Manage

Help Documentation

Manage

Spool

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, click the Manage icon and expand the Spool in the navigation pane. To view all messages in the spool, both incoming and outgoing, click All Messages . To only view the messages waiting to be delivered, click Waiting to Deliver .

In general the following columns are available:

- Checkbox - Use these boxes to select multiple messages. Messages must be selected before choosing an action from the content pane toolbar.
- File Name - The filename on the hard disk.
- 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.
- Status - The current status of the message.
- Next Attempt - The date and time of the next delivery attempt.

The following actions are available from the content pane toolbar:

- Actions - Click this button and select the appropriate option to force the message, reset retries or change the priority of a message in the spool.

• Force - Pushes the message to the top of the spool. Note: The status of forced messages will not update until the server passes through the spool.
• Reset Retries - Resets the retry counts on all messages in the spool, effectively starting the delivery process over. This can be useful if a DNS or firewall problem has been recently resolved, or if you are using SmartHosting and the target server was down.
• Set Priority - Changes the priority level of a message.
• View - Click this button and select the appropriate option to view the text of a selected message or to see the list of recipents for the selected message.

• Message - Displays the text of the selected message in a new window.
• Recipients - Allows the system administrator to see who the message was sent to and the status of that message (i.e. delivered or pending).
• Delete - Clicking this button will allow the system administrator to delete messages from the spool. Note: No confirmation dialog will display, so use caution when deleting from the spool.
• Refresh - Clicking this button will allow the system administrator to update the page with the most recent contents of the spool.

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, click the manage icon and expand the Spool folder in the navigation pane. Then click Spam Quarantine . A list of messages currently under quarantine because they were flagged as spam by SmarterMail's antispam measures (including the Cyren Premium Antispam add-on, if enabled) will load in the content pane and the following columns will be available:

• Checkbox - Use these boxes to select multiple messages. Messages must be selected before choosing an action from the content pane toolbar.
• File Name - The filename on the hard disk.

- Date - The date the message was flagged for quarantine.
- Sender - The email address that initially sent the email.
- Recipients - The total number of recipients.
- Size - The total size of the message on the hard drive, in kilobytes.
- Time In Quarantine - The amount of time the message has been quarantined.
- Time of Removal - The amount of time until the message is automatically removed from quarantine and permanently deleted.

The following actions are available from the content pane toolbar:

- Actions - Click this button and select the appropriate option to resend a quarantined message.

- Resend - Moves the selected message(s) to the spool for delivery to its intended recipients.
- View - Click this button and select the appropriate option to view the text of a selected message or to see the list of recipents for the selected message.

- Message - Displays the text of the selected message in a new window.
- Recipients - Allows the system administrator to see who the message was sent to.
- Delete - Clicking this button will allow the system administrator to delete messages from quarantine.
- Refresh - Clicking this button will allow the system administrator to update the page with the most recent quarantined spam messages.

Note: Spam quarantine settings can be managed from the Antispam Administration page. To access this page, click the security icon and click Antispam Administration . The quarantine settings are on the SMTP Blocking tab.

Virus Quarantine

System administrators can quarantine outgoing messages that have been flagged as containing viruses by SmarterMail's ClamAV or the Cyren Zero-hour Antivirus add-on for a maximum of 30 days. Quarantining such messages allows administrators to investigate false positives and make appropriate adjustments or notify the developer of the virus scanner, if necessary.

To view a list of quarantined virus messages, click the manage icon and expand the Spool folder in the navigation pane. Then click Virus Quarantine . A list of messages currently under quarantine because they were flagged for a virus by SmarterMail antivirus measures will load in the content pane and the following columns will be available:

- Checkbox - Use these boxes to select multiple messages. Messages must be selected before choosing an action from the content pane toolbar.

- File Name - The filename on the hard disk.
- Date - The date the message was flagged for quarantine.
- Sender - The email address that initially sent the email.
- Recipients - The total number of recipients.
- Size - The total size of the message on the hard drive, in kilobytes.
- Time In Quarantine - The amount of time the message has been quarantined.
- Time of Removal - The amount of time until the message is automatically removed from quarantine and permanently deleted.

The following actions are available from the content pane toolbar:

- View - Click this button and select the appropriate option to view the text of a selected message or to see the list of recipents for the selected message.

- Message - Displays the text of the selected message in a new window.
- Recipients - Allows the system administrator to see who the message was sent to.
- Delete - Clicking this button will allow the system administrator to delete messages from quarantine.
- Refresh - Clicking this button will allow the system administrator to update the page with the most recent quarantined virus messages.

Note: Spam quarantine settings can be managed from the Antivirus Administration page. To access this page, click the security icon and click Antivirus Administration . The quarantine settings are on the Options tab.

User Activity

System administrators can use this section to monitor the activity of users on the server.

To view a list of users currently logged in to SmarterMail, click the Manage icon . Then expand User Activity and click Online Users in the navigation pane. A list of users that are online will load in the content pane.

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

- User - The name of the user.
- Type - The connection type. For example, IMAP or webmail.
- IP Address - This will tell the IP address of the user.
- Start Date - The start date and time of the connection.
- Duration - The length of the connection.

In general, the following options are available in the content pane toolbar:

- End Session - End the selected user's session.
- Disable User - Permanately disables the user from logging in to the system.
- Refresh - Refreshes the list of online users.

If you seen any anonymous users, there could be a number of reasons why. For example, these could be people who have the login page open in a browswer but they're not logged in or perhaps there is a monitoring app or service that is monitoring whether a login page responds to ping, etc.

Inactive Users

To view a list of inactive users, click the Manage icon . Then expand User Activity and click Inactive Users in the navigation pane. Then select whether you want to view users that have been inactive for 30 days, 90 days, 6 months, or 12 months.

Viewing inactive users is a good way to clean out users for a domain that are no longer needed. Perhaps these users and their mailboxes can be archived or copied and moved to another location to recover some disk space.

Current 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 a system administrator may need to help a migration along - or even stop it altogether. That's where the Current Migrations page comes in.

To view any current mailbox migrations occurring on a server, click the Manage icon . Then expand User Activity and click Current Migrations in the navigation pane. A list of all current mailbox migrations will load in the content pane.

In general, system administrators can view the following attributes of current migrations:

- User - The name 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.

In general, the following options are available in the content pane toolbar:

- End Session - End the selected user's migration. The migration will be stopped, regardless of where it is in process. As 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 shows as "Completed."
- Refresh - Refreshes the list of current mailbox migrations and their status.

Current Connections

SmarterMail will monitor the server and see who is connecting via the different protocols - SMTP, IMAP, POP and XMPP. System administrators can then blacklist a certain user if they believe a user is making too many connections. Connections can be viewed by protocol or all connections can be viewed at one time.

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 bring from a single source. Another thing to note is an "anonymous" connection. An "anonymous" user is someone who has created a session without logging in. For instance, if they hit the login page and don't actually log in, that will create a new session marked as anonymous. You can get a large number of these if a search engine attempts to index your site or if you have an uptime service monitoring your login page.

To view the current connections, click the manage icon and expand Current Connections in the navigation pane. Then click the appropriate connection type.

Current Blocks

This report displays all IPs that have been blocked by the mail server as a result of any abuse detection rules a system admin set up in SmarterMail's Security management area. As a result of these rules, SmarterMail will monitor the server and keep track of all users who are currently being blocked for SMTP, IMAP, POP, LDAP, XMPP 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.

System adminstrators can select an IP and click Delete in the content pane toolbar to remove an IP from the list. However, this does not affect the abuse detection rule that blocked the IP in the first place, it just removes the block from the IP.

Mass Messaging

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

Send Email

To send a mass email, click the manage icon . Then expand Mass Messaging in the navigation pane and click Send Email . The mass messaging options will load in the content pane 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 in the content pane toolbar to send the message.

Send Reminder

Reminders are a quick and easy way to send a follow-up to a previous, more detailed and stylized mass 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 Reminder to do a quick follow up reminding the users of the scheduled work.

To send a reminder, click the manage icon . Then expand Mass Messaging in the navigation pane and click Send Reminder . The mass messaging options will load in the content pane 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 in the content pane toolbar to send the message.

Services

System administrators can 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 a system administrator will 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.

To view the status of the services, click the manage icon and then click Services in the navigation pane. The list of available services will load in the content pane and the following columns will be available:

- Checkbox - Use these boxes to select multiple services. Services must be selected before choosing an action from the actions toolbar.
- Service - The name of the servivce.
- Status - The current status of the service, either Active or Inactive.
- Description - A brief summary of the service.

The following options will be available in the content pane toolbar:

- Start - Enables the service.
- Stop - Disables the service.

Services

In general, system administrators can enable/disable the following services:

- IMAP - A client/server protocol in which email is received and held by the mail server. IMAP requires continual access to the client during the time that it is working with the mail server.
- IMAP Retrieval - With IMAP retrieval, mail is retrieved from external IMAP servers (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 e-mail. However, since it's limited in its ability to queue messages at the receiving end, it's usually used with one of two other protocols, POP or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP or IMAP for receiving messages from their local server.

• Spool - The internal message queue used to deliver messages locally and to remote services.

• SyncML - An open synchronization techology that is most commonly used to synchronize mail account data (calendars, contacts, etc.) between a mail server and a mobile device.

• 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.

View Logs

System administrators can 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.

To view logs, click the manage icon and click View Logs in the navigation pane. The following options will be available in the content pane:

- Date - The start and end dates for the log files you want to view.
- Type - Select the type of log file (or the delivery method of the files) that you would like to view.
- Search String - Type the words or phrases to that should be contained in the log files.
- Display related traffic - Select this option to only display data that occurred within the same sesion.

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

Alternatively, system administrators can download the log file in a .zip format by clicking Download in the content pane toolbar. This page allows administrators to get quick access to a domain's entire log file so that they can review them more thoroughly on their local machine.

Message Archive Search

This feature is available to domain administrators and/or system administrators using SmarterMail Enterprise.

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

It is important to note that message archive search is availalbe to domain administrators only when rules are set up individually for their specific domains. If archiving is set up for "all domains" on a server, then only the system admininstrator will be able to search the message archive. Therefore, if a domain admin needs access to the email archive for the domain "example.com", then a new Message Archiving rule for example.com needs to be set by the system admin.

When message archiving is set up for a specific domain, that domain's administrator will see a Message Archive Search option in the navigation pane when they click on the Email icon. It will generally appear under My Today Page . Domain adminstrators can search for a message by date range, the sender's address, the recipient's address, or the subject.

System administrators can perform a message archive search by clicking on the manage icon and then clicking Message Archive Search in the navigation pane. System administrators can search for a message by date range, the sender's address, the recipient's address, or the subject.

For more information on archiving, see Message Archiving .

Indexing Status

SmarterMail Search Indexing allows users to instantly find any files -- including messages, attachments, appointments, contacts, tasks, or notes -- in their mailbox. 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.

To view the indexing status, click the manage icon and click Indexing Status in the navigation pane. A list of users being indexed (Processing) or users awaiting indexing (Queued) can be viewed.

Password Policy Compliance

System administrators can use the password policy compliance page to find users whose passwords do not meet any configured password requirements. Non-compliant users can then be notified via email that they need to change their passwords in accordance with the password requirements to maintain the security and integrity of the mail server.

To view a list of non-compliant users, click the Manage icon . Then click Password Policy Compliance in the navigation pane. A list of non-compliant users will load in the content pane and the following columns will be available:

- Checkbox - Use these boxes to select multiple users. Users must be selected before choosing an action from the content pane toolbar.
- User - The username that is non-compliant.
- Domain - The domain on which the user exists.

In general, the following options are available in the content pane toolbar:

- Send Email - Allows the system administrator to compose a message to send to the selected user(s), informing the user(s) of their non-compliance and advising the user(s) of how to remedy the situation and become compliant with the password policy for the domain.