SmarterTools Inc.

SmarterMail 1.x Documentation

LEGACY PRODUCT DOCUMENTATION

SmarterMail 1.x is now a legacy product and is no longer supported by SmarterTools Inc. This documentation is intended for reference only, and no warranties are made, expressed or implied.

Newer versions of SmarterMail are available from the SmarterTools web site at smartertools.com

Contents

Overview

SmarterMail Professional Edition 1.6 is a leading Windows Mail Server providing capabilities not found in any of its competitors. SmarterMail Professional Edition is built for every size organization with the capability of supporting up to thousands of domains on one server. With extensive research done by SmarterTools, SmarterMail implements advanced Spam Filtering and Content Filtering options, while at the same time allowing System Administrators to control end-users capability of managing their own Spam and Content Filtering / blocking anywhere, anytime using a Web Browser. In addition, full Web Mail functionality with address book capability is included.

Features:

- Full Web Mail functionality
- IMAP4, POP3, SMTP (including SMTP Authentication)
- Domain-level and User-specific spam and content filtering
- Mail Usage Statistics
- Full Address Book
- and much more!

Introduction

SmarterMail Professional Edition was designed and developed with the end user in mind, both administrators and clients alike. The features included in the SmarterMail package are a leap ahead of other comparable products, truly making it SmarterMail for smarter business. There is a FREE version of SmarterMail available that will work for one domain and ten email users, or you can purchase SmarterMail to support up to an unlimited number of domains and users on one mail server.

The flexibility of SmarterMail is what truly sets it apart from competing products: Administrators have the ability to configure SmarterMail to run as optimally as possible on the server, from setting POP3, IMAP and SMTP threads and timeouts to delivery delay and log file detail, end users with admin permissions for the domain can set individual account limits (e.g. mailbox size) and domain-level spam and content filtering, and end users themselves can set spam levels and check incoming mail against any number of spam and/or black lists. Additionally, both the FREE and purchased versions of SmarterMail contain a preconfigured web server that installs by default, enabling SmarterMail to run "right out of the box". Finally, as all SmarterTools products are built using the Microsoft .NET framework, enabling web services to centralize access through a single Web Interface, anyone, end users and Administrators, can access SmarterMail from anywhere, at anytime, using a simple web browser.

What is SmarterMail

SmarterMail Professional Edition gives email users and more power and control than ever before with the most flexible email server currently available.

SmarterMail is built and priced to be both beneficial and accessible to individuals and enterprise-level organizations alike, and is able to support anywhere from one to an unlimited number of domains and an unlimited number of email addresses. In addition to providing end users with advanced features like mail account statistics and precise user-controlled spam and content filtering, end users with admin permissions for the domain have the ability to set and retrieve domain level statistics, provide domain-level spam and content filtering (versus having individual end users set these), administer spam using any number of different spam and black lists (e.g. SpamCop, ORDB, etc.), set domain-level aliases, implement SMTP authentication, and much more.

As an added benefit, SmarterMail is accessible from a standard web browser, giving administrators and end users email capabilities anytime, from anywhere. SmarterMail uses industry standard mail protocols, like POP3 and IMAP4 for incoming mail and SMTP for outgoing mail, and is compatible with the most popular desktop email clients (e.g. Microsoft's Outlook and Outlook Express or Qualcomm's Eudora).

How SmarterMail Works

There are two main components that work together within SmarterMail Professional Edition, the Web Interface and the Web Server.

SmarterMail Web Interface

The Web Interface is a browser based administration platform that installs on a single server and supports administration of domains and email accounts as well as email account access by end users. End users are able to access and use their accounts using either web mail (email account access using a web browser) or with a desktop application (e.g. Outlook or Outlook Express, or Qualcomm's Eudora).

SmarterMail Web Sever

The Web Server installs with the SmarterMail Web Interface by default, easing the implementation of SmarterMail and meaning that there is zero configuration necessary for SmarterMail to work "right out of the box". This Web Server gives users and administrators access to the SmarterMail Web Interface from the Internet by utilizing the IP address assigned to the local machine. However, after installing SmarterMail, it is recommended that the Web Interface be moved from the SmarterMail Web Server to Microsoft IIS (if available) for more stability and security. For step-by-step instructions on how to transition SmarterMail to IIS, see Converting to IIS under the installation section of the help menu.

SmarterMail Professional System Requirements

The requirements of SmarterMail Professional Edition are minimal, so SmarterMail can coexist with other applications on the same server. Below you will find the minimal requirements and a sample installation which may help you decide how much your hardware can process.

Minimum Requirements

- Windows NT 4.0 (SP 6a), Windows 2000, Windows 2003 (all versions)
- RAM: 128mb
- CPU: PII 500
- DISK: 150 Megs
- IIS 4 or higher (defaults on install to SmarterMail Web Server)

It is suggested customers use IIS in place of the SmarterMail Web Server to provide additional security and stability. The intended purpose of the SmarterMail Web Server is so that the product is fully functional even without the existence of a marketed web server. IIS is an enterprise level web server, and SmarterMail takes advantage of many features in IIS which will provide the highest return on investment.

Copyright and Trademark Information

All contents of this Help file, as well as all contents on www.smartertools.com, are copyright© 2002-2003, SmarterTools

The SmarterMail™ and SmarterTools names and logos are trademarked and protected by SmarterTools

Product and Component Acknowledgements

Menu component produced by

Spell Check produced by

Charting component produced by

Logging in to SmarterMail

You will need to obtain the link to your SmarterMail server's web site from your Administrator or Domain Administrator.

To login to SmarterMail, type in your full email address and Password on the login screen. If everything matches up, you will be presented with the welcome page and a view of all folders in your mailbox. The full original email address (not an alias address) must be used to log into the corresponding mailbox

One thing to notice on the Login page is the "Remember Me" checkbox. By checking this box SmarterMail encrypts your login and password, then you can 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.

A standard User is able to view all email folders (inbox, sent, and Custom) for their designated account. Users with end users with admin permissions for the domain privileges are usually the owner of a domain who can add/remove users and change domain settings.

End User FAQ's

What role does the SmarterMail Web Interface play?

The Web Interface is a powerful tool that is easy to install and configure. The Web Interface is a dynamic web site that after installation on any one server in your network, it is accessible from any browser locally or from the Internet. It allows the creation of Internet accounts so up to an unlimited amount of users can log in and view email for any domain.

Can the Web Interface run on the same server as a stats server, or any other type of software?

Yes. SmarterMail Professional Edition can run in combination with any other products. A common configuration for a startup hosting company is a multi-purpose machine for stats, mail, web server etc. Optimize a server delegating large amounts of email traffic by dedicating it solely for email.

When I access my mailbox using web mail, why are my deleted messages only showing up as crossed out and not as being moved to my Deleted Items folder?

There is an option for end users to choose what action deleted items take. When deleted items are crossed out (to symbolize deletion) then you have the 'Mark as Deleted' option chosen. If you want the messages to move to a deleted items folder upon deletion, you can select the 'Move to Deleted Items Folder' option in your Config/My Settings page.

How can I ensure that mass mailings are received faster?

Sending the same message to fifty or more recipients can slow the delivery process. To ensure a speedy delivery, with mass mailings containing more than fifty recipients, send the same message to fifty or less addresses at once.

Administrator FAQ's

SmarterMail stops unexpectedly. What should I do?

In our experience, this generally happens due to bad blocks on the server's hard drive. Therefore, look for an event in the event viewer showing bad blocks on the hard drive or any other conflict that may stop a service. Regardless of whether you see an event of this type or not, perform a check disk and restart the service. See below for instructions on how to restart the service:

- Open control panel - Administrative tools - services
- Scroll down to "SmarterMail Service."
- Right click on it and select "restart."

How do I change skins?

Changing skins is an Administrator feature only. Utilizing custom skins is an extremely easy process: you simply unzip your chosen skin and replace the existing Style and Images folders within your SmarterMail installation. For example, go to "C:\Program Files\SmarterTools\SmarterMail\MRS\" and rename the existing "Styles" and "images" folders (e.g. "Styles_default" and "images_default" respectively) to preserve the SmarterMail default skin. Then, simply unzip your new skin into the MRS folder, and the new skin is active and in use. It's just that simple!

My pages won't load in to my browser, it just tries to download the pages. Why?

Chances are the .NET framework was installed prior to installing IIS. When you install IIS first, then install the .NET framework, all proper mappings for .aspx, .asmx, etc. pages are made. However, this does not happen if you install the .NET framework prior to installing IIS. If this is the case, there are three ways re-map .NET v1.1 to fix it:

Manually re-map .NET version 1.1:

- Go to Start -> Run -> and type "command.com".
- At the command prompt, type "aspnet_regiis - i" (less the quotation marks).
- This command will configure all applications to have the proper .NET extensions within IIS.
- Type "exit" (less the quotation marks) to exit the command prompt.

or

- From "add remove programs" in the "control panel", uninstall .NET v1.1, then reinstall with windows update."

or

- From "add remove programs" in the "control panel", uninstall SmarterMail, then reinstall

Email messages are not getting sent, could this be a problem with SMTP?

The SmarterMail Service could be conflicting with the IIS Virtual SMTP. To disable IIS Virtual SMTP:

- Open the Control Panel - Administrative Tools - Internet Information Services
- Open the "Web Sites" tree
- Look for IIS Virtual SMTP, if it exists, right click on it and select disable.

I am unable to activate SmarterMail, what do I do?

Once SmarterMail is installed, if you are unable to activate you need to contact our support department. Click here for our contact information.

Installation and Configuration

Pre-installation

Before installing SmarterMail, ensure that you have DirectX installed on your computer. To obtain the latest version of DirectX, click here, or use the Microsoft Windows Update service.

Installation

There is one Setup file to install SmarterMail Professional Edition that includes all components (the web server and Web Interface) necessary to allow SmarterMail to run right "out of the box."

Following the installation procedure, a browser will be prompted to open to the 'Getting Started' topic under this section. This topic will show you how to start using your SmarterMail server.

The Web Interface

The Web Interface installs with the SmarterMail Web Server, and, by default, the web server is set to respond to all IPs. When running SmarterMail on the SmarterMail web server, the administrative login to SmarterMail will bind to the localhost IP address of 127.0.0.1 and will use port 9998. Therefore, in order to initially access the Web Interface so you can start adding domains and setting up mail for those domains, you can double clicking the desktop shortcut or type "http://127.0.0.1:9998/login.aspx" into a browser. Please keep in mind, however, that when you start adding domains into SmarterMail, you will need an external IP address that can be used for sending and receiving email.

The first time you access the Web Interface, log in using the following default settings:

- Full Email Address= admin
- Password = admin

Select Free or Purchased Copy

Choose whether you will be using the free version, or a purchased version.

Add a Domain

Adding domains into SmarterMail is an extremely simple process. There is a Domain Information Wizard that actually walks you through the process. Be sure you fill out the necessary fields as thoroughly as possible. Recommended settings already exist where applicable.

General Domain Information

Domain Name: Enter your full domain name (e.g. smartertools.com). This domain name must match one that is registered with a Domain Name Server in order to send or receive mail.

Domain IP: From the drop down list, select the IP that you would like the SmarterMail Web Server to use. This IP will be how Administrators and End Users access the Web Interface.

Disable Domain: Checking this box disables the domain. The domain will be unable to send or recieve mail, and no users will be able to log into the web interface for this domain.

SMTP Port: The default Port that SMTP uses is 25. If you would like SMTP to use a different port on your mail server, enter a different number.

Alternate SMTP Port: This is an alternate Port that SMTP can use. This will be in addition to the standard SMTP Port.

POP Port: The default Port that POP uses is 110. If you would like POP to use a different port on your mail server, enter a different number.

IMAP Port: The default Port that IMAP uses is 143. If you would like IMAP to use a different port on your mail server, enter a different number.

Require SMTP Authentication: Check this box if you want SMTP Authentication to be used the end users of this domain. Each user must then supply an email address and password in order to send email with their account.

The authentication methods supported by SmarterMail are Cram-md5 and Login.

Click "Next"

Domain Admin Information
User Name: Enter the log in name for the domain administrator. The domain administrator is usually the owner of the domain and is responsible for adding and deleting email accounts and setting configurations associated with that domain.

Password: Enter the password for the domain administrator.

First Name: Enter the first name of the domain administrator.

Last Name: Enter the last name of the domain administrator. Please Note:The creation of an administrative email account for each domain on the server is required by SmarterMail.

Click "Next".

Domain Limits
Max Domain Size: The total amount of space, in kilobytes, that the Mail Server will allow the domain to use.

Max Mailbox Size: The total amount of space, in kilobytes, that each email account can have saved on the server at one time (including inbox, sent and deleted folders).

Max Users: The maximum number of email accounts that the domain admin can append to the domain.

Max Aliases: The maximum number of false email accounts (forwarded to a true email account) that are allowed per domain.

Show Domain Alias Menu: Check this box to show the "Domain Alias Administration" option in the menu under "config" for domain admins. This will allow domain admins to combine email addresses with different domain names into one mailbox. More information about this item is available under "end user options" in the help menu.

Max Domain Aliases: Enter the maximum amount of Domain Aliases allowed per domain.

Show List Menu: Check this box to show the "Mail List Administration" option in the menu under "config" for domain admins. This will allow domain admins to use the list serv features for sending emails to via lists to many users. More information about this item is available under "end user options" in the help menu.

Max Lists: Enter the maximum ammount of lists allowed for the domain.

Max Recipients: Enter the number of email addresses a user can send a message to at one time.

Max Message Size: Enter the maximum total size of an email (including text, html, images and attachments) that an end user can send at one time.

Domain Path: This is the path to the directory where all information pertaining to the domain resides (XML files, mail statistics, alias information, etc.). Before this is changed in SmarterMail, it needs to be manually changed in Windows Explorer on the server itself. After both places are changed, the domain will have to be "Reloaded" under "Manage Domains".

Mail List Command Address: This is the email address that list commands can be sent to via email. More information about the commands can be found under End User/Config/Mail List Admin/Edit Help File.

Click "Next".

Domain Admin Menu Options
Network Admins can grant access to the following options to each Domain Admin, dependant on the hardware and bandwidth available to your mail server.

Show Spam Menu: Check this box to enable "Domain Spam Administration" options for the domain admin under "config" in the main menu. Spam options are inherited by all end users within the domain. More information about this item is available under "end user options" in the help menu.

Show Content Filtering Menu: Check this box to enable "Domain Content Filtering" options for the domain admin under "config" in the main menu. Content filtering is inherited by all end users within the domain. More information about this item is available under "end user options" in the help menu.

Show Statistics Menu: Check this box to enable the "Domain Statistics" option for the domain admin under "config" in the main menu. More information about this item is available under "end user options" in the help menu.

Click on the "Save" button.

Activate Product

Upon installation, SmarterMail will offer licensing options for your selection. By default, SmarterMail will install as a fully-functional single domain ten user trial version with no expiration date set. The additon of more than one domain, or more than ten email accounts, will require the purchase of a full version license of SmarterMail. However, if you have already purchased a license for SmarterMail, you can input it here for activation.

The version of SmarterMail that activates on your server depends upon the type of license you purchase. Once the license is acquired, you can activate it by logging into SmarterMail as the administrator and selecting "Manage --> Licensing". By clicking on the 'activate key' button you are presented with the ability to input your license and the email address used during the license purchase. After the license and all pertinent information is added, the SmarterMail Web Interface will communicate with the SmarterTools Licensing Server for verification and activation. This communication occurs along port 80, so if for whatever reason, the communication is blocked (e.g. from a firewall) the license will not verify and activate.

When changing or upgrading license types, you simply need to come back to "Manage --> Licensing" and click the 'activate key' button. You will once again be prompted for your license number and email address. After clicking 'ok', the upgraded or changed license is activated and ready for use.

Administration

There are two different levels of users that can access the SmarterMail Web Interface: Administrators and End Users. Additionally, there is an end user with admin permissions for the domain that has specific privileges not granted to standard End Users.

The Administrator has complete control over the Web Interface and all of the domains within the SmarterMail Professional installation. The Administrator can add/remove domains as well as adjust the global settings for domains and email accounts.

The "Administrator" section of SmarterMail Professional Edition Help entails all the configurations available to the Administrator. All administration tasks of SmarterMail Professional Edition are handled from the Web Interface, so changes made to an individual domain or to configurations affecting all domains (globally) on the mail server are handled from the Web Interface. The Administration functions of SmarterMail are broken down into three main categories (Manage, Config and Status), and each main category has a number of different subcategories.

Manage Menu

From the manage menu, you will actually manage the server, its spool, licensing, and the domains contained on the server.

Manage items are broken into five sections: Manage Domains, Add Domains, Manage Spool/Queue, Enable/Disable Services and Licensing.

Manage Domains

After adding Domains, the Manage Domains option gives you the ability to search for a particular domain that is using SmarterMail and get the domain info, edit the domain, or delete the domain from the Web Interface.

View Domain

Clicking on "view" is the same link as clicking on the domain name. This link will automatically log the SmarterMail administrator into the mailbox of the primary domain holder with the end users login address and password (view all folders page) so you can change domain level configurations. See the "End User Options" section of help for further instructions, or click here to see the end users home page (view all folders page).

Adding Domains

Adding domains into SmarterMail is an extremely simple process. There is a Domain Information Wizard that actually walks you through the process. Be sure you fill out the necessary fields as thoroughly as possible. Recommended settings already exist where applicable.

Manage Spool/Queue

The information in Manage Spool/Queue 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 arrive, that are available for the server to read in and store.

Similarly, a queue is a sequence of email messages that are waiting to be processed and sent out. SmarterMail is multi-threaded, therefore if a message can not 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.

Click the drop down list and choose how many messages to show on one page. If the spool spans more than one page, the page numbers will link to new page in the lower right corner of the table. To subject messages to an action, check the box next to a message or push the "select all" button to check all of the boxes. To de-select all boxes, click the "deselect all" button. After checking the desired boxes, select an action from the drop down list: force delivery or delete the selected messages. To delete all messages in the spool, regardless of the check box, select "delete all messages" from the bottom of the drop down list. To perform the action that is selected, click on the "do action" button.

Each message consists of:

File Name: The numerical name that SmarterMail gives each message.

Sender: The email address the email originated from.

Time In Spool: The amount of time that the message has been in the spool since its arrival.

Delivery Attempts: This is the number of times that the message has been through the queue, or has tried to process a message for delivery.

Next Delivery Attempt: If the first delivery attempt for an email message fails, this column will display the number of minutes left until SmarterMail will try to deliver it again.

Recipients: When a message is sent to multiple recipients, this value represents the ratio of the number of messages delivered over the total number of recipients. Regardless of the number of recipients, each message will hold only one thread. If the total number of recipients is high (e.g. over fifty), the message will delay the release of a thread until delivery to all addresses is complete.

Click on the ratio to view the email address and the sent status of the recipients.

Status: This detail shows the status of each message in the queue. If it the messages are in line to be sent, the status will display "waiting." When SmarterMail is processing a large message, the status will display "processing", as it is close to being delivered.

Size: This is the total size in Kilobytes for the message and its attachment(s).

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. Click on the refresh button in the upper right corner above the table to get a new list of the messages that are actually in the spool.

Administrator Enable/Disable Services

The Administrator can choose to activate three different type of mail services: POP and/or IMAP for incoming mail, and SMTP for outgoing mail.

To disengage a service, simply click on the "stop" button next to the service name. To re-enable a service, click on the "start" button.

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.

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.

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 that have been received for them at their local server.

Administrative Settings

Log in as the Administrator and view the "config" menu item. The Configurations consist of Global options to set, which will affect all of the End Users and domains that use the mail server.

General Settings

The General Settings page is where you control many of the global settings for the SmarterMail server. For first time users, we recommend the first change to be the Global Admin Username and the Global Admin Password to avoid anyone getting into your system using the default login.

Global Admin UserName: This is the log in name associated with the Administrator's account for the SmarterMail Server. You will use this name instead of a "Full email address" when logging in as the Administrator for SmarterMail.

Global Admin Password: This is the password associated with the Administrator's account.

Primary dns: This is the dns server to use for mail exchange record lookups. These records tell SmarterMail where to send outgoing mail.

Secondary dns: This is the dns server to use if the first one cannot be reached for any reason.

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

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.

Log Level: The log level is the amount of detail produced in email logs. Mail server logs are text files that contain raw data for tracking actions that take place on the mail server. Select an option from the drop down list which is in order of least to greatest detail. Select one of the following formats to log all email messages for your Mail Server:

- Exceptions Only: Small Logs
- Normal
- Detailed: Medium Logs
- Light Debug
- Normal Debug
- Detailed Debug: This setting will track everything possible and produces large logs. It should be used for trouble shooting the mail server.

Auto delete log files: Log files older than the number of days specified in this field will be automatically deleted. Set it to 0 to disable this feature.

Disable Log Cache: If this option is unchecked the server will cache the log file for 16 kilobytes or 15 seconds (whichever comes first), checking this option forces the server to write every line as it occurs.

Delivery Delay: As the name implies, 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. 1000 milliseconds= 1 second.

Time Between Retries: 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. The server attempts to resend emails 4 times before it is bounced.

Double Bounce Action: When an inbound email does not match an account or alias, and it is unable to be returned to the original sender, you can select from the drop down list to either forward it to the postmaster account or delete the message.

Maximum Relay Threads: Enter the maximum amount 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 when a message can not be sent right away, it waits until it is resolved before moving on to the next one.

Allow Relay For: 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 altogether:

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 Hosts: Limits relay access only to mail hosts (domains) on your SmarterMail Server.

Only Local Users: Limits relay access to users (email accounts) for a valid domain 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.

Relay to Gateway: Check this box to turn this feature on. Relay to gateway will send or route all outgoing mail to another SMTP server before it reaches its final destination. The destination SMTP server would have to be configured to take relays from your particular IP address. For example, if the destination SMTP server was a SmarterMail Server, then the IP from the original mail server would need to be added to the White List unless "anyone" was selected for the "allowing relay for" option.

Gateway Server: Enter the IP address of the gateway/SMTP server listed in "Relay to Gateway".

Note: When using a mail gateway, SmarterMail statistics may not be accurate due to the fact that a single mail with multiple recipients, is only handed off as one, but would have been sent as multiple emails.

Mailbox cache timeout minutes: This setting allows server administrators to set the period the server will cache a mailbox. If the mailbox cache is reached, it will also release any message cache from that mailbox.

Message cache timeout: This setting allows server administrators to set the period a server will cache a message.

SMTP Settings
This window displays the different settings the Administrator has control over with regards to the SMTP protocol and sending mail from the server, regardless of whether the mail is sent from the server itself or relayed through the server.

Spool Path: This is the path to the directory where outgoing messages are held prior to delivery.

Maximum Threads: A thread supports one message and requires memory and CPU usage. Once the message reaches its final destination the thread is released and another message can use the thread. Raising the limit of threads will enable the server to handle more messages simultaneously, but requires more CPU usage and memory. If the maximum thread limit is reached, the server will reject messages and send an error to the sender.

Session Timeout: Timeout settings determine the length of time for the Internet connection between the mail server and the email client (e.g. Outlook or Outlook Express, or Eudora) on a desktop computer. A session timeout is the amount a time a session or connection stays open from the mail server to the email client, regardless of whether or not a command is issued. For example, clicking the "Send" button once to send messages to 1000 email addresses. While only a single command is issued ("send"), the mail server must allow enough time for the session to stay open so that all 1000 messages are sent successfully. Shortening the session timeout length can save memory and CPU usage, but will require a faster connection from an email client to maintain the same session. A larger timeout period will extend the amount of time an email client can interact with the server, but uses more server resources. Use an average time length to benefit both the mail server and its clients and account for slow or unstable connections.

Command Timeout: Enter the level of inactivity in seconds that my occur between the mail server and an email client (e.g. Outlook or Outlook Express, or Qualcomm's Eudora), that the server will tolerate prior to closing the connection. In order to keep the mail session open, the email client has to issue a command before this time limit expires.

Maximum Bad Commands: Enter the number of bad commands that the mail server will accept before closing the connection with the email client (ending the session). Bad commands take place when the email client from a desktop computer sends a command out of sequence or when the Internet connection is interrupted. Each time the mail server interacts with a bad command, it taxes server resources. You are able to limit the number of bad commands to lighten the work load and bandwidth on the server. However, a limit too low will disallow some email clients to finish a session due to an unstable connection. Enter a limit to benefit both the mail server and its clients. You may want to change these settings depending on the amount of users on the mail server and its hardware quality.

Enable verify mailbox: 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 expand list: 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.

Enable spool executable: Enabling the spool executable will set SmarterMail to launch the executable specified in the "Spool executable command line" field for every message that enters the spool.

Spool executable command line: Enter the full path to an executable you wish to process incoming messages with. Use %filepath as an argument to pass the path to the email file to the executable. It is important to set a reasonable delivery delay to prevent SmarterMail from attempting to deliver the message while the executable is still accessing it. It is safe for the executable to delete the message to prevent delivery.

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.

Enable auto spam notification: Enabling this option will have SmarterMail send a notification message to the email address specified in the Notification Address field when X messages of the same size from the same sender are received in Y minutes, where X and Y are values you specify.

Notification address: This is the address to send automatic spam notifications to.

POP3 Settings

From this page you are able to control the settings specific to the POP3 Protocol, used to receive incoming mail messages. These options consist of security options as well as optimization options.

Maximum Threads: A thread supports one message and requires memory and CPU usage. Once the message reaches its final destination the thread is released and another message can use the thread. Raising the limit of threads will enable the server to handle more messages simultaneously, but requires more CPU usage and memory. If the maximum thread limit is reached, the server will reject messages and send an error to the sender.

Session Timeout: Timeout settings determine the length of time for the Internet connection between the mail server and the email client (e.g. Outlook or Outlook Express, or Eudora) on a desktop computer. A session timeout is the amount a time a session or connection stays open from the mail server to the email client, regardless of whether or not a command is issued. For example, clicking the "Send" button once to send messages to 1000 email addresses. While only a single command is issued ("send"), the mail server must allow enough time for the session to stay open so that all 1000 messages are sent successfully. Shortening the session timeout length can save memory and CPU usage, but will require a faster connection from an email client to maintain the same session. A larger timeout period will extend the amount of time an email client can interact with the server, but uses more server resources. Use an average time length to benefit both the mail server and its clients and account for slow or unstable connections.

Command Timeout: Enter the level of inactivity in seconds that my occur between the mail server and an email client (e.g. Outlook or Outlook Express, or Qualcomm's Eudora), that the server will tolerate prior to closing the connection. In order to keep the mail session open, the email client has to issue a command before this time limit expires.

Maximum Bad Commands: Enter the number of bad commands that the mail server will accept before closing the connection with the email client (ending the session). Bad commands take place when the email client from a desktop computer sends a command out of sequence or when the Internet connection is interrupted. Each time the mail server interacts with a bad command, it taxes server resources. You are able to limit the number of bad commands to lighten the work load and bandwidth on the server. However, a limit too low will disallow some email clients to finish a session due to an unstable connection. Enter a limit to benefit both the mail server and its clients. You may want to change these settings depending on the amount of users on the mail server and its hardware quality.

Enable APOP: APOP stands for Authenticated Post Office Protocol. Every mail connection made sends your username and password across the network in clear text (no encryption). With APOP enabled, your password is encrypted while being transmitted over the Internet.

IMAP4 Settings

From this page you are able to control the settings specific to the IMAP Protocol, used for receiving mail. These options consist of security options as well as optimization options.

Session Timeout: Timeout settings determine the length of time for the Internet connection between the mail server and the email client (e.g. Outlook or Outlook Express, or Eudora) on a desktop computer. A session timeout is the amount a time a session or connection stays open from the mail server to the email client, regardless of whether or not a command is issued. For example, clicking the "Send" button once to send messages to 1000 email addresses. While only a single command is issued ("send"), the mail server must allow enough time for the session to stay open so that all 1000 messages are sent successfully. Shortening the session timeout length can save memory and CPU usage, but will require a faster connection from an email client to maintain the same session. A larger timeout period will extend the amount of time an email client can interact with the server, but uses more server resources. Use an average time length to benefit both the mail server and its clients and account for slow or unstable connections.

Command Timeout: Enter the level of inactivity in seconds that my occur between the mail server and an email client (e.g. Outlook or Outlook Express, or Qualcomm's Eudora), that the server will tolerate prior to closing the connection. In order to keep the mail session open, the email client has to issue a command before this time limit expires.

Maximum Bad Commands: Enter the number of bad commands that the mail server will accept before closing the connection with the email client (ending the session). Bad commands take place when the email client from a desktop computer sends a command out of sequence or when the Internet connection is interrupted. Each time the mail server interacts with a bad command, it taxes server resources. You are able to limit the number of bad commands to lighten the work load and bandwidth on the server. However, a limit too low will disallow some email clients to finish a session due to an unstable connection. Enter a limit to benefit both the mail server and its clients. You may want to change these settings depending on the amount of users on the mail server and its hardware quality.

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 the Web Services. These default settings can be overwritten and are only intended to avoid needless data entry.

These settings have no bearing on domains that have already been setup.

Domains path (prefix): This is the path where the domain data will be kept. This includes domain information, user information, email data, etc.

Domain Size Limit: Enter the default for the maximum amount of space, in megabytes, that one domain can use on the mail server at one time, including but not limited to inboxes, outboxes, attachments and configurations.

Mailbox Size Limit: Enter the default for the maximum amount of space, in megabytes, that one email account can use on the mail server at one time, including but not limited to, inbox, outbox and attachments.

IMAP Port: The default Port that IMAP uses is 143. If you would like IMAP to default to a different port on your mail server, enter a different number.

POP Port: The default Port that POP uses is 110. If you would like POP to default to a different port on your mail server, enter a different number.

SMTP Port: The default Port that SMTP uses is 25. If you would like SMTP to default to a different port on your mail server, enter a different number.

Alternate SMTP Port: This is an alternate Port that SMTP can use. This will be in addition to the standard SMTP Port.

Max Aliases: Enter the default for the maximum number of alias email accounts (an account that forwards incoming mail to a true email account on the server) that are allowed per domain.

Domain User Limit: Enter the default for the maximum number of email accounts that can be created for one domain.

Max Message Size: Enter the maximum total size of an email (including text, html, images and attachments) that an end user can send or receive at one time.

Max Recipients: Enter the limit of emails a user can send to at one time.

Show Domain Alias Menu: Check or uncheck this box to default the box for the "Domain Alias Administration" option in the menu under "config" for end users with admin permissions for the domain. This will allow end users with admin permissions for the domain to combine email addresses with different domain names into one mailbox. More information about this item is available under "end user options" in the help menu.

Max Domain Aliases: Enter the default for the maximum amount of Domain Aliases allowed per domain.

Max Lists: Enter the maximum ammount of lists allowed for domains by default.

Show Content Filtering Menu: Check this box to enable "Domain Content Filtering" options by default for the end users with admin permissions for the domain under "config" in the main menu. Content filtering is inherited by all end users within the domain. More information about this item is available under "end user options" in the help menu.

Show Spam Menu: Check this box to enable "Domain Spam Administration" options by default for the end users with admin permissions for the domain under "config" in the main menu. Spam options are inherited by all end users within the domain. More information about this item is available under "end user options" in the help menu.

Show Statistics Menu: Check this box to enable the "Domain Statistics" option by default for the end users with admin permissions for the domain under "config" in the main menu. More information about this item is available under "end user options" in the help menu.

Show List Menu: Check this box to show the "Mail List Administration" option in the 'Config' menu for end users with Domain Admin privlidges.

Require SMTP Authentication: Check this box if you want to enable SMTP Authentication for the end users of this domain by default. Each user must then supply an email address and password in order to send email with their account. *Most email clients will have a Secure Password Authentication checkbox for this option.

General Spam Settings

The General Spam Settings page allows you to control what spam options are available to the end user when logged into the Web Interface. When these options are available to the end user, they can apply a spam weight to a specific IP4R service, which can then be used to filter incoming messages.

Check these boxes to enable Reverse DNS and Verify Sender Spam options to End Users.

Reverse DNS Lookup: Verifies the domain of the sender by resolving its IP address (checks the address).

Verify Sender: Authenticates that the email account exists with the sender's mail server. If the mail server is down or unavailable at the time, it will not authenticate the email and the message might not reach its final destination.

Spam Timeout: Enter the time limit that the mail server will wait for a mail spam list from a DNS.

Skip Intra Domain Spam Check: This option is checked by default so that mail sent from accounts on the local server is not checked for spam integrity, saving time and resources.

Spam List Administration

The Spam List Administration page allows you to control which IP4R spam lists are available to the end user when logged into the Web Interface. When these options are available to the end user, end users can provide a spam weight to each list, which can then be used to filter incoming messages.

Delete a Spam List

To delete a list, highlight the list item and click on the "delete" button.

Add/Edit a Spam List

Click on the "add" or "edit" button.

Enter a name for the spam list

Some Domain Name Servers contain a list of known spam mail servers. SmarterMail makes it possible for Administrators to enter the URL and take advantage of these Domain Name Servers to filter out mail from known spammers. Enter the URL for a DNS (e.g. http://spamguard.leadmon.net). Enter your favorite spam mail Domain Name Servers, or perform an Internet search on "Spam Mail DNS List Lookup", for more information and URLs. Many URL lookups for spam mail on Domain Name Servers exist, SmarterTools™ suggests using the following:

SpamCop - bl.spamcop.net

ORDB - relays.ordb.org

SpamHaus - sbl.spamhaus.org

Monkeys Proxy - proxies.relays.monkeys.com

OSSRC - relays.osirusoft.com

Enter a description of the DNS Server

Click on the "save" button to finish adding DNS Server.

SMTP Kill List
A SMTP Kill List is an effective way of temporarily cancelling a domain's ability to send or receive email on the server. For example, if a particular account is sending an abnormal amount of email, you simply add their address to the Kill List and they are unable to use the mail server.

The SMTP kill list has an option to block users who have multiple bad sessions in a certain ammount of time. A bad session, is any session that ends without successfully sending a message. Simply choose the number of bad sessions for the timeframe in which they occur, and the ammount of time to block them. Be sure to click save.

Select from the drop down list how you would like to search for the domain name to ignore, from the begining or end of the domain associated with messages. Enter the domain, or partial domain to put on the kill list. Use a wildcard within the description to block domains. For example: *@domain.com to block all addresses from a specific domain, or sales@domain.* to block extensions, etc. Click on the "add" button finish. To delete an entry, select it from the list and dick on the "delete" button.

IP Black List and White List
From this page you can control which IPs are blacklisted (not allowed) from mail services on this machine, or white listed (allowed) to access the mail services on this machine. To enter in a range of IPs, please use the following syntax: 10.0.0.1-10.0.0.255.

There are three different white/black lists. Each applies only to its specific category: SMTP, POP, or IMAP

The options for each category are the same.

The three settings on the top of the table are for dynamic blocking. These limits are dependant on the on the amount of messages that the mail server is delegating. If you do not want dynamic IP Blacklisting, leave these values at zero.

Allow: Enter the number of times the mail server can receive a message from the same IP before an action will take place.

connections in: Enter the time in minutes that the IP has to reach its limit set in "Allow."

minutes, block for: Enter the time in minutes that the IP should be not allowed to send messages to the mail server. If an IP gets blocked, the IP will display in "currently blocked IPs" under "Stats" in the main menu.

Black List: Block IP addresses from sending mail to SmarterMail by adding them to this list.

White List: Add an IP addresses to this list to accept all mail from the sender, regardless of Black List generalization or content filtering.

IP Bypass For SMTP Authentication
From this page you can control which IPs will bypass any domain that has SMTP authentication enabled. This is often used to allow clients who have applications that do not support SMTP authentication to bypass this check. To enter in a range of IPs, please use the following syntax: 10.0.0.1-10.0.0.255

Add or delete individual IP addresses or blocks of IP addresses. Add IPs by entering the address into the add field and click the "add" button. Delete IP addresses by selecting the IP or range of IPs and clicking the "delete" button.

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.

Virus Scanning Enabled: Check this box to enable SmarterMail to start taking action for messages marked in the quarantine directory.

Virus Action: This menu allows the selection of the action to be taken on email containing a virus.

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.

Delete: This option will enable the SmarterMail service to delete any associated files attached to this message from the spool directory. This does not take any action on the quarantine directory.

Quarantine Directory: Enter the absolute path to the quarantine directory set for the server.

AntiVirus Solutions

While SmarterMail is compatible with a wide variety of antivirus products, SmarterTools recommends the use of Trend Micro's Server Protect in conjunction with SmarterMail. Server Protect is a premier enterprise level virus scanning tool, produced by a global leader in antivirus security. This product is a comprehensive virus scanning utility, not only for use with Smartermail, but also to be used on servers for all virus scanning needs. Server Protect is fully scalable and has centralized management options. Furthermore, Trend Micro's antivirus solution can be purchased through SmarterTools for use with SmarterMail, for a mere fraction of the cost of many other enterprise level virus solutions. Server Protect is compatible with almost all operating systems currently available.

For more information regarding integration and pricing of Server Protect from SmarterTools click here.

Recommended Setup and Options

A delivery delay will need to be setup on the spool so virus utilities have ample time to scan all messages. This delay can be setup under Config/General Settings. Depending on the virus utility used, and the server performance; the recommended delay is between 20-60 seconds. *Note 1000 milliseconds= 1 second.

A comprehensive scan of the drive is recommended upon initial installation of the virus software to ensure that there are no viruses currently on the server. After this, the Domains directory (by default C:\SmarterMail\domains\ ) should be excluded as all mail will be scanned prior to the message ending in the final folder.

Also, after the initial comprehensive scan, most antivirus utilities will allow you to scan files only upon be written to the physical disk. This will ensure all files are scanned, while minimizing read time for the virus scanner, allowing an optimum balance of security and performance.

Virus software such as Trend Server Protect will also allow an attempted 'cleaning' of the affected file prior to a quarantine. This is a recommended setting, as it will allow the original (infected) message to be received by the intended recipient minus the actual virus. If the message cannot be 'cleaned' the message is then quarantined, and the sender is notified

Statistics

The ability to track and manage your server is essential. SmarterMail allows the Administrators to keep total control of the server from anywhere, at any time, using a simple browser-based interface. The statistics available include, on the server level, the various threads (IMAP, POP, SMTP and relay) being processed by the mail server, the date and time the mail server was started, and the time the server has been up and running. Administrators also have various domain-level statistics to view, including the amount of mail processed, both incoming and outgoing, and the amount of spaced used on the mail server by the domain. If any IP addresses are blocked from accessing the mail server, Administrators can also monitor those. Statistics are also made available through Web Services that open up some Internet code from SmarterMail enabling easy implementation into existing applications useful for billing purposes. To see more on this ability, see Web Services in the Administrator section of the help.

Server Statistics

The Server Statistics page allows you to view active statistics for the mail server as a whole. This information can help in monitoring mail abuse or usage trends since the service was started.

The first table includes the exact date and time that the SmarterMail Service was started and how long it has been running.

On average, one POP or SMTP thread is capable of supporting one email message. IMAP is different in that IMAP can support multiple threads for a single connection. You can track the number of threads your mail server is processing, if you are getting close to your servers maximum, and more. If you do see that you are nearing the maximum thread settings, you may want to adjust your configurations or hardware as exceeding a thread maximum may result in a loss of email service untill more threads are made available. The second table has the current status, last five minute average, last hour average and the averages since the service started for the following items:

IMAP Threads: the number of threads processed for incoming mail using IMAP. As stated, IMAP can process multiple threads for a single connection.

POP Threads: the number of threads processed for incoming mail using POP. Generally, this is a one-to-one correlation (one incoming message per thread).

SMTP Threads: the number of threads processed for outgoing mail.

Relay Threads: the number of threads processed as a relay.

Messages in the Spool: the number of messages currently awaiting processing. All mail, regardless of whether it is incoming or outgoing mail, goes into the spool prior to either being sent or received.

Domain Statistics

The Domain Statistics page allows you to view mail usage by domain for a specified period of time. This information can be used to see abuse or usage trends for particular users or for the domain in general. In some cases, the end users with admin permissions for the domain can use this information to bill customers for excessive usage. All statistics are totals for the date range specified.

From left to right, the statistical table details are as follows:

Domain: The domain the statistics pertain to.

Bytes Received: The bandwidth in KiloBytes accumulated from incoming email messages, regardless of content filtering.

Bytes Sent: The bandwidth accumulated from the outgoing email messages.

Messages Received: A numerical count from the incoming email messages, regardless of content filtering.

Messages Sent: A numerical count of the outgoing email messages

Space Used: The total size, in Kilobytes, of email messages and their attachments that are on the mail server.

Connections

The connections page show all connections currently made to the SmarterMail service. These connection are broken down by the type of connection made: SMTP, POP, or IMAP.

Connections are shown in each category, listing the IP address making the connection, as well as how many connections that IP has.

*Note: Multiple connections does not neccessarily mean abuse or unclosed sessions. Often networks will use a single IP allowing multiple users and computers to connect from a single location/IP.

Current Blocks

Currently blocked IPs displays a list of all of the IP addresses that are denied from using the Mail Server. SmarterMail monitors the usage from other IP's and detects if a certain IP is abusive. The setting, which can be adjusted under "config" in "White/Black Listing", will make a list dynamically of IP's that are sending too many messages and block them temporarily. Currently Blocked IPs makes available more bandwidth, space, CPU usage and memory for actual clients and accounts.

Utilities

In the utilities menu are option(s) to assist you in managing, cleaning, and maintaining the mail server. Please ensure you read the help topics thoroughly, prior to using the utilities.

Mailbox Cleaner

The SmarterMail cleaner searches the config files for all sites managed by the server. All config files will be checked for validity. In addition, the server will be cleaned of orphaned files. Orphaned files are mail files that are not actively attached to a config file or mailbox. This process may take several minutes to complete depending on a variety of factors including, but not limited to, number of domain, number of mailboxes, and server hardware.

Refresh: This option strictly refreshes the status of the cleaner.

Check Only: This option will scan the server as though it were cleaning, but does not actually 'clean' or remove any files. It does report any files found as orphans.

Check and Clean: This will run the cleaning process and will remove any orphaned files found.

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 the Web Interface 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 their corresponding functions, available to you, go to your default Web Interface install location and append "services/services_page.asmx". Your particular SmarterMail location can be the specific IP address of the Web Interface (e.g. if you installed SmarterMail with the default installation you would use http://127.0.0.1:9999/services/SiteAdmin.asmx, etc. or a specific IP address you assigned for the Web Interface if you custom-installed SmarterMail or moved SmarterMail to a new web server) or a specific site name if you configured SmarterMail as an actual website within IIS (e.g. SmarterMail.yourdomain.com). Below you will find a brief explanation of the web services available to you, along with the default installation paths to the specific web services details page.

Alias Admin Web Service
(http://127.0.0.1:9998/Services/svcAliasAdmin.asmx):

There are six (6) functions of this service available for customization. These services allow developers and/or System Administrators to dynamically create email aliases using SOAP, an HTTP GET command, or an HTTP POST command (examples for each are provided as well). The functions, and their corresponding properties, are:

- DeleteAlias - will delete a specified email alias.
- UpdateAlias - will update a specified email alias.
- GetAlias - will return information on a specified email alias.
- AddAlias - will created an email alias and add it to the specified domain.
- GetAliases - will return all aliases that belong to a specified domain.
- SetCatchAll - Sets the specified alias to be the catch-all, or clears the catch-all if a blank alias name is provided.

Domain Web Service
(http://127.0.0.1:9998/Services/svcDomainAdmin.asmx):

There are twelve (12) functions of this service available for customization. These services allow developers and/or System Administrators to dynamically add or delete domains, return domain defaults, set a primary domain, and more using SOAP, an HTTP GET command, or an HTTP POST command (examples for each are provided as well). The functions, and their corresponding properties, are:

- RenameDomain - Renames the specified domain
- GetDomainSettings - Returns the default domain settings in a DomainSettingsResult object
- GetDomainInfo - Returns the default domain settings in a DomainSettingsResult object
- AddDomain - Creates a new domain in the specified folder
- UpdateDomain - Updates the settings for the specified domain
- GetAllDomains - Returns a list of all domain names
- GetDomainDefaults - Returns the default domain settings in a DomainSettingsResult object
- UpdateDomainNameAndPath - Changes the specified domain's name and/or path
- DeleteDomain - Deletes the specified domain

- GetDomainStatistics - Returns the statistics for the specified domain over the specified period of time
- ReloadDomain - Reloads the specified domain's settings
- SetPrimaryDomainAdmin - Sets the specified user to be the primary domain admin of the specified domain

Mail List Removal Web Service
(http://127.0.0.1:9998/Services/svcMailListAdmin.asmx):

There is only one function for this service. Due to amount of possible commands for list serv, it would require an almost unusable amount of commands to manage list serv via web services. What is offered as a web service is simply the removal of all lists (settings concerning lists are in the domain setup service).

- DeleteAllLists - Deletes all mailing lists that belong to the specified domain.

Product Info Web Service
 (http://127.0.0.1:9998/Services/svcProductInfo.asmx):

There are four (4) functions of this service available for customization. These services allow developers and/or System Administrators to dynamically activate or retrieve licensing information, return product name and version number, and more using SOAP, an HTTP GET command, or an HTTP POST command (examples for each are provided as well). The functions, and their corresponding properties, are:

- ActivateLicenseKey - will activate the product with a previously set license key using the specified SmarterTools account credentials.
- GetLicenseInfo - returns the license key for the product.
- GetProductInfo - will return the product name and version number.
- SetLicenseKey - will set the product license key.

Global Update Web Service
(http://127.0.0.1:9998/Services/svcGlobalUpdate.asmx):

There are three(3) functions for this service. These services allow server administrator to set/update settings for every domain on the server using SOAP, an HTTP GET command, or an HTTP POST command (examples for each are provided as well).. The functions, and their corresponding properties, are:

- UpdateAllDomainSettings – sets the supplied fields and values for all domains on the server.
- ListGlobalUpdateFields – lists all the fields that can be updated using UpdateAllDomainSettings.
- GetGlobalUpdateStatus – gets the current status of the update (550 of 1335 domains updated)

Domain Alias Admin Web Service
(http://127.0.0.1:9998/Services/svcDomainAliasAdmin.asmx):

There are four (4) functions for this service. These services allow server administrator to add/remove and check domain aliases for a given domain using SOAP, an HTTP GET command, or an HTTP POST command (examples for each are provided as well).. The functions, and their corresponding properties, are:

- DeleteDomainAlias – Deletes the specified domain alias.
- GetAliases – Returns all domain aliases that belong to the specified domain .
- AddDomainAlias – Creates a new domain alias and adds it to the specified domain.
- AddDomainAliasWithoutMxCheck – Creates a new domain alias and adds it to the specified domain without doing an MX lookup on the new alias.

User Admin Web Service
(http://127.0.0.1:9998/Services/svcUserAdmin.asmx):

There are twelve (12) functions of this service available for customization. These services allow developers and/or Administrators to dynamically create or delete users, return user statistics, return user attributes, update user information and more using SOAP, an HTTP GET command, or an HTTP POST command (examples for each are provided as well). The functions, and their corresponding properties, are:

- AddUser - Creates a new user and adds them to the specified domain
- GetUserStats - Returns statistics of the specified user for the specified time period
- GetUser - Returns attributes of the specified user
- UpdateUserAutoResponseInfo - Updates the specified user's auto response settings
- UpdateUserForwardingInfo - Updates the specified user's forwarding settings
- GetUsers - Returns attributes of each user in the specified domain
- DeleteUser - Deletes the specified user from the specified domain
- GetUserAutoResponseInfo - Returns the forwarding info of the specified user
- GetUserForwardingInfo - Returns the forwarding info of the specified user
- AuthenticateUser –Returns a response on whether the supplied user/domain/password is valid
- LoginValidated - Returns a LoginResult object with the LoginValidated field set to True if the specified username matches the specified password

Log Types and Information.
Mail server logs are text files that contain raw data for tracking actions that take place on the mail server. Logs can be used for tracking action on various emails, troubleshooting services, or for archiving information about the mail server.

Log Types
There are five log file types:

Load - The Load log only logs information concerning domains that fail to load at startup.

IMAP - This log contains the commands and responses between a connected user and the server for this mail access protocol. Session IDs are included so sessions can be traced and followed.

POP - This log contains the commands and responses between a connected user and the server for this mail access protocol. Session IDs are included so sessions can be traced and followed.

SMTP - The SMTP log only logs incoming message traffic up until the message is written to the Spool.

Delivery - This log contains information about the delivery of the message, regardless of whether the message is delivered locally or to a remote server.

Log Levels

The log level is the amount of detail produced in email logs. Log levels can be selected on a per log basis or by a general setting in the General Settings area. When selecting the log option from the drop down list the order is from least to greatest detail.

- Exceptions Only: Small Logs. This logging option will only log exceptions.
- Normal
- Detailed: Medium Logs
- Light Debug
- Normal Debug: Large Logs
- Detailed Debug: This setting will track everything possible and produces the largest logs. It should only be used for trouble shooting the mail server.

SMTP Logs

The SMTP log only logs incoming message traffic up until the message is written to the Spool and has nothing to do with the messages after that. The delivery server handles the messages from this point on. Any difficulties in receiving mail from external sources (other SMTP servers and email clients) will show up in this log.

A normal SMTP session will look something like this:

[192.168.1.104] connected at 8/7/2003 1:31:12 PM

[192.168.1.104] rsp: 220 mailserver.smartertools.com

[192.168.1.104] cmd: EHLO userbob

[192.168.1.104] rsp: 250-userbob Hello [192.168.1.4] 250-SIZE 250-AUTH LOGIN CRAM-MD5 250 OK

[192.168.1.104] cmd: MAIL FROM: <userbob@domainname.com>

[192.168.1.104] rsp: 250 OK <userbob@domainname.com> Sender ok

[192.168.1.104] cmd: RCPT TO: <bob@yahoo.com>

[192.168.1.104] rsp: 250 OK <bob@yahoo.com> Recipient ok

[192.168.1.104] cmd: DATA

[192.168.1.104] rsp: 354 Start mail input; end with <CRLF>.<CRLF>

[192.168.1.104] rsp: 250 OK

[192.168.1.104] cmd: QUIT

[192.168.1.104] rsp: 221 Service closing transmission channel

[192.168.1.104] disconnected at 8/7/2003 1:31:14 PM

There will be a "RCPT TO" command followed by a "250 OK" for every recipient of the message. Other than the number of "RCPT TO" commands, a successful SMTP session will follow the same pattern as the above example.

Response Codes

- Response codes starting with 2 (250,221) means the previous command was accepted (except for the initial 220 greeting the server sends).
- Response codes starting with 3 (354) means the previous command was accepted, but more data is required before the command completes.
- Response codes starting with 4 means a temporary error has occurred. A line in plain English should follow, saying what the error is. Could be server down for maintenance or the recipients mailbox is full.
- Response codes starting with 5 indicate a permanent error has occurred. A line in plain English should follow, saying what the error is. For example, it could be the recipient doesn't exist on that server.

Delivery Logs

The delivery log contains information about the delivery of the message, regardless of whether the message is delivered locally or to a remote server. The delivery server watches the spool for new messages, oblivious of how they got there. When it finds a new message it will handle either deliver it locally if the recipient is local, or else it will find the server to connect to and pass the message off there.

Local delivery example:

Delivery started for bob@domain.net at 11:59:52 PM [id:3522742399]

Delivery for bob@domain.net to Jim@domain2.com has completed (Delivered)

Delivery finished for bob@idomain.net at 12:00:02 AM [id:3522742399]

Remote delivery example:

The only thing that changes is the short description of what exactly happened to the message in parenthesis at the end of the second line (in this case "Delivered"). The possible values are "Delivered", "Bounced", "Forwarded" and "Deleted"

Remote deliveries will look a lot like the SMTP log:

Sending remote mail for Bob@Domain.com

Bob@Domain.com to Jake@DomainX2.com: Start blocking while talking to 192.168.1.14

Bob@Domain.com to Jake@DomainX2.com: RSP: 220 MailServer.SmarterTools.com: Welcome MailX2.SmarterTools.com (216.119.106.195)

Bob@Domain.com to Jake@DomainX2.com: CMD: EHLO MailX2.SmarterTools.com

Bob@Domain.com to Jake@DomainX2.com: RSP: 500 Syntax error, command unrecognized (MailX2.SmarterTools.com)

Bob@Domain.com to Jake@DomainX2.com: CMD: HELO MailX2.SmarterTools.com

Bob@Domain.com to Jake@DomainX2.com: RSP: 250 OK Hello

Bob@Domain.com to Jake@DomainX2.com: CMD: MAIL FROM: < Bob@Domain.com >

Bob@Domain.com to Jake@DomainX2.com: RSP: 250 OK It's from Bob@Domain.com

Bob@Domain.com to Jake@DomainX2.com: CMD: RCPT TO: <Jake@DomainX2.com>

Bob@Domain.com to Jake@DomainX2.com: RSP: 250 OK Recipient: "Jake@DomainX2.com"

Bob@Domain.com to Jake@DomainX2.com: CMD: DATA

Bob@Domain.com to Jake@DomainX2.com: RSP: 354 Ready for data, terminate with CRLF.CRLF

Bob@Domain.com to Jake@DomainX2.com: RSP: 250 Message Received OK

Bob@Domain.com to Jake@DomainX2.com: CMD: QUIT

Bob@Domain.com to Jake@DomainX2.com: RSP: 221 Goodbye

Delivery for Bob@Domain.com to Jake@DomainX2.com has completed (Delivered)

Delivery finished for Bob@Domain.com at 11:59:49 PM [id:3522742394]

This is what a successful remote send should look like. .

Any log sample that doesn't look like the above example means something happened incorrectly, which should be described in plain English.

Response Codes

- Response codes starting with 2 (250,221) means the previous command was accepted (except for the initial 220 greeting the server sends).
- Response codes starting with 3 (354) means the previous command was accepted, but more data is required before the command completes.
- Response codes starting with 4 means a temporary error has occurred. A line in plain English should follow, saying what the error is. Could be server down for maintenance or the recipients mailbox is full.
- Response codes starting with 5 indicate a permanent error has occurred. A line in plain English should follow, saying what the error is. For example, it could be the recipient doesn't exist on that server.

Backup Information

For server administrators who would like to backup the mail server the following information will provide you with the files and default paths you should be concerned with.

MailConfig.XML: (by default C:\Program Files\SmarterTools\SmarterMail\Service) This file contains all pertinent information about the SmarterMail setup and settings.

DomainList.XML: (by default C:\Program Files\SmarterTools\SmarterMail\Service) This file contains a list of all domains attached to the server.

Domains Directory: (by default: C:\SmarterMail\Domains\ )This directory as well as the child objects contain information about the domains, the users and aliases on that server. All files and folders in the domains directory will need to be backed up except as designated below in order to restore a domain and its users to the system.

EML Files: Inside the users folder are folders for the Inbox, sent items etc. In each of these folders are the EML files that are the actual messages. These files are not required to be backed up, as they are not required for the email account to function. Keep in mind if these files are lost, the user will loose all messages in their account though.

Restores

When a restore is done, certain things must be taken into account. The following items are things to keep in mind when doing a restore.

Complete Server Restore: If for any reason, the entire server needs to be restored; restoring SmarterMail and its files should be the last step.

Once the server is ready for the restore, Install SmarterMail on the server.

Next you will want to stop the SmarterMail Service in the MMC Services Snap In.

Restore/Copy all files listed in the Backup section above.

Restart the SmarterMail Service in the MMC Services Snap In.

Restore of a Single Domain: Often the restoration of a single domain is necessary. This may be because of corrupt data, deletion of data, or if the site was copied to a new server.

Log into SmarterMail as the server administrator.

Add a new domain with the exact name previously used.

It is recommended that you now stop the SmarterMail Service in the MMC Services Snap In. The restore can be completed without stopping the service, but corruption may occur.

Restore/Copy that domain's folder into the domain directory (as listed in the above backup section).

Restart the SmarterMail Service in the MMC Services Snap In if it was stopped.

If the service was running when you restored the files, log into SmarterMail as the server administrator, search for the domain, and choose to Reload Domain. More information about the reload option can be found here.

Restore of a User or Mailbox: The restore of a user or mailbox has more nuances than other restores and requires a very high attention to detail.

Log into SmarterMail as the server or domain administrator.

Add a new user with the exact username previously used. The username must be exactly the same name as the folder that will be copied/restored.

It is recommended that you now stop the SmarterMail Service in the MMC Services Snap In. The restore can be completed without stopping the service, but corruption may occur.

Restore/Copy that user's folder into the applicable domain's user directory (C:\SmarterMail\Domains\ApplicableDomain.com\Users\).

Restart the SmarterMail Service in the MMC Services Snap In if it was stopped.

If the service was running when you restored the files, log into SmarterMail as the server administrator, search for the domain, and choose to Reload Domain. More information about the reload option can be found here.

Restore of a Single Message: Single messages can be restored as well. Follow the steps below to complete this action.

Restore/Copy the email into the appropriate folder. (C:\SmarterMail\Domains\YourDomain.com\Users\UserName\Inbox\)

Following this you will have to delete the Mailbox.CFG in the same folder. This is because the .CFG file contains a list of all files in the mailbox.

Note* After you remove this file, upon the next login SmarterMail will rebuild the CFG file and will mark all messages as read regardless of whether they were read prior to the deletion of the CFG file. This will also remove any marked for deletion status, and simply mark the mails as read.

Restoring a Folder or Message On Top of an Existing Folder: This can be done but does have several special considerations.

If at any point you copy or restore mails or folders on top of an existing setup it is likely that you will have orphaned emails or folders. An orphaned item is an item that is not recognized as attached or having a place by the software.

The config file in the folder/account may be from prior to the restore, or it may be from the restore. Either way the file may not know about the other messages or folders.

There are two ways to remove orphaned items.

If you do not need the orphaned items (for example if you did a full restore, then restored a newer differential on top of that) you can run the SmarterMail Mailbox Cleaner utility.

If you want to capture the ophaned items and re-attach them to the folder/user you will have to delete the Mailbox.CFG (for attaching messages in a folder) in the same folder or the root.cfg (for attaching folders) in the that users primary folder. . This is because the .CFG file contains a list of all files in the mailbox and all folders for that user. .

Note* After you remove this file, upon the next login SmarterMail will rebuild the CFG file and will mark all messages as read regardless of whether they were read prior to the deletion of the CFG file. This will also remove any marked for deletion status, and simply mark the mails as read.

End User Documentation

There are two different levels of users that can access the SmarterMail Web Interface: Administrators and End Users. Additionally, there is an end user with admin permissions for the domain that has specific privileges not granted to standard End Users.

A standard User is able to send and receive email and set configurations for their designated email account, so the creation of a standard User is perfect for people who want client side email.

End users with admin permissions for the domain are usually the owner of a domain who can add/remove email accounts and change domain settings.

Mailbox

The mailbox consists of all folders pertaining to one email account. It is the first item of the main menu as it is the item accessed most by email users. Under this menu item you will find View All Folders, Add New Folder, Inbox and Sent Items. From any box or folder, use the drop down lists at the top of the table to change the state of the message or move it to a different folder.

View All Folders

This is the first page of an email account when accessing it from the Web Interface. The window will display all folders including, but not limited to, the inbox, sent items and deleted items.

The beginning text informs the user about the current amount of allotted disk space being used (including percentage).

The "Search" option allows a user to search for certain criteria among all of the emails in the mailbox, regardless of the folders mail is stored in. Simply enter the search text and select, from the drop down list, which part of the message you would like to perform the search upon (subject, from address or message body) and click on the "Search" button.

To the right of each box or folder are a few options and various information.

Unread Messages: A total of the unread messages contained in that folder.

Total Messages: The total number of messages contained in that folder

Size: The total size (in kilobytes) of all messages contained in that folder.

Rename: Click on "rename" to enter a different name for the specific folder

Delete: Click on delete to erase the specific folder.

* Please Note: When deleting a particular folder, you will delete all mail messages stored within that folder. Therefore, please be sure you want to delete the folder prior to pressing the "delete" link.

The first time a message is sent from an account, a "Sent" folder will become available (provided it is enabled by the administrator) that will hold all of your sent items for future review.

Also, the first time a message is deleted, a deleted items folder will be created (assuming you have the 'Move {Deleted Messages}to Deleted Items Folder' selected in your settings).

Add New Folder

There will come times that you will want, or need, to add a folder to help sort your incoming email. For example, you may want a folder for questionable spam, to help organize your regular inbox. You simply create a folder named "spam" then, when used in conjunction with "my content filtering", instruct the wizard to put messages that may be spam into the spam folder.

To add a folder to your mail account, select Add New Folder from the main "mailbox" menu item. Enter the name of your new folder and click the "ok" button to confirm creation. Only standard characters (0-255) are currently supported in the folder name.

Please Note: In order for the folders you create to become available from your email client (e.g. Microsoft Outlook) you will need to create a mail account with IMAP set as your incoming mail server type. If you use POP mail, you only have access to your mail account Inbox, not any folders that are created for storing mail. IMAP accounts are different that POP because they are directly connected to the server from the time you open an interface until the time it is closed. Fot this reason, deleted messages will are crossed out untill they are purged from the folder. This is different from POP account, when the messages are deleted, it is gone from the folder or erased.

Inbox

Your Inbox is exactly that: a repository for all mail that your email account receives. Unless you have filters set up for moving mail to specific folders, all incoming mail will show up when you access your inbox.

Sent Items

From the main menu item, "mailbox" select "Sent Items" to open the list of messages you have sent. You can also access the Sent Items by clicking on the Sent Items folder from the default Web Interface welcome page named, "View All Folders."

The "sent items" list has all of the actions and options, and shows all of the same information, as the Inbox.

Inbox, or any mail box/folder

An infinite number of folders can be added, depending on your needs.

From the top of the table under the folder name from left to right there are options for each message selected:

Actions drop down list:

- Delete: In an IMAP dient and server environment, the delete function will cross out the message making it available to read.
- Undelete: This function will uncross a deleted message.

- Mark as Unread: When a new message comes into the mailbox, the message will have red text next to it that reads "unread". After reading a message this test will disappear. To put the text message back, select "mark as unread."
- Mark as Read: This option will remove the red text by a new message that reads "unread."
- Purge Deleted Items: This function will permanently remove all deleted messages, or those that are crossed out. There is no undo for this option.

Click on the "do action" button to complete action.

"Put in folder" drop down list: Options in this list will allow a user to move messages to different folders:

Items in this list will appear as they are added with "add new folder" under the "mailbox" option in the main menu.

Click on the "move" button to complete the moving process.

"select all" button: Click this button to select all of the messages in the folder at one time to perform an action on them or move them.

"deselect all" button" Click this button to deselect all messages previously selected.

Read Message Window

The Read Message allows users to read, respond, delete, and take a variety of other actions on the messages in their folders.

Users have access to a variety of buttons and options to take different action.

- Back to 'Folder': This button will take the user back to the folder they were in prior to reading the message.
- Go to...: This pull down menu will allow you to navigate to other areas without taking action regarding the message being read.
- Reply: This button will take users to a Compose Window. The email address the read message was sent from will already be filled in the To: field, and the original message is included in the compose window.
- Reply to all: This button is similar to the Reply button, except that all other recipients in the To:, and Cc fields of the received message will be addressed in the To: field as well.
- Forward as text: This option will take users to a Compose Window and allows users to forward the read message on as plain text already filled out in the compose window.
- Forward as attachment: This option allows users to forward the read message on as an attachment. This can be especially useful if the original message was sent as HTML, or Rich Text.
- Delete: This option allows users to delete the message from the read window. After deleting the current message the next email in the folder will then be displayed in the read window.
- Next: Clicking this button will cause the next email in the folder to be displayed in the read window.

- Printer Friendly: This option will bring up a separate window with a printer friendly (text only) version of the read window.
- Show Header: This will open a separate window to display the header of the email.
- Add to Contacts: This option will allow you to select any or all of the email addresses contained in the From, To, or CC fields to your address book.

Following the above action buttons is information about the email, and the actual content of the email.

- From: This is the email address the message was sent from.
- To: The primary recipients' email address.
- Cc: This field shows carbon copied email addresses
- Subject: The subject of the email.
- Attachments: This will show any attachments sent with the email.
- Sent: Time and date the message was sent.
- Message size: Size of the message in kilobytes.
- Message body: The body of the message.

Address Book

The address book is where you can not only keep the email addresses of all of your important contacts, but all of their other professional information as well. All contact information, like all features of SmarterMail, is accessible through the Web Interface from anywhere on the Internet enabling an online address book. Up to ten contacts will appear at the bottom of this menu drop down list after they are added in "Add New Contact" as a favorites.

View Contacts

This page displays all contacts by name with the ability to edit or delete each contact. At the top of the list is a search field where you can enter content to find a contact by name or email address.

Add New Contact

Select "Add New Contact" from the "Address Book" in the main menu and enter information about contacts. Enter information for:

- Name
- Email Address
- Personal Web Site
- Birth Date
- Add to Favorites (check box), checking this box will add the user to the main menu drop down under "address book", up to ten individual contacts.
- Home, work and mobile phone number
- Home Address
- Company Name
- Title/Position
- Company Address

- Country

Config Settings

The Config items are where End Users can configure the how email accounts interact with messages. An end user has an account which consists of an email address and a password. The end user uses the account information to log into an interface and view their mailboxes or folders.

User Admin

The user administration page is accessible by administrators and end users with admin permissions. This is where end user accounts can be added, edited, deleted and configured.

End users with Admin permissions can easily add and delete email accounts for a particular domain. To delete a user, highlight the account and push the "delete" button.

Add/Edit User

Click on the "Add" or "Edit" button.

Username: The email address (e.g. "user" in user@domain.com).

First Name: Enter the first name of the person using the email account.

Last Name: Enter the last name of the person using the email account.

Password: Enter a password for the email account

Confirm Password: Confirms the above password

Lock Password: This option 'locks' the password for end users. If this option is checked the user will not be able to change their password.

Disable User: This will completely disable this user. The user will not be able to log in, send or recieve email for this account.

Domain Administrator: If this option is checked, the user will have domain administrator provides.

Header Display on reply: The header is the information about a reply, appended to the top of an email. Select an option in the drop down list:

Full: Display all information about a message (e.g. SMTPSVC, thread-index, Content-Class, etc.).

Basic: A limited list about the information about a message (e.g. To, From, Subject and Date).

Sort Messages by: When viewing web mail, sort the list of messages in the current directory from top to bottom according to one of the following: To, From, Subject, Size or Date.

Check the "descending" box to switch the sorted order of the list from bottom to top

Sort Folders by: When viewing all folders (including the default entry page), sort the folders from top to bottom according to one of the following: Name, Unread Messages, Total Messages, or Size.

Check the "descending" box to switch the sorted order from bottom to top

Messages List Refresh Rate: Selecting this option will cause a refresh of the message list as the specified interval.

When Messages are Deleted: This pull down menu will allow you to select what action is taken when a mail is deleted.

Move to Deleted Items Folder: When items are deleted they are moved to a folder named Deleted Items. This folder is automatically create the first time an item is deleted and this option is selected.

Auto Purge Folder: When messages are deleted from the inbox, they need to be purged before they are completely removed. This option foregoes the second step by purging the message as soon as you delete the message.

*Note: When messages are purged, the action is final. You will not be able to retrieve these messages later.

Mark as Deleted: When the message is deleted with this option, the message remains in the current folder, but will be crossed out as deleted. If the folder is then purged all items marked for deletion will be removed.

Hide Deleted Messages: Any message that has been marked as deleted, will be hidden. This will allow you to keep deleted messages, without seeing them every time you log into your mailbox.

When Messages are Deleted: This pull down menu will allow you to select what action is taken when a mail is deleted.

Move to Deleted Items Folder: When items are deleted they are moved to a folder named Deleted Items. This folder is automatically create the first time an item is deleted and this option is selected.

Auto Purge Folder: When messages are deleted from the inbox, they need to be purged before they are completely removed. This option foregoes the second step by purging the message as soon as you delete the message.

*Note: When messages are purged, the action is final. You will not be able to retrieve these messages later.

Mark as Deleted: When the message is deleted with this option, the message remains in the current folder, but will be crossed out as deleted. If the folder is then purged all items marked for deletion will be removed.

Hide Deleted Messages: Any message that has been marked as deleted, will be hidden. This will allow you to keep deleted messages, without seeing them every time you log into your mailbox.

Messages Per Page: Select how many messages to be displayed per page.

Reply message indicator: This allows you to select the symbol that will appear before each line of the message you are replying to.

Embed Replies: When viewing web mail, check this box to include all previous replies when replying.

Save Copy as Sent: When viewing web mail, check this box to save sent messages in the sent folder for later retrieval.

Reply-to Address: Enter an alternate reply address you wish to use. This will be the default reply to address for mail sent from this account.

Forwarding Address: Enter an address to forward every inbound email message to. For example, if your mobile phone has an email account and you will be away from your computer for a few days, enter the mobile phones email address here to receive the messages sent to the original address. You can only forward to a single email address. If you need to send to multiple addresses, you must use an alias.

Delete Messages on Forward: Check this box to delete the message from the inbox of the original email account after forwarding it to the new email address.

Mailbox Size This is a setting to specify the maximum mailbox size in MegaBytes for the user you are creating.

Signature: Add text to this area that will display at the bottom of each composed email message.

Click the "Save" button to complete the changes.

Alias Administration

The Alias Administration page allows the creation of aliases for a domain. Aliases are simply email addresses that forward messages to the list of emails provided for that alias. Even though an alias acts as an email address, users cannot login to an alias like they do a standard email address as no email is ever actually stored for the alias, it is just sent to the list of addresses provided for the alias. For example, in a working environment with multiple email addresses, the office may want to make a central email address that distributes messages to all personnel. The alias workplace@yourDomain.com can be made for messages to be sent and then distributed to all of the employees.

Catch All Alias

The "toggle catch all" button will enable the selected alias email address to receive all mail associated with the domain that does not have an assigned user name. The alias you are pointing to needs to be created prior to clicking the 'toogle catch all'.

Click on the "add", "edit" or "delete" button to administer aliases.

Under "Alias Name" enter the name only, excluding the domain (e.g. just the "name" in name@domain.com)

Enter one original email address per line

Domain Alias Administration

A Domain Alias is an additional email address, using an additional domain name, that points to an existing email account on the server.

For example, a full email addresses requires a user name at a domain name: test@domain.com. If you add a domain alias of "a-new-domain.com" then not only will "test@domain.com" be valid, but the same mailbox will also work with the "test@a-new-domain.com". If an email was sent to both domains/emails then the "test" mailbox would get two copies of the emails. A user cannot log into the Web Interface under a domain alias, just the original domain, nor can a user send an email from the domain alias. Remember, any alias is simply an additional email address that points to an existing email account on the server.

Notes:

Messages cannot be retrieved with a domain alias email address unless the domain is properly registered at a domain registrar.

The mail exchange (MX) record for the domain being added must already be pointing at the server prior to this process. This prevents users from 'hijacking' mail from valid domains. For example if this check were not in place a user could add a domain alias of SmarterTools.com. Then, any mail sent from the server to Anything@SmarterTools.com would go to the domain with the SmarterTools.com domain alias, rather than to the actual domain.

Domain Spam Admin

End users with Admin permissions have the ability to add, delete and edit Spam checks that are provided by the administrator. After assigning a weight to a spam check according to its validity and competency, the weight is bound to the spam check for end users. Adding spam checks here does not delete or filter messages until they are activated in "content filtering."

To delete a spam check, highlight the spam check and click the button "delete."

Add/Edit Spam

Each individual spam check is assigned a weight, or numerical value. When a message qualifies for a spam check, its associated weight is tallied and the total is compared to the configurations in "Content Filtering" for an action to take place. Domain admins can access "Domain Content Filtering" under "Config" in the main menu. End User's can access "My Content Filtering" under "Config" in the main menu. The weight system gives End Users the ability to have the highest level of spam protection while decreasing the possibility of lost messages.

Spam "Short Name": From the drop down list, select "Reverse DNS Lookup", "Verify Sender", these and other options are made available by the Administrator.

Reverse DNS Lookup: Verifies the domain of the sender by resolving its IP address (checks the address).

Verify Sender: Authenticates that the email account exists with the sender's mail server. If the mail server is down or unavailable at the time, it will not authenticate the email and the message might not reach its final destination.

Other options available are Domain Name Servers that hold lists of known spam mail servers and domains. When these spam checks are selected, it gives End Users the opportunity to filter their received email with these lists of spam mail servers.

This list can be modified by the Administrator

Weight: Assign a numerical value to the Spam Check. When an email qualifies for a particular spam check, the assigned value will be added to the spam weight of the email message. If the accumulative spam weight of the email message is equal to or greater than a numerical value that you set for the spam rule in "Content Filtering", it will be moved to a customized folder or deleted, which ever action the End User configures.

Domain Statistics

Select the date range for the report that you would like to see statistics on.

The Domain Statistics page allows you an overview of usage by user. This information can be used to see abuse or usage trends for particular users or for the domain in general. In some cases, the end user with admin permissions for the domain can use this information to bill customers for excessive usage. All statistics are totals for the date range specified. Statistics are also made available through Web Services that open up some Internet code from SmarterMail enabling easy implementation into existing applications. To see more on this ability, see Web Services in the Administrator section of the help.

From left to right, the statistical table details are as follows:

- Email address: The email account list for the domain.
- Bytes Received: The bandwidth in KiloBytes accumulated from incoming email messages, reguardless of content filtering.
- Bytes Sent: The bandwidth accumulated from the outgoing email messages.
- Messages Received: A numerical count from the incoming email messages, reguardless of content filtering.
- Messages Sent: A numerical count of the outgoing email messages
- Space Used: The total size in KiloBytes of email messages and their attachments that is on the mail server.

Notes About Domain Statistics

Email address that come in through aliases then forwarded to a local user will not show up as incoming for that user, but rather as incoming under the Alias Statistics.

Emails using the catch-all (I.E. invalid email addresses) will be displayed under the Other Statistics Section.

Email accounts with forwarding will show the forwarded mails as Sent Messages.

Domain Content Filtering

From this page you can configure content filtering for all emails that are destined for your domain. An unlimited number of filters can be created with different actions allowing users to organize their emails or in an attempt to eliminate spam.

Be aware, this will filter emails prior to being sent to the user's mailbox. Since users can configure their own content filtering, you may want to minimize the loss of emails at the domain level, eliminating or filtering only items that affect the entire domain.

Content filtering allows an End User to define exactly what passes through the mail server and into the mailbox. As soon as any filter is triggered, the mail takes the designated action, no other filters will be checked for that mail.

To delete a filter, highlight the filter name and click the "delete" button.

Click the "add" button to start the filter wizard

For each rule type, continue through step 3, and then start another rule type. Add an unlimited amount of rule types using this method. There are eight different rule types available to build filters for: Subject, From Address, Body Text, To Address, Sender, Header Text, Sending Server IP and Spam:

Rule Type: From the drop down list, select which part of the email you would like to build a filter for and click the "next" button:

*Regardless of what rule type you choose, the final three steps are the same, except for the Spam filter.

Subject: Define a filter for the subject line of an incoming message.

From Address: Define a filter for the senders Address of an incoming message.

Body Text: Define a filter for the body of an incoming message.

To Address: Define a filter for an incoming message for who it is addressed to.

Sender: Define a filter for the return path of an incoming message. The Sender can contain more information that just the From Address dependant upon each mail server (e.g. the date).

Header Text: Define a filter for the header text of an incoming message. This will apply to everything in the header including but not limited to subject, from address, to address, etc.

Sending Server IP: Define a filter for the IP address of a mail server from an incoming message.

Search String: Enter the text to include in the filter and Click the "next" button.

Condition: Append a condition to the subject to further define your filter:

Contains: When the search string is found anywhere in the subject

Begins With: When the search string starts with the subject

Ends With: When the search string is at the end of the subject

Equals: When the search string is exactly the subject, no more and no less

Doesn't Equal: When the search string is not exactly the subject, any disqualifying character will set this condition true.

Click the "next" button

Action:

Delete Message: This action will erase an email message completely

Forward Message: This action will send the email message to a different mail box

Enter an email address

Bounce Message to Sender: This action will send the email message back the original sender

Move to Folder: This option is only available at the end user level. Select the folder in which to send spam messages to.

click the "finish" button

Spam: Spam checking filters by weight. The weight is a value assigned to a spam check according to its validity and competency. In the "Current domain spam weights" table, is a list of Spam Checks and their respective weights, made available by the Administrator. When an email qualifies for a particular spam check, its weight is added to the email message. For example, a message qualifies for the spam check "Reverse Dns Lookup". The weight for "Reverse Dns Lookup" is 10, which is added to the message. The same message also qualifies for the spam check "Verify Sender". The weight for "Verify Sender" is 10, which is added to the message. Now the total weight of the message is 20.

Enter the accumulative spam weight that an email message must obtain to take an action:

Action:

Delete Message: This action will erase an email message completely

Forward Message: This action will send the email message to a different mail box

Enter an email address

Move to Folder: This option is only available at the end user level. Select the folder in which to send spam messages to.

Click the "finish" button

Mail List Administration

From this page you can add/ delete/ manage your Mailing Lists. Mailing lists allow communications among many users through email. This feature is only accessible to administrators and end users with admin permissions.

Add

This area shows the list name, moderator selected for that list, and a breif description of the list. It also has a menu to the different options available to you to administer the list. To navigate to the various options available in the list administration, pull down the menu on the right had side and select the option you want. Then press the 'go' button to change to that page.

Edit Mail List

From this page you can control all the general settings for your Mailing Lists. Many of these settings can help reduce abuse or control how your users will interact with your list.

List name: This will be the name of the list as well as the email address that emails will be sent to and from.

List moderator: This is the 'owner' of the list; the email address at your domain that will be the moderator of the list.

Description: This is for internal identification purposes only.

Post options: Mail that is sent to a list and then resent to the list recipients is considered to be posted. In this field you will determine who can post to the list. In addition to the selected post option, you can enable the posters list. That list would be in addition to the group you select here.

Anyone: Setting the list to anyone means that when anyone sends an email to the list, it will be sent out to all members. This setting can cause abuse if it is not closely monitored.

Subscribers only: Setting the list to subscribers only allows the list subscribers to send and receive posts.

Moderator only: If the moderator is set as the post option, only the moderator will be able to post to the list

Reply to list: When this option is checked, replies from a subscriber go to the list. If this option is off, the reply goes to the person who posted the message on the list.

Disable list command: This disables the ability for someone to send a mail to the list and receive a reply of all list users.

Disable subscriptions: This disables the ability for users to subscribe to the list via a subscribe email. This normally used on a list that is intended to be kept private. Only the moderator will be able to add subscribers.

Enable digest mode: This enables digest mode. When using digest, the server stores all posts to the list in a set folder. When the 'trigger' is set off, all accumulated posts are sent out as a single message.

Enable posters list. In addition to the post options you can also enable the posters list. This will allow anyone on the posters list to post to the list as well.

Enable subject prefix: With this option enabled you will be able to have a prefix in the subject of every post that is sent out.

Subject prefix: This is where you actually enter the subject prefix you want for all list posts.

Enable password: Posting on a list can also be restricted by requiring a password. To post to a list that is password protected you must send the password in the subject enclosed by brackets and colons (e.g. Subject: [:password:] Attention all subscribers).

Enable header: When selected, you can include a header with every list post.

Enable footer: When selected, you can include a footer with every list post.

Allow unsubscribe from subject: If you want to allow user to unsubscribe by replying to the list with Unsubscribe in the subject line, this option needs to be checked. Keeping this option checked will also help with abuse complaints, as users can easily unsubscribe themselves.

Max message size: The maximum size (in bytes) of a message that can be posted to the list. For Unlimited size, enter 0.

Max recipients per message: This is the number of recipients per message sent out. For example, if there were 500 subscribers to a list, and the max recipients was set to 100, 5 emails (each with 100 recipients) would be sent out. This setting can affect the load on the server.

Digest Settings

If you have enabled Digest Mode for your Mailing List, the users will be allowed to subscribe to the list with the digest mode option

You can specify which users are receiving the list as a digest by setting them up in digest subscribers vs. standard subscribers. When using digest, the server stores all posts to the list in a set folder. When the 'trigger' is set off, all accumulated posts are sent out as a single message.

Changing these settings will allow you to control how digest mode will operate for these subscribers.

List name: This is simply the list name you are currently working on.

Digest Folder Size: This is the current size (in Kilobytes) of the digest folder, and all posts.

Last send date: This is the last date that the digest was sent out.

Next send date: This is the next date the digest is scheduled to be sent out.

*Note: This option may or may not be displayed, depending on what trigger you have selected.

Send trigger type: These are the various 'triggers' you can use to send out the digest.

Send Now: You can send the list at any time by clicking the send now button. This will clear the digest folder as if it had been triggered by the selected option. You will need to use this if you select the Manual option for trigger.

Subject: Due to many list posts being sent out at once, and that they all may have different subjects, you can specify a subject for the digest here.

Strip non-text attachments: Digests can be much larger than standard lists, for this reason you may want to minimize the actual sending size of the digest by removing non-text attachments.

User header: This is a header that will precede the digest. There will only be one header at the begriming of the digest.

User separator: This will allow you to separate each post sent out in the digest with text.

Use trailer: This is a footer that will end the digest. There will only be one trailer at the very end of the digest.

Edit Header
This is where you can add the header for list posts. The text entered here will be added to the top of every message before it is sent to the subscribers. This does not get added to the digest, it has its own header.

Edit Footer
This is where you can add the footer for list posts. The text entered here will be added to the bottom of every message before it is sent to the subscribers. This does not get added to the digest, it has its own footer.

Edit Digest Header
This is where you can add the header for the digest when it is sent out. The text entered here will be added only to the top of the digest message before it is sent to the subscribers. This does not alter or get added to the regular list posts, lists have their own header.

Edit Digest Footer
This is where you can add the footer for the digest when it is sent out. The text entered here will be added only to the bottom of the digest message before it is sent to the subscribers. This does not alter or get added to the regular list posts, lists have their own footer.

Edit Digest Separator
The digest separator is placed in between every post that is included when the digest is sent out. Enter the text here that you want to separate each post in the digest.

Edit Subscribe File

When a user successfully subscribes to your list, this text will be sent. Often this is used to welcome them to the list and what rules they should follow.

Simply type the message you would like to use in the text box, and click the save button in the upper right.

Edit Help File

When people fail to subscribe properly or they do not post messages properly a response will be sent to view the help. From this page you will be able to edit the help file that is sent. The standard help file is listed below.

Kill List Management

To help aid in controlling which people can/can not subscribe your list, you can add email addresses in the kill list. These are the addresses you do not want to be able to subscribe to the list.

You can add email addresses individually, or you can upload an entire list of email address using the 'upload list file' option.

Any list you want to upload needs to be a simple text file. It must be formatted with a single email address per line, with no extra characters. For example

Bob@DomainName1.com

John@DomainName2.com

Jane@DomainName3.net

etc.

Poster List Management

If you have enabled "use poster list" on the general settings page for the list, only email addresses in this list and the group you selected as posters will be allowed to post messages to the list.

Subscriber List Management

This is a list of subscribers to your list. This page includes email addresses who have subscribed to the list or emails addresses that were added by the administrator. This list does not include individuals that subscribe to the list in digest mode, those users are on the Digest Subscriber List.

You can add email addresses individually, or you can upload an entire list of email address using the 'upload list file' option.

Digest Subscriber List Management

This is a list of subscribers to your list who wish to use digest mode . This page includes email addresses who have subscribed to the list or emails addresses that were added by the administrator. This list does not include individuals that subscribe to the standard list , those users are on the Subscriber List.

You can add email addresses individually, or you can upload an entire list of email address using the 'upload list file' option.

Mail List Deletion

This page allows you to delete the list you have selected. Deleting a list is a permanent operation. Be sure you understand the implications of performing this operation before you do so. If you choose to delete the list, all files associated with the list will be deleted as well.

My Settings

These settings will affect how SmarterMail behaves when you are logged in via Web Interface.

Username: The email address (e.g. "user" in user@domain.com).

First Name: Enter the first name of the person using the email account.

Last Name: Enter the last name of the person using the email account.

Password: Enter a password for the email account

Change: If a user has permissions to change their password, the Change button will appear on this line as well. Pressing this button will allow a user to type a new password, and confirm password. Save must be pressed before the password will be changed.

Header Display on reply: The header is the information about a reply, appended to the top of an email. Select an option in the drop down list:

Full: Display all information about a message (e.g. SMTPSVC, thread-index, Content-Class, etc.).

Basic: A limited list about the information about a message (e.g. To, From, Subject and Date).

Sort Messages by: When viewing web mail, sort the list of messages in the current directory from top to bottom according to one of the following: To, From, Subject, Size or Date.

Check the "descending" box to switch the sorted order of the list from bottom to top

Sort Folders by: When viewing all folders (including the default entry page), sort the folders from top to bottom according to one of the following: Name, Unread Messages, Total Messages, or Size.

Check the "descending" box to switch the sorted order from bottom to top

Message List Refresh Rate: Selecting this option will cause a refresh of the message list as the specified interval.

When Messages are Deleted: This pull down menu will allow you to select what action is taken when a mail is deleted.

Move to Deleted Items Folder: When items are deleted they are moved to a folder named Deleted Items. This folder is automatically create the first time an item is deleted and this option is selected.

Auto Purge Folder: When messages are deleted from the inbox, they need to be purged before they are completely removed. This option foregoes the second step by purging the message as soon as you delete the message.

*Note: When messages are purged, the action is final. You will not be able to retrieve these messages later.

Mark as Deleted: When the message is deleted with this option, the message remains in the current folder, but will be crossed out as deleted. If the folder is then purged all items marked for deletion will be removed.

Hide Deleted Messages: Any message that has been marked as deleted, will be hidden. This will allow you to keep deleted messages, without seeing them every time you log into your mailbox.

Messages per Page: When viewing web mail, customize how many messages display per page or window.

Reply message indicator: This allows you to select the symbol that will appear before each line of the message you are replying to.

Embed Replies: When viewing web mail, check this box to include all previous replies when replying.

Hide Deleted Messages: Any message that has been marked as deleted, will be hidden. This will allow you to keep deleted messages, without seeing them every time you log into your mailbox.

Save Copy as Sent: When viewing web mail, check this box to save sent messages in the sent folder for later retrieval.

Reply-to Address: Enter an alternate reply address you wish to use. This will be the default reply to address for mail sent from this account.

Forwarding Address: Enter an address to forward every inbound email message to. For example, if your mobile phone has an email account and you will be away from your computer for a few days, enter the mobile phones email address here to receive the messages sent to the original address. You can only forward to a single email address. If you need to send to multiple addresses, you must use an alias.

Delete Messages on Forward: Check this box to delete the message from the inbox of the original email account after forwarding it to the new email address.

Signature: Add text to this area for a 'signature' that will display at the bottom of each composed email message.

Click the "save" button to complete the changes.

My Statistics

Select the date range for the report that you woule like to see statistics on.

The My Statistics page allows you to view your mail usage. This information can be used to see usage trends. In some cases, you can use this information to stay under any limits that may be imposed by a service provider. All statistics are totals for the date range specified.

From left to right, the statistical table details are as follows:

Received Messages: A numerical count from the incoming email messages, reguardless of content filtering.

Sent Messages: A numerical count of the outgoing email messages

Bandwidth Received: The bandwidth in KiloBytes accumulated from incoming email messages, reguardless of content filtering.

Bandwidth Sent: The bandwidth accumulated from the outgoing email messages.

My Content Filtering

Content filtering allows an End User to define exactly what passes through the mail server and into the mailbox. As soon as any filter is triggered, the mail takes the designated action, no other filters will be checked for that mail.

To delete a filter, highlight the filter name and click the "delete" button.

Click the "add" button to start the filter wizard

For each rule type, continue through step 3, and then start another rule type. Add an unlimited amount of rule types using this method. There are eight different rule types available to build filters for: Subject, From Address, Body Text, To Address, Sender, Header Text, Sending Server IP and Spam:

Rule Type: From the drop down list, select which part of the email you would like to build a filter for and click the "next" button:

*Regardless of what rule type you choose, the final three steps are the same, except for the Spam filter.

Subject: Define a filter for the subject line of an incoming message.

From Address: Define a filter for the senders Address of an incoming message.

Body Text: Define a filter for the body of an incoming message.

To Address: Define a filter for an incoming message for who it is addressed to.

Sender: Define a filter for the return path of an incoming message. The Sender can contain more information that just the From Address dependant upon each mail server (e.g. the date).

Header Text: Define a filter for the header text of an incoming message. This will apply to everything in the header including but not limited to subject, from address, to address, etc.

Sending Server IP: Define a filter for the IP address of a mail server from an incoming message.

Search String: Enter the text to include in the filter and Click the "next" button.

Condition: Append a condition to the subject to further define your filter:

Contains: When the search string is found anywhere in the subject

Begins With: When the search string starts with the subject

Ends With: When the search string is at the end of the subject

Equals: When the search string is exactly the subject, no more and no less

Doesn't Equal: When the search string is not exactly the subject, any disqualifying character will set this condition true.

Click the "next" button

Action:

Delete Message: This action will erase an email message completely

Forward Message: This action will send the email message to a different mail box

Enter an email address

Bounce Message to Sender: This action will send the email message back the original sender

Move to Folder: This option is only available at the end user level. Select the folder in which to send spam messages to.

click the "finish" button

Spam: Spam checking filters by weight. The weight is a value assigned to a spam check according to its validity and competency. In the "Current domain spam weights" table, is a list of Spam Checks and their respective weights, made available by the Administrator. When an email qualifies for a particular spam check, its weight is added to the email message. For example, a message qualifies for the spam check "Reverse Dns Lookup". The weight for "Reverse Dns Lookup" is 10, which is added to the message. The same message also qualifies for the spam check "Verify Sender". The weight for "Verify Sender" is 10, which is added to the message. Now the total weight of the message is 20.

Enter the accumulative spam weight that an email message must obtain to take an action:

Action:

Delete Message: This action will erase an email message completely

Forward Message: This action will send the email message to a different mail box

Enter an email address

Move to Folder: This option is only available at the end user level. Select the folder in which to send spam messages to.

Click the "finish" button

My Auto Responder

The auto responder will immediately send a pre-composed response automatically to the sender of a message that arrives in your mailbox.

Enable Auto Responder: Click the check box on top to enable the Auto Responder.

Subject: Enter a subject for the auto response (e.g. Vacation).

Body: Enter a body, or text that you would like to include in the automatic response, for example, "I am on vacation in Hawaii, and will not have access to a computer until Monday."

Limit Responses: This will limit the auto responder to only sending out one auto response per day for each sender of a message that arrives in your mailbox.

Click on the "save" button to activate and finish an auto response.

Compose Message

Select "Compose Message" from the main menu to write an email.

From: This field is pre-filled with your email address.

Reply to: Using this field you can specify an alternate email address for recipients to respond to.

To: Enter a recipient's email address, or click the 'To:' on the left of this field to select from a list of your contacts.

CC: Enter a recipient's email address, or click the 'CC:' on the left of this field to select from a list of your contacts.

BCC: Enter a hidden recipient's email address, or click the 'BCC:' on the left of this field to select from a list of your contacts.

Subject: Enter the main subject of your composed message.

Attachments: Beside this text will appear your attachments. Click on 'Attachments' to add files to this message.

Enter the path to the file that you would like to send with the message or click on the browse button to navigate to the file.

Click on the "upload" button to confirm attachment.

The attachment will display in the large white text area for approval.

If you do not want to send attached file with the message, highlight the attachment from the large text window and click the "delete" button.

Click on the "ok" button to finalize attachment.

Check Spelling: This option will open an additional java-script window to check your spelling.

Compose Area: The Compose Area menu will allow you to change the size of the compose window to suit your needs and preferences. This setting will automatically be stored for future reference.

Send Message:Click on the "send message" button at the bottom of the compose window to send.

Sample Spam Scenario

A server administrator can add Spam Mail DNS Servers (also known as Spam Lists) under Config/Spam List Administration. For example, the server administrator might add 2 Spam Mail DNS Servers (SpamCop and ORDB).

These will now be available for the domain administrator under the Domain Spam Administration Link. The domain administrator can add these servers and assign weights to each list. Any weight can be assigned to each lookup, for this example we will use a weight of 10 for each.

The domain administrator then sets up Domain Content Filtering so that if the Spam Weight of an incoming email was greater than to or equal to 20 (meaning the incoming mail was from a sender that is listed on at least 2 different spam lists, where each list has a weight of '10' assigned), the mail is deleted or forwards to a "spam" address for that domain.

Finally, an end user could set their filters (found in My Content Filtering) so the spam filter weight is equal to 10, to tighten the filter. Then, any emails failing the spam weight test (in this case, meaning the incoming mail was from a sender on only one of the spam lists) forwards to a folder in their account, so they could check the emails briefly before deletion.

List Serv Commands

The List Serv in SmarterMail can be controlled through email by sending a variety of commands to the List Serv command address.

Any commands need to be sent to the List Serv command address in the subject of the email.

By default commands are sent to STServ@'YourDomain.com'. The List Serv command address can be changed by the server administrator under Manage Domain/ Domain Limits/ Mail List Command Address.

All commands should be sent to the command address in the message body.

Commands:

Any references to "listname" should be replaced with the list you are trying to use.

- Help
- Help listname
- List
- List listname
- Subscribe listname
- Unsubscribe listname
- Set mode digest listname
- Set mode standard listname

Command descriptions:

Using the "Help" command without a list name will reply with this email.

Using the "Help listname" command will reply with help associated to that list name

Using the "List" command without a list name will show all lists available.

Using the "List listname" command will return all subscribers for that list. This can be disabled by the moderator.

Using the "Subscribe listname" command will subscribe you to the list. This could be disabled if it is a private list.

Using the "Unsubscribe listname" command will unsubscribe you from the list you provided.

Using the "Set mode digest listname" command will send all messages from lists within one file based on an interval by the moderator.

Using the "Set mode standard listname" command will send all messages individually and is the standard option.

Glossary

Below is an alphabetized list of the various terms and phrases used in describing a Mail Server package.

Administrator - The person or company that purchased and installed SmarterMail Professional Edition on a server with abilities to set global configurations and create and delete email domains and end users.

Account - An account consists of an email address and a password, used to log into a mail server to retrieve or send mail.

Alias - An email address representing another address that only forwards received mail to another address or group of addresses. For example, if your email address is you@yourDomain.com and you wanted to make an account for purchases without actually having separate inboxes to check, simply create the email Alias purchases@yourdomain.com and the mail for purchases will be redirected to your original mailbox.

APOP - APOP stands for Authenticated Post Office Protocol. Every mail connection made sends your username and password across the network in clear text (no encryption). With APOP, your password is encrypted while being transmitted over the Internet.

Auto Responder - A preconfigured message immediately sent back to anyone you receive an email from.

Black List - Block email from email addresses and domains added to this list.

Content Filtering - This filter allows a user to search incoming messages for certain words or string of words to either delete, so it never reaches its final destination, or move to a separate folder away from the main inbox.

Domain - A domain is the name associated with the last half of an email address, it resides after the @ symbol. (e.g. in support@smartertools.com, smartertools.com is the domain.)

Domain Admin - The owner of a particular domain responsible for adding and deleting email accounts and setting configurations associated with that domain.

Domain Alias - An additional domain that forwards received mail to another address or group of addresses. For example, you may have two email addresses with different domain names, to combine their inboxes, add one email address to the Domain Alias List.

Domain Name Server (DNS) - A Domain Name Server is a computer designated to holding a list of domain names and their corresponding IP addresses. For the purposes of SmarterMail, some Domain Name Servers hold a list of domain names and IP addresses associated with mass spam mail outs. SmarterMail makes it possible for Administrators to enter the URL and take advantage of these Domain Name Servers to filter out mail from known spammers.

End User - A person who uses SmarterMail to send and receive mail, or to manage a domain consisting of other end user email accounts.

Forward - To redirect a received email to another email address.

IMAP / IMAP4 - Internet Message Access Protocol (IMAP) is a standard protocol for accessing e-mail from your local server. IMAP (the latest version is IMAP4) is a client/server protocol in which e-mail is received and held for you by your Internet server. IMAP requires continual access to the server during the time that you are working with your mail.

IP - Internet Protocol address is the numeric physical address of any computer. Therefore, you can access a computer by entering either the domain name or the IP address for the domain (e.g. 127.0.0.1).

IP Bypass - Pardon IP addresses from SMTP authentication enabled on any domain. This is often used to allow clients who have applications that do not support SMTP authentication to bypass this check.

IP4R - A DNS lookup that attempts to determine if a mail server is likely to be sending spam. You take the IP address of the mail server, turn it around, and query a "DNS zone", to come up with something like "2.0.0.127.relays.example.com". If the mail server is listed in the spam database you queried, it will return an answer indicating that the mail server is listed.

Killlist - A list of domains that are denied access to the mail server.

List Server - A list server (mailing list server) is a program, or a feature in a program, that handles subscription requests for a mailing list and distributes new messages, newsletters, or other postings from the list's members to the entire list of subscribers as they occur or are scheduled. (A list server should not be confused with a mail server, which handles incoming and outgoing e-mail for Internet users.)

Mailbox - A folder that contains messages.

Mail List - A mailing list is a list of people who subscribe to a periodic mailing distribution on a particular topic. Mailing lists include each person's e-mail address. Mailing lists have become a popular way for Internet users to keep up with topics they're interested in. Many software producers and other vendors are now using them as a way to keep in touch with customers.

POP3 - With Post Office Protocol version 3 (POP3) your mail is saved for you in your mail box on the mail server. When you read your mail, all of it is immediately downloaded to your computer and no longer maintained on the mail server.

Postmaster - A required default email account for a domain. In order to receive email from the postmaster account, it has to be forwarded to another email address.

Relay - Allows an SMTP server to accept any email destined for other hosts and re-deliver that mail to the proper host, much like a feild and track relay race where the SMTP servers are the the runners and the email message is the baton.

SMTP - Simple Mail Transfer Protocol is a TCP/IP (Internet) protocol used in 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, POP3 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 POP3 or IMAP for receiving messages that have been received for them at their local server.

SMTP Authentication - When the mail server requires an email address and password that matches an account in order to send mail, as opposed to requiring just an email address.

Spam Check - A resource used for checking the validity of an email sender.

Spam List - Some Domain Name Servers (DNS) on the Internet contain a list of addresses from mail servers that are solely used for email spam. Therefore, the Spam List is a editable list of DNS's so you can compare your incoming mail to those known spam email servers and filter them out accordingly (An example of an "anti-spam" DNS is opm.blitzed.org).

Spool/Queue - A directory on the mail server that holds emails before they are viewed or downloaded from a client.

Stats - The over all calculations about email from a domain including total messages and bandwidth.

User - A client with an email account.

URL - The Uniform Resource Locator is an address that links to a web page or web server that is usually entered into the top of a browser.

Web Interface - The point of access for administrators and end users to the Mail Server via browser, created by SmarterTools called SmarterMail.

Web Mail - An interface for sending and receiving email through the use of a browser (e.g. Internet Explorer or Netscape) instead of an email program (e.g. Outlook). Configuring client side email is as simple as hyper linking to the correct URL and Logging in with a user name and password.

Weight - The weight is a value assigned to a spam check according to its validity and competency.

White List - Add an email address to this list to accept all mail from the sender, regardless of Black List generalization.