Settings

Help Documentation

Settings

General Settings

The General Settings page is where you control many of the global settings for the SmarterMail server. This page is tabbed for easy editing. No settings will be saved until you click on the Save button.

NOTE: For first time users, we recommend the first change to be the System Admin Username and the System Admin Password on the Administrator tab to avoid anyone getting into your system using the default login.

Administrator

Username - This is the login name associated with the System Administrator account for the SmarterMail Server. You will use this name instead of a full email address when logging in as the System Administrator.

Old Password - In order to change the System Administrator password you must the current password associated with the System Administrator account. Passwords are case-sensitive.

New Password - Enter the desired password for the System Administrator account. Passwords are case-sensitive.

Confirm New Password - Verify the desired password for the System Administrator account. Passwords are case-sensitive.

Server Info

Host Name - Enter the host name of this server. It is sent to connecting servers to identify the server. Host names should be in the format computername.domain.com .

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

IP of Primary / Secondary DNS - Enter the IP address of the DNS servers. If left blank, the DNS server information will be pulled from the the Windows Networking settings (Recommended).

Security

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, you can set the type of relays you will allow, or completely disallow mail relay completely:

- Nobody - This option will restrict mail sent to only work via SMTP authentication, and with accounts on the local SmarterMail Server except for IPs on the White List.
- Only Local Users (Recommended) - 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.

Auto Responsers - Allows you to restrict what types of auto-responses are permitted for the system. Certain anti-spam organizations are starting to block those servers that auto-respond to spam traps. To reduce the possibility of this occurring, set the auto-response option to be as restrictive as your clients will permit.

Content Filter Bouncing - As with auto-responses, certain anti-spam organizations also blacklist those servers that send bounce messages back to spam trap accounts. SmarterTools recommends setting this option to be as restrictive as your clients will allow.

Catch-Alls - Check the "Enable bounces and auto-responders for email messages sent to catch-all accounts" if you rely on auto-responders being sent when a message comes in through a catch-all. In general, this is a bad idea, so it should be left unchecked unless your situation specifically requires it.

Password Strength Requirements - The System Administrator is able to set the requirements for passwords and, as a result, all users must adhere to those standards. The password options available to the System Administrator are: minimum length, upper and lower case letters, numbers, and symbols.

Redirect Log Outs - This feature allows System Administrators to redirect users who log out to a certain URL. The redirect options available are:

- Redirect to Server URL on log out.
- Allow Domain Administrators to override the redirect URL

Spool

Spool Path - This is 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 allows 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.

Delivery Delay - This option will hold mail in its spool for this amount of time prior to sending the mail. The benefit of a delivery delay is so that if you have a secondary service, like a virus checker, that needs access to the mail prior to its delivery, you give the secondary service ample time to interact with the message prior to it leaving the mail server.

Time Between Retries - When the mail server is unable to contact the receiving server, the email attempting to be sent is held for a period of time before attempting to be resent. This is the time between retries. Users can specify multiple retry times to resend emails before it is bounced. By default, this is set to 4 times - 15min, 30min, 60 min and 90 min.

Command-line file to run on new mail - Enter the full path to an executable you wish to process incoming messages with. Use %filepath as an argument to pass the path to the email file to the executable. It is important to set a reasonable delivery delay to prevent SmarterMail from attempting to deliver the message while the executable is still accessing it. It is safe for the executable to delete the message to prevent delivery. 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. The command will not be executed if the Enabled box is not checked.

Command-line timeout - The amount of time, in seconds, that the server will wait while waiting for information from the remote server. In general, a timeout between 45 to 75 seconds should suffice.

Protocol Settings

This configuration page allows you to establish policies for the standard email protocols. This page is tabbed and no settings will be saved until you click on the Save button.

POP Session Timeout - After a connection fails to respond or issue new commands for this number of seconds, the connection will be closed.

--%> 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.

Maximum Bad Commands - After this many unrecognized or improper commands, a connection will be automatically terminated.

Maximum 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.

IMAP

Session Timeout - After a connection fails to respond or issue new commands for this number of seconds, the connection will be closed.

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.

Maximum Bad Commands - After this many unrecognized or improper commands, a connection will be automatically terminated.

IDLE Command - Check this box to turn on 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. Please note, IMAP clients that do not fully support IMAP IDLE, like Microsoft Outlook, may use the command in such a way that it actually degrades performance.

LDAP

Session Timeout - After a connection fails to respond or issue new commands for this number of seconds, the connection will be closed.

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.

Maximum 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.

SMTP In

Session Timeout - After a connection fails to respond or issue new commands for this number of seconds, the connection will be closed.

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.

Maximum Bad Commands - After this many unrecognized or improper commands, a connection will be automatically terminated.

Maximum 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. 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.

Max Message Size - Messages greater than this size will be rejected by the mail server.

Max Bad Recipients - After this many bad recipients, 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.

Submission IP:Port - The submission port is a special SMTP port that requires SMTP Authentication in order to be used to deliver any mail whatsoever, regardless of domain-specific settings. This setting is an advanced feature that is typically used when a whitelisted inbound gateway is being used for spam and virus scanning, and all other SMTP traffic is blacklisted. Note: This setting will not function until the Enabled checkbox next to the setting is checked.

Enable VRFY command - Check this box to enable the Verify Mailbox command in SMTP. This will allow others (including other mail servers) to verify an email address on the server. This is considered by some to a security risk, and should not be checked without understanding the ramifications.

Enable EXPN command - Check this box to enable the Expand List command in SMTP. This will allow others to list all users associated with an alias or list. This is considered by some to a security risk, and should not be checked without understanding the ramifications.

Bypass relay settings when using SMTP authentication - When this option is checked, senders that are verified with SMTP authentication can send from any address, and relay settings are ignored. When this option is not checked, relay restrictions are enforced even if the sender is authenticated.

Enforce SMTP authentication - When this option is enabled, SmarterMail will 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.

SMTP Out Gateway Server - Specifying the IP address of a gateway server in this box and checking the Enabled checkbox will turn on gateway mode. Relaying to a gateway will send or route all outgoing mail to another SMTP server before it reaches its final destination. The destination SMTP server would have to be configured to take relays from your particular IP address. For example, if the destination SMTP server was a SmarterMail Server, then the IP from the original mail server would need to be added to the White List unless "anyone" was selected for the "allowing relay for"

option. For more information about the roles of Gatewaying, please see Gateways and Other Server Roles .

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

Outbound IP - Use this box to select what IP address is used to deliver outbound messages.

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.

Max Delivery Threads - Enter 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 can not be sent right away.

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. Prior to this addition, SmarterMail could only specify one hostname for all IPs.

Default Domain Settings

From this page you can create global default settings that will automatically be used when adding a new site through either the Web Interface or through Web Services. These default settings can be overwritten and are only intended to avoid needless data entry.

The settings on this page are identical to those found in the topic Editing a Domain .

Note: Changing these settings has no bearing on domains that have already been setup, unless the "Propagate Settings" option is used.

Propagating Settings

To apply some or all of the default settings to all domains on your server, change the settings to how you want them, and then click on the Save and Propagate Settings button. Check all of the settings that you want to apply to your domains, then click on the Propagate Now button.

Log Settings

In order for you to know what activity is happening on your server, SmarterMail has multiple logging options for various parts of the mail server. Use this page to manage how logs are written and how much detail is written.

To make this page easier to use, it has been tabbed. Settings will not be applied to any tab until you click on the Save button.

Log Files

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

Delete Log Files After - Log files older than the number of days specified in this field will be automatically deleted. Set it to 0 to disable this feature.

Log Detail Levels

These settings change the amount of detail that is stored in the protocol logs. Possible values for each are shown below:

- 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.

Delivery Log Level - The log level for message delivery and spool operations (Default = Detailed).

SMTP Log Level - The log level for SMTP sessions (Default = Normal).

POP Log Level - The log level for POP sessions (Default = Exceptions Only).

POP Retrieval Log Level - The log level for POP retrieval sessions (Default = Exceptions Only).

IMAP Log Level - The log level for IMAP sessions (Default = Exceptions Only).

LDAP Log Level - The log level for LDAP sessions (Default = Exceptions Only).

Message-ID Log - The log level for logging Message-ID's of all messages sent to mailing lists. (Default = None).

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. For more information about the roles of Domain Forwarding, please see Gateways and Other Server Roles .

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.

To establish domain forwarding, go to the Settings -> Domain Forwarding menu and choose to add a target server. Enter the server that should receive the mail and add the domains that should be forwarded to it, one per line.

Note: If you do not host any actual domains on the server, in order for your mail server to listen for traffic, you need to set up a dummy domain (example.com) to listen on the IP and ports from which you expect traffic.

SmartHost Servers

SmartHosting allows one SmarterMail server to accept mail for another SmarterMail server. This can be used in a backup scenario so that if the primary mail server goes down, the secondary server will accept mail for it until the server goes back online. For more information about the roles of SmartHosting, please see Gateways and Other Server Roles .

To configure SmartHosting correctly, changes need to be made on the secondary server and to DNS records of domains that will have SmartHosting supported.

- Add SmartHosts - In the secondary server, add all IP addresses of the primary server to the SmartHost list. Mail that resolves to MX records that do not match these IP addresses or accounts on the secondary server will be rejected.
- Setup MX records - In DNS, add an MX record for the secondary mail server that has a LARGER preference value than the primary mail server. Refer to your DNS server documentation for instructions on adding MX records. Note: In MX records, lower preference value servers are tried first.
- Set appropriate retry times - Since the intent of SmartHosting is for the secondary server to be a backup server, adjust the retry times in General Settings to values that are more conservative. Good defaults would be: 10 minutes, 10 minutes, 10 minutes, 1440 minutes.

Note that it is good practice to disable the spool service on the secondary server if the primary server goes down for more than 30 minutes, then restart the spool once the primary server is back online. In this way, all messages will still be accepted through the SMTP service, but delivery will not keep trying to deliver the messages. Once you get the primary server online again, start the spool service on the secondary server and all the messages will start to be delivered.

Gateway Servers

Gateway Servers allow you to use another server, SmarterMail or not, to handle outgoing mail in order to reduce load on your primary server. They can also be used to combat blacklisting. If the server gets blacklisted, simply rotate the primary IP on the network card to a different one to send out on the new IP.

- Add Gateway - Click this button to add a Gateway Server

- Server Address - The IP address of the Gateway Server
- Enabled - Whether this server should be enabled
- This gateway is a SmarterMail server - Is this gateway another SmarterMail server
- SmarterMail URL - The value to enter in this field is the URL used to check webmail. This will allow the use of web services to find out how many messages are in the spool in order to do an intelligent round robin distribution.
- Admin Username - The admin username on the gateway server
- Admin Password - The admin password on the gateway server

Folder Auto-Clean

The purpose of the Folder Auto-Clean feature of SmarterMail is to aid you in keeping your mailbox size(s) under control. Using Folder Auto-Clean, common folders like Junk E-Mail, Sent Items, and Deleted Items can be regularly cleaned of old messages so they do not clutter your mailbox. System administrators can choose to let domains and users override your suggested settings, or require them to use the policies you set. Domain administrators also have this priviledge over users.

Options (System Admin)

Allow domains to override auto-clean settings - Check this box to allow domains to change the settings on this page. This is recommended, as many domain administrators have their own ideas of what an acceptable auto-clean policy is. Uncheck this box to lock the settings for all domains and all users.

Options (Domain Admin)

Use default auto-clean settings - Check this box to use the system administration's auto-clean settings.

Override auto-clean settings for this domain - Check this box to allow you to change the settings for your domain.

Allow users to override auto-clean settings - Check this box to allow users to change the settings on for their individual account.

Options (Users)

Use default auto-clean settings - Check this box to use the domain administration's auto-clean settings.

Override auto-clean settings for this account - Check this box to allow you to change the auto-clean settings for your account.

Folders

Under each folder that has auto-clean options or if you click the Add Rule button, you will see the settings below:

Folder - Selectthe folder that you would like to add the Auto-Clean to. Only seen if you click the Add Rule button.

Auto-clean this folder - Check this box to auto-clean the folder when it gets too big.

Folder size before auto-clean - When the folder reaches this size (in megabytes), auto-cleaning will be activated.

Folder size after auto-clean - Auto-clean will attempt to reduce the folder to this size or smaller when auto-cleaning is performed.

Message Archiving

This feature is available in Enterprise Edition only

Message Archiving is a method of storing all email traffic for a domain 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. Message archiving allows you to set up rules for saving messages for specific domains.

Note: 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.

Adding / Editing a Rule

To apply an archiving rule to all domains on the server, click on "All Domains" in the list. To add a rule for a single domain, click on Add Archive Rule.

Domain - The domain that should be archived, in the format of example.com.

Archive Path - The path on the hard drive that should be used to store the messages.

Rule - Choose to save all messages, or inbound / outbound messages only.

Skins

The SmarterMail Web interface contains built-in skins for your convenience. The various skins can be found under Settings > My Settings > Webmail. Users can also create custom skins to emultae their own style or that of their company. Please refer to the SmarterMail 4.x Skinning Guide for more information about creating custom skins.