminder Occurred Event - Enable this to have "Task Reminder Occurred" added as an event type.

Email

Enable Message Received Event - Enable this to have "Message Received" added as an event type.

Enable Message Sent Event - Enable this to have "Message Sent" added as an event type.

Mailing List

Enable Mailing List Added Event - Enable this to have "Mailing List Added" added as an event type.

Enable Mailing List Deleted Event - Enable this to have "Mailing List Deleted" added as an event type.

Enable Message Sent to Mailing List Event - Enable this to have "Message Sent to Mailing List" added as an event type.

Throttling

Enable User Throttled Event - Enable this to have "User Throttled" added as an event type.

Enable Domain Throttled Event - Enable this to have "Domain Throttled" added as an event type.

User

Enable User Added Event - Enable this to have "User Added" added as an event type.

Enable User Deleted Event - Enable this to have "User Deleted" added as an event type.

Enable User Disk Space Used Event - Enable this to have "User Disk Space Used" added an event type.

Manage Spool

The information in Manage Spool pertains to the messages held by the SmarterMail server pending delivery. The email spool (which stands for "Simultaneous Peripheral Operations OnLine") 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 get started, click the Manage button on the main toolbar, then select All Messages under the Spool tree view.

You have different actions which are available for you to chose located on the Actions toolbar— Force , Reset Retries , View , Recipients , Priority , Delete , and Refresh . See below for a description of each possible action.

Data Columns

File Name - The filename on the hard disk. Click on the filename to view the message.

Sender - The email address that initially sent the email.

Time in Spool - This indicates 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.

Recipients - Shows how many delivered/total recipients there are for the message. Clicking on the value will open the recipients detail page. When viewing a recipients, you can tell why they are pending.

Status - Contains the current status of the message.

Size - The total size of the message on the hard drive, in kilobytes.

Spool Path - This shows which spool the message resides in. If you have subspools enabled, the message may be placed in one of those locations.

Action Toolbar

Items in the spool must be checked before actions will work on them. Click on the checkbox in the table header for a quick method of selecting all or none of the items.

Force Messages - Forcing messages can be performed by either selecting the message you want forced and clicking the Force icon on the actions too bar, or right-clicking the message and selecting Force from the drop down menu. The statuses of the messages will not be updated until the server passes through the spool.

Reset Retries - Resets the retry counts on all messages in the spool, effectively starting the delivery process over. This can be useful if a DNS or firewall problem has been recently resolved, or if you are using SmartHosting and the target server was down.

View - Use this icon to show you that selected message.

Recipients - This will show you who the message was sent to and the status of that message (i.e. delivered or pending)

Priority - System Administrators can change the priority levels of specific messages.

Delete - Deleting messages can be performed by either selecting the message you want deleted and clicking the Delete icon on the actions too bar, or right-clicking the message and selecting Delete from

the drop down menu. No confirmation dialog will show up, so use caution when deleting from the spool.

Refresh - Click this button 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.

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 .

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.

Settings

General Settings

The General Settings page is where you control many of the global settings for the SmarterMail server. No settings will be saved until you click on the Save icon.

To get started, click the Settings button on the main toolbar, then select General Settings from the Settings tree view.

Administrator

Username - This is the login name associated with the System Administrator account for the SmarterMail Server. You will use this name instead of a full email address when logging in as the System Administrator.

Old Password - In order to change the System Administrator password you must the current password associated with the System Administrator account. Passwords are case-sensitive.

New Password - Enter the desired password for the System Administrator account. Passwords are case-sensitive.

Confirm New Password - Verify the desired password for the System Administrator account. Passwords are case-sensitive.

Items per Page - When viewing the messages in a folder, this option lets you customize how many items will appear per page throughout SmarterMail.

Server Info

Host Name - Enter the host name of this server. It is sent to connecting servers to identify the server. Host names should be in the format computername.domain.com .

Postmaster Mailbox - Every mail server requires a main email for the postmaster. This is usually the owner or Administrator of SmarterMail.

IP of Primary / Secondary DNS - Enter the IP address of the DNS servers. If left blank, the DNS server information will be pulled from the the Windows Networking settings (Recommended).

Logout URL - Enable this feature to allow the System Administrator to redirect users who log out to a certain URL.

Enable Domain Admins to Override Logout URL - Enable this option to have domain admins select the URL they want their users to go to when logging out. If this option is not enabled, it will not be visible to domain admins.

Spool

Spool Path - This is 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 option will hold mail in its spool for this amount of time prior to sending the mail. The benefit of a delivery delay is so that if you have a secondary service, like a virus checker, that needs access to the mail prior to its delivery, you give the secondary service ample time to interact with the message prior to it leaving the mail server. (Default is 15 seconds)

Time Between Delivery Attempts - 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 15min, 30min, 60 min, and 90 min intervals.

Attempts before bouncing DNS errors - Enter the maximum number of attempts SmarterMail should make before the message is bounced back due to a DNS error. This will happen most commonly with a misspelled domain. This will be beneficial for administrators 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. (Default is 2. 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 message retry attempts which is determined in the line above TimeBetween Delivery Attempts)

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. The command will not be executed if the Enabled box is not checked.

Command-Line Timeout - The amount of time, in seconds, that the server will wait while waiting for information from the remote server. In general, a timeout of 5 seconds should suffice.

Statistics

Delete Server Stats After - Enable this and enter the number of months that the server stats will be deleted. (Default is 13 months)

Delete Domain Stats After - Enable this and enter the number of months that the domain stats will be deleted. (Default is 13 months)

Delete User Stats After - Enable this and enter the number of months that the user stats will be deleted. (Default is 13 months)

Protocol Settings

This configuration page allows you to establish policies for the standard email protocols. No settings will be saved until you click the Save icon.

To get started, click the Settings button on the main toolbar, then select Protocol Settings from the Settings tree view.

POP

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. (Default is 5 minutes)

Max Bad Commands - After this many unrecognized or improper commands, a connection will be automatically terminated. (Default 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. Enter a "0" if you want unlimited connections. (Default is 500)

Pop Retrieval Download Path - System Admins can enter a path where mail will be stored from POP accounts until it is read.

Max Pop Retrieval Threads - Enter the maximum number of threads you want SmarterMail to work on concurrently. (Default is 10)

Pop Retrieval Interval - This is how often SmarterMail will check POP accounts based upon the amount of work needed to complete. (Default is 10)

IMAP

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. (Default is 15 minutes)

Max Bad Commands - After this many unrecognized or improper commands, a connection will be automatically terminated. (Default 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. Enter a "0" if you want unlimited connections. (Default is 1000)

Enable IDLE Command - Enable this to turn on 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. Please note, IMAP clients that do not fully support IMAP IDLE, like Microsoft Outlook, may use the command in such a way that it actually degrades performance.

LDAP

Session Timeout - After a connection fails to respond or issue new commands for this number of seconds, the connection will be closed.

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.

SMTP In

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 - This option will restrict mail sent to only work via SMTP authentication and with accounts on the local SmarterMail Server (except for IPs on the White List).
- Only Local Users (Recommended) - 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 - Enable this and after a connection fails to respond or issue new commands for this number of minutes, the connection will be closed. (Default is 15 minutes)

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. (Default is 120 seconds)

Max Bad Commands - After this many unrecognized or improper commands, a connection will be automatically terminated. (Default 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. (Default 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. (Default is 20)

Max Message Size - Messages greater than this size will be rejected by the mail server. (Default is 30 MB)

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 - Enable the Verify Mailbox command in SMTP. This will allow others (including other mail servers) to verify an email address on the server. This is considered by some to a security risk, and should not be checked without understanding the ramifications.

Enable EXPN command - Enable the Expand List command in SMTP. This will allow others to list all users associated with an alias or list. This is considered by some to a security risk, and should not be checked without understanding the ramifications.

Disable relay settings when using SMTP authentication - This will disable the "Allow Relay" setting from above.

Enable Domain's SMTP auth setting for local deliveries - When this option is enabled, SmarterMail will 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 - This will disable plain text authentication.

SMTP Out

Outbound IP - Use this box to select what IP address is used to deliver outbound messages.

Enable fallback to Primary IP on failure - Enable this 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. (Default is 60 seconds)

Max Spam Check Threads - Enter the maximum number of messages that can be spam checked at one time.

Max Delivery Threads - Enter 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. (Default is 50)

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.

Default Domain Settings

From this page you can create global default settings that will automatically be used when adding a

new site through either the Web Interface or through Web Services. These default settings can be overwritten and are only intended to avoid needless data entry.

The settings on this page are identical to those found in the topic Editing a Domain .

To get started, click on the Settings button on the main toolbar, then select Domain Defaults from the Defaults tree view.

Note: Changing these settings has no bearing on domains that have already been setup, unless the "Propagate Settings" option is used.

Propagating Settings

To apply some or all of the default settings to all domains on your server—change the settings to how you want them, and then click Settings from the main toolbar. Check all of the settings that you want to apply to your domains, then click on the Propagate Now icon.

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 (Default = Detailed).

IMAP Log Level - The log level for IMAP sessions (Default = Exceptions Only).

LDAP Log Level - The log level for LDAP sessions (Default = Exceptions Only).

Message-ID Log - The log level for logging Message-ID's of all messages sent to mailing lists. (Default = None).

Event Log - The log level for event sessions (Default = Exceptions Only).

SycnML Log Level - The log level for SyncML sessions (Default = Normal).

POP Log Level - The log level for POP sessions (Default = Exceptions Only).

POP Retrieval Log Level - The log level for POP retrieval sessions (Default = Exceptions Only).

SMTP Log Level - The log level for SMTP sessions (Default = Normal).

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.

To establish domain forwarding, click the Settings button on the main toolbar, then choose Domain Forwarding from the Routing tree view and click the New Server icon on the actions toolbar.

IP Address - Enter the server that should receive the mail.

Disable Greylisting - This will disable greylisting for all mail being forwarded to the server.

Domains to Forward (one per line) - Add the domains that should be forwarded to it, one per line.

Note: If you do not host any actual domains on the server, in order for your mail server to listen for traffic, you need to set up a dummy domain (example.com) to listen on the IP and ports from which you expect traffic.

SmartHost Servers

SmartHosting allows one SmarterMail server to accept mail for any mail server. This can be used in a backup scenario so that if the primary mail server goes down, the secondary server will accept mail for it until the server goes back online. Note: The target server does not need to be a SmarterMail Server.

The SmarterMail server can host local domains and act as a SmartHost server at the same time, allowing it to act as an incoming gateway server for those servers that are listed in the SmartHost settings and to act as the primary server for any domains that are set up locally in that SmarterMail server.

To configure SmartHost correctly, changes need to be made on the secondary server and to DNS records of domains that will have SmartHost supported.

To get started, click on the Settings button on the main toolbar, then select SmartHost Servers from the Routing tree view.

- Add SmartHosts - In the secondary server, add all IP addresses of the primary server to the SmartHost list. Mail that resolves to MX records that do not match these IP addresses or accounts on the secondary server will be rejected.
- Setup MX records - In DNS, add an MX record for the secondary mail server that has a LARGER preference value than the primary mail server. Refer to your DNS server documentation for instructions on adding MX records. Note: In MX records, lower preference value servers are tried first.
- Set appropriate retry times - Since the intent of SmartHost is for the secondary server to be a backup server, adjust the retry times in General Settings to values that are more conservative. Good defaults would be: 10 minutes, 10 minutes, 10 minutes, 1440 minutes.

Note that it is good practice to disable the spool service on the secondary server if the primary server goes down for more than 30 minutes, then restart the spool once the primary server is back online. In this way, all messages will still be accepted through the SMTP service, but delivery will not keep attempting to deliver the messages. Once you get the primary server online again, start the spool service on the secondary server and all the messages will start to be delivered.

Gateway Servers

Gateway Servers allow you to use another server, SmarterMail or not, to process outgoing mail in order to reduce load on your primary server. They can also be used to combat blacklisting. If the server gets blacklisted, simply rotate the primary IP on the network card to a different one to send out on the new IP.

To get started, click the Settings button on the main toolbar, then select Gateway Servers from the Routing tree view. You will see three icons on the actions toolbar—New, Edit, and Delete.

New - Click this button to add a Gateway Server.

Edit - This will allow you to edit an existing gateway server.

Delete - This will allow you to delete an existing gateway server.

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 - Is this gateway another SmarterMail server.

SmarterMail Gateway

SmarterMail URL - The value to enter in this field is the URL used to check webmail. 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 admin username on the gateway server.

Admin Password - The admin password on the gateway server.

Folder Auto-Clean

The purpose of the Folder Auto-Clean feature of SmarterMail is to aid you in keeping your mailbox size(s) under control. Using Folder Auto-Clean, common folders like Junk E-Mail, Sent Items, and Deleted Items can be regularly cleaned of old messages so they do not clutter your mailbox. System administrators can choose to let domains and users override your suggested settings, or require them to use the policies you set. Domain administrators also have this priviledge over users.

To get started, click the Settings button on the main toolbar, then select Folder Auto-Clean from the Defaults folder tree view.

Options (System Admin)

Enable domains to override auto-clean settings - Enable this to allow domains to change the settings

on this page. This is recommended, as many domain administrators have their own ideas of what an acceptable auto-clean policy is. Uncheck this box to lock the settings for all domains and all users.

Enable users to auto-clean inbox - Enable this feature to give users the ability to auto-clean their own inbox.

Options (Domain Admin)

Use default auto-clean settings - Check this box to use the system administration's auto-clean settings.

Override auto-clean settings for this domain - Check this box to allow you to change the settings for your domain.

Allow users to override auto-clean settings - Check this box to allow users to change the settings on for their individual account.

Options (Users)

Use default auto-clean settings - Check this box to use the domain administration's auto-clean settings.

Override auto-clean settings for this account - Check this box to allow you to change the auto-clean settings for your account.

Default Rules

Under each folder that has auto-clean options or if you click the New Rule icon, you will see the settings below:

Folder - Select the folder that you would like to add the Auto-Clean to. Only seen if you click the New Rule button.

Enable Auto-clean for this folder - Enable this to auto-clean the folder when it gets too large.

Type - Choose which criteria to enforce auto-clean with:

- Size

- Folder size before auto-clean - When the folder reaches this size (in megabytes), auto-cleaning will be activated.
- Folder size after auto-clean - Auto-clean will attempt to reduce the folder to this size or smaller when auto-cleaning is performed.
- Date - Choose the max number of days messages should stay in your folder.

Message Archiving

This feature is available in Enterprise Edition only

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. Message archiving allows you to set up rules for saving messages for specific domains.

To get started, click the Settings button on the main toolbar, then select Message Archiving from the Routing tree view.

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.

Adding / Editing a Rule

To apply an archiving rule to all domains on the server, click on "All Domains" in the list. To add a rule for a single domain, click on New Rule icon.

Domain - The domain that should be archived, in the format of example.com.

Archive Path - The path on the hard drive that should be used to store the messages.

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

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.

Security

Anti-Virus Administration

From this page you can enable SmarterMail to work with virus scanners that support a quarantine

directory. SmarterMail has the ability to check the quarantine directory and respond to users who attempted to send an email containing a virus.

To get started, click the Security button on the main toolbar, then select Anti-Virus Administration from the Email Protection folder tree view.

Options

Enable ClamAV - Enable this to use ClamAV anti-virus scanning.

Enable Real-Time AV - Enable this to use Real-Time AV

Enable Command-Line AV - Enable this to use a command line virus scanner.

ClamAV

Clam AntiVirus is a 3rd party open source anti-virus toolkit, designed especially for scanning e-mail 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.

Timeout (in seconds) - System Admins can enter the maximum number of seconds they want to wait before moving on. (Default is 10 seconds)

Failures Before Restart - System Admins can enter the maximum number of timeouts allowed before ClamAV is restarted. (Default is 5)

Virus Definitions - Displays when the virus definitions were last updated. The definitions are updated whenever the service starts and every 6 hours thereafter. Click the Update link to do an immediate update.

Real-Time AV

Quarantine Directory - Enter the full path to the quarantine directory set for the server.

Virus Action - Choose the action to be taken when an email contains a virus. The available options are shown below.

- Delete (Recommended) - This option will enable the SmarterMail service to delete any associated files attached to the message from the spool directory. This does not take any action on the quarantine directory.
- Inform Sender - This option will inform the 'From' address that a message was receive 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 - Enter the command that you want to execute. %FILEPATH will be replaced with the path to the file to be scanned.

Anti-Spam Administration

SmarterMail's anti-spam features allow you to be as aggressive as you want when combating spam.

To get started, click the Security button on the main toolbar, then select Anti-Spam Administration from the Email Protection tree view.

- Spam Checks - Check 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.
- Filtering - Choose the default weight thresholds and actions for various spam levels for filtering. Users can override these settings if you permit them to.
- SMTP Blocking - Set the weight to use as a threshold on this tab. Enabling this option will block email at the SMTP delivery level if too many spam checks fail.
- Options - This tab contains options relating to the processing of spam and overridability.

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.

Spam Checks

Due to the flexible nature of SmarterMail's Anti-Spam 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.

Note: Only enabled spam checks are used when calculating spam weight. To enable or disable a check, click on the appropriate checkbox next to it and click the Save icon.

The different types of Spam Checks are shown below. In most cases, clicking on the Edit icon will allow you to set various properties about it.

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. Declude is a 3rd party open source and more information can be found at: www.declude.com .

SpamAssassin

SpamAssassin is a powerful, 3rd party open source mail filter used to identify spam. It utilizes a wide array of tools to identify and report spam. More information about SpamAssassin can be found at: spamassassin.apache.org .

SmarterMail includes a Windows version of SpamAssassin out of the box. By default, SmarterMail will run a version of SpamAssassin on 127.0.0.1 port 783. The System Administrator can enable and disable SpamAssassin by clicking the Security button on the main toolbar, then selecting SpamAssassin Servers from the Email Protection folder tree view. The Windows Version of SpamAssassin is limited to about 40,000 messages per day, if you anticipate more than this you may require the use of a distributed, multi-threaded version. Additional information is available in the SmarterTools SpamAssassin Deployment Guide.

SmarterMail can use SpamAssassin with its weighting system. By default SpamAssassin will run on 127.0.0.1:783. Additional servers can be setup from the Security->SpamAssassin menu option.

Low Probability of Spam - The weight that will be assigned if SpamAssassin determines a low probability of spam.

Medium Probability of Spam - The weight that will be assigned if SpamAssassin determines a medium probability of spam.

High Probability of Spam - The weight that will be assigned if SpamAssassin determines a high probability of spam.

Timeout - The timeout that SmarterMail will impose on a server if it cannot connect.

Maximum Attempts per Message - This will designate how many times SmarterMail will attempt to acquire a SpamAssasasin score before it gives up on that email.

Custom Headers

Email can be assigned spam weight based on headers in the message. Use this selection to configure weights for custom headers.

Header - The custom header to search for in the e-mail message.

Value - The value of the custom header.

Weight - The amount to add to the e-mail message's spam weight.

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 re-analyze 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 e-mail authentication system designed to verify the DNS domain of an e-mail 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 - 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 - 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 - 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 - 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 - 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 - 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 on the Add List icon. Some common RBL lists are shown at the bottom of this topic.

Name - A friendly name for the list that will help you and your customers identify it.

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.

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.

Description - This field allows you to store additional information about the list.

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.

Weight Threshold - The email is sorted into probability levels based on the weight threshold values.

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)

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

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.

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.

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

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.

SpamAssassin

What is SpamAssassin and how does it work?

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

When should you use SpamAssassin?

You should use SpamAssassin when you care about limiting spam from getting to your mailbox but cannot afford a high priced spam solution.

How do I set up SpamAssassin?

SmarterMail includes a Windows version of SpamAssassin out of the box. By default, SmarterMail will run a version of SpamAssassin on 127.0.0.1 port 783. The System Administrator can enable and disable SpamAssassin by clicking the Security button on the main toolbar, then selecting SpamAssassin Servers from the Email Protection folder tree view. The Windows Version of SpamAssassin is limited to about 40,000 messages per day, if you anticipate more than this, then please read our Anti-Spam Administration page from the Security folder in the Systems Administration section of the help files.

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.

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.

The most common instance of needing this feature is 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.

*AOL and AOL.com are registered trademarks of America Online, Inc.

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).

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

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.

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>

Automation with Web Services

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

To view the web services and the corresponding functions available to you, go to your default Web Interface install location and append "services/SERVICENAME.asmx". With the default installation, you would use http://127.0.0.1:9998/Services/svcServerAdmin.asmx.

To get a brief explanation of the web services available to you, along with the default installation paths to the specific web services details page, download the Automation with Web Services document.

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 .