



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** - The email address for the postmaster. This is usually the owner or system administrator.
- **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 upon logout.
- **Enabled** - Select this checkbox to redirect users to the Logout URL after logging out of SmarterMail.
- **Enable domain admins to override logout URL** - Select this option to allow domain administrators to specify the Logout URL. If this option is not enabled, it will not be visible to domain administrators. **Enable Lite Mode** - SmarterMail Lite is a specially-developed version of the SmarterMail mail server that provides unlimited email accounts and domains and it is only available with specific product offerings from SmarterTools technology partners. If SmarterMail detects software from a company that has partnered with SmarterTools to make this edition available, SmarterMail Lite will automatically be enabled. Because SmarterMail Lite has a limited feature set, some customers may want to revert to SmarterMail Free edition. To do so, uncheck this box. Note: SmarterMail Free edition has the same functionality as SmarterMail Enterprise, but is limited to one domain with up to 10 users. --%>
- **Reset getting started** - Select this checkbox to view the Getting Started checklist. This checklist is designed to system administrators set up the mail server and appears automatically after installation. However, system administrators may choose to refer to the checklist at a later time as a reference guide when adding additional domains or users.

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 subpool. (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 attempting to be resent. 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.
- **Attempts before bouncing DNS errors** - 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 processing unnecessary messages 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.
- **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.

Reports

Use this tab to specify the following settings:

- Delete Server Stats After - The number of months that the server stats will be deleted. By default, the server stats are deleted after 13 months.
- Enabled - Select this checkbox to delete server stats after the specified time period.
- Delete Domain Stats After - The number of months that the domain stats will be deleted. By default, the domain stats are deleted after 13 months.
- Enabled - Select this checkbox to delete domain stats after the specified time period.
- Delete User Stats After - The number of months that the user stats will be deleted. By default, the user stats are deleted after 13 months.
- Enabled - Select this checkbox to delete user stats after the specified time period.

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 index more users simultaneously.
- 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 Indexing - 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 the user uses to login to SmarterMail.
- New Password - The corresponding password used to login to Smartermail.
- Confirm New Password - The corresponding 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 from. Note: This tab is only accessible if the option to enable login access by IP address was selected in the Options tab.

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.

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 and 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 - The maximum number of threads you want SmarterMail to work on concurrently. By default, the maximum number of POP retrieval threads is 10.
- POP Retrieval Interval - The frequency by which SmarterMail checks for new POP messages. By default, the POP retrieval interval is 1 minute.

IMAP

Use this 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 and 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 POP messages. By default, the POP 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.

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, you can set the type of relays you will allow, or completely disallow mail relay completely.
- 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 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.
- 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 - 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 - 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.
- Disable relay settings when using SMTP authentication - Select this checkbox to disable the "Allow Relay" setting from above.
- 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.
- Disable appending of received line for authenticated messages - Select this checkbox to prevent SmarterMail from appending the received line when a message is received over SMTP and the message is authenticated.

SMTP Out

Use this tab to specify the following outgoing SMTP settings:

- Outbound IP - Select the IP address that is used to deliver outbound messages from the list.
- Enable fallback to Primary IP on failure - Select this checkbox to have SmarterMail automatically fallback 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 and 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.
- 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.

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 -

ActiveSync Mailboxes

System administrators will use this section to enable and disable the Microsoft Exchange ActiveSync add-on for mailboxes. Note: Before you can configure a mailbox to sync using the ActiveSync technology, you must activate the ActiveSync add-on. 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.
- **Search** - Searches for a specific mailbox with Exchange ActiveSync enabled.

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 files that are no longer used from the server when 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 following settings:

- **Max File Size** - The maximum size in KB of any file uploaded to the server.
- **Enabled** - Select this option to enable the max file size setting.
- **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.
- **Enabled** - Select this option to enable the custom base URL setting.

Extension Blacklist

Use this tab to list any file types that cannot be uploaded to the server.

Hostnames

This feature allows administrators to assign a hostname for each IP address. For example: IP 1.1.1.1 can be assigned to `mail.domain1.com` and IP 1.1.1.2 can be for `mail.domain2.com`.

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).

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.

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.

Skins

SmarterMail supports custom skinning, so administrators can create skins that represent their own style or emulate the company's branding and appearance.

To view the skin settings, click the settings icon and click Skins in the navigation pane. The following skin settings will load in the content pane:

- **Default Skin** - Select the skin to use as the default from the list.

- Enable ability for domains to override skin - Select this option to allow domain administrators to choose a skin for their domain

Log Settings

System administrators can use this section to manage how logs are written and how much detail is included in 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.
- 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 Level - The log level for Exchange ActiveSync connections.
- Delivery Log Level - The log level for message delivery and spool operations.
- IMAP Log Level - The log level for IMAP sessions.
- IMAP Retrieval Log Level - The log level for IMAP retrieval sessions.
- LDAP Log Level - The log level for LDAP sessions.
- Message-ID Log Level - The log level for logging Message-ID's of all messages sent to mailing lists.
- Event Log Level - The log level for event sessions.
- POP Log Level - The log level for POP sessions.

- POP Retrieval Log Level - The log level for POP retrieval sessions.
- SMTP Log Level - The log level for SMTP sessions.
- SyncML Log Level - The log level for SyncML sessions.
- Mailbox Import Log Level - The log level for data imported during mailbox migrations.
- WebDAV Log Level - The log level for CalDav and CardDav sessions.
- Webmail Log Level - The log level for login and settings changes performed in the Web interface.

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

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 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 available in the content pane toolbar:

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

Ports

System administrators can use this section to configure the ports that can be assigned to IPs. In addition, this section is used to add Secure Socket Layer (SSL) and Transport Layer Security (TLS) rules.

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 available 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, select the appropriate option from the list. SSL always assumes the connection will be secure and sends the encryption immediately. TSL 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.
- Certificate Path - The path to the certificate file on the server. Typically, named a *.cer file.
Note: This option is only available if SSL or TLS encryption is enabled for the port. The certificate you are using must be added to the Certificates Microsoft Management Console within your Windows operating system. In addition, you must associate the Private Key with this same certificate.
- Description - A short description of the port.

Defaults

Domain Defaults

Use this section to create global default settings that will be applied to new domains 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 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.
- SMTP Port - The SMTP port used to connect to the email server. By default, the SMTP port is 25. Note: Changing the default port is not recommended unless you are behind a firewall that requires this setting to be changed.
- SMTP Port (Alternate) - The SMTP port used to connect to the email server if an ISP restricts the standard port 25.
- Enabled - Check this box to enable the alternate SMTP port.
- POP Port - The POP port used to connect to the email server. By default, the POP port is 110. Note: Changing the default port is not recommended unless you are behind a firewall that requires this setting to be changed.
- IMAP Port - The IMAP port used to connect to the email server. By default, the IMAP port is 143. Note: Changing the default port is not recommended unless you are behind a firewall that requires this setting to be changed.
- LDAP Port - The LDAP port used to connect to the server. By default, the LDAP port is 389. Note: This is an Enterprise only feature. Changing the default port is not recommended unless you are behind a firewall that requires this setting to be changed. --%>
- Auto-responder Exclusions - To prevent the system from sending automated messages 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 prevent encrypt the stream of messages sent from the mail server, select the appropriate option from the list.
- 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.
- Enable once per day per sender auto-responder - Select this option to limit how frequently an auto-responder is sent.
- Disable greylisting - Select this option to disable greylisting.
- Enable users to opt out of LDAP listings - Select this option to allow users to remove themselves from the Global Address List.

Features

Use this tab to enable or disable the following features:

- Enable calendar - Select this option to allow users to use the calendar feature.
- Enable catch-alls - Select this option to allow users to use catch-all email addresses.

- Enable contacts - Select this option to allow users to use the contacts feature.
- Enable content filtering - Select this option to allow users to use content filtering.
- Enable control of service access - Select this option to allow the domain administrator to restrict access to certain services.
- Enable domain aliases - Select this option to allow the domain administrator to create domain aliases.
- Enable domain reports - Select this option to provide additional reports for domain administrators.
- Enable email reports - Select this option to provide the ability to email reports.
- Enable IMAP retrieval - Select this option to allow users to download IMAP email from third-party mail servers.
- Enable mail signing - Select this option to enable email verification via mail signing.
- Enable mailing lists - Select this option to allow the domain administrator to create and use mailing lists to send mass emails.
- Enable notes - Select this option to allow users to use the notes feature.
- Enable POP retrieval - Select this option to allow users to download POP email from third-party mail servers.
- Enable spam filtering - Select this option to allow the domain administrator to override the spam filtering settings.
- Enable SyncML - Select this option to allow users to sync SmarterMail with Outlook, Thunderbird, and most smartphones using SyncML.
- Enable tasks - Select this option to allow users to use the tasks feature.
- Enable user reports - Select this option to provide reports for users.
- Enable XMPP communication -
- Enable Exchange Web Services -

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. 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. By default, domains are limited to two 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, this setting will be overridden.

- 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.
- Enable domain to override - Select this option to allow domain administrators to override the default maximum size message that can be sent to a mailing list.
- 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.

Sharing

This tab is only available in SmarterMail Enterprise edition.

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

- Enable 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.
- Enable shared calendars - Select this option to allow calendars to be shared with other users on the domain.
- Enable shared contacts - Select this option to allow contact lists to be shared with other users on the domain.
- Enable shared folders - Select this option to allow email folders to be shared with other users on the domain.
- Enable shared notes - Select this option to allow notes to be shared with other users on the domain.
- Enable shared tasks - Select this option to allow task lists to be shared with other users on the domain.

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.
- Enabled - Check this box to enable priority settings for standard messages.
- Mailing Lists - The priority level for mailing list messages.
- Enabled - Check this box to enable priority settings for mailing list messages.
- Priority When Over Size - The priority level for messages that exceed the message size threshold.
- Enabled - Check this box to enable priority settings for messages that exceed the message size threshold.
- 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.
- Enabled - Check this box to enable priority settings for auto-responders.
- Bounces - The priority level for non-delivery receipts.
- Enabled - Check this box to enable priority settings for bounced messages.
- Email Reports - The priority level for email reports.
- Enabled - Check this box to enable priority settings for email reports.
- Event Emails - The priority level for messages reminding users of upcoming events.
- Enabled - Check this box to enable priority settings for event emails.
- Priority After Attempt 1 - The priority level for messages that were not successfully sent after the specified number of tries.
- Enabled - Check this box to enable priority settings for subsequent delivery attempts.
- 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 sent after the specified number of tries.
- Enabled - Check this box to enable priority settings for subsequent delivery attempts.
- 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 the Defaults folder 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 settings 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 Defaults 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 .

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 - Select 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 always 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.

Routing

Forwarding Blacklist

Emails cannot be forwarded to the domains in this list. 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.

Message Archiving

| |
|---|
| This feature is only available in SmarterMail Enterprise edition. |
|---|

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.

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.

To view the message archiving rules for your SmarterMail installation, click the settings icon . Then

expand the Routing folder 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, incoming messages, or outgoing messages.

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.

Outgoing Gateway

Gateway servers allow you to reduce the load on your primary server by using a secondary server to process outgoing mail. Gateway servers 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.

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.
- 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 as 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 is to reduce server load. Generally, spam checks and antivirus scans should be performed on the incoming gateways.

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 receive all messages and forward them to your primary server.
- IP Address - The IP address 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:

- 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 as 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.
- Message Delivery Priority - The priority level assigned to this user's messages.
- Description - A brief summary why the sender priority override was created.

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.