Help for System Administrators

Help Documentation

Help for System Administrators

Logging in to SmarterMail

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

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

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

Microsoft Exchange Functionality

This feature is only available using SmarterMail Enterprise licensed with the EAS and/or MAPI/EWS add-ons.

Microsoft Exchange is the standard for corporate email servers. Whether using an on-premise installation or an Office 365 subscription, there is no doubt that Microsoft Exchange, coupled with Microsoft Outlook, offer the features and functionality that email users require for their day-to-day communication.

For years, there was very little competition with Exchange. While there were competing mail products on the market -- third-party products, Yahoo! mail, AOL, and even the rise of Gmail -- the functionality users had with Outlook coupled with Exchange were virtually untouchable. Then came SmarterMail.

Over the years, SmarterMail has grown to be one of the primary competitors to Microsoft Exchange. With the addition of EAS support, the power of mobile email was introduced. Now, SmarterMail offers MAPI/EWS, for true, native Microsoft Outlook integration that gives Exchange a run for its money. And, speaking of money, SmarterMail offers that functionality for a mere FRACTION of what it costs to run Exchange, either on premise or using Office 365.

MAPI/EWS

MAPI is Microsoft's "Outlook protocol". That means it is the foundation by which Outlook on Windows does things like share tasks, calendars and email folders; set up meetings; create contact groups and much more. EWS is a similar protocol, but one that was developed specifically for integration with the Apple ecosystem. While other, non-Mac email clients have adopted EWS (e.g., eM Client), it primarily works with Apple Mail on the Mac.

What makes SmarterMail's use of MAPI different than its competitors is that SmarterMail has native, server-level integration of MAPI, just like Microsoft Exchange. Other products use separate pieces of software that are installed on client machines to "emulate" Exchange functionality. These "Outlook Connectors" don't provide the full suite of Exchange features to Outlook. In addition, they're another piece of software that a client has to install, and that mail administrators or IT staff have to manage.

EAS

EAS is the industry standard for synchronizing mobile devices to SmarterMail, in addition to some email clients (e.g., Microsoft Outlook for Mac). It uses direct push technology to sync email and collaboration items to variety of mobile devices, including smartphones and tablets, as well as Windows Mail, which ships as part of Windows 10.

Enabling Exchange Functionality

Both MAPI/EWS and EAS are licensed protocols from Microsoft. As such, they're licensed add-ons for SmarterMail. So the first step is to ensure you've licensed the add-on you want and/or need.

Next, the System Administrator would need to enable either, or both, for a particular domain. To do this:

- Log in as the System Administrator.
- Go to the Manage area and select a domain from the list. Double-click on it to edit the domain.

- MAPI/EWS and EAS are actually enabled separately. Therefore, find the card for the protocol you want to enable for the domain.
- Add in the number of Accounts you want to allow to use either protocol.
- Ideally, as a System Administrator, you just want to enable the protocols, not manage which accounts actually have MAPI/EWS and/or EAS functionality. Therefore, to allow the Domain Administrator to manage this, enable User Management on. This allows the Domain Administrator to assign the protocol to an actual mailbox.

That's it: you've enabled Microsoft Exchange functionality for that domain.

Enabling Exchange Functionality for More Than One Domain

It IS possible to propagate Exchange Functionality to more than one domain at a time. You do this using Domain Defaults. You would manage the settings just as you do for a single domain, but then propagate those to all domains or even select domains. For more information on this, see the Domain Defaults and Propagation section of the Manage page.

Manage

Domains

System Administrators can use the Domains section to add or remove domains, manage the configuration of one or more domains, attach or detach domains, attach or detach users, send messages to users on the server, export a list of domains or users to CSV and more.

To access this section, log into SmarterMail as the System Administrator and click on the Manage icon. Then select Domains from the navigation pane. Existing domains will be displayed. (If no domains are listed, you will need to Add a New Domain .) Basic details about the domains are displayed, including the number of users, aliases and mailing lists configured, the number of EAS and/or MAPI/EWS mailboxes being used, and the disk space used by each domain. Within the Domains section, System Administrators can access the following items:

Jump To:

- Adding a New Domain
- Configuration - Modify the settings for new domains or modify existing domains and their configuration. This includes:

- Options
- Limits
- Features
- EAS (Enterprise Only)
- MAPI/EWS (Enterprise Only)
- Email
- Mailing Lists
- Security
- Miscellaneous
- Priority and Throttling
- Autodiscover
- Domain Details - If a System Administrator has the ability to manage individual domains,

when they select a domain in the Manage area, in addition to the domain's configuration they'll see the following tabs. These tabs represent how the domain is set up and are, essentially, the same options available to that domain's Administrator(s).

• Accounts - The list of all users set up for that domain. For more information see Users Overview .
• General - These are general settings for the domain such as the Domain Aliases being used, Folder Auto-Clean rules, Email Signing and more. For more information see General Domain Settings .
• Content Filtering - The content filtering rules set up for all users of the domain. For more information see Domain Content Filtering .
• Events The events set up for the entire domain. For more information see Domain Events .
• Sharing - The Shared Resources and User Groups set up for users of the domain. For more information see Domain Sharing ,
• Signatures - The Signatures and Default Signature mappings set up for users of the domain. For more information see Signatures .
• Spam Filtering - The spam filtering rules set up for users of the domain. For more information see Domain Spam Filtering .
• User Defaults - The default settings for each user of the domain such as the Mailbox Size Limit, Webmail options, Service Access and more. For more information see User Defaults .
• Domain Actions - When on the Domains page, there are several Actions available to System Administrators. To view these actions, click the Actions (...) button. You'll see the following:

• Attach User / Attach Folder / Rebuild Folder - These actions allow you to recover a user's account, folder or emails
• Export Domains / Users to CSV - These actions allow you to export a list of all domains, or all users for all domains, to a CSV file.
• Send Email / Notification - These actions allow you to send an email or reminder notification to users on the server.
• Attach / Reload / Detach Domain - These actions allow you to recover a domain or detach it so it can be moved to another server.
• Relevant Knowledge Base Articles - A brief list of articles from our Knowledge Base that cover topics such as moving Domains, attaching users, reloading domains, etc.

Domain Configuration

When the initial domain settings are saved, the following configuration options will appear in the content pane. In addition, the following will be displayed if you are modifying an existing domain by selecting it from the lis. Note: The default configuration of these settings are dependent on what's

configured in the Domain Defaults template. However, they can be adjusted manually per domain, as needed. To adjust the default configuration of new domains, modify the Domain Defaults template.

Options

• Domain Name - The name of the domain. For example, smartermail.com or example.com. To change the name of a domain in SmarterMail, use the Actions (...) button to click on Rename Domain . NOTE: If you rename a domain, users will have to adjust any desktop or mobile clients to use the new domain name. While SmarterMail changes the domain name internally, it can not push the name change to email clients directly. Those have to be updated manually.
• Domain Status - The current status of the domain: Enabled or Disabled. Disabled domains cannot send email and users cannot login to the Web interface. However, the domain will still receive email to prevent email loss. This option is a good way to temporarily shut off a domain without deleting it.
• Hostname - The URL of the mail server (e.g., mail.domain.com) to be returned for an Autodiscover query by a user of that domain. Instructions on how to Set up Autodiscover for SmarterMail can be found in the SmarterTools Knowledge Base . Note: On the Domain Defaults template, the Hostname field has a default value of "mail.%domain%". This variable allows the Hostname to match the name of the domain, though this setting can be adjusted manually, if desired. This Domain Default setting will be applied to new domains and can also be propagated to existing domains on the server.
• Folder - The directory in which all information (XML files, mail statistics, alias information, etc.) pertaining to the domain is saved. To modify the domain's folder path, use the Actions (...) button to click on Change Domain Path .
• Change Domain Admin - To adjust the primary Domain Administrator for the domain, click on the dropdown. Choose an existing user on the domain or click on New User to create a new account.
• Outbound Gateway - Outbound gateways can reduce the load on the server by using a secondary server to process outgoing mail. Specify an outbound gateway to use for messages sent from this domain. If no options are available, an outbound gateway has not been configured. Instructions on how to Configure SmarterMail as a Free Gateway Server can be found in the SmarterTools Knowledge Base .

Limits

• Disk Space (MB) - The maximum number of megabytes allocated for the domain. By default, the domain is allocated 500 MB of disk space. This disk space limit also includes file storage and meeting workspaces for users. Note: When this limit is reached, SmarterMail will send a warning to the domain administrator and mailboxes on the domain will not be able to receive

new mail.

• Domain Aliases - The maximum number of domain aliases allowed for the domain. A domain alias is bascially an alternate domain name for one that already exists in SmarterMail. For example, imagine you have a domain, 'example.com', in SmarterMail with a user, 'user@example.com'. By adding a domain alias for 'example.net', emails sent to 'user@example.net' will be delivered to 'user@example.com'. That means that emails sent to either domain will end up in the same mailbox. By default, domains are limited to two domain aliases.

• Users - The maximum number of mailboxes allowed for the domain. By default, domains are limited to 100 users. Note: If your SmarterMail license limits the number of mailboxes allowed on the domain, your license level will override this setting.

• User Aliases - The maximum number of alias email accounts allowed for the domain. An email alias is essentially a forwarding email address that can be used to forward messages to a single address or multiple email addresses. By default, domains are limited to 1,000 user aliases.

• Max Message Size - The maximum size email a user can send. By default, the max message size is 10,000 KB. This number includes text, HTML, images and attachments. Note: Base64 encoding of attachments increases the size of attachments by approximately 50%. This can impact the overall size of the message and can lead to confusion on the part of senders. For example, if Max Message Size is set to 12MB and a sender adds a 9MB attachment to a message it will essentially be 13MB due to the Base64 encoding. This means that the 9MB attachment will still exceed the message size limit due to this increase.

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

Features

• Active Directory Integration (Enterprise Only) - Select this option to enable active directory authentication. By enabling this, domain administrators will be able to add in the necessary LDAP binding string to import LDAP users.

• Automated Forwarding - Select this option to allow users to enter one or more forwarding addresses that automatically forwards any email that reaches their mailbox. When this feature is enabled, Domain Administrators can enable or disable Automated Forwarding on a per user basis.

• Catch-All Alias - Select this option to allow Domain Administrators to create catch-all email addresses. A catch-all alias is an email address that receives all incoming email that goes to invalid email addresses within the domain. NOTE: This simply enables the ability to set a catch-all alias -- an actual alias will need to be created, or an existing alias edited, and assigned as a

catch-all.

• Chat (XMPP) (Enterprise Only) - Select this option to allow users on the domain to chat with each other via the Web interface or any XMPP-compatible chat client. Note: This feature is only available when licensed with SmarterMail Enterprise.

• Cloud Storage Connections - Select this option to allow users to connect different services, like OneDrive and Dropbox, to their SmarterMail accounts to facilitate actions like attaching links to shared files.

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

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

• File Storage - Select this option to allow users to access the File Storage section, where users can upload files to the mail server and then share them by sending out links to those files.

• Global Address List - Select this option to provide a listing of all users who have accounts for the particular domain in the Contacts menu icon. If the Global Address List is disabled for a domain, collaboration items, like calendars or notes, will not use autocomplete when adding shared users. Note: This feature is only available when licensed with SmarterMail Enterprise.

• Webmail Login Customization - Select this option to allow domain administrators to customize the login screen to add a company logo, provide additional branding text, or adjust the default □Login to SmarterMail□ text. Note: If you enable this feature to allow the domain to override the custom login display, and the Domain Administrator does not enable customization for their domain, users will see the default SmarterMail login screen, regardless of whether the login display is customized in the System Administrator-level general settings.

• SMTP Accounts - Select this option to allow users to send email from a third-party mail server account right from within SmarterMail. When this feature is enabled, Domain Administrators can enable or disable SMTP Accounts on a per user basis.

• Team Workspaces (Enterprise Only) - Select this option to allow users to create Team Workspaces, which allow for video chatting and shared documents with users on the domain and guests alike. Technical Note: Video conferencing within Team Workspaces utilizes WebRTC. WebRTC will prefer UDP as the communications protocol, but it will use TCP if it's the only available method through the firewall. For ports, WebRTC will use anything in the 0-65535 range to transfer video and audio. In order to establish the connection, port 3478 should be open. In addition, WebRTC uses VP8 or H.264 for video codecs and Opus for audio, though this can vary depending on device, OS and browser. WebRTC handles this selection automatically.

EAS (Enterprise Only)

EAS is the industry standard for synchronizing email clients and mobile devices with email servers like SmarterMail. Using EAS, users can synchronize email, contacts and calendars (and tasks and notes, on supported devices) with email clients, like Windows Mail, and with smartphones and tablets from Apple, Samsung and others. When trialing the add-on or using a paid subscription, the following options will be available:

- Allow Domain Admininstrators to enable EAS for users - Enable this setting to allow Domain Administrators to assign EAS to the number of accounts allocated for the domain.
- Accounts - The maximum number of EAS accounts that can be assigned for the domain.

MAPI/EWS (Enterprise Only)

MAPI/EWS are both protocols used for connecting desktop email clients to SmarterMail to give them Microsoft Exchange-level functionality. MAPI is used by Microsoft Outlook 2016 and above for Windows machines while EWS is used by Apple Mail on Mac OS and eM Client on Windows.

- Allow Domain Admininstrators to enable MAPI/EWS for users - Enable this setting to allow Domain Administrators to assign MAPI/EWS to the number of accounts allocated for the domain.
- Accounts - The maximum number of MAPI/EWS accounts that can be assigned for the domain.

Email

- Autoresponder Exclusions - To prevent SmarterMail from sending automated messages, such as out-of-office replies, to addresses based on the spam level of the original message, select the appropriate option from the list.
- Forwarding Exclusions - To prevent the system from forwarding messages based on the spam level of the message, select the appropriate option from the list.
- Inbound Message Delivery - Administrators can specify the domain location for incoming email delivery. This allows you to specify whether the domain is hosted locally or partially/entirely on an external server. The following options are available:

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

be entered as an IP address or the Fully Qualified Domain Name (FQDN), such as mail.yourdomain.com. Select the option "Deliver locally if user exists" to perform a local delivery instead of external if the user exists locally.

• Enable Greylisting - Greylisting is a spam prevention method that temporarily rejects any email from an unrecognized sender. The idea is that a valid message will be re-tried and, therefore, accepted on its subsequent delivery attempt. Though effective, greylisting can lead to a delay in email delivery for a domain. Enable this option to activate greylisting for the domain.

Mailing Lists

Mailing Lists are a great way to allow users to communicate with a number of different individuals via a single email address. For example, many companies use mailing lists to email newsletters, promotional offers, or information about product updates to subscribers. Unlike an Alias, a mailing list allows people to subscribe or unsubscribe from email communications.

• Mailing Lists - Enable this option to allow Domain Administrators to create and manage mailing lists for their domain.

• Mailing Lists - The maximum number of mailing lists allowed for the domain. By default, this setting is set to Unlimited.

• Mailing List Max Message Size (KB) - The maximum size message that can be sent to a mailing list. By default, the maximum message size is set to Unlimited.

Security

• Two-Step Authentication - Two-Step Authentication is a method of providing a second verification of account ownership before a user can log into their account or connect to third-party clients and/or devices. For example, when a user has Two-Step Authentication enabled for their account, the SmarterMail login page will require their primary account password and a secondary verification of account ownership before the user can log into webmail. The second method of verification will be provided to the user through popular authentication apps, like Google or Microsoft Authenticator, or through a recovery email address. When this feature is enabled for a domain, the Domain Administrator can override the system setting and choose whether to enable or force Two-Step Authentication for their users. Two-Step Authentication can be Disabled, Enabled or Forced for the domain.

• TLS - To enable or disable TLS (SSL encryption) for outgoing mail, select the appropriate option from the list.

• SRS - To enable or disable SRS (the ability for the mail server to re-write the senders email address so that forwarded messages pass SPF checks) for mail, select the appropriate option from the list.

• Require SMTP Authentication - Enable this option to require SMTP authentication when

sending email. Note: If this option is enabled, users must provide an email address and password to send email from their account. SmarterMail supports cram-md5 and login authentication methods.

• Force all traffic over HTTPS - Select this option to force all SmarterMail traffic over HTTPS. This improves SmarterMail security by allowing all traffic to be encrypted. Note: Prior to enabling this setting, SmarterMail must be set up as a site in IIS and have a valid SSL certificate in place for the SmarterMail site. If this is enabled and a user navigates to the IP address, the server will attempt a rDNS lookup and then redirect accordingly.

• Show Passwords to Domain Administrators - Enable this option to allow Domain Administrators to view a user's account password (and app passwords, if the user is protected by Two-Step Authentication). Note that account passwords cannot be viewed for accounts authenticated by Active Directory.

Miscellaneous

• Calendar Auto Clean Month(s) - Use this to set a time frame that SmarterMail will use to automatically remove legacy calendar items from users' calendars. If allowed, Domain Administrators can override this setting when managing their own domain.

• Postmaster Mailbox - The System Administrator can specify an email account that's used as the postmaster address for a specific domain. If there's no specific postmaster@ account set up for a domain, then the Primary Domain Administrator address is generally entered here. The Postmaster address is essentially an Alias: if someone emails postmaster@, the email is forwarded to the address entered here, just as it is for an Alias. If an Account, Alias or Mailing List already exists with the "postmaster" username/name, then this field is ignored.

• Redirect to a webpage on logout from webmail - Generally, when users logout of webmail they're presented with the standard webmail login page. However, a System Administrator can enter a custom URL to a page that is presented to users when they log out of webmail.

• Allow Domain Admininstrators to create domain aliases - Enable this option to allow Domain Administrators to create domain aliases. A domain alias is bascially an alternate domain name for one that already exists in SmarterMail. For example, imagine you have a domain, 'example.com', in SmarterMail with a user, 'user@example.com'. By adding a domain alias for 'example.net', emails sent to 'user@example.net' will be delivered to 'user@example.com'. That means that emails sent to either domain will end up in the same mailbox.

• Exclude IP from received line - Select this option to remove the client's IP address from the received header on messages received through SMTP. Note: Removing the IP address from the received header is not recommended because it violates RFC.

• Restrict autoresponders to once per day per sender - Select this option to limit how frequently an autoresponder is sent. Continually sending something like an out-of-office reply to the same

address every time an email comes in can cause abuse issues. Therefore, it is recommended that this be set for all domains.

Priority and Throttling

Use this card to prioritize the remote delivery of standard messages and configure the throttling options for the domain. By default, all messages for all users are sent at a normal priority with an exception of mailing lists, which default to low priority. Messages that fail the first attempt to deliver get automatically "degraded" in priority to low.

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

- Delivery Priority - The priority level for messages that don't have another priority affecting it.
- Outbound Messages per Hour - The number of messages sent by the domain per hour. By default, the number of outgoing messages is 5,000.
- Message Throttling Action - The action SmarterMail should take when the message throttling threshold is reached.
- Outbound Bandwidth MB per Hour - The total number of MBs sent by the domain per hour. By default, the outgoing bandwidth is 100.
- Bandwidth Throttling Action - The action SmarterMail should take when the bandwidth throttling threshold is reached.
- Bounces Received per Hour - As bounce messages are received from null senders per RFCs, this setting dictates the number of messages from null senders a domain can receive over SMTP before any further messages from null senders will be rejected. By default, a domain can receive 1,000 bounces per hour.
- Bounces Throttling Action - The action SmarterMail should take when the bounces throttling threshold is reached.

Autodiscover

Autodiscover is a service that allows email clients to automatically determine a user□smail server address and port from that user□semail address and password alone. This greatly simplifies a user□s setup process when attempting to connect SmarterMail to a desktop client, like Outlook and Apple Mail, as well as mobile clients. Autodiscover settings can be configured per protocol and per domain. Instructions on how to Set up Autodiscover for SmarterMail can be found in the SmarterTools Knowledge Base .

With the appropriate DNS records and IIS configuration in place, you can use this section to enable or disable specific protocols from returning Autodiscover results. When a protocol is enabled for Autodiscover, clicking on that protocol's settings cog will open a window where the encryption type and port can be adjusted. Utilizing Autodiscover with MAPI/EWS or EAS requires encryption over SSL or TLS. Therefore, port 443 MUST be available and not blocked by a firewall. NOTE: If a user has POP disabled for their account, their POP Autodiscover request will not be fulfilled, even if POP is enabled for Autodiscover. This applies to all protocols in their account's Service Access settings.

Overriding the Default Desktop and/or Mobile XML Responses

Administrators with advanced Autodiscover knowledge can override the default XML response that is sent from the domain when Autodiscover is requested. However, please understand that these settings should NOT be modified without advanced knowledge of the XML responses used with Autodiscover. Adjusting the custom XML incorrectly can result in invalid responses returned meaning users will be unable to connect to their email client(s). Furthermore, if you turn on an override but never save any custom XML, SmarterMail will use the default protocol settings. However, if the override is turned on, ANY text you save to the Custom XML area will be used for the Autodiscover response. If you save custom text, then later remove that text and save a blank entry, Autodiscover will send a blank response. Therefore, it is imperative that you only enable the override and enter custom Autodiscover XML if you are absolutely sure what you're using is correct.

There are two types of Autodiscover responses that can be modified: Mobile XML and Desktop XML. The mobile XML response is strictly used with EAS. The desktop XML response is used with everything else, including IMAP, POP, SMTP In, MAPI and EWS.

In the textbox window that appears after enabling the override of the XML, clicking on Generate will show the XML response that SmarterMail would normally send on an Autodiscover request. You can generate this response to make adjustments as needed, or simply enter the XML response you would like to use. When adjusting the XML, don't remove or modify variables such as %EmailAddress%, %Base64EmailAddress% or %DisplayName%, since these are used to identify the user making the Autodiscover request. Also note that although changes are not validated by SmarterMail, any changes made to the XML response should be within RFC guidelines.

Attach User / Attach Folder / Rebuild Folder

System Administrators can restore a user's emails, email folders or their entire user account, which is extremely useful if a folder or email is mistakenly deleted or if there is corruption within the mailbox.

To restore user data, click on the Actions (...) button in the Domains section. Then choose the type of restore you would like to perform:

- Attach User - Select this option to attach a user that is on disk but not in the domain. In other words, to restore an entire user's account. Note: The user's folder needs to be correctly placed in the domain folder on the server prior to performing this action.
- Attach Folder - Select this option to attach a folder that is on disk but not in the account. In other words, to restore a user's email folder.
- Rebuild Folder - Select this option to copy .grp files or .eml files into an existing user's folder and have SmarterMail re-build that folder to include the new .grp and .eml files. In other words, to restore a user's emails.

The following options will be available, depending on the restore type selected.

- Email - The full email address of the user account being restored or the full email address of the owner of the folder being attached or rebuilt.
- Folder Path - The path of the folder within the Web interface that will be used to rebuild or restore an email folder. For example, if you're restoring a subfolder that was created under the Inbox, the folder path would look like: Inbox\Example Folder.
- Recursive - Enable this option to attach any subfolders that are found within a folder that is being attached or rebuilt.

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

Export Domains / Users to CSV

System Administrators can export a list of all domains or users on the server in CSV format. The domain CSV spreadsheet will include every domain name along with its status, size, number of users, number of aliases, user limits, throttling configuration, enabled features and more. The user CSV will list every username, sorted by domain, along with their display name, authentication type, title, full name, birthday, phone number, home address, work address, job title, disk space used, status, last login date and more.

System Administrators with Manage Domain permissions can also export the Users for specific domains. All they do is go to the Accounts tab for the domain -- there is an Export Users option under the Actions (...) button on the Accounts tab.

To use the export feature, click on the Actions (...) button in the Domains sections and then click on Export Domains to CSV to export a list of domains or Export Users to CSV to export a list of users.

Send Email / Notification

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

Send Email

To send a mass email, click the Actions (...) button in the Domains section and then click Send Email . The mass messaging options will load in a modal window and the following fields should be completed:

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

Once you complete all the fields, click the Send button to deliver the message.

Send Notification

Notifications are a quick and easy way to send information to a group of users on the mail server. Simliar to sending an email, a notification will stay within the mail server and be displayed in users' notifcations area rather than being sent to them as an actual email message. For example, if you send a message to all users of a domain about some upcoming maintenance work on the mail server, you can use use Send Notification to do a quick follow up reminding the users of the scheduled work.

To send a mass nmotification, click on the Actions (...) button in the Domains section and then click on Send Notification . The messaging options will load in a modal window and the following fields should be completed:

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

Once you complete all the fields, click the Send button to deliver the notification message.

Attach / Reload / Detach Domain

The ability to quickly and easily move domains from one SmarterMail server to another, without having to stop the mail server or halt the mail service, is crucial for System Administrators.

Attach Domain

Attaching a domain makes it easy to add a new domain, complete with users, configuration settings, etc. You simply move the files and folders to a new server, add in the Domain Path , and SmarterMail will add the domain to the domains.json file. In addition, if you're moving from an older version of SmarterMail to a current Build, if any conversion is necessary, after you attach the domain, SmarterMail will upgrade the domain on the spot.

Reload Domain

Reloading a domain is essentially "rebooting" the domain: it clears all webmail sessions, reloads the domain's settings, all user settings and files for the domain. If you see odd behavior with users or other odd behavior, reloading the domain may clear things up.

Detach Domain

Detaching a domain essentially prepares the domain for a move to another server, or even just moving the domain to another drive. Detaching removes the domain from the domains.json file, then, once you've made whatever changes are necessary, you simply attach the domain again. It also logs out any users who are logged in and, more importantly, will remove any Domain Aliases that are set up for the domain. These would have to be re-added once the domain is attached in its new location.

Relevant Knowledge Base Articles

We have created several knowledge base articles for common situations where use of "Attach Domain" or "Rebuild Folder" are necessary. Below is a partial list of articles that detail the steps necessary to do things such as restore a user's folders, migrating or moving a domain from one server to another, etc.

- Backup and Restore SmarterMail
- Restore a User's Account, Folders, or Emails
- Migrate SmarterMail to a Different Server
- Migrate SmarterMail to a Different Server (Using Robocopy)
- Move a Domain from One SmarterMail Server to Another
- Move a Domain to a Different Hard Drive on the Same Server
- Move SmarterMail from Hosted to Self-Installed
- Restore a User□s Account, Emails and Folders
-
-
- --%>

Spool

Spool Overview

The email spool is a list of emails, in order of when they are created, that are available for the server to send out to other mail servers or to deliver locally. Within the Spool Overview section, Administrators can monitor a dashboard of common aspects of the email spool, including message activity, top outbound senders, top inbound domains and more. In addition to reviewing the spool activity, Administrators can take action on any messages that are currently being held in the spool. For example, a sending IP address that is inundating the mail server with unwanted messages can be blocked, thereby preventing issues from becoming problems for email users.

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

To access the Spool Overview, log into SmarterMail as a System Administrator and click on the Manage icon. Click on Spool in the navigation pane, then click the Overview tab.

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

Message Activity

This section displays the total number of messages that have been delivered by all users, including

local and remote deliveries. From this table, see how many messages were sent in the last 5 minutes, last hour, last 24 hours and from the start of the installation.

Top Outbound Senders

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

- Manage User - Select this option to log in and impersonate the actual user. Impersonating the user allows you to check all of their settings and includes Domain settings if the user is a Domain Administrator. So if the account appears to be compromised, it can be disabled after due diligence is performed.
- Change Password - Select this option to change the password of a user's account. Changing the password is an ideal option when resolving a compromised account.
- Drop Connections - Select this option to end the user's connection(s) via webmail and different syncing protocols, including SMTP, IMAP, POP, XMPP and ActiveSync.
- Disable User - Select this option to immediately disable the user's account. This action utilizes the User Status setting found when editing a user . When a user is disabled within the Spool Overview, their User Status will be set to 'Disable and Allow Mail'. This prevents the user from sending outbound messages or accessing webmail; however, the mailbox will continue to receive incoming email. Enabling a user in the Spool Overview will adjust the setting in the user's account settings and vice versa.
- Delete Messages - Select this option to permanently delete the messages sent by the user that are currently in the spool. Note: This will only delete messages that are CURRENTLY being held in the spool.
- Move Messages - Select this option to move the messages sent by the user that are currently held in the spool to another folder on the server. Use the default path provided or enter any folder path on the server. Moving the .eml files to their own folder on the server is useful because it allows an Administrator to review the messages before taking actions against them.

Note: In general, this table will display SmarterMail user accounts only. However, there may be cases where remote email addresses appear, including if: the email address is authenticated with a local account, the sending IP address is listed in the SMTP Authentication Bypass list, SmarterMail is acting as an inbound gateway, or messages were manually dropped into the spool with sender addresses that don't exist locally. In these instances, the Manage User and Disable User actions cannot be performed.

Top Outbound IP Addresses

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

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

Top Inbound Recipients

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

- Manage User - Select this option to log in and impersonate the actual user. Impersonating the user allows you to check all of their settings. Impersonating the user allows you to check all of their settings and includes Domain settings if the user is a Domain Administrator. So if the account appears to be compromised, it can be disabled after due diligence is performed.
- Change Password - Select this option to change the password of a user's account. Changing the password is an ideal option when resolving a compromised account.
- Drop Connections - Select this option to end the user's connection(s) via webmail and different syncing protocols, including SMTP, IMAP, POP, XMPP and ActiveSync.
- Delete Messages - Select this option to permanently delete all of the inbound messages sent to the user that are currently in the spool. Note: This will only delete messages that are CURRENTLY being held in the spool.
- Move Messages - Select this option to move a user’s inbound messages that are currently held

in the spool to another folder on the server. Use the default path provided or enter any folder path on the server. Moving the .eml files to their own folder on the server is useful because it allows an Administrator to review the messages before taking actions against them.

Top Inbound Senders

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

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

Top Inbound IP Addresses

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

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

or enter any folder path on the server. Moving the .eml files to their own folder on the server is useful because it allows an Administrator to review the messages before taking actions against them.

Top Inbound Domains

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

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

Spool (and Waiting to Deliver)

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

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

To view all messages in the spool, log into SmarterMail as a System Administrator and click on the Manage icon. Click on Spool from the navigation pane, then the Spool tab. All inbound and outbound

messages, including ones that are attempting to be delivered or waiting to be delivered, will be displayed. To view a filtered display of the spool for only messages that are waiting to be delivered, click on the Waiting to Deliver tab.

Important Notes:

- Messages that are Waiting to Deliver have typically encountered an error on one or more recipients of the message and are waiting for the next retry interval to attempt delivery again. Emails that are stuck on local delivery or waiting to deliver without any retry attempts are typically the result of IO Bottleneck at the CPU or storage array.
- Spool and Waiting to Deliver tabs will only load a maximum of 50,000 messages combined. (E.g., 20,000 Spool messages are displayed and 30,000 Waiting to Deliver messages are displayed - together they'll never show more than 50,000 messages). That means that if the two numbers add up to 50,000, it's very likely there are MORE than the number of individual emails for each type than can be displayed.

The following details can be seen for each entry in the spool:

- Filename - The unique name of the EML file on the hard disk of the SmarterMail server.
- Spool Path - The spool the message resides in. If you have subspools enabled, the message may be placed in one of those locations.
- Sender - The email address that initially sent the email.
- Recipients - The number of delivered/total recipients.
- Size - The total size of the message on the hard drive, in kilobytes.
- Attempts - The number of delivery attempts that have been made.
- Time in Spool - The total amount of time the message has been in the spool.
- Priority - The priority level of the message: low, normal or high.
- Status - The current status of the message. Messages in the spool have four delivery statuses:

- Delivery Delay - This is the first status of any message in the spool. Administrators can configure a Delivery Delay within the system's General Settings. This delay represents the number of seconds mail will be held in the spool before it is delivered. A delivery delay is beneficial when you are running a secondary service (such as a virus checker) that needs access to messages prior to delivery, as it provides ample time for the secondary service to interact with the message.
- Spam Check - At the second stage of an email's delivery process, SmarterMail runs the configured spam checks against the contents of the email. Messages from whitelisted senders will bypass this delivery status.
- Waiting to Deliver - Emails with a status of Waiting to Deliver have typically encountered an error on one or more recipients of the message and is waiting for the next retry interval to hit.

On the next retry interval, the delivery process will start from the top with its configured Delivery Delay.

• Remote / Local Delivery - This is the final stage of an email's delivery, where the message is sent to its intended recipients. A status of Local Delivery will appear for messages sent between local users on the server and is shown is when SmarterMail is writing to the actual GRP files. Remote Delivery will appear for any outgoing messages that are destined for outside of the mail server.

• Next Attempt - The date and time of the next delivery attempt, based on the retry intervals configured in General Settings.

To view the contents of a message or its intended recipients, click on the entry's row. The email will load in a popup window. If you are presented with a note that the "Message no longer exists," it's possible that the message was already delivered or removed by antivirus software or that the spool contains an orphaned HDR file without the associated EML.

The following actions can be taken on selected entries using the Actions (...) button:

• Force - Pushes the selected message(s) to the top of the spool by setting its priority to High. Note: The status of forced messages will not update until the server passes through the spool.

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

• Change Priority - Changes the priority level of the selected message(s).

• Delete - Removes the selected message(s) from the spool. Note: No confirmation dialog will display, so use caution when deleting from the spool.

• Move Messages - Moves the location of the selected message(s) from the general email directory to a new path on the server. Use the default path provided or enter any folder path on the server. Moving the .eml files to their own folder on the server is useful because it allows an administrator to review the messages before taking actions against them.

Searching the Spool

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

Spool (and Waiting to Deliver)

The email spool is a list of emails, in order of when they are created, that are available for the server to send out to other mail servers or to deliver locally. SmarterMail is multi-threaded, which means that if

a message cannot process out of the spool, SmarterMail simply moves on to the next message until the maximum number of threads that are designated in the administrative configurations are in use. Administrators can use the information here to adjust threads and resources to allocate for concurrent messages.

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

To view all messages in the spool, log into SmarterMail as a System Administrator and click on the Manage icon. Click on Spool from the navigation pane, then the Spool tab. All inbound and outbound messages, including ones that are attempting to be delivered or waiting to be delivered, will be displayed. To view a filtered display of the spool for only messages that are waiting to be delivered, click on the Waiting to Deliver tab.

Important Notes:

- Messages that are Waiting to Deliver have typically encountered an error on one or more recipients of the message and are waiting for the next retry interval to attempt delivery again. Emails that are stuck on local delivery or waiting to deliver without any retry attempts are typically the result of IO Bottleneck at the CPU or storage array.
- Spool and Waiting to Deliver tabs will only load a maximum of 50,000 messages combined. (E.g., 20,000 Spool messages are displayed and 30,000 Waiting to Deliver messages are displayed - together they'll never show more than 50,000 messages). That means that if the two numbers add up to 50,000, it's very likely there are MORE than the number of individual emails for each type than can be displayed.

The following details can be seen for each entry in the spool:

- Filename - The unique name of the EML file on the hard disk of the SmarterMail server.
- Spool Path - The spool the message resides in. If you have subspools enabled, the message may be placed in one of those locations.
- Sender - The email address that initially sent the email.
- Recipients - The number of delivered/total recipients.
- Size - The total size of the message on the hard drive, in kilobytes.
- Attempts - The number of delivery attempts that have been made.
- Time in Spool - The total amount of time the message has been in the spool.
- Priority - The priority level of the message: low, normal or high.
- Status - The current status of the message. Messages in the spool have four delivery statuses:

- Delivery Delay - This is the first status of any message in the spool. Administrators can configure a Delivery Delay within the system's General Settings. This delay represents the number of seconds mail will be held in the spool before it is delivered. A delivery delay is beneficial when you are running a secondary service (such as a virus checker) that needs access to messages prior to delivery, as it provides ample time for the secondary service to interact with the message.
- Spam Check - At the second stage of an email's delivery process, SmarterMail runs the configured spam checks against the contents of the email. Messages from whitelisted senders will bypass this delivery status.
- Waiting to Deliver - Emails with a status of Waiting to Deliver have typically encountered an error on one or more recipients of the message and is waiting for the next retry interval to hit. On the next retry interval, the delivery process will start from the top with its configured Delivery Delay.
- Remote / Local Delivery - This is the final stage of an email's delivery, where the message is sent to its intended recipients. A status of Local Delivery will appear for messages sent between local users on the server and is shown is when SmarterMail is writing to the actual GRP files. Remote Delivery will appear for any outgoing messages that are destined for outside of the mail server.
- Next Attempt - The date and time of the next delivery attempt, based on the retry intervals configured in General Settings.

To view the contents of a message or its intended recipients, click on the entry's row. The email will load in a popup window. If you are presented with a note that the "Message no longer exists," it's possible that the message was already delivered or removed by antivirus software or that the spool contains an orphaned HDR file without the associated EML.

The following actions can be taken on selected entries using the Actions (...) button:

- Force - Pushes the selected message(s) to the top of the spool by setting its priority to High. Note: The status of forced messages will not update until the server passes through the spool.
- Reset Retries - Resets the retry counts on the selected message(s) in the spool, effectively starting the delivery process over. This can be useful if a DNS or firewall problem has been recently resolved, or if you are using SmartHosting and the target server was down.
- Change Priority - Changes the priority level of the selected message(s).
- Delete - Removes the selected message(s) from the spool. Note: No confirmation dialog will display, so use caution when deleting from the spool.
- Move Messages - Moves the location of the selected message(s) from the general email directory to a new path on the server. Use the default path provided or enter any folder path on

the server. Moving the .eml files to their own folder on the server is useful because it allows an administrator to review the messages before taking actions against them.

Searching the Spool

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

Spam Quarantine

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

To view a list of quarantined spam messages, log into SmarterMail as a System Administrator and click on the Manage icon. Click on Spool in the navigation pane, then click on the Spam Quarantine tab. Messages that have been flagged and quarantined by SmarterMail's antispam measures (including the Message Sniffer or Cyren Premium Antispam add-ons, if enabled) will be listed. The following details can be seen for each entry:

- File Name - The unique name of the EML file on the hard disk of the SmarterMail server.
- Date - The date and time the message was flagged for quarantine.
- Sender - The email address that initially sent the email.
- Recipients - The number of delivered/total recipients.
- Size - The total size of the message on the hard drive, in kilobytes.
- Attempts - The number of delivery attempts that have been made.
- Time in Spool - The amount of time the message has been quarantined.
- Time of Removal - The date and time message will be automatically removed from quarantine and permanently deleted.

To view the contents of a message or its intended recipients, click on the entry's row. The email will load in a popup window.

The following actions can be taken on selected entries using the Actions (...) button:

- Resend - Moves the selected message(s) to the spool for delivery to its intended recipients.
- Delete - Remove the selected message(s) from the quarantine list.
- Move Messages - Moves the location of the selected message(s) from the general email

directory to a new path on the server. Use the default path provided or enter any folder path on the server. Moving the .eml files to their own folder on the server is useful because it allows an administrator to review the messages before taking actions against them.

Important Notes:

- Spam Quarantine settings can be managed from the Antispam section. To access this page, click on the Settings icon. Then click on Antispam in the navigation pane. Make sure the Options tab is highlighted. The quarantine settings can be found on the SMTP Blocking card. For more information, refer to the Antispam page.
- Spam Quarantine and Virus Quarantine tabs will only load a maximum of 5,000 messages combined. (E.g., 2,000 Spam Quarantine items displayed and 3,000 Virus Quarantine items displayed - together they'll never show more than 5,000 messages). That means that if the two numbers add up to 5000, it's very likely there are MORE than the number of individual emails for each Quarantine type than can be displayed. If there are, they will need to be reviewed/handled from within the appropriate directory on the server.

Virus Quarantine

Inbound and outbound messages that have been flagged as containing viruses by SmarterMail's ClamAV or the Cyren Zero-hour Outbreak Detection add-on are quarantined, by default, for 30 days. Quarantining such messages allows Administrators to investigate for any false positives and make appropriate adjustments or notify the developer of the virus scanner, if necessary.

To view a list of quarantined virus messages, log into SmarterMail as a System Administrator and click on Manage icon. Click on Spool from the navigation pane, then click on the Virus Quarantine tab. Messages that have been flagged and quarantined by SmarterMail's antivirus measures (including the Cyren Zero-hour Outbreak Detection add-on, if enabled) will be listed. The following details can be seen for each entry:

- File Name - The unique name of the EML file on the hard disk of the SmarterMail server.
- Date - The date and time the message was flagged for quarantine.
- Sender - The email address that initially sent the email.
- Recipients - The number of delivered/total recipients.
- Size - The total size of the message on the hard drive, in kilobytes.
- Attempts - The number of delivery attempts that have been made.
- Time in Spool - The amount of time the message has been quarantined.

- Time of Removal - The date and time that a message will be automatically removed from quarantine and permanently deleted.

To view the contents of a message or its intended recipients, click on the entry's row. The email will load in a popup window.

The following actions can be taken on selected entries using the Actions (...) button:

- Resend - Moves the selected message(s) to the spool for delivery to its intended recipients.
- Delete - Remove the selected message(s) from the quarantine list.
- Move Messages - Moves the location of the selected message(s) from the general email directory to a new path on the server. Use the default path provided or enter any folder path on the server. For example, it's possible to move messages to a "Moved Items" folder within the Spool folder using this path "C:\SmarterMail\Spool\MovedItems\". Moving the .eml files to their own folder on the server is useful because it allows an administrator to review the messages before taking actions against them. While it is possible to move quarantined messages to another user's folder (the folder path would look like "C:\SmarterMail\Domains\[Domain.com]\Users\[Username]\Mail\[Folder Name]\"), this isn't recommended as these messages have been flagged as possibly containing viruses; moving them to a user folder could "enable" any virus contained in a message if it's not handled properly.

Important Notes:

- Virus Quarantine settings can be managed from the Antivirus section. To access this section, click on the Settings icon. Then click on Antivirus in the navigation pane. For more information, refer to the Antivirus page.
- Spam Quarantine and Virus Quarantine tabs will only load a maximum of 5,000 messages combined. (E.g., 2,000 Spam Quarantine items displayed and 3,000 Virus Quarantine items displayed - together they'll never show more than 5,000 messages). That means that if the two numbers add up to 5000, it's very likely there are MORE than the number of individual emails for each Quarantine type than can be displayed. If there are, they will need to be reviewed/handled from within the appropriate directory on the server.

Throttled Users

Bandwidth and email throttling allow System Administrators to limit the quantity of data that a SmarterMail mail server transmits within a specified period of time. This limit can be set by the amount of outgoing bandwidth used or the number of outgoing emails sent.

To view the users on the server who are currently being throttled, log into SmarterMail as a System Administrator and click on the Manage icon. Click on Spool in the navigation panel, then click on the Throttled Users tab.

Note: User throttling rules can be configured on the User Defaults template in the Manage > Domains section. This configuration can be further managed by Domain Administrators on a per user basis.

The following details can be seen for each entry in the list:

- User - The email address of the user account currently being throttled.
- Mailing List - This acts as an indicator to specify whether the 'user' being throttled is a mailing list address. Note: Mailing list throttling is managed by Domain Administrators on a per mailing list basis.
- Domain - The domain of the user that is currently being throttled.
- Reason - The type of action that triggered the throttle: Messages Out or Bandwidth Out.
- Date - The date and time the user triggered the throttling action.

Throttled Domains

Bandwidth and email throttling allow System Administrators to limit the quantity of data that a SmarterMail mail server transmits and/or receives within a specified period of time. This limit can be set by bandwidth, the number of emails transmitted, and/or by the number of bounced messages received.

To view the domains on the server that are currently being throttled, log into SmarterMail as a System Administrator and click on the Manage icon. Click on Spool in the navigation pane, then click on the Throttled Domains tab.

Note: Domain throttling rules can be configured in the Manage > Domains section on the Domain Defaults page or on a per domain basis.

The following details can be seen for each entry in the list:

- Domain - The domain on the server that is currently being throttled.
- Reason - The type of action that triggered the throttle: Messages Out, Bandwidth Out or Bounces Received.
- Date - The date and time the domain triggered the throttling action.

User Activity

System Administrators can use this section to monitor the activity of users on the server. To access

this section, log into SmarterMail as a System Administrator and click on the Manage icon. Then click on User Activity in the navigation pane.

Online Users

From this section, you can view each online/active user on the server and determine how many connections are occurring for each protocol, including webmail, SMTP, IMAP, POP, XMPP, EAS and MAPI/EWS. If a user is currently logged into webmail, their IP address and the length of their webmail connection will appear in the list as well. The following actions can be taken:

- Refresh - This button refreshes the list of online users.
- Drop Connections - This Action ends the selected user's session(s).

There are a number of reasons why you may see 'Anonymous Users' in this list. For example, these could be people who have the login page open in a browser but are not currently logged in or there could be a monitoring app or service that is monitoring whether a login page responds to ping, etc.

Inactive Users

Viewing Inactive Users is a good way to clean out users from the domain that are no longer needed. For example, perhaps these users and their mailboxes can be archived or copied and moved to another location in order to to recover some disk space for the domain.

An "Inactive User" is an account that hasn't authenticated against the SmarterMail server in whatever period of time is selected from the Actions (...) menu. If a account is set up in an email client on desktop or mobile, if an account is set up to be pulled into another mail server or mail service, like if a user has their SmarterMail account set up in Gmail to pull messages into Gmail via IMAP or POP3, or other situations, these accounts are still "active" in that whatever action is taken in that client or service will have to authenticate against SmarterMail to peform some action. Inactive Accounts don't perform any of those actions. Therefore, they're probably unused.

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

Note: The entries shown in this section can be sorted using the various grid column titles.

- User - The email address of the user.
- Enabled - The account status of the user, indicating whether they are enabled or disabled.
- Domain Administration - An indication of whether the user has Domain Administrator privileges.
- Last Login - The date of the last time the user logged in.

When viewing Inactive Users, it's important to first select the inactive timeframe you would like to review. This can be done by clicking on the Actions (...) button.

- 30 days - Users who have been inactive for 30 days or more. This is also the default timeframe for Inactive Users.
- 90 days - Users who have been inactive for 90 days or more.
- 6 months - Users who have been inactive for 6 months or more.
- 12 months - Users who have been inactive for 12 months or more.
- Refresh - Refreshes the list of inactive users.

Along with the inactive timeframe, the following actions can be taken within the Inactive Users section:

- Delete - Deletes the selected user(s) from SmarterMail. NOTE: This will actually delete the user from the domain. Therefore, it's extremely important to work with the domain administrator before you delete users from this area.
- Disable - Simply disables the user account. This is a good way to determine whether a user is still using their account, they simply haven't logged in for some period of time. By disabling the account, if the user DOES log in, they will contact their administrator.
- Enable - Simply enables the user account. This is generally used after a user has been disabled, per the above.
- Export All to CSV - It's possible to download all information as a Comma Separated Values list to be used in somethign like Microsoft Excel, to compare against a billing system, etc.

Connections

SmarterMail will monitor the server and see who is connecting via the different syncing protocols, including SMTP, IMAP, POP, XMPP, EAS and MAPI/EWS. System administrators can then use this section to blacklist a certain IP address or drop an IP's current connection if they believe too many connections are being made. Current connections can be viewed all at once or separated by protocol.

To view the current connections, log into SmarterMail as a System Administrator and click on Manage in the navigation pane. Then click on Connections from the navigation pane.

Regardless of the type of Connection you're viewing, the following options are avaiable:

- Refresh - Refreshes the list of online users.
- Actions (...) - Additional actions are available via this dropdown:

- Blacklist - Adds the IP address to the server blacklist file.
- Drop Connections - End the selected user's session.

Regarding connections that appear to last longer than they should, this could be due to a number of reasons. For example, SMTP connections that stay active for hours could be due to multiple people

connecting from behind a firewall. These people all appear to connect from a single IP, but they're actually individual connections, one for each user. The firewall simply portrays the connections as being from a single source. In addition, some numbers may always show up as 0. For example, EWS and MAPI tabs will only show connections when users connecting via those protocols are actually attempting to connect and are pulling or pushing a sync. MAPI and EWS don't IDLE like EAS or IMAP, so the numbers will fluctuate or possibly show 0.

IDS Blocks

System Administrators can use this section to review all IP addresses that have been blocked by the mail server as a result of any IDS (abuse detection) rules that have been configured in SmarterMail's Security area. As a result of these rules, SmarterMail will monitor the server and keep track of all IP addresses that are currently being blocked for SMTP, IMAP, POP, LDAP, XMPP, Webmail or for potential email harvesting abuse. System admins can view a list of blocked IPs by abuse type or view all blocked connections at one time.

Each IDS category has its own tab, and on each tab is displayed the number of sources blocked within that category. These categories include:

- All Blocks
- SMTP
- IMAP
- POP
- Delivery
- LDAP
- XMPP
- Webmail
- Email Harvesting

Clicking on a tab displays the following information:

- Source - The IP address that tripped the IDS rule. NOTE: The use of VPNs and proxies mean that the Source of the intrusion may not be the actual origination of the intrusion.
- Time Left - The time remaining for the specific block. When setting up IDS rules, System Administrators can attach time limits for each type of block. Time Left offers a countdown timer based on what is set by the System Admininstrator.
- Country - The country of origin for the Source IP.
- Protocol - The protocol used for the intrusion.
- Type - The type of intrusion detection rule that was triggered.

- Rule Description - The description of the Rule Type as provided by the System Administrator when the Rule was created.

System adminstrators can remove the selected Source IP(s) from the list by selecting the IP(s) and clicking Unblock . However, this does not affect the abuse detection rule that blocked the IP in the first place; it only removes the block from the IP. If the System Administrator feels the block is warranted, and should be enforced past the Time Left, they can Blacklist the IP.

Server Blacklist

Rather than logging into various websites and performing manual checks of their IP addresses, System Administrators can use the Server Blacklist section to check whether their mail server has been listed by one of the realtime black lists (RBL) that SmarterMail incorporates into its spam checks. These checks are performed automatically everyday for all IP addresses added to the server, regardless of whether the RBL is actively being used as a spam check. Note: Creating a Blacklist Status Changed system event is a great way to be immediately notified if a server becomes listed by an RBL.

To access the Server Blacklist, log into SmarterMail as a System Administrator and click the Manage icon. Then click on Server Blacklist from the navigation pane. You can review Blocks by IP , which will list any server IPs that have been blacklisted, or Blocks by RBL , which lists the RBLs that have blocked server IPs. Regardless of which tab you select, the following details can be seen for each entry:

- IP Address - The IP address used for a domain, or for several domains, on that mail server.
- Spam Check - The name of the RBL or URIBL that is being checked.
- IPs Blocked - The number of IP addresses that are currently blocked by the corresponding spam check. Click on the entry's row to view the exact IP addresses.
- RBLs Blocked - The number of RBLs that are currently blocked by the corresponding IP address. Click on the entry's row to view the exact RBLs.
- Changed - The last date and time the IP showed a different block status against the specific item.
- Checked - The last date and time the IP was checked against the specific item.

It's also possible to manually run the Server Blacklist check. This is especially useful if you've had to contact an RBL to requst the block be lifted. To run this, click on the Actions (...) button. From the dropdown, select Run Server Blacklist Check .

Domain Defaults

The job of the System Administrator is to make sure that the SmarterMail server runs as efficiently as

possible. Part of that responsibility is putting measures in place to limit the potential for system abuses and "user error" that could cause problems.

SmarterMail gives System Administrators the ability to create a default template that's used as a starting point for all domains that are added to the mail server. This includes the ability to set disk space limits for for the domain, set the number of domain aliases that can be created, the number of users and user aliases, the features available for users and more. These defaults can be set at any time and propagated to all domains on the server. From here, Domain Admininstrators can futher lock down user accounts and set their own user limits.

Domain Defaults

To review the default configuration for new domains, click on the Manage icon. Then select Domain Defaults from the navigation pane. (The default domain settings are identical to those found when adding or editing a domain. For more information on these settings, refer to the Domains page.

You can make whatever changes you want to these settings, and any NEW domains that are added to the server will have these defaults applied for their users. However, it's also possible to change these settings, then push those settings to all domains.

Propagation

To apply selected default domain settings to all of the existing domains, do the following:

- First, make any changes you want on this page, then click the Save button.
- Next, click on the Propagate button. A modal window opens up.
- Scroll down the list of settings, placing a check mark next to the settings you want to push to your domains.
- Once you've selected your changes, click the Propagate button.

User Defaults

The job of the System Administrator is to make sure that the SmarterMail server runs as efficiently as possible. Part of that responsibility is putting measures in place to limit the potential for system abuses and "user error" that could cause problems.

SmarterMail gives System Administrators the ability to create a default template that's used as a starting point for all users of the mail server. This includes the ability to set size limits for mailboxes, delete email actions, set up throttling for users and more. These defaults can be set at any time and propagated to a single domain, multiple domains or all domains on the server. From here, Domain Admininstrators can futher lock down user accounts and set their own user limits.

User Defaults

To review the default configuration for new users, click on User Defaults in the navigation menu. (The default user settings are identical to those found when adding or editing a user. For more information on these settings, refer to the Managing Users page.).

You can make whatever changes you want to these settings, and any NEW domains that are added to the server will have these defaults applied for their users. However, it's also possible to change these settings, then push those settings to one or more domains, or to all domains.

Propagation

To apply some or all of the default user settings to some or all of the existing domains, do the following:

- First, make any changes you want on this page, then click the Save button.
- Next, click on the Propagate button. A modal window opens up.
- Scroll down the list of settings, placing a check mark next to the settings you want to push to your user(s).
- Once all items have been selected, you can pick how you want to propagate the changes:

- Specific Domains - Selecting this allows you to start entering the domains you want to propagate the changes to. These changes will only propagate to the domains you enter.
- All Domains - This will propagate the changes to all domains on the server.
- Once you've selected your changes, and added the specific domains you want to propagate the changes to, click the Propagate button.

NOTE: Simply making a change to the User Defaults doesn't automatically propagate, so a change to default settings does not change users that are already in place for any domain. They're only a user template any new domains that are added to the server. In order for changes to take effect, they must be propagated.

Impersonate User

There are times when a System Administrator will need to access domain or user specific information. SmarterMail uses impersonation to accomplish this goal. When you impersonate a user, you essentially log into their account as them without having to actually log in. This can be a useful method to examine settings or diagnose a problem directly.

To impersonate a user, do the following:

- Log into SmarterMail as a System Administrator, then click on the Manage icon.
- From the navigation pane, click on Impersonate User . A modal window opens.
- From the modal, select the Domain from the dropdown, then start typing the User's name. If you're already on the Configuration tab for a domain, that domain's name will automatically populate the Domain dropdown in the modal. (However, you can change this if needed.) When you start typign the User's name, SmarterMail should offer some autocomplete options. You can select one of those options or finish typing out the User's name.
- Once you've selected the Domain and User, click the Impersonate button. A new window will open and you'll be logged in as that user. By default, you'll be placed in that User's Settings.
- You can tell you're impersonating an account as an orange "Impersonating" flag is displayed in the upper, right corner of the SmarterMail interface.
- To exit impersonation, you can either log out of the impersonated account or simply close the browser window.

Once impersonating, you are able to edit user/domain settings, content filters, or whatever other part of the account that needs to be changed or reviewed.

Alternatively, you can impersonate a user by going to a Domain's Accounts tab, right clicking on a user and selecting Impersonate User from the context menu.

Changing Impersonated Users

It's also possible to change the User you're impersonating, or even change the domain and user, from the Impersonating window. Simply click the orange Impersonating flag in the upper right corner of the interface and a new Impersonate User modal window opens. Here, you can change the domain or user you want to impersonate and, by clicking the Impersonate button, change to that user or to a new domain and user.

Note: Only the primary System Administrator has impersonation privileges by default. If you are logged in as a secondary System Administrator and do not see the Impersonate User menu item in the Navigation pane, then impersonation privileges have not been enabled for your account. Please contact your primary System Administrator to request to have "Allow Impersonation" and, in addition, "Allow domain management" enabled for your account.

Troubleshooting

SmarterMail makes managing the mail server a breeze by isolating the monitoring and management aspects from the setup and configuration. In the Troubleshooting section, Administrators can access settings, tools and dashboards that will help them better understand what's occurring on their mail server and quickly take action while troubleshooting any issues that may arise.

A major part of troubleshooting issues is logging. By default, SmarterMail logs virtually every process and protocol available within the system. Having these logs means that, when issues DO occur, administrators can quickly and easily find out the what's going on and get the problems resolved. If nothing else, having access to logs makes working with SmarterTools much easier as it gives our support agents access to information that can then be used to further find and fix issues, or work with our developers to figure out what's going on so a fix can be implemented.

That said, logs CAN take up space on a server. By default, most of SmarterMail's log levels will be defaulted to "Exceptions Only". This means that the logs will capture and write out errors but not details. This keeps the log files small. At the other end of the spectrum, Detailed keeps the most amount of information available, but also means the log files can get quite large, quite quickly. However, this gives admininstrators the most information possible to help find the root cause of a problem.

To access standard troubleshooting tools, log in to SmarterMail as a System Administrator and click on Troubleshooting in the navigation pane. Within this section, System Administrators can access the following items:

Jump To:

- Options - Configure the log and indexing settings for the server
- View Logs - Review the logs to look for errors or monitor recent activity
- Services - Enable or disable specific services, including IMAP, SMTP, etc.
- Mailbox Indexing - View the status of user indexing occurring on the server
- Mailbox Migration - View the mailbox migrations occurring on the server

Options

Use this section to manage how the logs are written and to customize the indexing configuration:

Log Files

- Compress Log Files After - The number of days after which log files are automatically compressed. This preserves existing log files but also saves server space.
- Delete Log Files After - The number of days after which log files are automatically deleted. To enable this automatic deletion of log files.
- Debug Log IDs (one per line) - This section should only be used when instructed by SmarterTools Support. In order to better troubleshoot an issue within SmarterMail, SmarterTools Support may require additional logging. In this section, Debug Log IDs can be entered. Entering a log ID in this box will create a separate log file which will contain information Support needs for troubleshooting.

Protocol Logging

By default, SmarterMail sets all log detail levels to Exceptions Only. Use this section to adjust the log detail levels for the protocols used with SmarterMail. When set to Exception Only, SmarterMail will produce small-sized logs that record only errors. When set to Normal, SmarterMail will produce medium-sized logs that record most activity taken on the mail server. When set to Detailed, SmarterMail will produce log files that can get very large and contain extensive logging. Only change logs to Detailed when asked to by SmarterTools Support or when troubleshooting server operations.

The following log file types can be adjusted:

- EAS - The log level for EAS connections. Useful for helping find issues with things like why a user on an iPhone is having an issue syncing their calendar properly, etc.
- Autodiscover - The log level for Autodiscover. Useful for helping figure out why a particular user can't automatically connect their account to an email client.
- EWS - The log level for EWS sessions. Useful for helping find issues trying to connect an account to a client such as Apple Mail.
- IMAP - The log level for IMAP sessions. Useful for helping to figure out why a client can't connect to any email client that supports IMAP.
- LDAP - The log level for LDAP sessions. Useful for helping find issues when using Active Directory as an authention method.
- MAPI - The log level for MAPI sessions. Useful for helping find issues trying to connect an account to a client such as Microsoft Outlook 2019 for Windows.
- POP - The log level for POP sessions. Useful for helping to figure out why a client can't connect to any email client that supports IMAP.
- Sharepoint - The log level for Sharepoint Sync (Add to Outlook). Useful for helping to figure out why a client can't connect to any email client that supports Sharepoing Sync.
- SMTP - The log level for SMTP sessions. Useful for helping figure out why a message wasn't delivered to a recipient, and helps ensure the message was, in fact, sent by the user.
- WebDAV - The log level for CalDav and CardDav sessions. Useful for helping to figure out why a calendar or contacts app can't connect to any email client that supports CalDAV or CardDAV.
- XMPP - The log level for Live Chat and Team Workspaces. Useful for helping with issues such as a user that is unable to connect their account to a live chat client.

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

Process Logging

By default, SmarterMail sets all log detail levels to Exceptions Only. Use this section to adjust the log detail levels for common processed within SmarterMail. When set to Exception Only, SmarterMail will produce small-sized logs that record only errors. When set to Normal, SmarterMail will produce medium-sized logs that record most activity taken on the mail server. When set to Detailed, SmarterMail will produce log files that can get very large and contain extensive logging. Only change logs to Detailed when asked to by SmarterTools Support or when troubleshooting server operations.

Process Logging can help administrators in a number of ways. For example:

- Delivery Logs can help find out what happened to a particular message: if it was delivered, if it was delivered but rejected due to spam rules, whether it was moved based on a content filter, etc.
- SMTP Logs can show why a message was rejected by the recipient's mail server.
- Administrative Logs can show when a setting was changed, and which system administrator made the change.

The following log file types can be adjusted:

- Administrative - The log level for for any changes and/or modifications made by system administrator accounts.
- API Service - The log level for web service calls using SmarterMail's API.
- Calendars - The log level for calendar appointments.
- Content Filtering - The log level for any changes made due to Content Filtering rules.
- Delivery - The log level for message delivery and spool operations.
- Error - The log log for capturing any Errors returned by SmarterMail.
- Events - The log level for event sessions put in place for the system or user.
- Folder Auto-Clean - The log level for any folder auto-clean rules in place for the system or user.
- IIS - The log level for IIS sessions. This can be helpful for diagnosing issues with the SmarterMail website, app pool, etc.
- IMAP Retrieval - The log level for IMAP retrieval sessions.
- Indexing - The log level for SmarterMail indexing.
- Licensing - The log level for any Licensing issues, such as activation issues.
- Mailbox Importing - The log level for data imported during mailbox migrations.
- Mailing Lists - The log level for items pertaining to Mailing Lists.
- Maintenance - The log level for maintenance tasks performed by SmarterMail.
- Message-ID - The log level for logging Message-ID's of all messages sent to mailing lists.

- POP Retrieval - The log level for POP retrieval sessions.
- Spam Checks - The log level for all Spam Checks set up and in use.

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

Indexing

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

- Max Threads - The maximum number of threads to use for search indexing. Increasing this value will cause SmarterMail to use more CPU, but will allow the system to simultaneously index more users. (By default, this value is set to 2 less than the server's processing count. For example, if your server has 32 processors, this value will be set to 30.) Please note that this value cannot be set to 0.
- Segment Count Before Optimizing - The number of segment counts in an index before the index is reorganized. Increasing this number will increase file counts per mailbox, but will use less CPU. (By default, this value is set to 100.)
- Items Before Garbage Collection - The number of indexed items across the server before freeing as much memory as possible. Increasing this number will increase memory usage and lower CPU usage. (By default, this value is set to 5000.)
- Items to Index Per Pass - The number of items to index per user per index attempt. Increasing this number will increase memory usage and decrease the time it takes to index one user. However, it will increase the length of time it takes to index many small users if there are a few large users. (By default, this value is set to 2500.)
- Seconds In Queue Before Indexing - The amount of time a user must be in the indexing queue before being indexed. This setting provides a buffer for many changes to a mailbox to ensure the same user is not indexed multiple times. Increasing this number will cause search results to be delayed further, but will result in indexing heavier users less frequently. (By default, this value is set to 60.)
- Deleted Items Before Optimizing - The number of items that will be removed from the index before an optimization will occur. Increasing this number will slow search results. Decreasing this number will increase CPU and disk usage, but will increase search result speed. (By default, this value is set to 2000.)

MAPI Debug Captures can help diagnose issues users face when using MAPI to connect their SmarterMail accounts to Microsoft Outlook. They can also assist SmarterTools Technical Support Agents and/or Developers troubleshoot issues if support tickets are required. There are a few settings to enable if you want to start the debug logging:

- Stop logging after X requests - This is the total number of MAPI requests to save in the log. 5000 is a decent number as it provides a good amount of information, but doesn't create a log that takes up a lot of disk space.
- User to monitor - This is the email address of the user you want to help debug.

After a user has been added, and a debug log captured, it's possible to turn off the monitor. After a page refresh, a download link will appear for the log so it can be downloaded and reviewed or sent to SmarterTools in a support ticket. --%>

View Logs

Use this section to quickly view the server's log files. Viewing a server's log files, especially when it's possible to narrow down the type of server action or protocol that is being viewed, allows system administrators to look for any specific errors that could cause reliablity issues on the server or narrow down reasons why a specific behavior is being seen. For example, system administrators can review SMTP logs to see if an email was delivered or check ActiveSync logs to see if they can narrow down synchronization issues between a specific user's mailbox and their mobile device.

When viewing the SmarterMail logs, the following search strings will be available:

- Start and End - The start and end dates for the log files you want to view.
- Type - The type of log file that you would like to view.
- Search - Type the words or phrases should be contained in the log files that SmarterMail returns.
- Type - When searching the logs, you can choose whether to display only lines that match the search definitions or to display related traffic as well. Change this selection from Only Matching Rows to Display Related Traffic in order to display extra data that occurred within the same session.

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

To download the entire log file in a .zip format -- NOT just search results -- click on Download . This allows you to get quick access to a domain's entire log file so that it can be reviewed more thoroughly

on a local machine. If you only need the search results, click on Copy to Clipboard to copy the results to your clipboard, then past those results into your favorite text editor. (We recommend Notepad ++)

Services

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

The following services can be enabled or disabled on the server:

- IMAP - A client/server protocol in which email is received and held by the mail server. IMAP requires continual access to the client during the time that it is working with the mail server.
- IMAP Retrieval - With IMAP retrieval, mail is retrieved from external IMAP servers (e.g., another mail server like GMail) and saved in a mailbox on the mail server.
- Indexing - Indexes messages, contacts, calendars, tasks and notes so that users can search for specific mailbox items via the Web interface.
- LDAP (Enterprise Edition Only) - A communication protocol for accessing online directory services. Programs like Outlook and Thunderbird use LDAP to retrieve contact lists from SmarterMail. SmarterMail will validate email addresses for user accounts, aliases, and mailing lists.
- POP - An email protocol in which mail is saved in a mailbox on the mail server. When the end user reads the mail, it is immediately downloaded to the client computer and is no longer maintained on the mail server.
- POP Retrieval - Similar to IMAP Retrieval, with POP retrieval, mail is retrieved from external POP3 servers and saved in a mailbox on the mail server.
- SMTP - A TCP/IP (Internet) protocol used for sending and receiving email. 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 email and either POP or IMAP for receiving messages from their local server.
- Spool - The internal message queue used to deliver messages locally and to remote services.
- XMPP (Enterprise Edition Only) - An open-source IM protocol designed to allow

interoperability between different IM client programs. SmarterMail uses this protocol to power its chat functionality in the Web interface and/or third-party chat clients.

To modify the status of a service, select the desired service and click Start or Stop .

Mailbox Indexing

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

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

Mailbox Migrations

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

That being said, users can do this on their own, with little input from a SmarterMail System Administrator. While this normally is not an issue, there are times when an Administrator may need to stop a migration altogether. That's where the Mailbox Migrations page comes in.

The following details can be seen for each entry in the list:

- Email Address - The email address of the user performing the migration.
- Status - The status of the migration being performed. The status displayed will be one of the following:

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

To end the selected user's migration, select the user and click on the Actions (...) button and select End Session . The migration will be stopped, regardless of where it is in process. Mailbox migrations are an "all or nothing" proposition. If a migration is stopped in the middle, none of the migration steps will be finalized, unless the migration showed as "Completed."

For more information on the Mailbox Migration proces, including the fields necessary for different migration types, see the Migrating a Mailbox section of a User's Connectivity settings.
• In addition, if there are issues with a migration, SmarterMail logs all migration activity. Therefore, a System Administrator can check the Mailbox Importing logs for an account to see what happened, and find a resolution.

Reports

Reports Overview

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

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

System Admin Dashboards

SmarterMail includes several detailed, real-time performance dashboards that supply system administrators with important, on-demand statistics about their server as a whole as well as information on the traffic coming into and going out of, their servers.

Each card, on each dashboard, represents an overview of a specific metric. Clicking on the card takes system administrators to the overall report that gives a more detailed breakdown of what is being displayed. The exception is the general Dashboard, which gives overall information that doesn't have a specific report associated to the metrics shown.

The Dashboards available include:

Dashboard

The first dashbord covers general information on server hardware performance and the mail service. Cards include:

- Service Uptime
- DNS Cache Utilization
- Memory Usage
- Protocol Activity
- CPU Usage

- Messages in Spool
- Drive Statistics

Protocol

This dashboard provides information on message traffic and bandwidth usage across the server, as well as statitics for SMTP, IMAP and POP. Clicking on an individual card opens up the report for that specific item. Cards include:

- Bandwidth Overview
- Message Traffic
- Inbound Messages
- Message Bandwidth
- Throttled Messages
- SMTP Out Sessions
- SMTP In Sessions
- IMAP Sessions
- POP Sessions

Server Health

This dashboard provides information on server hardware and performance. Clicking on an individual card opens up the report for that specific item. Cards include:

- Average Hardware Usage
- Drive Average Statistics

Security

This dashboard provides information on security-related items such as viruses, abuse detection and more. Clicking on an individual card opens up the report for that specific item. Cards include:

- Connections
- IDS Violations
- ClamAV
- Cyren Zero-hour Outbreak Detection
- Viruses Caught

Note: Some Dashboard reports are only active on current data. For example, Service Uptime and Disk Average Statistics. Once a service reboots, the current data showing in the report would be lost, or changed, as these statistics are stored in memory only and not stored to disk.

Administrators

SmarterMail allows a single installation to have multiple System Administrator logins, each with their own unique login and password. To add secondary System Administrator accounts, log in to SmarterMail as the primary System Administrator and click on the Settings icon. Then click on Administrators in the navigation pane.

Once the page loads, you'll see a list of the Administrators that are set up for the SmarterMail installation. Initially, there will be a single "Primary" Administrator showing. As new administrative accounts are created, they will also be displayed. By default, the following columns are displayed:

- Account - The login name associated with the account.
- Name - The friendly name associated with the account.
- Type - The account type: Primary Administrator or Administrator.
- Manage Admins - If the administrative account has been granted permissions to create/manage other administrative accounts, a check box will appear next to their name.
- IP Restrictions - If the administrative account is restricted to connecting from a specific IP address, or an IP range, a check box will appear next to their name.
- Created - The creation date/time of the administrative account.
- Enabled - Whether the specific Account is able to be used or not. No checkmark means the Account has been disabled.
- Last Login - The date/time the specific Account was logged into.

To create a new Administrator account, click the New button. Note: Only the primary Administrator and secondary Administrators with 'Manage secondary administrators' permission can create new or modify existing accounts. When adding or editing an account, the following settings will be available:

Options

- Username - The identifier used to log in to SmarterMail.
- New Password - The password used to log in to Smartermail.
- Confirm Password - Re-type the password used to log in to Smartermail.
- Display Name - A friendly name for the administrator. For example, "Dan Henderson".
- Status - Enabled or Disabled.
- Theme - The general color theme of the SmarterMail interface: Light or Dark.
- Allow system settings management - Select this option to allow the Administrator to manage the settings for the SmarterMail server. (E.g., all of the options available in the Settings area.) Some System Administrator accounts may only require the ability to manage the domains on the server, but not server settings as a whole. If this is not enabled, the Settings icon is

essentially "turned off" for this System Administrator and does not show up when they log in.
• Manage secondary administrators - Select this option to allow the Adminstrator to create new and modify existing administrator accounts. This setting is dependent on "Allow system settings management", so if that is disabled, this setting is as well. A System Administrator is not able to manage secondary administrators if they do NOT have the ability to manage system settings.
• Allow domain management - There are times when an administrator may need to access domain or user specific information. Select this option to allow the Administrator to view/manage domains and domain users. If this is not enabled, the Manage icon is essentially "turned off" for this System Administrator and does not show up when they log in.
• Allow impersonation - Select this option to allow the Administrator to impersonate a user account. Impersonating an account opens a new browser session that allows an Administrator to be "logged in" as that user.
• Allow show passwords while impersonating - User passwords are hidden, by default. Select this option to allow an Administrator with impersonation permissions to also view the passwords associated with user accounts. This option also allows the Administrator to retrieve passwords via the API. Note: The primary system administrator can view and retrieve user account passwords and app passwords by default. In addition, when using Active Directory authentication, passwords are NOT displayed.
• Restrict login access by IP - Select this option to only allow the administrator to log in from certain IP addresses. Then enter the authorized IP address(es) on the IP Restrictions card.

IP Retrictions

If an Administrator has "Restrict login access by IP" enabled for their account, this is where you add any IP addresses that are allowed access to the SmarterMail server.

Change Password

Administrators can reset their account password at any time by logging into the web interface. In addition, the primary System Administrator and Administrators with "Manage secondary administrators" permission can modify another Administrator's password. To modify an Administrator password, select the Administrator and click the Change Password button. Then enter and confirm the new password that will be used. Note: Secondary Administrators cannot modify the primary Administrator's account.

Primary Administrators who cannot remember their account password can find instructions to reset their username and password in the SmarterTools Knowledge Base .

Antispam

Antispam Options

SmarterMail comes equipped with a number of antispam features and functions that allow you to be as aggressive as you want when combatting spam. Default antispam settings were configured during installation, but these settings can be modified at any time.

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

An added benefit to SmarterMail's antispam administration is the ability to combat both inbound and outbound spam messages. Most mail servers only allow Administrators to keep spam from entering the mail server. SmarterMail helps protect mail users from inbound spam but also keeps mail servers from actually sending spam, thereby helping to protect the mail servers from being blacklisted.

To view the antispam options for your server, log in to SmarterMail as an Administrator and click on the Settings icon. Then click on Antispam in the navigation pane. On the Options tab, the following settings will be available:

Jump To:

- Import/Export Settings - Import or export a JSON file containing a server's antispam configuration
- Reset Antispam Settings - Reset the antispam options and spam checks to the default configuration
- Filtering - Define the weight thresholds and default actions for each spam level.
- Trusted Senders - Exempt specific email addresses or domains from spam filtering.
- SMTP Blocking - Configure the thresholds for blocking inbount and outbound spam messages

- Options - Adjust basic options relating to the processing of spam and the ability for individual domains to override system-level settings.
- Greylisting Options - Temporarily reject email from unrecognized senders.
- SpamAssassin Servers - Configure a SpamAssassin server for identifying and reporting spam.

Import or Export Spam Settings

SmarterMail can export all global spam settings as a single JSON file then allows that JSON file to be imported to other SmarterMail servers as needed. This means System Administrators can configure a solid set of antispam rules on one server, then easily move those settings over to any additional SmarterMail servers by importing the antispam JSON. Email administrators can even work together to create and share their antispam JSON files files, combining their experience and understanding to create the most reliable settings available.

It's important to note that the spamConfig.json file is not actually part of the SmarterMail system files -- it's generated during export by pulling individual spam settings from the Settings.json file. These settings are then merged with existing Settings.json files when the spamConfig.json file is imported. Therefore, spamConfig.json files can only be shared between servers running the same version of SmarterMail.

To import or export SmarterMail's spamConfig.json file, click on the Actions (...) button. Then click on Import Spam Settings or Export Spam Settings accordingly. When importing spam configurations, custom rules in the JSON will be merged with existing rules in SmarterMail; the imported JSON will not replace all existing rules. For example, if you import an JSON from another system, it will simply add any custom spam checks, RBLs and URIBLs that do not exist in SmarterMail. If you prefer that all existing rules are overwritten, you must delete those rules prior to importing.

Reset Antispam Settings

SmarterMail's antispam configuration can easily be reset to the default configuration by clicking on the Actions (...) button and selecting Reset Antispam Settings . Note that this reset will impact ALL sections of the Antispam area, with the exception of IP Bypasses. Resetting the antispam options will revert all settings on the Options tab, Spam Checks tab, RBLs tab, URIBLs tab, and Greylist Filters tab to their default configuration. This means all trusted senders and domains, SpamAssassin servers, custom spam checks/RBLs/URIBLs and greylist filters will be deleted. To confirm that you would like to erase all customized antispam options, click Reset on the confirmation modal.

Filtering

Emails are filtered into one of three categories based on their total weight: Low Probability of Being Spam, Medium Probability of Being Spam and High Probability of Being Spam. For example, if an email's spam weight is equal to or higher than a certain category, then it is assigned that probability of being spam. Use this section to define the weight thresholds and the default actions at each level.

- Allow domains to override spam settings - Many Domain Administrators have their own preference of how potential spam email should be handled for their domain. Enable this to allow

them to override the spam filtering actions, if they wish. NOTE: Enabling this will NOT allow Domain Administrators to manage the spam Weights -- they can only manage how they want messages flagged as spam, based on the weights set by the System Administrator, to be handled.

• Action - The action to take when a message ends up with this level of spam probability: No Action, Delete Message, Move to Junk Email Folder or Add Text to Subject. Note: The Delete Message action will permanently delete messages that match the corresponding weight, preventing them from reaching the user's mailbox. Exercise caution when selecting this action, as messages deleted via spam filtering cannot be recovered.
• Text to Add - If the Action is set to Add Text to Subject, enter the text that will be appended to the beginning of a subject when a message reaches a particular level of spam.
• Weight - The email is sorted into probability levels based on the weight threshold values. Adjust the weight threshold according to the probability status selected.

Trusted Senders

Use this section to globally exempt specific email addresses (such as jsmith@example.com) or domains (such as example.com) from SmarterMail's spam filtering. This lets the system know that these messages come from a trusted source and can prevent mail from friends, business associates and mailing lists from being blocked or sent to the Junk Email folder. By default, every contact in a user's Contacts list is considered a trusted sender and bypasses spam filtering.

Note: If SPF and DKIM spam checks are enabled, SmarterMail will run those checks on ALL emails, including those from trusted senders. Because anyone can write any return path that they want when sending a message, this extra check helps prevent spammers from flooding users with hundreds of messages that aren't truly from a trusted sender. If the SPF and DKIM weights on a message from a trusted sender meet the Low, Medium or High spam filtering threshold, the corresponding spam filtering action (Move to Junk Email Folder, Delete Message, Add Text to Subject) will be performed on that email, despite the email coming from a trusted sender.

When entering trusted senders or domains, enter only one item per line.

SMTP Blocking

The idea behind SMTP blocking of inbound and outbound email is to filter out spam messages before they can be delivered. With SMTP Blocking enabled, messages that are rejected don't even hit the spool. That means that they can't be delivered, but it also means they bypass any other function, like content filtering and even message archiving: messages rejected due to SMTP blocks simply don't exist to SmarterMail, so they aren't processed in any way by the server. Therefore, it's important to exercise caution when enabling SMTP Blocking as rejected messages can not be recovered.

Regarding the weight calculation, when setting up your Spam Checks, RBLs and URIBLs you have the ability to enable each of those for Inbound and/or Outbound SMTP. When enabled for either inbound or outbound, SmarterMail uses the weights associated with those various checks when determining whether a message should be blocked at the SMTP level or not.

For example, imagine you have four spam checks enabled for Inbound SMTP blocking and each of those spam checks have a weight of 10. If the Inbound Weight Threshold is set to 30, that means incoming messages will be rejected if they fail at least three of the four spam checks.

- Inbound Weight Threshold - By enabling this field, an inbound email must have a total spam weight score of this value or higher in order to be blocked. The score is established by the settings on the Spam Checks, RBLs and URIBLs tabs. (By default, this threshold is set to 50 and is enabled.)
- Greylist Weight Threshold - By enabling this field, an inbound email must have a total spam weight score of this value or higher in order to be greylisted. The score is established by the settings on the Spam Checks, RBLs and URIBLs tabs. (By default, this threshold is set to 30 and is disabled.)
- Outbound Weight Threshold - By enabling this field, an outbound email must have a total spam weight score of this value or higher in order to be blocked. The score is established by the settings on the Spam Checks, RBLs and URIBLs tabs. (By default, this threshold is set to 30 and is disabled.)
- Outbound Block Action - This setting is used in conjunction with the Outbound Weight Threshold and allows administrators to quarantine outgoing messages that have met the specified spam weight threshold or block them entirely. When Quarantine Message is selected, messages are quarantined for 30 days. (The quarantine period cannot be changed.) The quarantine can be found by clicking on the Manage icon, clicking on Spool in the navigation pane, then selecting the Spam Quarantine tab.
- Bounce messages when blocked by Outbound SMTP Blocking - Enable this to send a user a bounce email notification when their outbound message has not been sent due to its spam probability.

Options

- Autoresponders - This setting allows you to add restrictions to a user's ability to create or send autoresponders outside of the domain. (Autoresponders sent locally, to others on your domain, are not affected by these settings.) Certain antispam organizations will block servers that autorespond to spam traps. To reduce the possibility of this occurring, set the autoresponder option to be as restrictive as your clients will permit:

• Enabled - Users' autoresponder messages will be sent without any restrictions.
• Disabled - Users will not have the ability to configure an autoresponder.
• Require message pass SPF - A user's autoresponder will not be sent if the original sender's message failed the SPF spam check or if the sender's SPF record is not configured. Note that this setting won't impact the ability for an incoming message to be delivered to your users. It will only prevent the user's autoresponder from being sent if the original sender's SPF record is not configured or if the SPF check has failed. Note: The SPF spam check must be enabled for spool filtering in order for this setting to work as intended. If the SPF check is disabled, and this setting is enabled, autoresponder messages will not be sent. (By default, this option is selected.)
• Require message pass SPF if SPF record exists - A user's autoresponder will not be sent if the original sender's message failed the SPF spam check. Note that this setting won't impact the ability for an incoming message to be delivered to your users. It will only prevent the user's autoresponder from being sent if the original sender's SPF check fails. (This option is distinguishable from the option above as it will only impact messages where the SPF record IS configured and fails the check. If the original sender doesn't have SPF configured, the autoresponder message will be sent.) Note: The SPF spam check must be enabled for spool filtering in order for this setting to work as intended. If the SPF check is disabled, and this setting is enabled, autoresponder messages will not be sent.
• Content Filter Bouncing - This setting allows you to add restrictions to the content filter action 'Bounce message'. Certain antispam organizations will block servers that send bounce messages back to spam traps. To reduce the possibility of this occurring, set the autoresponder option to be as restrictive as your clients will permit:

• Require message pass SPF - An incoming message that triggers the content filter will not have the bounce message sent if the original sender's message failed the SPF spam check or if the sender's SPF record is not configured. Note that this setting won't impact the ability for an incoming message to be delivered to your users. It will only prevent the bounce message from being sent if the original sender's SPF record is not configured or if the SPF check has failed. Note: The SPF spam check must be enabled for spool filtering in order for this setting to work as intended. If the SPF check is disabled, and this setting is enabled, bounce messages via content filtering will not be sent. (By default, this option is selected.)
• Require message pass SPF if SPF record exists - An incoming message that triggers the content filter will not have the bounce message sent if the original sender's message failed the SPF spam check. Note that this setting won't impact the ability for an incoming message to be delivered to your users. It will only prevent the bounce message from being sent if the original sender's SPF check fails. (This option is distinguishable from the option above as it will only impact messages where the SPF record IS configured and fails the check. If the original sender

doesn't have SPF configured, the bounce message will be sent.) Note: The SPF spam check must be enabled for spool filtering in order for this setting to work as intended. If the SPF check is disabled, and this setting is enabled, bounce messages via content filtering will not be sent.
• Max message size to content scan (KB) - The maximum message size for which content-based spam checks will run. Content-based spam checks include SpamAssassin-based Pattern Matching, Remote SpamAssassin, Cyren Premium Antispam and any custom rules. Note: Increasing this number will also increase the mail server's memory usage. (By default, this limit is set to 4096.)
• Enable spool proc folder - Enable this to have SmarterMail place messages into a Spool\Proc folder to be analyzed in the background, usually by third-party products such as Declude or custom-built applications. (By default, the location of the Proc folder is C:\SmarterMail\Spool\Proc.) While the messages are in the Proc folder, .hdr can manipulate elements of the message, such as edit, write, and add headers. Once the scan has been completed, the third-party app is responsible for moving the message back into the spool to be handled by SmarterMail from that point on. This option is most often necessary when using the third-party program, Declude. However, this setting can be used to prevent the disruption of mail flow with any other third-party app that manipulates messages.
• Enable catch-all accounts to send autoresponders and bounce messages - Enable this if you rely on auto-responders being sent when a message comes in through a catch-all. In general, this is a bad idea, so it should be left unchecked unless your situation specifically requires it.
• Enable SRS when forwarding messages - Enable this to allow the mail server to re-email (as opposed to "forward") an email message so that it passes any SPF checks on the recipient's end.
• Enable DMARC policy compliance check - Enable this to allow the mail server to check messages against the DMARC policy standard. For more information, see the DMARC website .

Greylisting Options

What is greylisting and how does it work?

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

customers receive. (Emails sent from whitelisted and authenticated senders willautomatically bypass greylisting and are delivered directly to the spool.)

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

Why use greylisting?

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

Disadvantages of greylisting

The biggest disadvantage of greylisting is the delay of legitimate email from servers not yet verified. This is especially apparent when a server attempts to verify a new user's identity by sending them a confirmation email. Some email servers will not attempt to re-deliver email or the re-delivery window is too short. Whitelisting can help resolve this.

Greylisting configuration options

- Block Period (Minutes) - The period of time that mail will not be accepted. The default 15 minutes.
- Pass Period (Minutes) - The period of time in which the sender's mail server has to retry sending the message. The default 360 minutes.
- Record Expiration (Days) - The period of time that the sender will remain immune from greylisting once it has passed. The default 36 days.
- Enable Greylisting - Select this option to enable greylisting.
- Allow users to override greylisting - Select this option to allow users to selectively turn off greylisting. This is useful if you have an account that receives time sensitive mail.

Note: The following cases are exempt from greylisting: SMTP Whitelisted IPs, IP Bypasses that are specified to skip greylisting, anyone who authenticates (includes SMTP Auth Bypass list), trusted senders (includes users' contacts), anyone who has already sent you an email (this list generates only

after greylisting has been enabled), any IP address or country code specified as being exempt in the Greylist Filters tab.

SpamAssassin Servers

SpamAssassin is a powerful, free mail filter used to identify spam. It utilizes a wide array of tools to identify and report spam, including header and text analysis, Bayesian filtering, DNS blocklists and collaborative filtering databases. To setup a SpamAssassin server, click New Server . The following options will be available:

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

Spam Checks, RBL and URIBL Lists

SmarterMail comes equipped with a number of antispam features and functions that allow you to be as aggressive as you want when combating spam. Default antispam settings were configured during installation, but these settings can be modified at any time.

Due to the flexible nature of SmarterMail's antispam setup, spam checks can influence the spam decision as much or little as you want. Each spam check has one or more associated weights. When spam protection runs on an email, all enabled spam checks are performed. The total weight of all spam checks is what comprises the final spam weight for the email. A spam probability level (Low, Medium or High) is then assigned to the email using the weights configured by the System Administrator on the Filtering card of the Options tab. Based on the email's total spam weight / probability of being spam, the corresponding spam filtering action is taken.

An added benefit to SmarterMail's antispam administration is the ability to combat both inbound and outbound spam messages. Most mail servers only allow administrators to keep spam from entering the mail server. SmarterMail helps protect mail users from inbound spam and also includes the added benefit of keeping mail servers from actually sending spam, thereby helping to protect the mail server from being blacklisted.

To view and modify the spam checks for your server, log in to SmarterMail as an Administrator and click on the Settings icon. Then click on Antispam in the navigation pane. The Spam Checks , RBLs and URIBLs tabs can be used to create or modify existing spam checks and RBLs for the system.

Note: Only enabled spam checks, RBLs and URIBLs are used when calculating spam weight. To enable or disable a check, enable the appropriate spam check in its configuration options.

Spam Checks

The Spam Checks tab shows all non-RBL/non-URIBL checks that are performed on a message. These checks can include licensed add-ons such as Cyren and Message Sniffer, as well as standard checks such as DKIM, SPF and more. Any of these checks can be enabled or disabled for Inbound and/or Outbound SMTP, and each can be edited or removed. To edit a check, simply click it to open its settings. To add a new Spam Check, such as adding in an antispam appliance, click the New button.

SmarterMail includes several spam checks by default. Each check is described in detail, below.

- Enable Spool Filtering - When enabled, the weight assigned for the spam check is added to the message and used as part of its overall spam score. SmarterMail then handles the message based on the spam settings configured for a domain.
- Enable Inbound SMTP blocking - This option is used in conjunction with the SMTP Blocking settings configured in Antispam Options . When enabled, this spam check is counted toward to weight threshold for the blocking of inbound emails. As SMTP blocks are done at the IP level and not based on message content, some spam checks do not offer SMTP blocking. If this option is not available, then that particular spam check does not offer SMTP blocking and must rely on content filtering instead.
- Enable Outbound SMTP blocking - This option is used in conjunction with the SMTP Blocking settings configured in Antispam Options . When enabled, this spam check is counted toward to weight threshold for the blocking of outbound emails. As SMTP blocks are done at the IP level and not based on message content, some spam checks do not offer SMTP blocking. If this option is not available, then that particular spam check does not offer SMTP blocking and must rely on content filtering instead.
- Weight - The weight range available for the spam check. Each spam check may utilize unique spam weight options. --%>

Creating Custom Rules

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

- Rule Name - The name of the rule.
- Rule Source - What you want the rule to be based on: a message's header, body text or raw content. When selecting "body text" or "raw content", you'll need to supply additional information that is applied to the Rule Text: whether the Source "contains" the information, whether the a wildcard is used for a range of information or whether you want to supply a

regular expression. If you select Header you will need to supply header details separately from the Rule Text.

• Rule Text - The text that will be used in conjunction with the Rule Source. For example, if you use create a Rule Source based on Body, then an additional Rule Source for "Contains", Rule Text can include words such as "Cialis", "Viagra", etc.

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

• Enable Spool Filtering - See above for details.

• Enable Outbound SMTP Blocking - See above for details.

Cyren Premium Antispam

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

• Enable Spool Filtering - See above for details.

• Enable Outbound SMTP Blocking - See above for details.

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

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

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

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

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

Declude

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

- Low Spam Weight - The weight that will be assigned if Declude determines a low probability of spam.
- Medium Spam Weight - The weight that will be assigned if Declude determines a medium probability of spam.
- High Spam Weight - The weight that will be assigned if Declude determines a high probability of spam.

DKIM and DomainKeys

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

- Enable Spool Filtering - See above for details.
- Pass Weight - Indicates that the email sender and message integrity were successfully verified (less likely spam). The weight you set may be 0 (for no effect) or a negative number, thereby reducing the spam rating.
- Fail Weight - Indicates that the email sender and message integrity verifications failed (most likely spam). Set this to a relatively high weight, as the probability that the email was spoofed is very high.
- None Weight - Indicates that there was not a valid DomainKey/DKIM signature found to validate the sender and message integrity. Except in very special circumstances, leave this set to 0.
- Max message size to verify - The maximum inbound message size you want the mail server to verify.

Honey Pot

A "honey pot" spam check derives its name because implementing it can attract spammers -- or, more likely, spam bots -- like "bees to honey." Basically, a system administrator populates the honey pot spam check with email addresses that are designed to be seen by, or otherwise used by, spammers. These addresses can be commonly used addresses that spammers will automatically target such as admin@your-domain.com, info@your-domain.com, hr@your-domain.com, etc. These types of addresses are commonly targeted, but SHOULD NOT be addresses that are actually used by any user of a given domain. You don't want to add admin@your-domain.com IF that is an actual address used BY a user on that domain. In fact, any addresses added as honey pot addresses DO NOT need to be an actual account. So if you DO use admin@yourdomain.com as a honey pot address, you do NOT need

to add that as an actual account TO the domain. In addition, there's no limit to the number of addresses you can add. It's totally up to the system admin.

Another common way to instantiate a honey pot spam check is to add a hidden email address to a form used on a website. Spam bots can scrape email address from these forms, then populate spam lists that are used by, or potentially sold to, spammers. By adding in a hidden (using CSS) honey pot email address to a form, you can essentially trick these bots into scraping that email address, then block any sender who uses the address.

Regardless of HOW you set your trap, honey pots can be a simple, yet effective, way of finding, scoring and then disposing of email spam for your users as well as blocking sending IP addresses.

- Enable Spool Filtering - See above for details.
- Reject found entries at SMTP level - Enabling this will automatically reject the message prior to it being delivered if the IP of the sending mail server has already been listed. NOTE: This will occur as long as the IP is not whitelisted, is not a gateway and is not IP Bypassed.
- Pass Weight - The weight you set may be 0 (for no effect) or a negative number, thereby reducing the spam rating. (Setting negative numbers is not recommended.)
- Listed Weight - This is the weight that is assigned to a message sent from an IP address that was already part of the honey pot.
- Triggered Weight - This is the weight that is assigned to a message that is sent to one of your Honey Pot Addresses. The email address must match one in the list of Honey Pot Addresses for this weight to be added to the message.
- Honey Pot Addresses - These are the actual, full email addresses you're targeting for use by spammers. For example, generic email addresses can be used such as info@example.com or contact@example.com. These should NOT be actual email addresses that are used by anyone on any domain. Ideally, they're addresses that are general enough that spammers would target them with blanket spam attacks, but not addresses that are posted anywhere or used to actually send email. They are explictly to be used ONLY for trapping potential spammers.

Message Sniffer

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

- Enable Spool Filtering - See above for details.
- Enable Outbound SMTP Blocking - See above for details.
- Confirmed Weight - The weight that will be assigned if Message Sniffer determines the

message as coming from known spam sources.

• None Weight - The weight that will be assigned if Message Sniffer deems the message is not spam.

Null Sender

A common spam technique is to send messages with missing, or "Null" sender values. That means that the message appears to come from no one as the sender details are blank. This check allows you to assign a spam weight to messages that meet this criteria.

• Enable Spool Filtering - See above for details.
• Enable Outbound SMTP Blocking - See above for details.
• Weight - The weight assigned to messages that fail this check.

Remote SpamAssassin

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

SmarterMail can use SpamAssassin with its weighting system:

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

Reverse DNS

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

- Enable Spool Filtering - See above for details.
- Enable Inbound SMTP Blocking - See above for details.
- Weight - The default weight for this spam check. If an email sender does not have a reverse DNS entry, this is the value that will be added to the message's total spam weight.
- Forward Confirm Fail Weight - Forward Confirm Reverse DNS means that an hostname has both forward and reverse DNS entries that utilize the same IP address. Using this check, SmarterMail checks the rDNS and fDNS and if there is no A record, the check fails.
- Forward Confirm Mismatch Weight - Using this check, SmarterMail checks the rDNS and fDNS and if the IPs exist, but don't match, the check fails.

SpamAssassin-Based Pattern Matching

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

- Enable Spool Filtering - See above for details.
- Enable Outbound SMTP Blocking - See above for details.
- Low Spam Weight - The weight that will be assigned if the pattern matching engine determines a low probability of spam.
- Medium Spam Weight - The weight that will be assigned if the pattern matching engine determines a medium probability of spam.
- High Spam Weight - The weight that will be assigned if the pattern matching engine determines a high probability of spam.
- Header Log Level - The amount of information the pattern matching engine inserts into the header of the message.

SPF (Sender Policy Framework)

SPF is a method of verifying that the sender of an email message went through the appropriate email server when sending. Therefore, as it's verifying the sending server, SPF is set up by the sending server's System Administrator or the domain owner as a DNS record. (More information can be found at DMARC Analyzer .) As more and more companies add SPF information to their domain DNS records, this check will prevent spoofing at an increasing rate.

• Enable Spool Filtering - See above for details.
• Enable Inbound SMTP Blocking - See above for details.
• Scan From header instead of Return Path - Enabling this means the check will use the From address for the SPF check as opposed to the message's RETURN-PATH, which is where NDRs (bounce messages) are sent. Many times spammers will spoof messages by changing the From address to make it appear like a message is coming from a legitimate person/organization even though the RETURN-PATH may be for the actual source of the message. While it is possible to spoof a message's RETURN-PATH, spoofing the From address is a much more common method used by spammers.
• Pass Weight - Indicates that the email was sent from the server specified by the SPF record (more likely good mail). The weight you set may be 0 (for no effect) or a negative number, thereby reducing the spam rating.
• Fail Weight - Indicates that the email was sent from a server prohibited by the SPF record (highly likely spam). Set this to a relatively high weight, as the probability that the email was spoofed is very high.
• SoftFail Weight - Indicates that the email was sent by a server that is questionable in the SPF record. This should either be set to 0 or a low spam weight.
• Neutral Weight - Indicates that the SPF record makes no statement for or against the server that sent the email. Except in very special circumstances, leave this set to 0.
• PermError Weight - Indicates that there is a syntax error in the SPF record. Since SPF is relatively new, some domains have published improperly formatted SPF records. It is recommended that you leave this at 0 until SPF becomes more widely adopted.
• None Weight - Indicates that the domain has no published SPF record. Since SPF is relatively new, many legitimate domains do not have SPF records. It is recommended that you leave this at 0 until SPF becomes more widely adopted.

RBLs and URIBLs

RBL lists (also known as IP4R Lists) and URIBL lists are publicly accessible lists of known spammer IP addresses. These lists can be a very important part of spam protection. To attach a list, navigate to the appropriate tab and then click New . Dependent on the list you’re adding, the following settings are available:

• Name - A friendly name for the list that will help you and your customers identify it.
• Description - This field allows you to store additional information about the list.
• Weight - The default weight for this spam check. If an email sender is listed with the spam list, this is the value that will be added to the message's total spam weight.
• Max Weight - The maximum weight that a single URIBL check can add to the message.

• Hostname - The hostname of the blacklist being added. For example, uribl.spameatingmonkey.net.
• Lookup Prefix - Many subscription-based RBLs and URIBLs require some type of authorization or login token to be added to the front of the RBL/URIBL. When using such a service, that token is entered here.
• Required Lookup Values - The expected value(s) returned from an RBL if the sender's IP is listed with the RBL provider. Note: Multiple lookup values may be entered, separated by a comma. These values are generally available from the RBL/URIBL provider in their set up documentation.
• Enable Spool Filtering - When enabled, the weight assigned for the spam check is added to the message and used as part of its overall spam score. SmarterMail then handles the message based on the spam settings configured for a domain.
• Enable Inbound SMTP blocking - This option is used in conjunction with the SMTP Blocking settings configured in Antispam Options . When enabled, this RBL/URIBL is counted toward the weight threshold for the blocking of inbound emails.
• Enable for Outbound SMTP blocking - This option is used in conjunction with the SMTP Blocking settings configured in Antispam Options . When enabled, this RBL/URIBL is counted toward the weight threshold for the blocking of outbound emails.
• Enable bitmap checking - Enable this option if the RBL supports bitmapping. Bitmap checking can be used for RBL's and URIBL's that support this kind of spam check. For example, SURBL utilizes a multi-blacklist check. For more information and documentation on the appropriate usage, please visit www.surbl.org/lists .

IP Bypasses

IP Bypasses allow a System Administrator to prevent spam checks and greylisting on email delivered from specific IP addresses. Typically, this functionality is used to enter the IP address of an inbound gateway. In incoming messages, SmarterMail will analyze the .EML file and pull the most recent IP Address from the header, which will usually be an organization's inbound gateway. Inputting that IP address on this page will allow SmarterMail to analyze the IP of the originating server rather than focusing on the gateway that SmarterMail received the message from. This is important because the majority of the time an organization's incoming gateway will not be listed on any RBL lists, but the originating server may be.

To access the IP Bypasses section, log in to SmarterMail as an Administrator and click on the Settings icon . Then click on Antispam in the navigation pane and click on the IP Bypasses tab . To add an IP Address or IP Range, click New .

- IP Addresses (single, range or CIDR block) - Enter the IP address or IP range that should be bypassed.
- Description - Enter a note for identifying the bypass.
- Bypass spam checks - Keep this option enabled in order to prevent spam checks on messages sent from the specified IPs.
- Bypass greylisting - Keep this option enabled in order to prevent greylisting on messages sent from the specified IPs.

Greylist Filters

SmarterMail's antispam options include greylisting, which is a very effective method of spam blocking that comes at a minimal price in terms of performance. When enabled, the system will keep track of the sending IP address, sending email address and recipient's email address for every message received. If an incoming message has a combination of a sending IP, sending address and recipient address that has not previously been seen, it will return a temporary failure to the sending server. This temporary failure essentially tells the sending server to “Try again later.” Valid servers will retry the email a short time later, at which point SmarterMail accepts the message. Spammers, on the other hand, typically create scripts that bombard your server with emails, and they rarely retry on temporary failures. When these messages are bounced back because of greylisting, they are typically not retried, therefore reducing the amount of spam that your customers receive.

In addition to the greylisting configuration on the Antispam | Options tab, Administrators can use Greylist Filters to prevent greylisting based on the sender's country or IP address. To access greylist filters, log in to SmarterMail as an Administrator and click on the Settings icon. Then click on Antispam in the navigation pane and click on the Greylist Filters tab. To add an IP address or country code, click New . To edit an existing filter, simply click on it from the list. The following options will be available:

- Filter Type - Select the type of filter you would like to add: IP Address or Country Code.
- IP Address - If the filter type is set to IP Address, enter the IP address that should bypass greylisting / be greylisted.
- Country - If the filter type is set to Country Code, select a country code from the list. The greylisting exception / limitation will apply to all messages that are identified as coming from an IP address matching that country.
- Description - The friendly name or descriptor you want to give to the IPs. For example, Office365 or Yahoo!

Note: Some greylist filters are included by default and cannot be modified or removed. These default filters are indicated in the grid by having a checkmark in the Internal column.

Recommended Antispam and Antivirus Settings

SmarterMail comes equipped with several industry-standard antispam options that can block up to 97% of all spam from entering or leaving the server and help keep mail systems running smoothly. These built-in protections include SPF, DKIM, reverse DNS, greylisting, pre-configured settings for multiple popular and effective RBLs and URIBLs, and more. However, when considering your spam configuration, it's important to remember that spam administration is not a "fire and forget" task. Using these built-in options requires constant tweaking to keep that level of effectiveness, and mail administrators will need to monitor incoming and outgoing spam as spammers frequently change their tactics. (Learn more about configuring the built-in antispam options below.)

In addition, SmarterMail comes equipped with industry-standard, and open source, antivirus protection using ClamAV. It also supports quarantining messages, and the ability to manage messages in the quarantine, an Events system for dealing with quarantined items and much more.

On top of the included options, SmarterMail supports third-party protections like:

- Cyren Premium Antispam
- Message Sniffer
- Declude
- Command-line antivirus
- Antispam appliances, such as Barracuda
- Many more

Paid add-ons like Message Sniffer, Cyren Premium Antispam, Cyren Zero Hour Antivirus and more can definitely come in handy. These third-party services act as additional spam and virus checks and may be worthwhile investments as a multi-tiered solution is the best course of action when it comes to dealing with spam and antivirus. Often times, users are not satisfied with 97% spam protection out-of-the-box -- keeping in mind that, at this level of protection, for every 100 messages a user receives per day, only 3 of these could be spam. Both Message Sniffer and Cyren will catch a higher percentage of spam than the default options, and better yet, neither require consistent updating by a SmarterMail System Administrator - updates are handled by the service provider. Using one of these services, or ideally both together, is easily the most effective option in battling spam.

Regarding antivirus, When proper antivirus solutions are in place within SmarterMail -- using ClamAV plus something like Cyren Zero Hour -- using an antivirus solution at the network level is not necessary. In fact, antivirus solutions at the network level can cause numerous issues for system administrators and/or users. Therefore, it is NOT recommended. That's because antivirus solutions at the network level can't relay information to SmarterMail in a reliable way. If a network antivirus

solution removes suspected virus attachments from an incoming email, the email will still be delivered to the recipient. However, while the message list will show that the email contains an attachment, no attachments will be available. Not only does this leave the user with no information regarding the missing attachments, it leaves them vulnerable to receiving, and perhaps responding to, email from malicious sources.

Below are some recommendations for the various spam settings SmarterMail has to offer. Please keep in mind that these are only suggestions. Administrators can, and should, keep an eye on these settings and adjust them as necessary to concoct a viable antispam solution for their end users.

SPAM CHECKS

In the Spam Checks, RBL Lists and URIBL Lists sections, you can enable individual spam checks for email spool filtering and inbound/outbound SMTP blocking. (Checks that are not available for inbound or outbound SMTP blocking are denoted with 'N/A'.) Each spam check comes with unique spams weights, which can be adjusted as desired.

Determining the weight values of each spam check depends on how accurately you believe that check identifies spam messages. If you're confident that it accurately identifies spam and has very few false positives, you would give its weight a higher value. If you are less confident in a spam check's accuracy, assign it a lower value. By configuring your spam checks this way, those that you have less confidence in will not cause a message to be marked as spam on its own. However, if multiple checks that you have lower confidence in all consider a message to be spam, their combined weights would likely cause the messages to be marked as spam. Find our recommended spam weight values below:

Cyren Premium Antispam

(Leave disabled if you do not have the Cyren add-on)

- Confirmed Weight = 30
- Bulk Weight = 10
- Suspect Weight = 10
- Unknown Weight = 0
- None Weight = 0

Message Sniffer

(Leave disabled if you do not have the Message Sniffer add-on)

- Confirmed Weight = 30
- None Weight = 0

Remote SpamAssassin SpamAssassin itself is a powerful, third party open source mail filter used to identify spam that can be easily used alongside, or in place of,

SmarterMail's spam settings. It utilizes a wide array of tools to identify and report spam.

DKIM

(DKIM is the primary mechanism for signing messages which proves to the receiving user that the message was not altered during transit and was sent from the signing domain. Not all valid messages are signed however so no spam weight should be given for no signature.)

- Pass Weight = 0
- Fail Weight = 10
- None Weight = 5
- Max message size to sign (MB) = 100
- Max message size to verify (MB) = 100

SPF

- Pass weight = 0 (Sender's IP is valid for sender's domain)
- Fail weight = 10 (Sender's IP is not valid for sender's domain)
- Soft Fail weight = 5 (Sender's IP is questionable for sender's domain)
- Neutral weight = 0 (No strong statement can be made for or against sender's IP)
- PermError weight = 5 (The SPF record could not be processed.)
- None weight = 5 (No SPF record has been configured.)

Reverse DNS

- Reverse DNS Fail Weight = 10
- Forward Confirm Fail Weight = 10
- Forward Confirm Mismatch Weight = 5

RBL: SpamCop

- Weight = 10

RBL: SpamHaus CSS

- Weight = 10

RBL: SpamHaus PBL

- Weight = 10

RBL: SpamHaus SBL

- Weight = 10
- Additional RBLs can be added and weights applied.

FILTERING

On the Filtering card within the Options tab, you can adjust the global actions taken on emails that are considered to be spam, based on one of three probabilities determined by their spam weights: Low Probability, Medium Probability and High Probability. If a weight is equal to or higher than a certain category, then it is assigned that probability of being spam and the corresponding action is taken. The defaults for Filtering are as follows:

Low Probability of Spam weight = 10

- Default Action: None

Medium Probability of Spam weight = 20

- Default Action: Move to Junk Email folder

High Probability of Spam weight = 30

- Default Action: Move to Junk Email folder

Once you are comfortable with your antispam settings and have a better understanding of the spam messages that impact your domain, you may wish to adjust these settings. For example, you may consider changing the default action on the Low Probability to Move to Junk Email folder or the High Probability to Delete Message. (IMPORTANT NOTE: Email that is deleted via spam filtering CANNOT be recovered.)

SMTP BLOCKING

On the SMTP Blocking card within the Options tab, you can access the configuration options for SMTP Blocking. The idea behind SMTP blocking of incoming and outgoing email is to filter out spam messages before they are delivered. For example, imagine you have six spam checks enabled for Incoming SMTP Blocking and each of those spam checks have a weight of 10. If the Incoming Weight Threshold is set to 50, that means messages being received via SMTP will be rejected if they fail five or all six of the spam checks. (Because SMTP blocks are done at the IP level and not based on message content, some spam checks do not offer incoming or outgoing SMTP blocking.)

Choosing which spam checks are used for Incoming/Outgoing SMTP Blocking is done on the Spam Checks, RBLs and URIBLs tabs. In order to actually enable the blocking feature, enable the corresponding weight threshold on the SMTP Blocking card. When an email arrives or is attempted to be sent that exceeds the threshold value, the email will be blocked and never delivered. Note: By default, the Incoming Weight Threshold is enabled and set to 50. This means that messages that have a spam weight of 50 will be blocked and deleted before they reach the spool. You can decrease that weight threshold once you have a better understanding of the spam that impacts your domain.

In addition to SMTP Blocking, this section also contains settings for the Outgoing Quarantine and Greylisting. If Outgoing Quarantine is enabled, SmarterMail will quarantine any outbound blocked messages for the specified time period. (If set to 'None,' messages are immediately deleted from the spool.) The Greylisting Threshold allows you to add extra options for what items get greylisted. If you prefer that messages with a high potential of spam are delayed, you can set the greylist weight threshold on the SMTP Blocking card. We recommend starting the threshold at 30 and decreasing to 20 if you're confident in your spam checks.

GREYLISTING

On the Greylisting Options card within the Options tab, you can enable greylisting. Greylisting is a popular method of fighting spam as it temporarily rejects unrecognized incoming emails that are not sent by whitelisted or authenticated users, effectively saying, "Try again later." Valid servers will retry the email a short time later, which would be permitted and delivered. Spammers, on the other hand, rarely retry on temporary failures, therefore reducing the amount of spam that customers receive. Find our recommended values below:

- Block Period = 3 minutes
- Pass Period = 360 minutes (6 hours)
- Record Expiration = 36 days

As part of the greylisting configuration, you can choose to greylist messages from everyone, greylist messages from the specified countries / IP addresses, or greylist messages from everyone except the specified countries / IP addresses. If the greylisting 'Applies To' is set to 'Only specified countries / IP addresses' or 'Everyone except specified countries / IP addresses', you use the Greylist Filters tab to add those exceptions / limitations.

Summary

When it comes to antispam and antivirus administration, it's important to keep in mind that spammers change their tactics often and each installation/setup is unique. What one person may consider the ideal spam configuration, others may find too restrictive. What works for one mail server, may not work for all. Discussing your configuration with other server administrators is a great way to get ideas flowing on what will work best for you. If you've still got more questions or want additional ideas on how to configure SmarterMail's antispam, please consider posting in the Community or reviewing one of the many threads discussing antispam topics.

Antivirus

SmarterMail supports multiple methods of antivirus protection for securing your mail server. The default installation includes, at no additional cost, effective and self-updating antivirus protection with ClamAV. SmarterMail also supports additional third-party solutions, including command-line antivirus solutions and Cyren Zero-hour Outbreak Detection. (Cyren Zero-hour Outbreak Detection is a paid SmarterMail add-on and can be licensed in 12-month subscriptions. Start a 30 day trial in the Licensing settings, or contact SmarterTools Sales for purchasing details.) In addition, SmarterMail has the ability to quarantine messages that are suspected as containing viruses, and, using system events, can respond to senders that attempted to send an email containing a virus.

To view the antivirus settings for your server, log in to SmarterMail as an Administrator and click on the Setting icon. Then click on Antivirus in the navigation pane. The following settings will be available:

Options

- Scan Inbound/Outbound Messages - This dropdown list allows you to specify the types of messages that will be scanned for the virus quarantine: messages coming into the server, leaving the server or both.

NOTE: The virus Qurantine Directory -- or Quarantine Path -- is part of the General Settings .

ClamAV

ClamAV is a third-party open source antivirus toolkit that is included, at no additional cost, in the default installation of SmarterMail. For more information on ClamAV, visit: www.clamav.com

Note: ClamAV's virus definitions are updated whenever the service starts and every 6 hours thereafter, and its last updated date/time is displayed on the card. To manually update the ClamAV definitions, click on the Actions (...) button and select Update ClamAV Definitions .

- Enable ClamAV - Enable this setting to use ClamAV.
- When Virus is Found - This dropdown allows you to select what you want done with a message if ClamAV detects it contains a virus. These options include:

- No Action - Do nothing with the message.
- Delete Message - Delete the entire message. Note: The Delete Message action will permanently delete messages, preventing them from reaching the user's mailbox. Exercise caution when selecting this action, as messages deleted via virus filtering cannot be recovered.
- Quarantine Message - Move the message to the quarantine folder on the server. These messages can then be found on the Virus Quarantine tab on the Spool page. By default,

messages remain in quarantine for 30 days, after which time the .eml is deleted, unless other action is taken to move the message out of quarantine.
• ClamAV is on a remote server - Enable this setting if the server is a remote server.
• IP Address - The IP address of the ClamAV server to use. When running ClamAV as part of the SmarterMail install, this will default to localhost. (127.0.0.1)
• Port - The port that the ClamAV server is listening on. When running ClamAV as part of the SmarterMail install, this will default to port 3310.
• Timeout (Seconds) - The maximum number of seconds SmarterMail should wait for ClamAV to respond before moving on to the next message. By default, the timeout is 10 seconds.
• Failures Before Disable - The maximum number of ClamAV timeouts allowed before it is disabled. By default, ClamAv is limited to 5 failures.

Cyren Zero-hour Outbreak Detection

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

Cyren evaluates each message and determines the probability that the message contains a virus. For more information, or to purchase this add-on, visit the SmarterTools website .

Note: This service is intended to be used as a complement to conventional antivirus technology as an additional protection against zero-hour virus outbreaks. Cyren Zero-hour Outbreak Detection looks for new variants of malware and should not be used as the standalone antivirus program.

• Enable Cyren Zero-Hour Outbreak Detection - When licensed, enabling this setting allows the use of Cyren Zero-hour Outbreak Detection. Note: Cyren Zero-hour Outbreak Detection is a paid SmarterMail add-on and can be licensed in 12-month subscriptions. Start a 30 day trial in the Licensing settings, or contact SmarterTools Sales for purchasing details.
• When Virus is Found - This dropdown allows you to select what you want done with a message if Cyren detects it contains a virus. These options include:

• No Action - Do nothing with the message.
• Delete Message - Delete the entire message. Note: The Delete Message action will permanently delete messages, preventing them from reaching the user's mailbox. Exercise caution when selecting this action, as messages deleted via virus filtering cannot be recovered.
• Quarantine Message - Move the message to the quarantine folder on the server. These messages can then be found on the Virus Quarantine tab on the Spool page. By default,

messages remain in quarantine for 30 days, after which time the .eml is deleted, unless other action is taken to move the message out of quarantine.

Command-Line Antivirus

Administrators can integrate SmarterMail with third-party antivirus programs via a command-line execution. This can be an efficient solution for high-volume mail environments by reducing the burden on the mail server itself.

Once a message comes into the SmarterMail spool, it will then be scanned for viruses using the command-line antivirus and any built-in antivirus measures that have been enabled in SmarterMail. If the command-line scanner picks up a virus, it will be up to the command-line antivirus program to delete/quarantine the message according to the application's configuration.

- Enable command-line antivirus - Enable this setting to allow the use of command-line antivirus.
- Command Line - Enter the executable for the antivirus program. For example, if you'd like to integrate with ESET Endpoint Antivirus, you might enter something like:

```
C:\Program Files\ESET\ESET Endpoint Antivirus\ecls.exe /base-
dir="C:\Program Files\ESET\ESET Endpoint Antivirus" /aind /arch /sfx
/adware /clean-mode=Delete %FILEPATH
```

Note: %FILEPATH will be replaced with the path to the file to be scanned.

Bindings

System Administrators can use this section to specify on which ports the server IP address(es) -- both IPv4 and IPv6 addresses -- should listen, assign protocols to those ports or assign a hostname for each IP address. All ports being used should be assigned to at least one IP address on the server. However, SmarterMail provides system administrators with some flexibility when configuring bindings. This means, for example, that the system administrator can allow POP (port 110) on the IP 111.111.111.11 but not on the IP 222.222.222.22. In addition, some servers may have other programs installed that need to listen on mail ports. To accommodate this, the System Administrator can configure SmarterMail to listen on a subset of IP addresses, leaving the remaining IP addresses available for other programs.

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

To access SmarterMail's IP and port bindings, log into SmarterMail as a System Administrator and click on the Settings icon. Then select Bindings from the navigation pane. The following tabs will be available, and each tab will display the number of items configured for each:

IP Addresses

Every IP address stored on the server's Network Interface Card (NIC) will be displayed in this section. Click on the IP address to open its configuration options. If you need to add IPs to the list, click the New button. The following setting will be available:

- IP Address - The IP address from the server. This field cannot be edited.
- Hostname - The hostname that should be assigned to the IP address (e.g., mail.example.com). A hostname can be assigned to each IP address on the server. This is beneficial because it allows every domain on the server to be assisgned its own IP address, thereby limiting the chances of the entire mail server becoming blacklisted should a user on one domain send out unwanted emails.
- Description - A friendly explanation of the binding's purpose.
- Ports - Select each port on which this IP address should listen. All ports being used should be assigned to at least one IP address on the server.

The IP Addresses listed in this section are pulled from the server and can only be removed from SmarterMail by removing the IP Address from the Network Interface Card (NIC). Occassionally, however, an IP address that is NOT stored in the server's NIC may appear in this list. These IP addresses can be removed using the Delete button, if desired.

Ports

Use this section to assign specific protocols to ports or to add Secure Socket Layer (SSL) and Transport Layer Security (TLS) rules to any ports and protocols. To add a new port, click the New button. To edit an existing port, simply click on it. The following settings will be available:

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

the security certificate and its corresponding password.

• IP Addresses - Every IP address on the server will be listed here. Select the IP address(es) on which this port should listen.

Delivery Limits

Below are the features available when viewing the Delivery Limits section of SmarterMail. To access this section, log into SmarterMail as a System Administrator and click on the Settings icon. Then click on Delivery Limits in the navigation pane. This page has three tabs, and each tab has its own settings and options. These tabs are:

Do Not Forward

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

Note: Do Not Forward only prevents the automated forwarding of email, which is configured in the user's general settings. Any messages that are manually forwarded by Users are not impacted by the Do Not Forward list.

To add a new Do Not Forward domain, click the New button. To Edit an existing domain, click on it and you can change it. To Delete an existing entry, select the entry (or multiple entries) and click Delete . When adding or editing an entry, the following option will be available:

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

Sender Priority

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

To create a new sender priority override, click the New button. To edit an existing entry, click on it.

To Delete an existing entry, or multiple entries, select it and then click the Delete button. When adding or editing an entry, the following settings will be available:

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

Reserved Domains

System Administrators can prevent certain domains names from being added to SmarterMail. For example, domains that are already used for free email services, like gmail.com or yahoo.com, are ideal additions to the reserve list as allowing administrators to add such domains to SmarterMail could affect message delivery. Similarly, domains that are traditionally reserved for testing and documentation, such as test.com or example.com are also ideal candidates for the reserve list.

To add new Do Reserved Domains, click the New button. To Edit an existing domain, click on it and you can change it. To Delete an existing entry, select the entry (or multiple entries) and click Delete . When adding or editing an entry, the following option will be available:

- Domain Name - Enter the domain name. It's also possible to add multiple domains, and each should be on its own line.

System Events

This settings page is only available to Administrators of the SmarterMail installation.

The Event system in SmarterMail is an incredibly powerful and flexible tool that allows Administrators to automatically perform actions based on specific criteria and remain up-to-date with what is going on with the SmarterMail server, domains and user accounts. SmarterMail can detect events as they occur, generate messages for those events, and deliver the messages to users that need the information.

By default, SmarterMail is installed with several pre-defined system events. These are available to help System Admininstrators keep track of important information, such as the impending expiration of any paid add-ons, when a new version is available to be downloaded and installed, when the overall disk space usage on the server is getting to a critical point, when a User's disk space is getting to a critical point and more. Any "built-in" Events are labeled as such -- these Events can not be deleted, though they can be edited. Other pre-defined events can be edited and changed to match the needs of the system and System Administrator, or deleted entirely.

To create or view system events, log into SmarterMail as an Administrator and click on the Settings

icon. Then click on Events in the navigation pane. To create a new event, click New . The following options will be available:

General

• Event Name - The friendly name of the event.
• Event Status - New events default to a status of Enabled. However, to temporarily stop an event from triggering, you can change the status to Disabled.
• Event Category - The feature to which the event pertains: User, Mailing List, Alias, Throttling, Email or Collaboration.
• Event Type - The occurence that triggers the event. Each category has several specific event types that can trigger the action.

Conditions

Each event type has its own corresponding conditions. The global conditions that are seen across all event types are listed below.

• Time of Day - The time frame during which the event occurs.
• Day of Week - The day(s) of the week during which the event occurs.
• Service - The service impacted that would fire the event: SMTP, POP, IMAP, Delivery, POP Retrieval.

Actions

Each event type has its own corresponding actions. The global actions that are seen across all event types are listed below.

• Send a notification - This option will send a notification to the Notifications window. It can also send a popup browser notification and an email.
• Send an email - This option will send an email to the specified address.
• Command Line Action - Execute a specified command line.

Event Variables

Below is a list of variables available for any and all system events. NOTE: This list may change as variables may be added at any time.

• Alias Addresses -- #aliasaddresses#
• Alias Name -- #aliasname#
• All Domain Admins -- #alldomainadmins#
• Check Name -- #checkname#
• ClamAV IP -- #clamip#

- ClamAV Port -- #clamport#
- Consecutive Failures -- #consecutivefailures#
- Days Left -- #daysleft#
- Day of Week - #daysofweek#
- Description -- #description#
- Disk Drive -- #diskdrive#
- Free Disk Space (GB) -- #diskspacefree#
- Free Disk Space (%) -- #diskspacefreepercent#
- Disk Drive -- "#diskdrive#
- Disk Usage (GB) -- #diskspaceused#
- Disk Usage (%) -- #diskspaceusedpercent#
- Domain -- #domain#
- Domains Used - #domaincount#
- Domains User (%) -- #domainpercent#
- Domain Usage (MB) -- #domainusagemb#
- Domain Usage (%) -- #domainusagepercent#
- File Name -- #filename#
- File Size (KB) -- #filesize#
- Forwarding Address - #forwardingaddresses#
- From Address -- #emailfrom#
- From Domain -- #fromdomain#
- Full Name -- #fullname#
- Gateway Address -- #gatewayip#
- Hard Reject -- #hardreject#
- Intra Domain -- #intradomain#
- IP Address -- #ipaddress#
- Add-on Name -- #licensefor#
- List Name -- #listname#
- Location -- #location#
- Mailbox Allowed Size (MB) -- #mailboxsizemax#
- Mailbox Usage (MB) -- #mailboxusagemb#
- Mailbox Usage (%) -- #mailboxusagepercent#
- Mailing List Address -- #mailinglistaddress#
- Max Disk Size (GB) -- #diskspacegbmax#
- Max Domain Size -- #domainsizemax#
- Memory Used (MB) -- #memoryusedmb#
- Memory Used (%) -- #memoryusedpercent#

- Messages an Hour -- #amtinhour#
- Password -- #password#
- Percent Complete -- #percentcomplete#
- Primary Domain Admin -- #primarydomainadmin#
- Priority -- #priority#
- Rule Name -- #rulename#
- Rule Type -- #ruletype#
- Server Name -- #servername#
- Service -- #service#
- Size (KB) -- #sizekb#
- SpamAssassin IP -- #spamassassinip#
- (SpamAssassin) Name -- #spamassassinname#
- SpamAssassin Port -- #spamassassinport#
- Spam Level -- #spamlevel#
- Spam Weight -- #weight#
- Spool Count -- #spoolcount#
- Status -- #status#
- Subject -- #emailsubject#
- Subscribe Method -- #subscribemethod#
- Thread Count -- #threads#
- Throttle Limit Type -- #throttlelimittype#
- To Address -- #toaddress#
- To Domain -- #todomain#
- Unsubscribe Method -- #unsubscribemethod#
- Uptime (Days) -- #uptimedays#
- Username -- #username#
- Version -- #version#
- Virus Name -- #virusname#

Gateways / Failover

Outbound Gateway

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

To access the outbound gateway settings, log into SmarterMail as a System Administrator and click on the Settings icon. Then select Gateways / Failover in the navigation pane. The Outbound tab will be highlighted, by default.

To add a new outbound gateway, click the New button. When adding or editing an entry, the following settings will be available:

Options

- Server Address - The IP address of the gateway server.
- Port - The port used to connect to the gateway server.
- Encryption - Select the type of encryption from the list.
- Status - The status of the outbound gateway. To temporarily turn off the outbound gateway, select Disable from the list.
- Type - This sets the behavior of the gateway: it will either "Round Robin", meaning that when multiple gateways are configured, domains will use one then use the next to send mail, cycling through each gateway, or it's possible to set up a gateway to be used by "Specific Domains". When a gateway is set up to be used by Specific Domains, the gateway is selected FOR the domains when the domains are being set up. (Or, it's possible to set the gateway for a domain after it's been set up.)
- Enable Authentication - Enable this setting if your outbound gateway server requires authentication. Then enter the Auth Username and Password below.
- Auth Username - The authorized username of the gateway server.
- Auth Password - The corresponding password for the authorized username.

SmarterMail Gateway

- Enable SmarterMail gateway mode - Enable this setting to indicate that the outbound gateway server is another SmarterMail server.
- SmarterMail URL - The Webmail URL for the SmarterMail server being used an an outbound gateway. This will allow the use of web services to verify the users and domains.
- SmarterMail Username - The identifier used to login to the primary mail server.
- SmarterMail Password - The corresponding password used to login to the primary mail server.

Inbound Gateways

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

To access the inbound gateway settings, log into SmarterMail as a System Administrator and click on the Settings icon. Then click on Gateways / Failover in the navigation pane and select the Inbound tab.

To add a new inbound gateway, click New . When adding or editing an entry, the following settings will be available:

Options

- Gateway Mode - The function that the inbound gateway will perform. If the inbound gateway is set to Backup MX , it will only receive messages when your primary server is down. If the inbound gateway server is set to Domain Forward , it will receive all messages and forward them to your primary server.
- IP Addresses (single or range) - The IP address, or range of IP addresses, of the primary mail server.
- Status - New gateways default to a status of Enabled. To temporarily stop an inbound gateway, you can change the status to Disabled.
- SMTP User Verification - This setting makes SmarterMail verify that a recipient exists when accepting mail from the gateway.

Domains

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

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

Use this card to specify for which domains the inbound gateway will accept mail:

- Domain Verification - The method used by the inbound gateway to determine if a domain is valid or not: Specified Domains or All But Specified Domains. List the domain(s) below (one entry per field).

SmarterMail Gateway

- Enable SmarterMail Gateway Mode - Select this option to indicate that the inbound gateway server is another SmarterMail server.
- SmarterMail URL - The Webmail URL for the SmarterMail server being used an an inbound gateway. This will allow the use of Web services to verify the users and domains.

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

• User Verification - The method used by the inbound gateway to determine if a user is valid or not. Note: If none is selected, the inbound gateway server will accept all email addresses for the domain. If Web service is selected, the inbound gateway will check with the primary mail server for a list of valid email addresses.

Spam

Use this tab to specify the following spam checks:

• Not Spam Action - The action the inbound gateway will perform on messages NOT marked as spam.
• Spam Low Action - The action the inbound gateway will perform on messages with a low probability of being spam.
• Spam Medium Action - The action the inbound gateway will perform on messages with a medium probability of being spam.
• Spam High Action - The action the inbound gateway will perform on messages with a high probability of being spam.

Configuring SmarterMail for Failover

Who Should Use This

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

Failover Overview

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

To review the Failover Servers configured for an installation, log into SmarterMail as a System

Administrator and click on Gateways / Failover in the navigation pane. Then click on Failover Servers tab .

Understanding How Failover Works

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

If the primary server fails, SmarterMail can be configured to automatically enable the secondary server. When this occurs, the secondary server takes over responsibility for processing background threads and supporting all email functionality. This server will remain in active status until another failure occurs or the primary mail server comes back online.

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

Minimal System Requirements

- A minimum of two servers running Microsoft Windows Server 2012 R2 64-bit or higher. (Windows Server Core is not currently supported).
- Three IP addresses
- Both servers must have their server times synchronized
- A domain account or local system User or Group account with bi-directional authentication. (NOTE: SmarterMail can NOT be run using Local System, Local Service or Network Service in a failover configuration.)
- NFS/SMB share for mail and system files. We recommend that the share is running on a NAS/SAN that is configured as RAID 10

Adding Network Load Balancing to Your Servers

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

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

Configuring the Load Balanced Cluster for Use with Failover

• Navigate to Start -> Administrative Tools -> Network Load Balancing Manager

• Click the Cluster menu item and select New

• In the New Cluster: Connect window, type the IP of your primary server in the Host: text box and select New

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

• Since this is the primary node, ensure the host Priority is set to 1

• In the New Cluster: Host Parameters window, confirm the IP address and Subnet mask are correct and change the initial host state to Stopped . This is to prevent any issues with connectivity if a machine randomly reboots or suffers from a hardware failure. If all nodes are set to Started for their initial host state, traffic will be split between the two (or more) machines. Note: Monitoring software can be used to execute scripts that will start and stop hot standbys in the event of a failure and recovery. If you are not executing scripts via monitoring software then all failover will need to be handled manually.

• Click Next

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

• Select Next

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

• Ensure the cluster operation mode is set to Multicast

• Click Next

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

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

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

• Click OK

• Verify your settings and click Finish to complete the setup

Joining Additional Nodes to the Cluster

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

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

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

• Select the existing cluster that appears in the Clusters section and click Finish
• In the main Network Load Balancing Manager , expand Network Load Balancing Clusters and right click on your Cluster (it may be the IP address of your cluster) and select Add Host to Cluster
• In the Add Host to Cluster: Connect window, enter the IP address of the secondary server in the Host: section and click Connect
• When the Interface Name and Interface IP appear, select the Interface Name and click Next
• In the Add Host to Cluster: Host Parameters window, confirm the IP address and subnet mask and ensure the Initial Host State is set to Stopped . As this is the second node you're adding to your cluster, the Priority should be set at 2
• Click Next
• Just as with the primary node, in the Add Host to Cluster: Port Rules window you have the ability to set this node to respond via specific ports or a port range. If you wish to set these rules, click Edit . Otherwise, click Finish to complete the setup
• Wait for the nodes to converge and, if necessary, stop the secondary sever by right clicking the second server's name, select Control Host -> Stop

Configure a Shared Service Directory

• Using Network File Sharing (NFS) or Samba (SMB), create a shared directory named SmarterMail , preferably on a NAS or SAN. NOTE: We recommend that this shared directory be hosted on a server that utilizes a RAID 10 configuration for the data.
• Inside that new SmarterMail folder, create a Settings folder
• Configure your permissions accordingly. The SmarterMail service needs to run as a domain account or a local account with bi-directional authentication. You can configure this within the Windows Services console. When running SmarterMail with failover, Local System, Local Service and Network Service users are not allowed. Note: When performing updates to the software, the credentials will need to be re-applied to the service

Configuring a Fresh Installation of SmarterMail for Failover

• Install and configure a primary SmarterMail server. Then, stop the service on this primary installation.
• Install another SmarterMail Enterprise instance on a second server. This new installation will be your hot standby. Leave all setup information as the default settings and after setup is complete, configure SmarterMail as an IIS site.
• Stop the SmarterMail service on the hot standby
• Edit the failover.json file in the primary server's Settings folder as follows. (Default location is C:\Program Files (x86)\SmarterTools\SmarterMail\Service\Settings.)

- FailoverIPAddress - Set this to the IP address of the Network Load Balancer
- IsEnabled - Set this to True
- SharedSystemFilesPath - Set to the shared network shared system folder

A sample failover.json would look like this:

```
{ "NodeID": "09190514-4535-479a-85r7-g992v44nn96f", "FailoveIPAddress":
"122.32.55.241", "IsEnabled": true, "SharedSystemFilesPath":
"\\\\serverName\\FailOverTesting\\SmarterMail\\Service\\Settings" } NOTE:
The code should look like the above: casing, proper escaping of paths, etc.
in order for the JSON to be read properly. Also, due to size limitations,
in the sample above the SharedSystemFilesPath is split across 2 lines --
that should be ONE line.
• Save this file, then copy it to the hot standby's Settings folder,
replacing the existing failover.json
• Copy over all folders and files from C:\Program Files
(x86)\SmarterTools\SmarterMail\Service\Settings to the Settings folder in
the shared service directory you created
• Start the service on the hot standby server and verify that the paths are
pointing to the network shared paths
• Activate your Enterprise key on the hot standby by logging into
SmarterMail's management interface as the System Administrator and going to
the activation section. Then stop the SmarterMail service on the server
• Start the service on the primary server, then reactivate your Enterprise
license key in the SmarterMail management interface
• After re-activating the license, go to IP Addresses and bind all the
ports to the load balancer's IP address and make sure no other IPs have any
ports bound to them
• Both servers are now set up for failover. To verify this, log into the
primary server as the System Administrator and go to Gateways / Failover .
The servers that are part of the failover cluster will be displayed on the
Failover Servers tab.
```

Adding Failover to an Existing Installation of SmarterMail

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

- Ensure the primary server is running the latest version of SmarterMail and that it is also configured as an IIS site. Ensure the IIS binding is pointing to your cluster IP address

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

- FailoverIPAddress - Set this to the IP address of the Network Load Balancer
- IsEnabled - Set this to True
- SharedSystemFilesPath - Set to the shared network shared system folder

A sample failover.json would look like this:

```
{ "NodeID": "09190514-4535-479a-85r7-g992v44nn96f", "FailoveIPAddress": "122.32.55.241", "IsEnabled": true, "SharedSystemFilesPath": "\\\\serverName\\FailOverTesting\\SmarterMail\\Service\\Settings" } NOTE: The code should look like the above: casing, proper escaping of paths, etc. in order for the JSON to be read properly. Also, due to size limitations, in the sample above the SharedSystemFilesPath is split across 2 lines -- that should be ONE line.
• Copy that failover.json file, after you've edited it, and move it to the same location on the hot standby. You should replace the file on the hot standby, if it already exists.
• Run the robocopy one more time to copy over any modified files and remaining spool emails
• Copy over all folders and files from C:\Program Files (x86)\SmarterTools\SmarterMail\Service\Settings to the Settings folder in the shared service directory you created
• Edit the domains.json file in the shared Settings folder and change the path of your domains to match the new NFS\SMB path. (For example, \\NAS01\SmarterMail\Domains\mydomain.com)
• Edit the settings.json file and replace any instances of the old physical path's with your new network location for SmarterMail. (For example, if all of your data was hosted on E:\Smartermail, you would then perform a find and replace for all instances of E:\Smartermail to \\NAS01\Smartermail).
• On the primary server, go to Start -> Administrative Tools -> Network Load Balancing Manager and stop the cluster node, then start the NLB on the secondary node
```

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

Scripting Failover

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

Prepping PowerShell on the Servers

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

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

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

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

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

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

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

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

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

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

General System Settings

Below are the configuration options available when viewing the General Settings section of SmarterMail. To access this section, log into SmarterMail as a System Administrator and click on General in the navigation pane.

Jump to:

- Spool
- Footer

Server Info

- Hostname - The hostname of the server. Note: Hostnames should be in the format computername.domain.com.
- Primary DNS IP - The IP address of the primary DNS server. If left blank, the DNS server information will be pulled from the the Windows Networking settings. (Recommended.)
- Secondary DNS IP - Enter the IP address of the secondary DNS server. If left blank, the DNS server information will be pulled from the the Windows Networking settings. (Recommended.)

Paths

By default, SmarterMail stores certain information in pre-defined paths. However, there may be times when System Administrators want certain things stored in separate locations. A perfect example of this is the SmarterMail Spool: for many servers, having the Spool process on a separate drive on the server can increase performance and server reliability, not to mention save disk i/o. That's because the Spool for any mail server can tax a drive due to all the file reads and writes. Having the Spool on a separate drive -- say an SSD drive -- can help the overall lifetime of a mail server.

In this section, System Administrators can specify which drive paths to use for the following:

- Spool Path - Having the Spool on a separate drive is recommended for any mail server due to the i/o required. If you are using a real-time virus scanner, this is the path that must be scanned in order to properly handle viruses.
- Log Files - Storing SmarterMail log files on a separate drive means that more space is available for users. Depending on how log files are set up -- the level of detail stored for each -- having a separate, large hard drive specifically for log files means less potential for disk space issues for users. Note: Changing the log path will not take effect until you restart the SmarterMail service.
- POP Retrieval Download Path - Since POP retrieval is used for secondary, non-SmarterMail accounts, storing the data for those alternate accounts on a separate hard drive can help conserve space for SmarterMail user accounts.
- IMAP Retrieval Download Path - Since IMAP retrieval is used for secondary, non-SmarterMail accounts, storing the data for those alternate accounts on a separate hard drive can help conserve space for SmarterMail user accounts.
- Quarantine Path - This is the directory used for files caught by SmarterMail's antivirus and antispam integrations. Having quarantined items stored on a separate drive can further protect a mail server from issues caused by viruses.

Webmail Login

Small businesses using SmarterMail on their own servers, or even companies using SmarterMail from their hosting provider, will benefit from the ability to customize the SmarterMail login page to add a company logo, provide additional branding text, or simply adjust the default 'Login to SmarterMail' text to be more in line with an overall brand message. Note: System Administrators can allow Domain Administrators to override the custom login screen by editing the Domain and enabling Webmail Login Customization in the Features section.

- Logo Image - Upload an image, like a company logo, by dragging and dropping a file in the highlighted area or clicking to browse for a file (max file size of 3mb). Uploading an image using this upload control will host the image publicly on the server and enter the tag in the HTML section. Note: Uploading an image here alone will NOT display the image on the login screen. The HTML must remain in the Login Page HTML section. This upload control can be used by those who don't have their logo publicly hosted or who wish the image source to point back to their mail server. Furthermore, regardless of the image uploaded, the image's source URL will remain the same; only one image may be hosted at a time.
- Custom Login Text - Use this setting to customize the login page header to something more in line with an overall brand message. If Custom Login Text is left blank, SmarterMail's login page will show the default text "Welcome to SmarterMail".
- Custom Title Text - Use this setting to customize the title of the login page to something more in line with an overall brand message. If Custom Title Text is left blank, SmarterMail's login page will show the default text of "SmarterMail" in the browser tab title. Note: When a system administrator is logged in, the custom title text will appear on all pages. If the login display for a domain is not set to default or overridden, users will see this text on the login page only, with their email address displayed as the browser title for all other pages.
- Login Background - Use this option to select the background image(s) that displays on your login screen. Use the default images that come with SmarterMail, point to your own path on the server or select a solid color background. For custom images, the following image formats are supported: SVG, PNG, JPEG/JPG and GIF. Minimum size is dependent upon the image type being used. However, you can use 1920 x 1280 as a general guideline.
- Login Page Language - Use this option to set the default language for the login page of SmarterMail. SmarterMail contains several pre-defined language packs in each installation, so the languages listed in the dropdown have accompanying language packs pre-installed and avaialable for use.
- Check for Outdated Browser - When enabled, SmarterMail will check the version of the browser being used at the login page, and if it doesn't meet the minimum broswer requirements, the user will see a screen asking them to upgrade their browser. SmarterMail does have some

requirements that modern browsers meet -- things like WebRTC support for video conferencing, support for AngularJS and other newer technologies -- that ensure the ideal experience when using the SmarterMail web client. While older browsers may work, current browsers are highly recommended.

• Enable custom login page HTML - Check this box to enable the ability to use HTML to further modify the login screen to add additional text or adjust the layout.

• Login Page HTML - Enter the custom HTML that will be used to further modify the login screen (in-line custom CSS can be used as well). Note: To include white space around the Image on Login Screen, the div id "companyinfo" must be included.

Custom Logout

• Redirect to a webpage on logout from webmail - Enabling this setting allows you to add a URL to which users are redirected when they log out of SmarterMail. By default, users are presented with the log in page for the mail server. If this should be different, a new URL can be added. Enable this setting to add in a Logout URL.

• Allow domains to override Logout URL - Enable this setting to allow Domain Administrators to specify a Logout URL for their domain. If this option is not enabled, the option will not be visible to Domain Administrators.

Custom Help

When enabling Custom Help, whatever is entered as the Custom Help Text, and the URL that text redirects to, will replace the standard, default Online Help link that is displayed. That means you'll be redirecting users of the SmarterMail server to your OWN help documentation and away from the documentation created by SmarterTools.

• Custom Help URL - Entering a full URL in this field will add a custom link to the Help menu that users can access in the SmarterMail interface. Administrators can link to a variety of things, including server-specific instructions for syncing, help resources, contact information, etc.

• Custom Help Text - The hyperlink text for the custom URL in the Help menu.

Reports

Use this tab to specify the following settings:

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

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

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

Folder Auto-Clean

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

• Allow domains to override auto-clean settings - Enable this setting to allow Domain Administrators to create their own auto-clean policies for their domain.
• Allow users to auto-clean Inbox - Enable this setting to allow users to create auto-clean policies on the Inbox folder.

To add a new folder auto-clean rule that will apply to all users across all domains, click on the New Rule button.

If the Rule Type is set to Size, the following options will be available:

• Folder - The folder that will be auto-cleaned: Deleted Items, Junk Email or Sent Items.
• When size greater than (MB) - The maximum size of the folder, in megabytes. Once the folder reaches this size, the auto-clean process is started and older messages (messages that were received the longest time ago) are deleted.
• Reduce to (MB) - The size the folder should be after the auto-clean process has completed, in megabytes. When auto-cleaning, SmarterMail will delete older messages first until the folder reaches this size. Note: This number should aways be lower than the previous field.

If the Rule Type is set to Age, the following options will be available:

• Folder - The folder that will be auto-cleaned: Deleted Items, Junk Email or Sent Items.
• Days - The maximum number of days mail will stay in the selected folder before deletion.

File Storage

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

• Max File Size (KB) - The maximum size a file can be in order to be uploaded to the server.
• Root Webmail URL - The base URL of any file stored and shared in file storage. By default, the base URL corresponds to the domain the mail server is set up on (i.e.,

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

• Extension Blacklist - Use this section to select and list any file types that cannot be uploaded to the server via File Storage. System Administrators may want to limit the capabilites of users to upload certain file types, such as executables (.exe) or other file types that can possibly be used to cause problems on the server.

Attachments

• Inbound Extension Blacklist - This list allows you to limit the file types that are allowed INTO the mail server. For example, many email administrators won't allow executable files (EXE) as they can cause issues on the mail server, and possibly across an entire network. To add a blacklisted file type, simply type in the file extension, one per line. (E.g., .exe or EXE)

• Outbound Extension Blacklist - This list allows you to limit the file types that are users are allowed to send OUT OF the mail server. For example, many email administrators won't allow batch files (.BAT) as they can cause issues on the recipients' mail server, and possibly across their entire network. To add a blacklisted file type, simply type in the file extension, one per line. (E.g., .bat or BAT)

Spool

• SubSpools - SubSpools are within the spool path and allow SmarterMail to work around the NTFS limitation of 30,000 objects in an individual folder. SmarterMail will utilize subspools by evenly distributing mail among the subspools, allocating up to 10,000 messages per subspool. If the subspool count is set to 1, the Spool folder will be used. Note: If the subspool count is lowered, the old subspool folders will not be automatically deleted; however, you may manually delete the unused subspool folders if you wish. This design is to accommodate for situations where the subspool count is lowered while mail is still processing in those folders. (Default value is 10)

• Delivery Delay (Seconds) - This number of seconds mail will be held in the spool before it is delivered. A delivery delay is beneficial when you are running a secondary service (such as a virus checker) that needs access to messages prior to delivery, as it provides ample time for the secondary service to interact with the message. By default, the delivery delay is 1 second.

• Retry Intervals (Minutes separated by commas) - When the mail server is unable to contact the receiving server, the email attempting to be sent is held for a period of time before the mail server attempts to resend it. This is the time between retries. Users can specify multiple retry attempts to resend emails before it is bounced. By default, this is set to 4 attempts - at 1, 5, 5, 15, 30, 30, 30, 30, 60, 90, 120, 240, 480, 960, 1440, 2880.

• DNS Errors Before Bounce - The maximum number of attempts SmarterMail should make before the message is bounced due to a DNS error. The most common cause of a DNS error is a misspelled domain. Limiting the number of attempts before DNS errors are bounced is beneficial because messages will not sit in the queue for long periods of time taking up processing on the mail server and possibly slowing the system down. This will be helpful to users because messages will be bounced sooner and will give users the opportunity to fix any mistakes and get a message resent. By default, the server will make 2 attempts. Note: Setting this at 1 retry can be dangerous if the DNS server fails or if there is a loss of Internet connectivity. To disable this feature, set the number of bounces equal to the number of retry intervals.
• Notify Senders of Delay After (Attempts) - Sets the number of delivery attempts before the sender is notified that the email delivery is delayed. This can be beneficial as it lets the sender know that the mail server is still attempting to deliver the message but that the recipient has not received it yet. (Default value is 0.)
• Max Local Delivery Threads - Enter the maximum number of messages that can be sent at one time to email addresses that are on the local server. If a message cannot be sent, the server's multi-threading capabilities will move on to the next message and eventually get back to the one it skipped. This action can save tremendous amounts of time when compared to some other mail servers that stall the spool if a message cannot be sent right away. (Default is 50)
• Command Line File - Move the slider to the right to enable this option. Then enter the full path to an executable you wish to use to process incoming messages. Use %filepath as an argument to pass the path of the email file to the executable. It is allowable for the executable to delete the message to prevent delivery. Example: If you set this field to "c:\program files\myexe.exe %filepath", the program myexe.exe will be launched with the full path to the spool file as its first argument.
• Command-Line Timeout (Seconds) - The number of seconds that the server will wait for information from the remote server. By default, the timeout is set to 5 seconds.

Footer

System Administrators can configure server-wide message footers that SmarterMail will append on all incoming and outgoing messages. Messages that a SmarterMail user forwards that already has a footer will not have the system footer appended as well. Although similar to signatures, message footers are typically used to convey disclaimers or provide additional information. For example, a system administrator may want every message to include a notice that the message was scanned for viruses or the text "Sent by SmarterMail."

• Enable footer for all messages - Move the slider to the right to turn on the message footer for all incoming and outgoing messages. This setting does not need to be enabled to allow Domain

Admins to override. If domain admins do override this setting and it's enabled for all messages, emails will have the domain footer on outgoing messages but still have the system footer on incoming messages.

• Apply to mailing lists - Move to slider to the right to enable this setting and append the message footer to mailing list messages. Note: Mailing lists have their own configurable footers. If a custom mailing list footer is already configured, enabling this option will append a second footer at the end of each message posted to the mailing list subscribers. Because this may be confusing for mailing list moderators and recipients, most administrators will choose to keep this option disabled.

• Allow domains to override footer - Move the slider to the right to enable this setting and allow domain administrators to configure a unique message footer for their domain.

• Footer - Use this section to create the message footer text. Clicking the edit icon will open a modal that includes an HTML-based editor, allowing admins to create footers that seamlessly fit into any email message. Note: The message footer does not support the use of variables.

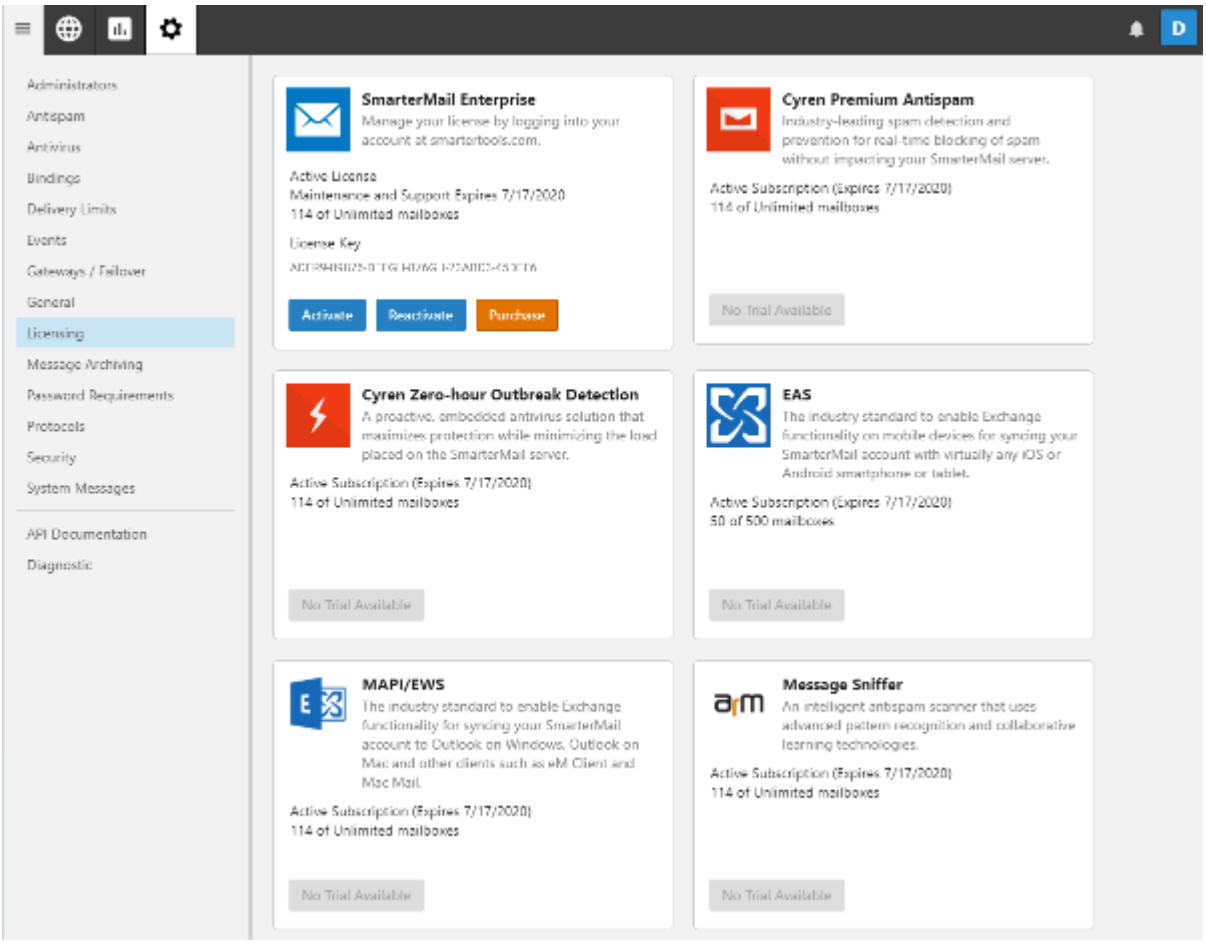
Licensing and Activation

During the installation process for SmarterMail, you're asked to input a license key, which defines the Edition and mailbox count that is activated once the installation completes. If you so desire, you can install SmarterMail as the Free Edition, which is good for use with 1 domain and up to 10 mailboxes.

To upgrade to a paid version and unlock additional mailboxes and/or gain access to use purchased SmarterMail Add-ons , a license key must be activated. Furthermore, if the SmarterMail installation is moved to another server or upgraded to a different version or product level, the product will need to be activated again. System Administrators can use the Licensing section to activate SmarterMail or view current licensing information and limits.

Note: Activation of a license key requires the server to contact SmarterTools over port 443 (HTTPS). Please ensure that any firewall or internet security software you have installed allows an outgoing TCP port 443 request. If the server cannot connect for security reasons or due to internet connectivity, please contact sales@smartertools.com to request steps for a manual activation. A manual activation requires the server's hostname, which can be found by entering 'hostname' into the server's command prompt.

To access the Licensing section, log into SmarterMail as a System Administrator and click on the Settings icon. From there, click on Licensing in the navigation pane. The current licensing details for SmarterMail and its add-ons will be displayed, including the license key, license level information, status of the license or subscriptions, the number of items used out of the total limit, and an indication of whether an add-on trial is available.



The following actions can be taken:

- Activate - Select this option to activate a new SmarterMail license key. Activating a paid license requires authentication by verifying the SmarterTools account login credentials. Trial license keys do not require authentication to be activated.
- Reactivate - Select this option to refresh the limits of the SmarterMail installation. This will cause SmarterMail to callback to the SmarterTools servers to refresh the limits of the license key and should be used after purchasing an add-on, upgrading to the Enterprise edition or increasing the mailbox limit. Reactivating is immediate and does not require authentication with the SmarterTools account credentials.
- Purchase - Select this option to be taken to the SmarterTools website where you can purchase a new license key or add-on.
- Start Trial - If an add-on trial is available, a Start Trial button will appear on its card. This allows the system administrator to test the functionality for up to 30 days. A trial can only be activated one time. To continue using the service after the trial, the add-on must be purchased. In addition, trials are not availble on Free Editions of SmarterMail. Note: The ActiveSync trial is limited to 25 Mailboxes.

Note: If you are running a trial version of SmarterMail, it will automatically revert to SmarterMail Free when the trial expires.

Message Archiving

This feature is only available in SmarterMail Enterprise edition.

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

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

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

To view the message archiving rules for your installation, log into SmarterMail as a System Administrator and click on the Settings icon. Then click on Message Archiving in the navigation pane. By default the Archiving Rules tab will be highlighted.

To create a new archiving rule, click on the New button. When adding or editing a message archive rule, the following settings will be available:

- Domain - The domain on the SmarterMail server to be archived.
- Archive Path - The directory on the hard drive in which archived messages are saved.
- Rule - Set the direction of the messages you want added to the Archive. The following Rules are available:

- Save All Messages
- Save Inbound Messages
- Save Outbound Messages

Once email archiving is set up, both System Administrators and Domain Administrators can search the archives. Note: Please note that Domain Administrator search requires individual domain archiving rules to be set up, as noted above.

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

Archive Search

When performing a message archive search, the following search strings will be available: filter for all domains or a specific one, date range, the sender's address, the recipient's address or the subject.

SmarterMail's archiving feature saves any inbound message, outbound message, or both, depending on the Rules that are set up for the domains. That means any spam message, junk message, messages that are eventually deleted, etc. are all saved. That means the ability to find messages, and then perform some action on those messages once found, is extremely important. This is especially true in environments that have compliance guidelines that need to be followed.

When message archiving is set up for a specific domain, that domain's administrator can find a Message Archive Search within the domain's Settings . System Admininstrators can search across any and all domains, regardless of the Rules that are set up. Regardless of whether a Domain Adminstrator or System Administrator is performing a search, the following is available for search criteria:

- Archive - Whether the search will encompass all domains or an individual domain.
- Start and End - The start and end dates for the search.
- From - The email address the message is sent from.
- To - The email address the message is sent to.
- Subject - A word or phrase that would be in the subject line. If a person wants to find all messages From or To a particular address, this can stay blank.

After a search is performed, and results are found, there are a few actions that can be taken on one or more of the search results:

- Download - This will download a copy of all messages selected as a .Zip file. The messages are saved in their original .eml format and can be opened by an email client, email utility or any other standard program that can open emails.
- Copy to Mailbox - In certain instances, it may be necessary to move messages to a separate mailbox. For example, in a situation where an outside organization, like an auditing company, requires access to certain messages. In these cases, a separate account can be set up for the organization, and any messages found via Archive Search can be moved to that new account for

later review. Messages can even be moved to a specific folder, or specific folders, within that new account so they're contained and easily organized.

Password Requirements

To ensure the security of the mail server and its mailboxes, system administrators can specify minimum requirements for user passwords. To access the password requirements settings, log into SmarterMail as a System Administrator and click on the Settings icon. Then click on Password Requirements in the navigation pane. The password requirement settings will load and the following Options tab will be highlighted by default. The following settings are available:

Requirements

- Minimum Password Length - Enter the minimum number of characters the password must have.
- At least one number - Select this option to force users to include a number in the password.
- At least one capital letter - Select this option to force users to include a capital letter in the password.
- At least one lowercase letter - Select this option to force users to include a lowercase letter in the password.
- At least one symbol - Select this option to force users to include a symbol in the password.
- May not match username - Select this option to ensure that the username and password do not match.

Options

- Prevent common passwords - Select this option to prevent users from configuring passwords that are included in the list of commonly used, insecure passwords. Note: The default location of the list of commonly used passwords is: C:\Program Files (x86)\SmarterTools\SmarterMail\Service\Common_Passwords.json.
- Prevent previous passwords reuse - Select this option to prevent users from using previously used passwords when changing their account password. Note: This setting prohibits old passwords from being used indefinitely. It is not based on a time interval.
- Skip enforcement for existing passwords - Select this option to skip existing users when making changes to password requirements -- meaning the changes will only affect new users or new passwords.
- Enable password retrieval - Select this option to allow users to reset their password if they forget it. Note: In order for users to utilize password retrieval, they must have a Recovery Address configured in their account settings.

Expiration

• Passwords expire automatically - Enable this setting to activate password expiration, forcing users to update their account passwords at your specified time.
• Password Expiration (Months) - The number of months that a password is valid. After the specified time, a user□soutgoing SMTP will be disabled and a password change will be forced upon Web interface login. Move the slider to the right to enable this setting. Note: If a user's 'Disable password changes' setting is enabled, their password will not expire.
• User Notification Timing (Days separated by commas) - The interval(s) used to notify users of when their password will expire or when their auto-block grace period will end and, subsequently, their outgoing SMTP will be disabled. The default values are 28, 14, 7, 3, 2, 1 days. This means SmarterMail will send out warning messages to the user to change their password 28 days, 14 days, 7 days, 3 days, 2 days and 1 day before their password officially expires or the grace period ends if their password violates the requirements. Note: SmarterMail will send one, single notification for all missed intervals. For example, imagine "Auto-block Grace Period" is set for 30 days and the "User Notification Timing" is set at 60, 45, 25, 10, 2, 1. When a user is in violation, SmarterMail will send a single notification for the 60 and 45 day intervals then continue as normal at the 25 day interval.
• Auto-block Grace Period (Days) - The number of days a user can wait to update their account password before outgoing SMTP is disabled due to password policy violation. Note: This setting only applies if the "Disable outgoing SMTP when auto-block grace period ends" setting is checked.
• Disable outbound mail after grace period ends - Select this option to disable outgoing SMTP after the auto-block grace period ends when a user□spassword does not meet the password requirements.

Password Compliance

The Password Compliance tab offers System Admininstrators a way to find users that aren't following the password requirements that have been set up. For any Users who appear on this list, the System Administrator is able to either email the Users individually, or force their non-compliant password to expire. This latter action means that the User will be forced to change their password the next time they log in to their email account. In addition, it's possible to export a list of the non-compliant Users in CSV format.

When Users appear on this page, the following information will be available:

• Username - The username of the non-compliant account
• Authentication - The Authentication Mode used by the account: SmarterMail or Active

Directory.

• Domain - The domain name that's associated to the Username.

• Violations - The number of password requirment violations encountered for the User.

Protocols

To access the settings for standard email protocols, log in to SmarterMail as a System Administrator and click on the Settings icon. Then click on Protocols in the navigation pane.

Jump to:

POP

Use this card to specify the following POP settings:

• POP Banner - The text that is displayed when initially connecting to the port.

• Command Timeout (Minutes) - If the server receives a command that sends large amounts of data but the data stops coming in for this number of minutes, the command will be aborted. By default, the command times out after 5 minutes.

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

• Max Connections (0 = Unlimited) - Some protocols in SmarterMail allow you to specify the maximum number of connections. Increasing this value allows SmarterMail to handle more connections of that type at once, but results in higher CPU and memory utilization. By default, the maximum number of connections is 500.

• Max POP Retrieval Threads - SmarterMail is multi-threaded, meaning it can do more than one thing at a time. This setting is for the maximum number of threads you want SmarterMail to work on concurrently for retrieving mail using the POP protocol. By default, the maximum number of POP retrieval threads is 10.

• POP Retrieval Interval - The frequency by which SmarterMail checks for new POP messages. By default, the POP retrieval interval is 1 minute.

IMAP

Use this card to specify the following IMAP settings:

• IMAP Banner - The text that is displayed when initially connecting to the port. The banner supports the use of the following variables, which will be replaced with their corresponding values:
• Command Timeout (Minutes) - If the server receives a command that sends large amounts of data but the data stops coming in for this number of minutes, the command will be aborted. By default, the command times out after 15 minutes.
• Max Bad Commands - After this many unrecognized or improper commands, a connection will be automatically terminated. By default, the maximum number of bad commands is 8.
• Max Connections (0 = Unlimited) - Some protocols in SmarterMail allow you to specify the maximum number of connections. Increasing this value allows SmarterMail to handle more connections of that type at once, but results in higher CPU and memory utilization. By default, the maximum number of connections is 1000.
• Max IMAP Retrieval Threads - The maximum number of threads you want SmarterMail to work on concurrently. By default, the maximum number of POP retrieval threads is 10.
• IMAP Retrieval Interval (Minutes) - The frequency by which SmarterMail checks for new IMAP messages. By default, the IMAP retrieval interval is 10 minutes.
• Enable IDLE Command - IMAP idle is an extension of the IMAP protocol that allows a mail server to send status updates in real time. Through IMAP IDLE, users can maintain a connection with the mail server via any mail client that supports IMAP IDLE, allowing them to be instantly aware of any changes or updates. When enabled, SmarterMail will inform any connecting IMAP client that it accepts the IDLE command. Note: IMAP clients that do not fully support IMAP IDLE, like Microsoft Outlook, may use the command in such a way that it actually hinders performance.

SMTP In

Use this card to specify the following inbound SMTP settings:

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

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

• #UnixTime# - The number of seconds since January 1, 1970.
• Allow Relay - If you are concerned about spammers using the relay function to send mail through your server, or do not want any other mail server to use your SMTP server as a gateway, set this to Nobody. (This is STRONGLY recommended.) However, you can set the type of relays you will allow, should you so desire.

• Nobody - Restricts sent mail to only work via SMTP authentication and with accounts on the local SmarterMail Server (except for IPs on the White List).
• Only Local Users - Limits relay access to users (email accounts) for a valid domain on your SmarterMail Server.
• Only Local Domains - Limits relay access only to mail hosts (domains) on your SmarterMail Server.
• Anyone - Allows any other mail server to pass messages through your mail server, increasing the chances of your mail server being used for sending large volumes of messages with domains not associated with your local mail server. Selecting this option turns off statistics for all domains, due to the high amount of messages that are passed through the mail server with an open relay.
• Session Timeout (Minutes) - After a connection fails to respond or issue new commands for this number of minutes, the connection will be closed. By default, the session times out after 15 minutes.
• Enabled - Select this checkbox to enable the session timeout setting.
• Command Timeout (Seconds) - If the server receives a command that sends large amounts of data but the data stops coming in for this number of seconds, the command will be aborted. By default, the command times out after 120 seconds.
• Max Bad Commands - After this many unrecognized or improper commands, a connection will be automatically terminated. By default, the maximum number of bad commands is 8.
• Max Connections (0 = Unlimited) - Some protocols in SmarterMail allow you to specify the maximum number of connections. Increasing this value allows SmarterMail to handle more connections of that type at once, but results in higher CPU and memory utilization. By default, the maximum number of connections is 1000.
• Max Hop Count - After a message gets delivered through this many mail servers, it is aborted by the software. This prevents looping due to DNS problems or misconfigurations. By default the max hop count is 20.
• Max Message Size (KB)(0 = Unlimited) - Messages greater than this size will be rejected by the mail server. By default, the max message size is 0 (unlimited).
• Max Bad Recipients (0 = Unlimited) - At times, spammers will hammer a domain with a dictionary harvesting attack. This means that software is used to send messages to many of the most common mailbox addresses (e.g., admin, user, contact, etc.) or username variations (e.g.,

alan@, alana@, alanb@, etc.) in order to find valid email addresses. Setting the max bad recipients means that after this many bad recipients (those that don't exist for the domain), the SMTP session will be terminated. This setting allows you to better protect yourself against email harvesting attacks. A value of 20 is recommended in most cases.

• Append Received Line - Select the option for appending the received line for All Inbound Messages, Non-authenticated messages or for no messages at all. NOTE: If a message has no Received headers, SmarterMail will add one to prevent issues with some mail clients.

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

• Max Messages Per Session (0 = Unlimited) - The maximum number of messages that can be sent in one session. This is useful in handling cases where spammers will make one connection and then send a large amount of messages with that connection.

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

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

• Enable Delivery Status Notifications (DSN) - Delivery status notifications are automated messages notifying a sender about the delivery status of a message: if it bounces, if it was delayed or if delivery was successful.

• Allow relay for authenticated users - This setting enables the "Allow Relay" setting when users are required to use SMTP Authentication for sending messages.

• Enable Domain's SMTP auth setting for local deliveries - Enable this setting to enforce SMTP authentication for all local deliveries. For example, mail from user1@example.com to user2@example.com must be authenticated even though the message is bound for local delivery.

• Disable AUTH LOGIN method for non-SSL SMTP authentication - This setting disables plain text authentication.

SMTP Out

Use this card to specify the following outgoing SMTP settings:

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

• Use Primary IP on NIC - This will use the IP address that's assigned to the Network Interface Card (NIC) on the SmarterMail server.
• Use the Domain's IP - When a domain is set up by a System Administrator, they can assign a specific IP address from the server as the "Outbound IPv4" address for that domain.
• Rotate IP List - Allows system administrators to select a number of different IP addresses that will be used, and the order in which they'll be used, to send email should connection failures or time outs occur.

• Order - The numerical position for the specified IP address.
• IP Address - The IP address associated to the specified position.
• Rotate List Fail Ratio - The percentage of successes to failures before the IP is rotated. (In decimal format, so .5 would be 50%)
• Rotate List Fail Threshold - The total number of successes and failures before the IP is rotated.

• NOTE: Both conditions have to be true for the IPs to be rotated. So if you have a Fail List Ratio of .5 AND a List Fail Threshold of 50 successes and failures, and BOTH of those conditions are met, the IP is rotated. Otherwise, mail will continue to flow.
• Outbound IPv6 - The IPv6 address used to connect to external SMTP servers when a message is sent by the domain. If multiple IPv6 IPs are on the server, they will be listed in the dropdown along with the following:

• Use Primary IP on NIC - This will use the IP address that's assigned to the Network Interface Card (NIC) on the SmarterMail server.
• Use the Domain's IP - When a domain is set up by a System Administrator, they can assign a specific IP address from the server as the "Outbound IPv6" address for that domain.
• Rotate IP List - Allows system administrators to select a number of different IP addresses that will be used, and the order in which they'll be used, to send email should connection failures or time outs occur.

• Order - The numerical position for the specified IP address.
• IP Address - The IP address associated to the specified position.
• Rotate List Fail Ratio - The percentage of successes to failures before the IP is rotated. (In decimal format, so .5 would be 50%)
• Rotate List Fail Threshold - The total number of successes and failures before the IP is rotated.

• NOTE: Both conditions have to be true for the IPs to be rotated. So if you have a Fail List Ratio of .5 AND a List Fail Threshold of 50 successes and failures, and BOTH of those conditions are met, the IP is rotated. Otherwise, mail will continue to flow.

• Disable - This disables the use of IPv6 on the server.
• Use Primary IP if selections are unavailable - Enable this setting to have SmarterMail automatically fall back to the primary IP when a failure has occurred. SmarterMail will only attempt to connect once if this option is enabled.
• Command Timeout (Seconds) - If the server receives a command that sends large amounts of data but the data stops coming in for this number of seconds, the command will be aborted. By default, the command times out after 60 seconds.
• Max Spam Check Threads - The maximum number of messages that can be spam checked at one time. By default, the maximum spam check threads is 30.
• Max Delivery Threads - The maximum number of messages that can be sent at one time to email addresses that are not on the local server. If a message cannot be sent, the SmarterMail server's multi-threading capabilities will move on to the next message and eventually get back to the one it skipped. This action can save tremendous amounts of time when compared to some other mail servers that stall the spool if a message cannot be sent right away. By default, the max delivery threads is 50.
• Max Recipients Per SMTP Session - The maximum number of recipients that can be included in one SMTP session. For example, with the limit set to the default of 500, an email containing 600 recipients would utilize two SMTP sessions for delivery - one with 500 recipients and the other with 100. This setting can useful if a receiving server rejects sessions that exceed their allotted recipient limit. Note: Setting this limit to Unlimited is not recommended unless there is a specific case for doing so.
• Enable DNS Caching - Enable this setting to cache the results of DNS calls in SmarterMail. When enabled, all DNS query results are stored for a period of time determined in the configuration (time-to-live) of domain name records. This decreases the query load placed on the authoritative servers and ensures that answers to these queries are stored locally for rapid querying, thereby speeding up the delivery of messages.
• Enable TLS if supported by the remote server - Enable this setting to use TLS (SSL encryption) if the server you are connected to supports it.
• Append X-Smartermail-Authenticated-As Header - Toggling the slider to the right means that outgoing messages will have a new line item in the message header called "x-smartermail-authenticated-as" that demonstrates that the message sender was verified using SMTP authentication. This header can then be used by anti-spam services for validation.
• Disable Remote Bounces - This setting disables bounce messages for messages that fail to reach remote recipients. That means that when a SmarterMail user emails an external recipient (any user not on their domain) and their email fails to deliver, they will NOT receive a bounce message from the recipient's server. Note: This setting disables bounce messages for

remote/external deliveries only. A SmarterMail user who sends an email to a user on the same domain will still receive a bounce message if that local delivery fails.

LDAP (Enterprise Only)

This feature is only available to Administrators using SmarterMail Enterprise.

Use this card to specify the following LDAP settings:

- Session Timeout (Seconds) - After a connection fails to respond or issue new commands for this number of seconds, the connection will be closed. By default, the session times out after 300 seconds.
- Command Timeout (Seconds) - If the server receives a command that sends large amounts of data and the data stops coming in for this number of seconds, the command will be aborted. By default, the command times out after 120 seconds.

XMPP (Enterprise Only)

This feature is only available to Administrators using SmarterMail Enterprise.

Use this card to specify the following XMPP settings:

- Max Connections (0 = Unlimited) - Some protocols in SmarterMail allow you to specify the maximum number of connections. Increasing this value allows SmarterMail to handle more connections of that type at once, but results in higher CPU and memory utilization. By default, the maximum number of connections is 1000.

Security Protocols

SSL and TLS are security protocols that encrypt the transmission of data, allowing users to access their email without the fear that someone has intercepted their data during transit. Use this card to modify the security protocols that are allowed to connect to your mail server.

Note: Prior to modifying these settings, SmarterMail must be configured for SSL or TLS connections which requires the installation of a security certificate on the server where SmarterMail is installed and the SmarterMail port(s) to be bound to the corresponding protocol(s). Please review the article, Configure SSL/TLS to Secure SmarterMail, in the SmarterTools Knowledge Base for more information.

- System Defaults - Use System Defaults to allow the operating system to choose the best protocol to use, and to block protocols that are not secure.
- SSL 3.0 - Enable this setting to allow inbound and outbound connections to your mail server over SSL 3.0. Note: Allowing connections over SSL 3.0 is NOT recommended. This protocol has been deprecated by the IETF and is considered to be highly insecure.

• TLS 1.0 - Enable this setting to allow inbound and outbound connections to your mail server over TLS 1.0. Note: Allowing connections over TLS 1.0 is NOT recommended. This protocol has been deprecated by the IETF and is considered to be highly insecure.
• TLS 1.1 - Enable this setting to allow inbound and outbound connections to your mail server over TLS 1.1.
• TLS 1.2 - Enable this setting to allow inbound and outbound connections to your mail server over TLS 1.2. Allowing connections via TLS 1.2 ONLY is strongly encouraged.

Security

IDS Rules

Through the use of SmarterMail's intrusion detection system (IDS), there are several methods for preventing abuse and denial of service (DoS) attacks on your mail server. For example, IDS rules (also known as abuse detection rules) can be configured to monitor a variety of activity on the mail server, including the number of connections coming from a single IP address, the number of messages sent within a specific timeframe, the number of login attempts and more. These rules allow SmarterMail to alert System Administrators of suspicious behavior or take action to prevent the attack.

To access the IDS Rules, log into SmarterMail as a System Administrator and click on the Settings icon. Then cick on Security in the navigation pane and select the IDS Rules tab.

Jump To:

IDS Rules Overview

By default, SmarterMail offers several rules that are pre-configured upon installation. These include Denial of Service rules for all major protocols, Brute Force protection for protocols and webmail, and more. The following details can be seen for each entry in the list:

• Type - The type of Abuse Detection rule configured: Denial of Service (DoS), Bad SMTP Sessions (Harvesting), Internal Spammer, Password Brute Force by Protocol or Bounces Indicate Spammer.
• Service - The protocol service associated wtih the rule: SMTP, IMAP, POP, LDAP, or XMPP.

• Action - The action to be taken when the rule is triggered.
• Time Frame - The period of time, in minutes, that is examined to determine if the rule's action should be triggered.

- Threshold - The threshold that is examined to determine if the rule's action should be triggered. For example, the number of messages sent, the number of connections made from an IP address, the number of bounce messages received, etc.
- Block Time - The time frame, in minutes, in which the IP address will be blocked. (NOTE: If a notification email is sent, then this setting is ignored as a Block does not occur.)
- Description - A friendly name or brief description of the rule.

Click on the Actions (...) button and then click Reset IDS Rules to replace all existing rules with the default configuration that's available upon installation.

By default, SmarterMail has several pre-configured IDS Rules for System Administrators. These rules are completely editable, and while most can be deleted as needed, there are 3 Rules that are permanent:

- Password Retrieval Brute Force
- Webmail Brute Force by IP
- Webmail Brute Force by Email

It is possible to edit the settings for these Rules, but they are permanent due to the likelihood of a System Administrator having brute force attacks against their various webmail URLs. To help mitigate these issues, SmarterMail has these permanent Rules in place as they are the most common types of attacks agains mail servers.

IDS Rules

To create a new Abuse Detection rule, click the New button. When adding or editing an entry, the following configuration settings will be available, based on the Detection Type chosen:

Denial of Service (DoS)

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

- Service - Where applicable, select the service that will be monitored for this type of attack: SMTP, IMAP, POP, XMPP or LDAP.
- Time Frame (Minutes) - The period of time, in minutes, that is examined to determine if an IP address should be blocked. Too many connections in this period of time, and a block will be initiated.
- Connections Before Block - The number of connections before a block is placed. It is common for several connections to be open at once from an IP address. Set this to a relatively high value

so that you can catch DoS attacks while not impacting legitimate customers.

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

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

Bad SMTP Sessions (Harvesting)

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

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

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

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

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

Internal Spammer

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

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

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

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

• Block Time (Minutes) - The number of minutes that a block will be placed once an IP address hits the threshold. (NOTE: If a notification email is sent, then this setting is ignored as a Block does not occur.)

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

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

Password Brute Force by Protocol

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

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

Bounces Indicate Spammer

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

- Action - Choose whether to send a notification email only, block messages from the sender or quarantine messages from the sender.
- Time Frame - The period of time, in minutes, that is examined to determine if the rule triggers. Too many emails from a single sender in this period of time, and the email notification is sent and the Action chosen is performed.
- Bounce Threshold - After this many bounce messages are received within the time period specified, the email notification is sent and the Action chosen is performed.
- Block Time (Minutes) - The number of minutes that a block will be placed once an IP address hits the threshold. (NOTE: If a notification email is sent, then this setting is ignored as a Block does not occur.)
- Notify Email - The email address of the administrator account to which the notification will be sent.
- Description - A friendly name or brief description of the rule.

Blacklist / Whitelist

System Administrators are able to control the IP addresses that are blacklisted from accessing, or whitelisted for access to, mail services. Blacklisting an IP address prevents it from making inbound

connections, while whitelisting an IP address adds the IP as a trusted source, allowing connections to bypass relay restrictions that may be imposed, including spam filtering, greylisting and IDS rules. Exercise caution when granting whitelist status to a server, and be sure that you know what services on that server may send mail through your own.

To manage the blacklist or whitelist, log into SmarterMail as a System Administrator and click on the Settings icon. Then click on Security in the navigation pane and select the Blacklist or Whitelist tab.

By default, both of these tabs will be empty as SmarterMail has no way of knowing the IPs or IP Ranges that need to be blocked or granted access to its various services. To create a new entry in the blacklist or whitelist, click New . When adding or editing an entry, the following options will be available:

- IP Addresses (single, range or CIDR block) - Enter a single IP address or an IP range in dotted quad notation (e.g., 123.45.678.90, or 12.345.67.89 - 12.345.67.890). If an IP range is entered, all IP addresses within that range will be contained in the list.
- Description - Use this field to enter optional notes for understanding the various whitelist / blacklist entries. For example, "Office LAN IPs"
- Protocol - Enable this setting to add the protocols you wish to include in the blacklist or whitelist entry. The available options are: SMTP, POP, IMAP and XMPP.
- SMTP Auth Bypass - Used for whitelists only, enabling this bypasses the need for SMTP authentication for whitelisted IPs.
- SMTP Spam Bypass - Used for whitelists only, enabling this bypasses spam checks for whitelisted IPs.

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

SMTP Auth Bypass

Whitelisted IP addresses can bypass SMTP authentication, which is a security measure that can be very beneficial in the fight against spam and unauthorized email as it forces the sender to authenticate their username and password before an email is sent through the mail server. Unfortunately, some applications do not have support for SMTP authentication when sending mail. Most often, these are web sites that have automated mail sending mechanisms. The solution is to add the IP addresses of these servers/sites to SmarterMail's Whitelist and enable SMTP Authentication Bypass. Whitelist entries with SMTP Auth Bypass enabled will not be asked to provide an SMTP Authentication login.

Blacklist / Whitelist

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

To manage the blacklist or whitelist, log into SmarterMail as a System Administrator and click on the Settings icon. Then click on Security in the navigation pane and select the Blacklist or Whitelist tab.

By default, both of these tabs will be empty as SmarterMail has no way of knowing the IPs or IP Ranges that need to be blocked or granted access to its various services. To create a new entry in the blacklist or whitelist, click New . When adding or editing an entry, the following options will be available:

- IP Addresses (single, range or CIDR block) - Enter a single IP address or an IP range in dotted quad notation (e.g., 123.45.678.90, or 12.345.67.89 - 12.345.67.890). If an IP range is entered, all IP addresses within that range will be contained in the list.
- Description - Use this field to enter optional notes for understanding the various whitelist / blacklist entries. For example, "Office LAN IPs"
- Protocol - Enable this setting to add the protocols you wish to include in the blacklist or whitelist entry. The available options are: SMTP, POP, IMAP and XMPP.
- SMTP Auth Bypass - Used for whitelists only, enabling this bypasses the need for SMTP authentication for whitelisted IPs.
- SMTP Spam Bypass - Used for whitelists only, enabling this bypasses spam checks for whitelisted IPs.

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

SMTP Auth Bypass

Whitelisted IP addresses can bypass SMTP authentication, which is a security measure that can be very beneficial in the fight against spam and unauthorized email as it forces the sender to authenticate their username and password before an email is sent through the mail server. Unfortunately, some

applications do not have support for SMTP authentication when sending mail. Most often, these are web sites that have automated mail sending mechanisms. The solution is to add the IP addresses of these servers/sites to SmarterMail's Whitelist and enable SMTP Authentication Bypass. Whitelist entries with SMTP Auth Bypass enabled will not be asked to provide an SMTP Authentication login.

SMTP Blocks

SMTP Blocks are an effective method for temporarily preventing a domain or indiviual user from sending email from the server. For example, if a particular account is sending an abnormal amount of email, you can add their address to the SMTP Blocks list and they will be unable to send email until you remove them. Users and/or domains can be left on the list for whatever time you deem appropriate. This action can be an effective stop-gap versus actually deleting the user and/or domain from the server, giving users or Domain Admininstrators the ability to clean up their act before having their mail server privileges revoked.

To access the SMTP Blocks, log into SmarterMail as a System Administrator and click on the Settings icon. Then click on Security in the navigation pane and select the SMTP Blocks tab.

To create a new block, click on New . When adding or editing an entry, the following configuration settings will be available, based on the Block Type chosen:

SMTP Blocking

- Block Type - Whether the block affects an email address or an entire domain, or an EHLO domain. An "EHLO domain" is the return value given when SmarterMail sends the EHLO or HELO command. A standard EHLO domain is the fully qualified domain name set up for the mail server you're wanting to block. (E.g., "mail.your_domain.com".) However, it IS possible that it will be something different based on whether the command is sent by the SmarterMail web interface or an email client. For example, it may be the local IP address of the sending machine. Therefore, there is no well-established rule for what should be entered until some testing is done by the System Administrator.
- Blocked Address - The complete email address of the user, the domain name or the value used for the EHLO domain.
- Direction - For user/domain (non-EHLO domain) blocks, this refers to the types of messages that should be blocked from sending: Inbound, Outbound or All Messages.
- Description - A friendly name or brief description of the block.

Note: SMTP blocking does NOT occur immediately when the EHLO command is given. Instead, a "soft" block is used and SmarterMail will fail any authentication attempts or RCPT TO commands. This is because if the failure occurs right after the EHLO commaned, any person attempting to spam from a mail server could figure out what the problem is and change the domain given with the

command on each send. A "soft" failure should, instead, make the spammer believe he is using an incorrect password.

System Messages

SmarterMail sends a variety of automated email messages for certain actions within SmarterMail. For example, system messages are sent to users when their password has expired or is in violation of the password policies set up for their domain. Administrators can modify certain messages sent out from the server to make them match a company's voice and style, add extra information or add a standard From address. If a system message does not have a From address, the system message will appear to come from "noreply@" the SmarterMail domain that made the request. For example, if a password reset request is made for a user on example.com, and there's no From address set for the system password reset request message, the user will receive that reset email from "noreply@example.com". NOTE: if the domain already has a "noreply@" account, alias or mailing list set up, they are not affected by this functionality.

To access this section, log into SmarterMail as a System Administrator and click on the Settings icon. Then click on System Messages in the navigation pane.

Click on a message's row to edit the text. The following settings will be available:

- Subject - The subject of the email. In some cases, the subject will contain system variables. It's a good idea to leave these variables "as-is" in the subject.
- Message Body - The message body of the email.
- From Address - By default, system messages send from "System Administrator" without a From address. Administrators can add a From address to allow users to respond to system messages or to decrease the likelihood a message will be caught by spam filters.
- Display Name - The friendly name or description of the sender that will appear in conjunction with the From address (if included) in the From field of the email.