Settings

Help Documentation

Settings

General Settings

To access the general settings for SmarterMail server, click the settings icon and click General Settings in the navigation pane. The general settings will load and the following tabs will be available:

Server Info

Use this tab to specify the following server settings:

- Hostname - The hostname of the server. Note: Hostnames should be in the format computername.domain.com.
- Postmaster Mailbox - This is usually the mail server system administrator's email address as this is where errors in e-mail processing are generally directed.
- IP of Primary DNS - The IP address of the primary DNS server. If left blank, the DNS server information will be pulled from the the Windows Networking settings (recommended).
- IP of Secondary DNS - Enter the IP address of the secondary DNS server. If left blank, the DNS server information will be pulled from the the Windows Networking settings (recommended).
- Logout URL - The URL to which users are redirected when they log out of SmarterMail. By default, users are presented with the log in page for the mail server. If this should be different, a new URL can be added.
- Enable domain admins to override logout URL - Select this option to allow domain administrators to specify a Logout URL for their domain. If this option is not enabled, the option will not be visible to domain administrators.

Spool

Use this tab to specify the following spool settings:

- Spool Path - The full path in which messages are stored prior to delivery. If you are using a real-time virus scanner, this is the path that must be scanned in order to properly handle viruses.
- SubSpools - SubSpools are within the spool path and allow SmarterMail to work around the NTFS limitation of 30,000 objects in an individual folder. SmarterMail will utilize subspools by allocating up to 10,000 messages per subspool. (Default is 10)
- Delivery Delay - This number of seconds mail will be held in the spool before it is delivered. A delivery delay is beneficial when you are running a secondary service (such as a virus checker) that needs access to messages prior to delivery, as it provides ample time for the secondary service to interact with the message. By default, the delivery delay is 15 seconds.

• Retry Intervals - When the mail server is unable to contact the receiving server, the email attempting to be sent is held for a period of time before the mail server attempts to resend it. This is the time between retries. Users can specify multiple retry attempts to resend emails before it is bounced. By default, this is set to 4 attempts - at 15 min, 30 min, 60 min, and 90 min intervals.
• Bounce DNS errors after - The maximum number of attempts SmarterMail should make before the message is bounced due to a DNS error. The most common cause of a DNS error is a misspelled domain. Limiting the number of attempts before DNS errors are bounced is beneficial because messages will not sit in the queue for long periods of time taking up processing on the mail server and possibly slowing the system down. This will be helpful to users because messages will be bounced sooner and will give users the opportunity to fix any mistakes and get a message resent. By default, the server will make 2 attempts. Note: Setting this at 1 retry can be dangerous if the DNS server fails or if there is a loss of Internet connectivity. To disable this feature, set the number of bounces equal to the number of retry intervals.
• Notify senders of delay after - Sets the number of delivery attempts before the sender is notified that the email delivery is delayed. This can be beneficial as it lets the sender know that the mail server is still attempting to deliver the message but that the recipient has not received it yet.
• Command-Line File - Enable this and enter the full path to an executable you wish to use to process incoming messages. Use %filepath as an argument to pass the path of the email file to the executable. It is allowable for the executable to delete the message to prevent delivery. Example: If you set this field to "c:\program files\myexe.exe %filepath", the program myexe.exe will be launched with the full path to the spool file as its first argument. Note: The command will not be executed if the Enabled box is not checked.
• Command-Line Timeout - The number of seconds that the server will wait for information from the remote server. In general, a timeout of 5 seconds should suffice.
• bounce.io API Token - This setting has been deprecated as bounce.io has discontinued their service.

Reports

Use this tab to specify the following settings:

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

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

Indexing

Use this tab to specify the following settings:

• 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.
• 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.
• 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.
• 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.
• 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.
• 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.

System Administrators

SmarterMail allows a single installation to have multiple system administrator logins, each with their own unique login and password. To view a list of system administrator accounts, click the settings icon and click System Administrators in the navigation pane. A list of users with system administrator access will load in the content pane and the following options will be available in the content pane toolbar:

• New - Creates a new system administrator account.
• Edit - Edits the selected system administrator account.
• Delete - Permanently deletes the selected system administrator account(s).

Creating New System Administrators

To create a new system administrator account, click New in the content pane toolbar. The system administrator settings will load in a popup window and the following tabs will be available:

Options

Use this tab to specify the following settings:

- Username - The identifier used to login to SmarterMail.
- New Password - The password used to login to Smartermail.
- Confirm Password - Re-type the password used to login to Smartermail.
- Description - A brief description of the administrator. For example, "for support department".
- Enable login access by IP address - Select this option to only allow system administrators to login from certain IP addresses.

Login Access

Use this tab to specify the IP address or IP range from which system administrators can login to SmarterMail. Note: This tab is only accessible if the option to enable login access by IP address was selected in the Options tab.

Protocol Settings

To access the settings for standard email protocols, click the settings icon and click Protocol Settings in the navigation pane. The protocol settings will load and the following tabs will be available:

POP

Use this tab to specify the following POP settings:

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

- #HostName# - The hostname of the IP address to which the connection is made.
- #ConnectedIP# - The IP address of the remote computer.
- #Time# - The system's local time.
- #TimeUTC# - The time in UTC.
- #UnixTime# - The number of seconds since January 1, 1970.
- Command Timeout - If the server receives a command that sends large amounts of data but the data stops coming in for this number of minutes, the command will be aborted. By default, the command times out after 5 minutes.

• Max Bad Commands - After this many unrecognized or improper commands, a connection will be automatically terminated. By default, the maximum number of bad commands is 8.
• Max Connections - Some protocols in SmarterMail allow you to specify the maximum number of connections. Increasing this value allows SmarterMail to handle more connections of that type at once, but results in higher CPU and memory utilization. By default, the maximum number of connections is 500.
• POP Retrieval Download Path - The path in which mail is stored from POP accounts until it is read.
• Max POP Retrieval Threads - SmarterMail is multi-threaded, meaning it can do more than one thing at a time. This setting is for the maximum number of threads you want SmarterMail to work on concurrently for retrieving mail using the POP protocol. By default, the maximum number of POP retrieval threads is 10.
• POP Retrieval Interval - The frequency by which SmarterMail checks for new POP messages. By default, the POP retrieval interval is 1 minute.
• Autodiscover Host - The URL of the mail server (e.g., mail.domain.com) to be returned by an auto discover query.
• Autodiscover Port - The port to autodiscover uses to communicate with the mail server.
• SSL - Check this box to enable autodiscover to use SSL. NOTE: Autodiscover generally requires the use of SSL, especially when used with Microsoft Outlook.

IMAP

Use this tab to specify the following IMAP settings:

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

• #HostName# - The hostname of the IP address to which the connection is made.
• #ConnectedIP# - The IP address of the remote computer.
• #Time# - The system's local time.
• #TimeUTC# - The time in UTC.
• #UnixTime# - The number of seconds since January 1, 1970.
• Command Timeout - If the server receives a command that sends large amounts of data but the data stops coming in for this number of minutes, the command will be aborted. By default, the command times out after 15 minutes.
• Max Bad Commands - After this many unrecognized or improper commands, a connection will be automatically terminated. By default, the maximum number of bad commands is 8.
• Max Connections - Some protocols in SmarterMail allow you to specify the maximum number

of connections. Increasing this value allows SmarterMail to handle more connections of that type at once, but results in higher CPU and memory utilization. By default, the maximum number of connections is 1000.

• IMAP Retrieval Download Path - The path in which mail is stored from IMAP accounts until it is read.

• Max IMAP Retrieval Threads - The maximum number of threads you want SmarterMail to work on concurrently. By default, the maximum number of POP retrieval threads is 10.

• IMAP Retrieval Interval - The frequency by which SmarterMail checks for new IMAP messages. By default, the IMAP retrieval interval is 10 minutes.

• Enable IDLE Command - Select this checkbox to enable IMAP IDLE. IMAP idle is an extension of the IMAP protocol that allows a mail server to send status updates in real time. Through IMAP IDLE, users can maintain a connection with the mail server via any mail client that supports IMAP IDLE, allowing them to be instantly aware of any changes or updates. When enabled, SmarterMail will inform any connecting IMAP client that it accepts the IDLE command. Note: IMAP clients that do not fully support IMAP IDLE, like Microsoft Outlook, may use the command in such a way that it actually hinders performance.

• Autodiscover Host - The URL of the mail server (e.g., mail.domain.com) to be returned by an auto discover query.

• Autodiscover Port - The IMAP port returned when autodiscover communicates with the mail server. System administrators can modify this port as needed to accommodate firewall settings, etc.

• SSL - Check this box to enable autodiscover to use SSL. NOTE: Autodiscover generally requires the use of SSL

LDAP

Use this tab to specify the following LDAP settings:

• Session Timeout - After a connection fails to respond or issue new commands for this number of seconds, the connection will be closed. By default, the session times out after 300 seconds.

• Command Timeout - If the server receives a command that sends large amounts of data and the data stops coming in for this number of seconds, the command will be aborted. By default, the command times out after 120 seconds.

SMTP In

Use this tab to specify the following incoming SMTP settings:

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

supports the use of the following variables, which will be replaced with their corresponding values:

• #HostName# - The hostname of the IP address to which the connection is made.
• #ConnectedIP# - The IP address of the remote computer.
• #Time# - The system's local time.
• #TimeUTC# - The time in UTC.
• #UnixTime# - The number of seconds since January 1, 1970.
• Allow Relay - If you are concerned about spam mailers using the relay function to send mail through your server or do not want any other mail server to use your SMTP server as a gateway, set this to Nobody (recommended). However, you can set the type of relays you will allow, should you so desire.

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

the max hop count is 20.

• Max Message Size - Messages greater than this size will be rejected by the mail server. By default, the max message size is 0 (unlimited).

• Max Bad Recipients - At times, spammers will hammer a domain with a dictionary harvesting attach. This means that sofware is used to send messages to many of the most common mailbox addresses (e.g., admin, user, contact, etc.) or username variations (e.g., alan@, alana@, alanb@, etc.) in order to find valide email addresses. Setting the max bad recipients means that after this many bad recipients (those that don't exisit for the domain), the SMTP session will be terminated. This setting allows you to better protect yourself against email harvesting attacks. A value of 20 is recommended in most cases.

• Append Received Line - Select the option for appending the received line for all messages, only for SMTP Authenticated messages or for no messages at all.

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

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

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

• Allow relay for authenticated users - Select this checkbox to enable the "Allow Relay" setting from above when users are required to use SMTP Authentication for sending messages.

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

• Disable AUTH LOGIN method for SMTP authentication - Select this checkbox to disable plain text authentication.

• Autodiscover Host - The URL of the mail server (e.g., mail.domain.com) to be returned by an auto discover query.

• Autodiscover Port - The SMTP In port returned when autodiscover communicates with the mail server. System administrators can modify this port as needed to accommodate firewall settings, SMTP restrictions by ISPs, etc.

• SSL - Check this box to enable autodiscover to use SSL. NOTE: Autodiscover generally requires the use of SSL

SMTP Out

Use this tab to specify the following outgoing SMTP settings:

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

• Outbound IPv6 - The IPv6 address used to connect to external SMTP servers when a message is sent by the domain. If multiple IPv6 IPs are on the server, they will be listed in the dropdown.

• Enable Primary IP on failure - Select this checkbox to have SmarterMail automatically fall back to the primary IP when a failure has occurred. SmarterMail will only attempt to connect once if this option is enabled.
• Command Timeout - If the server receives a command that sends large amounts of data but the data stops coming in for this number of seconds, the command will be aborted. By default, the command times out after 60 seconds.
• Max Spam Check Threads - The maximum number of messages that can be spam checked at one time. By default, the maximum spam check threads is 30.
• Max Delivery Threads - The maximum number of messages that can be sent at one time to email addresses that are not on the local server. If a message cannot be sent, the SmarterMail server's multi-threading capabilities will move on to the next message and eventually get back to the one it skipped. This action can save tremendous amounts of time when compared to some other mail servers that stall the spool if a message cannot be sent right away. By default, the max delivery threads is 50.
• Enable DNS Caching - Select this checkbox to cache the results of DNS calls in SmarterMail. This can help speed up delivery of messages.
• Enable TLS if supported by the remote server - Select this checkbox to use TLS (SSL encryption) if the server you are connected to supports it.
• Append authenticated as header for outgoing messages - Checking this box means that outgoing messages will have a new line item in the message header called "x-smartermail-authenticatedas" that demonstrates that the message sender was verified using SMTP authentication. This header can then be used by anti-spam services for validation.

XMPP

Use this tab to specify the following XMPP settings:

• Max Connections - Some protocols in SmarterMail allow you to specify the maximum number of connections. Increasing this value allows SmarterMail to handle more connections of that

type at once, but results in higher CPU and memory utilization. By default, the maximum number of connections is 1000.

• Web Chat URL Listeners - The URLs that XMPP services should listen to in order to ensure live chat connections are made. Examples include "http://+:80/http-bind/" or "https://+:443/http-bind"

EWS

• Modification Auto Clean - SmarterMail records when an account syncs using Exchange Web Services and stores those sync sessions in a file. This setting tells SmarterMail how long to keep those sync sessions before they are automatically purged from the file.

• Autodiscover Host - The URL of the mail server (e.g., mail.domain.com) to be returned by an auto discover query when Exchange Web Services are enabled.

EAS

• Autodiscover Host - The URL of the mail server (e.g., mail.domain.com) to be returned by an auto discover query when Exchange Active Sync is enabled.

Log Settings

System administrators can use this section to manage how logs are written and how much detail is included in SmarterMail's logs.

To access the log settings, click the settings icon and click Log Settings in the navigation pane. The log settings will load in the content pane and the following tabs will be available:

Log Files

Use this tab to specify the following settings:

• Log Path - The default location for the Logs that email messages in SmarterMail produce. If you would like to change the default location, enter a new path here.

• 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.

• Enabled - Select this option to allow log files to be deleted after a specific number of days.

Log Detail Levels

Use this tab to specify how detailed the logs should be:

- Exceptions Only - Small size logs that record only errors.
- Normal - Medium size logs that record most activity taken on the mail server.
- Detailed - Very detailed logs that can get very large. Only enable this option when asked to by SmarterTools Support, or when troubleshooting server operations.

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

System administrators can apply these settings to the following log file types:

- ActiveSync - The log level for Exchange ActiveSync connections.
- Administrative - The log level for for any changes and/or modifications made by system administrator accounts.
- Delivery - The log level for message delivery and spool operations.
- Events - The log level for event sessions.
- EWS - The log level for Exchange Web Services sessions.
- IMAP - The log level for IMAP sessions.
- IMAP Retrieval - The log level for IMAP retrieval sessions.
- Indexing - The log level for SmarterMail indexing.
- LDAP - The log level for LDAP sessions.
- Mailbox Importing - The log level for data imported during mailbox migrations.
- 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 - The log level for POP sessions.
- POP Retrieval - The log level for POP retrieval sessions.
- SMTP - The log level for SMTP sessions.
- SycnML - The log level for SyncML sessions.
- WebDAV - The log level for CalDav and CardDav sessions.

Note: By default, SmarterMail sets all log detail levels to exceptions only.

ActiveSync Mailboxes

Microsoft Exchange ActiveSync (EAS) is the industry standard for synchronizing email clients and mobile devices with email servers such as SmarterMail. Using EAS you can synchronize email, contacts and calendars with a number of email clients such as Microsoft Outlook 2013 as well as with smartphones, tablets and "phablets" from Apple, HTC, Samsung and others.

System administrators will use this section to enable and disable the EAS add-on for mailboxes across all domains on the SmarterMail server. Domain administrators will use this page to manage the EAS

add-on for their particular domain. Note: Before an administrator can configure a mailbox to sync using ActiveSync, the add-on needs to be activated and available for users of the domain. For more information, please refer to the KB article How To Activate Microsoft Exchange ActiveSync .

To access this section, click the settings icon and click ActiveSync Mailboxes in the navigation pane. A list of accounts for which the Exchange ActiveSync add-on is enabled will load in the content pane.

In general, the following columns are available:

- Checkbox - Use these boxes to select multiple mailboxes. Mailboxes must be selected before choosing an action from the actions toolbar.
- Email Address - The email address of the SmarterMail user.

The following options are available from the actions toolbar:

- Add - Adds Exchange ActiveSync to a mailbox on the domain.
- Delete - Removes Exchange ActiveSync from the selected mailbox.

Events

Events Overview

SmarterMail can detect events as they occur, generate messages for those events, and deliver the messages to system administrators and agents that need the information. For more information, see the Events folder of the Help for Users section of the online help.

Notification Profiles

SmarterMail can detect events as they occur, generate messages for those events, and deliver the messages to system administrators and agents that need the information. For example, users can receive notifications when a task is due or system administrators can receive notifications when the disk space for a domain reaches a certain percentage. Notification profiles determine how those messages are sent.

Although users can set up their own notification profiles, some organizations may find it beneficial to create a notification profile that applies to all system administrators. You can use this page to do so.

To view a list of notification profiles, click the settings icon and click Notification Profiles in the navigation pane. Your notification profiles will load in the content pane.

The following columns are available:

- Checkbox - Use these boxes to select multiple profiles. Notification profiles must be selected before choosing an action from the content pane toolbar.
- Notification Profile Name - The name of the profile.
- Type - The types of notification enabled for the selected profile.

The following options are available from the content pane toolbar:

- New - Creates a new notification profile.
- Edit - Edits an existing notification profile.
- Delete - Permanently deletes the selected notification profile(s).

To view a specific notification profile, simply double-click the appropriate profile. The profile will load in the content pane and the following fields will be available:

- Notification Profile Name - The name of the profile.
- Email Address(es) - The email address(es) to which notifications are sent.
- Enable - Select this option to enable email notifications.
- SMS Email Address(es) - The mobile device email address to which notifications are sent.
- Enable - Select this option to enable SMS notifications.
- Enable Reminders for all domain administrators - Select this option to send a reminder to all domain administrators when the event is triggered.

Bindings

IP Addresses

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

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

To access the IP address settings, click the settings icon and expand the Bindings folder in the navigation pane. Then click IP Addresses . A list of IP addresses on the server will load in the content pane and the following options will be availble in the content pane toolbar:

- Edit - Edits the ports assigned to the selected IP.

Ports

System administrators can use this section to assign protocols to ports that can then be assigned to IP Addresses . In addition, this section is used to add Secure Socket Layer (SSL) and Transport Layer Security (TLS) rules to any ports and protocols.

To access the port settings, click the settings icon and expand the Bindings folder in the navigation pane. Then click Ports . A list of ports will load in the content pane and the following options will be availble in the content pane toolbar:

- New - Creates a new port.
- Edit - Edits the selected port options.
- Delete - Permanently deletes the selected port(s).

Creating New Ports

When adding a new port there are several fields that need to be completed. These fields are:

- Protocol - The type of communications protocol that should be used (SMTP, IMAP, LDAP, POP or submission port).
- Encryption - If the port requires SSL or TLS encryption, check the appropriate option. SSL always assumes the connnection will be secure and sends the encryption immediately. TLS connects normally and then looks to see if the connection is secure before sending the encryption.
- Name - The friendly name for the port.
- Port - The port number on which to listen for the selected protocol.
- Description - A simple description of the port and/or the port name.

Hostnames

This feature allows administrators to assign a hostname for each IP address. For example: IP 1.1.1.1 can assigned to mail.domain1.com and IP 1.1.1.2 can be for mail.domain2.com. The benefit of assigning hostnames to IPs is that every domain on the server can be assigned its own IP address, thereby limiting the chances of the entire mail server becoming blacklisted should a user on one domain send out unwanted emails.

To view hostnames, click the manage icon and click Hostnames in the navigation pane. A list of hostnames will load in the content pane and the following options will be available from the content pane toolbar:

- New - Creates a new hostname.
- Edit - Edits the selected hostname.
- Delete - Deletes the selected hostname(s).

Defaults

Domain Defaults

Use this section to create global default settings that will be applied to new domains created through the Web interface or via SmarterMail's extensive Web services. These default settings can be overwritten and are only intended to avoid needless data entry. Note: Modifications to these settings will not affect existing domains.

To access the domain default settings, click the settings icon . Then expand the Defaults folder and click Domain Defaults in the navigation pane. The domain default settings will load in the content pane and the following tabs will be available:

Technical

Use this tab to specify the following technical settings:

- Folder Path - The directory in which all information (XML files, mail statistics, alias information, etc.) pertaining to the domain is saved. By default this is C:\SmarterMail. However, it can be modified as needed.
- Auto-Responder 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.
- 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.
- Calendar Auto Clean - Use this to set a time frame that SmarterMail will use to automatically remove legacy calendar items from users' calendars. This setting can also be managed by

domain administrators.

• Require SMTP Authentication - Select 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.

• Restrict auto-responders to once per day per sender - Select this option to limit how frequently an auto-responder is sent. Continually sending somethign 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.

• Disable greylisting - Select this option to disable the greylisting anti-spam option for the domain. Greylisting, though effective, can lead to a delay in email delivery for a domain.

• Enable users to opt out of LDAP listings - Select this option to allow users to remove themselves from the Global Address List.

• Allow domains to override mailing list message size - Select this option to allow domain administrators to specify the maximum size for mailing list messages.

• 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.

• > Allow users to override personalization settings - Select this option to allow users to modify the look and feel of their webmail experience with customer colors and/or use of custom CSS.

Features

Use this tab to enable or disable the following features:

• ActiveSync Remote Wipe - Select this to allow users with the Exchange ActiveSync add-on to have access to SmarterMail's remote wipe functionality.

• ActiveSync User Management - Select this to allow domain administrators add and delete mailboxes that can use the Exchange ActiveSync add-on.

• bounce.io - This setting has been deprecated as bounce.io has discontinued their service.

• Calendar - Select this option to allow users to use the calendar feature.

• Catch-All Alias - Select this option to allow users to create catch-all email addresses. When enabled, this setting can be managed by domain administrators as well.

• Contacts - Select this option to allow users to use the contacts feature. When enabled, this setting can be managed by domain administrators as well.

• Content Filtering - Select this option to allow users to use content filtering. When enabled, this setting can be managed by domain administrators as well.

• Control of Service Access - Select this option to give domain administrators the ability to manage access to POP, IMAP, SMTP and webmail services for users.

• Domain Aliases - Select this option to allow domain administrator to create domain aliases. When enabled, this setting can be managed by domain administrators as well.
• 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.
• Domain Reports - Select this option to provide additional reports for domain administrators.
• Enable spam filtering - Select this option to show or hide the spam filter settings for domain administrators. Hiding the spam filter settings will prevent domain administrators from changing the weights set by the system administrator for spam checks.
• Email Reports - Select this option to provide the ability to email reports.
• Exchange Web Services (EWS) - Select this option to enable users on the domain to synchronize SmarterMail with supported email clients using Exchange Web Services. Note: For domains that will support inboxes with large volumes of email, IMAP is encouraged as the primary protocol as EWS does not perform well with large amounts of email.
• File Storage - Select this option to allow users to use the file storage feature. When enabled, this setting can be managed by domain administrators as well.
• IMAP Retrieval - Select this option to allow users to download IMAP email from third-party mail servers. When enabled, this setting can be managed by domain administrators as well.
• Live Chat (XMPP) - Select this option to allow users on the domain to chat with each other via the Web interface or any XMPP-compatible chat client. When enabled, this setting can be managed by domain administrators as well.
• Mailing Lists Select this option to allow domain administrators to create and use mailing lists to send mass emails. When enabled, this setting can be managed by domain administrators as well.
• Mail Signing - Select this option to enable email verification via mail signing using DKIM and/or DomainKeys. When enabled, this setting can be managed by domain administrators as well.
• Notes - Select this option to allow users to use the notes feature. When enabled, this setting can be managed by domain administrators as well.
• POP Retrieval - Select this option to allow users to download POP email from third-party mail servers. When enabled, this setting can be managed by domain administrators as well.
• SyncML - Select this option to allow users to sync SmarterMail with Outlook, Thunderbird and most smartphones using SyncML.
• Tasks - Select this option to allow users to use the tasks feature. When enabled, this setting can be managed by domain administrators as well.
• User Reports - Select this option to provide reports for users.

Limits

Use this tab to specify the following limits:

- Disk Space - 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 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 acts as a secondary domain that users can user for sending and receiving emails. 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 (forwarded to a true email account) allowed for the domain. By default, domains are limited to 1,000 user aliases.
- Mailing Lists - The maximum number of mailing lists allowed for the domain. By default, this setting is unlimited.
- Mailing List Max Message Size - The maximum size message that can be sent to a mailing list. By default, the maximum message size is unlimited.
- POP Retrieval Accounts - The maximum number of POP email accounts a user can set up in SmarterMail. By default, users can receive download messages for 10 POP email accounts.
- IMAP Retrieval Accounts - The maximum number of IMAP email accounts a user can set up in SmarterMail. By default, users can receive download messages for 10 IMAP email accounts.
- Max Message Size - The maximum size email a user can send. By default, the max message size is 10,000 KB. Note: This number includes text, HTML, images and attachments.
- Recipients per Message - The maximum number of recipients a message can have. By default, users can send messages to 200 email addresses.
- ActiveSync Accounts> - Sets the maximum number of Microsoft Exchange ActiveSync accoutns a domain can have set up.

Sharing

This tab is only available in SmarterMail Enterprise edition.

Use this tab to enable sharing of the following collaboration features:

- Global Address List - Select this option to allow users on a domain to see all user profiles on the domain and participate in LDAP queries against the domain. When enabled, domain administrators can manage this feature as well.

• Shared Calendars - Select this option to allow calendars to be shared with other users on the domain. When enabled, domain administrators can manage this feature as well.
• Shared Contacts - Select this option to allow contact lists to be shared with other users on the domain. When enabled, domain administrators can manage this feature as well.
• Shared Folders - Select this option to allow email folders to be shared with other users on the domain. When enabled, domain administrators can manage this feature as well.
• Shared Notes - Select this option to allow notes to be shared with other users on the domain. When enabled, domain administrators can manage this feature as well.
• Shared Tasks - Select this option to allow task lists to be shared with other users on the domain. When enabled, domain administrators can manage this feature as well.

Priority

Use this tab to prioritize the remote delivery of certain messages. All messages default to a priority of 5 with a range of 1 to 10. Messages assigned a priority of 10 will have the highest priority and will be delivered first, while messages assigned a priority of 1 will have the lowest priority and will be delivered last.

The use of message delivery priorities also gives system administrators the ability to create automated actions based upon that priority. A common use would be to set up a separate specific outbound gateway to handle all mailing lists to avoid potential blacklisting of the primary IP and to efficiently deliver all messages. The system administrator could then assign all mailing lists a priority of 1, and would set up a gateway to handle only messages with a priority range of 1 to 1.

• Standard Messages - The priority level for messages that don't have another priority affecting it, as detailed below.
• Mailing Lists - The priority level for messages sent to a mailing list.
• Priority When Over Size - The priority level for messages that exceed the message size threshold. For example, system administrators may want to lower the priority of large messages to avoid slowing down the spool.
• Message Size Threshold - The maximum size a message can be without triggering the Priority When Over Size rule.
• Auto-Responders - The priority level for auto-responder messages, such as out-of-office responses.
• Bounces - The priority level for non-delivery receipts.
• Email Reports - The priority level for email reports.
• Appointment Reminders - The priority level for messages reminding users of upcoming appointments, meetings or events.
• Priority After Attempt 1 - The priority level for messages that were not successfully sent after

the specified number of tries.

• Attempt 1 Threshold - The number of retry attempts the system should make before the priority set in Priority After Attempt 1 is assigned to the message.

• Priority After Attempt 2 - The priority level for messages that were not successfully after the specified number of tries.

• Attempt 2 Threshold - The number of retry attempts the system should make before the priority set in Priority After Attempt 2 is assigned to the message.

Throttling

Throttling allows system administrators to limit the number of messages sent per hour and/or the amount of bandwidth used per hour to send messages. If the throttling threshold is reached, messages will stop sending for the remainder of the hour. Then the system will resume sending messages.

Use this tab to edit the following throttling settings:

• Outgoing 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.

• Outgoing Bandwidth 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 - The number of non-delivery receipts a domain can receive per hour. 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.

Event Restrictions

Use this tab to enable the following event types and categories:

Alias

• Enable Alias Added Event - Select this option to enable the Alias Added event type.

• Enable Alias Deleted Event - Select this option to enable the Alias Deleted event type.

Collaborate

- Enable Calendar Reminder Occured Event - Select this option to enable the Calendar Reminder event type.
- Enable Task Reminder Occured Event - Select this option to enable the Task Reminder event type.

Email

- Enable Message Received Event - Select this option to enable the Message Received event type.
- Enable Message Sent Event - Select this option to enable the Message Sent event type.

Mailing List

- Enable Mailing List Added Event - Select this option to enable the Mailing List Added event type.
- Enable Mailing List Deleted Event - Select this option to enable the Mailing List Deleted event type.
- Enable Message Sent to Mailing List Event - Select this option to enable the Message Sent to Mailing List event type.

Throttling

- Enable User Throttled Event - Select this option to enable the User Throttled event type.
- Enable Domain Throttled Event - Select this option to enable the Domain Throttled event type.

User

- Enable User Added Event - Select this option to enable the User Added event type.
- Enable User Deleted Event - Select this option to enable the User Deleted event type.
- Enable User Disk Space Used Event - Select this option to enable the User Disk Space event type.

Domain Propagation

Use this section to apply global default settings to all of the domains on the server. These default settings can be overwritten and are only intended to avoid needless data entry.

To access domain propagation, click the settings icon . Then expand Defaults and click Domain Propagation in the navigation pane. The default domain settings will load in the content pane. For more information on these settings, refer to Domain Defaults .

To apply some or all of the default settings to all of the domains on your server, select the appropriate settins and click Propagate Now .

User Defaults

Use this section to create global default settings that will be applied to new users created through the Web interface or Web services. These default settings can be overwritten and are only intended to avoid needless data entry. Note: Modifications to these settings will not affect existing users.

To access the user default settings, click the settings icon . Then expand the Defaults folder and click User Defaults in the navigation pane. The domain default settings will load in the content pane. For more information on these settings, refer to Users .

User Propagation

Use this section to apply global default settings to all of the users on the domain. These default settings can be overwritten and are only intended to avoid needless data entry.

To access user propagation, click the settings icon . Then expand the Advanced Settings folder and click User Propagation in the navigation pane. The default domain settings will load in the content pane. For more information on these settings, refer to Users .

To apply some or all of the default settings to all of the users on the domain, select the appropriate settings and click Propagate Now .

Routing

Forwarding Blacklist

Adding domains to this list means that users are not able to forward any emails to users of the domains. This is to prevent issues with companies that have strict spam policies and blacklist the sending server for forwarded spam.

This feature is commonly used for AOL, which blacklists servers that forward spam to their servers. If this becomes a problem, you may decide to add AOL.com to your forwarding blacklist.

Outgoing Gateway

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

To access the outgoing gateway settings, click the settings icon . Then expand the Routing folder and click Outgoing Gateways in the navigation pane. A list of outgoing gateways will load in the content pane.

To add a new outgoing gateway, click New in the content pane toolbar. To edit an existing gateway, select the desired gateway and click Edit . The outgoing gateway settings will load in the content pane and the following tabs will be available:

Options

Use this tab to specify the following settings:

- Server Address - The IP address of the gateway server.
- Port - The port used to connect to the gateway server. By default, the port is 25.
- Auth Username - The username of the gateway server given to you by your ISP.
- Auth Password - The password for your gateway server.
- Encryption - Select the type of encryption from the list.
- Priority Range - The priority range for this server. System administrators can use gateway servers to only send mails with a certain priority level. For example, gateways can be used only for lower priority messages, such as newsletters or messages over a certain size, to reduce load and free up processing on the primary mail server.
- Enable SmarterMail gateway mode - Select this option to indicate that the outgoing gateway server is another SmarterMail server.

SmarterMail Gateway

This tab is only available if the SmarterMail gateway mode is enabled in the Options tab. Use this tab to specify the following settings:

- SmarterMail URL - The Webmail URL for the SmarterMail server being used an an outgoing gateway. This will allow the use of Web services to verify the users and domains.

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

Incoming Gateways

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

To access the incoming gateway settings, click the settings icon . Then expand the Routing folder and click Incoming Gateways in the navigation pane. A list of incoming gateways will load in the content pane.

To add a new incoming gateway, click New in the content pane toolbar. To edit an existing gateway, select the desired gateway and click Edit . The incoming gateway settings will load in the content pane and the following tabs will be available:

Options

Use this tab to specify the following settings:

- Gateway Mode - The function that the incoming gateway will perform. If the incoming gateway is set to backup MX, it will only receive messages when your primary server is down. If the incoming gateway server is set to domain forwarding, it will received all message and forward them to your primary server.
- IP Address / IP Range - The IP address, or range of IP addresses, of the primary mail server.
- User Verification - The method used by the incoming gateway to determine if a user is valid or not. Note: If none is selected, the incoming gateway server will accept all email addresses for the domain. If Web service is selected, the incoming gateway will check with the primary mail server for a list of valid email addresses.
- Enable SmarterMail Gateway Mode - Select this option to indicate that the incoming gateway server is another SmarterMail server.
- Disable Greylisting - Select this option to disable greylisting for the domain.

Domains

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

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

Use this tab to specify for which domains the incoming gateway will accept mail:

- Domain Verification - The method used by the incoming gateway to determine if a domain is valid or not.
- Specified Domains - The specific domains for which the gateway will accept mail.

Spam

Use this tab to specify the following spam checks:

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

SmarterMail Gateway

This tab is only available if the SmarterMail gateway mode is enabled in the Options tab. Use this tab to specify the following settings:

- SmarterMail URL - The Webmail URL for the SmarterMail server being used an an incoming gateway. This will allow the use of Web services to verify the users and domains.
- SmarterMail Username - The identifier used to login to the primary mail server.
- SmarterMail Password - The corresponding password used to login to the primary mail server.

Sender Priority Overrides

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

To view the sender priority overrides, click the settings icon . Then expand the Routing folder and click Sender Priority Overrides in the navigation pane.

To create a new sender priority override, click New in the content pane toolbar. The following options will be available:

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

Storage

File Storage

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

To manage the file storage settings, click the settings icon and click File Storage in the navigation pane. The file storage settings will load in the content pane and the following tabs will be available:

Options

Use this tab to specify the folowing settings:

- Max File Size - The maximum size a file can be in order to be uploaded to the server.
- Root URL - The base URL of any file stored and shared in file storage. By default, the base URL corresponds to the domain the mail server is set up on (i.e., http://mail.example.com). If SmarterMail is configured on an external IP that allows a network address translation (NAT) to an external IP, the system administrator may need to modify the root URL.

Extension Blacklist

Use this tab to select and list any file types that cannot be uploaded to the server. System administrators may want to limit the capabilites of users to upload certain file types, such as executables (.exe) or other file types that can possibly be used to cause problems on the server.

Folder Auto-clean

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

To access the folder auto-clean settings, click the settings icon . Then expand the Defaults folder and click Folder Auto-Clean in the navigation pane.

The folder auto-clean settings will load in the content pane and the following tabs will be available:

Options

Use this tab to specify the following options:

- Enable domains to override auto-clean settings - Selet this option to allow domain administrators to create their own auto-clean policies.
- Enable users to auto-clean inbox - Select this option to allow users to create their own auto-clean policies.

Default Rules

If you are using the default auto-clean settings set up by your administrator, they will appear on this tab. If you chose to override the settings, you can click Add Rule in the content pane toolbar to create your own auto-clean policies based upon size or date.

These options will be visible if size is chosen:

- Folder Size Before Auto-clean - The maximum size of the folder. Once the folder reaches this size, the auto-clean process is started and older messages (messages that were received the longest time ago) are deleted.
- Folder Size After Auto-clean - The goal size of the folder. When auto-cleaning, SmarterMail will delete older messages until the folder reaches this size. Note: This number should aways be lower than the "before" number.
- Enable auto-clean for this folder - Select this box to activate auto-cleaning of the selected folder.

These options will be visible if date is chosen:

- Mail Age - The maximum number of days mail will stay in the selected folder before deletion.
- Enable auto-clean for this folder - Select this box to activate auto-cleaning of the selected folder.

Message Archiving

This feature is only available in SmarterMail Enterprise edition.

Message archiving is a method of storing all email traffic for a domain -- either incoming messages, outgoing messages or both -- in a separate location on the mail server. Typically, this is a feature used

for companies that need mail servers in compliance with the Sarbanes-Oxley Act of 2002 or other regulatory compliance.

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

When archiving is set up for a domain (or for all domains), messages are automatically archived as soon as they hit the spool and before they are handled by any spam and/or content filters. This means that all messages are archived, not simply those that are delivered to a user's mailbox. On a nightly basis, SmarterMail zips up archived messages and stores them to conserve disk space on the mail server. However, zipped messages are still searchable.

To view the message archiving rules for your SmarterMail installation, click the settings icon . Then expand Storage and click Message Archiving in the navigation pane. A list of archiving rules will load in the content pane.

To create a new archiving rule, click New in the content pane toolbar. To edit an existing rule, select the appropriate rule and click Edit in the content pane toolbar. The following options will be available:

- Domain - The domain on the SmarterMail server to be archived.
- Archive Path - The directory on the hard drive in which archived messages are saved.
- Rule - Choose to save none of your messages, all messages, only incoming messages or only outgoing messages.

Once email archiving is set up, both system administrators and domain administrators can search the archives. System administrators can only search across all domains whereas domain adminsitrators can search only within their own domain. NOTE: Please note that domain administrator search requires individual domain archiving rules to be set up, as noted above.

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

Advanced Settings

Configuring SmarterMail for Failover

Who Should Use This

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

Failover Overview

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

Understanding How Failover Works

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

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

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

Minimal System Requirements

- A minimum of two servers running Microsoft Windows Server 2008 R2 or higher. (Windows Server Core is not currently supported).
- Three IP addresses
- Both servers must have their server times synchronized
- NFS/SMB share for mail and system files. We recommend that the share is running on a NAS/SAN that is configured as RAID 10

Adding Network Load Balancing to Your Servers

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

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

Configuring the Load Balanced Cluster for Use with Failover

- Navigate to Start -> Administrative Tools -> Network Load Balancing Manager
- Click the Cluster menu item and select New
- In the New Cluster: Connect window, type the IP of your primary server in the Host: text box and select New
- When the Interface Name and Interface IP appear, select the Interface Name and click Next
- Since this is the primary node, ensure the host Priority is set to 1
- In the New Cluster: Host Parameters window, confirm the IP address and Subnet mask are correct and change the initial host state to Stopped . This is to prevent any issues with connectivity if a machine randomly reboots or suffers from a hardware failure. If all nodes are set to Started for their initial host state, traffic will be split between the two (or more) machines. Note: Monitoring software can be used to execute scripts that will start and stop hot standbys in the event of a failure and recovery. If you are not executing scripts via monitoring software then all failover will need to be handled manually.
- Click Next
- In the New Cluster: Cluster IP Addresses window, click Add and enter in your cluster IP address and the same subnet mask as in Step 6
- Select Next
- In the New Cluster: Cluster Parameters window, confirm the IP address and subnet mask, then enter a Full Internet Name , though this is optional

• Ensure the cluster operation mode is set to Multicast
• Click Next
• In the New Cluster: Port Rules window, click Edit

• If you want you can restrict the cluster IP to work on an individual port or across a port range. You can also simply allow the cluster IP to work across all ports on the server
• Ensure your port rules are set to Single Host in the Filtering Mode section
• Click OK
• Verify your settings and click Finish to complete the setup

Joining Additional Nodes to the Cluster

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

Configure a Shared Service Directory

• Using Network File Sharing (NFS) or Samba (SMB), create a shared directory named SmarterMail , preferably on a NAS or SAN. NOTE: We recommend that this shared directory be hosted on a server that utilizes a RAID 10 configuration for the data.

• Inside that new SmarterMail folder, create a Service folder

• Configure your permissions accordingly. If special permissions are required, configure the SmarterMail service to run with the proper credentials within the Windows Services console. Note: When performing updates to the software, the credentials will need to be re-applied to the service

Configuring a Fresh Installation of SmarterMail for Failover

• Install SmarterMail Enterprise on a server. This will be your hot standby. Leave all setup information as the default settings and after setup is complete, configure SmarterMail as an IIS site.

• Stop the SmarterMail service on the hot standby

• Edit the failoverConfig.xml file in the primary server's Service folder as follows:

• SharedSystemFilesPath - Set to the shared network shared system folder

• FailoverIPAddress - Set this to the IP address of the Network Load Balancer

• IsEnabled - Set this to True

• Save this file, then copy it to the hot standby's Service folder and replace the existing failoverConfig.xm l

• Copy over all folders, DAT and XML files from C:\Program Files (x86)\SmarterTools\SmarterMail\Service to the Service folder in the shared service directory you created

• Start the service on the hot standby server and verify that the paths are pointing to the network shared paths

• Activate your Enterprise key on the hot standby by logging into SmarterMail's management interface as the system admin and going to Settings -> Activation -> Licensing , then stop the SmarterMail service on the server

• Start the service on the primary server, then reactivate your Enterprise license key in the SmarterMail management interface

• After re-activating the license, go to Settings -> Bindings -> IP Address and bind all the ports to the load balancer's IP address and make sure no other IPs have any ports bound to them

• Both servers are now set up for failover. To verify this, when logged into the primary server as the system admin, go to Settings -> Failover Servers to view the servers that are part of the failover cluster

Adding Failover to an Existing Installation of SmarterMail

Note: You will need to configure both servers for Network Load Balancing and set up a shared service directory. See the steps outlined in the Adding Network Load Balancing to Your Servers , Configuring

the Load Balanced Cluster for Use with Failover , Joining Additional Nodes to the Cluster and Configure a Shared Service Directory sections earlier in this document for more information.

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

- SharedSystemFilesPath - Set to the shared network shared system folder
- FailoverIPAddress - Set this to the IP address of the Network Load Balancer
- IsEnabled - Set this to True
- Run the robocopy one more time to copy over any modified files and remaining spool e-mails
- Copy over all folders, DAT and XML files from C:\Program Files (x86)\SmarterTools\SmarterMail\Service to the Service folder in the shared service directory you created
- Edit the domainlist.xml file in the shared Service folder and change the path of your domains to match the new NFS\SMB path. (For example, \\NAS01\SmarterMail\Domains\mydomain.com)
- Edit the mailconfig.xml file and replace any instances of the old physical path's with your new network location for SmarterMail. (For example, if all of your data was hosted on E:\Smartermail, you would then perform a find and replace for all instances of E:\Smartermail to \\NAS01\Smartermail).
- On the primary server, go to Start -> Administrative Tools -> Network Load Balancing Manager and stop the cluster node, then start the NLB on the secondary node
- Start the SmarterMail service on the hot standby
- Access SmarterMail's web interface at the cluster IP and sign in as the system admin
- Activate your Enterprise key on the hot standby by going to Settings -> Activation -> Licensing
- Verify that the data and settings are being picked up from the shared Service directory
- Stop the SmarterMail service on the hot standby and stop the secondary cluster node
- Start the cluster node and the SmarterMail service on the primary server

- Sign into the web interface on the primary server and re-activate the Enterprise license key by going to Settings -> Activation -> Licensing
- Verify mail data and settings are being accessed from the shared service directory

Scripting Failover

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

Prepping PowerShell on the Servers

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

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

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

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

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

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

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

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

```
$StopSecondary = New-PSSession -ComputerName Server02 Invoke-Command -Session $StopSecondary -ScriptBlock { Import-Module
```

```
NetworkLoadBalancingClusters ; Stop-nlbclusternode -HostName Server02 -
InterfaceName "WAN" ; import-module WebAdministration ; stop-webapppool
SmarterMail; set-service -computerName Server02 -name mailservice -status
stopped ; remove-pssession Server02}

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

Message Footer

System administrators can configure server-wide message footers that SmarterMail will append on all outgoing and incoming messages. Although similar to signatures, message footers are typically used to convey disclaimers or provide additional information. For example, a system administrator may want every message to include a notice that the message was scanned for viruses or the text "Sent by SmarterMail."

To access the message footer options, click the settings icon and click Message Footer in the navigation pane. The message footer settings will load in the content pane and the following tabs will be available:

Options

Use this tab to specify the following settings:

- Enable footer for all messages - Select this option to turn the message footer on.
- Apply to mailing lists - Select this option to append the message footer to mailinglist messages. Note: Mailing lists have their own configurable footers, so enabling this option will append a second footer at the end of each message. Because this may be confusing for mailing list moderators and recipients, most administrators will choose to keep this option disabled.
- Enable domains to override footer settings - Select this option to allow domain administrators to configure their own message footer for the domain.

Footer

Use this tab to create the message footer text. Note: The message footer does not support the use of variables.

Automation with Web Services

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

The Automation with Web Services documentation may include services that have not been released to the public yet or are not available in the version you are using. For the most accurate Web services information, log into SmarterMail as the system administrator and click the settings icon . Then click Web Services in the navigation pane.

Note: Web services are intended for use by high-volume and automated businesses environments and hosting companies as they develop procedures tmanage their SmarterMail system and work flow. In addition, this document assumes a basic understanding of Web service technologies and ASP.NET programming.

Personalization

SmarterMail supports the ability to personalize the webmail interface so that administrators, or even users, can create skins that represent their own style or emulate the company's branding and appearance.

To view the personalization settings, click the settings icon and open either My Settings for user personalization, or Domain Settings and then click Personalization in the navigation pane. The following tabs will load in the content pane:

Settings

The Settings tab will be where users select whether to use the default settings for the domain or whether to customize the general color scheme and overall CSS of the SmarterMail interface. The following options are available, depending on the default domain settings:

- Use default settings - Selecting this will use as the default personalization settings.
- Override Settings - Selecting this activates the Colors and Custom CSS tabs and allows users to customize those settings.
- Enable users to override - This is a domain administrator only setting. Selecting this option will allow end users to modify the custom CSS and general color scheme for their webmail login.

• Skin - This dropdown will list any skins developed for SmarterMail. In general, the Default skin will always be available, but others may appear in this list as well.

Colors

The Colors tab allows users to modify the Primary, Secondary and Link colors for the SmarterMail interface.

• Primary Color - This is the color for the title bar in SmarterMail, the numbered notifications (e.g., for new messages), highlight colors for input boxes, calendar items, etc. The default is #519CDE
• Secondary Color - This is the color of the button bar. The default is #D1E8FC
• Link Color - This is the color of hyperlinks that appear in messages, calendar items, etc. The default is #1677C2

Custom CSS

The Custom CSS tab allows users to take the existing styles used in the SmarterMail interface and modify them based on branding or personal preference. As noted on the page, however, errors in custom CSS may cause the interface to have issues, so modifications should only be made if the person making the changes is extremely proficient with styles and stylesheets.

To modify a style, you should first use a Web browser like Chrome to inspect the element that you want to modify. (Using FireFox's Firebug plug-in will work as well). By inspecting the element you will see the class used and any styles associated with the class. You can then create a version of that style yourself, and then paste it in the box to override the default. Realize this will happen wherever that style is used, so changing one style can affect several pages within the interface. To enable the custom styles, simply check the Enabled box on the Custom CSS tab.

To remove any customization and personalization of the interface, simply remove the custom style and save the changes. This will reset the interface back to its original default settings.

Activation

Licensing

System administrators can use this area to view licensing information,

To access view licensing information for SmarterMail or any add-ons, click the settings icon . Then expand the Activation folder and click Licensing in the navigation pane. The edition, version, and license level information for the version of SmarterMail currently being used will load in the content pane. The licensing information for any add-ons will also display in the content pane.

The following options are available from the content pane toolbar:

- Activate - Activates a new SmarterMail license key.
- Reactivate - Reactivates a SmarterMail license key. License keys should be reactivated if you purchase add-ons or change the product edition or level.
- Details - Displays details about the license, including feature, status, expiration, limits and available trials.
- Buy Now - Allows the system administrator to purchase a new license key or add-on.
- Start Trial - Allows the system administrator to begin an available add-on trial. Trials for add-ons are limited to 30 days, after which the add-on needs to be purchased or it will no longer function.

Note: If you are running a trial version of SmarterMail, it will automatically revert to SmarterMail Free when the trial expires. This will be reflected in the licensing details.

SmarterMail Self Diagnostic

Use the SmarterMail Self Diagnostic to test your SmarterMail server for errors. To access this feature, click the settings icon . Then expand the Activation folder and click SmarterMail Self Diagnostic in the navigation pane. SmarterMail will perform a test and display the results in a popup window.