



# Installation and Deployment

Help Documentation

This document was auto-created from web content and is subject to change at any time.

Copyright (c) 2019 SmarterTools Inc.

# Installation and Deployment

## Browser Requirements

SmarterMail is fully supported by the browsers below.

- Internet Explorer 6 and higher
- Google Chrome 2 and higher
- FireFox 2 and higher
- Safari 3 and higher
- Opera 10 and higher

Note: SmarterMail supports a minimum screen resolution of 1024 x 768.

## SmarterMail System Requirements

SmarterMail was designed to coexist with multiple applications on the same server based on the following minimum requirements:

- Windows XP\*, Windows Vista\*, Windows Server 2003 or higher
- SmarterMail Web server included with product
- Microsoft .NET 4.0 Framework

However, SmarterTools recommends the following requirements for maximum efficiency:

- Windows Server 2003 or higher
- Microsoft IIS 7.0\*\*
- Microsoft .NET 4.0 Framework

Note: Each installation and environment is unique. Extra load caused by excessive messages or email accounts and/or other factors may require more disk space, memory, database allocation, etc. than suggested in the online help. SmarterTools recommends that system administrators slowly add domains to the server and watch how they impact the server. In addition, email patterns indicate that the number of email messages per account are increasing by approximately 60% every two years. It is important to keep this growth in mind when planning your rollout.

\*Microsoft's non-server based operating systems limit the maximum number of inbound connections to 10. For more information regarding this issue, refer to the Windows Vista EULA or the Windows XP Pro EULA .

\*\*SmarterMail includes a basic Web server, so the product is fully function upon installation□even without the existence of IIS or other Web servers. However, SmarterTools recommends installing Microsoft IIS 7.0 in place of the SmarterMail Web server for increased performance and security. For more information, see [Running SmarterMail as an IIS Site](#) .

## Installation

SmarterMail comes as a single installation file that contains everything necessary to run the product. The SmarterMail installer can be downloaded from <http://www.smartertools.com> . Both the free and the licensed editions of SmarterMail are contained within this installation file, so it is not necessary to download or install the file again if you purchase a license after trying the free edition.

Please refer to the KB article [How To - Install SmarterMail](#) for step-by-step installation instructions.

## Running as an IIS Site

By default, SmarterMail installs a basic Web server that allows companies to start using the application immediately after installation. However, SmarterTools recommends moving to a more robust and secure Web server, such as Microsoft IIS. For step-by-step instructions on configuring SmarterMail to run with Microsoft IIS 7.0, please refer to the KB article [How To - Set up SmarterMail as an IIS Site](#) .

Alternatively, you may run SmarterMail as a virtual directory under an existing site. However, this is not recommended. For more information, please refer to the KB article [How To - Set Up SmarterMail as a Virtual Directory Under an Existing IIS Site](#) .

Note: This help topic assumes familiarity with Microsoft IIS and how it works. SmarterTools recommends using the basic Web server included with SmarterMail if you are unfamiliar with or uncomfortable using Microsoft IIS.

## Activating SmarterMail

In order for SmarterMail to function for more than 10 users, the product must be activated using a valid license key. In addition, if SmarterMail is moved to another server or assigned to a different database, the product may need to be reactivated.

To access the product activation wizard, click the settings icon . Then expand the Activation folder and click Licensing in the navigation pane. The edition and license level information for the version of SmarterMail currently being used will load in the content pane.

To activate or reactivate a valid license key, click **Activate** in the content pane toolbar. For step-by-step activation instructions, please refer to the KB article [How To - Activate SmarterMail](#) . Note: Activation of a license key requires the server to contact SmarterTools over port 443 (HTTPS). Please ensure that any firewall or internet security software you have installed allows an outgoing TCP port 443 request.

[Return to Getting Started](#)

## Upgrading SmarterMail

Because the SmarterMail 8.x download contains all of the installation files needed for any licensing level or edition, upgrading editions or levels is relatively easy. With a valid license key, companies can easily upgrade to the professional or enterprise editions or increase the number of mailboxes available in SmarterMail. For more information, see the [Activating SmarterMail](#) section of the online help. For step-by-step instructions, please refer to the KB article [How To - Upgrade SmarterMail Levels and Editions](#) .

The steps for upgrading to SmarterMail 8.x from an older version of the application vary depending on which version you are currently using. For more information, please refer to the KB article [How To - Upgrade SmarterMail](#) .

## SmarterMail Add-ons

SmarterTools' add-on licensing system allows users to enhance the functionality of SmarterTools products. The following add-ons are available for SmarterMail 7.x:

- Microsoft Exchange ActiveSync
- Commtouch Premium Antispam
- Commtouch Zero-hour Antivirus

### Microsoft Exchange ActiveSync

Microsoft Exchange ActiveSync is a data synchronization protocol that enables over-the-air access to email, calendars, tasks, and notes from most mobile devices, including Blackberry, iPhone, Palm Pre, and Windows Mobile devices. In addition, Exchange ActiveSync enables SmarterMail users to have access their email, calendars, tasks, and notes while working offline.

For step-by-step instructions on how to activate and enable the Exchange ActiveSync add-on, please refer to the KB articles [How To - Activate Microsoft Exchange ActiveSync](#) and [How To - Configure Microsoft Exchange ActiveSync for Email Accounts](#) .

## **Commtouch Premium Antispam**

The Commtouch Premium Antispam add-on uses Recurrent Pattern Detection (RPD) technology to protect against spam outbreaks in real time as messages are mass-distributed over the Internet. Rather than evaluating the content of messages, the Commtouch Detection Center analyzes large volumes of Internet traffic in real time, recognizing and protecting against new spam outbreaks the moment they emerge.

For step-by-step instructions on how to activate and enable the Commtouch add-on, please refer to the KB articles [How To - Activate Commtouch Premium Antispam](#) and [How To - Enable Commtouch Premium Antispam](#).

## **Commtouch Zero-hour Antivirus**

The Commtouch Zero-hour Antivirus add-on identifies viruses based on their unique distribution patterns and provides a complementary shield to conventional AV technology, protecting in the earliest moments of malware outbreaks and continuing protection as each new variant emerges.

For step-by-step instructions on how to activate and enable the Commtouch add-on, please refer to the KB articles [How To - Activate Commtouch Zero-hour Antivirus](#) and [How To - Enable Commtouch Zero-hour Antivirus](#).

## **Automation with Web Services**

Completing Tasks and Functions from Control Panels and Third-party Applications

### **Who Should Use This Document**

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

### **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 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.

To view the available Web services and their corresponding functions, go to your Web interface installation location and append "Services/SERVICENAME.asmx". With the default installation, you would use <http://127.0.0.1:9998/Services/svcServerAdmin.asmx>.

When you set up a Web reference to these Web services you will want to include the full path to your SmarterMail installation with the service name indicated in each section below (for example, <http://support.example.com/Services/SERVICENAME.asmx>).

In the sections that follow, you will find a brief explanation of the available Web services, along with the default installation paths to the specific Web service details page.

### **User Alias Administration Services/svcAliasAdmin.asmx**

The Alias Admin Web service handles all functions dealing with user aliases. The following functions are available in this Web service:

- AddAlias : Creates a new alias and adds it to the specified domain
- Return Type : GenericResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
- AuthPassword : Password for the username
- DomainName : The domain to which the alias will be added
- AliasName : The name of the alias to add
- Addresses : An array of addresses that this alias represents
- DeleteAlias : Deletes the specified alias
- Return Type : GenericResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
- AuthPassword : Password for the username
- DomainName : The domain from which the alias will be deleted
- AliasName : The name of the alias to delete
- GetAlias : Returns the specified alias
- Return Type : AliasInfoResult
- Parameters :

- AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - DomainName : The domain from which to get the alias
  - AliasName : The name of the alias to get
  - GetAliases : Returns all aliases that belong to a specified domain
  - Return Type : AliasInfoListResult
  - Parameters :
- 
- AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - DomainName : The domain from which to get all aliases
  - SetCatchAll : Sets the specified alias to be the catch-all or clears the catch-all if a blank alias name is provided
  - Return Type : GenericResult
  - Parameters :
- 
- AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - DomainName : The domain for which to alter the catch-all
  - AliasName : The name of the alias that should be the new catch all. If this parameter is blank, the catch-all is disabled
  - UpdateAlias : Updates the specified alias
  - Return Type : GenericResult
  - Parameters :
- 
- AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - DomainName : The domain in which the alias will be updated
  - AliasName : The name of the alias to update
  - Addresses : An array of addresses that this alias represents

The following return types are used:

- GenericResult : Generic result information for a Web service request

- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- AliasInfoResult : Result for the GetAlias request
  
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- AliasInfo : An AliasInfstructure
- AliasInfoListResult : Result for the GetAliases request
  
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- AliasInfo : Array of AliasInfstructures
- AliasInfo : Represents an Alias
  
- Name : Name of the alias
- Addresses : Array of addresses that the alias represents

### **Domain Administration Services/svcDomainAdmin.asmx**

The Domain Admin Web service handles all functions dealing with domains. The following functions are available in this Web service:

- AddDomain : Creates a new domain
  
- Return Type : GenericResult
- Parameters :
  
- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- DomainName : The name of the domain tadd
- Path : The storage location of the domain's data
- PrimaryDomainAdminUserName : The username for the primary admin of this domain
- PrimaryDomainAdminPassword : The password for the primary domain admin
- PrimaryDomainAdminFirstName : The first name of the primary domain admin
- PrimaryDomainAdminLastName : The last name of the primary domain admin
- IP : The IP address that this domain should listen on
- ImapPort : The port this domain should accept IMAP connections on



- PopPort : The port this domain should accept POP connections on
  - SmtptPort : The port this domain should accept SMTP connections on
  - MaxAliases : The maximum number of aliases this domain is allowed have (0 = unlimited)
  - MaxDomainSizeInMB : The maximum size this domain is allowed to occupy (0 = unlimited)
  - MaxDomainUsers : The maximum number of users this domain is allowed have (0 = unlimited)
  - MaxMailboxSizeInMB : This parameter is no longer used
  - MaxMessageSize : The maximum size of a message users on this domain are allowed to send (0 = unlimited)
  - MaxRecipients : The maximum number of recipients that are allowed in a single email (0 = unlimited)
  - MaxDomainAliases : The maximum number of domain aliases this domain is allowed have (0 = unlimited)
  - MaxLists : The maximum number of mailing lists this domain is allowed have (0 = unlimited)
- 
- ShowDomainAliasMenu : If this is set to false, domain administrators will not be able to manage domain aliases
  - ShowContentFilteringMenu : If this is set to false, users will not be able to use content filtering
  - ShowSpamMenu : If this is set to false, users will not be able to manage their own spam settings
  - ShowStatsMenu : This parameter is no longer used
  - RequireSmtpAuthentication : If this is set to true, the domain will require SMTP Authentication for relay emails
  - ShowListMenu : If this is set to false, domain administrators will not be able to manage mailing lists
  - ListCommandAddress : This is the command address for mailing lists
  - AddDomainForwardingBlock : Adds a domain forwarding block
- 
- Return Type : GenericResult
  - Parameters :
- 
- AuthUserName : User name used to perform this function. Requires system administrator privileges
  - AuthPassword : Password for the username
  - TargetAddress : The IP address that will receive mail for the specified domains
  - Domains : An array of domain names for which to forward mail
  - DeleteDomain : Deletes the specified domain
- 
- Return Type : GenericResult
  - Parameters :

- AuthUserName : User name used to perform this function. Requires system administrator privileges
  - AuthPassword : Password for the username
  - DomainName : The domain tdelete
  - DeleteFiles : If this is set ttrue, all emails and configurations for this domain will be permanently deleted
  - DeleteDomainForwardBlockByTargetAddress : Deletes a domain forwarding block
  - Return Type : GenericResult
  - Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
  - AuthPassword : Password for the username
  - TargetAddress : The target address tdelete. Any forwards set tforward tthis IP address will be deleted
  - DeleteDomainForwardingBlock : Deletes a domain forwarding block
  - Return Type : GenericResult
  - Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
  - AuthPassword : Password for the username
  - blockID : The ID of the forwarding block tdelete
  - DisableDomain : Disable the given domain
  - Return Type : GenericResult
  - Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
  - AuthPassword : Password for the username
  - DomainName : The domain tdisable
  - EnableDomain : Enables the given domain
  - Return Type : GenericResult
  - Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges

- AuthPassword : Password for the username
- DomainName : The domain tenable
- GenerateDomainKeysCert : Generates a domainkeys certificate for the domain
- Return Type : DomainKeyResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- DomainName : Domain for which the certificate should be created
- KeySize : Size of the certificate key (512/768/1024/1536/2048 bit)
- Selector : DomainKeys selector tuse
- GetAllDomainStatistics : Returns the statistics for all domains over the specified period of time
- Return Type : AllDomainStatResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- StartDate : The starting range for statistics
- EndDate : The end range for statistics
- GetAllDomains : Returns a list of all domain names
- Return Type : DomainListResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- GetDomainCounts : Returns the usage counts for the specified domain
- Return Type : DomainCountInfoResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username

- DomainName : Domain for which the counts should be retrieved
- GetDomainDefaults : Returns the default domain settings
- Return Type : DomainSettingsResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- GetDomainForwarding : Returns the domain forwarding info
- Return Type : DomainForwardInfoResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- IncludeDomains : If this is true, the domains will be included in the results. If false, only the target addresses will be returned
- GetDomainForwardingBlock : Returns the domain forwarding block settings
- Return Type : DomainForwardBlockInfoResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- blockID : The ID of the domain forwarding block return
- GetDomainForwardingBlockByTargetAddress : Returns the domain forwarding block
- Return Type : DomainForwardBlockInfoResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- targetAddress : The target address of the forwarding block return
- GetDomainKeysCert : Retrieves information about the domainkeys certificate for the domain
- Return Type : DomainKeyResult
- Parameters :

- AuthUserName : User name used to perform this function. Requires system administrator privileges
  - AuthPassword : Password for the username
  - DomainName : Domain for which the certificate should be retrieved
  - GetDomainInfo : Returns the name and path of the specified domain
  - Return Type : DomainInfoResult
  - Parameters :
- 
- AuthUserName : User name used to perform this function. Requires system administrator privileges
  - AuthPassword : Password for the username
  - domainName : The name of the domain
  - GetDomainSettings : Returns the domain settings
  - Return Type : DomainSettingsResult
  - Parameters :
- 
- AuthUserName : User name used to perform this function. Requires system administrator privileges
  - AuthPassword : Password for the username
  - domainName : The name of the domain
  - GetDomainStatistics : Returns the statistics for the specified domain over the specified period of time
  - Return Type : StatInfoResult
  - Parameters :
- 
- AuthUserName : User name used to perform this function. Requires system administrator privileges
  - AuthPassword : Password for the username
  - domainName : The name of the domain
  - StartDate : The start range for the statistics
  - EndDate : The end range for the statistics
  - GetDomainUsers : Returns all valid usernames for the domain. Includes users, aliases, and mailing lists
  - Return Type : DomainUserInfoResult
  - Parameters :

- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- DomainName : Domain for which the users should be retrieved
- GetPrimaryDomainAdmin : Gets the primary domain administrator of the specified domain
- Return Type : PrimaryDomainAdminResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- domainName : The name of the domain
- GetRequestedDomainDefaults : Returns the requested default domain settings
- Return Type : SettingsRequestResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- requestedSettings : An array of settings to return. Valid keys are:
  - defaultaltsmtpport (Alternate SMTP Port)
  - defaultaltsmtpportenabled (Enable Alternate SMTP Port)
  - defaultautoresponderrestriction (Limit autoresponders once per day per sender)
  - defaultbypassgreylisting (Bypass greylisting)
  - defaultenablecatchalls (Enable Catch-alls)
  - defaultenabledomainkeys (Enable Domain Keys signing)
  - defaultenableemailreports (Enable Email Reports)
  - defaultenablefilestorage (Enable File Storage)
  - defaultenableimapretrieval (Enable IMAP Retrieval)
  - defaultenablepopretrieval (Enable POP Retrieval)
  - defaultimapport (IMAP Port)
  - defaultldapport (LDAP Port)
  - defaultmaxaliases (Maximum aliases, 0=unlimited)
  - defaultmaxdomainaliases (Maximum domain aliases, 0=unlimited)
  - defaultmaxdomainsize (Maximum domain size, 0=unlimited)
  - defaultmaxdomainusers (Maximum users, 0=unlimited)

- defaultmaximapretrievalaccounts (Maximum IMAP retrieval accounts, 0=unlimited)
- defaultmaxlists (Maximum mailing lists, 0=unlimited)
- defaultmaxmailboxsize (Maximum mailbox size, 0=unlimited)
- defaultmaxmessagesize (Maximum message size, 0=unlimited)
- defaultmaxmessagesperhour (Maximum messages allowed per hour)
- defaultmaxmessagesperhourenabled (Enable Max Messages Throttling)
- defaultmaxsmtpoutbandwidthperhour (Maximum bandwidth usage allowed per hour (MB))
- defaultmaxsmtpoutbandwidthperhourenabled (Enable Max Bandwidth Throttling)
- defaultmaxpopretrievalaccounts (Maximum POP retrieval accounts, 0=unlimited)
- defaultmaxrecipients (Maximum recipients per message, 0=unlimited)
- defaultpopport (POP Port)
- defaultsharedcalendar (Enable Shared Calendars)
- defaultsharedcontact (Enable Shared Contacts)
- defaultsharedfolder (Enable Shared Folders)
- defaultsharedgal (Enable Global Address List)
- defaultsharednotes (Enable Shared Notes)
- defaultsharedtasks (Enable Shared Tasks)
- defaultshowcalendar (Enable Calendaring)
- defaultshowcontacts (Enable Contacts)
- defaultshowcontentfilteringmenu (Enable Content Filters)
- defaultshowdomainaliasmenu (Enable Domain Aliases)
- defaultshowdomainreports (Enable Domain Reports)
- defaultshowlistmenu (Enable Mailing Lists)
- defaultshownotes (Enable Notes)
- defaultshowspammenu (Enable Spam Options)
- defaultshowtasks (Enable Tasks)
- defaultshowuserreports (Enable User Reports)
- defaultskin (Default Skin name)
- defaultsmtpauthenticationrequired (Require SMTP Auth)
- defaultsmtpport (SMTP Port)
- defaultspamresponderoption (Auto-responder spam restriction: none, low, medium, high)
- defaultspamforwardoption (Forward spam restriction: none, low, medium, high)
- GetRequestedDomainSettings : Gets the settings for the specified domain
- Return Type : SettingsRequestResult
- Parameters :

- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- DomainName : The name of the domain
- requestedSettings : An array of settings treturn. Valid keys are:
  - altsmtpport (Alternate SMTP port)
  - altsmtpportenabled (Enable alternate SMTP port)
  - autoresponderrestriction (Limit auto-responders tonce per day per sender)
  - bypassgreylisting (Bypass greylisting)
  - catchall (Name of the catch-all alias)
  - domainurl (Logout URL)
  - enablecatchalls (Enable catch-alls)
  - enabledomainkeys (Enable Domain Keys signing)
  - enabledomainuserservicecontrol (Enables control of Service Access Control)
  - enablemailsigning (Enables Domain Keys and DKIM signing)
  - enableemailreports (Enable email reports)
  - enablepopretrieval (Enable POP retrieval)
  - enableimapretrieval (Enable IMAP retrieval)
  - imapport (IMAP port)
  - isenabled (Domain enabled)
  - ldapport (LDAP port)
  - listcommandaddress Listserv command address)
  - maxaliases (Maximum aliases, 0=unlimited)
  - maxdomainaliases (Maximum domain aliases, 0=unlimited)
  - maximapretrievalaccounts (Maximum IMAP retrieval accounts, 0=unlimited)
  - maxlists (Maximum mailing lists, 0=unlimited)
  - maxmessagesize (Maximum message size, 0=unlimited)
  - maxmessagesperhour (Maximum messages allowed per hour)
  - maxmessagesperhourenabled (Maximum bandwidth usage allowed per hour (MB))
  - maxsmtpoutbandwidthperhourenabled (Enable max bandwidth throttling)
  - maxrecipients (Maximum recipients per message, 0=unlimited)
  - maxsize (Maximum domain size (KB), 0=unlimited)
  - maxusers (Maximum users, 0=unlimited)
  - popport (POP port)
  - requiresmtpauthentication (Require SMTP authentication)
  - serverip (IP address)



- sharedcalendar (Enable shared calendars)
  - sharedcontact (Enable shared contacts)
  - sharedfolder (Enable shared folders)
  - sharednotes (Enable shared notes)
  - sharedtasks (Enable shared tasks)
  - sharedgal (Enable Global Address List)
  - showcalendar (Enable calendaring)
  - showcontacts (Enable contacts)
  - showcontentfilteringmenu (Enable content filters)
  - showdomainaliasmenu (Enable domain aliases)
  - showdomainreports (Enable domain reports)
  - shownotes (Enable notes)
  - showuserreports (Enable user reports)
  - showtasks (Enable tasks)
  - showlistmenu (Enable mailing lists)
  - showspammenu (Enable spam options)
  - smtpport (SMTP port)
  - spamresponderoption (Auto-responder spam restriction: none, low, medium, high)
  - spamforwardoption (Forward spam restriction: none, low, medium, high)
  - ReloadDomain : Reloads the specified domain's settings
- 
- Return Type : GenericResult
  - Parameters :
- 
- AuthUserName : User name used to perform this function. Requires system administrator privileges
  - AuthPassword : Password for the username
  - domainName : The name of the domain
  - RenameDomain : Renames the specified domain
- 
- Return Type : GenericResult
  - Parameters :
- 
- AuthUserName : User name used to perform this function. Requires system administrator privileges
  - AuthPassword : Password for the username
  - OldDomainName : The current name of the domain
  - NewDomainName : The new name of the domain

- SetDomainForwardingBlock : Updates the target address and domains in a domain forwarding block

- Return Type : GenericResult

- Parameters :

- AuthUserName : User name used to perform this function. Requires system administrator privileges

- AuthPassword : Password for the username

- blockID : The ID of the forwarding block to update

- targetAddress : The new target address for the domain forwarding block

- domains : An array of domain names that will be forwarded to the specified target address

- SetDomainForwardingBlockByTargetAddress : Updates the domains in a domain forwarding block

- Return Type : GenericResult

- Parameters :

- AuthUserName : User name used to perform this function. Requires system administrator privileges

- AuthPassword : Password for the username

- targetAddress : The existing target address for the domain forwarding block

- domains : An array of domain names that will be forwarded to the specified target address

- SetPrimaryDomainAdmin : Sets the specified user to be the primary domain admin of the specified domain

- Return Type : GenericResult

- Parameters :

- AuthUserName : User name used to perform this function. Requires system administrator privileges

- AuthPassword : Password for the username

- DomainName : The name of the domain

- AdminUserName : The new primary domain admin

- SetRequestedDomainDefaults : Updates the specified default domain settings

- Return Type : GenericResult

- Parameters :

- AuthUserName : User name used to perform this function. Requires system administrator privileges

- AuthPassword : Password for the username
- newSettings : An array of settings tupdate. The format is “key=value” and the following keys are valid:
  - defaultaltsmtpport (Alternate SMTP port)
  - defaultaltsmtpportenabled (Enable alternate SMTP port)
  - defaultautoresponderrestriction (Limit auto-responders tonce per day per sender)
  - defaultbypassgreylisting (Bypass greylisting)
  - defaultenablecatchalls (Enable Catch-alls)
  - defaultenabledomainkeys (Enable Domain Keys signing)
  - defaultenableemailreports (Enable email reports)
  - defaultenablefilestorage (Enable file storage)
  - defaultenableimapretrieval (Enable IMAP retrieval)
  - defaultenablepopretrieval (Enable POP retrieval)
  - defaultimapport (IMAP port)
  - defaultldapport (LDAP port)
  - defaultmaxaliases (Maximum aliases, 0=unlimited)
  - defaultmaxdomainaliases (Maximum domain aliases, 0=unlimited)
  - defaultmaxdomainsize (Maximum domain size, 0=unlimited)
  - defaultmaxdomainusers (Maximum users, 0=unlimited)
  - defaultmaximapretrievalaccounts (Maximum IMAP retrieval accounts, 0=unlimited)
  - defaultmaxlists (Maximum mailing lists, 0=unlimited)
  - defaultmaxmailboxsize (Maximum mailbox size, 0=unlimited)
  - defaultmaxmessagesize (Maximum message size, 0=unlimited)
  - defaultmaxmessagesperhour (Maximum messages allowed per hour)
  - defaultmaxmessagesperhourenabled (Enable max messages throttling)
  - defaultmaxsmtpoutbandwidthperhour (Maximum bandwidth usage allowed per hour (MB))
  - defaultmaxsmtpoutbandwidthperhourenabled (Enable max bandwidth throttling)
  - defaultmaxpopretrievalaccounts (Maximum POP retrieval accounts, 0=unlimited)
  - defaultmaxrecipients (Maximum recipients per message, 0=unlimited)
  - defaultpopport (POP port)
  - defaultsharedcalendar (Enable shared calendars)
  - defaultsharedcontact (Enable shared contacts)
  - defaultsharedfolder (Enable shared folders)
  - defaultsharedgal (Enable Global Address List)
  - defaultsharednotes (Enable shared notes)
  - defaultsharedtasks (Enable shared tasks)
  - defaultshowcalendar (Enable calendaring)

- defaultshowcontacts (Enable contacts)
- defaultshowcontentfilteringmenu (Enable content filters)
- defaultshowdomainaliasmenu (Enable domain aliases)
- defaultshowdomainreports (Enable domain reports)
- defaultshowlistmenu (Enable mailing lists)
- defaultshownotes (Enable notes)
- defaultshowspammenu (Enable spam options)
- defaultshowtasks (Enable tasks)
- defaultshowuserreports (Enable user reports)
- defaultskin (Default skin name)
- defaultsmtpauthenticationrequired (Require SMTP auth)
- defaultsmtpport (SMTP port)
- defaultspamresponderoption (Auto-responder spam restriction: none, low, medium, high)
- defaultspamforwardoption (Forward spam restriction: none, low, medium, high)
- SetRequestedDomainSettings : Updates the settings for the specified domain
  
- Return Type : GenericResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator privileges
  - AuthPassword : Password for the username
  - newSettings : An array of settings tupdate. The format is “key=value” and the following keys are valid:
    - altsmtpport (Alternate SMTP port)
    - altsmtpportenabled (Enable alternate SMTP port)
    - autoresponderrestriction (Limit auto-responders tonce per day per sender)
    - bypassgreylisting (Bypass greylisting)
    - catchall (Name of the catch-all alias)
    - domainurl (Logout URL)
    - enablecatchalls (Enable Catch-all)
    - enabledomainkeys (Enable Domain Keys signing)
    - enabledomainuserservicecontrol (Enables control of Service Access Control)
    - enablemailsigning (Enables Domain Keys and DKIM signing)
    - enableemailreports (Enable email reports)
    - enableimapretrieval (Enable IMAP retrieval)
    - enablepopretrieval (Enable POP retrieval)
    - imapport (IMAP port)

- isenabled (Domain enabled)
- ldapport (LDAP port)
- listcommandaddress (Listserv command address)
- maxaliases (Maximum aliases, 0=unlimited)
- maxdomainaliases (Maximum domain aliases, 0=unlimited)
- maxlists (Maximum mailing lists, 0=unlimited)
- maximapretrievalaccounts (Maximum IMAP retrieval accounts, 0=unlimited)
- maxmessagesize (Maximum message size, 0=unlimited)
- maxmessagesize (Maximum message size, 0=unlimited)
- maxmessagesperhour (Maximum messages allowed per hour)
- maxmessagesperhourenabled (Enable max messages throttling)
- maxsmtpoutbandwidthperhour (Maximum bandwidth usage allowed per hour (MB))
- maxsmtpoutbandwidthperhourenabled (Enable max bandwidth throttling)
- maxrecipients (Maximum recipients per message, 0=unlimited)
- maxsize (Maximum domain size (KB), 0=unlimited)
- maxusers (Maximum users, 0=unlimited)
- popport (POP port)
- requiresmtpauthentication (Require SMTP auth)
- serverip (IP address)
- sharedcalendar (Enable shared calendars)
- sharedcontact (Enable shared contacts)
- sharedfolder (Enable shared folders)
- sharednotes (Enable shared notes)
- sharedtasks (Enable shared tasks)
- sharedgal (Enable Global Address List)
- showcalendar (Enable calendaring)
- showcontacts (Enable contacts)
- showcontentfilteringmenu (Enable content filters)
- showdomainaliasmenu (Enable domain aliases)
- showdomainreports (Enable domain reports)
- shownotes (Enable notes)
- showuserreports (Enable user reports)
- showtasks (Enable tasks)
- showlistmenu (Enable mailing lists)
- showspammenu (Enable spam options)
- smtpport (SMTP port)
- spamresponderoption (Auto-responder spam restriction: none, low, medium, high)

- spamforwardoption (Forward spam restriction: none, low, medium, high)
- UpdateDomain : Updates the settings for the specified domain
  
- Return Type : GenericResult
- Parameters :
  
- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- DomainName : The name of the domain tadd
- ServerIP : The IP address that this domain should listen on
- ImapPort : The port this domain should accept IMAP connections on
- PopPort : The port this domain should accept POP connections on
- Smtport : The port this domain should accept SMTP connections on
- MaxAliases : The maximum number of aliases this domain is allowed thave (0=unlimited)
- MaxDomainSizeInMB : The maximum size this domain is allowed to occupy. (0=unlimited)
- MaxDomainUsers : The maximum number of users this domain is allowed thave. (0=unlimited)
- MaxMailboxSizeInMB : This parameter is nlonger used
- MaxMessageSize : The maximum size of a message users on this domain are allowed tsend. (0=unlimited)
- MaxRecipients : The maximum number of recipients that are allowed in a single email. (0=unlimited)
- MaxDomainAliases : The maximum number of domain aliases this domain is allowed thave. (0=unlimited)
- MaxLists : The maximum number of mailing lists this domain is allowed thave. (0=unlimited)
- ShowDomainAliasMenu : If this is set tfalse, domain admins will not be able tmanage domain aliases.
- ShowContentFilteringMenu : If this is set tfalse, users will not be able tuse content filtering
- ShowSpamMenu : If this is set tfalse, users will not be able tmanage their own spam settings
- ShowStatsMenu : This parameter is nlonger used
- RequireSmtportAuthentication : If this is set ttrue, the domain will require SMTP authentication trelay emails
- ShowListMenu : If this is set tfalse, domain admins will not be able to manage mailing lists
- ListCommandAddress : This is the command address for mailing lists
- UpdateDomainNameAndPath : Changes the specified domain's name and/or path.
  
- Return Type : GenericResult
- Parameters :

- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- OldDomainName : The current name of the domain
- NewDomainName : The new name of the domain
- NewDomainPath : The new path for the domain

The following return types are used:

- GenericResult : Generic result information for a Web service request
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- SettingsRequestResult : Returned by GetRequestedDomainDefaults and GetRequestedDomainSettings
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- settingValues : Array of setting values, in the form of key=value
- DomainListResult : Returned by GetAllDomains
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- DomainNames : Array of domain names
- StatInfoResult : Returned by GetDomainStatistics
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- MessagesReceived : Total number of messages received in that time period
- MessagesSent : Total number of messages sent in that time period
- BytesSent : Total number of bytes sent in that time period
- BytesReceived : Total number of bytes received in that time period
- BytesSize : Total disk space used by the domain
- DomainSettingsResult : Returned by GetDomainDefaults and GetDomainSettings

- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- ServerIP : The IP the domain is listening on
- Path : The storage location of the domain's data
- ImapPort : The port this domain should accept IMAP connections on
- PopPort : The port this domain should accept POP connections on
- Smtpport : The port this domain should accept SMTP connections on
- MaxAliases : The maximum number of aliases this domain is allowed have (0=unlimited)
- MaxDomainSizeInMB : The maximum size this domain is allowed to occupy (0=unlimited)
- MaxDomainUsers : The maximum number of users this domain is allowed have (0=unlimited)
- MaxMailboxSizeInMB : This parameter is nlonger used
- MaxMessageSize : The maximum size of a message users on this domain are allowed tsend (0=unlimited)
- MaxRecipients : The maximum number of recipients that are allowed in a single email (0=unlimited)
- MaxDomainAliases : The maximum number of domain aliases this domain is allowed have (0=unlimited)
- MaxLists : The maximum number of mailing lists this domain is allowed have (0=unlimited)
- ShowDomainAliasMenu : If this is set tfalse, domain admins will not be able tmanage domain aliases
- ShowContentFilteringMenu : If this is set tfalse, users will not be able tuse content filtering
- ShowSpamMenu : If this is set tfalse, users will not be able tmanage their own spam settings
- ShowStatsMenu : This parameter is nlonger used
- RequireSmtpAuthentication : If this is set ttrue, the domain will require SMTP Authentication trelay emails
- ShowListMenu : If this is set tfalse, domain admins will not be able to manage mailing lists
- ListCommandAddress : This is the command address for mailing lists
- EnableFileStorage : This specifies whether file storage is enabled
- DomainInfoResult : Returned by GetDomainInfo
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- Path : Path tthe domain
- PrimaryDomainAdminResult : Returned by GetPrimaryDomainAdmin



- Result : True or false depending on the success of the Web service request
  - ResultCode : Specific failure code if the result is false
  - Message : Error message detailing why the result is false
  - PrimaryAdmin : Primary domain admin for the domain
  - AllDomainStatResult : Returned by GetAllDomainStatistics
- Result : True or false depending on the success of the Web service request
  - ResultCode : Specific failure code if the result is false
  - Message : Error message detailing why the result is false
  - Stats : An array of DomainStatInfstructs
  - DomainForwardInfoResult : Returned by GetDomainForwarding
- Result : True or false depending on the success of the Web service request
  - ResultCode : Specific failure code if the result is false
  - Message : Error message detailing why the result is false
  - Blocks : An array of DomainForwardBlockInfstructs
  - DomainForwardBlockInfoResult : Returned by GetDomainForwardingBlock
- Result : True or false depending on the success of the Web service request
  - ResultCode : Specific failure code if the result is false
  - Message : Error message detailing why the result is false
  - domainForwardBlock : A DomainForwardBlockInfstruct

### **Mail List Administration Services/svcMailListAdmin.asmx**

The Mail List Web service handles all functions dealing with mailing lists. The following functions are available in this Web service:

- AddDigestSubscriber : Adds a digest subscriber tthe specified list
- Return Type : GenericResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
- AuthPassword : Password for the username
- DomainName : The domain name for which tmodify the list
- ListName : Name of the list tmodify
- Subscriber : Email address tadd tthe digest list
- AddList : Adds a mailing list tthe specified domain

- Return Type : GenericResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - DomainName : The domain name for which tadd the list
  - ListName : Name of the list tadd
  - Moderator : Moderator of the list
  - Description : Description of the list
  - AddSubscriber : Adds a subscriber tthe specified list
- Return Type : GenericResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - DomainName : The domain name for which tmodify the list
  - ListName : Name of the list tmodify
  - Subscriber : Email address tadd tthe list
  - DeleteAllLists : Deletes all mailing lists that belong tthe specified domain
- Return Type : GenericResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - DomainName : The domain name for which tdelete all lists
  - DeleteList : Deletes a mailing list that belongs tthe specified domain
- Return Type : GenericResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - DomainName : The domain name for which tdelete the list

- ListName : Name of the list tdelete
- GetDigestSubscriberList : Returns the digest subscribers for the given list
- Return Type : SubscriberListResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - DomainName : The domain name from which treturn the list
  - ListName : The name of the list treturn
  - GetListCommandAddress : Gets the command list address for the specified domain
- Return Type : ListCommandResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - DomainName : The domain name for which treturn the command address
  - GetMailingListsByDomain : Returns all mailing lists for the specified domain
- Return Type : MailingListResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - DomainName : The domain name for which treturn the list
  - GetRequestedListSettings : Gets the requested settings for the specified list
- Return Type : SettingsRequestResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - DomainName : The domain name twhich the list belongs
  - ListName : Name of the list tget settings for
  - requestedSettings : Array of settings treturn. Valid keys are:

- description
- disabled
- moderator
- password
- whocanpost (anyone, subscribersonly, moderatoronly)
- subject (text tadd tsubject)
- prependsubject (true/false)
- maxmessagesize (in KB)
- replytolist (true/false)
- digestmode (true/false)
- sendsubscribe (true/false)
- sendunsubscribe (true/false)
- allowunsubscribe (true/false)
- disablelistcommand (true/false)
- disablesubscribecommand (true/false)
- GetSubscriberList : Returns the subscribers for the given list
  
- Return Type : SubscriberListResult
- Parameters :
  
- AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
- AuthPassword : Password for the username
- DomainName : The domain name from which treturn the list
- ListName : The name of the list treturn
- RemoveDigestSubscriber : Removes a digest subscriber tthe specified list
  
- Return Type : GenericResult
- Parameters :
  
- AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
- AuthPassword : Password for the username
- DomainName : The domain name for which tmodify the list
- ListName : The name of the list tmodify
- Subscriber : Email address tremove from the list
- RemoveSubscriber : Removes a subscriber tthe specified list

- Return Type : GenericResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - DomainName : The domain name for which tmodify the list
  - ListName : The name of the list tmodify
  - Subscriber : Email address tremove from the list
  - SetDigestSubscriberList : Sets the digest subscribers for the given list
- Return Type : GenericResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - DomainName : The domain name for which tmodify the list
  - ListName : The name of the list tmodify
  - Subscribers : An array of email addresses tset as the subscriber list
  - SetListCommandAddress : Sets the command list address for the specified domain
- Return Type : GenericResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - DomainName : The domain name for which tset the command address
  - SetRequestedListSettings : Sets the requested settings for the specified list
- Return Type : GenericResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - DomainName : The domain name twhich the list belongs
  - ListName : Name of the list tupdate
  - newSettings : An array of key/value pairs in the form of key=value

- description
- disabled
- moderator
- password
- requirepassword
- whocanpost (anyone, subscriberonly, moderatoronly)
- subject (text tadd tsubject)
- prependsubject (true/false)
- maxmessagesize (in KB)
- replytolist (true/false)
- digestmode (true/false)
- sendsubscribe (true/false)
- sendunsubscribe (true/false)
- allowunsubscribe (true/false)
- disablelistcommand (true/false)
- disablesubscribecommand (true/false)
- SetSubscriberList : Sets the subscribers for the given list
  
- Return Type : GenericResult
- Parameters :
  
- AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
- AuthPassword : Password for the username
- DomainName : The domain name for which tmodify the list
- ListName : The name of the list tmodify
- Subscribers : An array of email addresses tset as the subscriber list

The following return types are used:

- GenericResult : Generic result information for a Web service request
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- MailingListResult : Returned by GetMailingListsByDomain
  
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false

- listNames : An array of list names
- SubscriberListResult : Returned by GetSubscriberList and GetDigestSubscriberList
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- Subscribers : An array of subscriber email addresses
- SettingsRequestResult : Returned by SetRequestedListSettings
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- settingsValues : An array of key/value pairs in the form of key=value
- ListCommandResult : Returned by GetListCommandAddress
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- commandAddress : The command address of the mailing list

### **Product Info Web Service Services/svcProductInfo.asmx**

The Product Info Web service handles all functions dealing with product information and activation. The following functions are available in this Web service:

- ActivateLicenseKey : Will activate the product with a previously set license key using the specified SmarterTools account credentials
- Return Type : GenericResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- AccountEmailAddress : The email address associated with the key
- AccountPassword : The password associated with the key
- GetLicenseInfo : Returns the license key for the product
- Return Type : LicenseInfoResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges

- AuthPassword : Password for the username
- GetProductInfo : Will return the product name and version number
- Return Type : ProductInfoResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- SetLicenseKey : Will set the product license key
- Return Type : GenericResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- Key : The new license key

The following return types are used:

- GenericResult : Generic result information for a Web service request
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- ProductInfoResult : Returned by the GetProductInfofunction
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- ProductInfoResult : Returned by the GetProductInfofunction
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- ProductName : Name of the product
- ProductVersion : Version of the product
- LicenseInfoResult : Returned by the GetLicenseInfofunction
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false



- Message : Error message detailing why the result is false
- LicenseKey : The license key associated with the product

### **Global Update Web Service Services/svcGlobalUpdate.asmx**

The Global Update Web service allows for changing settings across all domains. The following functions are available in this Web service:

- UpdateAllDomainSettings : Sets the supplied fields and values for all domains on the server
- Return Type : GenericResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- Fields : An array of DomainSettingFieldStruct structs. This struct has a property for the key and the value of the setting to change. For a list of valid keys, call the ListGlobalUpdateFields function.
- ListGlobalUpdateFields : Lists all the fields that can be updated using UpdateAllDomainSettings
- Return Type : GlobalUpdateFieldListResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- GetGlobalUpdateStatus : Gets the current status of the update (ex. 550 of 1335 domains updated)
- Return Type : GlobalUpdateStatusResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username

The following return types are used:

- GenericResult : Generic result information for a Web service request
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false

- Message : Error message detailing why the result is false
- GlobalUpdateStatusResult : Returned by GetGlobalUpdateStatus
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- isRunning : True if a global update is in place
- totalUpdateCount : Total number of domains being updated
- finishedCount : Number of domains that have already been updated
- GlobalUpdateFieldListResult : Returned by ListGlobalUpdateFields
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- Fields : An array of GlobalUpdateFieldInfoResult structs. These structs contain properties for the name, description, type, and default value of the fields

### **Domain Alias Administration Services/svcDomainAliasAdmin.asmx**

The Domain Alias Web service handles all functionality dealing with domain aliases. The following functions are available in this Web service:

- DeleteDomainAlias : Deletes the specified domain alias
- Return Type : GenericResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- DomainName : Domain name for which tdelete an alias
- DomainAliasName : The name of the alias tdelete
- GetAliases : Returns all domain aliases that belong tthe specified domain
- Return Type : DomainAliasInfoListResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- DomainName : Domain name for which tlist aliases
- AddDomainAlias : Creates a new domain alias and adds it tthe specified domain

- Return Type : GenericResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator privileges
  - AuthPassword : Password for the username
  - DomainName : Domain name for which to create an alias
  - DomainAliasName : The name of the alias
  - AddDomainAliasWithoutMxCheck : Creates a new domain alias and adds it to the specified domain without doing an MX lookup on the new alias
- Return Type : GenericResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator privileges
  - AuthPassword : Password for the username
  - DomainName : Domain name for which to create an alias
  - DomainAliasName : The name of the alias

The following return types are used:

- GenericResult : Generic result information for a Web service request
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- DomainAliasInfoListResult : Returned by the GetAliases function
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- DomainAliasNames : An array of domain aliases that exist for the requested domain

## **User Administration Services/svcUserAdmin.asmx**

The User Admin Web service handles all functionality dealing with the users. The following functions are available in this Web service:

- AddRSSFeed : Adds the specified RSS feed to the account

- Return Type : GenericResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges tchange an account other than itself
  - AuthPassword : Password for the username
  - rssUrl : URL of the RSS feed
  - rssName : Name of the RSS feed
  - rssFolder : Folder tplace the RSS feed in
  - AddUser : Creates a new user and adds them tthe specified domain

- Return Type : GenericResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - DomainName : Domain for which tadd the user
  - FirstName : First name
  - LastName : Last name
  - NewUsername : The username of the user tcreate
  - NewPassword : The password of the user tcreate
  - IsDomainAdmin : True if the user should be a domain admin
  - AddUser2 : Creates a new user and adds them tthe specified domain

- Return Type : GenericResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - DomainName : Domain for which tadd the user
  - FirstName : First name
  - LastName : Last name
  - NewUsername : The username of the user tcreate
  - NewPassword : The password of the user tcreate
  - IsDomainAdmin : True if the user should be a domain admin
  - MaxMailboxSize : Maximum size for the user mailbox (in MB)
  - AddUserGroup : Creates a new user group adds it tthe specified domain

- Return Type : GenericResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - DomainName : Domain twich the user group should be added
  - UserGroupName : Name of the usergroup
  - UserNames : Array of usernames that should belong tthe group
  - AuthenticateUser : Returns a true ResultCode if the user name, domain name, and password match

- Return Type : GenericResult
- Parameters :
  - UserName : Username
  - DomainName : Domain name
  - Password : Password
  - DeleteUser : Deletes the specified user from the specified domain

- Return Type : GenericResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - Username : User tdelete
  - Domain : Domain from which tdelete the user
  - DeleteRSSFeed : Deletes the specified RSS feed from the account

- Return Type : GenericResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges tchange an account other than itself
  - AuthPassword : Password for the username
  - EmailAddress : Address from which tdelete the feed
  - UID : Unique identifier of the RSS feed tdelete
  - GetRequestedUserSettings : Gets the specified user's settings

- Return Type : SettingsRequestResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - EmailAddress : Account for which return settings
  - requestedSettings : An array of settings return. Valid keys are:
    - autocleanoverrideactive (Should user override domain settings)
    - autopopupreminders (Automatically popup reminders window)
    - autorespondondirectmailonly (Ignore emails sent through aliases)
    - autosavedrafttime (Save every x milliseconds)
    - composefont
    - composefontsize
    - composemethod (html, plain)
    - composerows (Delete messages after autoforwarding)
    - deleteoption (MoveToDeleteFolder, AutoPurge, MarkDeleted, MarkDeletedAndHide)
    - dictionarylanguag (en-US, etc)
    - disablegreylsting
    - displayname (Display name of the user)
    - embedreplies (Attach forwards)
    - enableanimations (obsolete)
    - enablesounds (Play sounds in the webmail interface)
    - forwardaddress (Address tforward to)
    - forwardas (attachment, normal, plain)
    - fullname (basic, full)
    - hidefromgal
    - isdomainadmin
    - isenabled
    - lockpassword
    - maxsize (Max mailbox size in MB)
    - password
    - passwordlocked
    - plusaddressingenabled
    - plusaddressingfolder
    - previewautopreview (Automatically preview messages)
    - previewautomarkasread (Automatically mark messages as read after 5 seconds)

- previewusepreview (Use preview pane)
- replymessageindicator (Plain text indicator, > by default)
- replytoaddress
- requestreceipts (Automatically request read receipts on new messages)
- savecopyassent (Use Sent Items folder)
- seenwelcome (Has the user seen the welcome page)
- servicelevelmap (The enabled services for a user. This field is a bitmap composed of 1=POP, 2=IMAP, 4=INCOMING SMTP, 8=OUTGOING SMTP, 16=WEBMAIL)
- showsusc (Show the synchronization center popup on login)
- signature
- skin
- sortby (sorting of messages page)
- sortdescending (sort in reverse order)
- spamcheckoverrideactive (Should user override spam check settings from domain)
- spamforwardoption (obsolete)
- startuptime (today, messages)
- syncpanels (not used)
- textencoding
- timezoneindex (time zone index)
- viewmessagesas (html, plain)
- weclomewizardprogress (progress of welcome page)
- GetUser : Returns attributes of the specified user
  
- Return Type : UserInfoResult
- Parameters :
  
- AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
- AuthPassword : Password for the username
- EmailAddress : Account for which return settings
- GetUserAutoResponseInfo : Returns the forwarding info of the specified user
  
- Return Type : UserAutoResponseResult
- Parameters :
  
- AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
- AuthPassword : Password for the username

- EmailAddress : Address for which return autresponder info
- GetUserForwardingInfo : Returns the forwarding info of the specified user
- Return Type : UserForwardingInfoResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
- AuthPassword : Password for the username
- EmailAddress : Address for which return forwarding info
- GetUserGroup : Gets a user group in the specified domain with the given ID
- Return Type : UserGroupInfoResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
- AuthPassword : Password for the username
- DomainName : Domain from which to get the user group
- UserGroupID : Unique ID of the user group
- GetUserGroupsByDomain : Get all user groups in the specified domain
- Return Type : UserGroupsResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
- AuthPassword : Password for the username
- DomainName : Domain from which to get user groups
- GetUserGroupsByUser : Get all user groups in the specified domain containing the given user
- Return Type : UserGroupsResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
- AuthPassword : Password for the username
- DomainName : Domain from which to return user groups
- UserName : Return groups which contain this username
- IncludeUserNames : Return the full user list for each group
- GetUserStats : Returns statistics of the specified user for the specified time period



- Return Type : GenericResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - EmailAddress : Address for which treturn stats
  - Start : Start of the statistics range
  - End : End of the statistics range
  - GetUsers : Returns attributes of each user in the specified domain
- Return Type : UserInfoListResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - DomainName : Domain for which treturn the user list
  - GetUserQuotas : Returns current and max disk space for each user of a domain
- Return Type : QuotaInforListResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - DomainName : Domain for which treturn the user list
  - ListRSSFeeds : Returns the list of RSS feeds for the specified account
- Return Type : RSSFeedListResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges tchange an account other than itself
  - AuthPassword : Password
  - EmailAddress : Email address of the account tlist RSS feeds
  - LoginValidated : Returns a LoginResult object with the LoginValidated field set tTrue if the specified username matches the specified password
- Return Type : LoginResult
- Parameters :

- Username : Username
- Password : Password
- RemoveUserGroup : Deletes a user group from the specified domain with the given ID
- Return Type : GenericResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - DomainName : Domain from which tdelete the user group
  - UserGroupID : Unique ID of the user group tremove
  - SetRequestedUserSettings : Updates the specified user's settings
- Return Type : GenericResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - EmailAddress : Account for which tset settings
  - newSettings : Xxxx
    - autocleanoverrideactive (Should user override domain settings)
    - autopopupreminders (Automatically popup reminders window)
    - autorespondondirectmailonly (Ignore emails sent through aliases)
    - autosavedrafttime (Save every x milliseconds)
    - autotrusteripients (Automatically add addresses ttrusted senders)
    - composefont
    - composefontsize
    - composmethod (html, plain)
    - composerows (obsolete)
    - deleteonforward (delete messages after autforwarding)
    - deleteoption (MoveToDeleteFolder, AutoPurge, MarkDeleted, MarkDeletedAndHide)
    - dictionarylanguage (en-US, etc)
    - disablegreylsting
    - displayname (display name of user)
    - embedreplies (attach forwards)
    - enableanimations (obsolete)

- enablesounds (play sounds in the webmail interface)
- forwardaddress (address to forward to)
- forwardas (attachment, normal, plain)
- fullname
- headerdisplay (basic, full)
- hidefromgal
- isdomainadmin
- isenabled
- lockpassword
- maxsize (Max mailbox size in MB)
- messagerefreshrateinseconds (Autorefresh inbox)
- messagesperpage (Rows per grid)
- password
- passwordlocked
- plusaddressingenabled
- plusaddressingfolder
- popupmessageinwindow (Read messages in new window)
- previewautopreview (Automatically preview messages)
- previewautomarkasread (Automatically mark messages as read after 5 seconds)
- previewusepreview (Use preview pane)
- replymessageindicator (Plain text indicator, > by default)
- replytoaddress
- requestreceipts (Automatically request read receipts on new messages)
- savecopyassent (Use Sent Items folder)
- seenwelcome (Has the user seen the welcome page)
- servicelevelmap (The enabled services for a user. This field is a bitmap composed of 1=POP, 2=IMAP, 4=INCOMING SMTP, 8=OUTGOING SMTP, 16=WEBMAIL)
- showsusc (Show synchronization center on login)
- signature
- skin
- sortby (sorting of messages page)
- sortdescending (sort in reverse order)
- spamcheckoverrideactive (Should user override spam check settings from domain)
- spamforwardoption (obsolete)
- startuppge (today, messages)
- syncpanels (not used)
- textencoding

- timezoneindex (time zone index)
- viewmessagesas (html, plain)
- weclomewizardprogress (progress of welcome page)
- ToggleActiveSync : Enables or disables ActiveSync for the specified user
- Return Type : GenericResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privledges
- AuthPassword : Password for the username
- EmailAddress : Mailbox for which ttoggle ActiveSync access
- Enabled : The new status for ActiveSync access for this mailbox
- UpdateUser : Updates the specified user's settings
- Return Type : GenericResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
- AuthPassword : Password for the username
- DomainName : Domain for which tadd the user
- FirstName : First name
- LastName : Last name
- IsDomainAdmin : True if the user should be a domain admin
- UpdateUser2 : Updates the specified user's settings
- Return Type : GenericResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
- AuthPassword : Password for the username
- DomainName : Domain for which tadd the user
- FirstName : First name
- LastName : Last name
- IsDomainAdmin : True if the user should be a domain admin
- MaxMailboxSize : Maximum size for the user mailbox (in MB)
- UpdateUserAutoResponseInfo : Updates the specified user's autresponse settings

- Return Type : GenericResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - EmailAddress : Account tupdate
  - Enable : Should the auto-responder be enabled
  - Subject : Subject of the auto-response
  - Body : Body of the auto-response
  - UpdateUserForwardingInfo : updates the specified user's forwarding settings
- Return Type : GenericResult
- Parameters :
  - AuthUserName : User name used to perform this function. Requires system administrator or domain administrator privileges
  - AuthPassword : Password for the username
  - EmailAddress : Account tupdate
  - DeleteOnForward : Should the account delete emails it forward
  - Subject : Subject of the auto-response
  - ForwardingAddress : twich Address forwards should be sent

the following return types are used:

- GenericResults : Generic result information for a Web service request.
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- StatInfoResult : Returned by GetUserStats
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- MessagesReceived : Total messages received in time frame
- MessagesSent : Total messages sent in time frame
- BytesReceived : Total bytes received in time frame
- BytesSent : Total bytes sent in time frame

- BytesSize :Disk space usage by user
- LoginResult :Returned by the LoginValidated function
- LoginValidated :True or false depending on the success of the Web service
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- SettingsRequestResult :
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- SettingsValues :Array of key/value pairs in the form of key=value
- UserInfoResult :Returned by the GetUser function
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- UserInfo :Struct containing user information
- UserForwardingInfoResult : Returned by GetUserAutoResponseInfo
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- DeleteOnForward :Should the message be deleted after forwarding
- ForwardingAddress :Address tforward messages to
- UserAutoResponseResult :Returned by GetUserAutoResponseInfo
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- Enabled :Is the autresponder enabled
- Subject :Subject of the message
- Body :Body of the message
- UserGroupInfoResult :Returned By GetUserGroup
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- UserGroup :Struct containing user group info
- UserGroupsResult :Returned by GetUserGroupsByDomain

- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- UserGroups : An array of structs containing user group info

## Server Administration Services/svcServerAdmin.asmx

The ServerAdmin Web service handles all functionality dealing with the mail server. The following functions are available in this Web service:

- GetEdition : Returns the current operational licensing mode
- Return Type : EditionResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- GetRequestedSystemSettings : Returns the requested system settings
- Return Type : RequestSettingsResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- reqSettings : An array of settings to return. Valid keys are:
  - adminpassword (system admin password)
  - adminusername (system admin username)
  - allowrelay (noone, localusers, localhosts, anyone)
  - deletedomainstatsafter (delete domain stats after x months)
  - deletedomainstatsafterenabled (enable deletion of domain stats)
  - deleteserverstatsafter (delete server stats after x months)
  - deleteserverstatsafterenabled (enable deletion of server stats)
  - deleteuserstatsafter (delete user stats after x months)
  - deleteuserstatsafterenabled (enable deletion of user stats)
  - deliverydelay (time to wait before delivering a message)
  - deliverythreads (number of simultaneous outbound connections)
  - disablereceivedappend (disable appending received header to authenticated SMTP sessions)
  - enablelite mode (enable lite mode if applicable)

- enforcesmtpauthlocaldelivery (require SMTP auth for local deliveries)
- executecommandline (command line texecute on every spool message)
- executecommandlineenabled (enable command line processing)
- executecommandlinetimeout (terminate command line after x seconds)
- greylistingblockperiod (period of the initial blocking when greylisted in minutes)
- greylistingpassperiod (period in which the sender's mail server has tretry sending the message)
  
- greylistingrecordexpiration (whgreylisting applies to)
- greylistingfilteroption (enable greylisting)
- greylistingenabled (allow users tdisable greylisting)
- greylistingenableuserstooverride (greylists all messages from IP addresses where the country is not known)
- greylistifthecountryfortheipaddressisunknown (minimum password length requirement)
- minimumpasswordlength (enforce minimum password length setting)
- minimumpasswordlengthenabled (password requires at least one number)
- passwordrequiresnumber (password requires at least one capital letter)
- passwordrequirescapitalletter (password requires at least one lowercase letter)
- passwordrequireslowercaseletter (password requires at least one symbol such as !, @, #, etc.)
- passwordrequiresymbol (disables password strength requirements for users whhave passwords already setup)
- passwordmustnotmatchusername (enables automatic password retrieval)
- passwordstrengthdisabledforexistingpasswords (number of attempts SmarterMail will make after a DNS error occurs)
- passwordretrievalenabled
- attemptsbeforebouncingduetodnserrors (password must not match the username twchic it applies)
- indexingmaxthreads (maximum number of threads the indexing engine is allowed tuse)
- indexingsegmentsbeforeoptimizing (number of index segment files that are allowed tbe created before the index is optimized)
- indexingitemsbeforegarbagecollection (number of indexed items before a forced garbage collection occurs)
- indexingitemsperpass (number of items tindex for a user before lowering their queue priority)
- indexingsecondsinqueuebeforeindex (number of seconds a user must wait in queue before they are indexed)
- indexingitemsdeletedbeforeoptimizing (number of indexed items deleted before optimizing the index)
- popbanner (the banner sent tconnecting POP clients)



- `imapbanner` (the banner sent tconnecting IMAP clients)
- `smtpbanner` (the banner sent tconnecting SMTP clients)
- `disableauthlogin` (disables the SMTP AUTH LOGIN command)
- `disableappendingofreceivedlineforauthenticatedmessages` (disables appending of the received line when an incoming message is authenticated)
- `dnscachingenabled` (enables dns caching)
- `usetlsifsupportedbyremoteserver` (enables SmarterMail tattempt tuse TLS for outgoing messages if the remote server supports it)
- `filestoragemaxfilesizeenabled` (enables `filestoragemaxfilesize`)
- `filestoragemaxfilesize` (the maximum file size allowed tbe stored in file storage)
- `logpath` (the path twhich SmarterMail stores log files)
- `deletelogfilesafterenabled` (enables `deletelogfilesafter`)
- `deletelogfilesafter` (the period of time in days for which SmarterMail will hold log files)
- `domainscanoverrideautocleansettings` (allows domains tooverride the system level auto-clean rules)
- `userscanautocleaninbox` (allows users tautclean their inbox)
- `footerenabledforalloutgoingmessages` (enables a footer for all outgoing messages)
- `fotterappliestomailinglists` (enables the footer tbe applied tmailing list messages)
- `footerallowdomainoverride` (allows the domain tooverride footers)
- `footertext` (host name of the server)
- `hostname` (disconnect if ncommands for x minutes)
- `imapcommandtimeout` (enable IMAP idle)
- `imapidleenabled` (disconnect if client issues x bad commands)
- `imapmaxbadcommands` (maximum concurrent connections)
- `imapmaxconnections` (IMAP retrieval download path)
- `imapretrievaldownloadpath` (IMAP retrieval interval)
- `imapretrievalinterval` (IMAP retrieval threads)
- `imapretrievalthreads` (disconnect if ncommands for x minutes)
- `ldapcommandtimeout` (disconnect if session exceeds x minutes)
- `ldapsessiontimeout` (redirect URL when logging out)
- `logouturl` (enable redirect on logout)
- `logouturlenabled` (allow domains tooverride logout URL)
- `logouturloverrideenabled` (IP tuse for outbound deliveries)
- `outboundip` (`domainsip`, `primaryip`, `specifiedip`)
- `outboundipoption` (disconnect if ncommands for x minutes)
- `popcommandtimeout` (disconnect if client issues x bad commands)
- `popmaxbadcommands` (maximum concurrent connections)

- popmaxconnections (location of temporary POP retrieval files)
  - popretrievaldownloadpath (retrieve POP every x minutes)
  - popretrievalinterval (maximum POP retrieval sessions)
  - popretrievalthreads (postmaster mailbox)
  - postmastermailbox (primary dns server, leave blank for automatic)
  - primarydns (secondary dns server, leave blank for automatic)
  - secondarydns (bypass relay settings when authenticated)
  - smtpauthbypassrelay (disconnect if client issues x bad commands)
  - smtpcommandtimeout (enable EXPN command)
  - smtpexpn (disconnect if client issues x bad commands)
  - smtpmaxbadcommands (disconnect if client issues x bad recipients)
  - smtpmaxbadrecipients (maximum concurrent connections)
  - smtpmaxconnections (maximum hop count)
  - smtpmaxhopcount (maximum message size in MB)
  - smtpmaxmessagesize (disconnect if session exceeds x minutes)
  - smtpsessiontimeout (enable session timeout)
  - smtpsessiontimeoutenabled (enable VRFY command)
  - smtpvrfy (Maximum concurrent spam checks)
  - spamcheckthreads (path tthe spool)
  - spoolpath (port used for submission port)
  - submissionport (enable submission port)
  - submissionportenabled (IP used for submission port)
  - submissionportip
  - subspools (number of subspools)
  - timebetweenattempts (comma separated list of retry times)
  - SetRequestedSystemSettings :Sets the requested system settings
- 
- Return Type :GenericResult
  - Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
  - AuthPassword :Password for the username
  - newSettings :An array of settings tchange in the form of “key=value”
- adminpassword (system admin password)
  - adminusername (system admin username)
  - allowrelay (noone, localusers, localhosts, anyone)
  - deletedomainstatsafter (delete domain stats after x months)

- `deletedomainstatsafterenabled` (enable deletion of domain stats)
- `deleteserverstatsafter` (delete server stats after x months)
- `deleteserverstatsafterenabled` (enable deletion of server stats)
- `deleteuserstatsafter` (delete user stats after x months)
- `deleteuserstatsafterenabled` (enable deletion of user stats)
- `deliverydelay` (enable deletion of user stats)
- `deliverythreads` (number of simultaneous outbound connections) sessions)
- `disablereceivedappend` (disable appending received header tauthenticated smtp sessions)
- `enablelitemode` (enable lite mode if applicable)
- `enforcesmtpauthlocaldelivery` (require smtp auth for local deliveries)
- `executecommandline` (command line texecute on every spool message)
- `executecommandlineenabled` (enable command line processing)
- `executecommandlinetimeout` (terminate command line after x seconds)
- `greylistingblockperiod` (period of the initial blocking when greylisted in minutes)
- `greylistingpassperiod` (period in which the sender's mail server has tretry sending the message)
  
- `greylistingrecordexpiration` (period for which a previously greylisted sender is allowed tsend without being greylisted in days)
- `greylistingfilteroption` (whgreylisting applies to)
- `greylistingenabled` (enable greylisting)
- `greylistingenableuserstooverride` (allow users tdisable greylisting)
- `greylistifthecountryfortheipaddressisunknown` (greylists all messages from IP addresses where the country is not known)
- `minimumpasswordlength` (minimum password length requirement)
- `minimumpasswordlengththenabled` (enforce minimum password length setting)
- `passwordrequiresnumber` (password requires at least one number)
- `passwordrequirescapitalletter` (password requires at least one capital letter)
- `passwordrequireslowercaseletter` (password requires at least one lowercase letter)
- `passwordrequiressymbol` (password requires at least one symbol such as !, @, #, etc.)
- `passwordmustnotmatchusername` (password must not match the username twhich it applies)
- `passwordstrengthdisabledforexistingpasswords` (password must not match the username twhich it applies)
- `passwordretrievalenabled` (enables automatic password retrieval)
- `attemptsbeforebouncingduetodnserrors` (number of attempts SmarterMail will make after a DNS error occurs)
- `indexingmaxthreads` (maximum number of threads the indexing engine is allowed tuse)
- `indexingsegmentsbeforeoptimizing` (number of index segment files that are allowed the

created before the index is optimized)

- indexingitemsbeforegarbagecollection (number of index segment files that are allowed to be created before the index is optimized)
- indexingitemsperpass (number of indexed items before a forced garbage collection occurs)
- indexingsecondsinqueuebeforeindex (number of seconds a user must wait in queue before they are indexed)
- indexingitemsdeletedbeforeoptimizing (number of indexed items deleted before optimizing the index)
- popbanner (the banner sent to connecting POP clients)
- imapbanner (the banner sent to connecting IMAP clients)
- smtpbanner (the banner sent to connecting SMTP clients)
- disableauthlogin (disables the SMTP AUTH LOGIN command)
- disableappendingofreceivedlineforauthenticatedmessages (disables appending of the received line when an incoming message is authenticated)
- dnscachingenabled (enables dns caching)
- usetlsifsupportedbyremoteserver (enables SmarterMail to attempt to use TLS for outgoing messages if the remote server supports it)
- filestoragemaxfilesizeenabled (enables filestoragemaxfilesize)
- filestoragemaxfilesize (the maximum file size allowed to be stored in file storage)
- logpath (the path to which SmarterMail stores log files)
- deletelogfilesafterenabled (enables deletelogfilesafter)
- deletelogfilesafter (the period of time in days for which SmarterMail will hold log files)
- domainscanoverrideautocleansettings (allows domains to override the system level auto-clean rules)
- userscanautocleaninbox (allows users to auto-clean their inbox)
- footerenabledforalloutgoingmessages (enables a footer for all outgoing messages)
- footerappliedtomailinglists (enables the footer to be applied to mailing list messages)
- footerallowdomainoverride (allows the domain to override footers)
- footertext (the text of the footer (HTML allowed))
- hostname (host name of the server)
- imapcommandtimeout (disconnect if n commands for x minutes)
- imapidleenabled (enable imap idle)
- imapmaxbadcommands (disconnect if client issues x bad commands)
- imapmaxconnections (maximum concurrent connections)
- imapretrievaldownloadpath (IMAP retrieval download path)
- imapretrievalinterval (IMAP retrieval interval)
- imapretrievalthreads (IMAP retrieval threads)

- ldapcommandtimeout (disconnect if ncommands for x minutes)
- ldapsessiontimeout (disconnect if session exceeds x minutes)
- logouturl (redirect URL when logging out)
- logouturlenabled (enable redirect on logout)
- logouturloverrideenabled (allow domains to override logout URL)
- outboundip (IP tuse for outbound deliveries)
- outboundipoption (domainsip, primaryip, specifiedip)
- popcommandtimeout (disconnect if ncommands for x minutes)
- popmaxbadcommands (disconnect if client issues x bad commands)
- popmaxconnections (maximum concurrent connections)
- popretrievaldownloadpath (location of temporary POP retrieval files)
- popretrievalinterval (retrieve POP every x minutes)
- popretrievalthreads (maximum POP retrieval sessions)
- postmastermailbox (postmaster mailbox)
- primarydns (primary dns server, leave blank for automatic)
- secondarydns (secondary dns server, leave blank for automatic)
- smtpauthbypassrelay (bypass relay settings when authenticated)
- smtpcommandtimeout (disconnect if client issues x bad commands)
- smtpexpn (enable EXPN command)
- smtpmaxbadcommands (disconnect if client issues x bad commands)
- smtpmaxbadrecipients (disconnect if client issues x bad recipients)
- smtpmaxconnections (maximum concurrent connections)
- smtpmaxhopcount (maximum hop count)
- smtpmaxmessagesize (maximum message size in MB)
- smtpsessiontimeout (disconnect if session exceeds x minutes)
- smtpsessiontimeoutenabled (enable session timeout)
- smtpvrfy (enable VRFY command)
- spamcheckthreads (Maximum concurrent spam checks)
- spoolpath (path tthe spool)
- submissionport (port used for submission port)
- submissionportenabled (enable submission port)
- submissionportip (IP used for submission port)
- subspools (number of subspools)
- timebetweenattempts (comma separated list of retry times)
- RequestStatus Requests information about the current state of the server
- Return Type :RequestStatusResult
- Parameters :

- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- reqStats :An array of keys for requested statistic items. The valid keys for this function are:
  - smtp\_isrunning (True if the SMTP service is running)
  - smtp\_threadcount (Number of SMTP connections)
  - pop\_isrunning (True if the POP service is running)
  - pop\_threadcount (Number of POP connections)
  - imap\_isrunning (True if the IMAP service is running)
  - imap\_threadcount (Number of IMAP connections)
  - spool\_isrunning (True if the spool is running)
  - spool\_threadcount (Number of delivery threads)
  - spool\_messagecount (Number of messages in the spool)
  - server\_uptime (How long the service has been running, in seconds)
- DeleteServerPort :Deletes a port from the server
- Return Type :GenericResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- PortID :The identifier of the port to be deleted. This is obtained through the function ListServerPorts
- ListServerPorts :Lists all ports currently setup on the server
- Return Type :ServerPortListResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- AddServerPort :Adds a port to the server
- Return Type :AddServerPortResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges

- AuthPassword Password for the username
- Protocol The protocol assigned to this port. Valid values include POP, SMTP, IMAP, LDAP, or SubmissionPort
- CertificatePath The path to the certificate on the server if this is an SSL or TLS port. This parameter is required if the Encryption parameter is set to anything other than an empty string
- Encryption The encryption method to use for the port. Valid values include SSL or TLS. This
- Name A descriptive name for the port
- Port The port number for this port
- Description A description of the port
- GetSMTPBlockedSenders :Returns a list of currently blocked SMTP senders
- Return Type :SMTPBlockedSenderListResult
- Parameters :
- AuthUserName : User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- AddDOSAbuseDetectionRule : Adds a denial of service (DOS) abuse detection rule to the server
- Return Type :GenericResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- Service :The service to which this rule applies. Valid options include SMTP, IMAP, and POP
- TimeFrame :The timeframe in minutes in which the rule can be triggered
- ConnectionsBeforeBlock :The number of connections the server will allow before blocking access
- TimeToBlock :The block period in minutes for which the server will block the offender
- Description :A brief description of the rule for display purposes
- AddHarvestingAbuseDetectionRule :Adds a harvesting abuse detection rule to the server
- Return Type :GenericResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username

- TimeFrame :The timeframe in minutes in which the rule can be triggered
- BadSessionsBeforeBlock :The number of bad SMTP sessions tallow before blocking the offender
- TimeToBlock :The time in minutes for which tblock
- Description :A brief description of the rule for display purposes
- AddInternalSpammerNotificationAbuseDetectionRule : Adds an internal spammer notification abuse detection rule tthe server
  
- Return Type :GenericResult
- Paramaters :
  
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- TimeFrame :The timeframe in minutes in which the rule can be triggered
- MessagesBeforeNotify :The number of messages sent by the offender before the rule is triggered
- EmailAddressToNotify :The email address tnotify when the rule is triggered
- Description :A brief description of the rule for display purposes
- DeleteAbuseDetectionRule : Deletes an abuse detection rule
  
- Return Type : GenericResult
- Parameters :
  
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- ID :The unique identifier of the abuse detection rules
- GetDOSAbuseDetectionRules : Returns the currently setup DOS detection rules on the server
  
- Return Type :DOSAbuseDetectionRulesListResult
- Parameters :
  
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- GetHarvestingAbuseDetectionRules :Returns the currently setup harvesting detection rules on the server
  
- Return Type :HarvestingAbuseDetectionRulesListResult
- Parameters :



- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- GetInternalSpammerNotificationAbuseDetectionRules : Returns the currently setup internal spammer notifications on the server
- Return Type :InternalSpammerNotificationAbuseDetectionRulesListResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- AddSMTPBlockedSender : Adds a new SMTP blocked sender
- Return Type : GenericResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- BlockedSender :The email address of the blocked sender
- Description :A brief description for display purposes
- DeleteSpamAssassinServer :Deletes a remote SpamAssassin server
- Return Type :GenericResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword : Password for the username
- ServerName :The name of the server you wish tdelete
- AddSpamAssassinServer :Adds a remote SpamAssassin server
- Return Type :GenericResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- ServerName :A descriptive name for the server
- IPAddress :The IP address of the server

- ServerPort :The port number that the server is listening on
- ListSpamAssassinServers :Gets a list of all currently configured remote SpamAssassin servers
- Return Type :SpamAssassinServerListResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- ListGreylistingFilters :Gets a list of all currently configured greylisting filters
- Return Type :GreylistingFilterListResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- ListPortsAssignedToIP :Gets a list of ports currently assigned and listening on an IP
- Return Type :ServerPortListResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- IPAddress :The IP which has the ports
- RemovePortFromIP : Removes a port assigned to an IP address
- Return Type :GenericResult
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- PortID :The unique identifier of the port to remove
- IPAddress :The IP address to remove the port from
- AssignPortToIP : Assigns a port to an IP address
- Return Type :GenericResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges

- AuthPassword :Password for the username
- PortID :The unique identifier of the port tassign tthe IP
- IPAddress :The IP address tassign the port to
- ListGateways : Gets a list of all gateways on a server
  
- Return Type :GatewayListResult
- Parameters :
  
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- GetGlobalTrustedSenders :Gets a list of all current globally trusted senders
  
- Return Type :TrustedSenderListResult
- Parameters :
  
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- AddGlobalTrustedSender : Adds a new globally trusted sender
  
- Return Type :GenericResult
- Parameters :
  
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- AddressOrDomain :The email address or domain tadd tthe global trusted senders list
- DeleteGlobalTrustedSender :Deletes a globally trusted sender
  
- Return Type : GenericResult
- Parameters :
  
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- AddressOrDomain :The address or domain tremove from the global trusted senders list
- DeleteGreylistingFilter : Removes a greylisting filter
  
- Return Type :GenericResult
- Parameters :

- AuthUserName :User name used to perform this function. Requires system administrator privileges
  - AuthPassword : Password for the username
  - FilterType :The filter type of the greylisting filter to be removed
  - IPRangeStart : (optional) The start of the IP range used by the filter to be removed
  - IPRangeEnd :(optional) The end of the IP range used by the filter to be removed
  - IPAddress :(optional) The IP address of the filter to be removed
  - CountryCode : (optional) The country code of the filter to be removed
  - GetWhitelistEntries :Gets the currently configured whitelist entries
- Return Type :WhitelistListResult
  - Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
  - AuthPassword :Password for the username
  - GetBlacklistEntries :Gets the currently configured blacklist entries
- Return Type :BlacklistListResult
  - Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
  - AuthPassword :Password for the username
  - SetBlacklistEntry :Adds a new blacklist entry or edits an existing blacklist entry
- Return Type :GenericResult
  - Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
  - AuthPassword :Password for the username
  - IPAddress :The IP address to be blacklisted
  - IPRangeStart :The start of the IP range to be blacklisted
  - IPRangeEnd :The end of the IP range to be blacklisted
  - BlacklistSMTP :Whether or not to blacklist for SMTP
  - BlacklistPOP :Whether or not to blacklist for POP
  - BlacklistIMAP :Whether or not to blacklist for IMAP
  - Description :A brief description of the rule for display purposes
  - SetWhitelistEntry :Adds a new whitelist entry or edits an existing whitelist entry

- Return Type : GenericResult
- Parameters :
  - AuthUserName :User name used to perform this function. Requires system administrator privileges
  - AuthPassword :Password for the username
  - IPAddress :The IP address tbe whitelisted
  - IPRangeStart :The start of the IP range tbe whitelisted
  - IPRangeEnd :The end of the IP range tbe whitelisted
  - BlacklistSMTP :Whether or not twhitelist for SMTP
  - BlacklistPOP :Whether or not twhitelist for POP
  - BlacklistIMAP :Wheter or not twhitelistfor IMAP
  - Description :A brief description of the rule for display purposes
  - AddGreylistingFilter :Adds a new greylisting filter
- Return Type :GenericResult
- Parameters :
  - AuthUserName :User name used to perform this function. Requires system administrator privileges
  - AuthPassword :Password for the username
  - FilterType :The filter type tadd. Valid values include: Country, IPAddress, or IPRange
  - IPRangeStart :The start of the IP range tfilter
  - IPRangeEnd :The end of the IP range tfilter
  - IPAddress :The IP address tfilter
  - CountryCode :The country code tfilter on
  - Description :A brief description of the filter for display purposes
  - AddSmtpAuthenticationBypass :Adds a new SMTP authentication bypass rule
- Return Type :GenericResult
- Parameters :
  - AuthUserName :User name used to perform this function. Requires system administrator privileges
  - AuthPassword :Password for the username
  - IPAddress :The IP address allowed tby pass SMTP authentication
  - IPRangeStart :The start of the IP range allowed tby pass SMTP authentication
  - IPRangeEnd :The end of the IP range allowed tby pass SMTP authentication

- Description :A brief description of the SMTP authentication bypass rule
- DeleteSmtpAuthenticationBypass :Deletes an SMTP authentication bypass rule
- Return Type :GenericResult
- Parameters :
  - AuthUserName :User name used to perform this function. Requires system administrator privileges
  - AuthPassword :Password for the username
  - IPAddress :The IP address of the rule tbe removed
  - IPRangeStart :The start of the IP range of the rule tbe removed
  - IPRangeEnd :The end of the IP range of the rule tbe removed
  - GetSmtpAuthenticationBypasses :Gets a list of the currently configured SMTP authentication bypass rules
- Return Type :SMTPAuthBypassListResult
- Parameters :
  - AuthUserName :User name used to perform this function. Requires system administrator privileges
  - AuthPassword :Password for the username
  - ListSystemAdmins :Lists the currently configured system admins on the server
- Return Type :SystemAdminListResult
- Parameters :
  - AuthUserName :User name used to perform this function. Requires system administrator privileges
  - AuthPassword :Password for the username
  - SetSystemAdminPassword :Sets the password of a configured system admin
- Return Type :GenericResult
- Parameters :
  - AuthUserName :User name used to perform this function. Requires system administrator privileges
  - AuthPassword :Password for the username
  - SystemAdminUsername :The username of the system admin tchange
  - NewPassword :The new password tset for the system administrator
  - DeleteSystemAdmin :Removes a system administrator from the server

- Return Type :GenericResult
- Parameters :
  - AuthUserName :User name used to perform this function. Requires system administrator privileges
  - AuthPassword :Password for the username
  - SystemAdminUsername :The username of the system admin tchange
  - AddSystemAdmin :Adds a new system administrator
- Return Type :GenericResult
- Parameters :
  - AuthUserName :User name used to perform this function. Requires system administrator privileges
  - AuthPassword :Password for the username
  - NewAdminUsername :The username of the new system admin
  - NewAdminPassword :The password of the new system admin
  - NewAdminDescription :A brief description of the system admin account for display purposes
  - AddIPRestrictionToSystemAdmin : Adds an IP address or IP range restriction on a system admin login
- Return Type :GenericResult
- Parameters :
  - AuthUserName :User name used to perform this function. Requires system administrator privileges
  - AuthPassword :Password for the username
  - AdminUsername :The username of the admin tadd the IP restriction to
  - IPAddressOrRange :The IP address or IP range (format: x.x.x.x-y.y.y.y) to allow access from
  - RestrictionDescription :A brief description of the restriction for display purposes
  - RemoveIPRestrictionFromSystemAdmin :Removes an IP address or IP range restriction from a system admin login
- Return Type :GenericResult
- Parameters :
  - AuthUserName :User name used to perform this function. Requires system administrator privileges
  - AuthPassword :Password for the username
  - AdminUsername :The username of the admin tremove the IP restriction from

- IPAddressOrRange :The IP address or IP range (format: x.x.x.x-y.y.y.y) to remove access from
- AddHostname :Adds a hostname tthe server
- Return Type :GenericResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- Hostname :The new hostname tadd tthe server
- IPAddress :The IP address twhich the hostname applies
- DeleteHostname :Deletes a hostname from the server
- Return Type :GenericResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- IPAddress :The IP address twhich the hostname applies
- ListHostnames :Lists all hostnames currently configured on the server
- Return Type :HostnameListResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- AddFolderAutocleanRule :Adds a server level folder autclean rule tthe server
- Return Type :GenericResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- Folder :The folder tautclean
- EnableRule :Should the rule be enabled
- Type :The rule type. Valid values include: Size and Date
- SizeBeforeAutoClean :For size rules, the size which a folder must reach before being



autcleaned

- SizeAfterClean :For size rules, the size which a folder will be trimmed to after it's cleaned
- MailAgeInDays :For date rules, the age at which email gets deleted
- DeleteFolderAutoCleanRule :Removes a server level folder autclean rule from the server
- Return Type :GenericResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- ID :The unique identifier of the rule tbe deleted
- ListFolderAutoCleanRules :Gets a list of all folder autclean rules currently setup on the server
- Return Type :FolderAutoCleanRuleListResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- AddForwardingBlacklistEntry :dds a forwarding blacklist entry tthe server
- Retrun Type :GenericResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- DomainName :The domain tadd tthe forwarding blacklist
- DeleteForwardingBlacklistEntry :Removes a forwarding blacklist entry from the server
- Return Type :GenericResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- DomainName :The domain tremove from the forwarding blacklist
- ListForwardingBlacklistEntries :Gets all current forwarding blacklist entries
- Return Type :ForwardingBlacklistRuleResult
- Parameters :

- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- GetSpoolMessageCount :Returns the number of messages in the spool.
  
- Return Type :MessageCountResult
- Parameters :
  
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- ListGateways :Returns information about the gateways SmarterMail has configured
  
- Return Type :GatewayListResult
- Parameters :
  
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- GetGateway :Returns information about a particular gateway
  
- Return Type :GatewayResult
- Parameters :
  
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- Guid Unique ID for the gateway
- AddGateway :Adds a non-SmarterMail gateway tSmarterMail
  
- Return Type :GenericResult
- Parameters :
  
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- Address :Address of the gateway server
- Enabled :Should SmarterMail use this gateway
- AddSmarterMailGateway :Adds a SmarterMail gateway tSmarterMail

- Return Type :GenericResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- Address :Address of the gateway server
- Enabled :Should SmarterMail use this gateway
- smURL :Url tthe SmarterMail Web interface
- smUserName :Admin username tthe SmarterMail gateway
- smPassword :Password tthe SmarterMail gateway
- RemoveGateway :Deletes a gateway from SmarterMail
- Return Type :GenericResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- Guid :Unique ID of the gateway tremove
- UpdateGateway :Updates the settings for a specific gateway
- Return Type :GenericResult
- Parameters :
- AuthUserName :User name used to perform this function. Requires system administrator privileges
- AuthPassword :Password for the username
- AuthPassword :Address of the gateway server
- Enabled :Should SmarterMail use this gateway
- smURL :Url tthe SmarterMail Web interface
- smUserName :Admin username tthe SmarterMail gateway
- smPassword :Password tthe SmarterMail gateway

The following return types are used:

- GenericResult :Generic result information for a Web service request
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false

- Message :Error message detailing why the result is false
- MessageCountResult :Returned by the GetSpoolMessageCount function
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- messageCount :Number of messages in the spool
- GatewayListResult :Returned by ListGateways
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- Gateways :An array of GatewayResult structs
- RequestStatusResult :
- Result : True or false depending on the success of the Web service request.
- ResultCode :Specific failure code if the result is false.
- Message : Error message detailing why the result is false.
- KeyValuePairs :An array of values for the requested keys, in the form of key=value
- GatewayResult :Returned by GetGateway
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- Guid :Unique ID of the gateway
- gatewayAddress :Address of the gateway
- enabled :Is this gateway enabled
- isSmarterMailServer :Is this a SmarterMail gateway
- smUrl :Url tthe SmarterMail Web interface of the gateway
- smUserName :Username for the SmarterMail Gateway
- smPassword :Password for the SmarterMail Gateway
- ForwardingBlacklistRuleResult
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- BlacklistedDomains :An array of strings representing the blacklisted domains
- FolderAutoCleanRuleListResult

- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- Rules : An array of FolderAutoCleanRuleResult
- FolderAutoCleanruleResult
  - Enabled : Is the rule enabled
  - ID : A unique identifier for the rule
  - SizeBeforeCleanInMB : The size a mailbox must get tbefore this rule is run
  - SizeBeforeCleanInMB : The size a mailbox will be reduced tafter this rule is run
  - MailAgeInDays : The number of days of mail that will be kept in the folder
  - Type : The type of the rule (Date, or Size)
  - HostNameListResult
    - Result : True or false depending on the success of the Web service request
    - ResultCode : Specific failure code if the result is false
    - Message : Error message detailing why the result is false
    - Hostnames : An array of HostnameResult
    - HostnameResult
      - IPAddress : The IP twhich the hostname applies
      - Hostname : The hostname string
      - SystemAdminListResult
        - Result : True or false depending on the success of the Web service request
        - ResultCode : Specific failure code if the result is false
        - Message : Error message detailing why the result is false
        - Admins : An array of SystemAdminResult
        - SystemAdminResult
          - ID : A unique identifier for a system admin
          - Username : The username of the system admin
          - IsPrimaryAdmin : True or false indicating whether the admin is the primary server admin
          - RestrictedByIp : True or false indicating whether the login is restricted to an IP or IP range
          - DateCreated : The date on which the admin was created
          - Description : A brief description of the admin account
          - SMTPAuthBypassListResult
            - Result : True or false depending on the success of the Web service request
            - ResultCode : Specific failure code if the result is false

- Message :Error message detailing why the result is false
- Entries :An array of SMTPAuthBypassResult
- SMTPAuthBypassResult
  
- IPAddress :The IP address on the SMTP Authentication Bypass List
- IPRangeStart :The start of the IP range on the SMTP Authentication Bypass List
- IPRangeEnd :The end of the IP range on the SMTP Authentication Bypass List
- Description : A brief
- BlacklistListResult
  
- Result :True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message :Error message detailing why the result is false
- Entries :An Array of BlacklistResult
- BlacklistResult
  
- IPAddress :The IP address on the blacklist
- IPRangeStart :The start of the IP range on the blacklist
- IPRangeEnd :The end of the IP range on the blacklist
- Description :A brief description of the blacklist rule for display purposes
- POPBlacklisted :True or false indicating whether the address(es) are blacklisted for POP
- IMAPBlacklisted :True or false indicating whether the address(es) are blacklisted for IMAP
- SMTPBlacklisted :True or false indicating whether the address(es) are blacklisted for SMTP
- AddServerPortResult :
  
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- NewID :The new unique identifier generated for the port
- ServerPortListResult :
  
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- Ports :An array of ServerPortResult
- ServerPortResult :
  
- ID :A unique identifier for the server port
- Protocol :The protocol twchich the port applies including: POP, SMTP, IMAP, and SubmissionPort

- Encryption :The encryption method applied tthe port: SSL, or TLS
- CertificatePath :The path on the server tthe certificate used for SSL or TLS
- Name :A descriptive name of the port
- Port :The port number of the port
- Description :A brief description of the port for display purposes
- WhitelistListResult :
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- Entries :An array of WhitelistResult
- WhitelistResult :
- IPAddress :The IP address on the whitelist
- IPRangeStart :The start of the IP range on the whitelist
- IPRangeEnd :The end of the IP range on the whitelist
- Description :A brief description of the whitelist rule for display purposes
- POPWhitelisted :True or false indicating whether the address(es) are whitelisted for POP
- IMAPWhitelisted :True or false indicating whether the address(es) are whitelisted for IMAP
- SMTPWhitelisted :True or false indicating whether the address(es) are whitelisted for SMTP
- TrustedSenderListResult :
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- TrustedSenders :An array of strings representing the currently configured global trusted senders
- SMTPBlockedSenderListResult :
- Result :Specific failure code if the result is false
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- SMTPBlockedSenders :An array of SMTPBlockedSenderResult
- SMTPBlockedSenderResult
- BlockedSender :The sender blocked from sending through SMTP
- Description :A brief description of the block for display purposes
- DOSAbuseDetectionRulesListResult

- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- Rules : An array of DOSAbuseDetectionRuleResult
- DOSAbuseDetectionRuleResult
  - Service : The service twchich the rule applies. Valid values include: SMTP, POP, and IMAP
  - Timeframe : The timeframe in which the connections must occur for the rule ttrigger
  - ConnectionsBeforeBlock : The number of connections in the timeframe for the rule ttrigger
  - TimeToBlock : The length of time tblock once the rule is triggered
  - Description : A brief description of the rule for display purposes
  - HarvestingAbuseDetectionRulesListResult
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- Rules : An array of HarvestingAbuseDetectionRuleResult
- HarvestingAbuseDetectionRuleResult
  - Timeframe : The timeframe in which the connections must occur for the rule ttrigger
  - ConnectionsBeforeBlock : The number of bad sessions in the timeframe for the rule ttrigger
  - TimeToBlock : The length of time tblock once the rule is triggered
  - Description : A brief description of the rule for display purposes
  - InternalSpammerNotificationAbuseDetectionRulesListResult
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- Rules : An array of InternalSpammerNotificationAbuseDetectionRuleResult
- InternalSpammerNotificationAbuseDetectionRuleResult
  - Timeframe : The timeframe in which the connections must occur for the rule ttrigger
  - MessagesBeforeNotify : The number of messages in the timeframe for the rule ttrigger
  - EmailAddressToNotify : The email address tnotify once the rule is triggered
  - Description : A brief description of the rule for display purposes
  - SpamAssassinServerListResult
- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false



- Servers :An array of SpamAssassinServerResult
- SpamAssassinServerResult
- Name :A name for the server
- IPAddress :The IP address of the SpamAssassin server
- Port :The port number of the SpamAssassin server
- ConsecutiveFailures :The number of consecutive failures for this SpamAssassin server
- Enabled :True or false indicating whether SmarterMail should use the server for checking
- TotalConnections :The total number of connections made tthe SpamAssassin Server
- GreylistingFilterListResult
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- Filters :An array of GreylistingFilterResult
- GreylistingFilterResult
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- FilterType :The type of greylisting filter. Valid values include: CountryCode, IP, or IPRange
- IPRangeStart :If the type is set tIPRange, the start of the IP range to filter
- IPRangeEnd :If the type is set tIPRange, the end of the IP range tfilter
- IPAddress :If the type is set tIP, the IP address tfilter
- Description :A brief description of the filter for display purposes
- CountryCode :If the type is set tCountryCode, the country code of the country tfilter

## Synchronization Services/svcOutlookAddin.asmx

The Outlook Addin Web service handles all functionality dealing with managing collaboration items.

The following functions are available in this Web service:

- AddCalendarEx :Adds a calendar item ta folder
- Return Type :AddCalendarResult
- Parameters :
- AuthUserName :User name used to perform this function
- AuthPassword :Password for the username
- ownerName :Owner of the specified calendar item

- item :An ExCalendarItem struct containing calendar information
- AddContactEx :Adds a contact item ta folder
  
- Return Type :AddContactResult
- Parameters :
  
- AuthUserName :User name used to perform this function
- AuthPassword :Password for the username
- ownerUserName : Owner of the specified contact
- item :An ExContactItem struct containing contact information
- AddContactEx :Adds a contact item ta folder
  
- Return Type :AddContactResult
- Parameters :
  
- AuthUserName :User name used to perform this function
- AuthPassword :Password for the username
- ownerUserName :Owner of the specified contact
- item :An ExContactItem struct containing contact information
- AddNoteEx :Adds a note item ta folder
  
- Return Type :AddNoteResult
- Parameters :
  
- AuthUserName :User name used to perform this function
- AuthPassword :Password for the username
- ownerName :Owner of the specified note
- item :An ExNoteItem struct containing note information
- AddTaskEx :Adds a task item ta folder
  
- Return Type :AddTaskResult
- Parameters :
  
- AuthUserName :User name used to perform this function
- AuthPassword :Password for the username
- ownerName :Owner of the specified task
- item :An ExTaskItem struct containing task information
- DeleteCalendarEx :Deletes a calendar from a folder
  
- Return Type :GenericResult
- Parameters :

- AuthUserName :User name used to perform this function
  - AuthPassword :Password for the username
  - ownerName :Owner of the calendar item tdelete
  - guid :Unique ID of the calendar item tdelete
  - DeleteContactEx : Deletes a contact from a folder
- Return Type :GenericResult
  - Parameters :
- AuthUserName :User name used to perform this function
  - AuthPassword :Password for the username
  - ownerUsername :Owner of the contact tdelete
  - Guid :Unique ID of the contact tdelete
  - DeleteNoteEx :Deletes a note from a folder.
- Return Type :GenericResult
  - Parameters :
- AuthUserName :User name used to perform this function
  - AuthPassword :Password for the username
  - ownerName :Owner of the note tdelete
  - guid :Unique ID of the note tdelete
  - DeleteTaskEx :Deletes a task from a folder
- Return Type :
  - Parameters :
- AuthUserName :User name used to perform this function
  - AuthPassword :Password for the username
  - ownerName :Owner of the task tdelete
  - guid :Unique ID of the task tdelete
  - FreeBusy :Returns times when a user's calendar is busy
- Return Type :Array of DateTime
  - Parameters :
- Username :Array of usernames to perform lookup. Multiple usernames can be used if a sync tool doesn't know which account tuse. If any username has access, the function will succeed
  - Password :Array of password to perform lookup
  - Lookup :Email address tobtain free/busy information for
  - GetCalendarEx :Returns a calendar based on guid

- Return Type :GetCalendarResult
- Parameters :
  - AuthUserName :User name used to perform this function
  - AuthPassword :Password for the username
  - ownerName :Owner of the calendar item tget
  - guid> :Unique ID of the calendar item tget
  - GetContactEx :Returns a contact based on guid
- Return Type :GetContactResult
- Parameters :
  - AuthUserName :User name used to perform this function
  - AuthPassword :Password for the username
  - ownerUsername :Owner of the contact tget
  - guid :Unique ID of the contact treturn
  - GetItemCount :Returns a count of each type of item.
- Return Type :CountResult
- Parameters :
  - AuthUserName :User name used to perform this function
  - AuthPassword :Password for the username
  - GetNoteEx :Returns a note based on guid
- Return Type :GetNoteResult
- Parameters :
  - AuthUserName :User name used to perform this function
  - AuthPassword :Password for the username
  - ownerName :Owner of the note tget
  - guid :Unique ID of the note tget
  - GetTaskEx :Returns a task based on guid
- Return Type :GetTaskResult
- Parameters :
  - AuthUserName :User name used to perform this function
  - AuthPassword :Password for the username
  - ownerName :Owner of the task tget

- guid :Unique ID of the task tget
- GetUserFolders :Returns the folders twchich the user has access
- Return Type :Folder array
- Parameters :
- AuthUserName :User name used to perform this function
- AuthPassword :Password for the username
- IsLicensed :
- Return Type :
- Parameters :
- AuthUserName :User name used to perform this function
- AuthPassword :Password for the username
- versionNumber :Not used
- Login :Returns true or false depending on if the login and password is correct
- Return Type :GenericResult
- Parameters :
- AuthUserName :User name used to perform this function
- AuthPassword :Password for the username
- RequestCalendarListEx :Returns a list of guids and their hashes corresponding tall calendar events
- Return Type :CalendarListRequest
- Parameters :
- AuthUserName :User name used to perform this function
- AuthPassword :Password for the username
- ownerName :Owner of the calendar tlist
- RequestContactListEx :Returns a list of guids and their hashes corresponding tall contacts
- Return Type :ContactListRequest
- Parameters :
- AuthUserName :User name used to perform this function
- AuthPassword :Password for the username
- ownerUserName :Owner of the contact list tretrieve
- RequestNoteListEx :Returns a list of guids and their hashes corresponding tall notes

- Return Type :NoteListRequest
- Parameters :
  - AuthUserName :User name used to perform this function
  - AuthPassword :Password for the username
  - ownerName :Owner of the note list trequest
  - RequestTaskListEx : Returns a list of guids and their hashes corresponding to all tasks
- Return Type : TaskListRequest
- Parameters :
  - AuthUserName :User name used to perform this function.
  - AuthPassword :Password for the username
  - ownerName :Owner of the task list trequest
  - VersionNumber :Returns the version of SmarterMail
- Return Type :string

The following return types are used:

- GenericResult : Generic result information for a Web service request
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- AddCalendarResult :Returned by AddCalendarEx
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- Hash :Hash of the item after it has been added. This can be used to compare the hash obtained at a later date to see if the item has changed
- AddContactResult :Returned by AddContactEx
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- Hash :Hash of the item after it has been added. This can be used to compare the hash obtained at a later date to see if the item has changed
- AddNoteResult :Returned by AddNoteEx

- Result : True or false depending on the success of the Web service request
  - ResultCode : Specific failure code if the result is false
  - Message : Error message detailing why the result is false
  - Hash : Hash of the item after it has been added. This can be used to compare the hash obtained at a later date to see if the item has changed
  - AddTaskResult : Returned by AddTaskEx
- 
- Result : True or false depending on the success of the Web service request
  - ResultCode : Specific failure code if the result is false
  - Message : Error message detailing why the result is false
  - Hash : Hash of the item after it has been added. This can be used to compare the hash obtained at a later date to see if the item has changed
  - CalendarListRequest : Returned by RequestCalendarListEx
- 
- Result : True or false depending on the success of the Web service request
  - ResultCode : Specific failure code if the result is false
  - Message : Error message detailing why the result is false
  - List : An array of CalendarMetaInfstructs. These structs contain Guid and Hash properties for each item
  - ContactListRequest : Returned by RequestContactListEx
- 
- Result : True or false depending on the success of the Web service request
  - ResultCode : Specific failure code if the result is false
  - Message : Error message detailing why the result is false
  - List : An array of ContactMetaInfstructs. These structs contain Guid and Hash properties for each item
  - NoteListRequest : Returned by RequestNoteListEx
- 
- Result : True or false depending on the success of the Web service request
  - ResultCode : Specific failure code if the result is false
  - Message : Error message detailing why the result is false
  - List : An array of NoteMetaInfstructs. These structs contain Guid and Hash properties for each item
  - TaskListRequest : Returned by RequestTaskListEx
- 
- Result : True or false depending on the success of the Web service request
  - ResultCode : Specific failure code if the result is false
  - Message : Error message detailing why the result is false
  - List : An array of TaskMetaInfstructs. These structs contain Guid and Hash properties for each

item

- CountResult :Returned by GetItemCount
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- CalendarCount :Number of calendar items in the list
- ContactCount :Number of contacts in the list
- TaskCount :Number of tasks in the list
- Folder :Returned by GetUserFolders
- Name :Name of the folder
- OwnerName :Owner of the folder
- ItemType :Type of folder (Appointment, Contact, Task, Note)
- ReadOnly :True if the folder is read only
- GetCalendarResult :Returned by GetCalendarEx
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- ExCalendar :An ExCalendarItem struct containing information about the item
- GetContactResult :Returned by GetContactEx
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- ExContact :An ExContactItem struct containing information about the item
- GetNoteResult :Returned by GetNoteEx
- Result :True or false depending on the success of the Web service request.
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- ExNote :An ExNoteItem struct containing information about the item
- GetTaskResult :Returned by GetTaskEx
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- ExTask :An ExTaskItem struct containing information about the item
- LicenseResult :Returned by IsLicensed



- Result : True or false depending on the success of the Web service request
- ResultCode : Specific failure code if the result is false
- Message : Error message detailing why the result is false
- Trial : Obsolete, always false
- Expiration : Obsolete
- UserMessage : Obsolete

Additional information on how read and write ExCalendarItem, ExContactItem, ExTaskItem, ExNoteItem structs:

- ExContactItem
  - Key : An array of keys. Each key corresponds to a piece of information about the contact. Valid keys are:
    - displayName
    - email
    - title (Mr, Mrs, Etc)
    - firstName
    - middleName
    - lastName
    - suffix
    - fullName
    - jobTitle
    - companyName
    - companyDepartment
    - companyOffice
    - companyFax
    - companyUrl
    - busStreet
    - busZip
    - busCity
    - busState
    - busCountry
    - busPhone
    - busIpPhone
    - busPager
    - homeStreet
    - homeZip

- homeCity
  - homeState
  - homeCountry
  - homePhone
  - homeFax
  - mobilePhone
  - WebPage
  - instantMessenger
  - birthDay (date)
  - categories (comma separated list of categories this entry belongs to)
  - guid (can be any unique ID)
  - Value :The value for the contact information. Value should be base 64 encoded
  - ExCalendarItem
- Key :An array of keys. Each key corresponds ta piece of information about the calendar item.

Valid keys are:

- subject
- location
- description
- startDate (date)
- endDate (date)
- invitites (one per invitee)
- exludeddates (not used)
- reminder (how many minutes before appointment)
- guid (can be any unique ID)
- recurring (true/false)
- daily (true/false, only one frequency should be set)
- weekly (true/false, only one frequency should be set)
- monthly (true/false, only one frequency should be set)
- yearly (true/false, only one frequency should be set)
- until (date tstop recurring event)
- monthyear (month of year, 1-12)
- interval (every x interval)
- occurrences (stop recurring after x occurrences)
- dayofmonth (day of month)
- daysofweek (days of week bitmap, Sunday = 1, Monday = 2, ..., Saturday = 64)
- nthday (xth occurrence of the days of week. i.e. second Saturday)

- setpos (xth position of the set)
- categories (comma separated list of categories this entry belongs to)
- Value :The value for the calendar information. Value should be base 64 encoded.
- ExTaskItem
  
- Key :An array of keys. Each key corresponds ta piece of information about the task. Valid keys are:
  - subject
  - startDate (date)
  - dueDate (date)
  - reminder (how many minutes before task)
  - status (NeedsAction, InProcess, Completed)
  - priority (0-10)
  - percentComplete (0-100)
  - description
  - guid (can be any unique ID)
  - categories (comma separated list of categories this entry belongs to)
  - Value :The value for the task information. Value should be base 64 encoded.

## **Spam Administration Services/svcSpamAdmin.asmx**

The Spam Administration Web service handles all functionality dealing with managing spam configuration. The following functions are available in this Web service:

- SetSpamWizardLevel : Sets the spam checks and weights to predefined wizard levels
  
- Return Type :GenericResult
- Parameters :
  
- AuthUserName :The system administrator username
- AuthPassword :The system administrator password
- level :The level twich the spam wizard will set the configuration (Low, Med, High, None)
- ListRBLs : Lists information about all RBL checks
  
- Return Type :ListRBLsResult
- Parameters :
  
- AuthUserName :The system administrator username
- AuthPassword :The system administrator password
- AddRBL : Adds an RBL

- Return Type : GenericResult
- Parameters :
  - AuthUserName :The system administrator username
  - AuthPassword :The system administrator password
  - rblSetting :The settings tuse for the new RBL
  - GetRBL : Gets an RBL
- Return Type :GetRBLResult
- Parameters :
  - AuthUserName :The system administrator username
  - AuthPassword :The system administrator password
  - name :Name of the RBL tretrieve
  - EditRBL : Edits an RBL
- Return Type :GenericResult
- Parameters :
  - AuthUserName :The system administrator username
  - AuthPassword :The system administrator password
  - nameOfRblToEdit :The name of the RBL tedit
  - rblSetting :The new settings tuse for the RBL
  - RemoveRBL : Removes an RBL
- Return Type :GenericResult
- Parameters :
  - AuthUserName :The system administrator username
  - AuthPassword :The system administrator password
  - nameOfRblToRemove :The name of the RBL which should be removed
  - ListSpamChecks : Lists information about all known spam checks, similar tthe Antispam Administration page
- Return Type :ListSpamChecksResult
- Parameters :
  - AuthUserName :The system administrator username
  - AuthPassword :The system administrator password
  - GetDecludeSettings : Gets Declude's settings

- Return Type :GetDecludeSettingsResult
- Parameters :
  - AuthUserName :The system administrator username
  - AuthPassword :The system administrator password
  - SetDecludeSettings : Sets Declude's settings
- Return Type :GenericResult
- Parameters :
  - AuthUserName :The system administrator username
  - AuthPassword :The system administrator password
  - decludeSettings :The new settings tuse
  - GetSABPMSettings : Gets SpamAssassin based Pattern Matching's settings
- Return Type :GetSABPMSettingsResult
- Parameters :
  - AuthUserName :The system administrator username
  - AuthPassword :The system administrator password
  - SetSAPBMSettings : Sets SpamAssassin based Pattern Matching's settings
- Return Type :GenericResult
- Parameters :
  - AuthUserName :The system administrator username
  - AuthPassword :The system administrator password
  - sapbmSettings :The new settings tuse
  - GetRemoteSASettings : Gets Remote SpamAssassin's settings
- Return Type :GetRemoteSASettingsResult
- Parameters :
  - AuthUserName :The system administrator username
  - AuthPassword :The system administrator password
  - SetRemoteSASettings : Sets Remote SpamAssassin's settings
- Return Type :GenericResult
- Parameters :
  - AuthUserName :The system administrator username
  - AuthPassword :The system administrator password

- remoteSASettings :The new settings tuse
- GetCommTouchSettings : Gets CommTouch's settings
- Return Type :GetCommTouchSettingsResult
- Parameters :
- AuthUserName : The system administrator username
- AuthPassword : The system administrator password
- SetCommTouchSettings : Sets CommTouch's settings
- Return Type :GenericResult
- Parameters :
- AuthUserName :The system administrator username
- AuthPassword :The system administrator password
- commTouchSettings :The new settings tuse
- GetBayesianSettings : Gets Bayesian Filtering's settings
- Return Type :GetVayesianSettingsResult
- Parameters :
- AuthUserName :The system administrator username
- AuthPassword :The system administrator password
- SetBayesianSettings : Sets Bayesian's settings
- Return Type :GenericResult
- Parameters :
- AuthUserName :The system administrator username
- AuthPassword :The system administrator password
- bayesSettings :The new settings tuse
- GetDomainKeysSettings : Gets DomainKeys' settings
- Return Type : GetDomainKeysSettingsResult
- Parameters :
- AuthUserName :The system administrator username
- AuthPassword :The system administrator password
- SetDomainKeysSettings : Sets DomainKeys' settings
- Return Type :GenericResult
- Parameters :

- AuthUserName :The system administrator username
- AuthPassword :The system administrator password
- dkSettings :The new settings tuse
- GetDKIMSettings : Gets DKIM's settings
  
- Return Type :GetDKIMSettingsResult
- Parameters :
  
- AuthUserName :The system administrator username
- AuthPassword :The system administrator password
- SetDKIMSettings : Sets DKIM's settings
  
- Return Type :GenericResult
- Parameters :
  
- AuthUserName :The system administrator username
- AuthPassword :The system administrator password
- dkSettings :The new settings tuse
- GetReverseDNSSettings : Gets Reverse DNS's settings
  
- Return Type : GetReverseDNSSettingsResult
- Parameters :
  
- AuthUserName :The system administrator username
- AuthPassword :The system administrator password
- SetReverseDNSSettings : Gets Reverse DNS's settings
  
- Return Type : GetReverseDNSSettingsResult
- Parameters :
  
- AuthUserName :The system administrator username
- AuthPassword :The system administrator password
- rdnsSettings :The new settings tuse
- GetSPFSettings : Gets SPF's settings
  
- Return Type : GetSPFSettingsResult
- Parameters :
  
- AuthUserName :The system administrator username
- AuthPassword :The system administrator password
- SetSPFSettings : Sets SPF's settings

- Return Type :GenericResult
- Parameters :
  - AuthUserName :The system administrator username
  - AuthPassword :The system administrator password
  - spfSettings :The new settings tuse

The following return types are used:

- GenericResult :Generic result information for a Web service request
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- GetRemoteSASettingsResult :Generic result information for a Web service request
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- Settings :RemoteSASettings
- GetBayesianSettingsResult :Generic result information for a Web service request
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- Settings :BayesianFilterSettings
- GetSABPMSettingsResult :Generic result information for a Web service request
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- Settings :SABPMSettings
- GetCommTouchSettingsResult :Generic result information for a Web service request
- Result :True or false depending on the success of the Web service request
- ResultCode :pecific failure code if the result is false
- Message :Error message detailing why the result is false
- Settings :CommTouchSettings
- GetDecludeSettingsResult :Generic result information for a Web service request



- Result : True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- Settings :DecludeSettings
- GetDomainKeysSettingsResult :Generic result information for a Web service request
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- Settings :DomainKeysSettings
- GetRBLResult :Generic result information for a Web service request
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- Settings :RBLSetting
- GetReverseDNSSettingsResult :Generic result information for a Web service request
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- Settings :ReverseDNSSettings
- GetSPFSettingsResult :Generic result information for a Web service request
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- Settings :SPFSettings
- ListSpamChecksResult :Generic result information for a Web service request
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- Settings :SpamCheckInfarray
- ListRBLsResult :Generic result information for a Web service request
- Result :True or false depending on the success of the Web service request
- ResultCode :Specific failure code if the result is false
- Message :Error message detailing why the result is false
- Settings :RBLSetting array

## Deployment Guides

### SmarterMail in Individual and Micro-business Deployments

#### Who Should Use This Document

This document is intended for use by individuals and micro-businesses as they develop an effective architecture for their SmarterMail system implementation. For best results, this document should be used in conjunction with the SmarterTools Knowledge Base .

#### Determining the Required Architecture

It is not unusual for a business to generate upwards of 50 legitimate mail messages, per employee, per day on average 1 . Considering the relative volume of spam and other abusive messages that are currently prevalent, the total number of messages processed per user/mailbox could easily exceed 250 per day 2 . Companies in technology, finance, and other communication-intensive industries might have much higher average email volumes. A tendency toward the prolific use of attachments and email graphics can also influence performance in mail environments. SmarterTools encourages readers to determine which architecture is right for them based upon anticipated email volume as opposed to head-count because email load is a far better predictor of server requirements than the number of mailboxes on a system.

SmarterMail is built around a fully scalable model, so moving from one architecture recommendation to another requires relatively simple enhancements or modifications that can yield significant increases in performance and volume capacity.

That said, the authors have chosen to divide their recommendations into three categories: individual and micro-business architectures, small to medium-sized business architectures, and high-volume deployment architectures. For the purposes of these recommendations:

- Individuals and micro-businesses shall be defined as mail environments with average email volumes of up to 25,000 messages per day (12,500 in/12,500 out). This infers a maximum of 100 employees/mailboxes. Information regarding these architectures is available in this SmarterTools document.
- Small to medium-sized businesses shall be defined as mail environments with average email volumes of up to 400,000 messages per day (200,000 in/200,000 out). This infers a maximum of 1,600 employees/mailboxes. Information regarding these architectures can be found in SmarterMail in Small to Medium-sized Business Deployments , which is available for download on the SmarterTools website.

- High-volume deployments shall include ISPs, hosting companies, large businesses, and enterprise organizations with average email volumes numbering in the millions. This infers organizations with many thousands of employees/mailboxes. Information regarding these architectures can be found in SmarterMail in High-Volume Deployments , which is available for download on the SmarterTools website.

1 Intel presentation, “IT Business Value”, 9-16-2005.

2 Nearly 80% of email messages sent world-wide are spam....”; Deleting Spam Costs Business Billions, Information Management Journal, May/June 2005, Nikki Swartz

## General Architecture

The general recommendation for SmarterMail architecture in an individual and micro-business environment (up to 25,000 messages per day) is as shown in Figure 1.

### SmarterMail Primary Server

This server is the central data processor and repository of your client’s email. Users connect to this server using POP and IMAP to receive email, and use SMTP to send email out. Webmail is also hosted on this server to help those without email client software. In addition, the SmarterMail server performs all spam-blocking and virus protection operations.

Hardware recommended in this configuration for individuals and micro-businesses includes:

- Single-core processor
- 1 GB of RAM
- 7200 RPM SATA drive

### Email Virtualization: SmarterMail in Virtual Server (VPS) Environments

A virtual server environment is when one physical hardware device is partitioned so as to operate as two or more separate servers. SmarterMail can be deployed in all types of virtual server environments and has been tested with most major virtualization software (such as Hyper-V, VMware, Virtual Box, Virtuozzo and Zen).

Note: If using Hyper-V, SmarterTools recommends attaching a physical network adapter from the Hyper-V host to the SmarterMail virtual machine instead of using the virtual network manager to create virtual LANs/bridges. This is because there is a risk of losing network access to all of the virtual machines if they are all tied to a single virtual network and a network-related issue occurs on one of the virtual machines. By allowing the SmarterMail virtual machine a dedicated physical connection, this risk can be eliminated.

## **Recommended Spam Protection Measures**

SmarterMail uses a flexible, multi-layered spam prevention strategy to achieve 97% spam protection out-of-the-box. Initial spam settings are configured during installation, but system administrators can modify these settings to meet their unique needs at any time.

Since spam prevention strategy is an integral component of mail server deployment, a few of the most important spam-fighting measures available for SmarterMail are discussed below.

### **CommTouch Premium Antispam**

Available as an optional add-on for SmarterMail, CommTouch Premium Antispam uses Recurrent Pattern Detection (RPD) technology to protect against spam outbreaks in real time. Rather than evaluating the content of messages, the CommTouch Detection Center analyzes large volumes of Internet traffic in real time, recognizing and protecting against new spam outbreaks the moment they emerge. When combined with SmarterMail's out-of-the box antispam measures, the CommTouch Premium Antispam add-on can effectively block 99.5% of spam from users' inboxes.

For more information about the CommTouch Premium Antispam add-on, please visit the SmarterTools website.

### **SpamAssassin-based Pattern Matching Engine**

SmarterMail incorporates the SpamAssassin-based Pattern Matching Engine as part of its multi-layered spam protection strategy. Based on SpamAssassin technology, this powerful pattern matching engine can process substantially higher volumes of email per day without the need for a distributed antispam server. For more information, please refer to the SmarterMail Online Help.

### **Greylisting**

SmarterMail also includes greylisting, an effective method of blocking spam at the SMTP level. Using the greylisting feature in conjunction with SpamAssassin will prevent a large percentage of spam messages from being received by the SmarterMail server and drastically reduce the SpamAssassin work load. At the time of this writing the greylisting feature is effectively blocking up to 85% of spam at the SMTP level and greatly enhancing the effectiveness of SpamAssassin. The authors expect that the effectiveness of greylisting will diminish over time as spammers learn to adjust to this technique. Additional information about greylisting can be found in the SmarterMail Online Help or at <http://greylisting.org>.

### **Other Built-in Antispam Measures**

SmarterMail's multi-layered spam prevention strategy also includes SPF, DomainKeys/DKIM, Bayesian filtering, reverse DNS, RBL, blacklist/whitelist, SMTP blocking, custom headers, and per-

user spam weighting. More information about these important features is available in the SmarterMail Online Help and/or the SmarterTools Knowledge Base.

### **Remote SpamAssassin**

SmarterMail includes support for SpamAssassin, an open source spam filtering program. When implemented, SmarterMail will pass an incoming message to SpamAssassin. SpamAssassin returns the message to SmarterMail with a spam score which can be used to filter mail alone or in conjunction with any or all of the other spam filtering options in SmarterMail.

Currently, the Windows version is limited to processing a single message at a time—effectively handling approximately 25,000 spam messages per day. This version of SpamAssassin is usually more than adequate to meet the needs of individual and micro-business environments. Additional information about SpamAssassin, including downloading instructions, is available at <http://spamassassin.apache.org>.

### **Recommended Virus Protection Measures**

SmarterMail includes several antivirus enhancements that prevent the mail server from being compromised, including support for incoming and outgoing SSL/TLS connections, administrator access restriction by IP, intrusion detection (IDS), active directory authentication, harvest attack detection, denial of service (DOS) attack prevention, malicious script authentication, and brute force detection for webmail.

### **Commtouch Zero-hour Antivirus**

Available as an optional add-on for SmarterMail, Commtouch Zero-hour Antivirus can further extend SmarterMail's built-in virus protection measures. Rather than depending on heuristics, Commtouch Zero-hour Antivirus uses Recurrent Pattern Detection (RPD) technology to scan the Internet and identify virus and malware outbreaks as soon as they emerge.

For more information about the Commtouch Zero-hour add-on, please visit the SmarterTools website.

## **SmarterMail in Small to Medium-sized Business Deployments**

### **Who Should Use This Document**

This document is intended for use by small to medium-sized businesses as they develop an effective architecture for their SmarterMail system implementation. For best results, this document should be used in conjunction with the SmarterMail Online Help and the SmarterTools Knowledge Base.

## **Determining the Required Architecture**

It is not unusual for a business to generate upwards of 50 legitimate mail messages, per employee, per day on average <sup>1</sup>. Considering the relative volume of spam and other abusive messages that are currently prevalent, the total number of messages processed per user/mailbox could easily exceed 250 per day <sup>2</sup>. Companies in technology, finance, and other communication-intensive industries might have much higher average email volumes. A tendency toward the prolific use of attachments and email graphics can also influence performance in mail environments. SmarterTools encourages readers to determine which architecture is right for them based upon anticipated email volume as opposed to head-count because email load is a far better predictor of server requirements than the number of mailboxes on a system.

SmarterMail is built around a fully scalable model, so moving from one architecture recommendation to another requires relatively simple enhancements or modifications that can yield significant increases in performance and volume capacity.

That said, the authors have chosen to divide their recommendations into three categories: individual and micro-business architectures, small to medium-sized business architectures, and high-volume deployment architectures. For the purposes of these recommendations:

- Individuals and micro-businesses shall be defined as mail environments with average email volumes of up to 25,000 messages per day (12,500 in/12,500 out). This infers a maximum of 100 employees/mailboxes. Information regarding these architectures is available in this SmarterTools document. Information regarding these architectures can be found in SmarterMail in Individual and Micro-business Deployments , which is available for download on the SmarterTools website.
- Small to medium-sized businesses shall be defined as mail environments with average email volumes of up to 400,000 messages per day (200,000 in/200,000 out). This infers a maximum of 1,600 employees/mailboxes. Information regarding these architectures is available in this SmarterTools document.
- High-volume deployments shall include ISPs, hosting companies, large businesses, and enterprise organizations with average email volumes numbering in the millions. This infers organizations with many thousands of employees/mailboxes. Information regarding these architectures can be found in SmarterMail in High-Volume Deployments , which is available for download on the SmarterTools website.

<sup>1</sup> Intel presentation, "IT Business Value", 9-16-2005.

<sup>2</sup> "Nearly 80% of email messages sent world-wide are spam..."; Deleting Spam Costs Business Billions, Information Management Journal, May/June 2005, Nikki Swartz

## General Architecture

The general recommendation for SmarterMail architecture in a small to medium-sized business environment (up to 200,000 messages per day) is as shown in Figure 1.

### **SmarterMail Primary Server**

This server is the central data processor and repository of your client's email. Users connect to this server using POP and IMAP to receive email, and use SMTP to send email out. Webmail is also hosted on this server to help those without email client software. In addition, the SmarterMail server performs spam-blocking (with the exception of SpamAssassin) and virus protection operations.

Hardware recommended for this configuration in small to medium-sized businesses includes:

- Dual-core processor
- 1 GB of RAM
- 7200 RPM SATA drive (minimum)
- RAID 10 3

3 While a RAID 10 configuration is recommended for SmarterMail Primary Servers, the Authors recognize that some companies have policies that require the use of alternate RAID configurations. In this case, other RAID configurations may be used with the exception of RAID 1. The use of RAID 1 arrays in this configuration will likely result in a significant reduction in disk performance (up to a 50% loss vs. a single drive and up to 8 times slower than a 4-drive RAID 10 implementation).

### **Email Virtualization: SmarterMail in Virtual Server (VPS) Environments**

A virtual server environment is when one physical hardware device is partitioned so as to operate as two or more separate servers. SmarterMail can be deployed in all types of virtual server environments and has been tested with most major virtualization software (such as Hyper-V, VMware, Virtual Box, Virtuozzo and Zen).

Note: If using Hyper-V, SmarterTools recommends attaching a physical network adapter from the Hyper-V host to the SmarterMail virtual machine instead of using the virtual network manager to create virtual LANs/bridges. This is because there is a risk of losing network access to all of the virtual machines if they are all tied to a single virtual network and a network-related issue occurs on one of the virtual machines. By allowing the SmarterMail virtual machine a dedicated physical connection, this risk can be eliminated.

### **Recommended Spam Protection Measures**

SmarterMail uses a flexible, multi-layered spam prevention strategy to achieve 97% spam protection

out-of-the-box. Initial spam settings are configured during installation, but system administrators can modify these settings to meet their unique needs at any time.

Since spam prevention strategy is an integral component of mail server deployment, a few of the most important spam-fighting measures available for SmarterMail are discussed below.

### **Commtouch Premium Antispam**

Available as an optional add-on for SmarterMail, Commtouch Premium Antispam uses recurrent pattern detection (RPD) technology to protect against spam outbreaks in real time. Rather than evaluating the content of messages, the Commtouch Detection Center analyzes large volumes of Internet traffic in real time, recognizing and protecting against new spam outbreaks the moment they emerge. When combined with SmarterMail's out-of-the box antispam measures, the Commtouch Premium Antispam add-on can effectively block 99.5% of spam from users' inboxes.

For more information about the Commtouch Premium Antispam add-on, please visit the SmarterTools website.

### **SpamAssassin-based Pattern Matching Engine**

SmarterMail incorporates the SpamAssassin-based Pattern Matching Engine as part of its multi-layered spam protection strategy. Based on SpamAssassin technology, this powerful pattern matching engine can process substantially higher volumes of email per day without the need for a distributed antispam server. For more information, please refer to the SmarterMail Online Help.

### **Greylisting**

SmarterMail includes greylisting—an effective method of blocking spam at the SMTP level. Using the greylisting feature in conjunction with SpamAssassin will prevent a large percentage of spam messages from being received by the SmarterMail server and drastically reduce the SpamAssassin work load. At the time of this writing the greylisting feature is effectively blocking up to 85% of spam at the SMTP level and greatly enhancing the effectiveness of SpamAssassin. The authors expect that the effectiveness of greylisting will diminish over time as spammers learn to adjust to this technique. Additional information about greylisting can be found in the SmarterMail Online Help or at <http://greylisting.org>.

### **Other Built-in Antispam Measures**

SmarterMail's multi-layered spam prevention strategy also includes SPF, DomainKeys/DKIM, Bayesian filtering, reverse DNS, RBL, blacklist/whitelist, SMTP blocking, custom headers, and per-user spam weighting. More information about these important features is available in the SmarterMail Online Help and/or the SmarterTools Knowledge Base.



### **Distributed SpamAssassin Servers**

SmarterMail 8.x includes support for SpamAssassin, an open source spam filtering program. When implemented, SmarterMail will pass an incoming message to SpamAssassin. SpamAssassin returns the message to SmarterMail with a spam score which can be used to filter mail alone or in conjunction with any or all of the other spam filtering options in SmarterMail.

Currently, the Windows version is limited to processing a single message at a time—effectively handling approximately 25,000 spam messages per day and usually more than adequate to the needs of individual and micro-business environments. However, the Linux version of SpamAssassin can process multiple spam messages simultaneously, allowing it to process significantly more messages than its Windows counterpart. Therefore, SmarterTools recommends the stand-alone Linux version of SpamAssassin for small to medium-sized business environments (see Figure 2).

The Linux version of SpamAssassin is available at no charge from the SpamAssassin website and is installed on its own server (distributed environment). Additional information about SpamAssassin, including downloading instructions, is available at <http://spamassassin.apache.org>.

SmarterTools recommends the following hardware for stand-alone, distributed SpamAssassin servers:

- Dual-core processor
- 1 GB of RAM
- Dedicated SATA drive

It is possible to use a virtual server environment (Virtual PC, VMWare, etc.) to run SmarterMail (primary) in Windows and SpamAssassin (distributed) in Linux on the same physical hardware. This configuration may even be preferable in certain situations due to physical space requirements, fast communication between SmarterMail and the distributed SpamAssassin, and the cost savings of purchasing only one physical device.

If a virtual server configuration is chosen, where one physical server device operates as the primary mail server and contains the SpamAssassin Linux version as a distributed virtual server, SmarterTools recommends the following hardware:

- Dual-core processor
- 2 GB of RAM
- 7200 RPM SATA drive (minimum)
- RAID 10 4

4 While a RAID 10 configuration is recommended for SmarterMail Primary Servers, the Authors recognize that some companies have policies that require the use of alternate RAID configurations. In this case, other RAID configurations may be used with the exception of RAID 1. The use of RAID 1

arrays in this configuration will likely result in a significant reduction in disk performance (up to a 50% loss vs. a single drive and up to 8 times slower than a 4-drive RAID 10 implementation).

### **Recommended Virus Protection Measures**

SmarterMail includes several antivirus enhancements that prevent the mail server from being compromised, including support for incoming and outgoing SSL/TLS connections, administrator access restriction by IP, intrusion detection (IDS), active directory authentication, harvest attack detection, denial of service (DOS) attack prevention, malicious script authentication, and brute force detection for webmail.

#### **CommTouch Zero-hour Antivirus**

Available as an optional add-on for SmarterMail, CommTouch Zero-hour Antivirus can further extend SmarterMail's built-in virus protection measures. Rather than depending on heuristics, CommTouch Zero-hour Antivirus uses Recurrent Pattern Detection (RPD) technology to scan the Internet and identify virus and malware outbreaks as soon as they emerge.

For more information about the CommTouch Zero-hour add-on, please visit the SmarterTools website.

### **Extending Capacity via Outbound Gateways**

Outbound gateways are used for handling the delivery of remote mail to reduce the load on the primary mail server(s). An outbound gateway does not perform the tasks of storage and/or retrieval of end users' mail—freeing it to process many times more outgoing messages than a primary server could be expected to handle effectively.

Most small to medium-sized business environments will not need an outbound gateway. However, as a business grows, the addition of an outbound gateway can add significant capacity to a mail network and smooth the transition to higher volumes and larger networks. In the opinion of the authors, a single primary server in this configuration with distributed spam handling and a SmarterMail outbound gateway can effectively process upwards of 400,000 messages per day (200,000 in/200,000 out). This infers a maximum of 1,600 employees/mailboxes.

Businesses that choose to extend capacity via an outbound gateway can download SmarterMail Free and set it up as a free gateway server. More information about configuring SmarterMail as a free gateway server is available in the SmarterTools Knowledge Base.

### **General Architecture with an Outbound Gateway**

The general recommendation for SmarterMail architectures in a small to medium-sized business environments including an outbound gateway (up to 400,000 messages per day) is as shown in Figure 3.

## **SmarterMail Outbound Gateway Servers**

The Authors recommend the following hardware configuration for SmarterMail outbound gateways:

- Dual-core processor
- 1 GB of RAM
- SATA drive dedicated for the spool

This hardware configuration can support many SmarterMail servers, but SmarterTools recommends an ideal ratio of one gateway server for every five primary mail servers—reducing the risks of blacklisting and the effects of potential hardware failures.

## **Using Third-party Solutions with SmarterMail**

### **Inbound Gateways**

SmarterMail is designed to function at very high levels of performance in a small business environment without the need for an inbound gateway. Some companies choose to use spam and virus filtering solutions in front of their mail server—an inbound gateway. In the opinion of the authors, it should not be expected that the addition of an inbound gateway will have a significant impact on the performance of the mail network in a small to medium-sized business environment.

The majority of spam checks built into SmarterMail work off the IP address of the sender. When you use an inbound gateway, SmarterMail will receive all mail from that gateway which will cause the IP-based spam filters to no longer function correctly. For this reason, you will want all spam filtering to be performed via the inbound gateway.

The authors recommend the consideration of the following third-party solutions for inbound gateways:

- Barracuda: [www.barracudanetworks.com](http://www.barracudanetworks.com)
- Postini: [www.postini.com](http://www.postini.com)

Generally, inbound gateways are applicable only in higher-volume environments. Additional information and recommendations on SmarterMail implementations in various environments is available at the SmarterTools website.

## **SmarterMail in High-volume Deployments**

### **Who Should Use This Document**

This document is intended for use by large and enterprise businesses as they develop an effective architecture for their SmarterMail system implementation. For best results, this document should be used in conjunction the SmarterTools Knowledge Base .

## **Determining the Required Architecture**

It is not unusual for a business to generate upwards of 50 legitimate mail messages, per employee, per day on average. Considering the relative volume of spam and other abusive messages that are currently prevalent, the total number of messages processed per user/mailbox could easily exceed 250 per day. Companies in technology, finance, and other communication-intensive industries might have much higher average email volumes. A tendency toward the prolific use of attachments and email graphics can also influence performance in mail environments. SmarterTools encourages readers to determine which architecture is right for them based upon anticipated email volume as opposed to head-count because email load is a far better predictor of server requirements than the number of mailboxes on a system.

SmarterMail is built around a fully scalable model, so moving from one architecture recommendation to another requires relatively simple enhancements or modifications that can yield significant increases in performance and volume capacity.

That said, the authors have chosen to divide their recommendations into three categories: individual and micro-business architectures, small to medium-sized business architectures, and high-volume deployment architectures. For the purposes of these recommendations:

- Individuals and micro-businesses shall be defined as mail environments with average email volumes of up to 25,000 messages per day (12,500 in/12,500 out). This infers a maximum of 100 employees/mailboxes. Information regarding these architectures can be found in SmarterMail in Individual and Micro-business Deployments, which is available for download on the SmarterTools website.
- Small to medium-sized businesses shall be defined as mail environments with average email volumes of up to 400,000 messages per day (200,000 in/200,000 out). This infers a maximum of 1,600 employees/mailboxes. Information regarding these architectures can be found in SmarterMail in Small to Medium-sized Business Deployments, which is available for download on the SmarterTools website.
- High-volume deployments shall include ISPs, hosting companies, large businesses, and enterprise organizations with average email volumes numbering in the millions. This infers organizations with many thousands of employees/mailboxes. Information regarding these architectures is available in this SmarterTools document.

## **General Architecture**

The general recommendation for the high-volume system architecture is detailed in Figure 1 below.

## **SmarterMail Primary Servers**

The SmarterMail servers are the central data repositories of email. Users connect to these servers using POP and IMAP to receive email, and use SMTP to send email out. Webmail is also established on these servers for those choosing to access email through the Web interface. A SmarterMail network may contain one or more mail servers. Under normal activity—and assuming sufficient disk space 3—each server should be able to handle up to 40,000 users per server (1 million messages per day).

For high-volume deployments utilizing this architecture, SmarterTools recommends the following server specifications for SmarterMail servers:

- Dual-core, server-grade processors
- 4 GB of RAM
- RAID 1 array for the operating system and program files
- One single drive or RAID 0 array for the email spool
- RAID 10 4 array to store user data and email
- Virtual machines are not recommended for large deployments as restrictions on disk I/O can seriously impact performance.

## **SmarterMail Outbound Gateways**

Outbound gateways are used for handling the delivery of remote mail to reduce the load on the primary mail server(s). An outbound gateway does not perform the tasks of storage and/or retrieval of end users' mail via POP, IMAP, or webmail—freeing it to process many times more outgoing messages than a primary server could be expected to handle effectively.

SmarterMail includes support for round-robin gateway delivery (all types of gateway servers) and advanced gateway load-balancing (SmarterMail gateways only) to further balance the load on your gateways and making them better at delivering high volumes of mail quickly. Businesses setting up an outbound gateway can download SmarterMail Free and set it up as a free gateway server. More information about configuring SmarterMail as a free gateway server is available in the SmarterTools Knowledge Base.

SmarterTools recommends the following hardware for SmarterMail outbound gateways:

- Dual-core processor
- 1 GB of RAM
- SATA drive dedicated for the spool

This hardware configuration can support many SmarterMail servers, but SmarterTools recommends an ideal ratio of one gateway server for every five primary mail servers—reducing the risks of blacklisting and the effects of potential hardware failures.

## **Recommended Spam Protection Measures**

SmarterMail uses a flexible, multi-layered spam prevention strategy to achieve 97% spam protection out-of-the-box. Initial spam settings are configured during installation, but system administrators can modify these settings to meet their unique needs at any time.

Since spam prevention strategy is an integral component of mail server deployment, a few of the most important spam-fighting measures available for SmarterMail are discussed below.

### **CommTouch Premium Antispam**

Available as an optional add-on for SmarterMail, CommTouch Premium Antispam uses Recurrent Pattern Detection (RPD) technology to protect against spam outbreaks in real time. Rather than evaluating the content of messages, the CommTouch Detection Center analyzes large volumes of Internet traffic in real time, recognizing and protecting against new spam outbreaks the moment they emerge. When combined with SmarterMail's out-of-the box antispam measures, the CommTouch Premium Antispam add-on can effectively block 99.5% of spam from users' inboxes.

For more information about the CommTouch Premium Antispam add-on, please visit the SmarterTools website.

### **SpamAssassin-based Pattern Matching Engine**

SmarterMail incorporates the SpamAssassin-based Pattern Matching Engine as part of its multi-layered spam protection strategy. Based on SpamAssassin technology, this powerful pattern matching engine can process substantially higher volumes of email per day without the need for a distributed antispam server. For more information, please refer to the SmarterMail Online Help.

### **Greylisting**

SmarterMail includes greylisting—an effective method of blocking spam at the SMTP level. Using the greylisting feature in conjunction with SpamAssassin will prevent a large percentage of spam messages from being received by the SmarterMail server and drastically reduce the SpamAssassin work load. At the time of this writing the greylisting feature is effectively blocking up to 85% of spam at the SMTP level and greatly enhancing the effectiveness of SpamAssassin. The authors expect that the effectiveness of greylisting will diminish over time as spammers learn to adjust to this technique. Additional information about greylisting can be found in the SmarterMail Online Help or at <http://greylisting.org>.

### **Other Built-in Antispam Measures**

SmarterMail's multi-layered spam prevention strategy also includes SPF, DomainKeys/DKIM, Bayesian filtering, reverse DNS, RBL, blacklist/whitelist, SMTP blocking, custom headers, and per-

user spam weighting. More information about these important features is available in the SmarterMail Online Help and/or the SmarterTools Knowledge Base.

### **Distributed SpamAssassin Servers**

SmarterMail 8.x includes support for SpamAssassin, an open source spam filtering program. When implemented, SmarterMail will pass an incoming message to SpamAssassin. SpamAssassin returns the message to SmarterMail with a spam score which can be used to filter mail alone or in conjunction with any or all of the other spam filtering options in SmarterMail.

Currently, the Windows version is limited to processing a single message at a time—effectively handling approximately 100-200k spam messages per day and is usually more than adequate to the needs of low and medium-volume environments. However, the Linux version of SpamAssassin can process multiple spam messages simultaneously, allowing it to process significantly more messages than its Windows counterpart. Therefore, SmarterTools recommends the stand-alone Linux version of SpamAssassin for high-volume environments (see Figure 1).

Additional information about SpamAssassin, including downloading instructions, is available at <http://spamassassin.apache.org>.

SmarterTools recommends the following hardware for stand-alone SpamAssassin servers:

- Dual-core processor
- 1 GB of RAM
- Dedicated SATA drive

### **Recommended Virus Protection Measures**

SmarterMail includes several antivirus enhancements that prevent the mail server from being compromised, including support for incoming and outgoing SSL/TLS connections, administrator access restriction by IP, intrusion detection (IDS), active directory authentication, harvest attack detection, denial of service (DOS) attack prevention, malicious script authentication, and brute force detection for webmail. Commtouch Zero-hour Antivirus

Available as an optional add-on for SmarterMail, Commtouch Zero-hour Antivirus can further extend SmarterMail's built-in virus protection measures. Rather than depending on heuristics, Commtouch Zero-hour Antivirus uses Recurrent Pattern Detection (RPD) technology to scan the Internet and identify virus and malware outbreaks as soon as they emerge.

For more information about the Commtouch Zero-hour add-on, please visit the SmarterTools website.

## Optional Servers

An alternative recommendation for the high-volume system architecture that incorporates optional servers is detailed in Figure 2 below.

### **Distributed SpamAssassin Servers**

SmarterMail 8.x includes support for SpamAssassin, an open source spam filtering program. When implemented, SmarterMail will pass an incoming message to SpamAssassin. SpamAssassin returns the message to SmarterMail with a spam score which can be used to filter mail alone or in conjunction with any or all of the other spam filtering options in SmarterMail.

Currently, the Windows version is limited to processing a single message at a time—effectively handling approximately 100-200k spam messages per day and is usually more than adequate to the needs of low and medium-volume environments. However, the Linux version of SpamAssassin can process multiple spam messages simultaneously, allowing it to process significantly more messages than its Windows counterpart. Therefore, SmarterTools recommends the stand-alone Linux version of SpamAssassin for high-volume environments (see Figure 2).

Additional information about SpamAssassin, including downloading instructions, is available at <http://spamassassin.apache.org>.

SmarterTools recommends the following hardware for stand-alone SpamAssassin servers:

- Dual-core processor
- 1 GB of RAM
- Dedicated SATA drive

### **ClamAV Servers**

SmarterMail includes support for ClamAV, an open-source project offering superior antivirus protection that resides on the primary mail server, or in high-volume environments, on a remote server in a Linux environment. More information about ClamAV is available at [www.clamav.net](http://www.clamav.net).

SmarterTools recommends the following hardware for stand-alone ClamAV servers:

- Dual-core processor
- 1 GB of RAM
- Dedicated SATA drive

### **DNS Cache Servers**

DNS cache servers can be added to speed email delivery through systems with exceptionally heavy traffic or to take the load off of existing network DNS servers in Web hosting (or other) environments



in which Web traffic is very high. Adding an email-dedicated DNS cache server also allows the control of caching rates for DNS queries for mail servers independently of the main network. The requirements—or lack thereof—for email-dedicated DNS servers vary greatly from organization to organization. Therefore, SmarterTools does not currently provide a hardware or configuration recommendation for DNS servers.

Additional information regarding DNS and DNS servers is available on the following websites:

- [www.dns.net/dnsrd/servers/](http://www.dns.net/dnsrd/servers/)
- [http://en.wikipedia.org/wiki/Domain\\_name\\_system](http://en.wikipedia.org/wiki/Domain_name_system)

If it is determined that a system requires email-dedicated DNS caching, SmarterTools recommends a BIND solution. Information regarding BIND solutions is available at <http://www.isc.org/index.pl?/sw/bind/>.

## Using SmarterMail with Third-party Solutions

### Inbound Gateways

In certain ultra-high-volume environments, inbound gateways are used to offload spam and virus checking from the primary server(s). In such environments, the SmarterTools does not recommend that SmarterMail servers be used as inbound gateways.

In the relatively rare event that an inbound gateway becomes necessary, SmarterTools suggests the consideration of a third-party solution. Most spam checks and filters built into SmarterMail utilize the IP address of the mail sender. When using a third-party inbound gateway, all mail passes through that gateway prior to arriving at the SmarterMail server(s), which will negatively impact the functioning of the IP-based spam filters. For this reason, you will want all spam filtering to be done via the incoming gateway when using a third-party inbound gateway solution.

SmarterTools recommends the following third-party solutions for inbound gateways in ultra-high-volume environments:

- Barracuda: [www.barracudanetworks.com](http://www.barracudanetworks.com).
- Postini: [www.postini.com](http://www.postini.com).

### Declude

SmarterMail also includes support for many third-party antispam products, including Declude. Declude is an effective spam filtering software that integrates well with SmarterMail in high-volume environments. For this reason, if your system requires additional spam filtering, SmarterTools recommends considering Declude. More information about Declude is available at [www.decluce.com](http://www.decluce.com).

For full list of third-party antispam/antivirus products that have been tested with SmarterMail, refer to the SmarterMail Resources Resources page on the SmarterTools website.

## Summary

SmarterMail is a good choice for high-volume mail environments. The proper configuration and system architecture outlined in this document will provide a solid, reliable foundation. Because variations exist due to different volumes and client needs, SmarterTools suggests starting with these recommendations and then adjusting server proportions, limits, and specifications based on the usage patterns that result.

1 Intel presentation, “IT Business Value”, 9-16-2005.

2 “Nearly 80% of email messages sent world-wide are spam...”; Deleting Spam Costs Business Billions, Information Management Journal, May/June 2005, Nikki Swartz.

3 The amount of disk space allocated per user and per domain is set by the System Administrator.

4 While a RAID 10 configuration is recommended for SmarterMail Primary Servers, the authors recognize that some companies have policies that require the use of alternate RAID configurations. In this case, other RAID configurations may be used with the exception of RAID 1. The use of RAID 1 arrays in this configuration will likely result in a significant reduction in disk performance (up to a 50% loss vs. a single drive and up to 8 times slower than a 4-drive RAID 10 implementation).