Manage

Help Documentation

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□s mail server address and port from that user□s email 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□tremove 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□semails, 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□saccount. Note: The user□sfolder 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□semail 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□sAccount, 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.