



SmarterMail 15.x

Help Documentation

SmarterMail Help

Welcome to the SmarterMail Help System. In the tree menu on the left you will find various help topics that will help you use SmarterMail more effectively. At the top of each page, there are links that will allow you to search the help, watch product videos, visit the SmarterTools Community, browse the knowledge base or either print the page you're on or view the page as a PDF file. At the bottom of each content window, there is also a "Link to this page" text link that can be used for to send people directly to that page of the help file.

If you need assistance beyond what's available in this documentation, feel free to review the paid support options and self-help resources found on the Support Portal .

Common Help Topics for Users

- Logging in to my email account
- Sending messages
- Reading messages

Common Help Topics for Domain Administrators

- Adding email accounts
- Adding email aliases
- Add shared resources (shared calendars, conference rooms, etc.)
- Configuring spam filtering

Common Help Topics for System Administrators

- Logging in for the first time
- Adding a domain
- Proper DNS configuration
- Locking down your server

Getting Started

SmarterMail is a feature-rich Windows mail server that brings the power of enterprise-level features and collaboration to businesses and hosting environments. Use the Getting Started section of the SmarterMail Online Help as a quick resource to help you set up the application.

Note: This section assumes you have already downloaded and installed SmarterMail from the SmarterTools website.

Setting up SmarterMail

- Getting Started Page - After SmarterMail is installed, a Getting Started page will load. This page includes a link to a video walkthrough of the initial setup of SmarterMail, including each step outlined below, as well as a link to launch the Setup Wizard.
- License Setup - The Setup Wizard will ask you for a valid license key to activate either the Professional or Enterprise edition of the software. If you choose not to provide a license key, the product will run as the Free edition. For more information, see Activation .
- Primary Administrator - This initial system administrator account will be used to manage your entire SmarterMail installation. The Setup Wizard will ask you for the username and password for this account. By default, the username is 'admin' but you can change it to any name you like. You can add additional system administrators after completing the Setup Wizard. For more information, see System Administrators .
- System Info - Here you'll provide information SmarterMail (or any mail server) requires in order to identify itself when sending email messages to other mail servers. The Setup Wizard will ask you for the hostname, the primary IP address that the SmarterMail service will bind to and the IP address(es) for DNS.
- SmarterMail Paths - Now you'll need to specify where SmarterMail stores configuration and mailbox information like domain data, the spool, log files, POP retrieval data and IMAP retrieval data. By default, SmarterMail sets paths for you on the local drive. However, if you want to store information on a separate drive, you simply need to specify the paths you want to use.
- Spam Profiles - Choose a spam profile to pre-configure spam settings on your server. The recommended spam profile is selected by default, but you can choose another profile with more or less spam checks if you desire. You may also further customize or change these settings after completing the Setup Wizard. For more information, see Antispam Administration .
- Security - Here you'll choose whether or not to boost your spam protection measures with greylisting and/or to protect your server from viruses with the built-in antivirus software, ClamAV. You can configure additional security options such as the Cyren Zero-Hour Antivirus

add-on or other third-party antivirus solutions after completing the Setup Wizard. For more information, see [Antivirus Administration](#).

- Abuse Detection - On this page, you'll choose whether to use preset abuse detection settings based on whether you'd like relaxed or strict security. These presets cover settings for DoS, SMTP brute force, email harvesting and more. You can choose a preset here or at any time on the abuse detection page. For more information, see [Abuse Detection](#).
- Login Display - At this page you can make any custom modifications to the default SmarterMail login page. Add a company logo, change the default "Login to SmarterMail" text to be more in line with an overall brand message or add a link to the Help menu. Checking the box for 'Add custom help information to login page' will add the following to the login page, based on your Help URL: "For help please go to our support page."
- When you click Finish in the Setup Wizard, you will automatically be logged in to SmarterMail using the primary administrator account you created earlier. From here, you'll be able to add domains and customize your mail server to meet your unique needs.

Adding the First Domain

- Add Domain - Now that the initial setup of your mail server is complete, you will need to add a domain to SmarterMail. Adding a domain to SmarterMail represents the business entity and the domain name (such as example.com) that will be used in the creation of individual user mailboxes. Note: Only domains that you purchased and own should be added to SmarterMail. For more information, see [All Domains](#) or the KB article [Add a Domain to SmarterMail](#).
- Configure DNS and Ports - Now that you've created your domain, you'll need to configure the DNS and port settings for the domain. Configuring DNS settings is important because these settings tell the Internet where to send email on your domain. For step-by-step instructions on configuring DNS settings, see the KB article [Configure DNS for a Domain](#). In addition, you will need to ensure that any ports that SmarterMail will use, including the standard default ports for POP3 (port 110), IMAP (port 143) and SMTP (port 25) are open on your firewall. In addition, additional ports may be required, depending on how you intend to use SmarterMail. For example, standard HTTP (port 80) for access to webmail, Secure SMTP (port 465), IMAP over SSL (port 993) or others. All of these should be opened on your firewall to ensure SmarterMail works as expected. Note: Your ISP might block specific ports, especially port 25 for SMTP, so it is recommended to contact your ISP to ensure SMTP traffic on these ports is allowed.
- Add Users - Now that your domain and network configurations are set up, you need to manage the domain by adding users. Any individual that should send and receive mail or have their own mailbox should be added as a user for the domain. This will create a mailbox and email address

for that user (e.g., user@example.com). For more information, see [Users](#) or the KB article [Create a User in SmarterMail](#).

Recommended Step to Secure Your Installation

- Set up SmarterMail as an IIS site, if necessary. For more information, see [Running as an IIS Site](#). Note: If your SmarterMail installation is deployed using the default Web server, the chat functionality will not work as the default Web server is not meant for production environments. SmarterTools recommends converting to IIS.

General Information

What is SmarterMail?

SmarterMail is an award-winning mail and collaboration server that easily meets the needs of any sized business, from the individual proprietor to large corporations and enterprise organizations.

Features include:

- A rich webmail interface optimized for desktops, tablets and "phablets"
- A mobile interface ideally suited for smartphones
- An integrated instant live messaging system that can be used right from the Web interface or integrated with third-party products like Adium, Pidgin or IM+
- Full collaboration and groupware features (shared contacts, calendars, tasks and notes)
- File storage
- Detailed reporting at the mailbox, domain and system levels
- Email and chat archiving, ideal for complicity requirements
- Intrusion detection/prevention
- Advanced synchronization with third-party email clients (Apple Mail, Microsoft Outlook, Mozilla Thunderbird, etc.) and mobile devices (Android, BlackBerry, iOS, Windows Phones, etc.)
- Structured and multi-layered antispam and antivirus tools included at no additional charge
- Optional add-ons for Microsoft Exchange ActiveSync, Exchange Web Services, Message Sniffer, Cyren Premium Antispam and Cyren Zero-hour Antivirus
- Failover functionality
- And more...

With lower hardware requirements, superior stability and reduced maintenance costs, SmarterMail has significantly lower TCO and is the best-in-class Microsoft Exchange alternative for businesses and hosting companies.

SmarterMail Edition Explanation

Professional Edition vs. Enterprise Edition

SmarterMail Professional Edition has all of the features required to host a fully-functional mail server. SmarterMail Enterprise Edition offers additional features, including:

- Failover functionality
- Ability to mark a domain as hosted externally
- Remote wiping of mobile devices

- Support for auto-discovery
- Scheduling Assistant support in Outlook for Mac (and future Outlook versions that support EWS)
- Advanced collaboration: shared calendars, contacts, tasks and notes
- LDAP support
- Message prioritization and throttling
- Active directory authentication
- Email and chat archiving for SOX, HIPAA or other regulatory requirements
- Over-the-air synchronization for Android, BlackBerry, iPhone and Windows Phones
- Two-way synchronization for Microsoft Outlook
- Mailing list management functions
- Custom and emailed reports
- The ability to purchase and integrate one, or all, of the following licensed add-ons:
 - Microsoft Exchange ActiveSync for mobile and desktop (Outlook 13) synchronization
 - Microsoft Exchange Web Services for Apple desktop client synchronization (Outlook 11 for Mac, Apple Mail)

SmarterMail Free

SmarterMail Free contains much of the same functionality as SmarterMail Enterprise, but is limited to one domain with up to 10 users. This is to give you an opportunity to try all of the features out before making a decision on what product to purchase.

SmarterMail Edition Comparison

You can also refer to the following edition comparison chart for more information about each edition.

Features	1 Free	Pro	Enterprise
Migration and Converters			
Mail server converters for a wide variety of competitors	•	•	•
Mailbox migration for email, calendar, contacts and tasks	•	•	•
Automation (Web Services/ SOAP)			
Compatible with wide variety of control panel companies	•	•	•
Add/edit domains and users	•	•	•

Add/edit calendars, tasks and notes	•	•	•
Add/edit RSS feeds	•	•	•
Retrieve user and domain statistics via Web services 2	•	•	•
Collaboration			
SyncML support	•		•
Exchange ActiveSync support			Add-on
CalDAV and CardDAV support	•		•
Exchange Web Services support			Add-on
Outlook Scheduling Assistant support (requires Exchange Web Services add-on)	•		•
Microsoft Outlook 2007 and higher (2-way) synchronization	•		•
Microsoft Outlook 2000 and higher synchronization	•		•
Mozilla Thunderbird and Lightning synchronization	•		•
Webmail reminders system	•	•	•
Webmail availability of attendees	•	•	•
Webmail personal contacts	•	•	•
Webmail personal calendars, tasks and notes	•	•	•
Shared calendars, contacts, tasks and notes	•		•
Instant Messaging			
Instant messaging server	•		•
Search, view and print archived chats	•		•
Compatible with XMPP-supported chat clients	•		•
Mail Server Protocols			
SMTP	•	•	•

IMAP4 and IMAP IDLE	•	•	•
POP3	•	•	•
LDAP	•		•
Message retrieval via POP and IMAP	•	•	•
Antispam Measures			
Message Sniffer		Add-on	Add-on
Cyren Premium Antispam		Add-on	Add-on
Incoming and outbound spam checking	•	•	•
Spam quarantine (outgoing messages only)	•	•	•
Spam checking on POP3 message retrieval	•	•	•
Outgoing spammer detection and limiting	•	•	•
SpamAssassin-based Pattern Matching Engine	•	•	•
Support for distributed SpamAssassin servers (Linux or Windows)	•	•	•
SPF record checking	•	•	•
RBL listing detection	•	•	•
Reverse DNS checking	•	•	•
Greylisting (based on IP, sender location, spam weight, etc.)	•	•	•
DKIM Mail Signing	•	•	•
Configurable spam weights for system, domain and users	•	•	•
Configurable spam headers	•	•	•
Trusted senders	•	•	•
Requiring SMTP authentication for outgoing messages	•	•	•
Support for Declute	•	•	•
Antivirus			

Cyren Zero-hour Antivirus		Add-on	Add-on
Out-of-the-box ClamAV	•	•	•
Support for third-party real-time antivirus solutions	•	•	•
Support for third-party command-line antivirus solutions	•	•	•
Support for a remote ClamAV server (Linux or Windows)	•	•	•
Virus quarantine (outgoing messages only)	•	•	•
Security/Attack Prevention			
Incoming and outgoing TLS	•	•	•
Incoming and outgoing SSL	•	•	•
Active Directory Authentication (ADX)	•		•
Optional alternate SMTP port	•	•	•
SMTP authentication by domain	•	•	•
Restrict administrator access via IP	•	•	•
Brute force detection for Webmail	•	•	•
Manual and automatic IP whitelisting/blacklisting	•	•	•
Automatic harvest attack prevention	•	•	•
Automatic denial of service prevention	•	•	•
Malicious script filtering in webmail	•	•	•
Throttle user and domain activity	•		•
Throttle incoming bounces to prevent saturation	•		•
Reporting			

Real-time performance dashboards (traffic stats)	•	•	•
Basic reports (disk usage, file storage, etc.)	•	•	•
Advanced summary/trend reports (connections, traffic, spam, virus, etc.)	•	•	•
Data drill down for summary reports	•	•	•
Define custom reports	•		•
Scheduled and on-demand email reports	•		•
Reporting statistics exposed as PerfMon counters	•		•
Export reports to CSV and tab formats	•	•	•
Events and Notifications			
Event-driven architecture	•	•	•
Notification profiles	•	•	•
Configurable system, domain and user events	•	•	•
Assign actions to events (e.g. command-line, notifications, etc.)	•	•	•
Default notification to all users when disk quotas are reached	•	•	•
Message Archiving			
Sarbanes-Oxley compliance 3	•		•
Enable message archiving by domain	•		•
Messages .ZIP compressed to reduce space necessary	•		•
Search, view and print archived messages	•		•
Messages stored in .EML format	•		•

Administration			
Mark a domain as hosted externally	•		•
Remote wipe of mobile devices (requires Exchange ActiveSync add-on)			•
Support for auto-discovery (requires Exchange ActiveSync add-on)			•
Failover functionality			•
Administration from a Web browser	•	•	•
Custom skinning	•	•	•
White labeling	•	•	•
Multiple system administrator accounts	•	•	•
Review and download log files from interface	•	•	•
Users can be limited to specific protocols (IMAP, POP, SMTP)	•	•	•
Mass propagation of settings for domains/users	•	•	•
Mass messaging to some or all users and domain administrators	•	•	•
Prioritize SMTP based on message type, domain or user	•		•
Spool functionality that allows third-party integration	•	•	•
Configurable outbound SMTP IP addresses	•	•	•
Multiple spools (smart spooling)	•	•	•
Manage all connections	•	•	•
Manage current blocks	•	•	•

Immediate blacklisting of connections and sessions	•	•	•
Configurable user password strength requirements	•	•	•
Configurable user settings by domain	•	•	•
Configurable logging for all protocols	•	•	•
Password compliance reporting and enforcement	•	•	•
Folder auto-clean to enforce user quotas	•	•	•
Domain-wide and system-wide footers	•	•	•
SmarterMail search indexing	•	•	•
Web Interface (Webmail)			
Multi-language compatible	•	•	•
Optimized AJAX controls provide desktop application performance	•	•	•
Compatible with most tablets (iPad, Nexus 7, etc.)	•	•	•
Preview message attachments	•	•	•
New message notifications from anywhere in interface	•	•	•
Thumbnails for image file attachments	•	•	•
Download all attachments as .ZIP	•	•	•
Upload attachments in the background	•	•	•
File storage	•	•	•
Automatic save as draft	•	•	•
Click-to-map, click-to-call and click-to-mail functionality	•	•	•
Follow-up flagging	•	•	•

Linked emails and tasks	•	•	•
Advanced content filtering	•	•	•
Advanced spam filtering rules	•	•	•
User-level auto-clean	•	•	•
Spell-check in 17 languages	•	•	•
Email address auto-complete similar to Microsoft Outlook	•	•	•
Import and export contacts	•	•	•
Support for user and domain aliases	•	•	•
Multiple signatures support	•	•	•
Multiple identity/SMTP support	•	•	•
Mobile Smartphone Interface			
Low bandwidth interface for Smartphones (iPhone, Android, etc.)	•	•	•
Mailing Lists			
Bounce detection	•	•	•
Automatic removal of subscribers on bounces	•	•	•
Optional double opt-in	•	•	•
Subscriber custom fields	•	•	•
Friendly unsubscribe links in messages	•	•	•
Common subscriber database for all mailing lists	•	•	•
Merge variables and custom fields into messages (mail merge)	•	•	•
Toggle auto-generated response to mailing list commands	•	•	•

Enhanced mailing list compose with attachments	•	•	•
Customized command messages	•	•	•
Mail logging per subscriber	•	•	•
Message prioritization of mailing list	•		•
Throttling of mailing lists	•		•
Gateways			
Use as SmartHost or incoming gateway	•	•	•
Use as backup MX server	•	•	•
Use as outgoing gateway	•	•	•
User authentication and SSL/TLS support for outgoing gateways	•	•	•
Gateway authentication with other SmarterMail servers	•	•	•
Gateway can have domain exceptions	•	•	•
Spam checking available on gateways	•	•	•
Greylisting available on gateways	•	•	•

1 SmarterMail Free contains much of the same functionality as SmarterMail Enterprise, but is limited to one domain with up to 10 users. This is to give you an opportunity to try all of the features out before making a decision on what product to purchase.

2 For more information about using Web services with SmarterMail, see Automation with Web Services .

3 Consult your compliance professional to determine applicability to your organization.

For further assistance choosing the right edition, please contact the sales department by emailing sales@smartertools.com . During business hours you can also start a live chat or call us at 1.877.357.6278.

Mail Server Competitor Comparison

Pricing and features are taken directly from related websites, customer support, and marketing materials as of March 1, 2013, unless otherwise noted. Information, features and pricing are subject to change. To report corrections, please contact the sales department by emailing sales@smartertools.com. During business hours you can also start a live chat or call us at 1.877.357.6278. For a more detailed comparison of SmarterMail and Microsoft Exchange, see SmarterMail and Microsoft Exchange: An Administrative Comparison

Features	MDaemon Pro	Mailsite Fusion SE	IMail Premium	Icewarp Enterprise	Kerio Connect	Exchange 2010 Enterprise	SmarterMail Enterprise
Initial cost for 500 mailboxes	\$1,510	\$2,000	\$1,795	\$2,180 1	\$13,830	\$57,970 2	\$699
Over-the-air iPhone sync	•	\$2,000 3	\$249	•	•	•	•
Over-the-air BlackBerry sync	•	•	•	•	•		
Over-the-air Windows Mobile sync	•	•	•	•	•		
Exchange ActiveSync (50 mailboxes)	–	\$469	•	•	\$349		
Microsoft Outlook sync	\$2,400	•	•	\$4,859	•	•	•
Exchange Web Services	–	–	–	–	–	•	\$149
Webmail interface with collaboration	•	•	•	\$744	•	•	•
Instant messaging server	•	–	•	\$744	–	•	•

FTP server	–	–	–	•	–	–	–
SIP server	–	–	–	\$79	–	–	–
SMS server	–	–	–	\$79	–	•	–
Events & notifications system	–	–	–	–	–	–	•
SyncML synchronization	•	–	–	\$3,239	–	–	•
Antivirus	•	\$2,000	•	•	\$1,500	–	•
Antispam	•	\$2,000	–	•	•	–	•
Premium antivirus	\$1,035	–	\$1,629	\$839	–	• 4	\$349
Premium antispam	–	\$1,200	\$1,509	–	• 5	\$349	
Intrusion detection system	•	–	–	•	–	–	•
Message archiving	•	•	\$4,480	•	•	•	•
File storage	–	–	–	–	–	Available 6	•
Upgrade protection (12 months)	•	•	•	–	•	\$1,985	•
Business hour support	\$650	•	•	•	•	Available 7	• 8
Emergency support (24/7/365)	–	\$995	\$999	–	–	Available 9	\$349 10
Total Cost	\$5,595	\$8,995	\$10,352	11 \$14,240	\$15,330	\$59,995	\$2,644

1 Icewarp pricing based on the cost of 450 mailboxes as of March 3, 2011, as pricing information is no longer available directly from their website.

2 Exchange 2010 Enterprise pricing as of March 3, 2011, as pricing information is not available on the Microsoft website, and includes Enterprise Client Access Licenses (CALs) for 500 users.

3 Exchange ActiveSync license required for every mailbox.

4 Included with Enterprise CAL.

5 Included with Enterprise CAL.

6 Available with the inclusion of Sharepoint Server at an extra charge (licensing varies).

7 Available at a substantial extra charge.

8 SmarterTools provides two email support incidents with every purchase.

9 Available at a substantial extra charge.

10 Emergency support is available if needed and is part of the Platinum Support Package. More information about our support packages can be found on the Support page of the SmarterTools website.

11 Icewarp provides 30 GroupWare, 30 instant messaging, 30 SIP, 30 SMS, 5 Outlook connectors, 5 SyncML, 5 desktop client and 5 Exchange ActiveSync licenses at no cost by deducting \$628 from the total cost at checkout. This discount is reflected in the product's total cost in the chart above.

How SmarterMail Works

There are three main components that work together within SmarterMail: the Web interface (and a complementary mobile interface for smartphones), the Windows Service, and the SmarterMail web server.

Web Interface

From an administration standpoint, the Web interface can be used by both system admins and domain admins to manage all functions of the entire mail server as well as individual domains and user accounts. In addition, it offers end users a versatile, yet light weight, method of accessing their mailboxes, calendars, contacts and more using any standard Web browser. Note: In addition to using the Web interface, end users are able to use a desktop application such as Outlook, Apple Mail, Thunderbird, etc.

SmarterMail also provides a mobile interface that was designed specifically for smartphones. This is a light, yet fully functional interface that allows SmarterMail users to access their email, contacts, calendars, tasks and notes regardless of their location and connection speed.

Windows Service

The SmarterMail Service is the backbone of SmarterMail. Running as a Windows Service, it controls data storage and retrieval, protocol services, and administrative functions. SmarterMail will not function without this service installed and running.

SmarterMail Web Server

The SmarterMail web server installs automatically as part of the standard installation process. This web server gives users and administrators access to the SmarterMail web interface from the Internet by utilizing the IP address assigned to the local machine. NOTE: After installing SmarterMail, it is recommended that the web interface be moved from the SmarterMail web server to Microsoft IIS (if available) for more stability and security. For step-by-step instructions on how to make SmarterMail run under IIS, see [Running as an IIS Site](#).

Installation and Deployment

Browser Requirements

Desktop

SmarterMail is fully supported by the desktop browsers below.

- Google Chrome 10 and higher
- FireFox 3.6 and higher
- Safari 3 and higher
- Opera 10 and higher
- Internet Explorer 8* and higher

Mobile

With regards to mobile browsers, the SmarterMail webmail interface works well on most major browsers available for tablets and other larger-format mobile devices (e.g., tablets and "phablets" that use mobile browsers) as long as they support CSS, JavaScript and other modern scripting platforms.

Smartphone users should use the mobile interface SmarterMail provides as it is better suited for smaller screens and resolutions. For information on the SmarterMail mobile interface for smartphones, see the mobile support outlined on the jQuery mobile framework website.

* While SmarterMail will work with IE 8, it is strongly recommended that anyone using IE 8 upgrade to at least IE 9 to ensure all SmarterMail functionality works and that the interface performs as expected. IE 8 is now a legacy product and Microsoft is no longer supporting it.

SmarterMail System Requirements

SmarterMail was designed to operate efficiently with multiple applications on the same server, based on the following system requirements:

- Windows Server 2008 R2 64-bit or higher
- Microsoft .NET 4.5 Framework
- Dedicated IP Address
- Active internet connection
- Microsoft Internet Information Server (IIS)*
- Minimal IIS Settings
- Application Development Features

- .NET Extensibility
- ASP.NET
- ISAPI Extensions
- ISAPI Filters
- Common HTTP Features
 - Default Documents
 - Directory Browsing
 - HTTP Errors
 - Static Content
 - Health and Diagnostics
- HTTP Logging
- Request Monitor
- Performance Features
- Static Content Compression
- Security
- Request Filtering

Can SmarterMail Be Installed on Amazon's EC2 Platform?

To put it simply, yes. However, Amazon's EC2 platform, and other cloud providers, have some things to consider when determining how well any mail server will run. For example, some cloud services rotate the IP addresses that are used, which can cause issues with items like DNS records and affect mail delivery. Some have issues with disk I/O or have various other issues that adversely affect SmarterMail's performance. Therefore, while you can install SmarterMail on a cloud service such as Amazon's EC2, it is not necessarily recommended.

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.

*SmarterMail includes a basic Web server, so the product is fully functional upon installation, even without the existence of IIS or other Web servers. However, SmarterTools recommends installing Microsoft IIS 7.5+ in place of the SmarterMail Web server for increased performance and security. For more information, see the SmarterTools Knowledge Base .

Installation

SmarterMail comes as a single installation file that contains everything necessary to run the product. The SmarterMail installer can be downloaded from the SmarterTools website . 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. The features available to you, and the edition that eventually runs, is determined by the license key you enter.

Please refer to the KB article [How To Install SmarterMail](#) for step-by-step installation instructions. You may also want to review the KB article on how to [Activate SmarterMail](#) .

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, please refer to the KB article [How To Set up SmarterMail as an IIS Site \(IIS 7.0\)](#) or [How To Set up SmarterMail as an IIS Site \(IIS 6.0\)](#) .

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 \(IIS 7.0\)](#) or [How To Set Up SmarterMail as a Virtual Directory Under an Existing IIS Site \(IIS 6.0\)](#) .

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. It should also be noted that the chat feature will not work with the default Web server.

Activating SmarterMail

In order for SmarterMail to function for more than a single domain and 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 many 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 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 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](#).

Configuring SmarterMail for Failover

Who Should Use This

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

Failover Overview

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

Understanding How Failover Works

The main components of failover functionality are a primary server that acts as the default SmarterMail server and manages the licensing of the server cluster and a secondary server that

remains connected and available in a “hot standby” mode until the primary server experiences problems with network access or system hardware.

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

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

Minimal System Requirements

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

Adding Network Load Balancing to Your Servers

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

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

Configuring the Load Balanced Cluster for Use with Failover

- Navigate to Start -> Administrative Tools -> Network Load Balancing Manager
- Click the Cluster menu item and select New
- In the New Cluster: Connect window, type the IP of your primary server in the Host: text box and select New
- When the Interface Name and Interface IP appear, select the Interface Name and click Next
- Since this is the primary node, ensure the host Priority is set to 1
- In the New Cluster: Host Parameters window, confirm the IP address and Subnet mask are

correct and change the initial host state to Stopped . This is to prevent any issues with connectivity if a machine randomly reboots or suffers from a hardware failure. If all nodes are set to Started for their initial host state, traffic will be split between the two (or more) machines. Note: Monitoring software can be used to execute scripts that will start and stop hot standbys in the event of a failure and recovery. If you are not executing scripts via monitoring software then all failover will need to be handled manually.

- Click Next
- In the New Cluster: Cluster IP Addresses window, click Add and enter in your cluster IP address and the same subnet mask as in Step 6
- Select Next
- In the New Cluster: Cluster Parameters window, confirm the IP address and subnet mask, then enter a Full Internet Name , though this is optional
- Ensure the cluster operation mode is set to Multicast
- Click Next
- In the New Cluster: Port Rules window, click Edit
 - If you want you can restrict the cluster IP to work on an individual port or across a port range. You can also simply allow the cluster IP to work across all ports on the server
- Ensure your port rules are set to Single Host in the Filtering Mode section
- Click OK
- Verify your settings and click Finish to complete the setup

Joining Additional Nodes to the Cluster

- From the secondary server navigate to Start -> Administrative Tools -> Network Load Balancing Manager
- Click the Cluster menu item and select Connect to Existing . Note: the existing cluster will need to be running before a secondary node can be added
- In the Connect to Existing: Connect window, enter the IP address of your existing cluster as the Host and click Connect
- Select the existing cluster that appears in the Clusters section and click Finish
- In the main Network Load Balancing Manager , expand Network Load Balancing Clusters and right click on your Cluster (it may be the IP address of your cluster) and select Add Host to Cluster
- In the Add Host to Cluster: Connect window, enter the IP address of the secondary server in the Host: section and click Connect
- When the Interface Name and Interface IP appear, select the Interface Name and click Next
- In the Add Host to Cluster: Host Parameters window, confirm the IP address and subnet mask and ensure the Initial Host State is set to Stopped . As this is the second node you're adding to

your cluster, the Priority should be set at 2

- Click Next
- Just as with the primary node, in the Add Host to Cluster: Port Rules window you have the ability to set this node to respond via specific ports or a port range. If you wish to set these rules, click Edit . Otherwise, click Finish to complete the setup
- Wait for the nodes to converge and, if necessary, stop the secondary sever by right clicking the second server's name, select Control Host -> Stop

Configure a Shared Service Directory

- Using Network File Sharing (NFS) or Samba (SMB), create a shared directory named SmarterMail , preferably on a NAS or SAN. NOTE: We recommend that this shared directory be hosted on a server that utilizes a RAID 10 configuration for the data.
 - Inside that new SmarterMail folder, create a Service folder
 - Configure your permissions accordingly. If special permissions are required, configure the SmarterMail service to run with the proper credentials within the Windows Services console.
- Note: When performing updates to the software, the credentials will need to be re-applied to the service

Configuring a Fresh Installation of SmarterMail for Failover

- Install SmarterMail Enterprise on a server. This will be your hot standby. Leave all setup information as the default settings and after setup is complete, configure SmarterMail as an IIS site.
- Stop the SmarterMail service on the hot standby
- Edit the failoverConfig.xml file in the primary server's Service folder as follows:

 - SharedSystemFilePath - Set to the shared network shared system folder
 - FailoverIPAddress - Set this to the IP address of the Network Load Balancer
 - IsEnabled - Set this to True
 - Save this file, then copy it to the hot standby's Service folder and replace the existing failoverConfig.xml
 - Copy over all folders, DAT and XML files from C:\Program Files (x86)\SmarterTools\SmarterMail\Service to the Service folder in the shared service directory you created
 - Start the service on the hot standby server and verify that the paths are pointing to the network shared paths
 - Activate your Enterprise key on the hot standby by logging into SmarterMail's management interface as the system admin and going to Settings -> Activation -> Licensing , then stop the SmarterMail service on the server

- Start the service on the primary server, then reactivate your Enterprise license key in the SmarterMail management interface
- After re-activating the license, go to Settings -> Bindings -> IP Address and bind all the ports to the load balancer's IP address and make sure no other IPs have any ports bound to them
- Both servers are now set up for failover. To verify this, when logged into the primary server as the system admin, go to Settings -> Failover Servers to view the servers that are part of the failover cluster

Adding Failover to an Existing Installation of SmarterMail

Note: You will need to configure both servers for Network Load Balancing and set up a shared service directory. See the steps outlined in the Adding Network Load Balancing to Your Servers , Configuring the Load Balanced Cluster for Use with Failover , Joining Additional Nodes to the Cluster and Configure a Shared Service Directory sections earlier in this document for more information.

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

 - SharedSystemFilePath - Set to the shared network shared system folder
 - FailoverIPAddress - Set this to the IP address of the Network Load Balancer
 - IsEnabled - Set this to True
 - Run the robocopy one more time to copy over any modified files and remaining spool e-mails
 - Copy over all folders, DAT and XML files from C:\Program Files (x86)\SmarterTools\SmarterMail\Service to the Service folder in the shared service directory you created
 - Edit the domainlist.xml file in the shared Service folder and change the path of your domains to match the new NFS\SMB path. (For example, \\NAS01\SmarterMail\Domains\mydomain.com)
 - Edit the mailconfig.xml file and replace any instances of the old physical path's with your new network location for SmarterMail. (For example, if all of your data was hosted on

E:\Smartermail, you would then perform a find and replace for all instances of E:\Smartermail to \\NAS01\Smartermail).

- On the primary server, go to Start -> Administrative Tools -> Network Load Balancing Manager and stop the cluster node, then start the NLB on the secondary node
- Start the SmarterMail service on the hot standby
- Access SmarterMail's web interface at the cluster IP and sign in as the system admin
- Activate your Enterprise key on the hot standby by going to Settings -> Activation -> Licensing
- Verify that the data and settings are being picked up from the shared Service directory
- Stop the SmarterMail service on the hot standby and stop the secondary cluster node
- Start the cluster node and the SmarterMail service on the primary server
- Sign into the web interface on the primary server and re-activate the Enterprise license key by going to Settings -> Activation -> Licensing
- Verify mail data and settings are being accessed from the shared service directory

Scripting Failover

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

Prepping PowerShell on the Servers

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

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

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

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

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

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

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

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

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

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

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:

- Microsoft Exchange ActiveSync
- Exchange Web Services
- Message Sniffer
- Cyren Premium Antispam
- Cyren 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 Android, Blackberry, iOS and Windows Phone devices. In addition, Exchange ActiveSync enables SmarterMail users to have access

their email, calendars, tasks, and notes while working offline. Finally, Outlook 2013 for Windows also supports EAS for syncing mail, contacts and calendars.

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

Exchange Web Services

Exchange Web Services (EWS) seamlessly syncs SmarterMail messages, contacts, calendars and tasks to third-party email clients, including Microsoft Outlook 2015 for Mac from Office 365, Microsoft Outlook 2011 for Mac, Apple Mail, the Outlook client for iPad and eM Client. Exchange Web Services will eventually replace the outdated MAPI protocol, as EWS allows for faster communication between an email client and the mail server.

For step-by-step instructions on how to activate the EWS add-on, please refer to the KB article [Activate Exchange Web Services](#).

Message Sniffer

Message Sniffer complements SmarterMail's built-in antispam and antivirus features and accurately captures more than 99% of spam, viruses, and malware right out of the box. It learns about your environment automatically to optimize its performance and accuracy without your intervention; and it can be easily customized to meet your requirements. Because Message Sniffer runs all of its signatures locally, it doesn't need to communicate with any services outside of the mail server, making it quicker and more efficient. Furthermore, the database is regularly and automatically updated to protect against new spam and malware attacks.

For step-by-step instructions on how to activate and enable the Message Sniffer add-on, please refer to the KB articles [Activate Message Sniffer](#) and [Enable Message Sniffer](#).

Cyren Premium Antispam

The Cyren Premium Antispam add-on is a service that 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 Cyren 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 Cyren add-on, please refer to the KB articles [Activate Cyren Premium Antispam](#) and [Enable Cyren Premium Antispam](#).

Cyren Zero-hour Antivirus

The Cyren Zero-hour Antivirus add-on is a service that 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 Cyren add-on, please refer to the KB articles [Activate Cyren Zero-hour Antivirus](#) and [Enable Cyren Zero-hour Antivirus](#).

Antispam and Antivirus Integration

Powerful antispam and antivirus functionality is included with every copy of SmarterMail. However, some users may need extra protection or have fixed infrastructures. The solutions listed on this page have been tested with SmarterMail, but you can integrate almost any command-line scanner or real-time scanner with SmarterMail.

Message Sniffer

Message Sniffer complements SmarterMail's built-in antispam and antivirus features and accurately captures more than 99% of spam, viruses, and malware right out of the box. It learns about your environment automatically to optimize its performance and accuracy without your intervention; and it can be easily customized to meet your requirements. Because Message Sniffer runs all of its signatures locally, it doesn't need to communicate with any services outside of the mail server, making it quicker and more efficient. Furthermore, the database is regularly and automatically updated to protect against new spam and malware attacks. The Message Sniffer solution is available as an integrated add-on to SmarterMail from the SmarterTools website and authorized SmarterTools resellers.

- [Learn more](#)
- [Buy now](#)

Cyren Premium Antispam

When coupled with SmarterMail, Cyren Premium Spam protection delivers upwards of 99% spam protection. Cyren technology complements SmarterMail's out-of-the-box antispam features by adding email transmission pattern recognition. The Cyren Premium Antispam solution is available as an optional add-on to SmarterMail from the SmarterTools website and authorized SmarterTools resellers.

- [Learn more](#)
- [Buy now](#)

Cyren Zero-hour Antivirus

The Cyren Zero-hour Antivirus uses Recurrent Pattern Detection to identify viruses based on their unique distribution patterns and provides a complementary shield to conventional AV technology. The Cyren Zero-hour Antivirus is available as an optional add-on to SmarterMail through the SmarterTools website and authorized SmarterTools resellers.

- [Learn more](#)
- [Buy now](#)

Barracuda Networks Inc.

Barracuda Networks Inc. is the worldwide leader in email and Web security appliances. Barracuda Networks also provides world-class IM protection, application server load balancing, and message archiving appliances. More than 50,000 companies are protecting their networks with Barracuda Networks' comprehensive solutions. For integration instructions, please search the SmarterTools Knowledge Base .

- [Learn more](#)

ClamAV

ClamAV is an open-source project that provides mail servers with decent protection from viruses at no cost. SmarterTools has found ClamAV to be a valuable scanner to use, especially in lower-volume environments. For integration instructions, please search the SmarterTools Knowledge Base .

- [Learn more](#)

Declude

Declude is a third-party product that fills the role of antivirus, antispam, and e-mail threat elimination. Declude offers complete integration with SmarterMail and has been optimized for high-load environments. Declude can use multiple scanners, reducing your exposure to new virus outbreaks.
Note: As of July, 2013, the property rights and assets for the Declude product were purchased by, and are currently supported and managed by, Mail's Best Friend.

- [Learn more](#)

F-Prot

F-Prot, made by Frisk Software International, is a low-cost but effective solution that works well on low to medium volume environments. For integration instructions, please search the SmarterTools Knowledge Base .

- Learn more

Trend Micro OfficeScan/Server Suite, Trend Micro ServerProtect

Trend Micro provides quality email scanning at a fraction of the price of comparable solutions. OfficeScan is built for enterprise environments and includes support for scanning non-Windows machines and an optional spyware blocker. For integration instructions, please search the SmarterTools Knowledge Base .

- Learn more

Trend Micro Client/Server Suite for SMB

Trend Micro products get our recommendation for quality email scanning at a fraction of the price of comparable solutions. Protect your whole small or medium-sized business with one product. For integration instructions, please search the SmarterTools Knowledge Base .

- Learn more

Control Panels

SmarterTools has spent considerable effort into providing a solid Web services implementation in its products in order to facilitate automation systems. As a result, more and more control panel providers are finding it easy to tie our products into their interfaces.

Odin Automation

The integration of SmarterMail with Odin Automation is fully embedded within the Odin Automation product. Just download the APS package from within the Odin app portal.

- Learn more

Odin Plesk Panel (7.5 or higher)

The integration of SmarterMail with Plesk is fully embedded within the Plesk product. No additional downloads are necessary to complete the integration.

- Learn more

WebSitePanel

The integration of SmarterMail with WebSitePanel is fully embedded within the WebSitePanel product. No additional downloads are necessary to complete the integration.

- Learn more

WHMCS

The integration of SmarterMail with WHMCS is available as a free add-on, which can be downloaded from the WHMCS App Store. Two modules are available: an admin area module for basic SmarterMail management, and a provisioning module that allows for multiple SmarterMail servers, adding domains, webmail log in and more.

- [Learn more](#)

Helm (part of the Plesk family)

The integration of SmarterMail with Helm is fully embedded within the Helm product. No additional downloads are necessary to complete the integration.

- [Learn more](#)

HostingController

The integration of SmarterMail with HostingController is fully embedded within the HostingController product. No additional downloads are necessary to complete the integration.

- [Learn more](#)

Automation with Web Services

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

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

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

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 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 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.

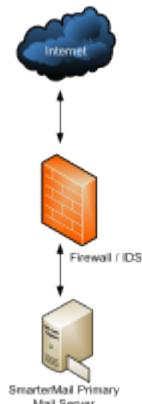
- High-volume deployments shall include ISPs, hosting companies, large businesses, and enterprise organizations with average email volumes numbering in the millions. This infers organizations with many thousands of mailboxes. Information regarding these architectures can be found in SmarterMail in High-Volume 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
- Windows Server 2008 R2 64-bit
- 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 95% 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.

Message Sniffer

Available as an optional add-on for SmarterMail, Message Sniffer complements SmarterMail's built-in antispam and antivirus features and accurately captures more than 99% of spam, viruses, and malware right out of the box. It learns about your environment automatically to optimize its performance and accuracy without your intervention; and it can be easily customized to meet your requirements. Because Message Sniffer runs all of its signatures locally, it doesn't need to communicate with any services outside of the mail server, making it quicker and more efficient. Furthermore, the database is regularly and automatically updated to protect against new spam and malware attacks.

For more information about the Message Sniffer add-on, please visit the SmarterTools website.

Cyren Premium Antispam

Available as an optional add-on for SmarterMail, Cyren Premium Antispam uses Recurrent Pattern Detection (RPD) technology to protect against spam outbreaks in real time. Rather than evaluating the content of messages, the Cyren 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 Cyren Premium Antispam add-on can effectively block 99% of spam from users' inboxes.

For more information about the Cyren 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, DKIM, 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 with a spam score that can be used to filter mail alone or in conjunction with other spam filtering options in SmarterMail.

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 download 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.

Cyren Zero-hour Antivirus

Available as an optional add-on for SmarterMail, Cyren Zero-hour Antivirus can further extend SmarterMail's built-in virus protection measures. Rather than depending on heuristics, Cyren 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 Cyren 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 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 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.

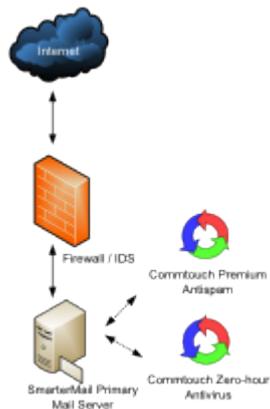
- Small to medium-sized businesses shall be defined as mail environments with average email volumes of up to 400,000 messages per day (200,000 in/200,000 out). This infers a maximum of 1,600 mailboxes. Information regarding these architectures is available in this SmarterTools document.
- High-volume 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 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 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
- 2 GB of RAM
- Windows Server 2008 R2 64-bit
- 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.

Message Sniffer

Available as an optional add-on for SmarterMail, Message Sniffer complements SmarterMail's built-in antispam and antivirus features and accurately captures more than 99% of spam, viruses, and malware right out of the box. It learns about your environment automatically to optimize its performance and accuracy without your intervention; and it can be easily customized to meet your requirements. Because Message Sniffer runs all of its signatures locally, it doesn't need to

communicate with any services outside of the mail server, making it quicker and more efficient. Furthermore, the database is regularly and automatically updated to protect against new spam and malware attacks.

For more information about the Message Sniffer add-on, please visit the SmarterTools website.

Cyren Premium Antispam

Available as an optional add-on for SmarterMail, Cyren Premium Antispam uses recurrent pattern detection (RPD) technology to protect against spam outbreaks in real time. Rather than evaluating the content of messages, the Cyren 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 Cyren Premium Antispam add-on can effectively block 99% of spam from users' inboxes.

For more information about the Cyren 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, DKIM, 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 includes support for SpamAssassin, an open source spam filtering program. When implemented, SmarterMail will pass an incoming message to SpamAssassin. SpamAssassin returns the message with a spam score that can be used to filter mail alone or in conjunction with the other spam filtering options in SmarterMail.

The Windows version is limited to processing a single message at a time, effectively handling approximately 25,000 spam messages per day and is 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>.

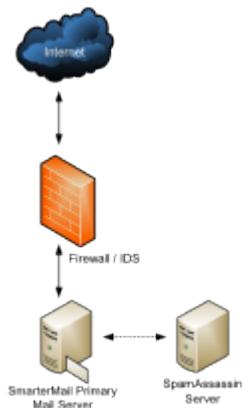
SmarterTools recommends the following hardware for stand-alone, distributed SpamAssassin servers:

- 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.

Cyren Zero-hour Antivirus

Available as an optional add-on for SmarterMail, Cyren Zero-hour Antivirus can further extend SmarterMail's built-in virus protection measures. Rather than depending on heuristics, Cyren 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 Cyren 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.

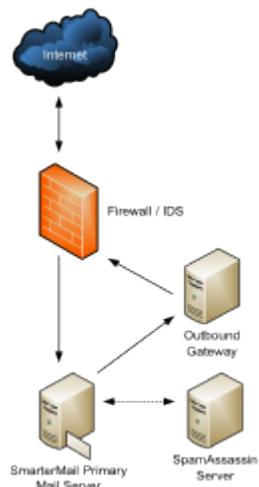
Most small to medium-sized business environments will not need an outbound gateway. However, as a business grows, the addition of an outbound gateway can add significant capacity to a mail network and smooth the transition to higher volumes and larger networks. In the opinion of the authors, a

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
- Postini: 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.

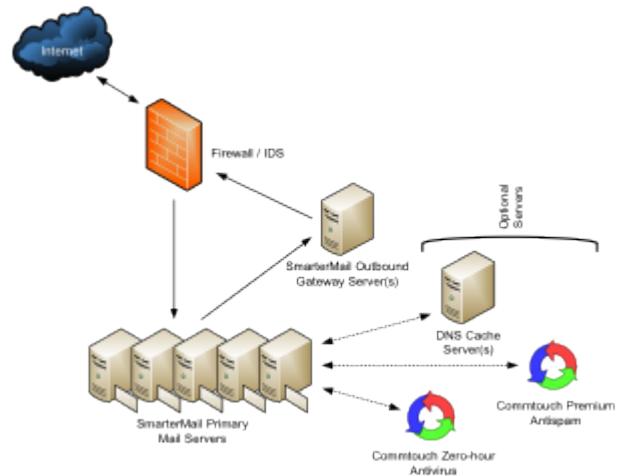
That said, the authors have chosen to divide their recommendations into three categories: individual

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 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 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 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
- Windows Server 2008 R2 64-bit
- 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.

Configuring SmarterMail for Failover

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

communicate and that productivity remains at the highest levels possible, even if there is a primary server failure.

For more information on configuring failover, see the Configuring SmarterMail for Failover section of the online help.

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.

Message Sniffer

Available as an optional add-on for SmarterMail, Message Sniffer complements SmarterMail's built-in antispam and antivirus features and accurately captures more than 99% of spam, viruses, and malware right out of the box. It learns about your environment automatically to optimize its performance and accuracy without your intervention; and it can be easily customized to meet your requirements. Because Message Sniffer runs all of its signatures locally, it doesn't need to communicate with any services outside of the mail server, making it quicker and more efficient. Furthermore, the database is regularly and automatically updated to protect against new spam and malware attacks.

For more information about the Message Sniffer add-on, please visit the SmarterTools website.

Cyren Premium Antispam

Available as an optional add-on for SmarterMail, Cyren Premium Antispam uses Recurrent Pattern Detection (RPD) technology to protect against spam outbreaks in real time. Rather than evaluating the content of messages, the Cyren 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 Cyren Premium Antispam add-on can effectively block 99% of spam from users' inboxes.

For more information about the Cyren 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, DKIM, 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.

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.

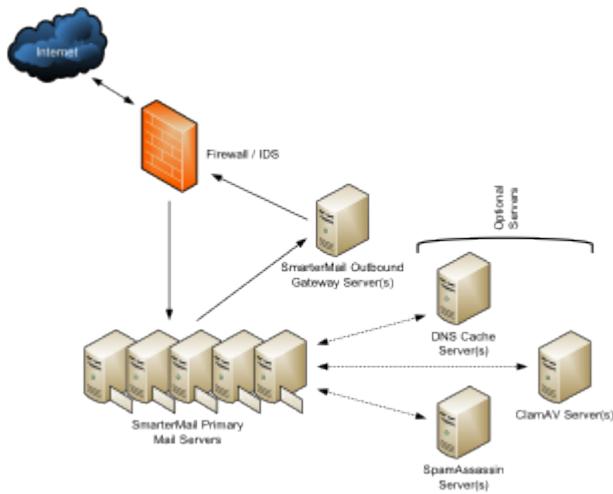
Cyren Zero-hour Antivirus

Available as an optional add-on for SmarterMail, Cyren Zero-hour Antivirus can further extend SmarterMail's built-in virus protection measures. Rather than depending on heuristics, Cyren 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 Cyren Zero-hour Antivirus 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 includes support for SpamAssassin, an open source spam filtering program. When implemented, SmarterMail will pass an incoming message to SpamAssassin. SpamAssassin returns the message with a spam score which can be used to filter mail alone or in conjunction the other spam filtering options in SmarterMail.

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 . .

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://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, 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.
- Postini: www.postini.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).

Integrations

Base WHMCS SmarterMail Provisioning Module

Package Description

The WHMCS SmarterMail module is an open source module developed in PHP that integrates SmarterMail as an add-on into WHMCS that can be attached to Product/Services to provision SmarterMail domains as well as point MX and CNAME records on WHM/CPANEL to a SmarterMail server using standard settings across all WHMCS users.

Package Goals

The primary goal of the WHMCS SmarterMail module was to reduce server administrator labor. Previously, MX and CNAME records would have to be entered manually, as well as the domain creation in SmarterMail. With the module installed, the whole process is automated. Not only is everything created for you on initialization, but also for suspension, deletion, un suspension, and termination.

The package provides the following services:

- Create, Suspend, UnSuspend, Terminate, and Delete Domains from a SmarterMail server using a standard set of defaults.
- Multiple SmarterMail Server Support with Management side interface for adding, deleting, suspending, unsuspending SmarterMail servers as well as setting max domain levels per server.
- Client side link to SmarterMail login.
- SSL support.

Prerequisites

- Existing installation of WHMCS (version 5.0 and above)
- Existing installation of WHM/CPanel
- Licensed installation of SmarterMail

Installing the SmarterMail Module

Installing the SmarterMail module is no different than installing any modules within WHMCS. Below are the steps necessary to get a SmarterMail installation added to WHMCS.

- Extract the SmarterMail module
- Place contents in your WHMCS directory under "..modules/addons/smartermail"
- Navigate to http://your_WHMCS_hostname.com/admin/configaddonmods.php
- Click "Activate" next to the SmarterMail Provisioning Module
- Go back to http://your_WHMCS_hostname.com/admin/configaddonmods.php
- Click "Add New Add On"
- Set desired add-on settings and make sure you attach to at least one product/service
- Next, find the Addon ID
- If this is the first add-on created in this WHMCS instance, then the ID will be 1.
- If there are multiple add-ons in WHMCS, you may need to look in the database to find out the SmarterMail add-on ID.
- To find the add-on ID in the database, use a MySQL database tool like MySQL Workbench
- Connect to your database and run the following query:

```
SELECT addontable.id FROM yourDatabaseName.tblAddons as addontable WHERE
addontable.name=yourAddonName Make sure you replace 'yourDatabaseName' with
the name of your database and 'yourAddonName' with the name of the add-on
you created in Steps 6 - 7.
```

- Go back to http://your_WHMCS_hostname.com/admin/configaddonmods.php
- Click "Configure" (it's to the right of "Activate")

- Fill in the Addon ID you found in Step 8
- Check "Module Logging" (you can turn this off later when everything is running smoothly or simply leave it running indefinitely)
- Check "SSL" if your WHMCS address begins with 'https://'
- If you want to give specific Roles the ability to modify the SmarterMail servers from within the management interface of WHMCS, select them from the list
- Click "Save Changes" and that's it! The SmarterMail module is installed and you can now configure SmarterMail servers

Configuring Servers

Once the SmarterMail module is installed, you can begin adding new mail servers to your WHMCS installation and begin provisioning domains and mailboxes within SmarterMail.

- Navigate to
[http\(s\)://your_WHMCS_hostname.com/admin/configaddonmods.php?module=smartermail](http(s)://your_WHMCS_hostname.com/admin/configaddonmods.php?module=smartermail)
- Here, you're presented with the SmarterMail server interface. This is where you create, suspend, set max domain counts and delete SmarterMail servers
- Click "New Server"
- Fill in the following settings:
 - Server Name - The friendly name for your SmarterMail server within WHMCS
 - Server URL - The domain name and URL of the server. (E.g., https://mail.YourDomain.com)
 - Domain Path - The path on the server where you store the Domain folders. (E.g., c:\\SmarterMail\\Domains)
 - Server Admin Username - The administrator username for this server
 - Server Admin Password - The password associated with the Server Admin Username
 - Max Domains - The maximum number of domains allowed on the server
 - Status - The status of the server. Note: Only "Active" servers will allow provisioning of domains
- Click "Submit" to create the new server
- You can now test provisioning domains and accounts in SmarterMail
- If you experience problems, and Module Logging is enabled, you can go to
[http\(s\)://your_WHMCS_hostname.com/admin/addonmodules.php?module=smartermail](http(s)://your_WHMCS_hostname.com/admin/addonmodules.php?module=smartermail) to check the error logs

WHMCS Product/Service Module

Package Description

The WHMCS SmarterMail module is an open source module developed in PHP that integrates SmarterMail as a Product\Service into WHMCS. This allows the ability to create packages based off of custom settings available within the SmarterMail software that can then be used by administrators to offer varying levels of SmarterMail access to end users. For example, the ability to create packages based off of mailbox counts, disk space allocations, etc. Additionally in the Client Area of WHMCS, the ability to manage SmarterMail has been added as well for end users.

Package Goals

The primary goal of the WHMCS server module is to give server administrators more flexibility in regards to how SmarterMail is offered as a service. With the use of this SmarterMail Server module, Product\Service items can be created specific to the SmarterMail settings. This means that WHMCS users can create custom packages, unique to users across the WHMCS install versus standard packages that are applied to all users. These customizable features include but not limited to: specifying the number of domain users, domain size limits, number of aliases, etc.

The package also provides the following services:

Admin Area Features

- Create Domain
- Suspend Domain
- Unsuspend Domain
- Terminate Domain
- Change Package
- Change Password

Client Area Features

- Manage Mailboxes
- Add Mailboxes
- Delete Mailboxes
- Modify Mailbox Settings
- Change Mailbox Password
- Manage User Aliases

- Add Aliases
- Delete Aliases
- Change Password

Prerequisites

- Existing installation of WHMCS (version 5.0 and above)
- Existing installation of WHM/CPanel
- Licensed installatino of SmarterMail (10.x and above)

Installing the SmarterMail Server Module

First the package will need to be installed in the WHMCS Control Panel. To do so, use the following instructions:

- Download ZIP package to your WHMCS server
- Navigate to `./modules/servers/` and create a folder called ‘smartermail’, all lower case
- Extract and upload contents of the zip file you downloaded into the smartermail folder you created

Configure WHMCS to Access and Group SmarterMail Servers

Once the SmarterMail package has been added, you now have the ability to configure the SmarterMail servers to be used. To configure the SmarterMail servers to be used, do the following:

- Login to WHMCS as a system administrator
- Click Setup → Products\Services → Servers
- Click add new server across the top
- Enter Server information for the SmarterMail server to be added
- Under Server Details, select the Type of ‘smartermail’ and enter system administrator credentials
- Save your changes

Once the server has been added, you then have the ability to create a group of SmarterMail servers.

- Click Create New Group across the top
- Enter a name for the group of SmarterMail servers, select and add your server that was recently added
- Save your changes

Configure Your Product/Service

Now that the package has been added and the SmarterMail servers have been configured, you now have the ability to configure individual Product\Service packages within WHMCS. To do so:

- Click Setup → Products\Services → Products\Services
- You have the option of creating a new product group if you see fit, otherwise click Create a new product
- Select product type, product group, and give product name
- Click continue
- Edit the various product tabs as you see fit such as details and pricing
- For the Module Settings Tab - Select Smartermail as the Module Name, and select the appropriate Server Group that was created earlier
- This will then allow you to configure data specific to the packages being created

WHMCS Client Area

The WHMCS SmarterMail module also allows WHMCS users to interact with their SmarterMail domain. Abilities include actions such as adding and editing both users as well as user aliases. To access this feature as a WHMCS end user:

Client Area To access SmarterMail through the client area:

- Click My Services → Product details
- Click Manage SmarterMail Users and Aliases
- You will find the option to add both users as well as aliases. Also the option to edit each of the corresponding items

Add User To add a user:

- Click Add SmarterMail User
- Enter requested information
- Click Create SmarterMail User

Edit User To edit a user:

- From the Manage SmarterMail Users page, select the user to edit, and click Edit SmarterMail User
- Change or update any of the specified fields for each user
- Also note the ability to change the status of an account or delete an account. NOTE: deleting the account is permanent

Add Alias To add an alias:

- Click Add SmarterMail Alias
- Enter name for alias
- Enter accounts the alias will send too
- Click Create SmarterMail Alias

Edit Alias To edit an alias:

- From the Manage SmarterMail Aliases page, select the alias to edit, and click Edit SmarterMail Alias
- Add or remove any email addresses that you'd like
- Also note the ability to delete an alias. NOTE: deleting the alias is permanent

Odin APS (Automated Provisioning System) Package for SmarterMail

Package Description

The SmarterMail APS package is designed to integrate SmarterTools' SmarterMail email server software within the Parallels Operations Automation system. SmarterMail can then be used as the mail server of choice for Odin administrators when creating hosting plans for resale, when adding domains that require email services and more.

Package Goals

The goal of the SmarterMail APS package was to provide a means of easily managing domains, mailboxes, mailings lists and aliases. To those ends, services provided include:

- Domain Services
- Add / Remove Domains
- Add / Edit / Remove Domain Aliases
- Add / Edit / Remove User Aliases
- Domain Disk Space Reporting
- Mailbox Services
- Add / Edit / Remove Mailboxes
- Configure Email Forwarding Settings
- Configure Auto-responder Settings
- Mail List Services

- Add / Edit / Remove Mailing Lists
- Add / Edit / Remove Mailing List Subscribers

Prerequisites

This goes over the list of requirements that are needed before installing, configuring and using the SmarterMail APS package. These requirements are as follows:

- Existing installation of Parallels Operations Automation (PoA)
- Existing, licensed installation of SmarterMail 9.x or above
- Required knowledge in the following areas:
 - Application Manager
 - APS catalog
 - Importing packages
 - Provisioning Manager
 - Resource templates
 - Service templates
 - Customer Manager
- Creating of customers
- System director
- Task manager

Installation

This covers getting the APS package set up with the PoA system. There are two ways to install the SmarterMail APS package within PoA using the Application Manager: from Applications or the APS Catalog

- Applications
 - Expand Service Director
 - Expand Application Manager
 - Select Applications
 - Click on “Import Package”
 - Select “local file” option and click “Choose File”
 - Provide the path to the SmarterMail APS
 - Check “Enabled” option

- Finally click “Submit” and the package will be scheduled for importing
- APS Catalog
 - Expand Service Director
 - Expand Application Manager
 - Select APS Catalog
- Select the “Application” field and search for ‘SmarterMail*’
- ‘SmarterMailAPS’ package should appear in the list
- Check the box next to the Application column and click “Import Package”
- On the next screen click “Import Packages” and the package will be scheduled for importing

Configuration

This covers the configuration of the SmarterMail APS package after it has been installed/imported into the PoA system.

Resource Types

Resource Types are used to define activation parameters, which are:

- General package settings
- Global settings
- Default settings
- Services

Creating an Application

The application resource is the crucial part of setting up the SmarterMail APS package. This defines the global settings that are used by each application service.

- Expand Service Director
- Expand Application Manager
- Select Applications
- Select the “Application” field and search for ‘SmarterMail*’
- The results should yield the ‘SmarterMailAPS’ package that was installed prior (where applicable)
- Select the ‘SmarterMailAPS’ package
- Click the “Resource Type” tab
- Click “Create”
- Select Application from the Resource Class list
- Give it a name (Ex: SmarterMail App) & Description, click “Next”
- Fill in the following fields under the “Global application settings” section:

- SmarterMail public site URL
- SmarterMail installation host
- SmarterMail installation IP
- Primary System Administrator Login
- Primary System Administrator Password
- Primary MX
- Click “Next”
- Uncheck “Automatically provision application,” click “Next”
- Check “External Provisioning,” click “Next”
- Click “Finish”

Creating an Application Service

The application service is what defines the defaults for each service that used by the SmarterMail APS package (domains, mailboxes, etc) .An application service will have to be created for each service that you want to provide.

- Navigate to the “Resource Types” section of the SmarterMail APS package. Follow the same steps when creating an application resource to get to this section.
- Click "Create"
- Select Application Service from the Resource Class List
- Give it a name (Ex: SmarterMail App Domain Service) & Description, click “Next”
- Select from the list of services the application service will be (Ex: SmarterMail Domain Service)
- Provide default values for this resource, then click “Next”
- Priority can be any number, so let's go with 1, Click “Next”
- Click “Finish”

Again, these steps must be repeated for each application service that is offered with the package.

Service Templates

This covers the creation of service templates for the package. A service template defines both subscription limits as well as what services are provided when using the package.

Creating a Service Template

- Expand Service Director
- Expand Provisioning Manager
- Select Service Templates
- Click “Add New Service Template”

- Provide a name & description
- Uncheck “Autoprovisioning”
- Set “Type” to Custom
- Click “Next”
- A list of available Resources will be shown
- Select the Resource Application that was created earlier as well as any of the Resource Application Services that were just created. For example, "SmarterMail App" and "SmarterMail App Domain Service"
- Click "Next"
- Set the limits of the service template
 - Check Unlimited for the Resource Application (Ex: SmarterMail App), Application Backup and Application User
 - Resource Application Services (Ex: SmarterMail App Domain Service) can be either set to unlimited or can have a limit applied to them
- Home Visibility is an optional field that can be checked, if desired, that provides usage information for the user when they log in
- Click "Next"
- Review your settings, then click "Finish"

Subscriptions

This covers the how to apply subscriptions to customers using the service template that was created early.

Creating a Subscription

- Expand Service Director
- Expand Provisioning Manager
- Select Service Templates
- Select the “Service Template” field and search for, then select, the service that was created prior
- Click “Activate” under the General section of the service template (the service template must be activated prior to adding a subscription)
- Click “Subscriptions” tab
- Click “Create New Subscription”
- Select the “Company” field and search for the company that will be subscribing to this template, then select the company from the search results
- Set additional resource limits for the subscription if desired (subscriptions will inherit the

values from the service template by default)

- Click “Next”
- Review the settings and click “Finish”

The company selected now has the ability to use the SmarterMail APS package.

Package Setup and Usage

This covers the steps required before provisioning and usage of the package can be conducted.

Setup

Creating a Domain

- Expand Operations Director
- Expand Customer Manager
- Select Customers
- Select the "Company" field and search for a company, then select the company from the search results
- Click the Resources tab
- Click "Add New Domain"
- Provide a domain name (e.g., example.com)
- Check "Set Registrar Status to Ready"
- Select the SmarterMail APS subscription from the "Subscription" dropdown
- Click "Next"
- Click "Next" again
- Review the settings and click "Finish"

A domain is required to be associated with the package so the domain can be properly added with the package. After a domain has been added, the package can start being used.

Usage

This covers an example usage of using the package by creating a domain as a customer.

Login

- Expand Operations Director
- Expand Customer Manager
- Select Customers
- Select the “Company” field and search for the company, then select the company from the search results
- Click “General” tab

- Click “Staff Members” and a list of staff members will be shown
- Click “Login as Customer”

Configure

- Click the “SmarterMailAPS” link towards the bottom of the page
- Click “Add New”
- Fill in the following fields:
 - Display Name
 - Check “Login in existing domain”
 - Fill in the user name
 - Fill in the password (Generate New Password can be used to generate a random password for this account)
 - Click “Next”
 - If “Display Name” was supplied from the previous step, the System Administrator’s first & last name will be filled in. If not, it is optional to provide a first & last name
 - Click “Next”
 - Review the settings and click “Finish”
 - The account and the domain will be scheduled for provisioning

The steps when configuring each service are the same for each service the package provides. Simply fill out the required fields for each service and follow through each wizard.

Website Panel Module for SmarterMail

Package Description

WebsitePanel is a multi-tenant, enterprise hosting automation tool with support for private cloud servers. It enables you to centralize the management of your hosting infrastructure and share resources across multiple customer accounts. This product can be used with SmarterMail and SmarterStats to deploy users and domains\sites from a single interface.

Package Goals

The SmarterMail WebsitePanel module allows the administrator to create, remove, and manage domains, users, mailing lists, and aliases. User settings that can be modified include the ability to change mailbox size, manage passwords, set domain admins, manage autoresponders and mail forwarding. Advanced settings and server settings are managed from within the SmarterMail Domain and / or System Administrator logins in SmarterMail itself. Server defaults will want to be configured prior to integrating with WSP.

The SmarterStats WebsitePanel module allows site and user creation, and allows the ability to link directly to the site to view reports as a particular user. Server and site/domain settings will need to be managed on the server itself.

Prerequisites

- You will need to be registered with WebsitePanel in order to access the download links
- Microsoft.NET framework 4.0 (ensure this is registered within IIS)
- IIS 6.0 or higher
- Microsoft SQL Server, installed locally or hosted remotely
- Licensed install of SmarterMail 9.x or higher and / or SmarterStats 7.x or higher

Configuration

Once all of the prerequisites are met, configuring the modules is fairly straightforward. The steps below cover adding a new server to your environment, creating a hosting plan, and creating a customer account to utilize the server resource that was set up.

[Adding a Server](#)

When you're ready to add a new server, ensure the server password is configured in the Website Panel installer.

- Navigate to Configuration -> Servers
- Click Add Server
- Enter in the Server Name, the URL, and Server Password (this is configured in the WebsitePanel installer)
 - Server URL: http://127.0.0.1:9003 (default)
 - Enter the password configured during the initial setup
 - Ensure “Check for installed software” is selected
 - SmarterMail and SmarterStats should be picked up during the installed software check. These services will need to be configured separately, however. Navigate to Configuration -> Servers. You should see your server, and the services associated.
- Click on SmarterMail 10.x +
- Set the SmarterMail web services URL
- Select a public IP address
- Set the Admin Login
- Configure any additional options
- Click Update
- You should be back in the server configuration page.

- To configure SmarterStats, scroll down and Click SmarterStats 5.x +. Otherwise, skip to step 5
- Set the SmarterStats web service URL
- Specify admin credentials
- Select the SmarterStats server
- Click Update
- You should now have a server set up for the particular service resource.

Creating a Hosting Plan

Below you will find the steps for creating a hosting plan that uses the particular server and service resource you've created.

- Navigate to Account Home
- Click on hosting plans in the left hand menu
- Click Create Hosting Plan
- Set the Plan Name
- Set the target server to your desired server with the particular service resource attached
- Set your quotas
- Check System, then set desired options
- Check Websites (Only necessary for SmarterStats) , then set desired options
- Check Mail, then set desired options
- Check Statistics, then set desired options
- Click Save
- You should now have a hosting plan set up that uses the particular service resource.

Creating a Customer Account

Below are the instructions for creating a customer account that will utilize the resource and hosting plan created.

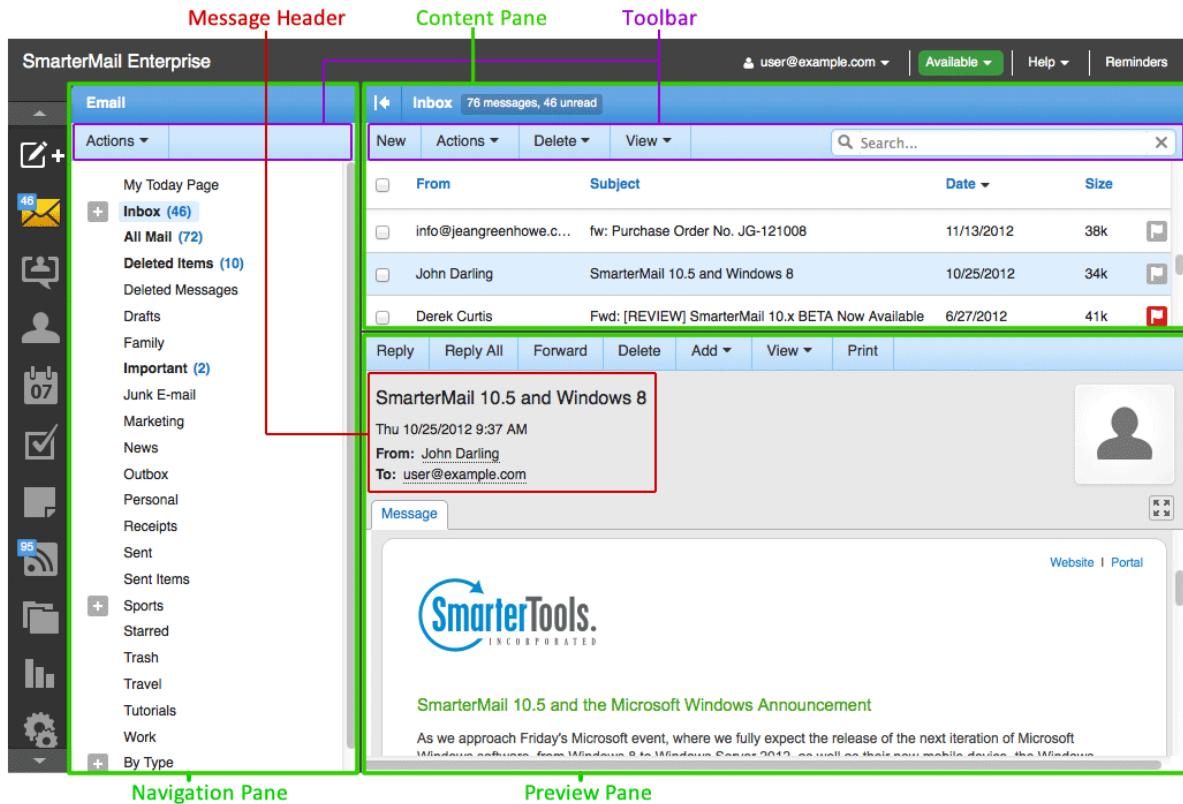
- Navigate to Account Home
- Select Customers from the left hand menu
- Click Create user
- Enter in a Username and Password
- Fill in all other required information
- Click Create
- It will bring you to a new window with an option to create a new hosting space. Click Create hosting space to begin the process

- Select your hosting plan that this will apply to, fill out required fields and select Create Space
- After the space has been created you will need to create a domain for your users within SmarterMail
 - Sign into WSP with the newly created user
 - Navigate to Domains, and select Add Domain
 - Set the domain name, ensure create website is checked (for SmarterStats)
 - Leave the other checkboxes unticked
 - Click Add Domain
- Using the hosting space menu on the left, navigate to Mail -> Accounts, and select Create Mail Account
 - Fill in the e-mail address, and select the domain that was created in step 6
 - Enter a Password
 - Set the Mailbox Size Limit
 - Specify customer information, and a signature if necessary
 - Enable\Disable Autoresponder
 - Enable\Disable Mail forwarding
 - Click Save
- This will prompt WSP to call the SmarterMail web services to create the domain, and the newly created user. I have not found a way to purely add just a domain to SmarterMail using WSP. A user must be created to prompt the domain creation
- Using the hosting space menu on the left, navigate to Advanced Web Statistics and click Add Statistics Site
 - Select the website that was created in step 6c, the site ID will populate on it's own once the site is created
 - Specify your users, and passwords
 - Click Add Site
- The statistics site will then be added into SmarterStats. You can view the site statistics by navigating to Advanced Web Statistics and click View Statistics, you will automatically be signed in as the user.
- You should now have a new customer set up that can take advantage of your hosting plan that uses SmarterMail.

Interface Diagrams

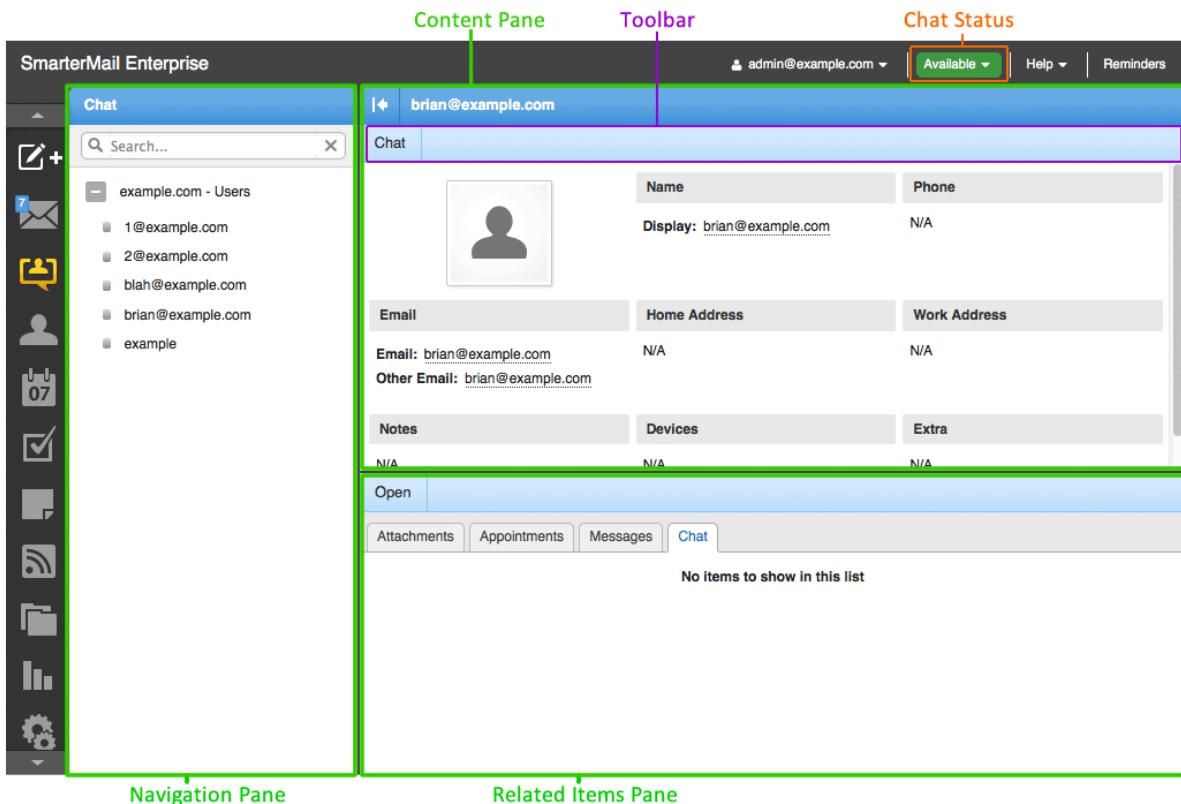
Inbox

To better understand the different areas of the inbox, please refer to the diagram below:



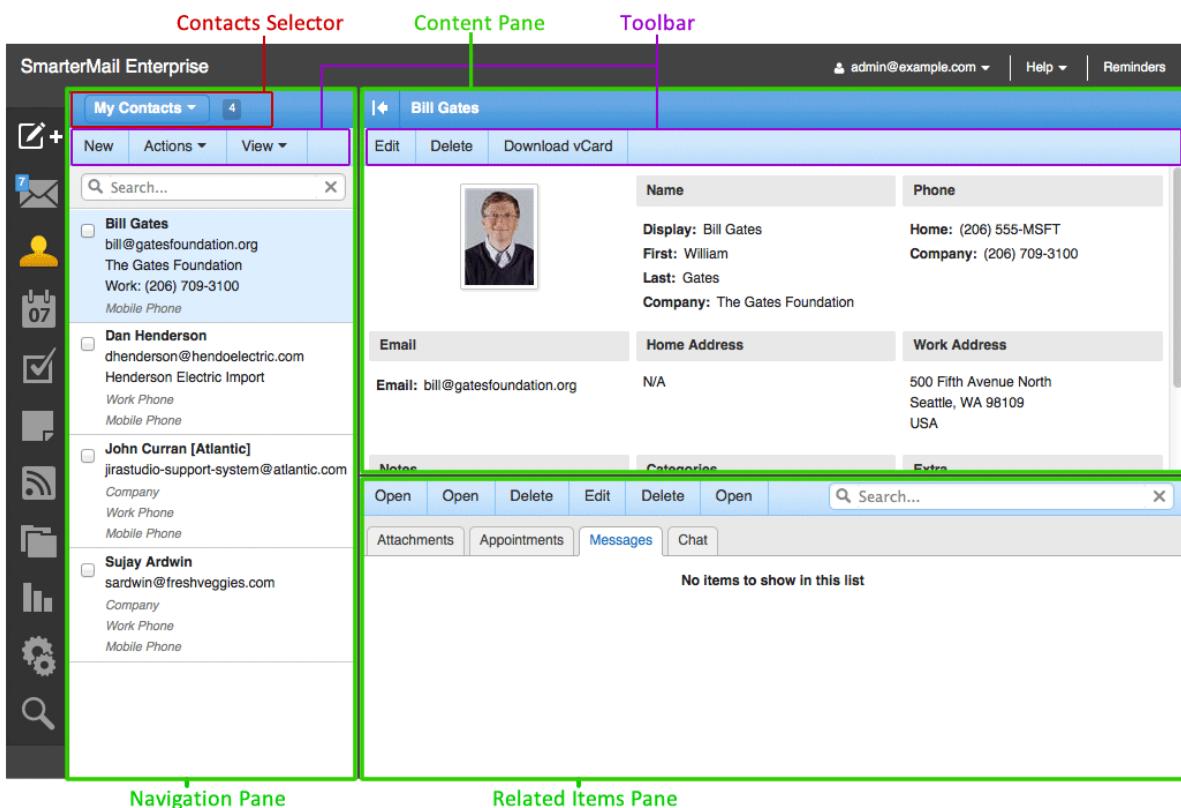
Chat

To better understand the different areas of the chat section, please refer to the diagram below:



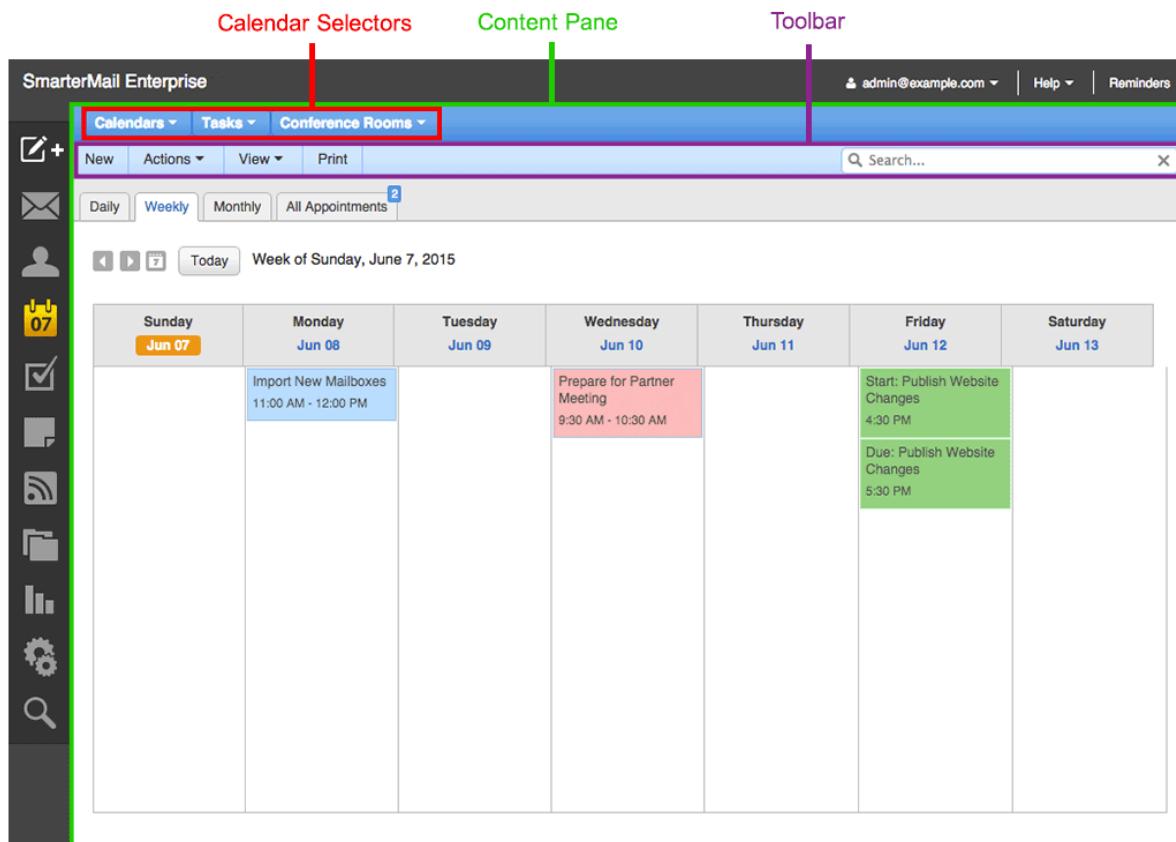
Contacts

To better understand the different areas of the contacts section, please refer to the diagram below:



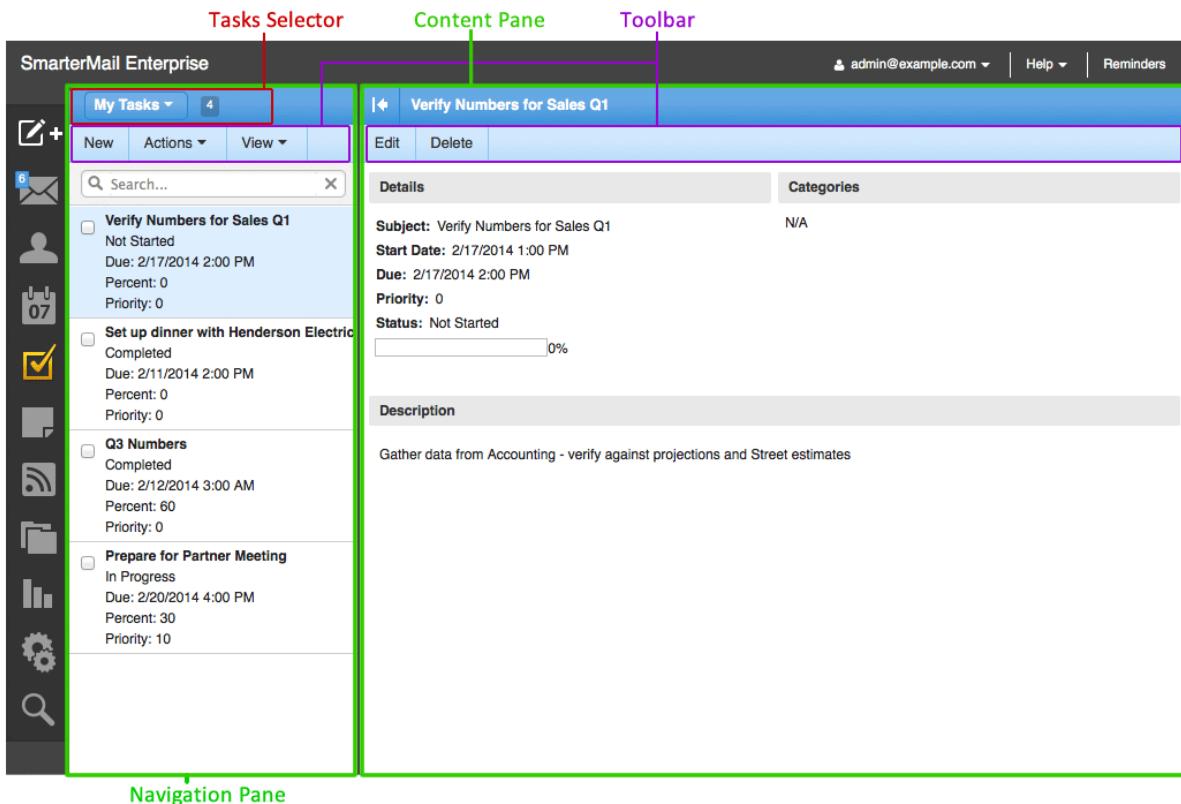
Calendar

To better understand the different areas of the calendar section, please refer to the diagram below:



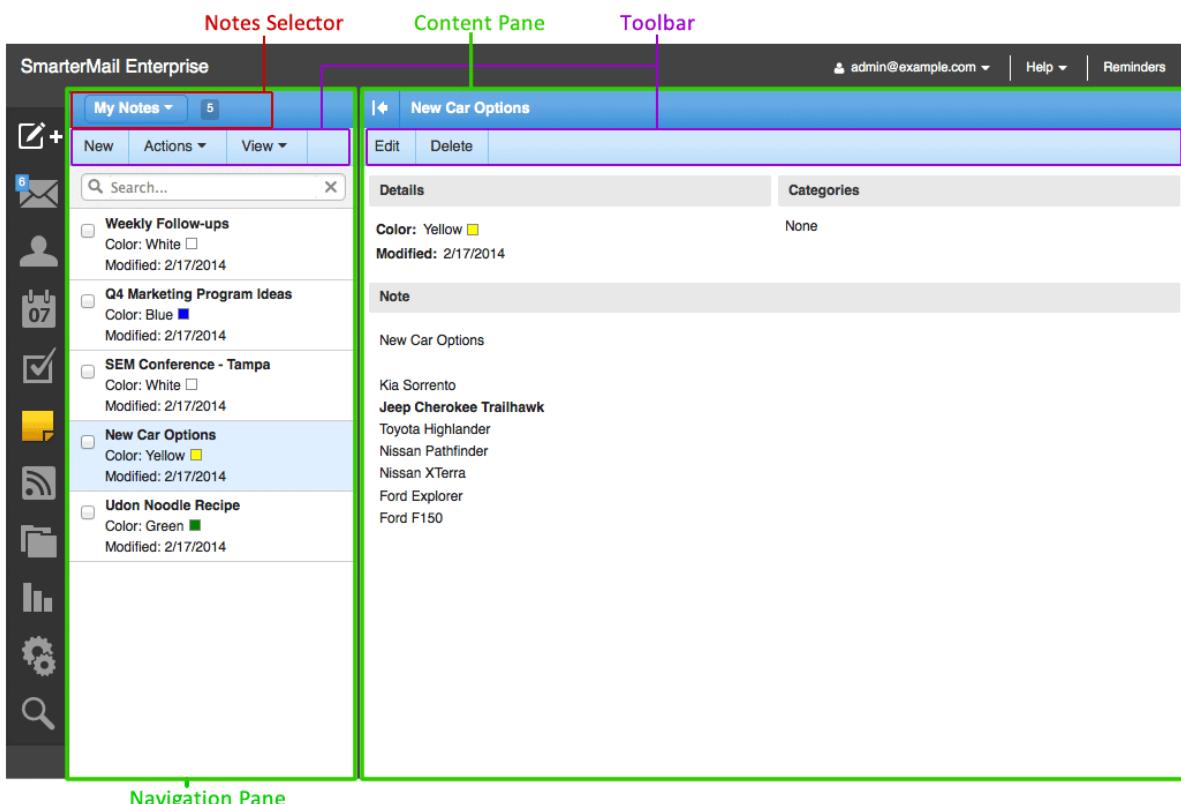
Tasks

To better understand the different areas of the tasks section, please refer to the diagram below:



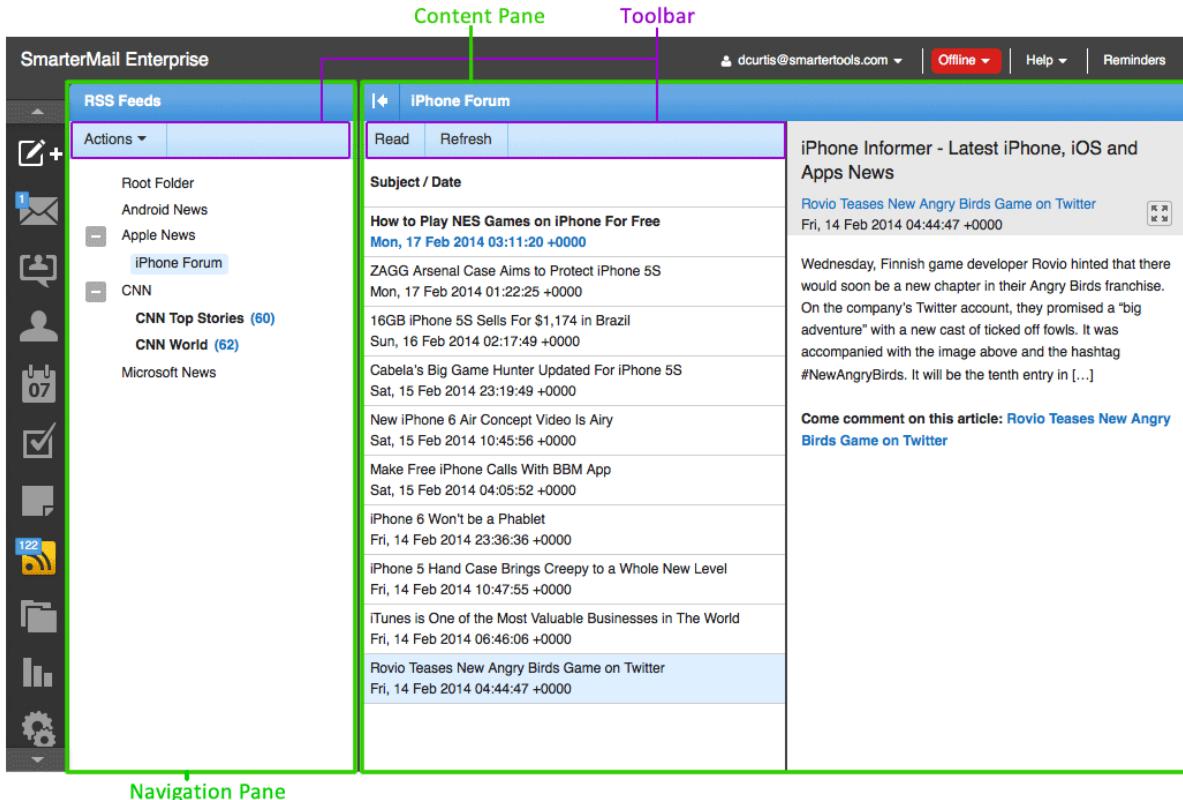
Notes

To better understand the different areas of the notes section, please refer to the diagram below:



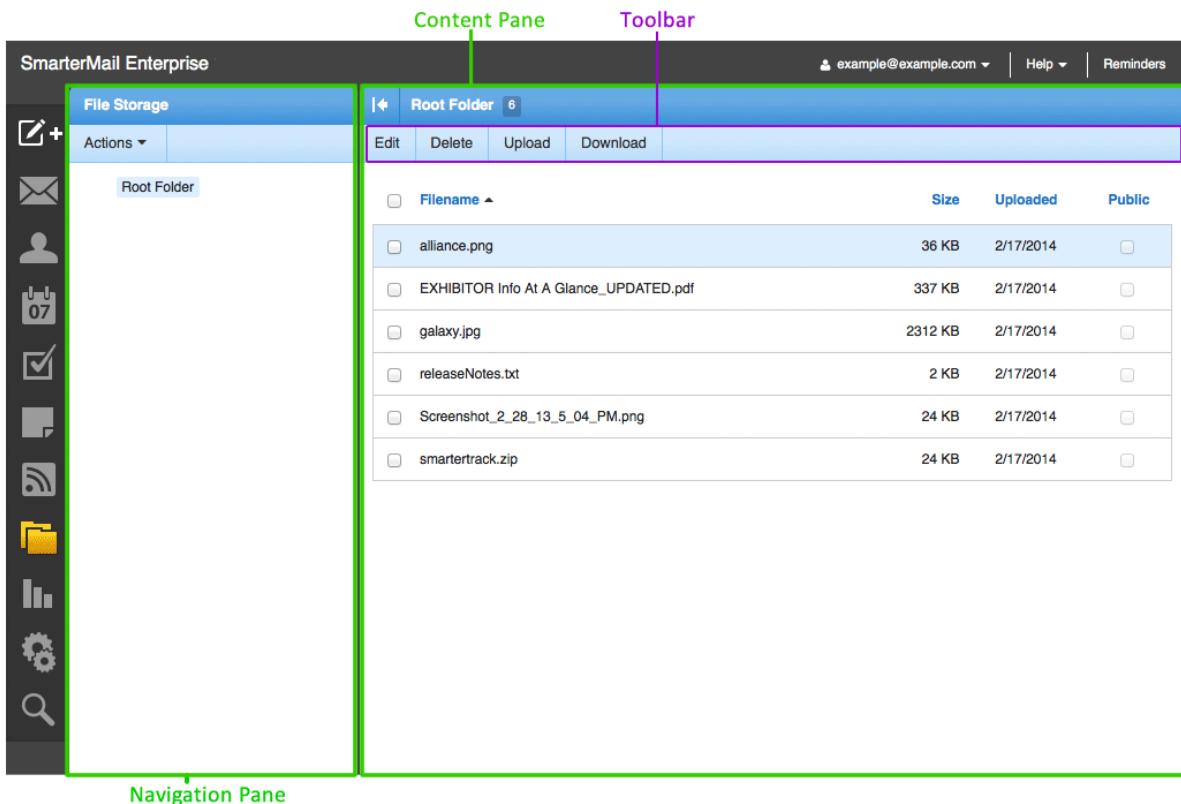
RSS Feeds

To better understand the different areas of the RSS feeds section, please refer to the diagram below:



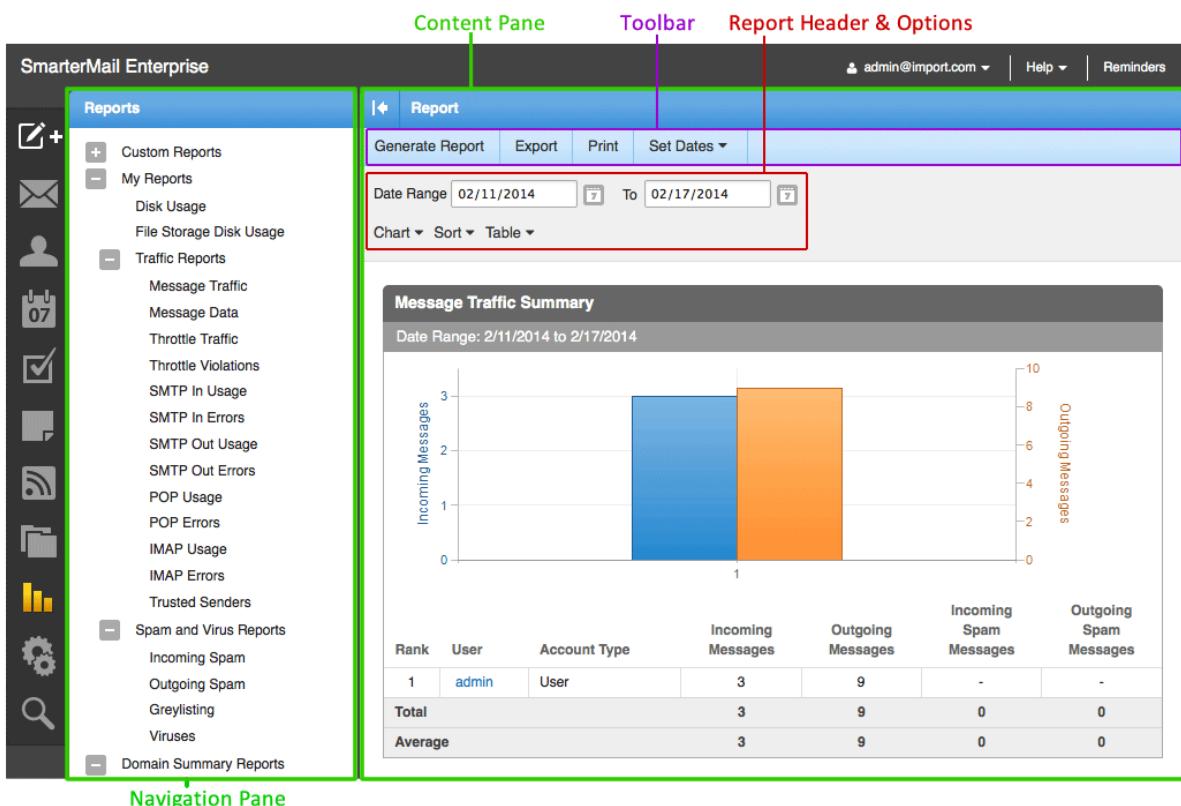
File Storage

To better understand the different areas of the file storage section, please refer to the diagram below:



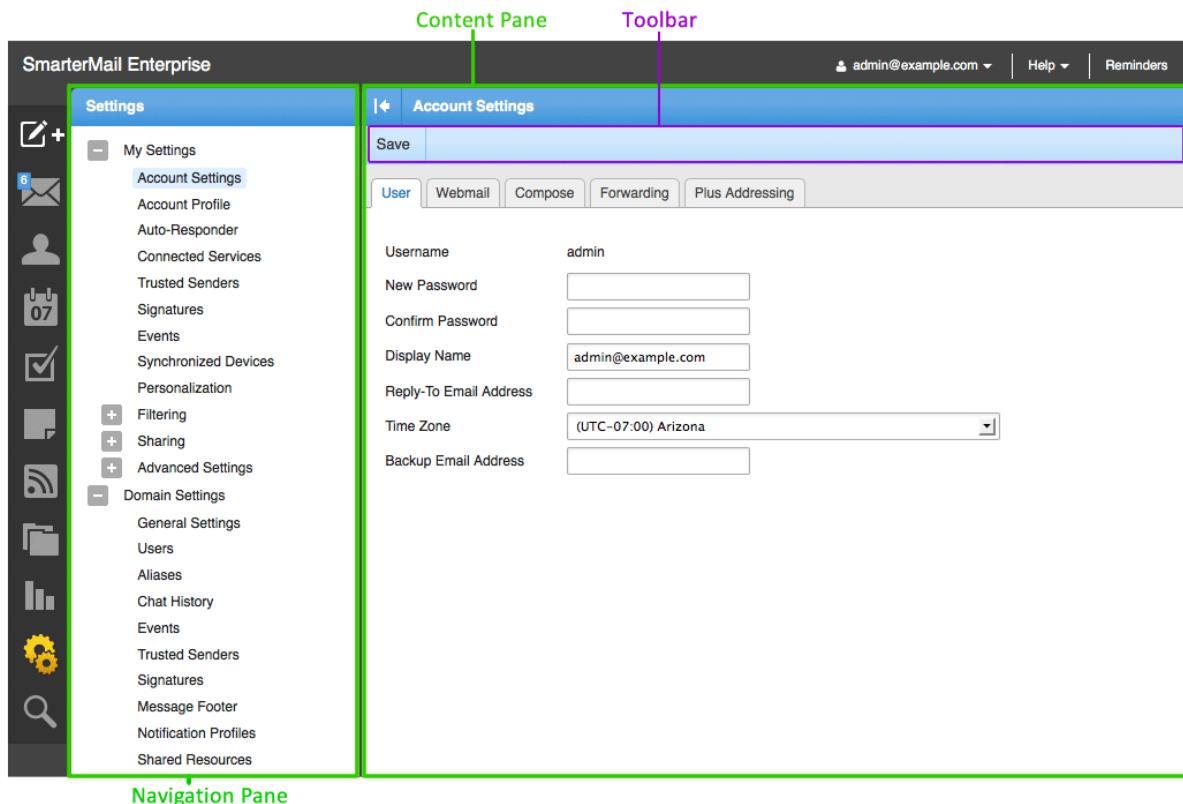
Reports

To better understand the different areas of the reporting section, please refer to the diagram below:



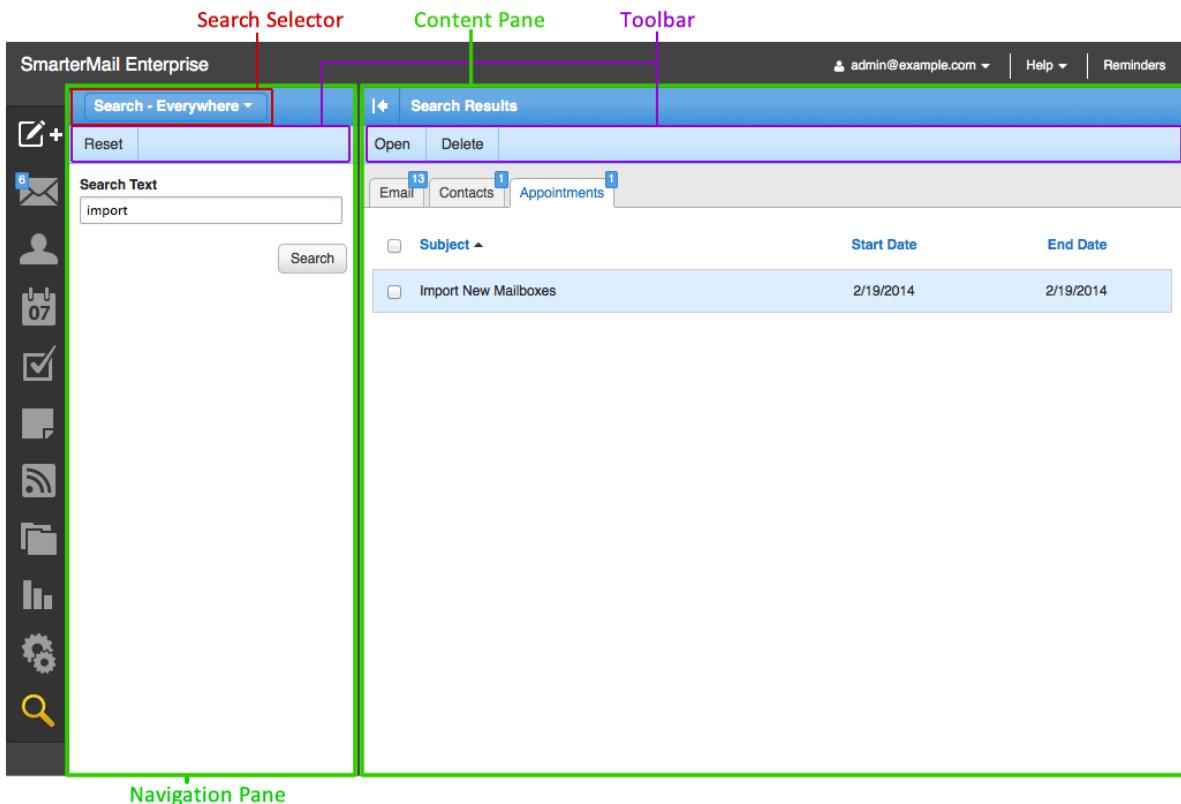
Settings

To better understand the different areas of the settings section, please refer to the diagram below:



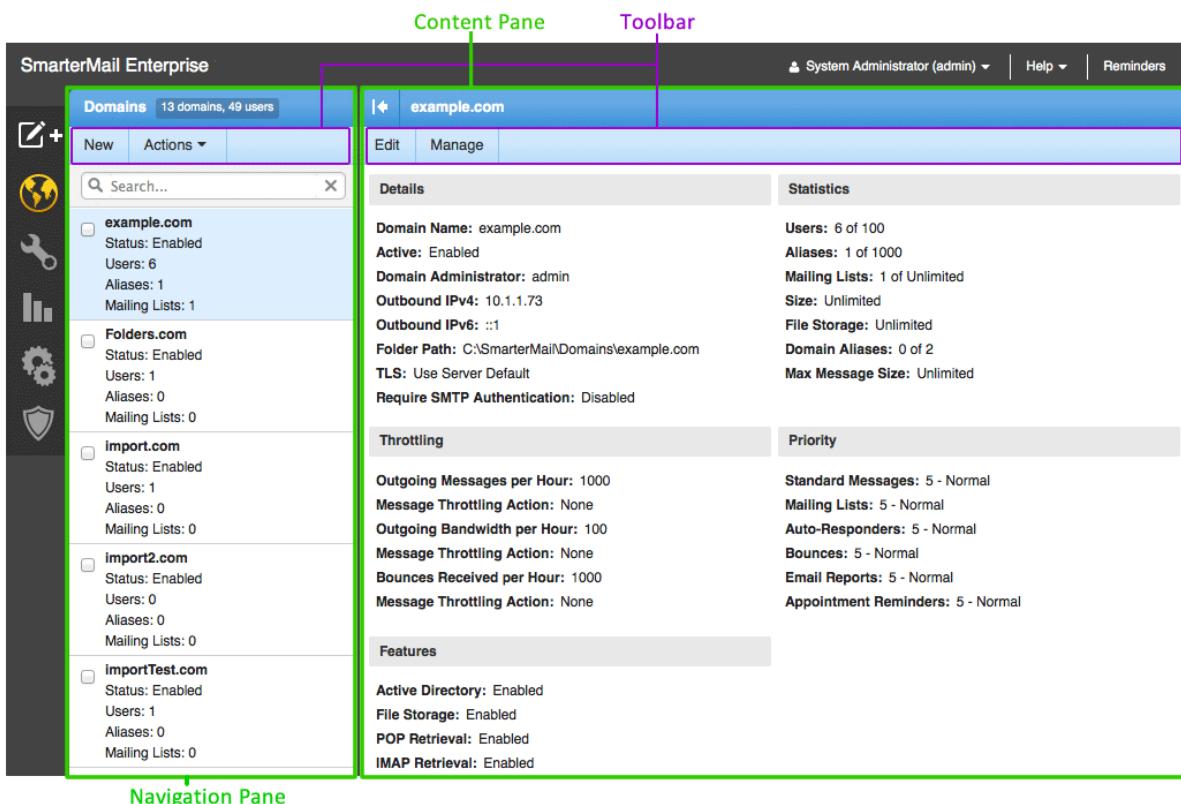
Search

To better understand the different areas of the advanced search section, please refer to the diagram below:



System Administrator

To better understand the different areas of the system administrator's interface, please refer to the diagram below:



Concepts

Roles of SmarterMail

SmarterMail is a feature-rich Windows mail server that brings the power of enterprise-level functionality and collaboration to businesses and hosting environments. SmarterMail is powerful enough to be used as a complete mail system that performs all of the following roles from a single server. SmarterMail installations can also be used to perform specific functions on mail networks to enhance an existing infrastructure or to gain performance—whether you are running SmarterMail as your primary mail server or to support another mail server that is having difficulty performing under the current load.

As you will discover, SmarterMail can be used to fulfill a variety of roles that can be deployed for little to no cost. Adding SmarterMail in one—or several—of these roles will increase the stability and longevity of your email system.

Provide a Feature-rich Primary Mail Server with a World-class Interface

Use SmarterMail as your primary mail server and provide customers with an unmatched email service that includes industry standard connection methods like POP3, SMTP, and IMAP4; multi-language support; and a browser-friendly design. In addition, SmarterMail delivers all of the coordination, communication, and world-class collaboration functionality that you expect through a familiar and intuitive Web interface. Users have access to shared calendars and the availability of their co-workers to schedule appointments. Tasks can be assigned and emails managed 24/7 with accuracy, speed, and security.

Reduce Server Load and Pre-scan Incoming Messages for Spam

Configure SmarterMail as your incoming gateway server and reduce the load on your primary server. In this role, SmarterMail can manage all incoming SMTP sessions and detect abuse and intrusion attempts. In addition, SmarterMail can also host third-party antivirus and antis팸 software, such as Declude, Trend Micro Server Protect, or JunkMail, and pre-scan messages prior to delivery to the primary mail server. Best of all, these functions can be integrated at no cost by downloading and installing SmarterMail Free Edition to operate as your incoming gateway server.

Reduce Server Load and Spool Outgoing Messages

In high-volume scenarios, SmarterMail can reduce primary server load by functioning as your outgoing gateway server to spool outbound messages. One benefit of configuring SmarterMail in this role is that it functions as an effective method to combat blacklisting and can help ensure a quick

system recovery. For example, if one of your IP addresses is blacklisted by an external email provider, you can resolve the issue by changing the IP address of the gateway server or turning off the gateway server until the IP address is removed from the blacklist (providing there are multiple gateway servers set up). In addition, this configuration of SmarterMail can run spam checks on outbound messages to prevent spam messages from being sent to remote servers, thereby reducing the likelihood of a blacklisted IP address. These functions can also be integrated at no cost by downloading and installing SmarterMail Free Edition to operate as your outgoing gateway device.

Ensure Up-time with a Backup MX Server

In the case that your primary mail server goes down, ensure that your users will continue to receive incoming email by setting up a backup MX server. When the primary mail server cannot be contacted, email servers on the Web will attempt delivery to the backup MX server. When the primary server comes back online, the backup MX server will deliver all held email.

Use One Server for All of Your Needs

SmarterMail's unique configuration system allows the flexibility to configure a server to function in a single role or in multiple roles at once. For example, SmarterMail can be to function as both the incoming and the outgoing gateways, which will improve the flow of traffic through your network without large cost increases.

SmarterMail and Microsoft Exchange An Administrative Comparison

Who Should Use This Document

This document provides a comparison of SmarterTools' SmarterMail Enterprise mail server software and Microsoft's Exchange 2010 Enterprise mail server. It is designed specifically for server and system administrators and provides information on the hardware, software and licensing requirements of both products, with an overall cost breakdown in each category.

It is equally important to review the end user experience for both products as well. Therefore, please review the white paper SmarterMail and Microsoft Exchange 2010: An End User Comparison for a more complete feature-by-feature comparison of both products from the end user's point of view.

For the purpose of the comparison in this document the following criteria were used:

- Based on a small to medium business (SMB) utilizing multiple domains, potentially for multiple brands.
- Up to 250 mailboxes populating the mail server. This is simply a user limit for the sake of comparison and in no way infers a maximum user limitation, either within Exchange or

SmarterMail.

- Accommodations for organizations wanting both webmail access as well as organizations wanting a mixture of webmail and standard desktop email clients.
- Mobility using multiple “smart phones” (e.g., Apple iPhone, Samsung Galaxy SIII / Note 2, LG Optimus 9, Nokia N-900) and other mobile devices (e.g., Apple iPad, Android tablets).
- Complete synchronization across a variety of mobile and desktop environments.

Overview

At first glance, comparing a mail solution against the historical significance of Microsoft’s Exchange Server may seem like a rather daunting task. After all, a study in 2008 estimated that a full 65% of workers worldwide were using Microsoft’s email server. However, at that time there was a lack of competitive products that offered comparable functionality. That is no longer the case, and once you start peeling layer upon layer of complexity away from the Exchange infrastructure, vulnerabilities begin to appear. This is especially true when you look at Exchange from an administrative standpoint.

With that in mind, there are several areas where SmarterMail Enterprise far surpasses Exchange Server 2010—areas that are of vital importance to small businesses and server administrators alike:

- Licensing — All of the software required comes with a cost—and that can be high on the list of priorities when planning out a new system or even a migration/change of an existing system.
- SmarterMail has a much smaller footprint and lower cost of entry and, as you’ll see, a lower long-term cost as well.
- Requirements and planning — There are hardware and software considerations when planning to build out an email and messaging platform. Exchange is well known for its complexity and difficult planning and installation requirements.
- SmarterMail offers a simpler set of requirements and nothing more than basic server administration and implementation skills are necessary.
- Management and Maintenance — Once the mail server is installed, someone needs to be able to monitor the day-to-day activity and health of the server, users need to be added or removed, settings need adjusted, and more. Being able to perform these tasks quickly, easily and from anywhere is extremely important.
- SmarterMail provides a simple and understandable set of management and maintenance tools built into an “access anywhere, at any time” web-based interface.
- Backups/Restores — Storage and recovery capabilities of online communications is hugely important. What options are there and what are the costs?

- SmarterMail can be backed up and restored using standard backup and recovery technology. No further investment in specialized hardware or software is needed.

Comparison of Licensing

From a licensing perspective, a clear and concise licensing structure makes it much easier to plan out both an initial installation as well as any migration. Taking this into account, is it better to require an all-in-one licensing model or one that requires virtually each individual piece to have its own licensing requirement?

Comparison based on 250 Mailboxes		
	SmarterMail Mail Server	Microsoft Exchange™
Base License	\$ 499.00	\$ 3,970.00
Client Access License	N/A	\$ 25,000.00
Anti-Spam	\$ 249.00	Included*
Anti-Virus	\$ 249.00	Included*
ActiveSync**	\$ 799.00	Included
Hardware	\$ 1,998.00	\$ 1,998.00
Upgrade Protection	Included***	\$ 1,998.00
Employee Expense	Low	High
Total:	\$ 3,794.00	\$ 32,953.00

*Antispam and antivirus are part of Microsoft's Forefront Security Suite as part of the Enterprise CALs

**Exchange ActiveSync (EAS) comes standard with Exchange. Pricing shown for SmarterMail is for 200 licenses. You can scale EAS licensing to meet your needs, separate from your SmarterMail license.

***SmarterTools' upgrade protection is included with every new license purchase and provides customers with major upgrades at no cost for 12 months.

Server Licensing

First, let's look at simple server licensing costs. This is licensing solely for the mail server software that is installed. Remember, for the purposes of this comparison we are going to look at a business that requires up to 250 mailboxes.

- Exchange 2010 — Enterprise is \$3,970.00.
- SmarterMail — Enterprise licensing for 250 mailboxes is \$499.00.

Client Access Licensing

A CAL is simply what the name implies: it's a license required for a client—whether that is a user or a device—to access a server.

- Exchange 2010 — Requires user or device CALs, depending on how or what is connecting to the Exchange server.
- A user CAL is generally defined as a license for the person connecting, regardless of whether they connect via Microsoft Outlook, webmail or mobile device. User CALs are approximately \$42.00 each.
- A device CAL is defined as a license for each device that is connecting (e.g., desktop, mobile device, etc.). Device CALs are approximately \$68.00 each.
- SmarterMail — Does NOT require individual licensing for each person or device that accesses a mailbox. In fact, you can buy a license that will accommodate the number of mailboxes you need—plus give you some room for growth. Whether you need 250 mailboxes, 500 mailboxes, 1,000 mailboxes or even an unlimited number, there is a licensing model to fit your need (SmarterTools even offers a fully-functional Enterprise license for 10 mailboxes as a free trial).

Employee Expense

Employee expenses are somewhat subjective. With Exchange you have a very complex infrastructure, requiring multiple server roles, high-end hardware and software, and extensive project planning and management. On the other hand, SmarterMail offers a much simpler installation requirement and footprint. On these merits alone, the employee expense incurred with just the installation of Exchange—not to mention the day-to-day management and maintenance of it—logically dictates that a very experienced and well-trained individual or group is required. This, in turn, equates to a higher cost.

With SmarterMail, an existing employee with a good grasp of server technologies and management skills is all that is required. That's how SmarterMail was built: with ease of use and ease of management in mind.

Comparison of Requirements and Planning

Rather than looking at the overall feature set of both products, let's take a close look at the requirements of both Exchange 2010 and SmarterMail.

Hardware

- Exchange 2010 — Requires 64-bit architecture. While not an issue at first glance, this restriction may require separate servers for each server role in the Exchange setup. This can be

problematic for businesses wanting to use existing legacy hardware or that lack capital to invest in new hardware. Also, Exchange requires several server roles, managing various parts of the platform. This could mean the need for multiple servers.

- SmarterMail — Has a very acceptable minimum set of hardware requirements. This means businesses can run on either 32-bit or 64-bit hardware. As there are no server roles to configure, a single server may be all that is required. In fact, SmarterMail can run on an existing server in a dual-use role. That is, SmarterMail can run on a Web server or file server and doesn't require its own hardware to run.

Software

- Exchange 2010 — There is, of course, mail server licensing (either Standard or Enterprise) to consider. Additionally, Exchange requires Client Access Licenses (CALs) for each mailbox/user and in order to get security and antivirus, Enterprise CALs are required - at a substantially higher cost. And all needs to run within an active directory tree. Finally, Exchange 2010 must be run on a 64-bit version of Windows Server 2008.
- SmarterMail — A simple purchase of the mail server is all that is required. Antivirus and antispam are included with SmarterMail Enterprise, but there are options to increase coverage with Message Sniffer and Cyren. In addition, SmarterMail does NOT require a 64-bit version of Windows Server, making it incredibly easy to set up on an existing 32-bit or 64-bit server.

Planning the Architecture

- Exchange 2010 — As mentioned, Exchange has multiple different server roles (edge transport, hub transport, mailbox, client, etc.) running within an active directory tree. As noted earlier, each role may require separate servers. That means extensive planning is required, from active directory on up to actual Exchange server installation.
- SmarterMail — Considering hardware and software requirements, one server can act as the mail server and also run any necessary antispam and antivirus add-ons. Furthermore, SmarterMail also does not require active directory, although it can integrate into an active directory tree so single-authentication can be used throughout an existing infrastructure. It should be noted, however, that the lack of an active directory requirement may reduce the time needed to plan out an implementation and installation strategy.

Management and Maintenance

With any software implementation, system and server administrators are challenged with keeping tabs on the mail server(s) hardware and software. Furthermore, there are day-to-day tasks, things like user management, domain management, management of blacklists and content filters, and much more.

Management and Maintenance

- Exchange 2010 — As Exchange runs on a server OS, the majority of management and maintenance of the server has to be performed on the server. That means administrators generally have to remote or console into the server. In addition, management occurs via an Exchange tool that plugs into the Microsoft Management Console (MMC). If an administrator is offsite, these connections must occur through secured VPN. All of this can decrease the connection speed and therefore increase the time it takes to complete even routine maintenance tasks. Besides, it's a somewhat convoluted and complex setup.
- SmarterMail — SmarterMail offers a powerful and extremely accessible web-based administrative front end. With the ability to set up different roles (e.g., system administrators vs. domain administrators), plus the ability to set up multiple, different system administrator accounts (so no one has to share logins, which results in better tracking and change management) SmarterMail administration is fast, is easy, and it can be accomplished on-site or remotely using any standard browser. SSL connections are available, and you can even limit access to the admin area by specific IP, further enhancing security. And unlike the Exchange plug-in for the MMC, SmarterMail's administrators have access to numerous reports, from incoming/outgoing spam to server health, disk space usage to abuse detection.

Learning Curve

- Exchange 2010 — When looking at everything that goes into planning an Exchange installation, there's no doubt the people planning and carrying out the installation are professionals. This, in turn, means they significantly factor into the costs associated with that installation. In addition, there are possibly increase employee costs for the level of individual necessary to manage and maintain an Exchange infrastructure. Most system and server administrators for Exchange have years of experience and untold hours of training and product-specific education under their belts. Therefore, they won't come cheap.
- SmarterMail — SmarterMail runs in a very simple, very easy to manage and maintain environment that is not unlike any base server installation. Therefore, a company can get by with existing staff and existing system and server administrators. The learning curve is much easier to manage with SmarterMail as standard server administration knowledge is about all that is required.

Backups and Restoration

Your data is only as good as its most recent available backup. And even then, a backup isn't of any use unless it is recoverable and restorable. However, backups and restoration of data do not have to be complex and expensive initiatives.

- Exchange 2010 — Exchange can be backed up with most existing backup technologies. However, its one big exemption is that Exchange requires a separate and specialized backup agent in order to be able to back up mail files. Anyone who has priced these agents out knows this an expense to them, and in many cases the expense can be substantial.
- SmarterMail — SmarterMail can be backed up with any existing backup technology and does NOT require the use of a separate, specialized agent. This reduces the costs of backup and restoration and also is one less thing for administrators to manage and maintain on the mail server.

Summary

When you look at all of the differences between Exchange 2010 and SmarterMail a few things really stand out:

- The planning necessary for an implementation of Exchange 2010 is far more detailed and involved than what is necessary for an installation of SmarterMail. With Exchange, you don't simply set up a Web server and a database. Things like active directory trees need to be considered, plus the necessity of various server roles—how to configure each role, figuring out what can you combine into a single server, planning how to configure the server connections and interactions, etc. Complexity is Exchange's strong point; simplicity and ease-of-use are SmarterMail's.
- Licensing is generally a sore spot with most software implementations. However, it's extremely apparent that you get just as much with SmarterMail as Exchange, but with substantially less payout. Looking at the comparison tables alone demonstrates a 5X to 11X savings with SmarterMail over Exchange.
- Requirements, both from a hardware and software standpoint, again point to SmarterMail being a much wiser investment than Exchange. Minimal server OS concerns, no active directory (unless you need it), and much more flexible hardware options all place SmarterMail above Exchange.
- When looking at maintenance and management, plus the learning curve required, SmarterMail again gets the nod. Without the need for lengthy training or education, and simple server administration experience all that is required, SmarterMail is easily administrated by existing employees, again saving time and money.

Trust and Availability

There's no doubt Microsoft has the name. They've been around a long time, and have a long history of building quality software and being on the leading edge of technology, especially when it comes to providing a robust and feature-rich email solution. However, becoming one of the largest, if not THE

largest, software and services company doesn't come without some sacrifice. These sacrifices tend towards offering reliable, accessible access to support and customer service, at least affordable access to these critical needs.

That's where SmarterTools comes in.

Over the last eight years SmarterTools has grown to over 15 million users, but still sees each user as important. They have grown through investment in products and development versus in advertising and marketing, building SmarterMail into one of the most popular and respected mail servers on the market. They realize how safe, secure and reliable communication is vital to each and every user of their product. That's why SmarterTools offers services that cater directly to their customer base:

- Access to LIVE tech support, 24/7/365
- Upgrade and installation services
- A popular, free public community to interact with support and fellow users
- Responsiveness to customers that often leads to product enhancements

While it may be true SmarterTools doesn't have the name recognition as Microsoft, what is certainly not up for debate is SmarterTools' commitment to their customers, to their products, and to their desire to create the most reliable and secure mail server solution on the market.

Taking all of this into consideration, it may not be a question of "why move to SmarterMail from Exchange," or "why choose SmarterMail over Exchange," but more a question of a "why not?"¹
<http://www.ferris.com/hidden-pages/ferris-research-completes-most-comprehensive-survey-of-business-email-systems-to-date/>

SmarterMail and Microsoft Exchange An End User Comparison

Who Should Use This Document

This document provides a comparison of SmarterTools' SmarterMail Enterprise mail server software and Microsoft's Exchange 2010 Enterprise mail server. The comparison is from the end user's point of view.

It is equally important to review the system and server administration experience for both products as well. Therefore, please review the white paper SmarterMail and Microsoft Exchange 2010: An Administrative Comparison for a more complete comparison of both products from the administrative point of view.

For the purpose of any comparisons in this document the following criteria were used:

- Based on a small to medium business (SMB) utilizing multiple domains, potentially for multiple brands.
- Up to 250 mailboxes populating the mail server.
- Accommodations for organizations wanting both webmail access and standard desktop email clients.
- Mobility using multiple “smart phones” (e.g., Apple iPhone, Samsung Galaxy SIII / Note 2, LG Optimus 9, Nokia N-900) and other mobile devices (e.g., Apple iPad, Android tablets).
- Complete synchronization across a variety of mobile and desktop environments.

Overview

Email is the cornerstone of modern communication. In fact, even after the growth in various forms of social media like Twitter and Facebook, email is still considered THE "Killer App." As such, it is of vital importance that email communication is as secure, stable, powerful and versatile as possible. With SmarterMail, you get tools to not only make your email experience more enjoyable, but safer and more secure as well.

In addition to protecting users, SmarterMail offers a flexible and versatile set of tools for users to access email. These tools include an advanced webmail interface that can be used with most popular Web browsers, synchronization protocols such as CalDAV, CardDAV, Microsoft Exchange ActiveSync and Exchange Web Services for mobile devices like the Galaxy S4 and Apple's iPad, and integration with desktop clients such as Microsoft Outlook, Microsoft Outlook for Mac, Apple Mail and Mozilla Thunderbird.

Of course, there are other products that do the same; Microsoft's Exchange is one example. However, once you start comparing the two products it is evident that SmarterMail Enterprise far surpasses Exchange Server 2010 in many areas:

- Collaboration — This means the ability to share things like your daily calendar, your contacts, and even your tasks. From a calendar standpoint, equally important is the ability to set up meetings and check the availability of your friends and colleagues.
- SmarterMail contains virtually identical collaboration tools as Microsoft Exchange and adds a few extra, such as file storage and file sharing.
- Security and Antivirus — Computer/infrastructure security from online threats is a big concern, so this section discusses included options as well as third-party integration.
- SmarterMail offers powerful antivirus measures without the need to purchase third-party add-ons (although you can, if desired).
- Antispam — According to Symantec's MessageLabs, spam is responsible for over 88% of all

email. Options to combat these numbers, both included as well as third-party integration, are discussed in this section.

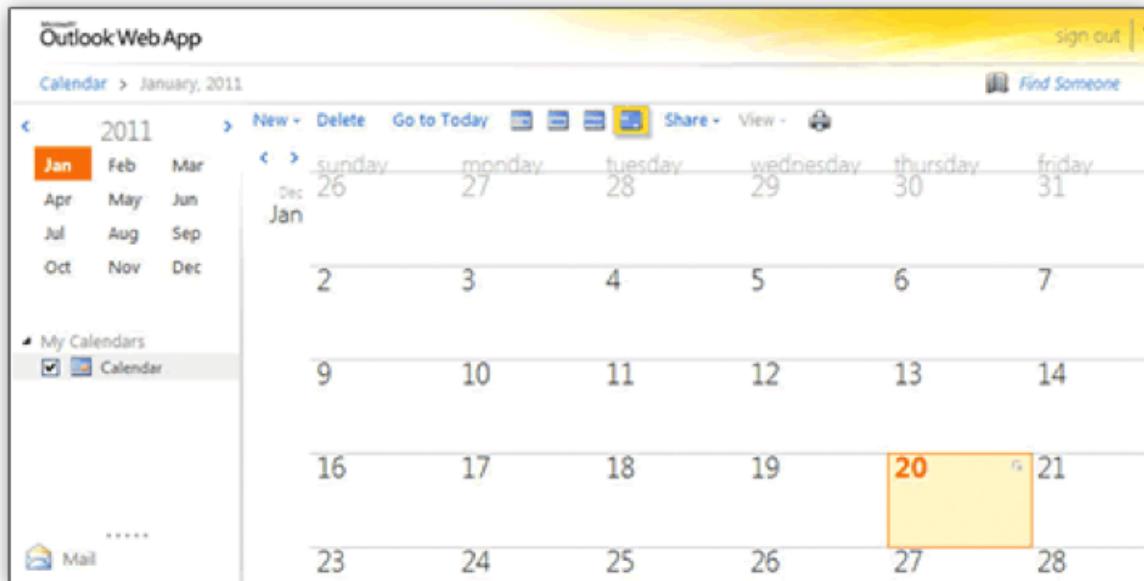
- SmarterMail offers industry-standard antispam measures upon install without the need to purchase third-party add-ons (although you can integrate third-party solutions, if desired), with over 97% of spam blocked with a default installation.
- Synchronization and Mobility — According to a Pew Internet study¹, 26% of adults own an e-reader, whereas 31% own a tablet computer. In addition, 55% access the Internet on a mobile phone. With that kind of growth and reach into everyday life, what are the options in Exchange and SmarterMail?
- SmarterMail offers a number of ways to sync with your mobile devices and actually beats Exchange in some cases by supporting multiple synchronization options.
- Access to Information and Email Migration — Having access to information is crucial in today's fast-paced environment. You need to know what's going on in the world, you need to keep track of contacts and your interaction with them, and you need to know your own status within your organization: your usage stats, your available space, both for your email as well as for your files, and much more.
- SmarterMail offers a number of “push” type technologies that give you the ability to subscribe and manage RSS feeds, reporting options of virtually all of your email usage, detailed contact information, and a quick and easy way to migrate your files, contacts, calendars and emails into SmarterMail—all within the robust webmail interface, giving you access to this information anytime, anywhere.

Collaboration

Collaboration is simply the ability to share information with friends and co-workers, from your calendar to your contacts. Additional features include the ability to schedule appointments with people, check their free-busy availability, reserve conference rooms, modify shared tasks, share contacts and “virtual cards” (vCards) and more.

Shared Calendars, Contacts, Tasks and Notes

- Exchange 2010 — One of the more notable and powerful features Microsoft introduced with Exchange is the ability to share calendars, contacts, notes and tasks with other people in an organization.
- SmarterMail — SmarterMail also offers sharing of calendars, contacts, tasks and notes. However, SmarterMail offers a way to store documents and other files and link to those in emails and tasks so others can access them as well. As an aside, while you can share links to the files, you don't have to, making SmarterMail's file storage feature even more versatile.



Microsoft Outlook Web App - Calendar

Sunday Feb 13	Monday Feb 14	Tuesday Feb 15	Wednesday Feb 16	Thursday Feb 17	Friday Feb 18
62° 44°	60° 43°	75° 53°	71° 51°	60° 43°	62° 43°
9:00 AM - 10:00 AM SEM Webinar (Conference Room #2)	Monitor New Customer Support Rep	8:15 AM - 9:15 AM Finance Meeting	3:00 PM - 4:00 PM Sales Team Meeting	9:00 AM Start: Move to new Office	
11:00 AM Due: Define Email Marketing Plan	9:00 AM Due: Define Email Marketing Plan	12:00 PM - 1:00 PM Return Rental Car	2:00 PM - 3:00 PM Dentist Appointment	2:00 PM Due: Move to new Office	
12:00 PM - 1:00 PM Company Lunch Meeting	3:00 PM - 4:00 PM Email Marketing Plan			4:00 PM - 6:00 PM Take Kids to see Gnomeo & Juliet (Marking down the street)	
3:00 PM - 4:00 PM Final Interview with					

SmarterMail Calendar

Security and Antivirus

Everyone wants their email to be secure—secure from virus infection, free from phishing attempts, and free from malware and dangerous attachments. Additionally, no one wants their mail servers used for spamming or for attacking others as that can lead to untold hours of downtime once unwanted activity is detected and dealt with—both internally and by those affected.

Antivirus

- Exchange 2010 — Does NOT contain any antivirus protection out of the box. That means that it must be added after the fact and can end up costing more money. At the very least, the

Enterprise Client Access Licenses (CALs) are needed in order to use Microsoft's Forefront Security Suite.

- SmarterMail — Each installation of SmarterMail contains industry standard antivirus protection through Clam AV. This is at NO EXTRA COST to users. SmarterMail also offers the ability to add in a number of other antivirus applications and services, including Cyren Zero-hour Antivirus.

Other Security Features

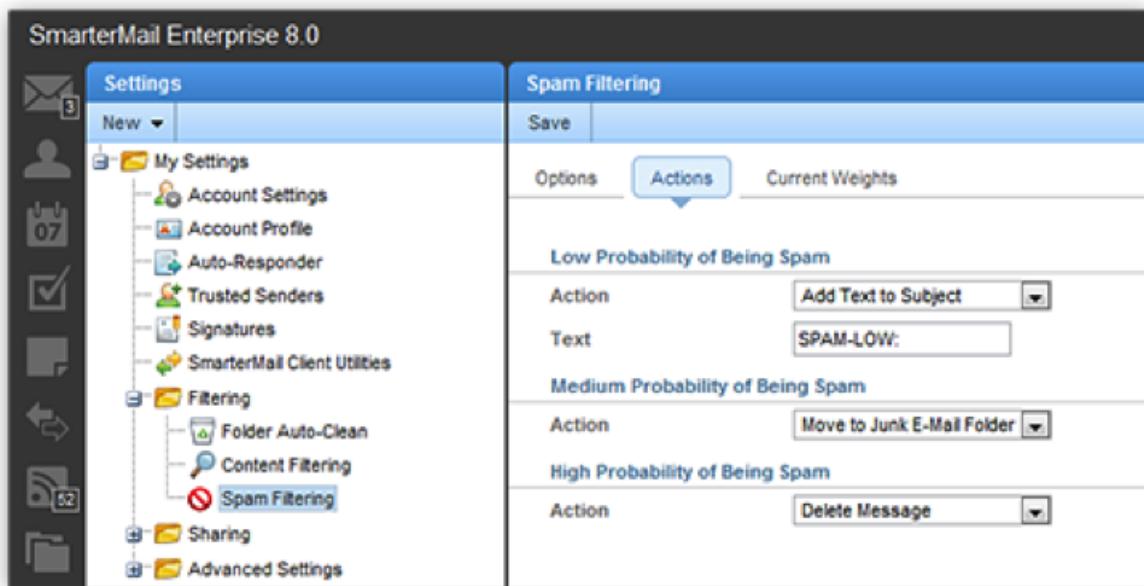
- Exchange 2010 — Exchange offers the ability to send/receive email using Secure Socket Layers (SSL), offers active directory authentication (actually, active directory is required for Exchange), and SMTP authentication by domain. This latter option means that a user must provide an authenticated username and password in order to send email from the server.
- SmarterMail — SmarterMail includes all of the features listed above, but also takes things further by offering email administrators a large number of whitelisting/blacklisting features, brute force detection, automatic denial of service (DoS) prevention, automatic harvest attack prevention and more. This is an added layer of security that protects users from unwanted events hampering communication.

Antispam

Spam is, without a doubt, the scourge of the internet. In 2012, researchers at Microsoft and Google estimated that spam costs society up to \$20 billion, a figure comparable to the GDP of Bolivia.⁴ Factor in the time and money spent by people during their off hours, and that number can grow significantly.

Available Antispam

- Exchange 2010 — Just as with antivirus, Exchange does not offer any antispam protection out of the box for a user's inbox. It requires a third-party solution or Enterprise CAL. That's not to say Exchange doesn't offer antispam measures for the server and for sending email (things like domain keys and DKIM, trusted senders, SPF records, etc.).
- SmarterMail — Similar to its antivirus protection, SmarterMail offers industry-standard spam measures on a variety of fronts. For example, SmarterMail supports more than 24 separate industry black lists as well as SPF and DKIM. In addition, SmarterMail offers further protection through a proprietary pattern matching engine built upon the SpamAssassin technology and support for remote SpamAssassin servers at no additional cost to end users. SmarterMail also supports Message Sniffer and Cyren Premium Antispam, which can be included for a minimal yearly license fee.



SmarterMail Antispam Settings

Mobility and Synchronization

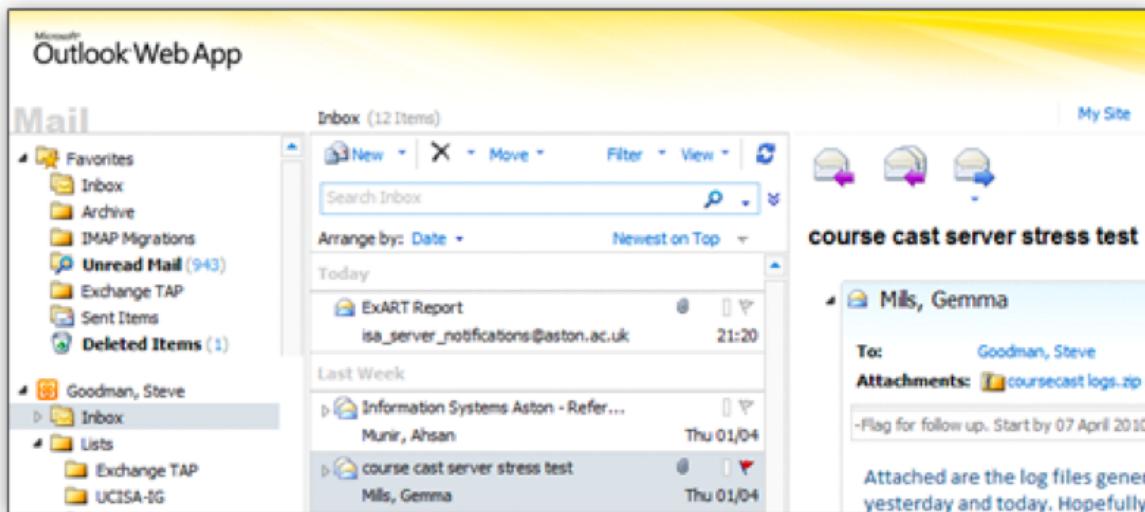
With more and more of today's workforce occupying home offices or finding themselves on the go, having an email system that can not only accommodate mobile devices—beyond simply smartphones and including iPads and Android tablets—is essential. In addition, people no longer just text or email each other, they share photos and documents as well.

Mobility and Synchronization

- Exchange 2010 — Exchange ActiveSync (EAS) is a Microsoft technology that is built into Exchange, giving users on the domain the ability to share contacts, calendars, notes and tasks. In addition, Exchange email can be accessed from a variety of email clients like Outlook, Outlook Express, Entourage and more.
- SmarterMail — SmarterMail also supports Exchange ActiveSync as an optional add-on. However, SmarterMail also supports a variety of open source synchronization technologies like SyncML and specific contact and calendar protocols like CardDav and CalDav (for most Apple products, as well as third-party support for Android and upcoming support on Windows Phone). Therefore, while SmarterMail supports EAS as a best-in-breed paid add-on, it may not be required in some situations. SmarterMail also syncs with a variety of email clients such as Outlook, Entourage and Thunderbird. In addition, SmarterMail's webmail client is extremely robust and offers a fully functional email interface for mobile and remote users that is accessible from anywhere there is an Internet connection.

Access to Information and Email Migration

In addition to email, users expect a single interface for a variety of other communications mechanisms. In addition, transitioning from one mail system to another and the movement of email and contacts can be difficult at best. Both the gathering of information—whether in the form of news feeds or contact information—and the migration of your email communication should be as seamless and pain-free as possible.



Microsoft Outlook Web App - Webmail Interface

The screenshot shows the SmarterMail Enterprise 8.0 Webmail interface. The left sidebar includes icons for My Today Page, Inbox (6), Deleted Items (12), Drafts, Family, Link E-mail, Marketing, Notes (highlighted with a cursor), News, Sent Items, Sports, Trash, and Tutorials. The main area shows the 'Inbox (6)' with messages from Jacob Jones, Matthew Marks, Hiro Ano Nymous, and Bob V. The right panel displays the details of a selected message from Jacob Jones, which includes a reply section with the text 'Hey.' and a note about an office party.

SmarterMail Webmail Interface

- Exchange 2010 — The use of Outlook with Exchange means you have a single source for your RSS reader (for reading subscriptions to blogs and news outlets). The feeds you subscribe to from within Outlook translate to your Web App access as well. However, you can't subscribe to RSS feeds from Outlook Web App—those feeds can only be managed from within the Outlook

client. In addition, using Outlook gives you the ability to see a variety of information about your contacts. Again, however, that information is only available from within the Outlook client. Also, what if you wanted to know about your email usage patterns? What about the amount of disk space you used compared to the amount you have available? These reports are not available, either from Outlook Web or from the Outlook client. And what if you wanted to be notified if a particular contact sent you an email? What if you wanted to know when your mailbox reached a certain disk limit? None of that information is available from Exchange. Yes, you can create rules in Exchange and Outlook, but those are for email management, not email notification. Finally, while Exchange itself offers the ability to migrate email accounts from one system to another, this isn't possible for end users and must be accomplished by an administrator.

- SmarterMail — SmarterMail brings power to the webmail interface with the ability to subscribe and manage your RSS feeds right from a browser window. In addition, if you want to know your usage stats, that information is at your fingertips plus information on your traffic stats, POP/IMAP usage, any errors you've received—all of this across any date range that you can manage and set. As for contact info, SmarterMail gives you access to a number of related items when you view your contacts: recent emails plus the total number of emails you've received from that contact, any appointments, and a list of all the attachments you received. As for events, SmarterMail has them: you can set up events on collaboration features, email or even your disk usage. Events let you know when something occurs, so you have the information you want when you need it. Finally there are the migration tools. Once your account is set up in SmarterMail, you have the ability to manage the migration of email to that new account, regardless of whether it is from Gmail, Hotmail or any other POP/IMAP account. The tools are yours to use at your convenience. And don't forget: all of this is available from an access anywhere, at any time browser-based interface. You're not restricted to a single email client that resides on a computer you may, or may not, have access to.

Summary

When you look at all of the differences between Exchange 2010 and SmarterMail a few things really stand out:

- The collaboration features match on practically a one-to-one basis. Therefore, it amounts to the branding issue—just like people buy Nike shoes over Adidas. The sneakers are practically identical, but people just recognize the Nike brand since it's associated with so many sports figures.
- SmarterMail offers antispam and antivirus at no additional cost upon installation. While you can use add-on services and applications (like the wonderful products from Message Sniffer and Cyren), there's no need.

- Mobility and synchronization are the future, and SmarterMail is there.
- The information is right there, at your fingertips—from anywhere, at any time. Whether it's information on who has sent you what, or if you need to find that spreadsheet that the CMO sent; whether you want to know when you reach 75% of your disk space capacity or need access to your RSS feeds, SmarterMail offers it all right from your Web browser.

Trust and Availability

There's no doubt Microsoft has the name. They've been around a long time, and have a long history of building quality software and being on the leading edge of technology, especially when it comes to providing a robust and feature-rich email solution. However, becoming one of the largest, if not the largest, software and services company doesn't come without some sacrifice. These sacrifices tend towards giving users access to support and customer service - at least affordable access to these critical needs.

That's where SmarterTools comes in.

Over the last eight years, SmarterTools has grown to over 15 million users, but still sees each user as important. They have grown through investment in products and development versus in advertising and marketing, building SmarterMail into one of the most popular and respected mail servers on the market. They realize how safe, secure and reliable communication is vital to each and every user of their product. That's why SmarterTools offers services that cater directly to their customer base:

- Access to LIVE tech support, 24/7/365
- Upgrade and installation services
- A popular, free public community to interact with support and fellow users
- Responsiveness to customers that often leads to product enhancements

While it may be true SmarterTools doesn't have the name recognition as Microsoft, what is certainly not up for debate is SmarterTools' commitment to their customers, to their products, and to their desire to create the most reliable and secure mail server solution on the market.

Taking all of this into consideration, it may not be a question of "why move to SmarterMail from Exchange," or "why choose SmarterMail over Exchange," but more a question of a "why not?"

1 <http://pewinternet.org/Commentary/2012/February/Pew-Internet-Mobile.aspx>

2 <http://www.message-labs.com/intelligence.aspx>

3 <http://www.pewinternet.org/Reports/2010/Mobile-Access-2010.aspx>

4 The Economics of Spam, Justin M. Rao and David H. Reiley

Help for Users & Domain Administrators

Logging in to SmarterMail's Webmail Interface

SmarterMail users can access SmarterMail through a webmail interface in addition to connecting their mailbox to an email client such as Microsoft Outlook for Windows or Mac, MacMail or even using the email clients on most mobile devices. The major advantage of using the webmail interface, however, is that users can login to their SmarterMail mailbox from any computer with an Internet access, anywhere in the world.

To log in to the SmarterMail Web interface, users will need to obtain the appropriate link from their domain administrator or system administrator. Generally, this will take the form of a standard email URL such as <http://mail.example.com>. To login to SmarterMail, simply type your full email address and password in the appropriate fields and click Login .

To stay logged in to SmarterMail even after closing the browser, be sure to select the Remember Me checkbox. This will allow SmarterMail to encrypt the email address and password. Note: Browser cookies must be enabled for this feature to work. In addition, SmarterTools does not recommend selecting this option if you use a public or shared computer.

After clicking the log in button, you will be logged into your SmarterMail mailbox and, depending on your settings, the My Today Page or your inbox will display in the content pane. If you have trouble logging in or experience issues with your email account, contact your domain administrator for troubleshooting help. The domain administrator is usually the owner of the domain or the person who set up your email account.

Logging in with a Smartphone

SmarterMail also provides a mobile interface that was designed specifically for smartphones and other mobile devices with smaller screens (4 inches or less). This is a light, yet fully functional interface that allows SmarterMail users to access their email, contacts, calendars, tasks and notes regardless of their location and connection speed. This mobile interface is accessible either from the link provided on the main SmarterMail webmail interface login page or by appending "/mobile" to the end of the SmarterMail login URL that is provided by a domain or system administrator.

Synchronizing with SmarterMail

Overview

SmarterMail is a powerful collaboration mail server that supports the synchronization of calendars,

tasks, notes, and contacts on desktop applications like Microsoft Outlook and over-the-air synchronization for most popular mobile devices.

It should be noted that synchronization capabilities may vary depending on the edition of SmarterMail that you are using:

- For full synchronization capabilities, SmarterTools recommends upgrading to SmarterMail Enterprise. SmarterMail Enterprise users have the ability to synchronize their mailboxes using any of the protocols discussed in this document.
- SmarterMail Professional users can download their email using IMAP or POP3 retrieval, but they cannot sync calendars, contacts, tasks or notes.
- SmarterMail Free users have the ability to synchronize their mailboxes using any of the protocols discussed in this document except Microsoft Exchange ActiveSync and Exchange Web Services, which are only available as add-ons to SmarterMail Enterprise.
- NOTE: Regarding Windows 8 and Windows Server 2012, only the most current version of SmarterMail was tested and validated for these operating systems. Previous versions may work as well but they may also require you to work around known issues. See the SmarterTools knowledge base for more information.

This document covers the synchronization methods and processes for the following applications and devices:

- Apple OS X
- Apple Address Book
- Apple iCal
- Apple Mail
- Microsoft Windows 8
- Windows 8 Mail
- Windows 8 People
- Windows 8 Calendar
- Cross Platform Options
- Microsoft Outlook
- Mozilla Thunderbird
- Mobile Devices
- Apple iOS
- BlackBerry
- Google Android

- Symbian
- Windows Phone

Note: This is not an exhaustive list of all compatible applications and mobile devices. SmarterTools recommends contacting the manufacturer for details regarding the available synchronization protocols for applications and/or mobile devices not listed in this document.

Who Should Use This Document

This document is intended to be used in conjunction with the SmarterMail Online Help, Knowledge Base articles (KBs), and other SmarterTools reference sources as part of an overall solution. It should be used by:

- Hosting companies, Internet Service Providers (ISPs) and IT professionals as part of a complete SmarterMail communications solution for their customers
- Individual users of SmarterMail seeking to maximize the functionality and features of the SmarterMail account

Synchronization Protocols

SmarterMail uses multiple synchronization technologies to sync mailbox items with email clients and mobile devices:

- Microsoft Exchange ActiveSync is an optional add-on that syncs SmarterMail mailboxes, calendars, contacts -- including contact pictures -- with most mobile devices and many mail clients integrated in the latest operating systems (e.g., Windows 8) as well as with Outlook 2013 for Windows.
- Exchange Web Services is an optional add-on that syncs SmarterMail messages, contacts, calendars and tasks to third-party email clients that support the protocol, including Microsoft Outlook 2015 for Mac from Office 365, Microsoft Outlook 2011 for Mac, Apple Mail, the Outlook client for iPad and eM Client..
- SyncML is a platform-independent synchronization standard that syncs SmarterMail mailboxes with Outlook 2007 and above (32-bit version), Thunderbird, and most mobile devices. NOTE: As of SmarterMail 10.x, SyncML support is no longer being updated as there are fewer and fewer SyncML clients that are continuing development and support. That being said, SyncML will continue to work "as-is" in current and future versions of SmarterMail.
- CalDAV is an extension of the WebDAV protocol that syncs SmarterMail calendars natively with Macs, iPads, iPhones, Thunderbird, and other devices/applications that use the technology. Windows Phone 8 will eventually include native support for CalDAV and there are apps for Android that support CalDAV as well. More information on CalDAV implementations can be found by reviewing Implementations of CalDAV and CardDAV .

- CardDAV is an extension of the WebDAV protocol that syncs SmarterMail contacts -- including contact pictures -- natively with Macs, iPads, iPhones, and other devices/applications that use the technology. Windows Phone 8 will eventually include native support for CardDAV and there are apps for Android that support CardDAV as well. More information on CardDAV implementations can be found by reviewing Implementations of CalDAV and CardDAV .
- The Add to Outlook (Sharepoint Sync) feature within the SmarterMail Webmail interface uses two-way synchronization technology to sync a SmarterMail mailbox with Outlook 2007 or higher and provides read-only capability for Outlook 2003, including a user's shared resources. Calendars and contacts shared at the domain level are not supported. However, Sharepoint Sync does not support notification features, so items like SmarterMail calendar reminders will not be available within Outlook. In addition, Add to Outlook does not sync contact pictures. For full integration, Microsoft Exchange ActiveSync (for mobile devices and Outlook 2013 and above for Windows) or Microsoft Exchange Web Services (for Outlook for Mac and Apple Mail) should be used.

Synchronized Devices

To view the devices and protocols used to synchronize your mailbox, log in to the SmarterMail interface and click the settings icon . Then expand the My Settings and Advanced Settings folders in the navigation pane and click Synchronized Devices . Logging of information, last successful synchronization and the ability to reset the synchronization state of devices is available from this area.

Desktop Applications

SmarterMail supports synchronization with many desktop applications and email clients, including:

- Apple Address Book
- Apple iCal
- Apple Mail
- Windows 8 Mail
- Windows 8 Calendar
- Windows 8 Contacts
- Microsoft Outlook
- Mozilla Thunderbird --%>

Apple OS X

Apple OS X is the primary operating system for the MacBook, Mac mini, iMac and Mac Pro lines of desktops and laptops.

Apple Address Book

Apple Address Book is an application for Mac OS X users built for managing contact data. It is intended to be used in conjunction with Apple's Mail and iCal programs to provide Mac users with full email, calendar, and contact management.

CardDav

Users can synchronize their SmarterMail contacts -- including contact pictures -- with Address Book using the CardDAV protocol. Support for CardDAV is built into both products, so there is no need to download and install additional applications to sync contact data.

For more information, refer to the KB article that applies to the OSX you are using:

- OSX 10.7 Lion: How To Sync SmarterMail with Apple Address Book and iCal
- OSX 10.6 Snow Leopard: How To Sync SmarterMail with Apple Address Book and iCal

SyncML

This method synchronizes contacts by using the Funambol Sync Client for Mac OS X, which is available for download at <https://www.forge.funambol.org/download>. The Funambol Sync Client uses the SyncML 1.2 protocol, which is included within SmarterMail. NOTE: As of SmarterMail 10.x, SyncML support is no longer being updated as there are fewer and fewer SyncML clients that are continuing development and support. That being said, SyncML will continue to work "as-is" in current and future versions of SmarterMail.

Apple iCal

Apple iCal is an application for Mac OS X users built for managing calendar data. It is intended to be used in conjunction with Apple's Mail and Address Book programs to provide Mac users with full email, calendar, and contact management.

CalDav

Users can synchronize their SmarterMail calendars with iCal using the CalDAV protocol. Support for CalDAV is built into both products, so there is no need to download and install additional applications to sync calendar data. For more information, refer to the KB article that applies to the OSX you are using:

- OSX 10.7 Lion: How To Sync SmarterMail with Apple Address Book and iCal
- OSX 10.6 Snow Leopard: How To Sync SmarterMail with Apple Address Book and iCal

Apple Mail

Apple Mail is an email application for Mac OS X users. It is intended to be used in conjunction with Apple's Address Book and iCal programs to provide Mac users with full email, calendar, and contact management.

Exchange Web Services

The Exchange Web Services add-on is available as an optional add-on for SmarterMail Enterprise and can be purchased from the SmarterTools website. Users can use Exchange Web Services to sync messages with Apple Mail on computers running OSX 10.6 (Snow Leopard) or OSX 10.7 (Lion).

Once the Exchange Web Services add-on has been purchased, the system administrator will need to reactivate SmarterMail and enable the add-on for the domain. For more information, refer to the KB article [How To Activate Exchange Web Services](#).

Once the add-on is activated for the domain, users can sync to Apple Mail using the protocol. For more information, refer to the KB article [How To Synchronize SmarterMail with Apple Mail Using Exchange Web Services](#).

NOTE: For mailboxes that will process and store large volumes of email, it is recommended that they be set up to connect to SmarterMail using IMAP as EWS performance suffers when processing large volumes of email.

Message Retrieval

For SmarterMail users with Exchange Web Services, messages will automatically be synchronized with the Apple Mail. SmarterMail users that are using any of the other technologies to sync their mailboxes should set up an account within Apple Mail using either IMAP or POP3.

IMAP is a robust protocol that easily handles mailboxes that process and/or store large volumes of email. In addition, IMAP idle is an optional feature of the IMAP protocol that pushes all new messages out as they are received by the mail server. Unlike POP, IMAP offers two-way communication between your SmarterMail mailbox and your email client(s). This means when you log in to the SmarterMail Web interface, actions you performed on email clients and mobile devices will automatically appear in the Web interface (and vice versa). In addition, IMAP keeps all messages and folders on the server whereas POP downloads all messages to an email client.

With POP3, your mail is saved in a mailbox on the remote server until you check your mail. When you check your mail, all of the mail is downloaded to your computer and is no longer maintained on the server. If you use POP3 and are traveling or check your mail from multiple locations, you will not be able to view any of your old mail because the messages only exist on the computer on which you originally received your mail.

Microsoft Windows 8

Windows 8 is the latest operating system offered by Microsoft that is available for a variety of desktops, laptops and the Microsoft Surface tablet. Windows 8 includes an email client as well as both calendar and contacts applications as part of its default installation, similar to those same features offered by Apple's OS X operating system.

Windows 8 Mail

Windows 8 Mail is an email client that comes pre-installed with Windows 8. It allows users to set up accounts using a variety of methods.

Microsoft Exchange ActiveSync

The Microsoft Exchange ActiveSync add-on is available as an optional add-on for SmarterMail Enterprise and can be purchased from the SmarterTools website. Unlike the other synchronization methods, Exchange ActiveSync uses direct push technology to sync email, calendars, and contacts in real time, ensuring any changes to collaboration data are automatically recorded in both SmarterMail and within Windows 8 Mail.

With the release of Windows 8, Microsoft integrated Exchange ActiveSync with both Microsoft Office 13 as well as within the Windows 8 Mail application that comes as part of the Windows 8 installation. Therefore, administrators and end users can set up Outlook 2013 and/or Windows 8 Mail using the Exchange ActiveSync add-on as well as via IMAP or POP. NOTE: Outlook 2010 and earlier DO NOT support Exchange ActiveSync. ActiveSync is only supported in Outlook 2013 and above.

Once the Exchange ActiveSync add-on has been purchased, the system administrator will need to reactivate SmarterMail and enable the add-on for the user's mailbox. For more information, refer to the KB article [How To Activate Microsoft Exchange ActiveSync](#).

If SmarterMail is running under IIS, the system administrator will also need to disable Windows authentication before adding Exchange ActiveSync to specific mailboxes. For more information, refer to the KB article [How To Configure IIS for Microsoft Exchange ActiveSync](#).

Message Retrieval

For SmarterMail users with Exchange ActiveSync, messages will automatically be synchronized with Outlook. SmarterMail users that are using any of the other technologies to sync their mailboxes should set up an account within Windows 8 Mail using either IMAP or POP3, where possible.

IMAP is a robust protocol that easily handles mailboxes that process and/or store large volumes of email. In addition, IMAP idle is an optional feature of the IMAP protocol that pushes all new messages out as they are received by the mail server. Unlike POP, IMAP offers two-way

communication between your SmarterMail mailbox and your email client(s). This means when you log in to the SmarterMail Web interface, actions you performed on email clients and mobile devices will automatically appear in the Web interface (and vice versa). In addition, IMAP keeps all messages and folders on the server whereas POP downloads all messages to an email client.

With POP3, your mail is saved in a mailbox on the remote server until you check your mail. When you check your mail, all of the mail is downloaded to your computer and is no longer maintained on the server. If you use POP3 and are traveling or check your mail from multiple locations, you will not be able to view any of your old mail because the messages only exist on the computer on which you originally received your mail. (Note: If you have enabled Outlook to keep messages on the server, you will be able to access your messages and folders from any computer via the SmarterMail Web interface or your mobile device.)

Windows 8 People

Windows 8 People is a contacts system that comes pre-installed with Windows 8. It allows users to set up contacts within Windows 8 that can be used for a variety of purposes (e.g., emailing).

Microsoft Exchange ActiveSync

The Microsoft Exchange ActiveSync add-on is available as an optional add-on for SmarterMail Enterprise and can be purchased from the SmarterTools website. Unlike the other synchronization methods, Exchange ActiveSync uses direct push technology to sync email, calendars, and contacts -- including contact pictures -- in real time, ensuring any changes to collaboration data are automatically recorded in both SmarterMail and within Windows 8 Mail.

With the release of Windows 8, Microsoft integrated Exchange ActiveSync with both Microsoft Office 13 as well as within the Windows 8 Mail, People and Calendar applications that come as part of the Windows 8 installation. Therefore, administrators and end users can set up Outlook 2013 and/or Windows 8 Mail using the Exchange ActiveSync add-on as well as via IMAP or POP.

Once the Exchange ActiveSync add-on has been purchased, the system administrator will need to reactivate SmarterMail and enable the add-on for the user's mailbox. For more information, refer to the KB article [How To Activate Microsoft Exchange ActiveSync](#).

If SmarterMail is running under IIS, the system administrator will also need to disable Windows authentication before adding Exchange ActiveSync to specific mailboxes. For more information, refer to the KB article [How To Configure IIS for Microsoft Exchange ActiveSync](#).

Windows 8 Calendar

Windows 8 Calendar is an calendar application that comes pre-installed with Windows 8. It allows

users to set up calendars within Windows 8 that can be used for a variety of purposes (e.g., keeping track of appointments).

Microsoft Exchange ActiveSync

The Microsoft Exchange ActiveSync add-on is available as an optional add-on for SmarterMail Enterprise and can be purchased from the SmarterTools website. Unlike the other synchronization methods, Exchange ActiveSync uses direct push technology to sync email, calendars, and contacts in real time, ensuring any changes to collaboration data are automatically recorded in both SmarterMail and within Windows 8 Mail.

With the release of Windows 8, Microsoft integrated Exchange ActiveSync with both Microsoft Office 13 as well as within the Windows 8 Mail, People and Calendar applications that come as part of the Windows 8 installation. Therefore, administrators and end users can set up Outlook 2013 and/or Windows 8 Mail using the Exchange ActiveSync add-on as well as via IMAP or POP.

Once the Exchange ActiveSync add-on has been purchased, the system administrator will need to reactivate SmarterMail and enable the add-on for the user's mailbox. For more information, refer to the KB article [How To Activate Microsoft Exchange ActiveSync](#).

If SmarterMail is running under IIS, the system administrator will also need to disable Windows authentication before adding Exchange ActiveSync to specific mailboxes. For more information, refer to the KB article [How To Configure IIS for Microsoft Exchange ActiveSync](#).

Cross Platform Options

Microsoft Outlook

Microsoft Outlook is an email client developed by Microsoft Inc. for managing messages, contacts, notes, tasks, and appointments and is commonly distributed as part of the Microsoft Office suite. Outlook is offered on both the Windows and Mac OS X platforms. SmarterMail supports synchronization of email, contacts, calendars, tasks and notes with Outlook 2003 or higher, both on Windows and OS X.

Microsoft Exchange ActiveSync

The Microsoft Exchange ActiveSync add-on is available as an optional add-on for SmarterMail Enterprise and can be purchased from the SmarterTools website. Unlike the other synchronization methods, Exchange ActiveSync uses direct push technology to sync email, calendars, and contacts -- including contact pictures -- in real time, ensuring any changes to collaboration data are automatically recorded in both SmarterMail and within Outlook.

With the release of Windows 8, Microsoft integrated Exchange ActiveSync with both Microsoft Office 13 as well as within the Windows 8 Mail application that comes as part of the Windows 8

installation. Therefore, administrators and end users can set up Outlook 2013 and/or Windows 8 Mail using the Exchange ActiveSync add-on as well as via IMAP or POP.

Once the Exchange ActiveSync add-on has been purchased, the system administrator will need to reactivate SmarterMail and enable the add-on for the user's mailbox. For more information, refer to the KB article [How To Activate Microsoft Exchange ActiveSync](#).

If SmarterMail is running under IIS, the system administrator will also need to disable Windows authentication before adding Exchange ActiveSync to specific mailboxes. For more information, refer to the KB article [How To Configure IIS for Microsoft Exchange ActiveSync](#).

Exchange Web Services

The Exchange Web Services add-on is available as an optional add-on for SmarterMail Enterprise and can be purchased from the SmarterTools website. Users can currently use Exchange Web Services to sync messages, contacts, calendars and tasks with Outlook 2015 for Mac from Office 365, Outlook 2011 for Mac and Apple Mail. At this time, Outlook for Windows does not offer support for EWS.

Once the Exchange Web Services add-on has been purchased, the system administrator will need to reactivate SmarterMail and enable the add-on for the domain. For more information, refer to the KB article [How To Activate Exchange Web Services](#).

Once the add-on is activated for the domain, users can sync to Outlook using the protocol. For more information, refer to the KB article [How To Synchronize SmarterMail with Outlook 2011 for Mac Using Exchange Web Services](#).

NOTE: For mailboxes that will process and store large volumes of email, it is recommended that they be set up to connect to SmarterMail using IMAP as EWS performance suffers when processing large volumes of email.

Add to Outlook

The Add to Outlook (Sharepoint Sync) feature allows for two-way synchronization of calendars, contacts (but not contact pictures) and tasks with Outlook 2007 or higher, including a user's shared resources. Calendars and contacts shared at the domain level are not supported. For more information, refer to the KB article [How To Synchronize SmarterMail with Outlook Using the Add to Outlook Feature](#). However, Sharepoint Sync does not support notification features, so items like SmarterMail calendar reminders will not be available within Outlook. For full integration, Microsoft Exchange ActiveSync (for mobile devices and Outlook 13 and above for Windows) or Microsoft Exchange Web Services (for Outlook for Mac and Apple Mail) should be used.

SyncML

This method synchronizes contacts (but not contact pictures), calendars, tasks, and notes by using the Funambol Sync Client for Microsoft Outlook, which is available for download at http://forge.ow2.org/project/showfiles.php?group_id=96. The Funambol Sync Client uses the SyncML 1.2 protocol, which is included within SmarterMail. Funambol SyncML works for Outlook 2007 and above (32-bit only). NOTE: As of SmarterMail 10.x, SyncML support is no longer being updated as there are fewer and fewer SyncML clients that are continuing development and support. That being said, SyncML will continue to work "as-is" in current and future versions of SmarterMail.

For more information, refer to the KB article [How To Synchronize SmarterMail Accounts with Outlook Using SyncML](#)

Message Retrieval

For SmarterMail users with Exchange Web Services, messages will automatically be synchronized with Outlook. SmarterMail users that are using any of the other technologies to sync their mailboxes should set up an account within Outlook using either IMAP or POP3.

IMAP is a robust protocol that easily handles mailboxes that process and/or store large volumes of email. In addition, IMAP idle is an optional feature of the IMAP protocol that pushes all new messages out as they are received by the mail server. Unlike POP, IMAP offers two-way communication between your SmarterMail mailbox and your email client(s). This means when you log in to the SmarterMail Web interface, actions you performed on email clients and mobile devices will automatically appear in the Web interface (and vice versa). In addition, IMAP keeps all messages and folders on the server whereas POP downloads all messages to an email client.

With POP3, your mail is saved in a mailbox on the remote server until you check your mail. When you check your mail, all of the mail is downloaded to your computer and is no longer maintained on the server. If you use POP3 and are traveling or check your mail from multiple locations, you will not be able to view any of your old mail because the messages only exist on the computer on which you originally received your mail. (Note: If you have enabled Outlook to keep messages on the server, you will be able to access your messages and folders from any computer via the SmarterMail Web interface or your mobile device.)

Mozilla Thunderbird

Mozilla Thunderbird is a free, open source email client developed by the Mozilla Foundation. SmarterMail supports synchronization of email, contacts and calendars with Thunderbird 3.

SyncML

Users can synchronize contacts (but not contact pictures) and calendars with Thunderbird using the Funambol and the Lightning add-ons. Both add-ons are available for free from the Mozilla Thunderbird website. The Funambol add-on uses the SyncML 1.2 protocol to synchronize collaboration items and the Lightning add-on provides calendar functionality for Thunderbird. NOTE: As of SmarterMail 10.x, SyncML support is no longer being updated as there are fewer and fewer SyncML clients that are continuing development and support. That being said, SyncML will continue to work "as-is" in current and future versions of SmarterMail.

After installing the add-ons, users will need to configure the Funambol add-on from within the Thunderbird interface.

For more information, refer to the KB article [How To Install and Configure Lightning and Funambol for Thunderbird](#)

CalDav

Users can also synchronize their SmarterMail calendars with Thunderbird using the CalDAV protocol and the Lightning add-on. For more information, refer to the KB article [Sync with Thunderbird Using CalDAV for Lightning](#)

Message Retrieval

For messages, users should set up an account within Thunderbird using either IMAP or POP3.

IMAP is a robust protocol that easily handles mailboxes that process and/or store large volumes of email. In addition, IMAP idle is an optional feature of the IMAP protocol that pushes all new messages out as they are received by the mail server. Unlike POP, IMAP offers two-way communication between your SmarterMail mailbox and your email client(s). This means when you log in to the SmarterMail Web interface, actions you performed on email clients and mobile devices will automatically appear in the Web interface (and vice versa). In addition, IMAP keeps all messages and folders on the server whereas POP downloads all messages to an email client.

With POP3, your mail is saved in a mailbox on the remote server until you check your mail. When you check your mail, all of the mail is downloaded to your computer and is no longer maintained on the server. If you use POP3 and are traveling or check your mail from multiple locations, you will not be able to view any of your old mail because the messages only exist on the computer on which you originally received your mail.

Mobile Devices

SmarterMail supports synchronization with most mobile devices on the market, including:

- Apple iOS
- BlackBerry
- Google Android
- Symbian
- Windows Phone

Apple iOS

Apple iOS devices include the iPod Touch, iPhone and the iPad. SmarterMail supports synchronization of email, contacts, and calendars with iOS devices.

Microsoft Exchange ActiveSync

The Microsoft Exchange ActiveSync add-on is available as an optional add-on for SmarterMail Enterprise and can be purchased from the SmarterTools website. Unlike the other synchronization methods, Exchange ActiveSync uses direct push technology to sync email, calendars, and contacts -- including contact pictures -- in real time, ensuring any changes to collaboration data are automatically recorded in both SmarterMail and the mobile device.

Once the Exchange ActiveSync add-on has been purchased, the system administrator will need to reactivate SmarterMail and enable the add-on for the user's mailbox. For more information, refer to the KB article [How To Activate Microsoft Exchange ActiveSync](#).

If SmarterMail is running under IIS, the system administrator will also need to disable Windows authentication before adding Exchange ActiveSync to specific mailboxes. For more information, refer to the KB article [How To Configure IIS for Microsoft Exchange ActiveSync](#).

For synchronization instructions for a specific mobile device, refer to the manufacturer's website. Additional information may be available in the SmarterTools Knowledge Base.

CardDAV and CalDAV

SmarterMail users that choose not to purchase the Exchange ActiveSync add-on can synchronize their SmarterMail contacts -- including contact pictures -- and calendars with iOS devices using the CardDAV and CalDAV protocols. Support for CardDAV and CalDAV is built into these products, so there is no need to download and install additional applications to sync contact and calendar data.

For more information, refer to the KB article that applies to the OSX you are using:

- OSX 10.7 Lion: [How To Sync SmarterMail with Apple Address Book and iCal](#)
- OSX 10.6 Snow Leopard: [How To Sync SmarterMail with Apple Address Book and iCal](#)

SyncML

A third solution is also available to sync contacts over-the-air. This solution uses the iPhone Sync Client from Funambol, which is available for download in Apple's App Store. The iPhone Sync Client uses the SyncML 1.2 protocol, which is included within SmarterMail. NOTE: As of SmarterMail 10.x, SyncML support is no longer being updated as there are fewer and fewer SyncML clients that are continuing development and support. That being said, SyncML will continue to work "as-is" in current and future versions of SmarterMail.

For more information, refer to the KB article [How To Synchronize SmarterMail with Mobile Devices Using SyncML](#).

BlackBerry

BlackBerry is a line of smartphones developed by Research In Motion. SmarterMail supports synchronization of email, contacts, calendars, tasks, and notes with the BlackBerry.

Microsoft Exchange ActiveSync

The Microsoft Exchange ActiveSync add-on is available as an optional add-on for SmarterMail Enterprise and can be purchased from the SmarterTools website. Unlike the other synchronization methods, Exchange ActiveSync uses direct push technology to sync email, calendars, and contacts in real time, ensuring any changes to collaboration data are automatically recorded in both SmarterMail and the mobile device.

Although the Blackberry does not directly support over-the-air synchronization with Exchange ActiveSync, there are two applications available for purchase that enable Exchange ActiveSync functionality on the Blackberry: AstraSync and NotifySync. For more information, refer to www.astrasync.com and www.notifysync.com.

Once the Exchange ActiveSync add-on has been purchased, the system administrator will need to reactivate SmarterMail and enable the add-on for the user's mailbox. For more information, refer to the KB article [How To Activate Microsoft Exchange ActiveSync](#).

If SmarterMail is running under IIS, the system administrator will also need to disable Windows authentication before adding Exchange ActiveSync to specific mailboxes. For more information, refer to the KB article [How To Configure IIS for Microsoft Exchange ActiveSync](#).

For synchronization instructions for a specific mobile device, refer to the manufacturer's website. Additional information may be available in the SmarterTools Knowledge Base.

SyncML

For those users that choose not to purchase the Exchange ActiveSync add-on, an alternate solution is available to sync contacts (but not contact pictures), calendars, tasks, and notes over-the-air. This solution is to use the BlackBerry Sync Client from Funambol, which is available for download at http://forge.ow2.org/project/showfiles.php?group_id=96. The BlackBerry Sync Client uses the SyncML 1.2 protocol, which is included within SmarterMail. The client supports most BlackBerry devices, and SmarterTools has tested models 8830, 8810, and Curve devices. NOTE: As of SmarterMail 10.x, SyncML support is no longer being updated as there are fewer and fewer SyncML clients that are continuing development and support. That being said, SyncML will continue to work "as-is" in current and future versions of SmarterMail.

For more information, refer to the KB article [How To Synchronize SmarterMail with Mobile Devices Using SyncML](#).

Message Retrieval

For regular and push email usage, SmarterTools offers the following methods:

- The BlackBerry Internet Service is a free method to push email to your BlackBerry and is a service provided by your mobile phone provider (Sprint, Verizon, etc.) and can be configured to check your SmarterMail mailbox and push all new and unread messages to your mobile phone. Messages are normally pushed to the BlackBerry device with a short delay. This can be configured with any version of SmarterMail as the BlackBerry Internet Service will connect to the mailbox via the IMAP protocol.
- An alternative free method to push messages to your mobile phone which is normally only delayed a couple minutes and simulates the expensive BlackBerry Enterprise Server (BES) which is often associated with Microsoft Exchange is to use the open source provider Funambol. By signing up with the free Funambol service, you can (just as with the BlackBerry Internet Service), configure Funambol to scan your SmarterMail mailbox for new and unread messages. If a new message is found, the Funambol service will push the message to the BlackBerry device and the Funambol client program. When you sign up for the Funambol service, they will provide you the appropriate client that should be installed on your BlackBerry device. This method provides a significant cost savings over the formal BES method with only a modest diminishment in performance.
- Since the BlackBerry is focused on pushing email, many consumers who are familiar with IMAP and PocketPCs miss the advantage of having access to all their messages that they see within Outlook or the webmail interface. For people who would like to log into the SmarterMail mailbox from the BlackBerry and see all of their messages as if they were in webmail,

additional clients can be installed on the BlackBerry, such as the free open source application LogicMail .

Google Android

Android is an operating system designed for use in a variety of smartphones and mobile devices. Examples of devices that run on Google Android include the Motorola Droid 3, Samsung Galaxy Tab, and HTC Droid Incredible. In addition, the Kindle Fire runs on a modified version of the Android operating system. SmarterMail supports synchronization of email, contacts, and calendars with Android devices.

Microsoft Exchange ActiveSync

The Microsoft Exchange ActiveSync add-on is available as an optional add-on for SmarterMail Enterprise and can be purchased from the SmarterTools website. Unlike the other synchronization methods, Exchange ActiveSync uses direct push technology to sync email, calendars, and contacts -- including contact pictures -- in real time, ensuring any changes to collaboration data are automatically recorded in both SmarterMail and the mobile device.

Note: Only Android devices running version 2.0 or later support synchronization via Exchange ActiveSync. Support for Exchange ActiveSync may also vary by device. For example, Exchange ActiveSync does not support Corporate Calendar or email applications for the Motorola Droid, Droid 2 or Droid X because they are custom applications that do not comply with Exchange ActiveSync specifications.

Once the Exchange ActiveSync add-on has been purchased, the system administrator will need to reactivate SmarterMail and enable the add-on for the user's mailbox. For more information, refer to the KB article [How To Activate Microsoft Exchange ActiveSync](#) .

If SmarterMail is running under IIS, the system administrator will also need to disable Windows authentication before adding Exchange ActiveSync to specific mailboxes. For more information, refer to the KB article [How To Configure IIS for Microsoft Exchange ActiveSync](#) .

For synchronization instructions for a specific mobile device, refer to the manufacturer's website. Additional information may be available in the SmarterTools Knowledge Base.

CardDAV and CalDAV

SmarterMail users that choose not to purchase the Exchange ActiveSync add-on can synchronize their SmarterMail contacts and calendars with Android devices using the CardDAV and CalDAV protocols. While the default calendar and contacts apps may NOT support either protocol, there are some Android apps that do support both. IN addition, there are CalDAV and CardDAV specific apps that

can facilitate synchronization, though these may be paid apps. More information and implementations of CalDAV and CardDAV can be found by reviewing [Implementations of CalDAV and CardDAV](#).

Message Retrieval

For SmarterMail users with Exchange ActiveSync mailboxes, messages will automatically be pushed to their mobile devices as they are received. SmarterMail users that are using any of the other technologies to sync their mailboxes with a mobile device should set up an account within the mail application provided on the mobile device using either IMAP or POP3.

IMAP is a robust protocol that easily handles mailboxes that process and/or store large volumes of email. In addition, IMAP idle is an optional feature of the IMAP protocol that pushes all new messages out as they are received by the mail server. Unlike POP, IMAP offers two-way communication between your SmarterMail mailbox and your email client(s). This means when you log in to the SmarterMail Web interface, actions you performed on email clients and mobile devices will automatically appear in the Web interface (and vice versa). In addition, IMAP keeps all messages and folders on the server whereas POP downloads all messages to an email client.

With POP3, your mail is saved in a mailbox on the remote server until you check your mail. When you check your mail, all of the mail is downloaded to your computer and is no longer maintained on the server. If you use POP3 and are traveling or check your mail from multiple locations, you will not be able to view any of your old mail because the messages only exist on the computer on which you originally received your mail.

Windows Phones

Windows Phone is a compact operating system developed by Microsoft and designed for use in a variety of smartphones and mobile devices. Examples of devices that run on Windows Phone (or the Windows Mobile OS) include the Samsung Focus, HTC HD7 and Nokia Lumia. SmarterMail supports synchronization of email, calendars, contacts, tasks and notes with Windows Phones.

Microsoft Exchange ActiveSync

The Microsoft Exchange ActiveSync add-on is available as an optional add-on for SmarterMail Enterprise and can be purchased from the SmarterTools website. Unlike the other synchronization methods, Exchange ActiveSync uses direct push technology to sync email, calendars, and contacts -- including contact pictures -- in real time, ensuring any changes to collaboration data are automatically recorded in both SmarterMail and the mobile device.

Once the Exchange ActiveSync add-on has been purchased, the system administrator will need to reactivate SmarterMail and enable the add-on for the user's mailbox. For more information, refer to the KB article [How To Activate Microsoft Exchange ActiveSync](#).

If SmarterMail is running under IIS, the system administrator will also need to disable Windows authentication before adding Exchange ActiveSync to specific mailboxes. For more information, refer to the KB article [How To Configure IIS for Microsoft Exchange ActiveSync](#).

For synchronization instructions for a specific mobile device, refer to the manufacturer's website.

Additional information may be available in the SmarterTools Knowledge Base.

SyncML

SyncML For those users that choose not to purchase the Exchange ActiveSync add-on, an alternate solution is available to sync contacts (but not contact pictures), calendars, and tasks over-the-air. This solution is the Pocket PC Sync Client or SmartPhone Sync Client Funambol, which are available for download at http://forge.ow2.org/project/showfiles.php?group_id=96. These sync clients use the SyncML 1.2 protocol, which is included within SmarterMail. NOTE: As of SmarterMail 10.x, SyncML support is no longer being updated as there are fewer and fewer SyncML clients that are continuing development and support. That being said, SyncML will continue to work "as-is" in current and future versions of SmarterMail.

For more information, refer to the KB article [How To Synchronize SmarterMail with Mobile Devices Using SyncML](#).

Message Retrieval

For SmarterMail users with Exchange ActiveSync mailboxes, messages will automatically be pushed to their mobile devices as they are received. SmarterMail users that are using any of the other technologies to sync their mailboxes with a mobile device should set up an account within the Pocket Outlook application provided on the mobile device using either IMAP or POP3.

IMAP is a robust protocol that easily handles mailboxes that process and/or store large volumes of email. In addition, IMAP idle is an optional feature of the IMAP protocol that pushes all new messages out as they are received by the mail server. Unlike POP, IMAP offers two-way communication between your SmarterMail mailbox and your email client(s). This means when you log in to the SmarterMail Web interface, actions you performed on email clients and mobile devices will automatically appear in the Web interface (and vice versa). In addition, IMAP keeps all messages and folders on the server whereas POP downloads all messages to an email client.

With POP3, your mail is saved in a mailbox on the remote server until you check your mail. When you check your mail, all of the mail is downloaded to your computer and is no longer maintained on the server. If you use POP3 and are traveling or check your mail from multiple locations, you will not be able to view any of your old mail because the messages only exist on the computer on which you originally received your mail.

My Today Page

Upon logging in to SmarterMail for the first time, the My Today Page will load. This page provides is divided into five sections and gives users an at-a-glance view of their account. Note: Although the My Today Page is the default page upon login, users can configure SmarterMail to load their inbox upon login instead. For more information, please refer to Account Settings .

- Calendar - Lists upcoming meetings and events, by day and time, for the current week. See the Calendars overview for more information.
- Unread Messages - Lists the number of unread messages in your inbox and in your drafts and junk e-mail folders. Seeing the number of items in your junk e-mail folders can help with any potential disk space issues. For example, if you are closing in on a disk space limit and have a lot of messages in your junk e-mail folder, clearing out those messages may recover some disk space for your mailbox.
- Disk Space Limits - Lists the amount of available disk space and the amount of space currently being used. These are set by the domain administrator. Therefore, if you notice that you are nearing a limit, contact your domain administrator for more information on how to recover some disk space.
- Tasks - Lists any unfinished tasks you may have. See the Tasks overview for more information.
- Latest RSS Items - Lists the most recent updates to the RSS feeds to which you are subscribed. See the RSS Feeds overview for more information.

Email

Email Overview

SmarterMail users can send and receive email messages from anywhere in the world using any computer with a Web browser and Internet access. To login to SmarterMail simply use the link to the webmail interface login page provided by your domain administrator or system administrator. On the login page, type your full email address and password in the appropriate fields and click Login . Depending on your account settings, either your SmarterMail inbox or the My Today Page will load.

To help you understand the different areas of your inbox, we created a simple inbox interface diagram that lists the various features and viewing areas of the SmarterMail webmail interface.

Navigating Your Inbox

To sort messages, click on the appropriate column header for either a descending or ascending sort order for that column. For example, clicking the Size column header will sort items in order of size. Click the header again and the sort will go in the opposite direction.

In general, the following columns are available in the content pane:

- Checkbox - Use these boxes to select multiple messages. Messages must be selected before choosing an action from the actions toolbar.
- From - The sender of the email message.
- Subject - The subject of the email message.
- Date - The date and/or time the mail system received the email.
- Size - The size of the email in kilobytes.
- Status and attachment Indicators - The status icons inform the user of what actions have been taken for each message in their inbox and they appear just to the left of the message size. The icons are as follows: a blue arrow pointing left indicates a reply; a green arrow pointing right indicates a forward; the calendar indicates a new appointment invite or appointment invite response; a paperclip indicates the message has an attachment.
- Follow-up Flag - If the message is marked for follow-up, the flag icon next to the message size will be red. If the message is not marked for follow-up, the flag icon will have a gray outline.

Performing Email Actions

In general, the following options are available from the navigation pane toolbar:

- Actions -
 - New Folder - Select this option to create a new folder. Note: Users should create new folders in the root of the folder tree and NOT inside their Inbox. This is because many email clients have a hard time syncing with folders that are created inside a user's Inbox.
 - Rename Folder - With the desired folder selected, click this option to rename the folder. Note: Default folders can not be renamed. This option applies only to additional folders that have been created.
 - Delete Folder - With the desired folder selected, click this option to delete the folder. Note: Default folders can not be renamed. This option applies only to additional folders that have been created.
 - Disposable Address - Select this option to create a randomly generated address, completely independent of a user's current email address. This email address acts as a timed alias, forwarding mail to the designated folder for the time specified. When the time limit has been

reached, the address is no longer valid and email will not reach your mailbox from this address. (This option is useful when temporarily signing up for newsletters, when an alternate email address is only needed for a short amount of time, etc.) Only one Disposable Address may be created at a time. After creation, extend the time remaining or revoke the address by clicking on Disposable Address again in the Actions toolbar and choosing the corresponding button. Choosing to extend the address will add 4 more hours to the remaining time. Note: Temporary email accounts automatically bypass greylisting and spam checks; however, they still run through any virus scan, if set up.

Note: For more information on the folder options above, see [Managing Email Folders](#).

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

- New - Click this button to create a new email message.
- Actions - Click this button and select the appropriate option to mark messages, move messages, forward multiple messages or block/unblock senders.
- Mark - Click this button and select the appropriate option to mark the selected message(s) as read, unread, follow-up, no follow-up, spam, or not spam.
- Read - Marks the selected message(s) as read and changes the status indicator appropriately.
- Unread - Marks the selected message(s) as unread and changes the status indicator appropriately. This can be useful for reviewing messages at a later time.
- Follow-up - Marks the selected message(s) for follow-up and changes the color of the follow-up flag appropriately. Alternatively, users can click on the flag icon next to the message to mark it for follow-up.
- No follow-up - Removes the selected message(s) as being marked for follow-up and changes the color of the follow-up flag appropriately. Alternatively, users can click on the flag icon next to a message marked for follow-up to remove the follow-up flag.
- Spam - Moves the message to the Junk Email folder.
- Not Spam - Marks the selected message(s) as not spam and automatically adds the email address to your trusted senders list.
- Move - Moves the selected message(s) to any available folder. Note: You can also drag-and-drop messages to an available folder.
- Forward - Forwards the selected message(s). Note: This option is best used when trying to forward multiple messages as .eml attachments.
- Block Sender - Prevents the sender of the selected message(s) from sending any more messages to the account. When you block a sender, a new Internal Blocked Senders Content Filter is created. Any user you block is added to that list, and their email is, by default, deleted.
- Unblock Sender - Allows the sender of the selected message(s) to begin sending messages to

the account again by removing the address from the Internal Blocked Senders content filter.

- Delete - Click this button and select the appropriate option to delete, undelete, purge deleted messages, or delete all messages in a folder.

- Delete - Moves the selected message(s) to the Deleted Items folder. Note: This is the default action taken when a message is deleted. Depending on your account settings, the delete action may be different. For more information, see [Deleting Email Messages](#).

- Undelete - Retrieves deleted messages from your Deleted Items folder provided the system hasn't been purged yet. Note: After the system purges any items marked for deletion, you can't retrieve the deleted messages.

- Purge Marked as Deleted - Permanently deletes the messages in your Deleted Items folder.

Note: This action cannot be undone.

- Delete All Messages in Folder - Moves all of the messages within a selected folder to the Deleted Items folder. This option takes the same action as delete, except that it will perform the delete operation on every email in the folder, regardless of whether the message is checked or not. This option is most useful in folders like Junk E-Mail or Deleted Items.

- View - Click this button and select the appropriate option to filter messages or refresh the content pane.

- Refresh - Manually refreshes the list of messages in the content pane.

- Filter - Filters messages based on the criteria you choose: messages that have been read/unread, replied to or not or forwarded.

In general, the following options are available from the preview pane toolbar:

- Reply - Allows you to reply to the the sender only.
- Reply All - Addresses a response to the sender and everyone else who received the message. This includes all email addresses listed in the To and Cc fields, except your own email address.
- Forward - Sends the message to someone else.
- Delete - Moves the message to the Deleted Items folder. Note: This is the default action taken when a message is deleted. Depending on your account settings, the delete action may be different. For more information, see [Deleting Email Messages](#).
- Add - Creates a new task and links it to the message. For more information, see [Linking to Email Tasks](#).
- View - Allows you to view the original message in alternate formats, including HTML (default), as text only, view the raw content of the message (including the header) or view the header only. Viewing the raw content or just the header can assist with diagnosing potential issues with viewing the message.
- Print - Prints the message.

Reading Email Messages

SmarterMail displays whether you have unread email in your inbox, or in any folders, a number of different ways. Note: The first three notification types are demonstrated in the email interface diagram

- The number of unread messages will display next to the name of the folder in the navigation pane.
- Unread messages display as bold in the content pane.
- The number of unread messages in your inbox displays as part of the Email icon in the icon bar, to the left of the content pane.
- A new message notification, also known as a "toast notification," will temporarily display in the lower left corner of the webmail interface. Note: This feature can be disabled from the Account Settings page.

To view the contents of a message, simply click the desired message and it will load in the preview pane. You can also double-click the message and it will open in a separate pop-up window.

In general, the following options are available when viewing a message in a pop-up window:

- Reply - Allows you to respond to the sender only.
- Reply All - Allows you to respond to the sender and everyone else who received the message. This includes all email addresses listed in the To and Cc fields, except your own email address.
- Forward - Allows you to send the message to a third-party, not in the To or Cc fields.
- Delete - Moves the message to the Deleted Items folder. Note: This is the default action taken when a message is deleted. Depending on your account settings, the delete action may be different. For more information, see Deleting Email Messages .
- Move - Moves the selected message(s) to any available folder.
- Mark - Click this button and select the appropriate option to mark the selected message(s) as follow-up, no follow-up, or spam.
- Follow-up - Marks the selected message(s) for follow-up and changes the color of the follow-up flag appropriately.
- No follow-up - Removes the selected message(s) as being marked for follow-up and changes the color of the follow-up flag appropriately.
- Spam - Moves the message to the Junk Email folder.
- Add - Creates a new task and links it to the message. For more information, see Linking to Email Tasks .
- View - By default, SmarterMail displays messages in HTML format because it provides

formatting and markup capabilities that are not available in plain text. However, there may be times when you want to view the message in a different format or you need to view more than the message content. The different view options are as follows:

- HTML - Displays the message in HTML format, which allows for colors, fonts, graphics, and other formatting.
- Text - Displays the message in plain text, which only allows text content with no special formatting or graphics.
- Raw Content - Displays the content of the email exactly as the server received it. This is helpful if you cannot view the message in any other display mode.
- Header - Displays the header of the message, which indicates the path the email took to get to your email account, along with several other pieces of information.
- Print - Prints the message in whatever View you're in. For example, if you're viewing the raw content of the message then hit the print button, you will print the raw content.
- Close - If a message is opened in a new window, this closes the window.

Downloading Email Attachments

If the message has an attachment, a paperclip will display in the header of the message. In addition, an attachments tab will display under the message header in the preview pane. To view a file that was attached to a message, click the attachments tab and then click the appropriate file. Attachments can be downloaded and viewed individually or it's possible to download all attachments in one .ZIP file by simply clicking the Download All Attachments link that appears at the top of the Attachments tab.

SmarterMail also makes it easy for users to see all messages that contain attachments. Simply, expand the By Type click All Attachments at the bottom of the navigation pane.

Composing Email Messages

It's very easy to create new messages in SmarterMail as well as reply to existing messages or forward messages on to other individuals or groups. Below you'll find a brief walkthrough of each scenario.

Creating a New Message

To create a new message, click New in the navigation pane toolbar or click New + Message from the icon bar. This will open a new message window that you will use to compose the email message.

The following fields will appear in the header of the message:

- From - Select the email address from which the message will be sent and/or the signature to use in this message. Note: This field only displays if the user has multiple addresses from which messages can be sent in SmarterMail (SMTP accounts or domain aliases) or has multiple

signatures configured for the account. If the domain administrator has disabled the ability to override domain-level signatures, the user cannot choose an alternative signature for their SmarterMail email address.

- To - Type the email address for each primary recipient you want to receive your email. Multiple addresses can be used, simply separate each with a comma or semi-colon. Alternatively, click To in order to open your address book/contacts list and select recipients from there. SmarterMail Enterprise users can change the address book used to select email addresses from the Global Address List. Note: When entering addresses into the To, Cc, and Bcc fields, SmarterMail will auto-complete addresses by referencing your contacts list, mailing lists, your Auto-complete list , aliases or the Global Address List.
- Cc - Type the email addresses of recipients that should receive a carbon copy of the message. Alternatively, click Cc in order to open your address book/contacts list and select recipients from there.
- Bcc - Type the email addresses of recipients that should receive a blind carbon copy of the message. Alternatively, click Bcc in order to open your address book/contacts list and select recipients from there. Note: Emails listed in this field will be concealed from the complete list of recipients (those listed in the To and Cc fields). In addition, in a Reply All scenario, Bcc users do NOT receive a copy of the reply. For this reason, it is common practice to use the Bcc field when addressing a very long list of recipients or a list of recipients that should not (necessarily) know each other.
- Subject - Type a descriptive subject or title of the email.

The following options are available in the toolbar of the new message window:

- Send - Sends your message to the designated recipients.
- Save as Draft - Saves the message in its current state to the Drafts folder without actually sending it. This is useful if you need to continue writing the message at a later time.
- Attach Files - Allows you to attach files to the message. When files are attached to an outgoing message, a file manager will display at the bottom of the new message window. The file manager will display the name, size, and upload status of the file. Attachments must reach an upload status of 100% before the item is actually attached to the message. In addition, files that are attached to messages should NOT contain commas as this will corrupt the upload and attachment. Note: To remove an attached file prior to sending the message, click the trash icon in the file manager.
- Link From - Uses SmarterMail's File Storage feature to insert a link to a file saved on the mail server or connect a Google Drive account to SmarterMail. Either way, the links can be sent to recipients who can then download the linked file(s).
- Flags - Specifies delivery options and/or marks the message for follow-up.

- Message Priority - Specifies the importance of the message. By default, messages have a normal level of priority.
- Request a Read Receipt - Sends an email confirmation to the sender when the recipient opens the message.
- Mark for Follow-up - Marks the message for follow-up. For more information, see [Marking Email for Follow-ups](#).

Replying to Email Messages

Alternatively, you may want to reply to the sender or to all of the recipients of a message. SmarterMail gives users two options for replying to a message:

- Reply - Addresses a response to the sender only.
- Reply All - Addresses a response to the sender and everyone else who received the message. This includes all email addresses listed in the To and Cc fields, except your own email address.

When replying to a message, SmarterMail automatically fills in the address fields with the email addresses of the recipients from the original message, the subject field with the subject from the original message preceded by "Re" (which means "regarding" or "in regards to"), and the text box with the text from the original message. It is possible to edit any of these pre-filed fields, however, as needed. All other message options are the same as when composing a new message.

Forwarding Email Messages

You may also want to simply forward a message to a third-party or to someone not already copied on the original message. This is very easy to do:

- Forward - Allows you to send the message to a third-party, not in the To or Cc fields.

When forwarding a message, SmarterMail automatically fills in the subject field with the subject from the original message preceded by "Fwd" (which means "Forward"), and the text box with the text from the original message. It is possible to edit any of these pre-filed fields, however, as needed. All other message options are the same as when composing a new message.

Additional Options

- Delete - Moves the message to the Deleted Items folder. Note: This is the default action taken when a message is deleted. Depending on your account settings, the delete action may be different. For more information, see [Deleting Email Messages](#).
- Move - Moves the selected message(s) to any available folder.
- Mark - Click this button and select the appropriate option to mark the selected message(s) as follow-up, no follow-up, or spam.

- Follow-up - Marks the selected message(s) for follow-up and changes the color of the follow-up flag appropriately.
- No follow-up - Removes the selected message(s) as being marked for follow-up and changes the color of the follow-up flag appropriately.
- Spam - Moves the message to the Junk Email folder.
- Add - Creates a new task and links it to the message. For more information, see [Linking to Email Tasks](#).
- View - By default, SmarterMail displays messages in HTML format because it provides formatting and markup capabilities that are not available in plain text. However, there may be times when you want to view the message in a different format or you need to view more than the message content. The different view options are as follows:
 - HTML - Displays the message in HTML format, which allows for colors, fonts, graphics, and other formatting.
 - Text - Displays the message in plain text, which only allows text content with no special formatting or graphics.
 - Raw Content - Displays the content of the email exactly as the server received it. This is helpful if you cannot view the message in any other display mode.
 - Header - Displays the header of the message, which indicates the path the email took to get to your email account, along with several other pieces of information.
 - Print - Prints the message in whatever View you're in. For example, if you're viewing the raw content of the message then hit the print button, you will print the raw content.
 - Close - If a message is opened in a new window, this closes the window.

Searching Email Messages

As time passes, finding a specific email can become increasingly difficult. Fortunately, SmarterMail's basic search tool allows users to find emails quickly and easily.

To perform a basic search, type the search criteria in the search bar located near the top of the content pane. Then click the magnifying glass or press Enter on your keyboard. SmarterMail will automatically search the the messages within the folder you are viewing for matches and display the results in the content pane. Note: Your search criteria may include letters and numbers. SmarterMail does not search for special characters such as "@" "#" or "%."

To search multiple folders at once or to search other areas of your SmarterMail mailbox, use the advanced search feature. For more information, see [Advanced Search Overview](#).

Deleting Email Messages

SmarterMail has two different methods for deleting messages. You can either drag and drop messages from a folder to Deleted Items or delete them using the Delete menu.

The action SmarterMail takes when you delete a message depends on the option you choose for the Delete Action on the Webmail tab in your Account Settings . These options include:

- Move to Deleted Items folder - When items are deleted they are moved to the Deleted Items folder. If the Deleted Items folder does not exist, it will be created automatically the first time you delete a message.
- Auto-purge folder - When using IMAP or webmail and messages are deleted from a folder, they are only marked as deleted. Messages are not physically removed from the folder until they are purged. This option will automatically purge the folder after deleting the message. Note: When deleted messages are purged, the action is final. You will not be able to retrieve these messages later.
- Mark as deleted - When the message is deleted with this option, the message remains in the current folder, but will be crossed out and marked as deleted. If the folder is then purged, all items marked for deletion will be removed.
- Mark as deleted and hide - With this option, any message that has been marked as deleted will be hidden from view in webmail. This will allow you to keep deleted messages without seeing them every time you log into your mailbox. Note: It is important to keep an eye on your email account disk usage when using this option, as your mailbox may be fuller than you realize.

It is important to note that the action taken for deleted items will ONLY be taken when deleting items through webmail. Deleting an item from Outlook or another email client will NOT use the setting that you choose. Note: When your email client connects to SmarterMail via POP3, any emails that are marked as deleted are automatically purged. To prevent this from happening, select the Move to Deleted Items folder option to avoid accidentally purging deleted items.

Undeleting Messages

Didn't mean to delete a message? You can retrieve deleted messages from your Deleted Items folder as long as the system hasn't been purged yet. Just open the Deleted Items folder and select the desired message(s). Then drag the selected message(s) to your Inbox or another folder. Alternatively, you can select the message(s), click the Delete button and select Undelete from the dropdown. Note: Your system administrator can permanently remove the messages in your Deleted Items folder at any time without warning, so don't delete messages if you might want them later. After the system purges any items marked for deletion, you can't retrieve the deleted messages.

Effects of Folder Auto-clean

Your system administrator may have established auto-clean policies that may delete older junk e-mail, deleted items, and/or sent items when these folders get too large. However, they may have left the option available for you to override auto-clean settings. For more information, see [Folder Auto-clean](#).

Marking Email for Follow-up

One method for managing email messages in SmarterMail is by flagging them so that they can be dealt with at a later time. For example, if you can't respond to an important message right away, you can flag that message as soon as you read it. This allows you to easily see that the message requires follow-up action.

There are a couple of ways for users to flag a message. The first is to simply click on the flag icon at the far right side of the message list in the content pane in webmail. Secondly, users can select the desired message and click the Actions menu in the content pane toolbar, then click Mark and click Follow-up. In both instances, the flag icon will turn red and the message will also appear in the follow-up view, giving you easy access to all messages that require a further action.

It should be noted that the ability to flag messages in SmarterMail is primarily intended to help users easily identify messages that need follow-up. The functionality is supported through the IMAP protocol and some sync protocols, such as the Microsoft Exchange ActiveSync add-on, so that flagged messages will sync with email clients like Outlook as well as email clients on some mobile devices.

Finding Flagged Messages

Although flags help messages stand out in a list, it may be difficult to find a specific flagged message if you have a lot of messages in your inbox. To quickly view all messages marked for follow-up, expand the By Type treeview menu item at the bottom of the navigation pane and click Follow-up and a list of all flagged messages will appear.

Removing a Follow-up Flag

To unmark a message for follow-up, select the desired message and click the Actions menu in the content pane toolbar. Then click Mark and click No Follow-up. The flag icon will turn white and the message will no longer appear in the follow-up view. Note: Users can also toggle the follow-up flag on and off by clicking the flag from the content pane.

Linking Email to Tasks

Email exchanges can often result in the need to create one or two more tasks. For example, an email exchange with a vendor may require updates to price sheets or shipping requirements. Perhaps an

email from a significant other mentions an upcoming birthday or anniversary. Because of this, SmarterMail includes the ability to create a new task right from within an email message. This is called "linking" an email message to a task.

To link a task to a message, first you'll want to open and view the desired message. From the preview pane, click the Add menu and then click Task . This will open a new task window that you will use to create the task. Once the new task has been saved, a tasks tab will display at the top of the message window. Clicking on this tab will allow you to see all the tasks that are linked to the message.

Finding Messages with Linked Tasks

To quickly view all emails that are linked to tasks, expand the By Type treeview menu option at the bottom of the navigation pane and click Linked to Tasks to display all messages that also have tasks attached to them.

Managing Email Folders

On first glance, SmarterMail users will notice that their mailbox has five special-purpose, permanent folders that can't be removed or renamed:

- **Inbox** - All incoming messages automatically go to your Inbox folder. You can read your mail in the Inbox, then delete it, move it to another folder or leave it in the Inbox. Note: If you have set up content filtering for your mailbox, incoming messages may bypass your Inbox per your content filtering settings.
- **Deleted Items** - When you delete messages, by default they're moved to the Deleted Items folder. (Just know that, this default action can change based on your settings - see Deleting Email Messages for more information). Messages in the Deleted Items folder can be deleted at any time without warning depending on any auto-clean settings your system administrator has in place, so it's best if you don't delete messages if you think you'll want them later. The Deleted Items folder is the default folder SmarterMail creates for deleted items. When migrating from other email systems to SmarterMail, the migration may create a different folder for deleted items based on what that email system uses as its default. Note: When creating folders, it's not recommended to create them within the Inbox as many email clients, especially mobile clients, have difficulty syncing folders created within the Inbox. For more information on creating folders, see the corresponding section, below.
- **Drafts** - This folder holds messages that you've composed but haven't sent yet. A message saved in your Drafts folder stays there until you either send it or delete it. SmarterMail allows users to adjust the time a new message is automatically saved. For more information, see the Auto Save Frequency description on the Account Settings page.
- **Junk E-mail** - Messages SmarterMail believes to be junk mail bypass your inbox and go to the

Junk E-mail folder. You should periodically check this folder to ensure that valid messages were not accidentally delivered to the Junk E-mail folder. When valid email is delivered to the Junk E-mail folder, select the message and click the Actions menu in the content pane toolbar. Then click Mark and select Not Spam .

- Sent Items - All outgoing messages are automatically saved to your Sent Items folder, making it easy to review or resend a message if necessary. Note: This folder only displays if it has been enabled in account settings. In addition, messages sent from a third-party client such as Outlook will not be saved in the Sent Items folder.

Creating Email Folders

To make your email easy to manage, SmarterMail lets users create as many personal mail folders as they want. Personal folders help users organize incoming and outgoing messages in ways that make sense to the individual user. That being said, creating a very large number of folders sub-folders can impact the performance of any email server, not to mention syncing your account with email clients. Note: When creating new folders, DO NOT create sub-folders within your Inbox. While technically possible, many third-party email clients and most mobile devices can not sync sub-folders that are part of a user's Inbox.

To create a new folder, click Actions in the navigation pane toolbar and select New Folder . This will open a new folder window. In the Parent field, select the appropriate directory to save the folder to. In the Folder field, type the name of the new folder. Folder names can include letters, numbers, and the hyphen (-), space (), and underline (_) characters only. Note: Using a backslash character (\) when naming a new folder will create both a parent and a sub-folder. For example: Family\mom will create a "Family" parent folder with a "mom" sub-folder within Family. Then click Save .

To make your SmarterMail folders available from a third-party email client such as Microsoft Outlook, when you set up the account in your client you will need to set it up using IMAP as your incoming mail server type. If you use POP mail, you only have access to your SmarterMail inbox, not any personal mail folders you created to organize messages. In addition, when using syncing protocols like Microsoft Exchange ActiveSync (EAS), any folders that are created will also sync with whatever mobile or desktop client you're setting up with EAS. Just be aware of the issues noted previously with the number of folders and sub-folders that exist as well as the issues with syncing sub-folders created within your Inbox.

Moving Messages to Another Folder

Moving messages between folders in SmarterMail is easy. You can either drag and drop messages from one folder to another or move them using the Actions menu.

To move messages using the Actions menu, first open the folder containing the message(s) you want to move. Then select the desired message(s) and click the Actions menu in the content pane toolbar. Click Move and select the name of the destination folder. The message(s) will automatically move into the folder you selected.

Renaming and Deleting Folders

You can change the name of a personal mail folder anytime or delete it completely when you no longer need it.

To rename a folder, select the appropriate folder in the navigation pane. Click Actions in the navigation pane toolbar and select Rename Folder . In the New Folder Name field, type the name of the new field. You can also change the directory that the folder is saved to by selecting another directory in the Parent field. Then click Save .

To delete a folder, select the appropriate folder in the navigation pane. Click Actions in the navigation pane toolbar and select Delete Folder . Then click OK to delete the folder and all of its contents.

Message Archive Search

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

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

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

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

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

For more information on archiving, see [Message Archiving](#).

Chat

Chat Overview

This feature is only available in SmarterMail Enterprise.

SmarterMail's chat feature allows users on the domain to chat with each other, instantly and securely, right within the webmail interface or by using most third-party chat clients that support the XMPP (Jabber) protocol. There's no doubt email is a great communications mechanism, but there are times when real-time communication is crucial. Note: If your SmarterMail installation is deployed using the default Web server, the chat functionality will not work. SmarterTools recommends converting to IIS for chat to function properly. For information on converting to IIS, refer to [Running SmarterMail as an IIS Site](#).

To access the chat feature, click the chat icon . For help understanding the different areas of chat, see the [chat interface diagram](#).

Note for tablet users: In many cases, tablet operating systems and applications are simplified in order to preserve battery life. For example, many mobile browsers will restrict the number of concurrent threads that can be used to access the same resource. In those cases users will need to use third-party chat clients such as IM+, IMO or others to use SmarterMail's live chat on a tablet or smartphone. Therefore, the live chat icon is not available in the Web interface for SmarterMail when viewed on a tablet or smartphone.

Navigating Your Chat Contacts

The chat section of SmarterMail is divided into three main areas:

- The navigation pane displays the contacts on your domain you can chat with. To view details for a specific contact, simply click the desired contact.
- The content pane displays all available details about the selected contact.
- The preview pane displays a list of the most recent chat conversations, as well as any attachments, appointments or email messages, related to the selected contact.

Note: The same information is available for any email aliases you may be a member of. For example, an alias for `salesteam@example.com` may be used to send chat messages to all members of that department that are online and functions identically to an individual chat contact.

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

- Chat - Starts a chat with the selected contact/alias in a new window.

Changing Your Chat Status

Users can manage their chat status within the webmail interface by clicking the chat status menu in the upper right corner. Users can change their status to one of the following:

- Available - You are available to receive and respond to chat messages via the webmail interface. When a user is marked as Available, they will see other members of their domain who are also active and available in chat.
- Away - You are logged into chat, but are away from your computer and may not respond right away.
- Busy - You are logged into chat, but are busy and may not respond right away.
- Offline - You are logged out of chat in the webmail interface and cannot receive chat messages using the webmail interface. In addition, all other members of your domain will appear Unavailable. However, if you are using a third-party client for chat, and are logged into that chat client, setting your chat status to offline in webmail will not affect your chat status in the third-party client. Therefore, chats will only display in your third-party client rather than in both the client and the webmail interface.

Viewing a Contact's Chat History

On occasion, you may need to refer to a previous chat conversation you had with a contact. To review the chats you've had with a specific contact, select the desired contact in the navigation pane. A Chat tab with the list of recent chat conversations will load in the preview pane, regardless of whether they occurred within the Web interface or using a third-party chat client. To view the details of the chat conversation, simple select the desired conversation and click Open . The chat history will open in a new window. Saving chat history is a default action and can not be turned off at the domain or system level.

In addition, as SmarterMail indexes all communication, other tabs are shown as well, including tabs for email Messages, calendar Appointments and Attachments.

Searching Chat Contacts

This feature is only available in SmarterMail Enterprise.

If there are a large number of users on the domain, finding a specific chat contact can become increasingly difficult. Fortunately, SmarterMail's basic search tool allows users to find chat contacts quickly and easily.

To perform a basic search, type the search criteria in the search bar located near the top of the navigation pane. Then click the magnifying glass or press Enter on your keyboard. SmarterMail will automatically search the chat contacts list for matches and display the results in the navigation pane. Note: Your search criteria may include letters and numbers. SmarterMail does not search for special characters such as "@," "#" or "%."

Connecting to Third-Party Chat Clients

This feature is only available in SmarterMail Enterprise.

If you prefer to use a third-party client to receive and respond chat messages, you will need to ensure the chat client supports the XMPP (or Jabber) protocol. Examples of chat clients that support XMPP include Adium, Digsby, iChat, Pidgin and Trillian.

More information on integrating SmarterMail's chat feature with commonly used third-party clients may be found in the SmarterTools Knowledge Base .

Contacts

Contacts Overview

SmarterMail features an online contact manager that helps users organize and communicate with the people in their life. Users can view and manage their contacts from any computer with Internet access, anywhere in the world, using the webmail interface.

To access your contacts, click the Contacts icon . To view different contact lists (such as the Global Address List, shared lists, or mapped resources), use the Contacts Selector at the top of the navigation pane and select the contact list you want to view. If Overlay Contacts is enabled in View menu, you can view My Contacts and any user-shared contact lists at the same time. Disable OverLay Contacts to view these lists separately. Note: The Global Address List (GAL) can only be viewed on its own. Despite Overlay Contacts being enabled, the GAL cannot be viewed with My Contacts or any user-shared contact lists.

For help understanding the different areas of the contacts section, see the contacts interface diagram .

Navigating Your Contacts

When you view your SmarterMail contacts, the page is divided into three sections:

- The navigation pane displays the contacts in the list you are viewing. To view details for a specific contact, simply click the desired contact.
- The content pane displays all available details about the selected contact.

- The preview pane displays a list of the most recent messages, appointments, chats and attachments related to the selected contact.

In general, the following options are available from the navigation pane toolbar:

- New - Creates a new contact.
- Actions - Click this button and select the appropriate option to delete contacts, send email to contacts, import/export contacts, or add the contacts to Outlook.
- Select All - Selects all contacts in the list you are viewing.
- Delete - Deletes the selected contact(s).
- Send Email - Addresses an email message to the selected contact(s).
- Send vCard(s) - Allows you to send an email with the the selected contact(s) electronic business card(s) (vCard) attached.
- Add to Outlook - Connects SmarterMail to Microsoft Outlook and synchronizes contact information. Note: This feature is only available in SmarterMail Enterprise.
- Import/Export - Import or export some or all of your contacts in vCard or comma separated value (CSV) format. For more information, see [Importing and Exporting Contacts](#).
- Import - Allows you to import contacts from another email system into your contact database. SmarterMail can bulk import contacts in either vCard or CSV format.
- Export to vCard - Exports only the selected contact(s) in vCard format.
- Export all to vCard - Exports all of your contacts in vCard format.
- Export to CSV - Exports only the selected contact(s) in CSV format.
- Export all to CSV - Exports all of your contacts in CSV format.
- View - Click this button and select the appropriate option do filter contacts by category, sort contacts, or choose the details (Visible Fields) that are displayed about a contact in the navigation pane.
- Filter - Filters contacts by the selected category. Categories are created when you add new contacts to your address book. For more information, see [Creating New Contacts](#).
- Sort - Sorts contacts by display name, email, or company in ascending or descending order.
- Visible Fields - Choose which contact details are displayed in the navigation pane.
- Overlay Contacts - When unchecked, adjusting the Contact Selector will toggle views rather than overlaying contact lists to view multiple resources at one time. Note: Due to the way the Global Address List (GAL) is generated, the Global Address List cannot be overlaid with the default Contact list or shared contacts.

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

- Edit - Edits the selected contact.
- Delete - Deletes the selected contact. Note: When accessing the Global Address List, the ability to delete contacts depends on the permissions granted. For example, if the GAL is read-only, the delete button will not appear.
- Download vCard - Saves the contact information as an electronic business card, which can later be imported to another program such as Outlook or sent through email as an attachment.

Viewing Items Related to a Contact

To help users better understand their relationships and communications with each contact, SmarterMail automatically displays a list of recent messages, appointments, attachments and live chats related to each contact. This information can be found in the related items grid in the preview pane.

In general, the following options are available from the preview pane toolbar:

- Open - Opens the selected message, appointment, attachment or live chat related to the contact.
- Delete - Deletes the selected message, appointment, attachment or live chat related to the contact.

To perform a basic search of the related items listed for a contact, type the search criteria in the search bar located near the top of the preview pane. Then click the magnifying glass or press Enter on your keyboard. SmarterMail will automatically search the related items for matches and display the results in the related items grid. Note: Your search criteria may include letters and numbers. SmarterMail does not search for special characters such as "@," "#" or "%."

Creating New Contacts

There are several ways to add new contacts to SmarterMail, depending on whether you want to add a contact from an email message, import contacts from another provider, or add a contact by typing the name and other information directly in SmarterMail.

To add a contact from an incoming email message, simply view the desired message either by double clicking on it or viewing it in the preview pane. SmarterMail includes "touch and go" functionality that highlights all email addresses in the header of the message. By clicking on a highlighted address, a small window opens with three options: Email, Add/Edit Contact and Block Sender. Click the Add/Edit Contact link and a new contact window opens up. SmarterMail will automatically complete the display name and email address fields, then you can enter additional details and save the contact.

To add a contact by typing the name and other information directly in SmarterMail, click New in the navigation pane toolbar and then click Contact . This will open a new contact window that you will

use to add the contact to SmarterMail. In addition, you can create a new contact within the Contacts section of SmarterMail.

For information on adding new contacts by importing contacts from another email service, see Importing and Exporting Contacts .

Saving Contact Details

When you add a new contact to SmarterMail, you can save as many or as few details about the person as you like. In general, contact details are divided into five sections:

- Personal Info - Type the contact's display name, title, first name, middle name, last name, suffix, email address(es), instant messenger, home page, and date of birth. Note: The display name is the only required field to save a contact.
- Add a Picture - SmarterMail allows you to upload a picture for any contact in your address book. These pictures are available within the webmail interface and for anyone using CardDAV or the Microsoft Exchange ActiveSync add-on to sync their calendars with email clients and/or mobile devices. Unfortunately, pictures will not sync for customers using Add to Outlook for synchronization. Upload a contact picture by dragging and dropping a file in the highlighted area or clicking to browse for a file.
- Contact Info - Type the contact's home phone number, work phone number, mobile phone number, pager number, home and work fax numbers, and home address.
- Work Info - Type the contact's company name, job title, department, office, work address, and website URL.
- Additional Info - Type any additional details about the contact.

Master Categories

Categories are a great way to organize your contacts. Using categories, you can organize business, personal or any other type of contact into tidy circles, keeping people separated based on whatever criteria you want. Contacts can be in multiple categories or none. It's up to you. Note: Categories are only a way to organize contacts. They are NOT ways to send emails to a group of individuals. For that you would want to create an Alias or use SmarterMail's Mailing List feature.

- To add a category, simply click the Master Categories button and type the new category name. Note: Be sure to separate categories with a comma.

Searching Contacts

If you have a large number of people in your contacts list, finding a specific contact can become

increasingly difficult. Fortunately, SmarterMail's basic search tool allows users to find contacts quickly and easily.

To perform a basic search, type the search criteria in the search bar located near the top of the content pane. Then click the magnifying glass or press Enter on your keyboard. SmarterMail will automatically search the contacts list you are viewing for matches and display the results in the navigation pane. Note: Your search criteria may include letters and numbers. SmarterMail does not search for special characters such as "@," "#" or "%" .

To search other areas of your SmarterMail mailbox, use the advanced search feature. For more information, see Advanced Search Overview .

Importing and Exporting Contacts

Because people often have multiple email accounts from different providers, SmarterMail makes it easy for users to securely transfer contacts to and from other online address books.

Importing Contacts to SmarterMail

SmarterMail supports importing contacts from two different types of files: vCards (.vcf) and comma-separated text files (.csv). SmarterMail also supports importing from a .zip file containing any combination of these file formats. For step-by-step instructions on importing contacts to SmarterMail, please refer to the KB article How To Import Contacts to SmarterMail .

Exporting Contacts from SmarterMail

Contacts can be exported individually in vCard or CSV format or in bulk as a .zip file containing either vCard or CSV files. These files can then be imported into Microsoft Outlook or into another SmarterMail account. For step-by-step instructions on exporting contacts from SmarterMail, please refer to the KB article How To Export SmarterMail Contacts .

Sending Contacts from SmarterMail

SmarterMail also allows users to email contact data as vCard files. For step-by-step instructions, please refer to the Kb article How To Send a Contact as a vCard .

Global Address List

The Global Address List, sometimes referred to as the "GAL," is most commonly identified with Microsoft Exchange. The GAL is essentially a directory service within SmarterMail that contains a dynamic list of all contact information for every user on your domain. While individual mailboxes are contained within the GAL, domain administrators can futher manage what's included in the GAL in

order to hide users that may not represent real people, such as a support@example.com alias and/or mailing lists.

Contact information for the Global Address List is pulled from the individual account profiles of users. To update your listing, click the settings icon . Then expand the My Settings folder and click Account Profile in the navigation pane.

Note: If the Global Address List is enabled for your domain, all information you enter into your profile can be seen by all other members of your domain.

The Global Address List functions almost identically as My Contacts.

Calendar

Calendar Overview

SmarterMail's calendar feature takes the burden out of organizing your schedule and is accessible from any desktop, laptop or mobile device with Internet access. SmarterMail's calendar system is extremely flexible and includes many options that make it easy to keep track of important events, including:

- Ability to create and sync multiple personal calendars.
- Fully configurable appointments with optional recurrence rules.
- Email notification and notification within SmarterMail of upcoming appointments.
- Overlay view to display multiple calendars, tasks and conference rooms on the same calendar.
- Attendee and invitation status tracking.
- Conference room availability and scheduling.
- Availability information about attendees (Enterprise Edition only).
- Integration with Outlook (Enterprise Edition only).

To access your calendar, click the Calendar icon . Depending on your account settings, the daily, weekly, monthly, or all appointments calendar view will load. To view multiple resources at once or to toggle between views, use the Resource Selectors (dropdown menu options at the top of the content pane toolbar) and check the desired resource. Items found in these dropdowns are based on a user's personal calendars and task list and any domain/user shared resources that have been mapped.

For help understanding the different areas of the calendar, see the calendar interface diagram .

Navigating Your Calendar

When you view your SmarterMail calendar, you can toggle between four different views:

- Daily - The daily view is a planner-type view that displays all appointments scheduled for the day. If configured, this view also displays the weather forecast for the date you are viewing and any applicable start or due times for tasks.
- Weekly - The weekly view is intended as more of an agenda-type view and displays all appointments scheduled for the week. If configured, this view also displays the 7-day weather forecast and the start and due dates for tasks.
- Monthly - The monthly view displays all appointments and tasks scheduled for the month. It serves as an at-a-glance type of calendar that outlines a general idea of the upcoming events over the next 30 days.
- All Appointments - The all appointments view lists all appointments on your calendar and can be sorted by the appointment subject, start date, or end date.

There are a couple of ways to differentiate between different appointment types and events:

- Each resource can be given its own color in the Calendar Settings .
- All-day appointments are denoted with a triangle.
- Recurring events are denoted with a curved arrow.

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

- New - Creates a new appointment.
- Actions -
- Add to Outlook - Click this button and select Add to Outlook to import all calendar appointments to Microsoft Outlook. Note: The ability to add your calendar to Outlook is only available in SmarterMail Enterprise and SmarterMail Free editions.
- View -
- Filter - Filtering appointments allows you to view all of your appointments, including ones that are recurring or all day, or to only view appointments in particular categories.
- Overlay Calendars - When unchecked, adjusting the Resource Selectors will toggle views rather than overlaying resources to view multiple resources at one time.
- Print - Prints the data displayed in the current calendar view.

Viewing Calendar Event Details

When looking at your calendar in webmail, and viewing your appointments by day, week or month, only the barest details are initially displayed in order to save space. However, there may be times when you want to view more information about a specific appointment. You can do this one of two ways:

First, double clicking on an appointment will open it in a pop-up window. That pop-up window displays the full appointment details just as it does when you create a new appointment, and, if you were the original creator of the appointment, you can edit it as needed. If the appointment was created by someone else, that is denoted at the top of the pop-up window and you are not able to edit the appointment details.

Additionally, simply moving your mouse over a specific appointment in your daily, weekly or monthly view will display the details of the appointment in a call out. The call out will display the subject of the meeting as well as the time and any location data.

Creating New Calendar Appointments

To create a new calendar appointment, click **New** in the content pane toolbar. This will open a new appointment window that you will use to add the appointment to SmarterMail and to invite attendees.

Saving Appointment Details

When you add a new appointment to your calendar, you can save as much or as few details about the appointment as you like. In general, appointment details are divided into four tabbed sections:

Event

The event is essentially whatever you want to schedule in your calendar. It can be a lunch or dinner, a meeting, an anniversary or birthday, or virtually any other type of event you want to keep organized in your calendar. To create an Event, you will need to include the following information. Note: The Subject and Start date are the only fields required to save an appointment.

- **Calendar** - Use the dropdown menu to select which calendar the event is for. The default calendar can be chosen in **Calendar Settings**.
- **Subject** - The subject is the friendly name for the event you're creating.
- **Attendees** - Attendees are the people you want to invite to your event. When adding Attendees, each will receive an event invitation that they can either accept or reject. You will receive notifications back regardless of whether the attendee accepts or rejects the invitation. To add attendees, you can either type their email address directly or simply click the "Attendees" field name to open your list of contacts. You can select contacts from your various contact lists, including the Global Address List (GAL), as well as cycle through contacts you have listed in categories.
- **Conflicts** - If you add an attendee from your Global Address List, and their schedule conflicts with the date and time of your event, it will be displayed as a Conflict. To find a new day or time for the event, click on the availability icon next to the Attendees field to bring up a grid of all GAL Attendees' availability.

- Location - Where the Event will be taking place. The location can be a room or building, an address, or even some descriptive text, such as "via Webex". Regarding Room selection versus Location, these are mutually exclusive, yet compatible fields. Separating them allows for users to specify more general locations, such as a geographical location or specific office building, while still being able to reserve conference rooms at those locations.
- Room - If your domain administrator has added any shared resources, like conference rooms, the list of rooms will be available in this dropdown. Just as with attendee availability, if a conference room is already reserved for a specific day and time an Event is to be set, this information will display in the Conflicts field of the new appointment window. Conference room availability will also show when users click the availability icon next to the Attendees field in the new appointment window.
- Start and End Dates and Times - A Start Date is required to save the event. By default, Events start as the current date and time and end 1 hour later. These fields are fully customizable.
- Availability - Here you can set your own availability - either Busy or Free. Setting your status as Busy will be reflected if others within your Global Address List try inviting you to their own events.
- Reminder - Setting a reminder will make a pop-up window appear in webmail at whatever reminder interval you set.
- Email Notification - Adding in an email address will send the event reminder to that email address based on the time interval set by the reminder.
- Private event - This setting can be used for those who share their calendar with other users. Events marked as private will only be shown to those with Full Access. Those with Availability-Only or Read-Only permission will instead see "Busy Time" and cannot view appointment details.

Recurrence Information

In some cases, Events will need to occur on a regular basis. For example, weekly meetings, monthly lunches, holidays, anniversaries or business appointments. In these cases, an Event's recurrence is set. The recurrence feature is very flexible and can be as simple or as complex as necessary. Examples include a birthday that occurs every August 7th, a meeting that happens the second Monday of every month, or an appointment that occurs every four days for three weeks.

When you select the timeframe for how often the Event needs to repeat, you're presented with several options. The first is how often the Event occurs, in weeks. For example, if the Event occurs every week, you leave the recurrence at "Every 1 week(s)." If the Event happens every third week, you set the recurrence at "Every 3 week(s)," etc.

Next, you select the day of week the you want the Event to repeat on.

Finally, you set the end time for the Event recurrence. The Event can repeat indefinitely or can end after a certain number of occurrences or on a specific date.

Description

Use the Description area to keep any important notes or a description of the Event. You can also include any webinar information, call in numbers, or other information you want your Attendees to see. The Event Description is passed along with the Event invitation and will appear in your Attendees' calendars and Event details.

Categories

A category provides a way to organize your Events into manageable groups. To add a category, simply click the Master Categories button and type the new category name. Note: Be sure to separate categories with a comma.

Managing Calendar Appointments

To view the details of an appointment, click on the appointment from any calendar view. The appointment details will load in a popup window.

Editing Appointment Details

To edit the details of an appointment, click on the appointment or right-click and choose Edit from any calendar view. The appointment details will load in a popup window. To change the calendar that the appointment is assigned to, use the Move button found in the toolbar. Note: Meeting invites (appointments with attendees) cannot be moved. Make any other appropriate changes and click Save . The appointment details will update on your calendar and any attendees will receive a new invitation notifying them of the change. Note: Editing a recurring appointment will update all instances of the appointment on your calendar. There is no way to edit a single date of a recurring appointment series.

Deleting an Appointment

On occasion, you may need to delete a calendar appointment. To delete and remove an appointment from your calendar, click on the appointment from any calendar view. The appointment details will load in a popup window. Click Delete . You can also right-click and choose Delete. The appointment will no longer appear on your calendar and any attendees will receive a notification that the appointment has been cancelled. Note: Deleting a recurring appointment will delete all instances of the appointment from your calendar. To delete a single instance, choose Delete Instance.

Deleting an Instance

When creating an appointment, it's possible to create it as a recurring event. That means the appointment will occur at a specific interval for a specific amount of time. The most common types of recurring appointments are weekly or monthly meetings. However, there may be a time when a recurring meeting needs to be canceled due to unforeseen circumstances. That's where deleting an "instance" of a meeting comes in handy.

Deleting an instance of a recurring event allows you to delete a single meeting from a recurring sequence. That meeting can then be formally canceled or re-scheduled for a later day and time. To delete an instance, open up the meeting by double clicking on it and clicking the Delete Instance button. You can also right-click and choose Delete Instance . Deleting an instance of a meeting will not affect any future or past instances - only the instance you delete.

Tentative Appointments

SmarterMail utilizes tentative meeting requests to help prevent meeting requests or event invitations from getting lost or overlooked. When a meeting invitation is sent, a tentative appointment will be automatically added to the calendar. The appointment can then either be accepted or declined from the email request or directly within the calendar interface. In addition, if a meeting or event is tentative, the reminder will still be sent if one was added to the invite!

To manage a tentative meeting request from the calendar, right-click on the appointment and choose Accept or Decline . You can also click on the appointment to load its details in a popup window. (Alternatively, you can right-click and choose View.) After viewing the appointment details, you can choose to Accept or Decline the meeting using the buttons found in the popup window's toolbar. Tentative meeting requests are denoted with a yellow flag in the appointment window.

Note: Users who do not wish to utilize tentative appointments can disable this functionality within their personal Calendar Settings .

Tasks

Tasks Overview

SmarterMail's robust tasks system is designed to help users keep track of anything they need to do. From shopping lists to long-term tasks, users can create lists of items, set due dates, update status and completion percentage, and even prioritize tasks. And, as there are times when an email exchange leads to a task needing to be done, email messages can be linked to tasks so that all communication surrounding the task is kept organized.

To access your tasks, click the Tasks icon . To view different Tasks lists (such as shared lists or mapped resources), use the Tasks Selector at the top of the navigation pane and select the list you want to view. Depending on your overlay settings found in the View menu, you can view multiple lists together or toggle between views.

For help understanding the different areas of the tasks section, see the tasks interface diagram .

Navigating Your Tasks

When you view your tasks, the page is divided into two sections:

- The navigation pane displays the tasks in the list you are viewing. To view details for a specific task, simple click the desired task.
- The content pane displays all available details about the selected task.

In general, the following options are available from the navigation pane toolbar:

- New - Creates a new task.
- Actions - Click this button and select the appropriate option to select all tasks, delete tasks, or add the tasks to Outlook.
- Select All - Selects all tasks in the list you are viewing.
- Delete - Deletes the selected task(s).
- Add to Outlook - Connects SmarterMail to Microsoft Outlook and synchronizes task information. Note: This feature is only available in SmarterMail Enterprise.
- View - Click this button and select the appropriate option do filter tasks, sort tasks, or choose the details that are displayed about a task in the navigation pane.
- Filter - Filters tasks by the selected category or by whether the task is completed.
- Sort - Sorts tasks by subject, due date, percentage complete, or priority level in ascending or descending order.
- Visible Fields - Choose which task details are displayed in the navigation pane.
- Overlay Tasks - When unchecked, adjusting the Tasks Selector will toggle views rather than overlaying tasks to view multiple lists at one time.

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

- Edit - Edits the selected task.
- Delete - Deletes the selected task.

Creating New Tasks

To create a new task, click New in the navigation pane toolbar. This will open a new task window that you will use to add the task to SmarterMail.

Saving Task Details

When you add a new task in SmarterMail, you can save as much or as few details about the task as you like. In general, task details are divided into three sections:

- Details - The details of the task include the subject of the tasks, start and end dates, and other information. Note: The subject, start date and due date are the only required fields to save a task.
- Account - This option is used to select the account the task should be created under. This includes the default task list and any shared resources that have been mapped to the user's account.
- Subject - This is a friendly name for the task. A more detailed description of the task can be added in the next tab.
- Start and End Dates and Times - The date and time the task will begin, then end. You can either manually enter the dates and times or click on the date selector icon and/or the time selector icon.
- Reminder - Setting a reminder will make a pop-up window appear in webmail at whatever reminder interval you set.
- Priority - Setting a priority helps you keep tasks organized by importance.
- Status - The status of the task keeps you, and anyone else you may be sharing tasks with, apprised of where the task is in terms of being worked on. Options include:
 - Not Started - The task is created but not being worked on at the present time.
 - In Progress - The task is currently active and being worked on.
 - Completed - The task was worked on and is now finished.
 - Canceled - The task is not needed, is not worth starting or a decision was made to not move forward with it.
 - % Complete - As a task is being worked on, a user can update the status by denoting how far along the task is in terms of being marked Completed. This is a good way to keep people who share tasks apprised of where the task is in terms of completion.
- Description - The description field can be used to type up the initial thoughts/ideas or goals of the task, then updated as needed with any important notes, if desired, as the task is worked on.
- Categories - A category provides a way to organize your notes into manageable groups. To

add a category, simply click the Master Categories button and type the new category name.

Note: Be sure to separate categories with a comma.

Once the task is saved, it will appear on your calendar. Note: Users can disable the display of task start and end times on the calendar. For more information, see [Calendar Settings](#).

Searching Tasks

If you have a large number of tasks in your tasks list, finding a specific task can become increasingly difficult. Fortunately, SmarterMail's basic search tool allows users to find tasks quickly and easily.

To perform a basic search, type the search criteria in the search bar located near the top of the navigation pane. Then click the magnifying glass or press Enter on your keyboard. SmarterMail will automatically search the tasks list you are viewing for matches and display the results in the navigation pane. Note: Your search criteria may include letters and numbers. SmarterMail does not search for special characters such as "@," "#" or "%."

To search other areas of your SmarterMail mailbox, use the advanced search feature. For more information, see [Advanced Search Overview](#).

Notes

Notes Overview

SmarterMail's notes feature provides users with the electronic equivalent of paper sticky notes. Use notes to jot down questions, ideas, reminders or anything else you would write on note paper. This feature is especially convenient when used to save bits of information you may need later, such as directions or text you want to reuse in other items or documents.

To access your notes, click the Notes icon . To view different Notes lists (such as shared lists or mapped resources), use the Notes Selector at the top of the navigation pane and select the Notes list you want to view. Depending on your overlay settings found in the View menu, you can view multiple lists together or toggle between views.

For help understanding the different areas of the notes section, see the notes diagram .

For help creating a new note, see [Creating New Notes](#) .

Navigating Your Notes

When you view your notes, the page is divided into two sections:

- The navigation pane displays the notes in the list you are viewing. To view details for a specific note, simply click the desired note.
- The content pane displays all available details about the selected note.

In general, the following options are available from the navigation pane toolbar:

- New - Creates a new note.
- Actions - Click this button and select the appropriate option to select all notes or delete notes.
- Select All - Selects all notes in the list you are viewing.
- Delete - Deletes the selected note(s).
- View - Click this button and select the appropriate option to filter notes, sort notes, or choose the details that are displayed about a note in the navigation pane.
- Filter - Filters notes by the selected category or color.
- Sort - Sorts notes by text, color, or date in ascending or descending order.
- Visible Fields - Choose which note details are displayed in the navigation pane.
- Overlay Notes - When unchecked, adjusting the Notes Selector will toggle views rather than overlaying Notes to view multiple lists at one time.

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

- Edit - Edits the selected note.
- Delete - Deletes the selected note.

Creating New Notes

To create a new note, click New in the navigation pane toolbar. This will open a new note window that you will use to add the note to SmarterMail.

Saving Note Details

When you add a new task in SmarterMail, you can save as much or as few details about the note as you like. In general, task details are divided into two sections:

- Details - Type the text of the note and specify the color of the note. Note colors are a great way to keep notes of specific type neatly organized. As a side note, the colors available match the colors of traditional paper sticky notes. In addition, there is a complete text editor available when creating new notes, so adding in images, screenshots, links to Web pages, highlighting text and more are available so that users can create truly dynamic and inspiring notes. Note: The color and text of the note are the only required fields to save a note.
- Categories - A category provides a way to organize your notes into manageable groups. To

add a category, simply click the Master Categories button and type the new category name.

Note: Be sure to separate categories with a comma.

Searching Notes

If you have a large number of notes in your notes list, finding a specific notes can become increasingly difficult. Fortunately, SmarterMail's basic search tool allows users to find notes quickly and easily.

To perform a basic search, type the search criteria in the search bar located near the top of the navigation pane. Then click the magnifying glass or press Enter on your keyboard. SmarterMail will automatically search the notes list you are viewing for matches and display the results in the navigation pane. Note: Your search criteria may include letters and numbers. SmarterMail does not search for special characters such as "@," "#" or "%."

To search other areas of your SmarterMail mailbox, use the advanced search feature. For more information, see Advanced Search Overview .

RSS Feeds

RSS Feeds Overview

Real Simple Syndication (RSS) is a way for website owners to make their content available for people to read and review. Websites publish lists of updates via "feeds" that indicate when new content is available. Rather than regularly visiting a website, you can add a new feed to SmarterMail (also called subscribing to a feed) and then see when new content is available from that site. Any new content posted to your feeds will appear in the RSS feeds section of your mailbox.

Using RSS, combined with organizing your feeds into folders, makes it easy to stay up-to-date on information from news sites, blogs, social media outlets, Google alerts, new forum topics and much more, right from within SmarterMail.

To access your RSS feeds, click the RSS feeds icon .

For help understanding the different areas of the RSS feeds section, see the RSS feeds interface diagram .

Navigating Your RSS Feeds

When you view your RSS feeds, the page is divided into two sections:

- The navigation pane displays all of the RSS feeds you have added to SmarterMail. To view

recent updates to a specific RSS feed, simply click the desired feed.

- The content pane displays the RSS feeds in the folder you are viewing.

In general, the following options are available from the navigation pane toolbar:

- Actions - Click this button and select the appropriate option to create a new folder, rename a folder, or delete a selected folder. Using folders makes it easy to keep your news items organized. For example, create folders for technology items, politics, business or other categories.

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

- New - Adds a new RSS feed to SmarterMail.
- Edit - Edits the selected RSS feed.
- Delete - Deletes the selected RSS feed(s).

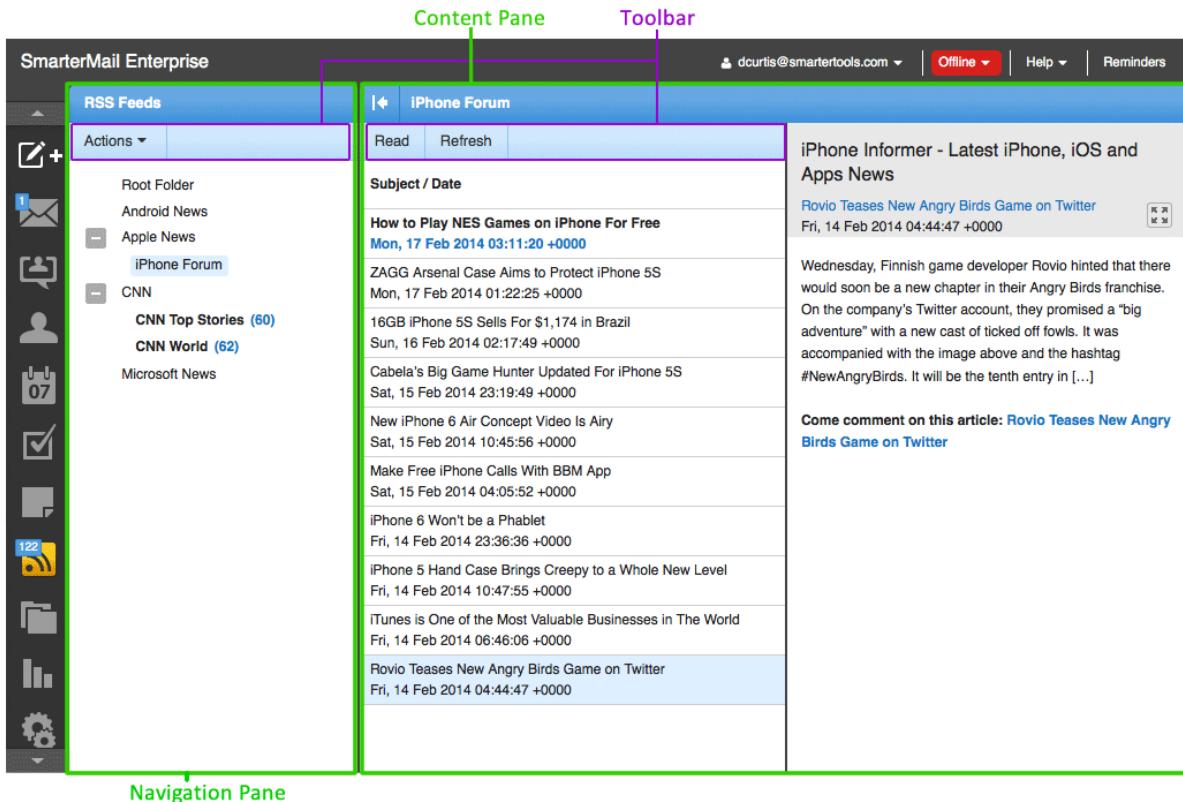
Adding New RSS Feeds

To subscribe to a new RSS feed, click New in the content pane toolbar. Adding a feed requires two pieces of information:

- Name - A friendly name for the RSS feed. Typically, you'll want to make this a short name so you can easily find it. You can use a backslash character to make the feed appear in a subdirectory, such as in News\Fox News or Technology\Microsoft Updates.
- URL - The URL for the website's RSS feed. Note: The RSS feed URL is not the same as the website URL. For example, the SmarterTools Blog can be found at blog.smartertools.com , but the RSS feed for the blog is at blog.smartertools.com/rss.aspx .

Finding a Site's RSS Feed

An RSS feed can usually be identified by an orange symbol (such as). When you see it on a website, clicking on the icon will usually direct you to that site's RSS feed. From there, you can simply copy the link and then paste it into SmarterMail to subscribe to the feed. If the site does not have the orange RSS feed symbol, try looking for a text link to the RSS feed. Text links to feeds may include any of the following terms: subscribe, syndicate, feed, RSS, xml, or atom. Note: Not all sites offer RSS feeds.



For a list of sample RSS feeds you may be interested in subscribing to, please see [Sample Feeds](#).

Sample Feeds

There are many RSS feeds on the internet today. This topic contains many of the more common feeds, although this list is by no means exhaustive.

The following links are either direct RSS feed URLs or links to web pages containing an RSS feed list. To add a feed to SmarterMail, right-click on the link and select "copy shortcut" from the context menu. Then paste this value into the RSS URL in SmarterMail.

Feed lists (designated by [feed-list]) will typically have orange XML icons next to each feed. Follow the same procedure (copy shortcut) to get the URL of those feeds.

<p>News and Information</p> <ul style="list-style-type: none"> • SmarterTools Blog • Fox News [feed-list] • CNN News [feed-list] • Yahoo! News [feed-list] • Reuters News Online [feed-list] • CNET News [feed-list] • Washington Post [feed-list] • BBC News <p>Entertainment</p> <ul style="list-style-type: none"> • E! Online [feed-list] • NY Times: Opinion • Dictionary word of the day <p>Finance</p> <ul style="list-style-type: none"> • Kiplinger Personal Finance • SmartMoney 	<p>Technology</p> <ul style="list-style-type: none"> • PC Magazine: New Product Reviews • Slashdot News • TheWHIR Web Host News • Wired News • AnandTech's DailyTech News <p>Sports</p> <ul style="list-style-type: none"> • ESPN News • Fox Sports • CBS SportsLine [feed-list] • NY Times: Sports
---	--

Managing RSS Folders

To make your RSS feeds easy to manage, SmarterMail lets users create as many RSS folders as they want. RSS folders help users organize feeds in ways that make sense to the individual user.

To create a new folder, click Actions in the navigation pane toolbar and select New Folder . This will open a new folder window. In the Parent field, select the appropriate directory to save the folder to. In the Folder field, type the name of the new folder. Folder names can include letters, numbers, and the hyphen (-), space (), and underline (_) characters only. Note: Using a backslash character (\)when naming a new folder will create a sub-folder. For example: Technology\Software. Then click Save .

Renaming and Deleting Folders

You can change the name of a RSS folder anytime or delete it completely when you no longer need it.

To rename a folder, select the appropriate folder in the navigation pane. Click Actions in the navigation pane toolbar and select Rename Folder . In the New Folder Name field, type the name of the new field. You can also change the directory that the folder is saved to by selecting another directory in the Parent field. Then click Save .

To delete a folder, select the appropriate folder in the navigation pane. Click Actions in the navigation pane toolbar and select Delete Folder . Then click OK to delete the folder and all of its contents.

File Storage

File Storage Overview

SmarterMail's file storage feature allows users to upload files to the mail server and share them by sending out links to those files. Files can be public or private, can be eternal or have expiration dates and more. Note: - Uploaded files should not contain commas in the file name.

One benefit of using SmarterMail's file storage versus sending attachments is that file storage reduces the stress on the mail server by keeping large files out of the server's email spool. Another benefit of using file storage is that it allows users to send larger files without worrying about hitting any attachment size restrictions that a domain administrator, system administrator or hosting company put in place. Note: Files uploaded to the server are counted toward the user's disk space allocation, so users are encouraged to delete files that are no longer used from the server whenever possible.

To access the file storage area, click the file storage icon . By default, a list of files uploaded to the server will load in the content pane.

For help understanding the different areas of the file storage section, see the file storage interface diagram .

Navigating File Storage

When you view your uploaded files, the page is divided into two sections:

- The navigation pane displays the folders available for managing the files that are uploaded to the server. By default, a Root Folder is created.
- The content pane displays all available files within the selected folder.

In general, the following options are available from the navigation pane toolbar:

- Actions - Click this button and select the appropriate option to create a new folder, rename a folder, or delete a selected folder. Using folders makes it easy to keep your uploaded files organized. For example, create folders for images, videos, business documents or other categories.

In general, the following options are available from the content pane:

- Edit - Edits the sharing settings for the selected file.
- Delete - Permanently removes the selected file(s) from the server.
- Upload - Uploads a new file to the server.
- Download - Downloads the selected file(s).

Sharing Uploaded Files

Before a file can be shared you will first need to upload it to the mail server. After uploading your file, you will need to edit the file sharing settings by selecting the file and clicking Edit in the content pane toolbar. The file sharing settings will load and the following options will be available:

- Filename - The name of the file.
- Link Expires - The date and time that the public link to download the file expires. Leave this blank and the link will never expire.
- Enabled - Select this option to enable the link expiration date.
- Access Password - The password used to download the file. Leave this blank if you don't want to password protect the link.
- Enabled - Select this option to make the file password protected.
- Enable public access - Select this option to make the file available for sharing via a public link.

When you share a file by inserting the public link to the file into an email message, the recipient will be directed to a file storage download page with instructions on how to download the file.

Reports

Reports Overview

Using SmarterMail's extensive reporting engine and routinely generating and evaluating reports provides users, domain administrators and system administrators with the information they need to uncover issues before they become problems, discover and evaluate trends, identify the need for policy adjustment and much more.

Users have access to a variety of reports that are directly related to their use of SmarterMail. These include disk usage and file storage usage reports in addition to a variety of traffic reports, such as IMAP usage, message traffic, POP usage and more.

Domain administrators have access to all standard user reports in addition to reports that deal directly with the domain they are managing. For example, both summary and trend reports relating to domain traffic as well as spam and virus reports.

Finally, system administrators have access to a number of system-wide reports that give a detailed overview, as well as minute detail, about the server functions like drive usage and read/write statistics, domain usage reports that can be drilled into all the way to the user level, spam and antivirus reports and more. In addition, system administrators have access to detailed security reports such as abuse detection reports and information on blacklisted/whitelisted domains.

Summary and Trend Reports

SmarterMail includes dozens of predefined summary and trend reports and also allows users, domain administrators and/or system administrators to generate their own custom reports.

- Summary reports display summarized data at the system, domain, and user level within a user defined block of time. Summary reports are especially useful for determining the overall usage and performance of systems, domains, and users relative to each other.
- Trend reports display data points -- connected by trend lines -- for a system, domain, or user over a selected time span. Trend reports are especially useful for determining the usages and performance month-by month, day-by-day, and hour-by-hour (etc.).

These reports can be grouped and filtered to create custom reports. With summary, trend, and custom reporting, SmarterMail provides domain and system administrators with the information they need to efficiently monitor the performance of their mail server software. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

For help understanding the different areas of the reporting section, see the reports interface diagram .

Scheduled Email Reports

This feature is only available in SmarterMail Enterprise.

SmarterMail Enterprise has the ability to email standard and custom reports on a daily, weekly, and monthly basis. Note: If a scheduled email report is empty of data, it will NOT be sent until there is data to actually view.

- Daily email reports are sent after 12:00 AM.
- Weekly email reports are sent after 12:00 AM Sunday.
- Monthly email reports are sent after 12:00 AM on the first day of the month.

The reports are generated and sent by SmarterMail according to the time zone configured for that particular user.

To see which reports are scheduled to be emailed, click the reports icon . Then click Scheduled Email Reports in the navigation pane and select the desired report. A list of scheduled email reports will load in the content pane and the following options will be available in the content pane toolbar:

- New - Creates a new scheduled email report.
- Send Now - Emails a copy of the report to the desired recipient(s).
- Edit - Edit the email options for the report.
- Delete - Permanently removes the report from the emailed reports list.

Custom Reports

With custom reports, statistics from multiple reports can be combined to give users and administrators a comprehensive analysis of the mail server's performance, of individual mailbox performance, or an overview of a number of other metrics and measurements.

To access custom reports that were already created, click the reporting icon . Then expand the Custom Reports folder in the navigation pane. Then, select the desired report from the menu and it will load in the content pane. You can also get a list of the custom reports available by clicking on Manage Custom Reports. When you do, the custom reports that are already available will appear in the content pane. Regardless of the method you use, the following options will be available in the content pane toolbar:

- New - Creates a new custom report.
- Edit - Edit the report's settings and configuration options.
- Delete - Permanently remove the report from the custom reports list.

Creating a Custom Report

To create a custom report, click the reporting icon . Then expand the Custom Reports folder in the navigation pane and click Manage Custom Reports and click New in the content pane toolbar. The following configuration tabs will be available:

Custom Report

Use this tab to specify the following options:

- Name - The name of the custom report.
- Default Date Range - The default time period from which report data is collected.

Report Items

Use this tab to specify which report items to include in the custom report:

- Report Items - The specific report to be added to the custom report. Note: Depending on the report item selected, some of the options listed below may not be available.
- Name - The name of the report item.
- Rows - The number of rows displayed in the report.
- Sort By - The sort order of the data.
- Chart - To specify a specific chart type, select the appropriate option from the list.
- Values - The values that will be charted.
- Group By - The timeframe for which rows are grouped.

Summary Reports

Disk Reports

Disk Usage Reports

This report provides statistics regarding input/output operations of the system's hard drive, also known as "disk i/o". System administrators may use this report to correlate high disk usage on the server with SmarterMail activity and identify areas in which adjustments can be made. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Avg. Read - The average size in KB/sec of disk reads.
- Avg. Write - The average size in KB/sec of disk writes.

Traffic Reports

Disk Space Usage

This report displays the amount of disk space currently being used by all domains on your server. Domain administrators may run this report if the domain is nearing its storage limits to identify which users are using the most disk space. System administrators may run this report to identify domains that

are utilizing the most server space. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Disk Usage - The number of MB that each folder is occupying on the server.
- Rank - The order users or domains are listed within the report.
- User - The specific user on the domain.

File Storage Disk Space Usage

This report informs users how much disk space is currently being used for file storage. Users may use this report to identify which file storage folder is utilizing the most disk space. This is especially useful if the user is nearing his mailbox disk space limits and needs to clear up space for new data. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Disk Usage - The number of MB that each folder is taking up on the server.
- Rank - Where each folder falls in terms over overall space used.

Message Traffic

This report will tell you the number of messages that are being sent and received by all users of a domain (at the domain admin level) or all domains on your server (at the system admin level). System administrators may use this report for overage billing, to identify potential spammers on the server or to identify high-usage domains. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Rank - The order in which users or domains are listed within the report.
- Domain - For system admins, the specific domain on a server.
- User - For domain admins, the specific user on the domain.
- Account Type - For domain admins, the type of account the email address is associated with (user, domain administrator, or system administrator).
- Incoming Messages - The total number of messages the account has received.
- Outgoing Messages - The total number of messages the account has sent.
- Incoming Spam Messages - The total number of spam messages delivered to the mailbox.
- Outgoing Spam Messages - The total number of spam messages sent from the account.

Message Data

This report tells you the amount of data that was sent and received in KB by all users of a domain (at the domain admin level) or all domains on your server (at the system admin level). System administrators may use this report to identify potential spammers on the server or to identify high-usage domains. Note: Not all reports are available for users and/or domains. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Rank - The order in which users or domains are listed within the report.
- Domain - For system admins, the specific domain on the server.
- User - For domain admins, the specific user on the domain.
- Account Type - For domain admins, the type of account the email address is associated with (user, domain administrator, or system administrator).
- Data Sent - The total size in KB of all data sent by the account.
- Data Received - The total size in KB of all data received by the account.

Throttle Traffic

This report shows the number of messages that have been throttled on your server for all users of a domain (at the domain admin level) or all domains on your server (at the system admin level). Domain and system administrators may use this report to identify issues with high usage customers. For example, if a user is sending a high number of bounced messages, that is an unnecessary use of system resources that can be easily corrected. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Rank - The order in which users or domains are listed within the report.
- Domain - For system admins, a specific domain on the server.
- User - For domain admins, the specific user on the domain.
- Bounces Received - The number of bounced messages throttled.
- Messages Sent - The number of sent messages throttled.
- SMTP Out Bandwidth - The amount of bandwidth throttled.

Throttle Violations

This report shows the number of throttle violations on your server for all users of a domain (at the domain admin level) or all domains on your server (at the system admin level). Domain and system administrators may use this report to identify issues with high usage customers. For example, if a user is sending a high number of bounced messages, that is an unnecessary use of system resources that can be easily corrected. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Rank - The order in which users or domains are listed within the report.
- Domain - For system admins, a specific domain on the server.
- User - For domain admins, the specific user on the domain.
- Bounces Received - The number of bounced messages throttled.
- Messages Sent - The number of sent messages throttled.
- SMTP Out Bandwidth - The amount of bandwidth throttled.

SMTP In Usage

This report tells you the size of the bandwidth and the number of connections that have been made from SMTP incoming mail for all users of a domain (at the domain admin level) or all domains on your server (at the system admin level). Domain and system administrators may use this report to identify high usage accounts. This information can be used to evaluate whether to move such accounts to another server or to set limits on such accounts. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Rank - The order in which users or domains are listed within the report.
- Domain - For system admins, the specific domain on a server.
- User - For domain admins, the specific user on the domain.
- Account Type - For domain admins, the type of account the email address is associated with (user, domain administrator, or system administrator).
- Bandwidth - The bandwidth in KB for all incoming SMTP mail.
- Connections - The total number of connections made to a particular server (i.e., SMTP, POP, IMAP)

SMTP In Errors

This report tells if any errors occurred from SMTP incoming mail for all users of a domain (at the domain admin level) or all domains on your server (at the system admin level). Domain and system administrators may use this report to identify users that are using faulty email clients or unnecessarily using system resources. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Rank - The order in which users or domains are listed within the report.
- Domain - For system admins, the specific domain on a server.
- User - For domain admins, the specific user on the domain.
- Account Type - For domain admins, the type of account the email address is associated with (user, domain administrator, or system administrator).
- Blocked Connections - The total number of connections that were blocked.
- Bad Commands - The total number of bad commands given.
- Terminations - The total number of terminations that occurred for incoming mail.

SMTP Out Usage

This report tells you the size of the bandwidth and the number of connections that have been made from SMTP outgoing mail from all users of a domain (at the domain admin level) or all domains on your server (at the system admin level). Domain and system administrators may use this report to identify high usage accounts. This information can be used to evaluate whether to move such accounts to another server or to set limits on such accounts.

Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Rank - The order in which users or domains are listed within the report.
- Domain - For system admins, a specific domain on the server.
- User - For domain admins, the specific user on the domain.
- Account Type - For domain admins, the type of account the email address is associated with (user, domain administrator, or system administrator).
- Bandwidth - The bandwidth in KB for all outgoing SMTP mail.
- Connections - The total number of connections made to a particular server (i.e., SMTP, POP, IMAP)

SMTP Out Errors

This report tells if any errors occurred from SMTP outgoing mail from all users of a domain (at the domain admin level) or all domains on your server (at the system admin level). Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Rank - The order in which users or domains are listed within the report.
- Domain - For system admins, the specific domain on a server.
- User - For domain admins, the specific user on the domain.
- Account Type - For domain admins, the type of account the email address is associated with (user, domain administrator, or system administrator).
- Bad Commands - The total number of bad commands given.
- Terminations - The total number of terminations that occurred for incoming mail.

POP Usage

This report tells you the size of the bandwidth and the number of connections that have been made from POP incoming mail for all users of a domain (at the domain admin level) or all domains on your server (at the system admin level). Domain and system administrators may use this report to identify high usage accounts. This information can be used to evaluate whether to move such accounts to another server or to set limits on such accounts. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Rank - The order in which users or domains are listed within the report.
- Domain - For system admins, the specific domain on a server.
- User - For domain admins, the specific user on the domain.
- Account Type - For domain admins, the type of account the email address is associated with (user, domain administrator, or system administrator).
- Bandwidth - The bandwidth in KB for all incoming SMTP mail.
- Connections - The total number of connections made to a particular server (i.e., SMTP, POP, IMAP)

POP Errors

This report tells if any errors occurred from POP incoming mail for all users of a domain (at the domain admin level) or all domains on your server (at the system admin level). Domain and system administrators may use this report to identify users that are using faulty email clients or unnecessarily using system resources. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Rank - The order in which users or domains are listed within the report.
- Domain - For system admins, the specific domain on a server.
- User - For domain admins, the specific user on the domain.
- Account Type - For domain admins, the type of account the email address is associated with (user, domain administrator, or system administrator).
- Blocked Connections - The total number of connections that were blocked.
- Bad Commands - The total number of bad commands given.
- Terminations - The total number of terminations that occurred for incoming mail.

IMAP Usage

This report tells you the size of the bandwidth and the number of connections that have been made from IMAP incoming mail for all users of a domain (at the domain admin level) or all domains on your server (at the system admin level). Domain and system administrators may use this report to identify high usage accounts. This information can be used to evaluate whether to move such accounts to another server or to set limits on such accounts. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Rank - The order in which users or domains are listed within the report.
- Domain - For system admins, the specific domain on the server.
- User - For domain admins, the specific user on the domain.
- Account Type - For domain admins, the type of account the email address is associated with (user, domain administrator, or system administrator).
- Bandwidth - The bandwidth in KB for all incoming SMTP mail.
- Connections - The total number of connections made to a particular server (i.e., SMTP, POP, IMAP)

IMAP Errors

This report tells if any errors occurred from IMAP incoming mail for all users of a domain (at the domain admin level) or all domains on your server (at the system admin level). Domain and system administrators may use this report to identify users that are using faulty email clients or unnecessarily using system resources. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Rank - The order in which users or domains are listed within the report.
- Domain - For system admins, the specific domain on the server.
- User - For domain admins, the specific user on the domain.
- Account Type - For domain admins, the type of account the email address is associated with (user, domain administrator, or system administrator).
- Blocked Connections - The total number of connections that were blocked.
- Bad Commands - The total number of bad commands given.
- Terminations - The total number of terminations that occurred for incoming mail.

Trusted Senders

This report shows the number of messages received from email addresses listed as trusted senders for all domains on your server. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Account Type - The type of account the email address is associated with (user, domain administrator, or system administrator).
- Messages Trusted - The total number of messages received from addresses in the trusted senders list.
- Rank - The order in which users or domains are listed within the report.
- User - The specific user on the domain.

Spam and Virus Reports

Incoming Spam

This report tells you the number of spam messages which were received at different tolerance levels for all users of a domain (at the domain admin level) or all domains on your server (at the system

admin level). Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Rank - The order in which users or domains are listed within the report.
- Domain - For system admins, the specific domain on the server.
- User - For domain admins, the specific user on the domain.
- Account Type - For domain admins, the type of account the email address is associated with (user, domain administrator, or system administrator).
- Low Spam Messages - The total number of messages received with a low spam tolerance level.
- Medium Spam Messages - The total number of messages received with a medium spam tolerance level.
- High Spam Messages - The total number of messages received with a high spam tolerance level.
- Total Spam Messages - The total number of messages received with any spam tolerance level assigned to it.

Outgoing Spam

This report tells you the number of outgoing messages that were blocked due to spam for all users of a domain (at the domain admin level) or all domains on your server (at the system admin level). Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Rank - The order in which users or domains are listed within the report.
- Domain - For system admins, the specific domain on a server.
- User - For domain admin, the specific user on the domain.
- Account Type - For domain admins, the type of account the email address is associated with (user, domain administrator, or system administrator).
- Blocked Messages - The total number of messages that were sent and blocked as spam.

Greylisting

This report tells you the number of connections which were allowed and delayed due to greylisting for all users of a domain (at the domain admin level) or all domains on your server (at the system admin level). Clicking on individual domains, or individual users, will display a more detailed view of each.

Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Rank - The order in which users or domains are listed within the report.
- Domain - For system admins, the specific domain on the server.
- User - For domain admins, the specific user on the domain.
- Account Type - For domain admins, the type of account the email address is associated with (user, domain administrator, or system administrator).
- Allowed Connections - The total number of messages that passed greylisting and were delivered to the mailbox.
- Delayed Connections - The total number of messages that were delayed due to greylisting.
- Total Connections - The total number of connections made to a particular server (i.e., SMTP, POP, IMAP, etc.)

Viruses

This report tells you the number of viruses which were received through email for a specific domain (at the domain admin level) or all domains on your server (at the system admin level). Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The day of the week covered by the report.
- Viruses - The total number of viruses detected from incoming mail.

Trend Reports

Traffic Reports

Server Status

This report will tell you the amount of memory currently being used on your server. System administrators may use this report to identify issues such as spool count spikes, thread count spikes, memory spikes etc. and troubleshoot ways to correct them. For example, if the average CPU spikes, the system administrator may want to check the spam check and indexing settings. If the average memory usage spikes, the system administrator may want to check indexing and greylisting settings

and the max message size to content scan spam setting. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Avg. CPU - The average CPU usage percentage for the SmarterMail process.
- Avg. Memory - The average memory usage for the SmarterMail process.
- Avg. Nonpaged Memory - The average nonpaged memory usage for the SmarterMail process.
- Avg. Handles - The average number of handles used for the SmarterMail process.
- Avg. Threads - The average number of threads used for the SmarterMail process.
- Avg. Active Connections - The average number of active connections made by SmarterMail.
- Avg. Spool Count - The average number of messages in the spool.

Message Traffic

This report will tell you the number of messages that are being sent and received for a specific domain (at the domain admin level) or all domains on your server (at the system admin level). System administrators may use this report for overage billing, to identify potential spammers on the server or to identify high-usage domains. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Incoming Messages - The total number of messages the account has received.
- Outgoing Messages - The total number of messages the account has sent.
- Incoming Spam Messages - The total number of spam messages delivered to the mailbox.
- Outgoing Spam Messages - The total number of spam messages sent from the account.

Message Data

This report tells you the amount of data which was sent and received in KB for a specific domain (at the domain admin level) or all domains on your server (at the system admin level). System administrators may use this report to identify potential spammers on the server or to identify high-usage domains. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.

- Data Sent - The total size in KB of all data sent by the account.
- Data Received - The total size in KB of all data received by the account.

Throttle Traffic

This report shows the number of messages that have been throttled for a specific domain (at the domain admin level) or all domains on your server (at the system admin level). Domain and system administrators may use this report to identify issues with high usage customers. For example, if a user is sending a high number of bounced messages, that is an unnecessary use of system resources that can be easily corrected. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Bounces Received - The number of bounced messages throttled.
- Messages Sent - The number of sent messages throttled.
- SMTP Out Bandwidth - The amount of bandwidth throttled.

Throttle Violations

This report shows the number of throttle violations for a specific domain (at the domain admin level) or all domains on your server (at the system admin level). Domain and system administrators may use this report to identify issues with high usage customers. For example, if a user is sending a high number of bounced messages, that is an unnecessary use of system resources that can be easily corrected. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Bounces Received - The number of bounced messages throttled.
- Messages Sent - The number of sent messages throttled.
- SMTP Out Bandwidth - The amount of bandwidth throttled.

Traffic By Priority

This report shows how many messages going through the spool were assigned priority levels. For example, if the system administrator set mailing lists to a lower priority than regular messages, this report can be used compare mailing list traffic and normal traffic on the server. Note: Not all reports

are available for users and/or domains. Consult your system or domain administrator for report availability.

Bandwidth By Priority

This report shows the bandwidth for all messages in each priority level. For example, if the system administrator sets mailing lists to a lower priority than regular messages, this report can be used to compare mailing list traffic and normal traffic on the server and that bandwidth usage is occurring as expected. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

SMTP In Usage

This report tells you the size of the bandwidth and the number of connections that have been made from SMTP incoming mail for a specific domain (at the domain admin level) or all domains on your server (at the system admin level). Domain and system administrators may use this report to identify high usage accounts. This information can be used to evaluate whether to move such accounts to another server or to set limits on such accounts. This report can also be used to find potentially compromised reports because the administrator would see a jump in SMTP connections over time.

Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Bandwidth - The bandwidth in KB for all incoming SMTP mail.
- Avg. Active Connections - For system admins, the average number of active connections made by Smartermail.
- Connections - The total number of connections made to a particular server (i.e., SMTP, POP, IMAP, etc.)
- Blocked Connections - For system admins, the total number of connections that were blocked.

SMTP In Errors

This report tells if any errors occurred from SMTP incoming mail for all domains on your server. Domain and system administrators may use this report to identify users that are using faulty email clients or unnecessarily using system resources. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Blocked Connections - The total number of connections that were blocked.
- Bad Commands - The total number of bad commands given.
- Terminations - The total number of terminations that occurred for incoming mail.

SMTP Out Usage

This report tells you the size of the bandwidth and the number of connections that have been made from SMTP outgoing mail for a specific domain (at the domain admin level) or all domains on your server (at the system admin level). Domain and system administrators may use this report to identify high usage accounts. This information can be used to evaluate whether to move such accounts to another server or to set limits on such accounts. This report can also be used to find potentially compromised reports because the administrator would see a jump in SMTP connections over time.

Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Bandwidth - The bandwidth in KB for all incoming SMTP mail.
- Avg. Active Connections - The average number of active connections made by Smartermail.
- Connections - The total number of connections made to a particular server (i.e., SMTP, POP, IMAP, etc.)

SMTP Out Errors

This report tells if any errors occurred from SMTP outgoing mail from all domains on your server.

Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Bad Commands - The total number of bad commands given.
- Terminations - The total number of terminations that occurred for incoming mail.

POP Usage

This report tells you the size of the bandwidth and the number of connections that have been made from POP incoming mail for a specific domain (at the domain admin level) or all domains on your server (at the system admin level). Domain and system administrators may use this report to identify

high usage accounts. This information can be used to evaluate whether to move such accounts to another server or to set limits on such accounts. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Bandwidth - The bandwidth in KB for all incoming SMTP mail.
- Avg. Active Connections - For system admins, the average number of active connections made by Smartermail.
- Connections - The total number of connections made to a particular server (i.e., SMTP, POP, IMAP, etc.)
- Blocked Connections - For system admins, the total number of connections that were blocked.

POP Errors

This report tells if any errors occurred from POP incoming mail for all domains on your server. System administrators may use this report to identify users that are using faulty email clients or unnecessarily using system resources.

Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Blocked Connections - The total number of connections that were blocked.
- Bad Commands - The total number of bad commands given.
- Terminations - The total number of terminations that occurred for incoming mail.

IMAP Usage

This report tells you the size of the bandwidth and the number of connections that have been made from IMAP incoming mail for all domains on your server. Domain and system administrators may use this report to identify high usage accounts. This information can be used to evaluate whether to move such accounts to another server or to set limits on such accounts.

Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Avg. Active Connections - The average number of active connections made by Smartermail.
- Bandwidth - The bandwidth in KB for all incoming SMTP mail.
- Blocked Connections - The total number of connections that were blocked.
- Day - The specified amount of time that the report data falls within.

IMAP Errors

This report tells if any errors occurred from IMAP incoming mail for a specific domain (at the domain admin level) or all domains on your server (at the system admin level). Domain and system administrators may use this report to identify users that are using faulty email clients or unnecessarily using system resources.

Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Blocked Connections - The total number of connections that were blocked.
- Bad Commands - The total number of bad commands given.
- Terminations - The total number of terminations that occurred for incoming mail.

SpamAssassin Servers

This report shows general data regarding connections to external SpamAssassin servers. System administrators may use this report to identify faulty SpamAssassin servers and troubleshoot ways to correct the issue. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Avg. Active Connections - This is the average number of active connections made by SmarterMail.
- Connections - This is the total number of connections made to a SpamAssassin server.
- Failed Connections - The total number of failed connections to a SpamAssassin server.

SMTP Out Connections

This report tells you the number of SMTP out connections made for a specific domain (at the domain admin level) or all domains on your server (at the system admin level). Note: Not all reports are

available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Avg. Active Connections - For system admins, the average number of active connections made by Smartermail.
- Connections - The total number of connections made to a particular server (i.e., SMTP, POP, IMAP, etc.)
- Failed Connections - The total number of connections that failed.

ClamAV

This report tells you the number of connections your server has made to the ClamAV service. System administrators may use this report to identify and troubleshoot issues between SmarterMail and the ClamAV service. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Avg. Active Connections - The average number of active connections made to ClamAV by Smartermail.
- Connections - The total number of connections made to a particular server.
- Failed Connections - The total number of connections that failed.

Spam and Virus Reports

Incoming Spam Counts

This report tells you the number of spam messages which were received at different tolerance levels for a specific domain (at the domain admin level) or all domains on your server (at the system admin level). Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Low Spam Messages - The total number of messages received with a low spam tolerance level.

- Medium Spam Messages - The total number of messages received with a medium spam tolerance level.
- High Spam Messages - The total number of messages received with a high spam tolerance level.
- Total Spam Messages - The total number of messages received with any spam tolerance level assigned to it.

Outgoing Spam Counts

This report tells you the number of outgoing messages that were blocked due to spam for a specific domain (at the domain admin level) or all domains on your server (at the system admin level). System administrators can use this report to determine if the server is sending out a large amount of spam.

Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Blocked Messages - The total number of messages that were sent and blocked as spam. Note: The system administrator must enable outgoing spam checks or this report will not contain data.

Incoming Spam Percentages

This report tells you the percentages of spam messages which were received at different tolerance levels for a specific domain (at the domain admin level) or all domains on your server (at the system admin level). System administrators may use this report to adjust spam weight settings. For example, if the system administrator notices a large percentage of medium spam messages, it is highly likely that these messages actually are spam. For this reason, the system administrator may want to adjust the spam weights so that many of these messages will be marked as a high spam tolerance level in the future. Doing so may decrease the amount of spam delivered to users' inboxes. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Low Spam Percentage - The total percentage of spam messages received with a low spam tolerance level.
- Medium Spam Percentage - The total percentage of spam messages received with a medium spam tolerance level.
- High Spam Percentage - The total percentage of spam messages received with a high spam

tolerance level. Total Spam Percentage - The total percentage of spam messages received with any spam tolerance level assigned to it.

Outgoing Spam Percentages

This report tells you the percentage of outgoing messages that were blocked as spam for a specific domain (at the domain admin level) or all domains on your server (at the system admin level). Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Blocked Messages - The total percentage of outgoing messages that were sent and blocked as spam.

Greylisting

This report tells you the number of connections which were allowed and delayed due to greylisting for a specific domain (at the domain admin level) or all domains on your server (at the system admin level). Domain and system administrators may use this report to verify that greylisting is working.

Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Allowed Connections - The total number of messages that passed greylisting and were delivered to the mailbox without delay.
- Delayed Connections - The total number of messages that were delayed due to greylisting.
- Total Connections - The total number of connections made to a particular server (i.e., SMTP, POP, IMAP, etc.)

Viruses

This report tells you the number of viruses which were received through email for a specific domain (at the domain admin level) or all domains on your server (at the system admin level). Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Viruses - The total number of viruses that were detected from incoming mail.

Cyren Premium Antispam

This report tells you the number of messages that the Cyren Detection Center classified as potential spam on your server. System administrators may use this report to verify that the Cyren Premium Antispam add-on is working, to gauge the amount of spam coming into the server and more. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Confirmed - The number of messages the Cyren Detection Center confirmed as coming from known spam sources.
- Suspected - The number of messages the Cyren Detection Center suspected might be spam because they were sent to a slightly larger than average distribution.
- Bulk - The number of messages the Cyren Detection Center deemed as sent in bulk. Note: Newsletters or mailing list messages may be included in this classification.
- Not Spam - The number of messages the Cyren Detection Center deemed were not spam.

Cyren Zero-hour Antivirus

This report tells you the number of incoming messages that the Cyren Detection Center flagged as containing potential viruses. System administrators may use this report to verify that the Cyren Zero-hour Antivirus add-on is working, the number of viruses coming into the server and more. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Virus Result - The number of messages in which the Cyren Detection Center confirmed they contained a virus.
- High Result - The number of messages the Cyren Detection Center deemed have a high likelihood of presenting a virus threat.
- Medium Result - The number of messages in which the Cyren Detection Center found a probable threat of viruses.
- Non-virus Result - The number of messages the Cyren Detection Center confirmed did not

contain viruses.

- Unknown Result - The number of messages in which the Cyren Detection Center could not determine the threat for viruses.

Message Sniffer

This report tells you the number of messages that Message Sniffer classified as potential spam on your server. System administrators may use this report to verify that the Message Sniffer add-on is working, to gauge the amount of spam coming into the server and more. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The specified amount of time that the report data falls within.
- Confirmed - The number of messages Message Sniffer confirmed as coming from known spam sources.
- Not Spam - The number of messages Message Sniffer deemed were not spam.

Security Reports

Abuse Detection

This report shows the number of attacks on the server. For example, if a system administrator notices an increase in DOS or harvesting violations, he may review server logs to determine the IP address that is triggering the violations and consider permanently blocking the IP. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The day of the week covered by the report.
- DOS Violations - The total number of DOS violations.
- Harvesting Violations - The total number of harvesting violations.
- Internal Spammer Violations - The total number of spam violations from users on the SmarterMail server.

Blacklist / Whitelist

This report shows the number of connections made from blacklisted and whitelisted IPs. Note: Not all reports are available for users and/or domains. Consult your system or domain administrator for report availability.

The following report items are available:

- Day - The day of the week covered by the report.
- Blacklisted Connections - The number of connections SmarterMail made to blacklisted IPs.
- Whitelisted Connections - The number of connections SmarterMail made to whitelisted IPs.

Events

Events Overview

The Event system in SmarterMail is an incredibly powerful tool for staying up-to-date with what is going on with the SmarterMail server.

SmarterMail can detect events as they occur, generate messages for those events, and deliver the messages to administrators and users that need the information. For example, users can receive notifications when a task is due or system administrators can receive notifications when the disk space for a domain reaches a certain percentage. With notifications, administrators don't have to query for the status of the items in the system--they just receive messages when specific events occur so they can take care of them.

There are two categories of events in SmarterMail: user-level events and system-level events:

- User-level events are specific to each user.
- System-level events can only be set by system administrators.

To view events, click the settings icon . For user events, expand the My Settings folder and click Events in the navigation pane. For domain-level events, expand the System Settings folder and click Events in the navigation pane. Events can also be viewed by event group or category (collaboration, email, domain, etc.). Any configured events will load in the content pane. Note: Only system administrators can access system-level events.

In general, the following columns are available:

- Checkbox - Use these boxes to select multiple events. Events must be selected before choosing an action from the content pane toolbar.
- Name - The name of the event.
- Status - Indication of whether the event is enabled or disabled. The event will only trigger if it is enabled.
- Event Category - The feature to which the event pertains (collaboration, email, security, etc.)
- Event Type - The event that triggers the action.

- Conditions - The criteria the event must meet to trigger the action.
- Actions - The actions that occur when an event is triggered.

The following actions are available from the content pane toolbar:

- New - Creates a new event.
- Edit - Allows the user/system administrator to make changes to an event's settings.
- Delete - Permanently deletes the selected event(s).
- Search - Allows the user/system administrator to search for a specific event.

To view the settings for a specific event, simply double-click the event and the event settings will load in the content pane.

Creating New Events

To add a new event, click the settings icon . For user-level events, expand the My Settings folder and click Events in the navigation pane. Then click New in the content pane toolbar. The new event settings will load in the content pane.

Saving Event Details

When you add a new event, event details are divided into two sections: options and actions.

Options

Use this section to specify the following event options:

- Event Name - The name of the event.
- Event Category - The feature to which the event pertains (collaboration, email, security, etc.)
- Event Type - Each category has several specific event types that can trigger the action.
- Domain - The domain name the event was created for.
- Time of Day - The time frame during which the event occurs.
- Day of Week - The day(s) of the week during which the event occurs.
- Enabled - Checkmark this selection to enable the event. This can be used to temporarily disable events.

Depending on the event category and type selected, different event action criteria will be available.

For more information on the various event action criterions, see the corresponding event category page of the online help.

Actions

Use this section to specify the following event actions:

- Action - The actions that occur when an event is triggered (or how the system notifies you).
- Maximum Frequency - To specify how frequently the action is performed, select the appropriate option from the list.
- Notification Profile - To specify which notification profile to use, select the appropriate option from the list.
- From Address - The email address the system uses to send the event notification

Subject, Short Body, and Body will all be populated by the system using the variables listed.

Additional fields may be available depending on the event category chosen.

Click the Save button in the actions popup window and then click Save in the content pane toolbar to save that event.

Notification Profiles

Users of SmarterMail can create Events that allow them to select criteria and apply specific actions when the criteria are met. One of the actions is to receive email notifications when an event is triggered. For example, users can receive notifications when a task is due or system administrators can receive notifications when the disk space for a domain reaches a certain percentage. Notification profiles determine how those messages are sent.

To view a list of current notification profiles, click the settings icon . Then expand the My Settings and Advanced Settings folders and click Notification Profiles . Your notification profiles will load in the content pane.

The following columns are available:

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

The following options are available from the content pane toolbar:

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

To view a specific notification profile, simply double-click the appropriate profile. Alternatively, you can select the profile and click on the Edit button. Regardless of how you open the profile, it will load as a modal window in the content pane.

Creating a Notification Profile

Creating a notification profile is very simple. Just click on the New button, and a new modal window will open with the following options:

- Notification Profile Name - The name you set for the profile.
- Email Address(es) - The email address(es) to which notifications are sent. More than one email address can be added to this field, they just need to be separated with a comma.
- Enable - Checking this box will enable email notifications.
- SMS Email Address(es) - Sometimes users will want notifications sent to their mobile devices via text message. Here you'll input the mobile device email address to which notifications are sent. If you're unsure of this address, contact your mobile provider.
- Enable - Checking this box will enable SMS notifications.
- Enable Reminders - Checking this box will display reminders for tasks and appointments in a popup window in webmail.

Use of Notification Profiles

As mentioned, notification profiles are primarily used in conjunction with Events. When a new event is created, users have the ability to select a notification profile to use when that event fires. If more than one notification profile is available, each will be listed and users will need to make sure they've selected the proper profile to use with that event.

Event Categories

Alias Events

System administrators can receive notifications based on the following alias events:

- Alias Added - Notifies system administrators when a user creates a new email alias.
- Alias Deleted - Notifies system administrators when a user deletes an existing email alias.

Conditions

Depending on the event selected, the following event criteria are available:

- Event Name - The name of the event.
- Event Category - The feature to which the event pertains (collaboration, email, security, etc.)
- Event Type - Each category has several specific event types that can trigger the action.
- Domain - The domain on which the event occurs.
- Time of Day - The time frame during which the event occurs.

- Day of Week - The day(s) of the week during which the event occurs.
- Alias Name - The alias name that will trigger the event.
- Alias Addresses - The alias address that will trigger the event.
- Enabled - The Enabled checkbox must be marked in order for this event to trigger. Use this setting to temporarily disable events.

Actions

Depending on the event selected, the following actions are available:

- Use notification profile
- Send email
- Toast notification
- Execute command-line

Collaboration Events

Users and system administrators can receive notifications based on the following collaboration events:

- Calendar Reminder Occured - Notifies users that there is an upcoming appointment.
- Task Reminder Occured - Notifies users that a task deadline is approaching.

Conditions

Depending on the event selected, the following event criteria are available:

- Event Name - The name of the event.
- Event Category - The feature to which the event pertains (collaboration, email, security, etc.)
- Event Type - Each category has several specific event types that can trigger the action.
- Domain - The domain on which the event occurs.
- Time of Day - The time frame during which the event occurs.
- Day of Week - The day(s) of the week during which the event occurs.
- Subject - The words that will trigger the event if found within the appointment or task subject.
- Location - The appointment location that will trigger the event.
- Description - The words that will trigger the event if found within the appointment or task description.
- Email Address - The email address that will trigger the event.
- Enabled - The Enabled checkbox must be marked in order for this event to trigger. Use this setting to temporarily disable events.

Actions

Depending on the event selected, the following actions are available:

- Use default notification profile for user
- Use my notification profile
- Send email
- Toast notification
- Execute command-line

Domain Events

Conditions

System administrators can receive notifications based on the following domain events:

- Domain Added - Notifies system administrators when a new domain is added to the server.
- Domain Deleted - Notifies system administrators when an existing domain is deleted from the server.
- Domain Disk Space Used - Notifies system administrators when a domain's disk space usage reaches a certain threshold.

Conditions

Depending on the event selected, the following event criteria are available:

- Event Name - The name of the event.
- Event Category - The feature to which the event pertains (collaboration, email, security, etc.)
- Event Type - Each category has several specific event types that can trigger the action.
- Time of Day - The time frame during which the event occurs.
- Day of Week - The day(s) of the week during which the event occurs.
- Domain - The domain on which the event occurs.
- Domain Usage (%) - The percentage of disk space utilization that will trigger the event.
- Domain Usage (MB) - The disk space utilization in MB that will trigger the event.
- Domains Used - The number of domains that will trigger this event.
- Domains User (%) - The percentage of the total number of domains allowed that will trigger the event.
- Enabled - The Enabled checkbox must be marked in order for this event to trigger. Use this setting to temporarily disable events.

Actions

Depending on the event selected, the following actions are available:

- Use my notification profile
- Send email

- Toast notification
- Execute command-line

Email Events

Users and system administrators can receive notifications based on the following email events:

- Message Received - Notifies users that they received a new email message.
- Message Sent - Notifies users that the mail server sent a message.

Conditions

Depending on the event selected, the following event criteria are available:

- Event Name - The name of the event.
- Event Category - The feature to which the event pertains (collaboration, email, security, etc.)
- Event Type - Each category has several specific event types that can trigger the action.
- Time of Day - The time frame during which the event occurs.
- Day of Week - The day(s) of the week during which the event occurs.
- To Address - The email address to which the message was sent.
- To Domain - The domain the email was sent to or received from that will trigger the on which the event.
- From Address - The email address from which the email message was sent.
- From Domain - The domain from which the email message was sent.
- Subject - The words that will trigger the event if found within the subject of the message.
- Intra Domain - Select this option to trigger the event when an email is sent/received from within the domain.
- Size - The message size in KB that will trigger the event.
- Enabled - The Enabled checkbox must be marked in order for this event to trigger. Use this setting to temporarily disable events.

Actions

Depending on the event selected, the following actions are available:

- Use my notification profile
- Send email
- Toast notification
- Execute command-line

Mailing List Events

System administrators can receive notifications based on the following mailing list events:

- Mailing List Added - Notifies system administrators when a new mailing list is created.
- Mailing List Bounce Removal - Notifies system administrators when an email address is removed from the mailing list due to bounced messages.
- Mailing List Deleted - Notifies system administrators when an existing mailing list is deleted.
- Mailing List Subscribe - Notifies system administrators when an email address subscribes to a mailing list.
- Mailing List Unsubscribe - Notifies system administrators when an email address unsubscribes from a mailing list.
- Message Sent to Mailing List - Notifies system administrators when a new message is sent to the mailing list.

Conditions

Depending on the event selected, the following event criteria are available:

- Event Name - The name of the event.
- Event Category - The feature to which the event pertains (collaboration, email, security, etc.)
- Event Type - Each category has several specific event types that can trigger the action.
- Time of Day - The time frame during which the event occurs.
- Day of Week - The day(s) of the week during which the event occurs.
- Domain - The domain on which the event occurs.
- Email Address - The email address that will trigger the event.
- From Address - The email address from which the message is sent to the mailing list.
- List Name - The mailing list name that will trigger the event.
- Subscribe Method - The subscription signup method that will trigger the event.
- Unsubscribe Method - The subscription removal method that will trigger the event.
- Enabled - The Enabled checkbox must be marked in order for this event to trigger. Use this setting to temporarily disable events.

Actions

Depending on the event selected, the following actions are available:

- Use my notification profile
- Send email

- Toast notification
- Execute command-line

Security Events

System administrators can receive notifications based on the following security events:

- Abuse Detection Rule Triggered - Notifies system administrators when an abuse detection rule has been triggered.
- ClamAV Failure - Notifies system administrators when there has been a failure with the ClamAV service.
- Blacklist Status Changed - Notifies system administrators when there has been a change in the automatic blacklist check of a particular mail server IP. This can be triggered when a server's blocked status is set to True or False. (Added or removed.)
- Outgoing Message Blocked - Notifies system administrators when an outgoing message is blocked.
- SpamAssassin Failure - Notifies system administrators when there has been a failure with the SpamAssassin service.
- Virus Found - Notifies system administrator if a virus is found on the server.

Conditions

Depending on the event selected, the following event criteria are available:

- Event Name - The name of the event.
- Event Category - The feature to which the event pertains (collaboration, email, security, etc.)
- Event Type - Each category has several specific event types that can trigger the action.
- Time of Day - The time frame during which the event occurs.
- Day of Week - The day(s) of the week during which the event occurs.
- ClamAV IP - The IP address of the ClamAV server that will trigger the event.
- ClamAV Port - The port of the ClamAV server that will trigger the event.
- Consecutive Failures - The number of consecutive failures that will trigger the event.
- File Name - The file name that will trigger the event.
- File Size - The size of the file in KB that will trigger the event.
- Name - The full name of the person that will trigger the event.
- IP Address - The IP address that will trigger the event.
- Rule Name - The rule name that will trigger the event.
- Rule Type - The type of security rule that will trigger the event.
- Spam Weight - The spam weight of the message that will trigger the event.
- SpamAssassin IP - The IP address of the SpamAssassin server that will trigger the event.

- SpamAssassin Port - The port of the SpamAssassin server that will trigger the event.
- Subject - The words that will trigger the event if found within the subject of the message.
- To Address - The email address to which the message was sent.
- From Address - The email address from what the message was sent.
- Virus Name - The virus name that will trigger the event.
- Enabled - The Enabled checkbox must be marked in order for this event to trigger. Use this setting to temporarily disable events.

Actions

Depending on the event selected, the following actions are available:

- Execute command-line
- Send email
- Use notification profile

System Events

System administrators can receive notifications based on the following system events:

- Add-on Expiration - Notifies system administrators when a paid add-on, like Exchange ActiveSync, is expiring soon.
- Disk Availability - Notifies system administrators when a disk drive is nearly full.
- Gateway Failure - Notifies system administrators when a gateway server has failed.
- License Expiration - Notifies system administrators when a license is about to expire.
- Memory - Notifies system administrators when a domain's or user's memory usage reaches a certain threshold.
- New Version Available - Notifies system administrators when a new version of the product is available.
- Service Started - Notifies system administrators when a new service is started.
- Service Stopped - Notifies system administrators when a service is stopped.
- Spool Count - Notifies system administrators when the spool count reaches a certain level.
- System Settings Changed - Notifies system administrators when any settings have been changed.
- System Uptime - Notifies system administrators when the uptime for the system reaches a certain point.
- Threads - Notifies system administrators when the thread count reaches a certain level.
- Upgrade Protection Reminder - Notifies system administrators when the upgrade protection for their SmarterMail license is expiring.

Conditions

Depending on the event selected, the following event criteria are available:

- Event Name - The name of the event.
- Event Category - The feature to which the event pertains (collaboration, email, security, etc.)
- Event Type - Each category has several specific event types that can trigger the action.
- Time of Day - The time frame during which the event occurs.
- Day of Week - The day(s) of the week during which the event occurs.
- Days Left - The number of remaining days that will trigger the event.
- Add-on Name - The add-on that is going to expire.
- Disk Drive - The drive letter to monitor.
- Disk Usage (GB) - The drive usage limitation, in gigabytes, that will trigger the event.
- Disk Usage (%) - The drive usage limitation, as percentage of space, that will trigger the event.
- Free Disk Space (GB) - The free space limitation, in gigabytes, that will trigger the event.
- Free Disk Space (%) - The free space limitation, as percentage of available space, taht will trigger the event.
- Gateway Address - The address of the gateway that will trigger the event.
- Memory Used (%) - The percentage of memory used that will trigger the event.
- Memory Used (MB) - The amount of memory used in MB that will trigger the event.
- Service - The service that will trigger the event.
- Spool Count - The number of messages in the spool that will trigger the event.
- Thread Count - The number of threads that will trigger the event.
- Uptime (Days) - The number of days the system has been running that will trigger the event.
- Version - The version that will trigger the event.
- Enabled - The Enabled checkbox must be marked in order for this event to trigger. Use this setting to temporarily disable events.

Actions

Depending on the event selected, the following actions are available:

- Execute command-line
- Send email
- Toast notification
- Use my notification profile

Throttling Events

System administrators can receive notifications based on the following throttling events:

- Domain Throttled - Notifies system administrators when a domain reaches the throttling threshold.
- User Throttled - Notifies system administrators when a license is about to expire.

Conditions

Depending on the event selected, the following event criteria are available:

- Event Name - The name of the event.
- Event Category - The feature to which the event pertains (collaboration, email, security, etc.)
- Event Type - Each category has several specific event types that can trigger the action.
- Time of Day - The time frame during which the event occurs.
- Day of Week - The day(s) of the week during which the event occurs.
- Domain - The domain on which the event occurs.
- Rejected - With throttling you can choose to delay or reject messages in the spool after the throttling threshold is hit. So if a domain is set to allow 500 messages per hour before throttling and the action is set to reject, those emails will get deleted instead of just being delayed for later delivery. If you have it set to delay, those messages stay in the spool and 500 more will send out in the next hour.
- From Address - The email address from which the message is sent.
- Enabled - The Enabled checkbox must be marked in order for this event to trigger. Use this setting to temporarily disable events.

Actions

Depending on the event selected, the following actions are available:

- Execute command-line
- Send email
- Use notification profile
- Toast notification

User Events

Users and system administrators can receive notifications based on the following user events:

- User Added - Notifies system administrators when a new user is added.
- User Changed Forward - Notifies system administrators when a user adds a forwarding

address or modifies an existing forwarding address.

- User Changed Password - Notifies system administrators when a user changes their password.
- User Deleted - Notifies system administrators when an existing user is deleted.
- User Disk Space Used - Notifies users when the mailbox space utilization reaches a certain threshold.

Conditions

Depending on the event selected, the following event criteria are available:

- Event Name - The name of the event.
- Event Category - The feature to which the event pertains (collaboration, email, security, etc.)
- Event Type - Each category has several specific event types that can trigger the action.
- Time of Day - The time frame during which the event occurs.
- Day of Week - The day(s) of the week during which the event occurs.
- Domain - The domain on which the event occurs.
- Full Name - The full name of the person that will trigger the event.
- Mailbox Usage (%) - The percentage of mailbox space utilization that will trigger the event.
- Mailbox Usage (MB) - The mailbox space utilization in MB that will trigger the event.
- Username - The username that will trigger the event.
- Enabled - The Enabled checkbox must be marked in order for this event to trigger. Use this setting to temporarily disable events.

Actions

Depending on the event selected, the following actions are available:

- Execute command-line
- Send email
- Use notification profile

Settings

My Settings

Account Settings

Account Settings contain basic information about the email user, including the friendly "Display Name" as well as information for forwarding and reply-to addresses. The information in some of these fields are also available to fill variables used when creating Signatures for users of the Professional Edition of SmarterMail.

To edit your personal settings, click the settings icon . Then expand the My Settings folder and click Account Settings from the navigation pane. The user settings will load in the content pane and the following tabs will be available:

User

Use this tab to specify the following user-based settings:

- Username - The identifier used to login to SmarterMail. This will be the personalized part of the full email address, such as the "JDoe" part of JDoe@example.com.
- Password - The password used to login to Smartermail. This will only appear if the authentication method used for the account is something other than Active Directory.
- Display Name - The name that is associated with the username and that is also displayed on outgoing messages.
- Reply-to Email Address - The email address used in the reply-to header of messages sent through webmail. This address will be used by receiving email clients when replying to a message.
- Time Zone - The user's time zone.
- Backup Email Address - The email address to which password reset instructions will be sent if the user forgets his password. Generally, this email address will need to be separate from this account - possibly a GMail or Yahoo! email address, or even the default email address of a domain administrator.
- Disable Greylisting - Select this option to disable greylisting .

Webmail

Use this tab to specify the following webmail settings:

- Initial Page on Login - The page you see upon logging in to SmarterMail. You can either set this for My Today Page or your inbox.
- Display Format - To specify the default format in which messages are displayed, select the appropriate option from the list. Options include:
 - HTML - This option will display HTML content, if present in the email. This content can include stylistic elements, like fonts or colors, as well as hyperlinks, images and other formatting elements.
 - Text - This option will only display text. While it is less interesting (no fonts, images, etc), it is also much more secure and is faster to view than HTML.
 - Sort Messages by - The order in which messages are displayed. By default, messages are displayed by date in descending in order.

- Delete Action - To specify the action performed on deleted messages, select the appropriate action from the list.
- Move to Deleted Items folder - Deleted items will appear in the deleted items folder, which will need to be regularly emptied.
- Auto Purge Folder - Permanently deletes the message. Note: When deleted messages are purged, the action is final. You will not be able to retrieve these messages later.
- Mark as Deleted - Flags the message for deletion, but it does not move messages to the Deleted Items folder and messages remain until the folder is purged.
- Mark as Deleted and Hide - Flags the messages for deletion and hides them from view, but they will not be removed until the folder is purged. Note: Be careful to monitor your disk space usage when using this option, as it may fill up with what appears to be a small number of messages.
- Skin - The domain or system administrator may have enabled different skins for users to choose from. To specify which skin to use, select the appropriate option from the list. The Default skin is the standard blue skin that SmarterTools includes with all products.
- Preview Pane - To specify where the preview pane displays in the webmail interface, select the appropriate option from the list. By default, the preview pane appears at the bottom of the content pane. Disabling the Preview Pane means only a list of messages appears in the content pane and each message will need to be opened separately in order to view their contents.
- Disable images in preview pane - Select this option to prevent images from displaying when viewing messages in the preview pane. You may want to select this so that messages load faster. Note: By selecting this option, images will still appear when a messages is opened outside of the Preview Pane.
- Enable reminder popup window - Selecting this option means that any reminders will display in popup windows. If your browser has a popup blocker, your email server URL may need to be added to allow reminder popups to display. In addition, this is enabled by default.
- Enable sounds - Select this option to enable sounds in webmail, such as when a new chat message is received.
- Enable new message notifications - Select this option to display a temporary notification in the webmail interface when a new email message is received. This notification will display no matter which section of the interface is selected and generally appears in the lower part of your screen.
- Disable reminders for appointments and tasks - Select this option to disable all reminders for appointments and tasks.
- Mark messages downloaded by POP3 as read - Select this option to mark all messages that are downloaded via a POP3 connection as read.
- Mark messages sent to junk as read - Select this option to mark messages as read on the server

when marked as spam.

- Show HTML hyperlinks when printing - Select this option to add link URLs in parenthesis to the right of the hyperlinks when printing email messages.

Compose

Use this tab to specify settings and options for how SmarterMail behaves when composing emails from the webmail interface.

- Text Encoding - To specify the character set used in messages composed through the Web interface, select the appropriate option from the list. By default, SmarterMails sets the encoding to Western European (ISO). However, SmarterMail supports encoding for over 35 different text formats, thereby supporting encoding for most parts of the world.
- Spell Check Dictionary - To specify the default dictionary to use for spell-checking emails, select the appropriate option from the list. SmarterMail offers dictionaries for over 17 different languages. If the user is unsure, they can select the option to use the same spell check dictionary that matches the language they selected when they logged in to SmarterMail.
- Forwarding Method - To specify the method by which messages are forwarded, select the appropriate option from the list.
 - Normal - Includes original content, including font styles from original message, as part of the new message.
 - Text - Inserts the plain text version of the original message into the new message. This is useful if you want to exclude links, fonts or other formatting.
 - Embed as Attachment - Attaches the original message to the new message as an attachment. The message will not appear in the body of your message.
- Auto Save Frequency - To specify how frequently SmarterMail saves a draft of a message you are writing, select the appropriate option from the list.

Note: For most users, basic headers will be sufficient. Basic headers include From, To, and Subject headings whereas the full header includes MIME type filter restrictions, etc.
- Compose Format - This specifies the type of message that is generated in the compose window. HTML format allows for greater customization and formatting, and full use of the HTML editor, but generates larger sized messages based on the amount of formatting done to the message. Text formatted messages are generally smaller in size and remove the ability to format text, add clickable links, etc.
- Reply Text Indicator - This sets the character that is appended to the beginning of each line of an original message when that message is replied to.
- Include previous replies in reply - Select this option to embed the text of the original message

in a message reply. This includes text from messages in reply threads.

- Enable sent items folder - Select this option to save all outgoing messages in the Sent Items folder. Note: If you send many messages, you may need to delete items from this folder regularly.
- Enable read receipts by default - Select this option to create read receipts for all outgoing messages. Users should be careful when enabling this and only do so if required for business or compliance or regulatory requirements.
- Enable trusted sender for webmail recipients - Select this option to add the email addresses that you have sent mail to through webmail to your trusted senders list. This means that any email from these addresses is automatically trusted by SmarterMail and will avoid any spam filters.
- Disable X-Originating_IP header in messages - Select this option to remove your IP address from the X-Originating_IP header when sending messages via webmail. Some people prefer that their IP address isn't included in the header of emails that are sent out as they feel it is a potential security risk.
- Warn about common email mistakes prior to sending - Enabling this means that SmarterMail will quickly review any message sent to check for items like missing attachments. This includes times when the word "attachment" is used in the body or subject of the message, but an attachment is not being sent with the email message.
- Automatically check spelling prior to sending - Enabling this means SmarterMail will quickly review any message sent to check for spelling and grammar issues when sending via webmail.

Forwarding Use this tab to set up SmarterMail to forward received messages to another email account.

- Forwarding Address - The email address(es) to which messages will be forwarded. Separate multiple email addresses with a semi-colon or comma.
- Delete messages when forwarded - Select this option to automatically delete messages from your SmarterMail inbox after they are forwarded.

Plus Addressing

Plus addressing is a feature of SmarterMail that allows you to automatically filter your incoming email without creating content filtering rules first. Plus addressing also allows users to use special email addresses if they do not want to give out their real email address. For example, if user@example.com needs to provide a valid email address to sign up for a newsletter, he can sign up for the newsletter using the address user+technewsletter@example.com. When the newsletter is delivered, it will automatically be routed to the Technewsletter folder. If the folder does not exist, it will be created automatically. Note: For plus addressing to work, it is important that the folder name appears AFTER

the username, but BEFORE the domain name. So the format should be:

username+foldername@domain .

- Action - The action SmarterMail should take when a plus-addressed email is received.
- Move to folder - If the target folder exists, the incoming message will be placed into it. If the folder does not exist, it will be created. No more than 10 folders can be auto-created in this method during a six hour period to prevent abuse.
- Move to folder (if it exists) - If the target folder exists, the incoming message will be placed into it. Otherwise, the email will get placed in the inbox.
- Leave in Inbox - Drops the message in to your inbox.
- Enable plus addressing - Select this checkbox to enable plus addressing.

Account Profile

The information contained in your account profile is publicly available to other users on the domain if the system administrator has enabled the Global Address List (GAL). Users can access your public contact information only by accessing the GAL through webmail or LDAP. Note: LDAP is a feature available to SmarterMail Enterprise users only.

Much of the information filled out in a user's Account Profile is also available as a variable that can be used when Domain Administrators create domain level signatures.

To view or edit your account profile, click the settings icon . Then expand the My Settings folder and click Account Profile in the navigation pane. Your contact details will load in the content pane.

Note: When changing your profile picture, while it will update automatically in the webmail interface, updated pictures won't update in any third-party chat clients like Adium or Pidgin until you actually log into the chat client and force a status change. That means that, when using the Web-based chat client in SmarterMail, users in third-party clients may not see your updated picture.

In general, contact details are divided into four sections:

- Personal Info - Your display name, title, first name, middle name, last name, suffix, email address, instant messenger, home page, and date of birth.
- Contact Info - Your home phone number, work phone number, mobile phone number, pager number, home and work fax numbers, and home address.
- Work Info - Your company name, job title, department, office, work address, and website URL.
- Additional Info - Type any additional details about yourself.

Auto-responder

Users can set up auto-responders to automatically send a prewritten response when an email message is received. They are commonly used to notify senders that the recipient is out of the office or on vacation.

To set up an auto-responder, click the settings icon . Then expand the My Settings folder and click Auto-Responder in the navigation pane. The auto-responder settings will load in the content pane and the following tabs will be available:

Options

Use this tab to specify the following options:

- Enable auto-responder - Select this checkbox to turn the auto-responder on.
- Disable responses to indirect mail - By selecting this checkbox, the auto-responder will only be triggered by email sent directly to you. Any email you receive through a mailing list, forward, or an alias will not trigger the auto-responder.
- Limit responses to once daily - Select this checkbox to ensure an email address only receives the auto-responder message once per day, even if they send you multiple messages. If you disable this option, every email you receive will trigger your auto-responder. It is HIGHLY recommended that you keep this option turned on to avoid the potential of your email address, your domain, or even potentially your entire mail server from becoming blacklisted by an ISP.

Auto-Responder Message

Use this tab to create your personalized auto-responder message. Note: This tab is only available if the auto-responder is enabled.

- Subject - The words or phrase that appears in the subject of the auto-responder message (e.g. Out of Office).
- Compose Format - To specify whether the auto-responder displays in plain text or HTML, select the appropriate option from the list.
- Start and End Dates - You can specify when your auto-responder will be active by setting start and end dates. This is particularly helpful for planned absences like during a vacation or extended holiday.
- Message - Type the text of the auto-responder in this field. You can customize the message with HTML formatting should you so desire. However, make sure that your compose format is set to HTML if you want to format your message with custom fonts, sizes, colors, links, etc. An example auto-responder is: "I will be out of the office from June 1 to June 15. I will respond to

your message upon my return to the office on June 16. If you need immediate assistance, please contact Jane Doe at jdoe@example.com."

Connected Services

SmarterMail allows users to connect different services to their SmarterMail accounts to facilitate things like attaching links to shared files. The simplest example is connecting Google Drive, Dropbox or OneDrive to your mailbox so that you can share links to files stored in your cloud account.

To view your connected services, click the Settings icon . Then expand the My Settings folder and click Connected Services in the navigation pane. A list of services that are connected to your mailbox will load in the content pane and the following options will be available in the content pane toolbar:

- New - Creates a new trusted sender.
- Delete - Permanently deletes the selected trusted sender(s).

Connecting a Service

To connect a new service to your account, simply click the New button in the content pane toolbar. A new window will appear that lists those services currently available to users. Select the service you wish to connect, and follow the on-screen prompts offered by SmarterMail to complete the process.

Removing a Connected Service

To remove a connected service, or to simply reset the connection, select the service from the list on the page, and click the Delete button in the content pane toolbar.

Trusted Senders

This setting allows users to list specific email addresses (such as jsmith@example.com) or domains (such as example.com) that will be exempted from spam filtering. This can prevent mail from friends, business associates and mailing lists from being blocked and lets the system know that these messages come from a trusted source. Note: The email address for messages that you unmark as spam are automatically included on your trusted senders list.

To view your trusted senders list, click the settings icon . Then expand the My Settings folder and click Trusted Senders in the navigation pane. A list of trusted senders will load in the content pane and the following options will be available in the content pane toolbar:

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

Signatures

An email signature is a block of text automatically appended at the bottom of an email message. Signatures may contain the sender's name, address, phone number, disclaimer, or other contact information. In addition, SmarterMail allows users to create HTML formatted signatures that can include stylized text, links, images, etc. For example, a signature can contain a company logo and tagline, an image that links to a personal or business social media account, or even links to other properties, like a company's help desk or management interface. Check out the SmarterTools knowledge base for more information on how to customize signatures.

To access your signature settings, click the settings icon . Then expand the My Settings folder and click Signatures in the navigation pane. The signature settings will load in the content pane and the following tabs will be available:

Mappings

Use this tab to assign a signature to your mailbox. Note: Domain administrators can enforce signatures on a domain-wide basis. In such cases, users may not be able to map a signature to their SmarterMail mailbox. However, users will still be able to map signatures to any SMTP mailboxes that have been added to their account.

Signatures

Use this tab to create or edit signatures. To create a new signature, click New in the content pane toolbar and complete the appropriate fields. To edit an existing signature, select the desired signature and click Edit in the content pane toolbar.

Depending on the SmarterMail Edition being used, some variables may be available for Domain Administrators to easily template out signatures for each user of a domain. Professional Edition administrators have access to a few variables that pull from a user's Account Settings whereas Enterprise Edition administrators have access to a much broader amount of information found in a user's Account Profile .

Events Overview

The Event system in SmarterMail is an incredibly powerful tool for staying up-to-date with what is going on with the SmarterMail server.

SmarterMail can detect events as they occur, generate messages for those events, and deliver the messages to administrators and users that need the information. For example, users can receive notifications when a task is due or system administrators can receive notifications when the disk space

for a domain reaches a certain percentage. With notifications, administrators don't have to query for the status of the items in the system--they just receive messages when specific events occur so they can take care of them.

There are two categories of events in SmarterMail: user-level events and system-level events:

- User-level events are specific to each user.
- System-level events can only be set by system administrators.

To view events, click the settings icon . For user events, expand the My Settings folder and click Events in the navigation pane. For domain-level events, expand the System Settings folder and click Events in the navigation pane. Events can also be viewed by event group or category (collaboration, email, domain, etc.). Any configured events will load in the content pane. Note: Only system administrators can access system-level events.

In general, the following columns are available:

- Checkbox - Use these boxes to select multiple events. Events must be selected before choosing an action from the content pane toolbar.
- Name - The name of the event.
- Status - Indication of whether the event is enabled or disabled. The event will only trigger if it is enabled.
- Event Category - The feature to which the event pertains (collaboration, email, security, etc.)
- Event Type - The event that triggers the action.
- Conditions - The criteria the event must meet to trigger the action.
- Actions - The actions that occur when an event is triggered.

The following actions are available from the content pane toolbar:

- New - Creates a new event.
- Edit - Allows the user/system administrator to make changes to an event's settings.
- Delete - Permanently deletes the selected event(s).
- Search - Allows the user/system administrator to search for a specific event.

To view the settings for a specific event, simply double-click the event and the event settings will load in the content pane.

Synchronized Devices

SmarterMail Enterprise uses multiple data synchronization technologies to sync mailbox data with email clients and mobile devices:

- Microsoft Exchange ActiveSync is an optional add-on that syncs SmarterMail mailboxes with most smartphones and tablets and Outlook 2015.
- Exchange Web Services is an optional add-on that seamlessly syncs SmarterMail messages, contacts, calendars and tasks to third-party email clients that support the protocol, including Microsoft Outlook 2015 for Mac from Office 365, Microsoft Outlook 2011 for Mac, Apple Mail, the Outlook client for iPad and eM Client.
- SyncML is a platform-independent information synchronization standard that syncs SmarterMail contacts, calendars, and tasks with Outlook, Thunderbird, and most smartphones.
- CalDAV is an extension of the WebDAV protocol that syncs SmarterMail calendars with Macs, iPads, iPhones, and other devices/applications that use the technology.
- CardDAV is an extension of the WebDAV protocol that syncs SmarterMail contacts with Macs, iPads, iPhones, Thunderbird and other devices/applications that use the technology.
- The Add to Outlook feature within the SmarterMail webmail interface uses two-way synchronization technology to sync SmarterMail calendars, contacts, and tasks with Outlook 2007 or higher and provides read-only capability for Outlook 2003.

For more information regarding the different synchronization methods available for SmarterMail and/or your device, please refer to [Synchronizing with SmarterMail](#).

To view a list of devices synced with SmarterMail, click the settings icon . Then expand the My Settings folder in the navigation pane and click Synchronized Devices . A list of all previous sync connections will load in the content pane and the following columns will be available:

- Name - The identifier for the device or protocol connecting to SmarterMail. Note: Users may not be able to edit the name of some devices.
- Type - The synchronization protocol used to connect with SmarterMail. Examples include Exchange ActiveSync, Exchange Web Services, SyncML and Add To Outlook. Some protocol types may match the Name.
- Last Sync - The date the device or protocol last connected to SmarterMail.

In general the following options are available from the content pane toolbar:

- Edit - Edits the device connection information. Note: Some devices, such as CardDav or CalDav, cannot be edited.
- Delete - Deletes the selected sync connection(s). Note: In general, users should not delete a sync connection, as this may cause the device to stop functioning with SmarterMail. Deleting a connection is only recommended if you are experiencing issues and want to completely re-configure the device's connection to SmarterMail.

Remote Wipe

Remote wipe is a feature that allows users to reset a device synced using Microsoft Exchange ActiveSync back to its original factory settings, quickly and easily, right from the webmail interface. This is especially handy for devices that are lost or stolen as it can prevent personal information that is stored on the device from falling into the wrong hands. The best thing is that any information stored in SmarterMail, including any notes, tasks, emails, contacts, calendar items, etc., will still be available when a new device, or even a recovered device, is re-synced with the account.

Calendar Settings

SmarterMail gives you several customized settings for how you want your calendars to appear. This includes the default timeframe to display, the location you want to use for displaying weather forecasts, the calendar auto clean rules, how many calendars to configure and more.

To view your calendar settings, click the Settings icon . Then expand the My Settings folder and click Calendar Settings in the navigation pane. The calendar settings will load in the content pane and the following tabs will be available:

Options

Use this tab to specify the following settings:

- Default Calendar View - To specify the default calendar view (daily, weekly, monthly, or all appointments), select the appropriate option from the list.
- Calendar Auto Clean - SmarterMail allows you to keep past calendar events from cluttering up your calendar views. Generally domain administrators will set this option for all users of the domain. However, if you have the ability to set your own auto-clean parameters, you can do so with this setting.
- Display weekends in the weekly view - Select this option to set the weekly calendar view to include the weekends. As some people only use their calendars for the "business week," disabling weekends can further keep the calendar clean and organized.
- Display weekends in the monthly view - Select this option to set the monthly calendar view to include the weekends. As some people only use their calendars for the "business week," disabling weekends can further keep the calendar clean and organized.
- Display task start times in the calendar view - Select this option to view the date and time a task is scheduled to start on the calendar.
- Display task due times in the calendar view - Select this option to view the date and time a task is scheduled to be completed on the calendar.
- Hide completed tasks - Select this option to remove completed tasks from the calendar view.

- Add invites as tentative appointments - Select this option to utilize tentative calendar appointments. When a meeting invitation is sent, a tentative appointment will be automatically added to the calendar. The appointment can then either be accepted or declined from the email request or directly within the calendar interface. If a meeting or event is tentative, the reminder will still be sent if one was added to the invite. Note: This setting is enabled by default.
- Zip Code - U.S. users can view the 7-day weather forecast in their area, or any area they choose, on their calendar. To enable this option, enter your postal code in the field and select the Enable weather checkbox. Weather forecasts are provided by the National Weather Service.

Note: Even though tasks may be set to display in your calendar, if you are syncing your calendar with a desktop and/or mobile email client the task will not show up on your calendar. Instead, they will generally be considered notifications and will display in mobile and/or desktop clients accordingly.

Visible Hours

SmarterMail users can use this tab to customize their calendar to display their typical hours. For example, if you typically schedule appointments from 8 a.m. to 5 p.m., you can configure the visible hours to correspond with those times. Users can also configure the visible hours for each day of the week to allow for flexibility in your schedule.

Calendars

Use this tab to modify the resources that can be displayed in your calendar. Users can add multiple personal calendars and adjust the color and name associated with each resource. By default, a user's personal calendar and tasks will be listed, as well as any domain resources, such as calendars or conference rooms.

In general, the following columns will be available:

- Checkbox - Use these boxes to select multiple resources.
- Display Name - The friendly name of the resource.
- Type - The type of resource shown: Calendar, Task or Room.
- Owner - This column specifies who the resource belongs to. Shared resources will display the username of whoever shared the resources, while domain shared resources display the domain name.
- Access - The level of access you have for the resource: Availability-Only, Read-Only or Full Control.
- Color - The color of the resource.

To add a new personal calendar, click Add in the content pane toolbar. To edit an existing resource, click Edit . The following options will be available:

- Resource Type - The type of resource: Calendar, Task or Room.
- Display Name - The friendly name of the resource.
- Color - The color of the resource. Enter the hex color code or choose an option from the color picker.
- Default - Select this checkbox to choose the default calendar selected for new appointments.

Filtering

Folder Auto-clean

Setting up auto-clean rules for your email folders is a simple, yet effective, way to limit how much of your account disk space is used by the Junk E-Mail, Sent Items, Deleted Items and/or any custom folders you created. By placing limits on the size of these folders, or by automatically deleting mail older than X number of days, you can help ensure that your email account does not fill up unnecessarily. In addition, if you want to set a size limit on a folder, messages are deleted in the order that they were received so that older messages get deleted first.

To access the folder auto-clean settings, click the settings icon . Then expand the My Settings and Filtering folders and click Folder Auto-Clean in the navigation pane. Note: Depending on the policies your administrator has established, you may or may not be able to change the settings on this page.

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

Options

Use this tab to specify the following options:

- Use default auto-clean settings - Select this checkbox to adopt the auto-clean policy set by your email host or domain administrator. Note: If the administrator changes the policy, yours will automatically change as well.
- Override auto-clean settings for this account - Select this checkbox to override the settings set by your administrator so that you can create your own rules. Any changes you make will not be affected if the administrator changes their policy, unless they disable your ability to create your own rules.

Rules

If you are using the default auto-clean settings set up by your administrator, this tab will be greyed out and you will not be able to click on it to open it. If you chose to override the settings, and if your administrator allows you to override the default settings, this tab will be active. In addition, if there are custom rules already created, a number will appear next to the Rules name on the tab showing how

many rules there are. Once you open it and you can click Add Rule in the content pane toolbar to create your own auto-clean policies based upon size or date.

Auto-clean by Size

These options will be visible if you set up the rule by folder Size :

- Folder - This dropdown will show you all folders for your mail account.
- Type - This allows you to create rules based on folder Size or by Date.
- Start Auto-Clean - The size the folder needs to reach BEFORE the auto-clean rule will run.
- End Auto-Clean - The size the folder will be reduced to once the auto-clean rule finishes.
- Enable auto-clean for this folder - Select this box to activate auto-cleaning of the selected folder.

Once the rule is saved, it will display on the Rules tab as follows:

- Folder - The folder the rule was created for.
- Type - The rule type, either Size or Date.
- Settings - A description of the rule. For example, if you set a Size rule to start when a folder is 10MB and to reduce the folder to 5MB, the Settings will show as "Over 10MB, reduce to 5MB"

Auto-clean by Date

These options will be visible if you set up the rule by Date :

- Folder - This dropdown will show you all folders for your mail account.
- Type - This allows you to create rules based on folder Size or by Date.
- Mail Age - This allows you have mail that is over a certain number of days old automatically deleted from the folder.
- Enable auto-clean for this folder - Select this box to activate auto-cleaning of the selected folder.

Once the rule is saved, it will display on the Rules tab as follows:

- Folder - The folder the rule was created for.
- Type - The rule type, either Size or Date.
- Settings - A description of the rule. For example, if you set a Date rule to run on mail that is over 120 days old, the Settings will show as "Over 120 days old"

Content Filtering

Content filtering is a great way to perform actions on emails that meet specific criteria. For example, you can use content filters to delete messages with certain attachments (e.g., attachments with a .exe

extension), forward messages from a specific email address to another account, or even alter the subject of specific types of email. Content filters are most commonly used to organize email by moving messages to specific folders. However, content filtering is extremely flexible and allows you to filter messages the way you want to.

To access your content filtering settings, click the settings icon . Then expand the My Settings and Filtering folders and click Content Filtering in the navigation pane. Note: If you have blocked any senders in your Inbox, there may be a content rule that was automatically created as a result of that action.

To add a new filter, click New in the content pane toolbar. The content filter wizard will load in the content pane.

To edit an existing filter, select the desired filter and click Edit in the content pane toolbar.

Note: Content filters are executed in the order in which they appear in the list . Therefore, when a content filter gets triggered and performs an action on a message, no other content filtering is performed on that message. To change the order, click on the arrows next to a filter.

Content Filter Wizard

The New Content Filter wizard is three pages long, and the wizard will walk you through each step necessary to create the filter. You can go back and forward within the wizard, and a rule will only be created when you actually Save it.

Step 1 - Filter Criteria

In this step of the wizard, choose the type of things that the filter will look at. Possible filter criteria types are listed at the end of this help topic. Multiple criteria can be chosen, and you can choose in the next step whether all criteria must be met, or only one of the criteria for the filter to activate. Note: If you select a filter or action that requires an value to be entered and the field is left blank, SmarterMail will ignore this rule.

Step 2 - Filter Type and Criteria Details

Choose whether this filter uses the "And" modifier, meaning it requires all criterion to be met from each and every section, or the "Or" modifier, meaning just one or more of the criteria in any section needs to be met, before an action is performed. Then choose whether you will be using any wildcards in your search strings. Usually, wildcards will not be necessary, but there are times when some people may want them.

For each of the criteria you chose in step 1, you will be able to enter details. Many types of content filters allow lists of items to be entered in, and these will be indicated. For example, if you chose to

filter on From Address, you can enter multiple email addresses in the box (one per line) and if a message is from any of them, that criteria will be met.

You also have the ability to reverse the logic of a specific criteria item by changing the "matches" box to "does not match" or the yesbox to no.

Step 3 - Rule and Actions

A summary of your content filter rule will appear near the top of the page. Check that it is filtering the way you intend, and enter a name for the rule so that you can easily identify it later.

Then, choose one or more actions to take when a message matches this filter. The available actions are explained below:

- Mark as read - Automatically marks the messages a read, which means it will not show up in your inbox, or any other folder, as unread.
- Mark as follow-up - Automatically flags the message for follow-up. This makes it easy to find messages that have been acted upon by your content filter.
- Delete message - Deletes the message so that it will never arrive at your Inbox. Note:
Messages deleted through content filtering are not recoverable.
- Bounce message - Sends a message back to the sender of the email saying that the message was bounced. Note that the message is still delivered to you unless you choose to delete it as well. Note: If the system administrator has disabled bouncing, this option will function the same as the delete action.
- Move message - Delivers the incoming message to the folder you choose from the drop-down list. If you later delete that folder and leave the content filter active, the filter will automatically create the folder when the action is triggered.
- Prefix subject - Will append a prefix to the subject line of the email. This is useful for categorizing emails as the subject line will be altered to include the text you specify in the Comment box.
- Add Header - Includes an email header into the message, which can be useful when performing additional filtering through Outlook or another email clients. Headers should be formatted like "X-someheadername: value"
- Copy message - Forwards a copy of the message to another email address and leaves a copy of the message in your account as well.
- Reroute message to another email address - Forwards the message to another email address. Unlike "Copy message", this option will not store a copy of the email in your own account.
- Set Priority - Will automatically elevate the priority of a message. For example, if you create a content filter that flags a message from a VIP, you may want to set the priority of the message to High as well to denote its importance.

Once the content filter is created, click Save to actually make the filter active. You can move back and forth throughout the wizard as well in order to check, and double check, your settings.

Content Filter Types

From Address

- From specific addresses
- From specific domains
- From trusted senders

Contains Specific Words or Phrases

- Subject
- Body
- Subject or Body
- From Address
- To Address
- Email header
- Anywhere in message

To Address

- To specific addresses
- To specific domains
- Only to me
- My address in to field
- My address not in to field
- My address in to or cc field

Attachments

- Has any attachment
- Specific filenames
- Specific extensions
- Over specific size

Other

- Message over size
- Message under size
- Received in date range

- Sent through a specific server (by IP address)
- Spam probability
- Flagged as high priority
- Flagged as normal priority
- Flagged as low priority
- Message automated (no return address)
- Sender authenticated

Spam Filtering

SmarterMail includes many antispam measures that will help keep your inbox free of unwanted mail. In most cases, your system administrator, or even your domain administrator, already has some basic spam filtering options set up. However, you can certainly modify those settings to further filter out potentially unwanted email.

To view your spam filtering settings, click the settings icon . Then expand the My Settings and Filtering folders and click and click Spam Filtering in the navigation pane. The spam filtering settings will load in the content pane and the following tabs will be available:

Options

Use this tab to specify the following settings:

- Use default spam settings - Select this checkbox to accept the default spam options provided by your domain administrator.
- Override spam settings for this account - Select this checkbox to customize the way spam is handled and to override the settings created by the domain administrator.

Actions

When you override the spam options set by your system administrator, you can choose the actions that are taken when email comes in that has a low, medium, or high probability of being spam. For each spam level, choose the action you wish to have taken. If you choose to add text to the subject line of messages, type the text in the box below the action drop down. Note: If you are using the default spam options that were set up by your administrator, these settings cannot be edited.

Current Weights

Each type of spam check has an associated weight that factors into the spam probability of a message. When an email comes in, all of the checks listed are run, and for each check that the message fails, the weight is added to the overall score of the email. The thresholds for each spam probability are examined, and the email is placed into the appropriate category.

Sharing

Shared Resources

This feature is only available in SmarterMail Enterprise.

SmarterMail Enterprise allows users to share email folders and collaboration items with other users on the domain. If a user shares any of the following items, they are called shared resources:

- Contacts
- Calendars
- Tasks
- Notes
- Email folders

To see a list of items you are sharing with others, click the settings icon . Then expand the My Settings and Sharing folders and click Shared Resources in the navigation pane. A list of shared resources will load in the content pane.

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

- New - Creates a new shared resource.
- Edit - Edits an existing shared resource.
- Delete - Permanently deletes the ability to share the selected item(s).

When a Shared Resource is set up, they are listed on the Shared Resources page. Each resource is listed by name, by type (e.g., Notes) and by the number of shares/permissions that were set up for the resource.

Adding a Shared Resource

Adding a Shared Resource is quite easy. Simply follow the steps below:

- Click on the New button
- You're presented with the options available to be shared. Select the resource you want to make available to others.
- Click Next
- You have the ability to share items with individuals or groups. You can select multiple individuals by holding down the Ctrl button (in Windows) or the Command button (in OSX).
- You can also set the permissions level on the Users or Groups you share items with. These permissions include the following. Note: Permission options are dependent upon the resource you are sharing.

- None
- Availability-only: For calendar resources, this allows users to only see the availability of others when setting up Events.
- Read only: Allows users to only see the shared data but not have any ability to edit it.
- Full control: Allows users to fully edit the shared resource.
- Click the Save button. Your Shared Resource now shows on the Shared Resources page.

Individual Permissions on Shared Resources

If you create a shared resource and then share that resource with a number of individuals -- say, the members of a team -- you can set special permissions for each user you share the resource with. For example, you have a group of people working on a specific task, you can give a team lead full control over the task and give the rest of the team read only permissions. This allows the entire team to share the task and any notes, changes, etc. made to it but it limits editability to only the team lead.

Mapped Resources

This feature is only available in SmarterMail Enterprise.

When you share a resource with someone else, it's called a Shared Resource . When someone shares a resource with you, SmarterMail considers that a Mapped Resource. Note: Conference Room resources shared with Everyone on a domain will not appear on an individual's Mapped Resources page. They only appear when creating a new event in the webmail interface. In general, the following can be shared with you by any individual:

- Email folders
- Contacts
- Calendars
- Tasks
- Notes

To see a list of items other users are sharing with you, click the settings icon . Then expand the My Settings and Sharing folders and click Mapped Resources in the navigation pane. A list of mapped resources will load in the content pane.

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

- Attach - Attaches the selected mapped resource(s) to your account so they are accessible. For example, if you attach a co-worker's calendar to your account, you can access this mapped resource from the contacts area of the webmail interface by clicking the contacts selector and choosing the appropriate option.

- Detach - Edits an existing mapped resource.
- Edit - Permanently removes the selected item(s) from the mapped resources list.

Attaching to Mapped Resources

When you go to your Mapped Resources page you will see a list of items others are sharing with you and the status of the share. Any item marked "Detached" will need to be attached to you before you can access it. In general, each item is listed by the Username of the person sharing the resource with you, the resource type, the name of the resource, the Friendly Name, the permission level granted to you and the status. To attach a resource, do the following:

- Select the resource you want to attach to your account by checking the box next to it.
- Once selected, click the Attach button.
- Once the item is attached, you'll see a screen listing the details of the resource. If you like, you can edit the Friendly Name of the resource to something more descriptive or to anything of your choosing. Note: This does not change the name of the resource for anyone but yourself.
- Click the Save button to finalize attaching the resource.

If you no longer need access to a shared resource, simply check the box next to the item and click the Detach button. Note: This does not delete the resource from your list. The resource will still show up in your list of Mapped Resources until the original user deletes it.

Advanced Settings

Auto-complete

Because most users generally send email to the same people or addresses, SmarterMail automatically pulls email addresses from your Sent Items folder, your contacts, the Global Address List (GAL), aliases and mailing lists and saves them all separately to an auto-complete list. This list is different than your Contacts list as it covers accounts you may not have actual contacts set up for. These auto-saved email addresses are then used to auto-complete the To, Cc and Bcc fields when applicable.

To view the list of email addresses used for the auto-complete feature, click the settings icon . Then expand the My Settings and Advanced Settings folders and click Auto-complete in the navigation pane. A list of email addresses will load in the content pane.

Editing the Auto-complete List

When you bring up the auto-complete list, you will see all of the addresses saved listed by Email Address, Display Name and Source. The source listed will be either one of the following:

- Sent items
- Contacts
- Global Address List
- Alias
- Contacts

You can only delete addresses that were pulled from your Sent Items folder. To do this, simply select the addresses and click Delete in the content pane toolbar. To delete other items you will need to do so from their respective locations within SmarterMail. That is, from your contacts, by deleting aliases, etc.

Calendar Settings

SmarterMail gives you several customized settings for how you want your calendars to appear. This includes the default timeframe to display, the location you want to use for displaying weather forecasts, the calendar auto clean rules, how many calendars to configure and more.

To view your calendar settings, click the Settings icon . Then expand the My Settings folder and click Calendar Settings in the navigation pane. The calendar settings will load in the content pane and the following tabs will be available:

Options

Use this tab to specify the following settings:

- Default Calendar View - To specify the default calendar view (daily, weekly, monthly, or all appointments), select the appropriate option from the list.
- Calendar Auto Clean - SmarterMail allows you to keep past calendar events from cluttering up your calendar views. Generally domain administrators will set this option for all users of the domain. However, if you have the ability to set your own auto-clean parameters, you can do so with this setting.
- Display weekends in the weekly view - Select this option to set the weekly calendar view to include the weekends. As some people only use their calendars for the "business week," disabling weekends can further keep the calendar clean and organized.
- Display weekends in the monthly view - Select this option to set the monthly calendar view to include the weekends. As some people only use their calendars for the "business week," disabling weekends can further keep the calendar clean and organized.
- Display task start times in the calendar view - Select this option to view the date and time a task is scheduled to start on the calendar.
- Display task due times in the calendar view - Select this option to view the date and time a

task is scheduled to be completed on the calendar.

- Hide completed tasks - Select this option to remove completed tasks from the calendar view.
- Add invites as tentative appointments - Select this option to utilize tentative calendar appointments. When a meeting invitation is sent, a tentative appointment will be automatically added to the calendar. The appointment can then either be accepted or declined from the email request or directly within the calendar interface. If a meeting or event is tentative, the reminder will still be sent if one was added to the invite. Note: This setting is enabled by default.
- Zip Code - U.S. users can view the 7-day weather forecast in their area, or any area they choose, on their calendar. To enable this option, enter your postal code in the field and select the Enable weather checkbox. Weather forecasts are provided by the National Weather Service.

Note: Even though tasks may be set to display in your calendar, if you are syncing your calendar with a desktop and/or mobile email client the task will not show up on your calendar. Instead, they will generally be considered notifications and will display in mobile and/or desktop clients accordingly.

Visible Hours

SmarterMail users can use this tab to customize their calendar to display their typical hours. For example, if you typically schedule appointments from 8 a.m. to 5 p.m., you can configure the visible hours to correspond with those times. Users can also configure the visible hours for each day of the week to allow for flexibility in your schedule.

Calendars

Use this tab to modify the resources that can be displayed in your calendar. Users can add multiple personal calendars and adjust the color and name associated with each resource. By default, a user's personal calendar and tasks will be listed, as well as any domain resources, such as calendars or conference rooms.

In general, the following columns will be available:

- Checkbox - Use these boxes to select multiple resources.
- Display Name - The friendly name of the resource.
- Type - The type of resource shown: Calendar, Task or Room.
- Owner - This column specifies who the resource belongs to. Shared resources will display the username of whoever shared the resources, while domain shared resources display the domain name.
- Access - The level of access you have for the resource: Availability-Only, Read-Only or Full Control.
- Color - The color of the resource.

To add a new personal calendar, click Add in the content pane toolbar. To edit an existing resource, click Edit . The following options will be available:

- Resource Type - The type of resource: Calendar, Task or Room.
- Display Name - The friendly name of the resource.
- Color - The color of the resource. Enter the hex color code or choose an option from the color picker.
- Default - Select this checkbox to choose the default calendar selected for new appointments.

Mailbox Migration

The mailbox migration tool makes switching email providers easy by importing email, contacts, calendars, tasks, and notes to SmarterMail from most third-party mail servers.

To access the mailbox migration tool, click the settings icon . Then expand the My Settings and Advanced Settings folders and click Mailbox Migration . The mailbox migration tool will open in a new window.

Follow the on-screen instructions to import email and collaboration data from a third-party mail server to your SmarterMail mailbox. Depending on the mail server you are migrating from, you may be asked to provide the mailbox protocol (POP, IMAP), the server address, port, username and password. Note: It may take some time for your mailbox data to import. You can continue using SmarterMail during this time as the migration process happens in the background. In addition, the type of items available for migration are purely dependent upon the service you're migrating from. SmarterMail can not migrate any item that is not allowed by the service provider.

A Note for Office 365 Users - Migrating from Office 365 is easy. However, there are a few things that aren't as clear-cut as moving from an Exchange server. Below is a step-by-step for anyone migrating from Office 365 to SmarterMail:

- When asked for the mailbox protocol, select "Exchange 2007 SP1 or Later".
- On the Account Settings portion of the migration you will need to log in to your Office 365 account and to get the Server Address for your Office 365 account. To do this, simply log in to your account and get it from the log in URL. For example, if your log in URL is something like <https://ch1prd0412.outlook.com/owa>, you will want to use "ch1prd-412.outlook.com" as the Server Address you're migrating from.
- Use the full email address you use to log in to Office 365 as your Username . For example, JDoe@example.com.
- Use your domain name as the Domain for the migration. For example, if you log in with JDoe@example.com you'll just need to use example.com for the domain.

- You will need to check the Requires SSL checkbox.
- From there, the rest is easy. Just finish up the migration wizard and your Office 365 information will now be in SmarterMail.

Message Retrieval

These days it's rare for someone to have, and use, a single email address. That's why SmarterMail's Message Retrieval feature is so great: it allows users to access email from another account simply using the SmarterMail Web interface. That means users can add their Gmail, Hotmail, Yahoo! or any other mail account to SmarterMail so that they can receive all of their emails, from a number of different accounts, from within a single interface. A nice complement to Message Retrieval is SMTP Accounts , which allows users to send email from additional accounts as well. Note: This feature is only available to users if their system administrator has enabled message retrieval.

To view your message retrieval settings, click the settings icon . Then expand the My Settings and Advanced Settings folders and click Message Retrieval in the navigation pane.

Adding a New Account Adding an account to message retrieval is quite simple. You will, however, need to fill in several pieces of information in order for SmarterMail to actually connect to the account and start retrieving messages. If you do not know any of these settings, it's a good idea to contact your IT or Email Administrator with the list, below, that corresponds to the type of connection you want to make with the account, either POP or IMAP.

POP Retrieval

SmarterMail's POP retrieval service will download email messages from another server via POP3 and deliver them to your SmarterMail mailbox. The primary difference between POP and IMAP is that a POP account will generally retrieve messages from the server, then delete them from the originating server. While SmarterMail's Message Retrieval feature DOES allow you to leave messages on the server, users need to make sure they enable it. Otherwise, POP retrieval will delete the messages.

When creating a new account for POP message retrieval, the following options are available:

- Type - Select either POP or IMAP.
- Server Address - The address for the email server for which you want to connect. This will most likely be the URL to the mail server. (E.g., mail.example.com).
- Port - The port used to connect to the email server. By default, the port is 110. However, some mail providers may require a separate port be used for POP retrieval.
- Username - The identifier used to authenticate with the email server. This will most likely be the full email address you want to bring into SmarterMail.

- Password - The password used to log into the mail account.
 - Retrieval Method - The method by which SmarterMail checks for new messages on the server, either Manual or Automatic. If you choose to manually retrieve messages, you will have to load the Message Retrieval page and click Retrieve to check for new messages. Automatic retrieval can be modified by the system administrator, but is set to 10 minutes by default. Automatic retrieval does not require you to return to the Message Retrieval page.
 - Destination Folder - The folder you want to use for messages that are downloaded from the server.
 - Enable APOP authentication - Select this option if the server requires additional login security.
-
- Leave messages on server - Select this option to keep your messages on the server after they are downloaded to your SmarterMail mailbox.
 - Requires SSL - Select this option if the connection to the server must be SSL.
 - Enable spam filtering - Select this option to apply your SmarterMail spam and content filtering settings to any messages downloaded from this server

IMAP Retrieval

SmarterMail's IMAP retrieval service will download email messages from another server via IMAP and deliver them to your SmarterMail mailbox while leaving the original messages on the original mail server. When creating a new account for IMAP message retrieval, the following options are available:

- Type - Select either POP or IMAP.
- Server Address - The address for the email server you want to connect to. This will most likely be the URL to the mail server. (E.g., mail.example.com).
- Port - The port used to connect to the email server. By default, the port is 143. However, some mail providers may require a separate port be used for IMAP retrieval.
- Username - The identifier used to authenticate with the email server. This will most likely be the full email address you want to bring into SmarterMail.
- Password - The password used to log into the mail account.
- Retrieval Method - The method by which SmarterMail checks for new messages on the server, either Manual or Automatic. If you choose to manually retrieve messages, you will have to load the Message Retrieval page and click Retrieve to check for new messages. Automatic retrieval can be modified by the system administrator, but is set to 10 minutes by default. Automatic retrieval does not require you to return to the Message Retrieval page.
- Folder Transfer Method - The method by which SmarterMail imports any email folders from the server. Unlike a POP connection, IMAP allows existing folders to be brought into SmarterMail. This is a benefit of using IMAP as your connection type.
- Requires SSL - Select this option if the connection to the server must be SSL.

Notification Profiles

Users of SmarterMail can create Events that allow them to select criteria and apply specific actions when the criteria are met. One of the actions is to receive email notifications when an event is triggered. For example, users can receive notifications when a task is due or system administrators can receive notifications when the disk space for a domain reaches a certain percentage. Notification profiles determine how those messages are sent.

To view a list of current notification profiles, click the settings icon . Then expand the My Settings and Advanced Settings folders and click Notification Profiles . Your notification profiles will load in the content pane.

The following columns are available:

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

The following options are available from the content pane toolbar:

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

To view a specific notification profile, simply double-click the appropriate profile. Alternatively, you can select the profile and click on the Edit button. Regardless of how you open the profile, it will load as a modal window in the content pane.

Creating a Notification Profile

Creating a notification profile is very simple. Just click on the New button, and a new modal window will open with the following options:

- Notification Profile Name - The name you set for the profile.
- Email Address(es) - The email address(es) to which notifications are sent. More than one email address can be added to this field, they just need to be separated with a comma.
- Enable - Checking this box will enable email notifications.
- SMS Email Address(es) - Sometimes users will want notifications sent to their mobile devices via text message. Here you'll input the mobile device email address to which notifications are sent. If you're unsure of this address, contact your mobile provider.
- Enable - Checking this box will enable SMS notifications.

- Enable Reminders - Checking this box will display reminders for tasks and appointments in a popup window in webmail.

Use of Notification Profiles

As mentioned, notification profiles are primarily used in conjunction with Events. When a new event is created, users have the ability to select a notification profile to use when that event fires. If more than one notification profile is available, each will be listed and users will need to make sure they've selected the proper profile to use with that event.

SMTP Accounts

Setting up an SMTP Account allows you to send email from a third-party mail server account right from within SmarterMail. Generally, you would also want to set up the corresponding Message Retrieval information. For example, imagine you have SmarterMail, Gmail, and Yahoo! email addresses. To view, reply and send out new messages from the Gmail and Yahoo accounts through SmarterMail's web interface you could do the following:

- Add a Message Retrieval item for the Yahoo and Gmail accounts to POP all messages to a Yahoo and Gmail folder within SmarterMail. Set the Retrieval Method to Automatic.
- Add an SMTP Account specifying the information needed to send messages through the Yahoo and Gmail SMTP servers. Using these two features in conjunction means you have a single webmail interface to use for virtually any email account you have across the Internet. As most people have, and use, more than one email address, being able to combine all accounts into one interface means you have access to all of your email in a single spot.

To view your message retrieval settings, click the settings icon . Then expand the My Settings and Advanced Settings folders and click SMTP Accounts in the navigation pane.

When creating a new SMTP account, the following options are available:

- Server Address - The address for the external email server for which you want to connect. This usually takes the form of mail.example.com.
- Port - The port used to connect to the email server. By default, the port is 25. However, some ISPs block port 25 by default. Therefore, it's a good idea to check with your email provider or email administrator to ensure that you're using the proper port for this account.
- Display Name - The name that you want to appear in the From field of emails sent using this account.
- Email Address - The email address that corresponds to the external email server. For example, jdoe@example.com.
- Username - The identifier used to authenticate with the external email server. In many cases,

this and the Email Address will need to be identical.

- Password - The password used to authenticate with the external email server.
- Encryption - The type of encryption required by the external email server. Many ISPs and service providers require you use SSL to send emails.
- Enable Authentication - Select this option if SMTP authentication is required to send mail from this email address. What that means is that, once you attempt to send a message using this account, SmarterMail will pass your credentials back to the sending server to authenticate your address and let the sending mail server know that you're authorized to send mail from that account.

Domain Settings

General Settings

This settings page is only available to domain administrators.

Domain administrators will use this section to adjust any general domain settings. To access this section, click the Settings icon . Then expand the Domain Settings folder and click General Settings in the navigation pane. The general settings will load in the content pane and the following tabs will be available:

Logout URL

By default, when users log out of SmarterMail, they're taken back to the standard log in screen. However, if the system administrator allows it, domain administrators can set a special page to load when users log out of webmail. This page be any page the domain administrator desires. For example, perhaps company management wants users redirected to an Intranet page, or some other company-specific page, to appear when users log out. The domain administrator simply clicks the Override System Settings check box and adds in the specific URL in the Logout URL text box, then checks the Enabled box. Now, once a user logs out they are redirected to that page in their browser.

Login Display

Small businesses using SmarterMail on their own servers, or even companies using SmarterMail from their hosting provider, will benefit from the ability to customize the SmarterMail login page to add a company logo, provide additional branding text, or simply adjust the default □Log into SmarterMail□ text to be more in line with an overall brand message. Note: This tab will only be visible if the system administrator has enabled Login Display Customization for the domain. Furthermore, if the system administrator allows a domain to override the custom login display and the domain administrator does

not enable customization for their domain, users will see the default SmarterMail login screen, regardless of whether the system administrator has enabled a custom login display for the system.

Use this tab to adjust the SmarterMail login display settings:

- Custom Help URL - Entering a full URL in this field will add a custom button to the Help menu that users can access in the SmarterMail interface. Administrators can link to a variety of things, including server-specific instructions for syncing, help resources, contact information, etc.
- Enabled - Check this box to enable the custom help URL in the Help menu.
- Custom Help Text - The hyperlink text for the custom URL in the Help menu.
- Custom Login Text - Use this field to adjust the default "Log into SmarterMail" text with something more in line with an overall brand message.
- Enabled - Check this box to enable the Custom Login Text.
- Company Logo - Click on Choose File to upload a company logo. Uploading a logo using this upload control will host the image publicly on the server and enter the tag in the HTML section. Note: Uploading an image here alone will NOT display the image on the login screen. The HTML must be entered in the Login Page HTML section. This upload control can be used by those who don't have their logo publicly hosted or who wish the image source to point back to their mail server. Furthermore, regardless of the image uploaded, the image's source URL will remain the same; only one image may be hosted at a time.
- Enable custom login page HTML - Check this box to enable the ability to use HTML to further modify the login screen to add additional text or adjust the layout. This is used in conjunction with the Login Page HTML section below.
- Login Page HTML - Enter the custom HTML that will be used to further modify the login screen (in-line custom CSS can be used as well). Note: To include white space around the company logo, the div id "companyinfo" must be included. In addition, domain administrators cannot enter scripts as this is considered to be unsafe code. System administrators do not have this limitation.

The following options are available in the content pane toolbar:

- Save - Saves the custom login display settings.
- Preview - Opens a new popup window displaying what the current settings render on the login screen. If this window remains open, live changes can be seen as settings are adjusted.

Sharing

When a user adds a member from the Global Address List as an attendee on a calendar appointment, SmarterMail can alert the user of any potential scheduling conflicts. In addition, the user can view an Availability window to review the times that their attendee is free/busy. The following setting impacts whether the calendar availability of GAL members is shown in the calendar conflicts and availability window:

- Show calendar availability for all users in domain - This setting is enabled by default and will allow users on the domain to review scheduling conflicts and availability for members in the Global Address List. When unchecked, domain users' scheduling information will not be displayed in the appointment window.

Mailing Lists

Mailing Lists are a great way to allow users to communicate with a number of different individuals via a single email address. Unlike an Alias , a mailing list allows people to subscribe to, or unsubscribe from, email communications. In addition, mailing lists can be public or private, be replied to by all users or managed by a single list administrator and more.

Use this tab to specify the following mailing list settings:

- Webmail URL - The URL for the SmarterMail login page. Note: URLs should include the http:// prefix. For example: http://mail.example.com/
- Enable - Select this option to override the server's configured hostname for use in mailing list communications.
- Deletion Bounce Threshold - The number of times a message to a specific subscriber may bounce before the subscriber is automatically removed from the mailing list. For example, if someone mis-types their email address, it is not efficient to continue attempting to send an email to that address. By default, the threshold is set to 5.
- Enable - Select this option to enable the deletion bounce threshold. By default, this setting is enabled.

Global Address List

The Global Address List (GAL) is basically a listing of all users who have accounts for your particular email domain. A GAL is extremely important for companies that have a number of employees as it is a central repository for information about everyone. In addition, it integrates with SmarterMail's Contacts feature and provides a listing of email addresses that users can then use for creating Events, emailing co-workers, sharing calendars and contacts, and much more. From a domain administrator's perspective, the following options are available:

- Enable mailing lists in the Global Address List - Checking this box means that any list that is created will appear as a contact in the Global Address List. In turn, that means anyone with access to the GAL will be able to see and/or possibly send emails to the list.
- Enable aliases in the Global Address List - Checking this box means that any aliases that are created will also appear in the GAL. By default this is checked, but domain administrators may want to exclude aliases from appearing in the GAL as they could be used to send emails to customers or to important contacts, or for a number of other reasons.

Users

This settings page is only available to domain administrators.

An email user account represents a person's actual mailbox and email address. For example, jdoe@example.com. User accounts can receive email, send email, and login to the Webmail interface in addition to using the other features of SmarterMail. This includes things like calendaring, creating and sharing contacts, creating and managing tasks using SmarterMail's live chat and much more.

To view a list of users on a domain, click the Settings icon . Then expand the Domain Settings folder and click Users in the navigation pane. A list of users will load in the content pane.

Adding a new user and editing an existing user are essentially the same process, and they both deal with similar settings. To create a new user, simply click on the New button in the content pane toolbar. To edit a user's settings, select the desired user and click Edit in the content pane toolbar. You can also double-click on a user to open their settings. Regardless of the method used, the user settings will load and the tabs listed below will be available. Note: When editing a user's settings, use the Rename button in the content pane toolbar to change the username.

User

Use this tab to specify the following user-based settings:

- Username - The identifier the user uses to login to SmarterMail. This is the portion of the email address that comes before the domain name. For example, the "jdoe" part of jdoe@example.com.
- Temporary Password - Note: Only System Administrators managing/impersonating the domain will see this option. This option allows System Administrators to create an additional, temporary password in order to troubleshoot account issues. A user's actual password will never be shown in the Web interface. Creating a temporary password, rather than impersonating the account, may be required when it's necessary to log into a user's email or IM client where impersonation is not available. In addition, administrators will find that some behavior in webmail may be slightly different depending if an account is impersonated or logged in

directly. For example, when you impersonate a user, the Domain Admin's settings always show, even if you're impersonating a user that isn't a Domain Admin. For a clear idea of the options available to the user, an administrator may wish to log in directly instead. Clicking Manage will open a modal window where the temporary password can be generated. Only one temporary password may be created at a time, and on creation, will be available for 24 hours. Extend the time remaining or revoke the password by clicking on Manage again in the user settings and choosing the corresponding button. Choosing to extend the password will add 24 more hours to the remaining time. Note: Creating and using a temporary password does not disable the user's standard account password or impact their ability to log in or access webmail.

- Authentication Mode - The authentication method used to login to SmarterMail. By default, SmarterMail will use its included username/password authentication. However, SmarterMail can also be integrated with customers using Microsoft Windows Active Directory for their corporate logins. For information on Active Directory integration, visit the SmarterTools Knowledge Base .
- Domain - The Domain to authenticate against when Active Directory is used for the Authentication Mode. Note: This feature is not displayed if SmarterMail is used as the Authentication Mode .
- Password - The password for the user to login to Smartermail. Note: This feature is not displayed if Active Directory is used as the Authentication Mode.
- Confirm Password - The password confirmation for the user to login to Smartermail. Note: This feature is not displayed if Active Directory is used as the Authentication Mode.
- Display Name - The friendly name that is displayed on outgoing messages.
- Reply-to Email Address - The email address used in the reply-to header of messages sent through webmail. This address will be used by receiving email clients when replying to a message.
- Time Zone - The time zone to use for marking the sending and receiving date and time.
- Backup Email Address - This is a backup email address that can be used for password recovery information should a user forget their mailbox credentials.
- User Status - Domain administrators can change the status on a mailbox to limit a user's access as needed. For example, if a user leaves the company, either voluntarily or not, a domain administrator can suspend the account pending further review by company management. Options include:
 - Enabled - The mailbox is in use by the user.
 - Disabled and allow mail - The mailbox continues to receive email but the user is unable to access their mailbox.
 - Disabled and don't allow mail - The mailbox no longer accepts incoming messages and the user is unable to access their mailbox.

- Mailbox Size Limit - The maximum size of the mailbox. By default, the maximum mailbox size is 100 MBs. However, domain administrators can change this to whatever they like to correspond to company limits. For unlimited disk space, type in 0.
- Calendar Auto-Clean - SmarterMail allows domain administrators to keep users' past calendar events from cluttering up calendar views. By default, this is set to Domain Default which is set in the Default User Settings .
- Enable domain administrator access - Select this option to allow the user to edit domain settings.
- Disable password changes - Select this option to prevent the user from changing the login password. This setting overrides the password expiration found in Security settings. A user's password will not expire or be required to be changed if this setting is enabled.
- Enable ActiveSync - Select this option to add Exchange ActiveSync to a mailbox.
- Show in Global Address List - Select this option to add the user to the Global Address List. Use this option on accounts that are tied to real people as opposed to addresses used by departments, such as support@example.com.
- Enable POP retrieval - Select this option to allow users to download email via POP from other email accounts. For example, if a user has a second email address that they monitor, enabling this option allows the user to set up POP Message Retrieval for that address and download email sent to that address into their SmarterTools mailbox. Note: POP retrieval will take the mail from the original mail server and download it into SmarterMail, thereby deleting the message from the original mailbox.
- Enable IMAP retrieval - Select this option to allow users to download email via IMAP from other email accounts. For example, if a user has a second email address that they monitor, enabling this option allows the user to set up IMAP Message Retrieval for that address and download email sent to that address into their SmarterTools mailbox. Note: IMAP retrieval will take the mail from the original mail server and download it into SmarterMail, but it leaves a copy of the message in the original mailbox.
- Enable SMTP Accounts - Select this option to allow users to send email from a third-party mail server account right from within SmarterMail. For example, if a user has a second email address that they regularly use, enabling this option would allow the user to set up an SMTP Account for that address and choose which account to send from when composing new messages.
- Disable greylisting - Greylisting is an anti-spam measure that rejects the initial incoming message from an unrecognized email address and waits for the sending mail server to attempt to resend the message before it's allowed to be delivered. While effective, this can also lead to a delay in message receipt. Domain administrators can disable greylisting on a user-by-user basis as needed, while allowing it for other mailboxes. Note: This setting will only be visible if

greylisting has been enabled for the server.

- Enable outgoing mail signing - Selecting this option means outgoing messages will be signed via DKIM.

Webmail

Use this tab to specify the following Webmail settings:

- Initial Page on Login - The page users will see upon logging in to SmarterMail. Users can either go directly to their Inbox or go to the My Today Page.
- Display Format - To specify the default format used for displaying messages, select the appropriate option from the list.
 - HTML - This option will display messages and their HTML content, if present in the email. This content can include stylistic elements such as special fonts or colors, as well as hyperlinks, images and other formatting elements.
 - Text - This option will only display text, without any special formatting. While it is less interesting (no fonts, images, etc), it is also much more secure and is faster to view than HTML.
- Sort Messages by - The order in which messages are displayed. By default, messages are displayed by date in descending order.
- Delete Action - To specify the action performed on deleted messages, select the appropriate action from the list.
 - Move to Deleted Items folder - Deleted items will appear in the deleted items folder, which will need to regularly be emptied.
 - Auto Purge Folder - Permanently deletes the message. Note: When deleted messages are purged, the action is final. You will not be able to retrieve these messages later.
 - Mark as deleted - Flags the message for deletion, but it will not be removed until the folder is purged.
 - Mark as deleted and hide - Flags the message for deletion and hides it from view, but it will not be removed until the folder is purged. Note: Be careful to monitor your disk space usage when using this option, as it may fill up with what appears to be a small number of messages.
- Preview Pane - To specify where the preview pane displays in the webmail interface for users, select the appropriate option from the list. By default, the preview pane appears at the bottom of the content pane. Disabling the Preview Pane means only a list of messages appears in the content pane and each message will need to be opened separately in order to view their contents.
- Disable image in preview pane - Select this option to prevent images from appearing when users view messages in the preview pane. You may want to select this to enable messages to

load faster. Note: By selecting this option, images will still appear when a messages is opened outside of the Preview Pane.

- Enable reminder popup window - Selecting this option means that any reminders will display in popup windows. If a user's browser has a popup blocker, the email server URL may need to be added to allow reminder popups to display. This is enabled by default.
- Enable sounds - Select this option to enable sounds in webmail, such as when a new chat message is received.
- Enable new message notifications - Select this option to display a temporary notification in the webmail interface when a new email message is received. This notification will display no matter which section of the interface is selected and generally appears in the lower part of your screen.
- Disable reminders for appointments and tasks - Select this option to disable all reminders for appointments and tasks for users.
- Mark messages downloaded by POP3 as read - Select this option to mark messages as read on the server when downloaded in the client by POP3.
- Mark messages sent to junk as read - Select this option to mark messages as read on the server when marked as spam.
- Show HTML hyperlinks when printing - Select this option to add link URLs in parenthesis to the right of the hyperlinks when printing email messages.

Compose

Use this tab to specify the following settings for the Compose window that opens when a users begin writing emails:

- Text Encoding - To specify the character set used in messages composed through the Web interface, select the appropriate option from the list. By default, SmarterMails sets the encoding to Western European (ISO). However, SmarterMail supports encoding for over 35 different text formats, thereby supporting message encoding for most parts of the world.
- Compose Font - To specify the default font and font size for emails, select the appropriate option from the list.
- Spell Check Dictionary - To specify the default dictionary to use for spell-checking emails, select the appropriate option from the list. SmarterMail offers dictionaries for over 17 different languages. If the user is unsure, they can select the option to use the same spell check dictionary that matches the language they selected when they logged in to SmarterMail.
- Forwarding Method - To specify the method by which messages are forwarded, select the appropriate option from the list.

- Normal - Includes original content, including font styles from original message, as part of the new message.
- Text - Inserts the plain text version of the original message into the new message. This is useful if you want to exclude links, fonts or other formatting.
- Embed as Attachment - Attaches the original message to the new message as an attachment. The message will not appear in the body of your message.
- Auto Save Frequency - To specify how frequently SmarterMail saves a draft of a message a user is writing, select the appropriate option from the list. The default setting is 2 minutes.
- Reply Header Type - To specify the header type, select the appropriate option from the list. Note: For most users, basic headers will be sufficient. Basic headers include From, To, and Subject headings whereas the full header includes MIME type filter restrictions, etc.
- Compose Format - To specify whether new messages are composed in HTML or plain text, select the appropriate option from the list.
- Reply Text Indicator - This sets the character that is appended to the beginning of each line of an original message when that message is replied to.
- Include previous replies in reply - Select this option to embed the text of the original message in a message reply. This includes text from messages in reply threads.
- Enable sent items folder - Select this option to save all outgoing messages in the Sent Items folder. Note: If you send many messages, you may need to delete items from this folder regularly.
- Enable read receipts by default - Select this option to create read receipts for all outgoing messages. Domain administrators should be careful when enabling this and only do so if required for business or compliance or regulatory requirements.
- Enable trusted sender for webmail recipients - Select this option to add the email addresses that users send mail to through webmail to their trusted senders list. This means that any email from these addresses is automatically trusted by SmarterMail and will avoid any spam filters.
- Disable X-Originating_IP header in messages - Select this option to remove the user's IP address from the X-Originating_IP header when sending messages via webmail. Some people prefer that their IP address isn't included in the header of emails that are sent out as they feel it is a potential security risk.
- Warn about common email mistakes prior to sending - Enabling this means that SmarterMail will quickly review any message sent to check for items like missing attachments. This includes times when the word "attachment" is used in the body or subject of the message, but an attachment is not being sent with the email message.
- Automatically check spelling prior to sending - Enabling this means SmarterMail will quickly review any message sent to check for spelling and grammar issues when sending via webmail.

Forwarding Use this tab to set up SmarterMail to forward received messages to another email account. This is a way to send copies of emails to an outside entity, or to a separate email address the user prefers to check.

- Forwarding Address - The email address(es) to which messages will be forwarded. Separate multiple email addresses with a semi-colon or comma.
- Delete messages when forwarded - Select this option to automatically delete messages from the user's SmarterMail inbox after those messages are forwarded.

Groups

This feature is only available in SmarterMail Enterprise edition.

User Groups are used to specify permissions for shared items and for the Global Address List. To specify which groups the user belongs to, select the appropriate groups. Note: Only domain administrators can assign users to groups. If the domain administrator has not defined any groups within the User Groups settings page, no groups will be available.

Throttling

Throttling limits the number of messages sent per hour and/or the amount of bandwidth used per hour to send messages. Domain administrators can use this to ensure users don't send out massive amounts of email through out the day, thereby possibly getting the domain blacklisted. Use this tab to edit the following throttling settings:

- Outgoing Messages per Hour - The number of messages sent by the user per hour. By default, the number of outgoing messages is 1,000.
- Outgoing Bandwidth per Hour - The total number of MBs sent by the user per hour. By default, the outgoing bandwidth is 100MB.
- Throttling Action - When using either message or bandwidth throttling, administrators can select an action for SmarterMail to take once the particular throttling level is reached. Of course, administrators can elect to do nothing at all, or they can either Delay or Reject messages until the amount of mail being sent falls beneath the throttling limit that is set.

Plus Addressing

Plus addressing is a feature of SmarterMail that allows the user to automatically filter incoming email without creating content filtering rules first. Plus addressing also allows users to use special email addresses if they do not want to give out their real email address. For example, if user@example.com needs to provide a valid email address to sign up for a newsletter, he can sign up for the newsletter using the address user+technewsletter@example.com. When the newsletter is delivered, it will automatically be routed to the Technewsletter folder. If the folder does not exist, it will be created

automatically. Note: For plus addressing to work, it is important that the folder name appears AFTER the username, but BEFORE the domain name. So the format should be:

username+foldername@domain .

- Action - The action SmarterMail should take when a plus-addressed email is received.
- Move to folder - If the target folder exists, the incoming message will be placed into it. If the folder does not exist, it will be created. No more than 10 folders can be auto-created in this method during a six hour period to prevent abuse.
- Move to folder (if it exists) - If the target folder exists, the incoming message will be placed into it. Otherwise, the email will get placed in the inbox.
- Leave in Inbox - Drops the message in to your inbox.
- Enable plus addressing - Select this checkbox to enable plus addressing.

Service Access

This tab indicates a user's access to POP, IMAP, SMTP and webmail services. Limiting services such as POP, IMAP and SMTP access means that users are not able to connect their email accounts to external email clients, etc.

- Enable POP access - Select this option to allow the user to download mail using POP3.
- Enable IMAP access - Select this option to allow the user to download mail using IMAP.
- Enable incoming SMTP Access - Select this option to allow users to receive email from external domains.
- Enable outgoing SMTP access - Select this option to allow users to send email to external domains.
- Enable webmail access - Select this option to allow users to login to SmarterMail from the webmail interface.
- Enable XMPP access - Select this option to allow users to set up third-party chat clients like Adium, Pidgin and Windows Live Messenger for use with SmarterMail's live chat features.

Email Aliases

This settings page is only available to domain administrators.

An email alias is essentially a forwarding email address that can be used to forward messages to a single address or multiple email addresses. Aliases are most commonly used for departments or groups of individuals, like a small team of people working on a project or task.

For example, in a working environment with multiple email addresses, the office may want to make a central email address that distributes messages to all personnel. The alias workplace@example.com can be made for messages to be sent and then distributed to all of the employees.

To view a list of email aliases for the domain, click the settings icon . Then expand the Domain Settings folder and click Aliases in the navigation pane. A list of existing aliases will appear in the content pane.

To create a new email alias, click New in the content pane toolbar. To edit an existing email alias, select it and then click Edit in the content pane toolbar. Whether creating a new alias or editing an existing one, the settings for these will appear in a modal pop-up and the following options will be available:

- Alias Name - The name of the alias. This name will be used to create the email alias address. For example, if you named the alias "info" and the domain was "example.com," the email alias address would be info@example.com.
- Email Address (one per line) - Type the full email address(es) of the user(s) who should receive the messages sent to this alias.
- Include all domain users - Select this option to include all domain users automatically in the alias. Note: This option does not override the email addresses listed in the Email Address box. If selected, all domain users will be included in addition to the users entered in the Email Address box.
- Enable in Live Chat (XMPP) - Select this to allow the alias to appear as a contact in live chat. Enabling aliases for live chat means that instant messages can be sent to the alias from within webmail as well as when using third-party chat clients.
- Show in Global Address List - Select this to display the alias in the Global Address List.
- Internal only - Select this option to only allow emails to be received from addresses within the alias domain.

Note: Even though an alias acts as an email address, users cannot login to an alias like they do a standard email address since no email is ever actually stored for the alias. Emails are just sent to the list of addresses provided for the alias.

A Note About Catch-All Aliases

A catch-all alias is simply that: an alias that catches all email sent to a domain that doesn't correspond to an actual account. Catch-all aliases can be useful as long as they are monitored and kept clear of unwanted email. However, due to the nature of email and the amount of spam that is sent every day, a catch-all can become a burden to email systems and to domain administrators. Therefore, it is suggested that they be used sparingly, or not at all if it can be avoided.

Chat History Search

This settings page is only available to domain administrators.

A major advantage of SmarterMail is that it stores all chats, regardless of whether the chats occur within the webmail interface, using a third-party client or a combination of both. Domain administrators have the ability to perform custom searches by date range, by the users involved in the chat conversations, by specific keywords or phrases used during a chat or a combination of all of these variables. Note: Chat history search is configured by the system administrator. For more information, see the Features area of the All Domains page of SmarterMail Help.

The options available when performing a chat history search are as follows:

- Date Range - The date range you want to use for your search. You can either type in the date or click on the calendar icon and use SmarterMail's calendar control to select your start and end date.
- User 1 - The username or email address of the person who originated the chat.
- User 2 - The username or email address of the person who was the recipient of the chat.
- Text - Any word or phrase that was used during a chat. For example, "2012 sales numbers" or "product ID 33489".

Trusted Senders

This settings page is only available to domain administrators.

This setting allows domain administrators to list specific email addresses (such as jsmith@example.com) or domains (such as example.com) that will be exempted from spam filtering for all users of the domain. This can prevent mail from friends, business associates, and mailing lists from being blocked and lets the system know that these messages come from a trusted source.

To view the trusted senders list for the domain, click the settings icon . Then expand the Domain Settings folder and click Trusted Senders in the navigation pane. A list of trusted senders will load in the content pane and the following options will be available in the content pane toolbar:

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

To add a trusted sender to the list, simply click the New button and add each address or domain in the modal window. Each separate entry should appear on a new line in the text box.

Signatures

This settings page is only available to domain administrators.

An email signature is a block of text automatically appended at the bottom of an email message. Signatures may contain the sender's name, address, phone number, disclaimer, or other contact information.

Businesses that want to ensure a consistent company appearance may require employees to follow a specific signature format. Instead of allowing the users to define their own signatures, the domain administrator can create a domain-wide signature that all employees must use. Depending on the signature configurations set up by the domain administrator, users may or may not be able to override the default signature.

To access the signature settings for a domain, click the settings icon . Then expand the Domain Settings folder and click Signatures in the navigation pane. The signature settings will load in the content pane and the following tabs will be available:

Mappings

Use this tab to assign a signature to specific domains. To allow users the ability to create and use their own signatures, select the Enable users to override checkbox. Note: If this setting is disabled, users must use the domain-wide signature.

Signatures

Use this tab to create or edit signatures. To create a new signature, click Add in the content pane toolbar and complete the appropriate fields. To edit an existing signature, select the desired signature and click Edit in the content pane toolbar.

Whether you add or edit a signature, the signature creation window appears. Here, you can create signatures using a full HTML editor that allows domain administrators to add in stylized text, links to websites, images and even icons linked to social media outlets. In addition, the signature can incorporate variables so that a generic template can be created for all users of the domain. The available variables are listed by clicking the Variables dropdown in the text box's toolbar.

Notification Profiles

This settings page is only available to domain administrators.

SmarterMail users can create Events that allow them to select criteria and apply specific actions when the criteria are met. One of the actions is to receive email notifications when an event is triggered. For example, users can receive notifications when a task is due or system administrators can receive notifications when the disk space for a domain reaches a certain percentage. Notification profiles determine how those messages are sent.

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

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

The following columns are available:

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

The following options are available from the content pane toolbar:

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

To view a specific notification profile, simply double-click the appropriate profile. Alternatively, you can select the profile and click on the Edit button. Regardless of how you open the profile, it will load as a modal window in the content pane.

Creating a Notification Profile

Creating a notification profile is very simple. Just click on the New button, and a new modal window will open with the following options:

- Notification Profile Name - The name you set for the profile.
- Email Address(es) - The email address(es) to which notifications are sent. More than one email address can be added to this field, they just need to be separated with a comma.
- Enabled - Checking this box will enable email notifications.
- SMS Email Address(es) - Sometimes domain administrators will want notifications sent to their mobile devices via text message. Here you'll input the mobile device email address to which notifications are sent.
- Enabled - Checking this box will enable SMS notifications.
- Enable reminders for all domain administrators - Checking this box will display reminders for tasks and appointments in a popup window in webmail.

Use of Notification Profiles

As mentioned, notification profiles are primarily used in conjunction with Events. When a new event is created, users have the ability to select a notification profile to use when that event fires. If more than one notification profile is available, each will be listed and users will need to make sure they've selected the proper profile to use with that event.

Domain Shared Resources

This settings page is only available to domain administrators.

SmarterMail allows domain administrators to create shared resources for all users of a specific domain. For example, calendars that can be used for tracking a department's vacation schedule or company holidays. In addition, this is where domain administrators set up calendar items that are used for shared conference room scheduling.

The following columns are available:

- Checkbox - Use these boxes to select multiple resources. A resource must be selected before choosing an action from the content pane toolbar.
- Resource - The friendly name of the resource.
- Type - The types of resource created.
- Number of Permissions - When a resource is created, a domain administrator can enable specific permissions for users or groups. This column displays how many permissions were set. The number displayed will correspond to the number of permissions added. Therefore, if the resource is shared with a group (alias), then only 1 will display, but if a resource is shared with multiple individuals, the total number of individuals will be displayed.

Adding a Shared Resource

Adding a shared resource is a fairly straightforward process. Simply click New in the content pane to open the add resource window. The following options are available:

- Name - The name of the resource. Note: If this resource is a conference room it is best to name the resource the same as the room designation. For example, South Conference Room or Main Hall.
- Type - The type of resource being added. For now, only Calendar is available.
- Resource is a conference room - Select this checkbox to designate the resource as a conference room.

Other Options

Apart from creating a new shared resource, domain administrators have the ability to do the following:

- Edit - Editing a resource allows admins to change the permissions assigned to the resource. For example, adding or removing users, groups, etc.
- Delete - Deletes the resource and any associated permissions. A deleted resource simply reverts to "None" in any associated appointments.
- Rename - Simply changes the name of the resource in the appointment dropdown and on any associated appointments.

Adding a Conference Room

When you add a shared resource as a conference room anyone with permissions to access the conference room will be able to add it to any event that they create. SmarterMail will check for availability and, if any conflicts are found, they will be displayed in the event creation window. Event coordinators will then have to select a new day and/or time in order to clear up the conflict. NOTE: Unlike actual shared calendars, shared conference rooms will NOT show up as an available shared calendar for users outside of creating new events.

ActiveSync Mailboxes

This feature is only available in SmarterMail Enterprise.

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

System administrators will use this section to enable and disable the EAS add-on for mailboxes across all domains on the SmarterMail server. Domain administrators will use this page to manage the EAS add-on for their particular domain. Note: Before an administrator can configure a mailbox to sync using ActiveSync, the add-on needs to be activated and available for users of the domain. For more information, please refer to the KB article [Activate Microsoft Exchange ActiveSync](#). Furthermore, domain administrators will only see this section available when the system administrator has enabled ActiveSync User Management for their domain.

To access this section as the System Administrator, click the Settings icon and click ActiveSync Mailboxes in the navigation pane. To access this section as the Domain Administrator, click the Settings icon , expand the Domain Settings folder and click ActiveSync Mailboxes in the navigation

pane. A list of accounts for which the Exchange ActiveSync add-on is enabled will load in the content pane.

In general, the following columns are available:

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

The following options are available from the actions toolbar:

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

Filtering

Domain Folder Auto-clean

This settings page is only available to domain administrators.

Setting up auto-clean rules for folders is a simple, yet effective, way to limit how much of the domain's disk space is taken up by users' Junk E-Mail, Sent Items, and Deleted Items folders. By placing limits on the size of these folders, or by automatically deleting mail older than X number of days, you can help ensure that your domain disk space does not fill up unnecessarily. In addition, if you want to set a size limit on a folder for users, their messages are deleted in the order that they were received so that older messages get deleted first.

To access the folder auto-clean settings, click the settings icon . Then expand the Domain Settings and Filtering folders and click Folder Auto-Clean in the navigation pane. The folder auto-clean settings will load in the content pane and the following tabs will be available:

Options

Use this tab to specify the following options:

- Use default auto-clean settings - Select this option to adopt the auto-clean policy set by your email host or domain administrator.
- Override auto-clean settings for this account - Select this option to override the settings set by your administrator. Any changes you make will not be affected if the administrator changes their policy, unless they disable user overrides.
- Enable users to override auto-clean settings - Select this option to allow users to create their own auto-clean policies.

Folder Settings

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

These options will be visible if size is chosen:

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

These options will be visible if date is chosen:

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

Domain Content Filtering

This settings page is only available to domain administrators.

Domain content filtering allows you to create the same types of content filters as you can on the user level, but the filters added will be applied to all members of a domain. The evaluation of domain content filters happens before the evaluation of account-specific content filters. For more information about how to add a content filter, refer Content Filtering .

Note: Be aware that many users will prefer to set their own content filtering. You may want to minimize filtering at the domain level to only filter items that affect the entire domain.

Spam Filtering

This settings page is only available to domain administrators.

SmarterMail includes many advanced antispam measures that will help protect your users from unwanted email. The system administrator has probably already set up some default spam options.

Domain administrators can further modify these settings as well as set up rules for Content Filtering and Domain Auto-cleaning .

To view the spam filtering settings for your domain, click the settings icon . First expand Domain Settings, then expand the Filtering section and click Spam Filtering in the navigation pane. The spam filtering settings will load in the content pane and the following tabs will be available:

Options

Use this tab to set the following spam filtering options for the domain:

- Use default spam settings - Choose this option to accept the default spam options provided by your system administrator. The settings will be displayed for your reference.
- Override spam settings for this domain - Select this option to customize the way spam is handled. Spam check weights and actions will become overridable by end users. More information about the types of actions allowed can be found below.

Actions

When you override the spam options set by your system administrator, you can choose the actions that are taken when email comes in that has a low, medium, or high probability of being spam. For each spam level, choose the action you wish to have taken. If you choose to add text to the subject line of messages, type the text in the box below the action drop down.

Current Weights

Each type of spam check has an associated weight that factors into the spam probability of a message. When an email comes in, all of the checks listed are run, and for each check that the message fails, the weight is added to the overall score of the email. The thresholds for each spam probability are examined, and the email is placed into the appropriate category.

Mailing Lists

Mailing Lists

This settings page is only available to domain administrators.

Mailing Lists are a great way to allow users to communicate with a number of different individuals via a single email address. For example, many companies use mailing lists to email newsletters, promotional offers, or information about product updates to subscribers. Unlike an Alias , a mailing list allows people to subscribe to, or unsubscribe from, email communications. In addition, mailing lists can be public or private, be replied to by all users or managed by a single list administrator and more. NOTE: SmarterMail can accommodate mailing lists of up to 75,000 subscribers. Anything

greater than that should be managed by a third-party mailing list service provider such as Constant Contact or MailChimp.

Using a mailing list is as simple as sending a standard email: the allowed posters simply send an email to the list address, which takes the form of the list name appended to the domain name. For example, if you create a mailing list called "newsletter" you send a message to newsletter@example.com. If there are other requirements, such as a password, etc. those need to be taken into account as well. For more information, see Creating a New Mailing List .

By default, when a subscriber reads a mailing list message, the From field in the subscriber's inbox will display the email address of the individual that sent the mailing list message; the To field will display the list name or mailing list email address; and the Reply To field will display the mailing list email address or the email address of the individual that sent the message, depending on the list settings. Note: Domain administrators and mailing list moderators can customize the From, To, and Reply To fields by editing the mailing list settings.

To view the mailing lists for your domain, click the settings icon . Then expand the Domain Settings and Mailing Lists folders and click Mailing Lists in the navigation pane. A list of the mailing lists for the domain will load in the content pane.

In general, the following columns are available:

- Checkbox - Use these boxes to select multiple mailing lists. Mailing lists must be selected before choosing an action from the actions toolbar.
- List Name - The name of the mailing list.
- Moderator - The "owner" of the mailing list.
- Description - A brief summary of the mailing list.
- Subscribers - The number of people currently subscribed to the mailing list.
- Digest Subscribers - The number of subscribers that receive a digest of mailing list postings. Users can either subscribe to the mailing list and receive each email sent to the list or to the digest, in which case they receive a summary of all messages sent to the list over a specific period of time. Users can not subscribe to both.

The following actions are available from the content pane toolbar:

- New - Clicking this button will allow the domain administrator to create a new mailing list.
- Edit - Clicking this button will allow the domain administrator to edit an existing mailing list's settings.
- Delete - Clicking this button will allow the domain administrator to delete an existing mailing list.

- Send Digest - Clicking this button will allow the domain administrator to send a digest of mailing list postings.

Variables

Mailing Lists support the use of the following variables. These can be used in the body or subject line of emails that are sent to the mailing list subscribers and also in the footer, header and subscriber System Messages . Though similar to Subscriber Fields in format, these variables need no additional configuration. Simply enter the variable below to display its associated information. Variables will always follow this format: #Variable#

- #UnsubscribeLink# - An unsubscribe variable is included to allow users to unsubscribe from the mailing list with a URL. Note: This URL can also be given friendly hyperlink text (rather than linking the URL) by modifying the Friendly Unsubscribe setting when configuring or modifying a mailing list. For more information, see [Creating a New Mailing List](#) .
- #Recipient# - The email address of the subscriber who was sent the message.
- #Sender# - The email address of the user sending the message.
- #DomainDateNow# - The current date (in shorthand) according to the domain's new user time zone defaults found in User Defaults. Ex: 07/13/2015.
- #DomainTimeNow# - The current time according to the domain's new user time zone defaults found in User Defaults. Displayed in 24-hour format.
- #DomainDateTimeNow# - The current date and time according to the domain's new user time zone defaults found in User Defaults. Disaplyed in shorthand and 24-hour format.
- #DomainDayNow# - The current date (date alone, without month and year) according to the domain's new user time zone defaults found in User Defaults. Ex: 13.
- #DomainMonthNow# - The current month (in numeric value) according to the domain's new user time zone defaults found in User Defaults. Ex: 07.
- #DomainYearNow# - The current year according to the domain's new user time zone defaults found in User Defaults. Ex: 2015.
- #DomainDayNameNow# - The current day of the week according to the domain's new user time zone defaults found in User Defaults. Ex: Monday.
- #DomainMonthNameNow# - The current month (by its name) according to the domain's new user time zone defaults found in User Defaults. Ex: July.
- #ModeratorDateNow# - The current date (in shorthand) according to the Moderator's time zone. Ex: 07/13/2015.
- #ModeratorTimeNow# - The current time according to the Moderator's time zone. Displayed in 24-hour format.
- #ModeratorDateTimeNow# - The current date and time according to the Moderator's time zone. Disaplyed in shorthand and 24-hour format.

- #ModeratorDayNow# - The current date (date alone, without month and year) according to the Moderator's time zone. Ex: 13.
- #ModeratorMonthNow# - The current month (in numeric value) according to the Moderator's time zone. Ex: 07.
- #ModeratorYearNow# - The current year according to the Moderator's time zone. Ex: 2015.
- #ModeratorDayNameNow# - The current day of the week according to the Moderator's time zone. Ex: Monday.
- #ModeratorMonthNameNow# - The current month (by its name) according to the Moderator's time zone. Ex: July.
- #ServerDateNow# - The current date (in shorthand) according to the server's system time zone. Ex: 07/13/2015.
- #ServerTimeNow# - The current time according to the server's system time zone. Displayed in 24-hour format.
- #ServerDateTimeNow# - The current date and time according to the server's system time zone. Disaplyed in shorthand and 24-hour format.
- #ServerDayNow# - The current date (date alone, without month and year) according to the server's system time zone. Ex: 13.
- #ServerMonthNow# - The current month (in numeric value) according to the server's system time zone. Ex: 07.
- #ServerYearNow# - The current year according to the server's system time zone. Ex: 2015.
- #ServerDayNameNow# - The current day of the week according to the server's system time zone. Ex: Monday.
- #ServerMonthNameNow# - The current month (by its name) according to the server's system time zone. Ex: July.

Create a New Mailing List

This settings page is only available to domain administrators.

To view the mailing lists for a specific domain, click the settings icon . Then expand the Domain Settings and Mailing Lists folders and click Mailing Lists in the navigation pane. To create a new mailing list, click the New button in the content pane toolbar. You can also edit an existing mailing list by selecting the desired mailing list and clicking the Edit button in the content pane toolbar.

List Settings

Use this tab to edit the following mailing list settings:

- Name - Essentially, the "username" for the mailing list. SmarterMail will use the name to create the actual email address that will be associated with the mailing list.

- Moderator - The "owner" of the mailing list. This person will actively manage the mailing list, posts to the list and any replies. The moderator must be an active email user for the domain.
- Password - To restrict subscribers from sending emails to a mailing list, type a password in this field. Note: To send emails to a mailing list that is password protected, you add the password to the subject line of the email, enclosed by brackets and colons. For example, [:password:] Attention all subscribers.
- Enabled - Check this box to enable password protection for this mailing list.
- Allowed Posters - An email that is sent to the mailing list (and therefore to its subscribers) is considered to be "posted". Use this field to specify who has access to post to the list.
- Anyone - Setting the list to "anyone" means that anyone can email the list, regardless of whether they are subscribed to the list or not. In turn, this sends an email to all members. Note: This setting can cause abuse if it is not closely monitored. Therefore, it is recommended to restrict the allowed posters to 'subscribers only', at the very least. For larger lists, allowing Moderator Only is a better idea and will cause less issues.
- Subscribers Only - Setting the list to "subscribers only" allows the list subscribers, and only the list subscribers, to send and receive posts. The moderator will still be permitted to post. This can cause abuse issues as well if you have an active list, so using Subscribers Only should only be used for smaller lists or for digest mode only.
- Moderators Only - If the moderator is set as the post option, the moderator is the only one who can post to the list. This means that no one else, not even list subscribers, will be able to post.
- Subject Prefix - The optional text that will appear in the subject line. SmarterTools recommends using a subject prefix for discussion lists to help subscribers easily filter through posts. For example, add a "List- " or "Discussion -" prefix so that users know that the message is posted to an email list. Recipients can then create filters to move those messages to a specific folder or manage them in some other way.
- Enabled - Check this box to enable the subject prefix for this mailing list.
- List To Address - The email address that will display in the To field when a subscriber receives a mailing list message. Setting this to List Address means that the email address associated with the list will display as the To: address when recipients receive the message.
- List From Address - The email address that will display in the From field when a subscriber receives a mailing list message. By default this is set to List Address.
- List Reply To Address - The email address that will display in the Reply To field when a subscriber receives a mailing list message. When a subscriber hits 'Reply' to the message, this address will receive the reply. If a subscriber hits 'Reply All' all list recipients will receive the reply. By default this is set to List Address
- Max Message Size - The maximum number of KBs a message can be. If the message exceeds

this size, it will not be posted. By default, the max message size is unlimited.

- Friendly Unsubscribe - The text entered here will be hyperlinked when using the Unsubscribe variable . Without this setting enabled, the unsubscribe link will hyperlink the full URL.
- Enabled - Check this box to enable the friendly text for the unsubscribe URL.
- Disable Mailing List - Check this box to disable the mailing list.
- Description - A brief summary of the mailing list.

Options

Use this tab to enable or disable the following mailing list options:

- Enable Digest Mode - Digest mode is a way to aggregate all postings to a list so that subscribers can receive a single, periodical email instead of individual replies to the list. This is especially useful for very active lists or lists with a larger number of subscribers. For more information, see the Digest Settings tab.
- Enable Header - Select this option to append header text to the beginning of the mailing list message. Note: To edit the header text, click the System Messages tab and edit the appropriate system message.
- Enable Footer - Select this option to append footer text to the end of the mailing list message. Note: To edit the footer text, click the System Messages tab and edit the appropriate system message.
- Send Subscribe Email - Select this option to automatically send an email to new subscribers confirming their subscription to the list. Note: This is not an opt-in message, only a confirmation email.
- Send Unsubscribe Email - Select this option to automatically send an email response to unsubscribe requests.
- Enable Poster Whitelist - Select this option to allow whitelisted email addresses to post to the mailing list.
- Enable SUBSCRIBE Command - Select this option to allow people to subscribe to the mailing list by emailing a listserv command to the command address. For more information, refer to Listserv Commands . Note: If this option is disabled, only list administrators can add new subscribers to the mailing list.
- Enable LIST Command - Select this option to allow people to receive a list of the mailing list subscribers by emailing a listerv command to the command address. For more information, refer to Listserv Commands . Note: It is recommended that you leave this option disabled, as people or automated systems could use the user list for malicious purposes.
- Enable Unsubscribe from Subject - Select this option to allow subscribers to unsubscribe from the mailing list by sending an email to the list with the word "unsubscribe" in the subject line. It

is recommended that you usually keep this option enabled, as it will reduce complaints of abuse by giving subscribers a way to quickly opt-out of the mailing list.

- Enable Double Opt-In - Select this option to automatically send an email to new subscribers that requires them to confirm that they are subscribing to the list by clicking on an activation link. Using double opt-in is a good way to confirm subscriptions to the list and to help reduce abuse complaints.
- Disable List Error Replies - Select this option to prevent the system from automatically replying to incorrect listserv commands.

Digest Settings

To reduce the number of emails mailing list subscribers receive, domain administrators can allow subscribers to sign up for digest mode or normal mode. Essentially, digest mode condenses all the messages sent to the list into a single email that is sent to subscribers on a monthly, biweekly, weekly, daily, or other defined basis. Use this tab to edit the following digest settings:

- Last Sent - The date and time a digest email was sent to subscribers.
- Subject - The subject line for the digest email.
- Trigger Type - The frequency of the digest emails.
- Digest Format - The format (HTML, text, etc.) in which digest emails are sent.
- Disable non-text attachments in digest - Select this option to remove non-text attachments from the digest email.
- Enable Header - Select this option to append header text to the beginning of the mailing list message. Note: To edit the header text, click the System Messages tab and edit the appropriate system message.
- Enable Separator - Select this option to place a separator between messages in a digest email.
- Enable Footer - Select this option to append footer text to the end of the mailing list message. Note: To edit the footer text, click the System Messages tab and edit the appropriate system message.

System Messages

Use this tab to edit system messages for mailing lists. Some system messages, such as headers and footers, are viewable by list subscribers. Other messages are only viewable when emailing listserv commands to the mailing list username. These messages are noted below, and more information is available to system administrators in their section of the SmarterMail help documentation. Note: This tab is not visible if you are creating a new mailing list. Variables can be used in the footer, header and subscribe system messages. For more information on variables, see [Mailing Lists](#).

Mailing List System Messages

- digestfooter - This is the footer that is displayed when digest emails are sent to digest list subscribers.
- digestheader - This is the header that is displayed when digest emails are sent to digets list subscribers.
- digestseparator - This is the character set (e.g., dashes) that will be used to separate messages within digest emails.
- disabledlistemail - This message is returned when a user attempts to post to a list that is no longer active.
- doubleoptin - This message is sent to subcribers to verify their subscription request when your mailing list utilized a double opt-in subscription model (recommended).
- doubleopinreply - This message is sent to subscribers notifying them that they were successfully subscribed to the list when the double opt-in subscription model is used.
- faildertosetdigestmode - LISTSERV COMMAND ONLY. This message is returned when the list command attempts to set digest mode but digest mode is not enabled for the specific list.
- failedtosetstandardmode - LISTSERV COMMAND ONLY. This message is returned when the list command tries to set the mode for a subscriber that is not actually subscribed to the list.
- footer - This is the footer (information at the very bottom of the message) that is displayed on messages that are sent to list subscribers.
- header - This is the header (informatin at the very top of the message) that is displayed on messages that are sent to list subscribers.
- help - LISTSERV COMMAND ONLY. This can be used to return information about the list, such as its creation date, last updated date, etc. or any other information the domain or list owner wants returned.
- helpmessage - LISTSERV COMMAND ONLY. This is the default message that is returned when a listserv command is sent to the mailing list username but the command is not recognized. By default it returns information on how to properly format commands.
- insufficientpostingpermissionemail - This email is sent to posters that do not have the proper permission to post to the list. For example, this is returned to list subscribers who reply to the list but only moderators are allowed to post.
- invalidlistpasswordemail - When a list is password-protected, this message is returned when a person posting to the list provides the incorrect information.
- listcommandresponse - LISTSERV COMMAND ONLY. This returns a list of subscribers for a particular list. This requires the LIST command to be set.
- listoflists - LISTSERV COMMAND ONLY. This reutrns a list of the mailing lists for a particular domain. This requires the LIST command to be set.

- maxmessagesizeexceededemail - This is returned when a message posted to a list is larger than the maximum size set for messages.
- nolistcommand - LISTSERV COMMAND ONLY. This is returned when a particular list is set to not allow a list of subscribers to be returned. That is, the LIST command is not enabled for that list.
- privatelist - This is returned when anyone tries to subscribe to the list but the list doesn't allow for automatic subscriptions. Instead, the list owner will need to add the subscriber manually.
- setdigestmode - LISTSERV COMMAND ONLY. This is returned when the list command sets the digest mode for a subscriber.
- setstandardmode - LISTSERV COMMAND ONLY. This is returned when the list command sets the standard mode (one email per list post) for a subscriber.
- subscribe - This is sent to a list subscriber when they subscribe to a specific list.
- unsubscribeemail - This is sent to a user when they unsubscribe from a specific list.

Subscribers

This settings page is only available to domain administrators.

Individuals that sign up to receive messages from the mailing lists are called subscribers. To view a list of the mailing list subscribers, click the settings icon . Then expand the Domain Settings and Mailing Lists folders and click Subscribers in the navigation pane. A list of subscribers will load in the content pane.

In general, the following columns are available:

- Checkbox - Use these boxes to select multiple subscribers. Subscribers must be selected before choosing an action from the actions toolbar.
- Email Address - The email address of the subscriber.
- Bounces - The number of bounced messages to the subscriber. If an email address has a large number of bounces, that could be an indication that the subscriber is no longer active and that the email address should be removed from the list of subscribers.

The following actions are available from the content pane toolbar:

- New - Allows you to add a new subscriber.
- Edit - Allows you to edit subscriber details.
- Delete - Allows you to delete a subscriber.
- Search - Allows you to search for a specific subscriber by email address or by any defined subscriber fields.
- Upload - Allows you to upload a list of subscribers to the mailing list. Note: Only .csv files can be uploaded. At a bare minimum, the .csv file must contain a column named

"EmailAddress". Any additional columns in the .csv file will be added to the Subscriber Fields for the corresponding subscriber/email address. See example below:

- Download - Allows you to download the list of subscribers as a text file.

	A	B
1	EmailAddress	Name
2	user1@example.com	John Smith
3	user2@example.com	Jane Smith
4	user3@example.com	John Stiles
5	user4@example.com	Richard Miles
6	user5@example.com	Mary Major
7		
8		

For step-by-step instructions on adding subscribers to a mailing list, please refer to the KB article [How To - Add Subscribers to Mailing Lists](#). To edit an existing subscriber's details, select the desired subscriber from the list and click Edit in the content pane toolbar.

Note: Individuals that opted to receive the digest mode will not be included in the Subscribers list. To view a list of digest subscribers, click the settings icon . Then expand the Domain Settings and Mailing Lists folders and click Mailing Lists in the navigation pane. Select the desired mailing list and click Edit. Then click Subscribers in the content pane toolbar and click Digest Subscribers .

Subscriber Fields

This settings page is only available to domain administrators.

Use subscriber fields to create custom fields to gather and manage information about subscribers. Subscriber fields are also used as variables in mailing list messages and can be used to include personal information about the subscriber when conducting a mail merge. For example, if you'd like your messages to be sent out with the subscriber's first name in the message greeting (ex. "Hello John,"), you'd first create the Subscriber Field then add it to each subscriber. To create or manage Subscriber Fields, click the Settings icon . Then expand the Domain Settings and Mailing Lists folders and click Subscriber Fields in the navigation pane.

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

- New - Adds a new Subscriber Field
- Edit - Allows changes to be made to the selected Subscriber Field.
- Delete - Remove the selected Subscriber Field(s).

Adding a New Subscriber Field

To add a new Subscriber Field, click the New button. A modal window will display the following options:

- Name - The name of the Subscriber Field. Note: The text entered here is used as the variable when sending subscriber fields in mailing list messages.
- Default Value - Enter the text that should be automatically entered for current subscribers.

Once the field is created, subscribers can be individually modified to change the value. Note: If a default value is not included, and the subscriber does not have their field configured, the variable will be removed from the message, leaving a blank space in its location.

Using Subscriber Fields in Messages

A Subscriber Field can be used in mailing list messages as a type of custom variable. To enter Subscriber Fields as variables, the name of the field must be enclosed with a #. For example, if a Subscriber Field was created for "Customer Name", you would enter #Customer Name# in your message.

Advanced Settings

Domain Aliases

This settings page is only available to domain administrators.

A domain alias is basically an alternate domain name for one that already exists in SmarterMail. For example, if the domain 'example.com' is in SmarterMail and has the user 'user@example.com' added to it, by adding a domain alias for 'example.net', emails sent to 'user@example.net' will be delivered to 'user@example.com'. That means that emails sent to either domain will end up in the same mailbox.

There are a few reasons why a domain alias is used. One is for branding purposes. If you have multiple extensions for an existing domain, using a domain alias for each extension means that you won't miss any emails if people send to one of your other domains. It is important to note that you must own each domain you're using in order to create domain aliases. In addition, messages cannot be retrieved with a domain alias email address unless the domain is properly registered at a domain registrar.

To view a list of domain aliases, click the settings icon . Then expand the Domain Settings and Advanced Settings folders and click then select Domain Aliases in the navigation pane.

To create a new domain alias, click New in the content pane toolbar. The domain alias settings will load in the content pane and the following options will be available:

- Name - The name of the domain alias. The name will be used to create the domain alias email address. For example, if the name of the alias is "example2," the domain alias email address will be user@example2.com.
- Points To - The domain the alias redirects to.
- Verify MX record in DNS before add - Select this option to check that the mail exchange record for the domain is pointing to the server. Note: This option is only available to system administrators and prevents users from "hijacking" mail from valid domains. For example if this check were not in place a user could add a domain alias of example.com. Then, any mail sent from the server to "anything@example.com" would go to the domain with the example.com domain alias, rather than to the actual domain.

Mail Signing

This settings page is only available to domain administrators.

Mail signing protocols, such as DKIM signing, verify the authenticity of a message and can be used to protect users from phishing schemes or spam attacks.

To edit the mail signing settings, click the Settings icon . Then expand the Domain Settings and Advanced Settings folders and click Mail Signing in the navigation pane.

Options

Use this tab to edit the following options:

- Enable DKIM Signing - Select this option to authenticate email with DKIM headers.

Certificate

Use this tab to edit the following settings:

- Selector - Type any identifier you like in this field. It is recommended the key is changed once every 12 months.
- Key Size - The size of the key. Remember, the larger the key, the stronger it is.
- TXT Record Name - After entering a unique identifier in the Selector field, selecting the Key Size and clicking Generate Key in the content pane toolbar, the TXT Record Name will populate. Set up the TXT Record in DNS using this name.
- TXT Record Value - After entering a unique identifier in the Selector field, selecting the Key Size and clicking Generate Key in the content pane toolbar, the TXT Record Value will populate. Set up the TXT Record in DNS with this value.

DKIM Signing

Use this tab to specify how closely you want the system to monitor messages in transit.

- Body Canonicalization - The method used to monitor in-transit changes to the body of a message.
- Header Canonicalization - The method used to monitor in-transit changes to the header of a message.
- Hash Algorithm - The method used to verify the DKIM signature.
- Header Field Signing - The header fields included in the hash algorithm. This is further defined by header fields.
- Header Fields - The header fields included in the hash algorithm. Note: List only one header field per line break.

Import LDAP Users

This feature is only available to domain administrators running SmarterMail Enterprise.

The Lightweight Directory Access Protocol (LDAP) is an Internet protocol that email servers and other programs use to connect to, and look up information from, a server. In SmarterMail, LDAP is most commonly used for integrating SmarterMail with Microsoft's Active Directory.

In order for domain administrators to add new SmarterMail users via the LDAP protocol they simply need to type the LDAP binding string in the LDAP Binding String field.

Note: LDAP integration will only function if SmarterMail is on the same domain as the LDAP server you are trying to connect to.

User Groups

This feature is only available to domain administrators running SmarterMail Enterprise.

User groups are used to give permissions to specific subsets of users on the domain to access shared resources. For example, if a business wanted to make it easy for members of its sales department to share their calendars with other team members, the domain administrator would create a user group for all the sales department employees.

By default, there are permanent user groups that cannot be edited:

- Everyone - All users on the domain belong to this group automatically.
- Administrators - All users that are marked as domain administrators for this domain belong to this group.

To view the user groups for the domain, click the settings icon . Then expand the Domain Settings and Advanced Settings folders and click User Groups in the navigation pane. A list of user groups will load in the content pane and the following options will be available in the content pane toolbar:

- New - Creates a new user group.
- Edit - Edits the members of the selected user group.
- Delete - Permanently deletes the selected user group(s).

Creating a User Group

To create a user group, simply click the New button, and a modal window will pop up with the following options:

- Name - The friendly name of the user group.
- Username - The individual users you want to add to the user group. To select multiple users, simply hold down the CTRL key (for Windows) or the Command key (for OSX) and click on each user to add. Note: Only actual users are available for addition to user groups. Aliases are not.

Default User Settings

This settings page is only available to domain administrators.

For domains that have a large number of users, it can be time consuming to have to make a change to user permissions and then make sure each user has the same change applied to their mailbox.

Additionally, if changes need to be made to a select few users, that can be difficult as well.

With Default User Settings, domain administrators can create a template for their users so that they only have to make the change in one location, and then Propagate User Settings to each user on the domain, or to a select few users. This makes changing settings quick and easy and ensures each user has the exact same permissions and settings applied. In addition, making a change to Default User Settings doesn't automatically propagate, so a change to default settings does not change users that are already in place for the domain.

The default user settings are identical to those found when adding a single user. For more information on these settings, refer to the help page that outlines setting up new Users .

User Propagation

This settings page is only available to domain administrators.

Use this section to apply global Default User Settings to some or all of the users on a domain. To access user propagation, click the settings icon . Then expand the Domain Settings and Advanced Settings folders and click user Propagation in the navigation pane. The default user settings will load in the content pane so that you can select which settings you want propagated to each user. For more information on these settings, refer to [Users](#) .

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

[Advanced Search](#)

[Advanced Search Overview](#)

SmarterMail users can take advantage of the mail server's powerful search feature to search specific sections of their mailbox (everywhere, email, contacts, or calendars). Search results are then displayed by the type of result (email, contacts, or appointments), making it easy to find the information you are looking for.

To access the advanced search feature, click the advanced search icon .

For help understanding the different areas of the advanced search section, see the advanced search diagram .

[Performing Advanced Searches](#)

To select which section of the mailbox to search, click the search selector and select the appropriate option from the list. In general, users can search everywhere, their email, contacts, or calendars.

Then type the search criteria in the search bar located near the top of the navigation pane and click the Search button. SmarterMail will automatically search the for matches and display the results in the content pane. Note: Your search criteria may include letters and numbers. SmarterMail does not search for special characters such as "@" "#" or "%".

In general, the following options are available from the navigation pane toolbar:

- New - Click this button and select the appropriate option to create a new message, contact, appointment, task, or note.
- Reset - Clears the search box and any previous search results that may be displayed in the content pane.

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

- Open - Opens the selected email, contact, or appointment item.
- Delete - Permanently deletes the selected email, contact, or appointment item.

Note: Users can also narrow the search locations by specifying search criteria. For example, if a user performing a search of his email can click Add Criteria and select From to ensure SmarterMail only returns results that have the search text in the From field.

Additional Help Topics

Mailing Lists

Generally, users do not have the ability to manage mailing lists. However, the domain administrator may assign an user as the moderator of a specific mailing list. If a user is the moderator of a mailing list, the user will be able to create new mailing list messages from his inbox. In addition, the user will have access to the mailing list settings for which he is a moderator. For more information, see Mailing Lists Overview .

Plus Addressing

Plus Addressing is a feature of SmarterMail that allows you to automatically filter your incoming email without creating content filtering rules first.

Example 1

Assume your email address is myname@example.com, and you want to sign up for a newsletter called ACME News. Furthermore, you want that newsletter to go to a folder in your email called "ACME". Assuming you have plus addressing enabled, all you have to do is sign up for the newsletter with the plus address myname+ACME@example.com Note: When writing the plus address, make sure the folder name is listed after the username but before the @example.com.

When the newsletter gets delivered to your email, it will automatically be placed in an ACME folder, which will be created automatically if it does not already exist. No additional steps are required. The whole process is automatic once you enable the feature.

Example 2

If you include the "/" character in your plus address, you can automatically create sub-folders. For example, the plus address myname+Newsletters/ACME@example.com will create a folder called Newsletters, then create an ACME folder under it, and drop the newsletter into the ACME folder.

As an added bonus, you can connect to folders in your email using POP3 by using plus addressed emails. The example above, when input into your POP email client as your login name, will return the contents of that folder.

Enabling Plus Addressing

For step-by-step instructions on enabling plus addressing, please refer to the KB article [How To Enable Plus Addressing](#).

Listserv commands

Listserv commands allow you to control the list through commands sent in email messages to the listserv command address. By default, the command address for a domain is "STServ@example.com", where example is the name of your domain. However, your system administrator may change this command address.

To send a command, compose an email to the command address with the command in the body of the message. The subject of the message is ignored.

Available Commands

Note: Any references to listname should be replaced with the list you are trying to use.

Help listname - Replies to the email with the contents of the Help system message for that list.

List - Replies to the email with a list of all available lists.

List listname - Replies to the email with a list of all subscribers for a particular list. Note: This command can be disabled by the domain administrator.

Subscribe listname - Adds your email address to the subscribers list of the mailing list. Note: This command can be disabled by the domain administrator.

Unsubscribe listname - Removes your email address from the subscribers list for the mailing list referenced by listname.

Set mode digest listname - Sets your email address to receive emails in digest mode, which will send all messages for the list combined into one email at regular intervals.

Set mode standard listname - Sets your email address to receive emails in standard mode (the default), which will send messages one at a time to your email account.

Using a Catch-All

This feature is only available to domain administrators.

A catch-all alias can be established that can receive all incoming email that goes to invalid email addresses within your domain. You may want to do this, for example, if customers frequently send to accounts that do not really exist. In general, however, use of a catch-all alias is not recommended, as it makes you more prone to harvesting attacks.

For information on setting up and assigning a catch-all alias, refer to the KB article [How To Enable or Disable Catch-alls](#).

Note: It is important to never set an auto-responder on an email account that the catch-all forwards to, as it may result in spammers sending more email to your domain. In addition, an increase in bandwidth usage will result. If you do not see the option for adding a catch-all, please contact your system administrator as they may have disabled the option.

Help for System Administrators

Logging in to SmarterMail

To access the login page, SmarterMail system administrators will need to navigate their Web browser to the location of the SmarterMail installation. By default, this URL is <http://127.0.0.1:9998> (if running the browser on the server itself, otherwise use the IP address of the server instead of 127.0.0.1), but it may be different if you have changed the location of SmarterMail.

To login to SmarterMail, type in the system administrator username and password in the appropriate fields and click Login . Note: By default, the username and password are both "admin" (without the quotes). If everything matches up, you will be presented with the manage domains page or the activation wizard (if you have yet to activate SmarterMail).

To stay logged in to SmarterMail even after closing the browser, be sure to select the Remember Me checkbox. This will allow SmarterMail to encrypt the email address and password. Note: Browser cookies must be enabled for this feature to work. In addition, SmarterTools does not recommend selecting this option if you use a public or shared computer.

Domains

All Domains

System administrators can use this section to manage all of the domains in SmarterMail. To access this section, click the Domains icon . A list of configured domains will load in the navigation pane, while the selected domain's details will load in the content pane. These details include information about the basic setup of the domain: statistics, such as the number of users and aliases for the domain; throttling and priority settings; as well as the various features enabled for the domain, including file storage, IMAP retrieval and more.

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

- New - Creates a new domain.
- Actions - Click this button and select the appropriate option to select all domains, delete the selected domain(s), manage or edit the selected domain, or export a list of the domains to CSV. Please note you can only manage or edit one domain at a time, though you can delete multiple domains.

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

- Edit - Edits the settings for the selected domain.
- Manage - Impersonates the domain administrator and give the system administrator access to all of the domain settings.

Creating New Domains

Adding a new domain and editing an existing domain are essentially the same process, and they both deal with the same settings. To create a new domain, click New in the navigation pane toolbar.

To edit a domain's settings, select the desired domain and choose Edit from the Actions menu found in the navigation pane toolbar. You can also double-click on a domain or right-click and choose Edit to open the settings. Regardless of the method used, the domain settings will load in a new window and the tabs below will be available. NOTE: When editing a domain's settings, use the Rename button in the window's toolbar to change the domain name.

Options

Use this tab to specify the following domain options:

- Name - The name of the domain. For example, smartermail.com or example.com. Note: To send or receive mail, the domain name must match the domain name registered with the DNS server.
- Folder Path - The directory in which all information (XML files, mail statistics, alias information, etc.) pertaining to the domain is saved. Note: If the directory does not already exist, it will be created. This directory should be solely dedicated to SmarterMail. By default, SmarterMail saves domain information to C:\SmarterMail\Domains.
- Mailing List Username - The email address for which listserv commands are emailed for the domain. By default, SmarterMail sets this as stServ.
- Disable Domain - Select this option to disable the domain. Disabled domains cannot send email and users cannot login to the Web interface. However, the domain will still receive email to prevent email loss. This option is a good way to temporarily shut off a domain without deleting it.
- Domain Location - Administrators can specify the domain location for email delivery. This allows you to specify whether the domain is hosted locally or partially/entirely on an external server. The following options are available:
 - Local - Select this option if the mail server is hosted locally.
 - External (use MX record) - Select this option if the mail server is hosted partially or entirely externally. Messages will be delivered based on an MX lookup. Note: Select the option "Deliver locally if user exists" to perform a local delivery instead of external if the user exists locally.

- External (use host address) - Select this option if the mail server is hosted partially or entirely externally. Messages will be delivered to the specified host address. The host address can either be entered as an IP address or the Fully Qualified Domain Name (FQDN), such as mail.yourdomain.com. Note: Select the option "Deliver locally if user exists" to perform a local delivery instead of external if the user exists locally.
- Domain Administrator - The domain administrator is responsible for adding and deleting email accounts and setting specific configurations for the domain. Domain administrator accounts also have the ability to send and receive email, manage contacts, etc., just like a user account. Select an existing user from the dropdown menu or enter new user credentials.
- Domain Administrator Username - The identifier the domain administrator uses to login to SmarterMail.
- Domain Administrator Password - The password associated to the domain administrator username. Enter the password twice to confirm it is entered correctly.

Technical

Use this tab to specify the following technical settings:

- Outbound IPv4 - The IPv4 address used to connect to external SMTP servers when a message is sent by the domain. If multiple IPv4 IPs are on the server, they will be listed in the dropdown.
- Outbound IPv6 - The IPv6 address used to connect to external SMTP servers when a message is sent by the domain. If multiple IPv6 IPs are on the server, they will be listed in the dropdown.
- Logout URL - By default, when users log out they are presented with the screen to log back into SmarterMail's Web interface. This feature allows for a separate URL that the user is redirected to upon logout. Check the Enabled box to enable the logout URL. This setting can also be managed by domain administrators.
- Auto-responder Exclusions - To prevent SmarterMail from sending automated messages, such as out-of-office replies, to addresses based on the spam level of the original message, select the appropriate option from the list.
- Forwarding Exclusions - To prevent the system from forwarding messages based on the spam level of the message, select the appropriate option from the list.
- TLS - To enable or disable TLS (SSL encryption) for outgoing mail, select the appropriate option from the list.
- SRS - To enable or disable SRS (the ability for the mail server to re-write the sender's email address so that forwarded messages pass SPF checks) for mail, select the appropriate option from the list.

- Calendar Auto Clean - Use this to set a time frame that SmarterMail will use to automatically remove legacy calendar items from users' calendars. This setting can also be managed by domain administrators.
- Require SMTP Authentication - Select this option to require SMTP authentication when sending email. Note: If this option is enabled, users must provide an email address and password to send email from their account. SmarterMail supports cram-md5 and login authentication methods.
- Restrict auto-responders to once per day per sender - Select this option to limit how frequently an auto-responder is sent. Continually sending something like an out-of-office reply to the same address every time an email comes in can cause abuse issues. Therefore, it is recommended that this be set for all domains.
- Disable greylisting - Select this option to disable the greylisting anti-spam option for the domain. Greylisting, though effective, can lead to a delay in email delivery for a domain.
- Allow users to opt out of LDAP listings - Select this option to allow users to remove themselves from the Global Address List.
- Allow domains to override mailing list message size - Select this option to allow domain administrators to specify the maximum size for mailing list messages.
- Exclude IP from received line - Select this option to remove the client's IP address from the received header on messages received through SMTP. Note: Removing the IP address from the received header is not recommended because it violates RFC.
- Allow users to override personalization settings - Select this option to allow users to modify the way their user interface appears in webmail.

Features

Use this tab to enable or disable the following features:

- Active Directory Integration - Select this option to enable active directory authentication. By enabling this, domain administrators will be able to add in the necessary LDAP binding string to import LDAP users.
- ActiveSync Remote Wipe - Select this to allow users with the Exchange ActiveSync add-on to have access to SmarterMail's remote wipe functionality.
- ActiveSync User Management - Select this to allow domain administrators to add and delete mailboxes that can use the Exchange ActiveSync add-on. Note: The option to limit the number of ActiveSync mailboxes allotted for the domain can be found on the Limits tab.
- Calendar - Select this option to allow users to use the calendar feature.
- Catch-All Alias - Select this option to allow users to create catch-all email addresses. When enabled, this setting can be managed by domain administrators as well.
- Connected Services - Select this option to allow users to connect different services to their

SmarterMail accounts to facilitate actions like attaching links to shared files.

- Contacts - Select this option to allow users to use the contacts feature. When enabled, this setting can be managed by domain administrators as well.
- Content Filtering - Select this option to allow users to use content filtering. When enabled, this setting can be managed by domain administrators as well.
- Control of Service Access - Select this option to give domain administrators the ability to manage access to POP, IMAP, SMTP and webmail services for users.
- Disposable Addresses - Select this option to allow users to create a temporary, disposable address independent of their email address.
- Domain Aliases - Select this option to allow domain administrator to create domain aliases. When enabled, this setting can be managed by domain administrators as well.
- Domain Chat History View - Select this option to allow domain administrators to be able to search through all chat history for any and all users of a domain.
- Domain Reports - Select this option to provide additional reports for domain administrators.
- Domain Spam Options - Select this option to show or hide the spam filter settings for domain administrators. Hiding the spam filter settings will prevent domain administrators from changing the weights set by the system administrator for spam checks.
- Email Reports - Select this option to provide the ability to email reports.
- Exchange Web Services (EWS) - Select this option to enable users on the domain to synchronize SmarterMail with supported email clients using Exchange Web Services (EWS).

Note: For domains that will support inboxes with large volumes of email, IMAP is encouraged as the primary protocol as EWS does not perform well with large amounts of email.
- File Storage - Select this option to allow users to use the file storage feature. When enabled, this setting can be managed by domain administrators as well.
- IMAP Retrieval - Select this option to allow users to download IMAP email from third-party mail servers. When enabled, this setting can be managed by domain administrators as well.
- Live Chat (XMPP) - Select this option to allow users on the domain to chat with each other via the Web interface or any XMPP-compatible chat client. When enabled, this setting can be managed by domain administrators as well.
- Login Display Customization - Select this option to allow domain administrators to customize the login screen to add a company logo, provide additional branding text, or adjust the default Login to SmarterMail text.
- Mail Signing - Select this option to enable email verification via mail signing. When enabled, this setting can be managed by domain administrators as well.
- Mailing Lists Select this option to allow domain administrators to create and use mailing lists to send mass emails. When enabled, this setting can be managed by domain administrators as well.

- Notes - Select this option to allow users to use the notes feature. When enabled, this setting can be managed by domain administrators as well.
- POP Retrieval - Select this option to allow users to download POP email from third-party mail servers. When enabled, this setting can be managed by domain administrators as well.
- SMTP Accounts - Select this option to allow users to send email from a third-party mail server account right from within SmarterMail. When enabled, this setting can be managed by domain administrators as well.
- SyncML - Select this option to allow users to sync SmarterMail with Outlook, Thunderbird and most smartphones using SyncML.
- Tasks - Select this option to allow users to use the tasks feature. When enabled, this setting can be managed by domain administrators as well.
- User Reports - Select this option to provide reports for users.

Limits

Use this tab to specify the following limits:

- Disk Space - The maximum number of megabytes allocated for the domain. By default, the domain is allocated 500 MB of disk space. This disk space limit also includes file storage for users. Note: When this limit is reached, SmarterMail will send a warning to the domain administrator and mailboxes on the domain will not be able to receive new mail.
- Domain Aliases - The maximum number of domain aliases allowed for the domain. A domain alias acts as a secondary domain that users can use for sending and receiving emails. By default, domains are limited to two domain aliases.
- Users - The maximum number of mailboxes allowed for the domain. By default, domains are limited to 100 users. Note: If your SmarterMail license limits the number of mailboxes allowed on the domain, your license level will override this setting.
- User Aliases - The maximum number of alias email accounts (forwarded to a true email account) allowed for the domain. By default, domains are limited to 1,000 user aliases.
- Mailing Lists - The maximum number of mailing lists allowed for the domain. By default, this setting is unlimited.
- Mailing List Max Message Size - The maximum size message that can be sent to a mailing list. By default, the maximum message size is unlimited.
- POP Retrieval Accounts - The maximum number of POP email accounts a user can set up in SmarterMail. By default, users can receive download messages for 10 POP email accounts.
- IMAP Retrieval Accounts - The maximum number of IMAP email accounts a user can set up in SmarterMail. By default, users can receive download messages for 10 IMAP email accounts.
- Max Message Size - The maximum size email a user can send. By default, the max message size is 10,000 KB. This number includes text, HTML, images and attachments. Note: Base64

encoding of attachments increases the size of attachments by approximately 50%. This can impact the overall size of the message and can lead to confusion on the part of senders. For example, if Max Message Size is set to 12MB and a sender adds a 9MB attachment to a message it will essentially be 13MB due to the Base64 encoding. This means that the 9MB attachment will still exceed the message size limit due to this increase.

- Recipients per Message - The maximum number of recipients a message can have. By default, users can send messages to 200 email addresses.
- ActiveSync Accounts - The maximum number of Microsoft Exchange ActiveSync accounts that can be set up for the domain. Note: This setting is used in conjunction with the ActiveSync User Management setting on the Features tab.

Sharing

This tab is only available in SmarterMail Enterprise edition.

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

- Global Address List - Select this option to allow users on a domain to see all user profiles on the domain and participate in LDAP queries against the domain. When enabled, domain administrators can manage this feature as well.
- Shared Calendars - Select this option to allow calendars to be shared with other users on the domain. When enabled, domain administrators can manage this feature as well.
- Shared Contacts - Select this option to allow contact lists to be shared with other users on the domain. When enabled, domain administrators can manage this feature as well.
- Shared Folders - Select this option to allow email folders to be shared with other users on the domain. When enabled, domain administrators can manage this feature as well.
- Shared Notes - Select this option to allow notes to be shared with other users on the domain. When enabled, domain administrators can manage this feature as well.
- Shared Tasks - Select this option to allow task lists to be shared with other users on the domain. When enabled, domain administrators can manage this feature as well.

Priority

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

The use of message delivery priorities also gives system administrators the ability to create automated actions based upon that priority. A common use would be to set up a separate specific outbound gateway to handle all mailing lists to avoid potential blacklisting of the primary IP and to efficiently

deliver all messages. The system administrator could then assign all mailing lists a priority of 1, and would set up a gateway to handle only messages with a priority range of 1 to 1.

- Standard Messages - The priority level for messages that don't have another priority affecting it, as detailed below.
- Enabled - Check this box to enable priority settings for standard messages.
- Mailing Lists - The priority level for messages sent to a mailing list.
- Enabled - Check this box to enable priority settings for mailing list messages.
- Priority When Over Size - The priority level for messages that exceed the message size threshold. For example, system administrators may want to lower the priority of large messages to avoid slowing down the spool.
- Enabled - Check this box to enable priority settings for messages that exceed the message size threshold.
- Message Size Threshold - The maximum size a message can be without triggering the Priority When Over Size rule.
- Auto-Responders - The priority level for auto-responder messages, such as out-of-office responses.
- Enabled - Check this box to enable priority settings for auto-responders.
- Bounces - The priority level for non-delivery receipts.
- Enabled - Check this box to enable priority settings for bounced messages.
- Email Reports - The priority level for email reports.
- Enabled - Check this box to enable priority settings for email reports.
- Appointment Reminders - The priority level for messages reminding users of upcoming appointments, meetings or events.
- Enabled - Check this box to enable priority settings for event emails.
- Priority After Attempt 1 - The priority level for messages that were not successfully sent after the specified number of tries.
- Enabled - Check this box to enable priority settings for subsequent delivery attempts.
- Attempt 1 Threshold - The number of retry attempts the system should make before the priority set in Priority After Attempt 1 is assigned to the message.
- Priority After Attempt 2 - The priority level for messages that were not successfully sent after the specified number of tries.

- Enabled - Check this box to enable priority settings for subsequent delivery attempts.
- Attempt 2 Threshold - The number of retry attempts the system should make before the priority set in Priority After Attempt 2 is assigned to the message.

Throttling

This tab is only available in SmarterMail Enterprise edition.

Throttling allows system administrators to limit the number of messages per hour and/or the amount of bandwidth used per hour to send messages. If the throttling action is set to Reject, SmarterMail will bounce any messages attempting to be sent after the threshold is met, until the next session. If the throttling action is set to Delay, SmarterMail will allow the message into the spool and trickle delivery.

Use this tab to edit the following throttling settings:

- Outgoing Messages per Hour - The number of messages sent by the domain per hour. By default, the number of outgoing messages is 5,000.
- Message Throttling Action - The action SmarterMail should take when the message throttling threshold is reached.
- Outgoing Bandwidth per Hour - The total number of MBs sent by the domain per hour. By default, the outgoing bandwidth is 100.
- Bandwidth Throttling Action - The action SmarterMail should take when the bandwidth throttling threshold is reached.
- Bounces Received per Hour - As bounce messages are received from null senders per RFCs, this setting dictates the number of messages from null senders a domain can receive over SMTP before any further messages from null senders will be rejected. By default, a domain can receive 1,000 bounces per hour.
- Bounces Throttling Action - The action SmarterMail should take when the bounces throttling threshold is reached.

Event Restrictions

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

Alias

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

Collaboration

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

Email

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

Mailing List

- Enable Mailing List Added event - Select this option to enable the Mailing List Added event type.
- Enable Mailing List Deleted event - Select this option to enable the Mailing List Deleted event type.
- Enable Message Sent to Mailing List event - Select this option to enable the Message Sent to Mailing List event type.
- Enable Mailing List Bounce Removal event - Select this option to enable the Mailing List Bounce Removal event type.
- Enable Mailing List Subscribe event - Select this option to enable the Mailing List Subscribe event type.
- Enable Mailing List Unsubscribe event - Select this option to enable the Mailing List Unsubscribe event type.

Throttling

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

User

- Enable User Added Event - Select this option to enable an event type for when a new user is added to a domain.
- Enable User Deleted event - Select this option to enable an event type for when a new user is deleted from a domain.
- Enable User Changed Password event - Select this option to enable an event type for instances where users change their passwords.
- Enable User Changed Forward event - Select this option to enable an event type for instances where users change the forwarding address they have set up for their account.

- Enable User Disk Space Used event - Select this option to enable an event to fire when a user approaches a certain amount of disk space usage.

Manage

Spool

The email spool is a list of emails, in order of when they are created, that are available for the server to send out to other mail servers or to deliver locally. SmarterMail is multi-threaded, which means that if a message cannot process out of the spool, SmarterMail simply moves on to the next message until the maximum number of threads that are designated in the administrative configurations are in use.

Administrators can use the information here to adjust threads and resources to allocate for concurrent messages.

Messages enter and leave the spool fairly quickly. In fact, some pass through so quickly that they will not display in the spool. Most messages in the spool are displayed because they are large, have many recipients, or are having trouble being sent to their final destination.

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

In general the following columns are available:

- Checkbox - Use these boxes to select multiple messages. Messages must be selected before choosing an action from the content pane toolbar.
- File Name - The filename on the hard disk.
- Spool Path - The spool the message resides in. If you have subs pools enabled, the message may be placed in one of those locations.
- Sender - The email address that initially sent the email.
- Recipients - The number of delivered/total recipients.
- Size - The total size of the message on the hard drive, in kilobytes.
- Attempts - The number of delivery attempts that have been made.
- Time in Spool - The total amount of time the message has been in the spool.
- Priority - The priority level of the message.
- Status - The current status of the message.
- Next Attempt - The date and time of the next delivery attempt.

The following actions are available from the content pane toolbar:

- Actions - Click this button and select the appropriate option to force the message, reset retries or change the priority of a message in the spool.
- Force - Pushes the message to the top of the spool. Note: The status of forced messages will not update until the server passes through the spool.
- Reset Retries - Resets the retry counts on all messages in the spool, effectively starting the delivery process over. This can be useful if a DNS or firewall problem has been recently resolved, or if you are using SmartHosting and the target server was down.
- Set Priority - Changes the priority level of a message.
- View - Click this button and select the appropriate option to view the text of a selected message or to see the list of recipients for the selected message.
- Message - Displays the text of the selected message in a new window.
- Recipients - Allows the system administrator to see who the message was sent to and the status of that message (i.e. delivered or pending).
- Delete - Clicking this button will allow the system administrator to delete messages from the spool. Note: No confirmation dialog will display, so use caution when deleting from the spool.
- Refresh - Clicking this button will allow the system administrator to update the page with the most recent contents of the spool.

Searching the Spool

Domain administrators can search for messages from particular senders in the spool. To do so, use the Search bar at the top of the content pane. Simply type in the email address of the sender and click the magnifying glass to search for any messages from that sender that are in the spool.

Spool Dashboard

The Spool Dashboard takes the headache out of spool management by allowing administrators to monitor common aspects of the email spool, including message activity, top outbound senders, top inbound domains and more. In addition to reviewing the spool activity, administrators can take action on any messages that are currently being held in the spool. For example, a sending IP address that is inundating the mail server with unwanted messages can be blocked, thereby preventing issues from becoming problems for email users.

And while monitoring the spool regularly is good practice, the dashboard is extremely helpful should the mail server become compromised. Easily spot a compromised account, block the sender and delete the unnecessary messages. The dashboard provides a real-time look at a mail server's activity, refreshing every 20 seconds, so admins always know what's going on.

To access this section, click the Manage icon and expand the Spool folder in the navigation pane. Then click on Spool Dashboard . The dashboard will load in the content pane, and the total number of messages held in the spool will be displayed in the title bar. The following sections are available:

Note: All tables, with the exception of Message Activity, sort entries based on the message count for the last 24 hours. For example, if an entry is the top sender/receiver within the last 5 minutes or hour, but 12th in the last 24 hours, they would not appear on the table.

Message Activity

This section displays the total number of messages that have been delivered by all users, including local and remote deliveries. From this table, see how many messages were sent in the last 5 minutes, last hour, last 24 hours and from the start of the installation.

Top Outbound Senders

This section displays the top 10 users with the highest number of outbound remote deliveries (for the specified time intervals). Note: The message count does not include local deliveries sent to user-to-user. The following actions can be performed on each user included in the table:

- Manage User - Select this option to impersonate the primary domain administrator that manages the user's email account. When clicked, a new window will load (logged in as the domain admin) and the user's settings will be displayed.
- Disable User - Select this option to immediately disable the user's account. This action utilizes the User Status setting found when editing a user . When a user is disabled within the Spool Dashboard, their User Status will be set to 'Disable and Allow Mail'. This prevents the user from sending outbound messages or accessing webmail; however, the mailbox will continue to receive incoming email. Enabling a user in the Spool Dashboard will adjust the setting in the user's account settings and vice versa.
- Delete Messages - Select this option to permanently delete the messages sent by the user that are currently in the spool. Note: This will only delete messages that are CURRENTLY being held in the spool.
- Move Messages - Select this option to move the messages sent by the user that are currently held in the spool to another folder on the server. Use the default path provided or enter any folder path on the server. Moving the .eml files to their own folder on the server is useful by allowing an administrator to review the messages before taking actions against them.

Note: In general, this table will display SmarterMail user accounts only. However, there may be cases where remote email addresses appear, including if: the email address is authenticated with a local account, the sending IP address is listed in the SMTP Authentication Bypass list, SmarterMail is

acting as an incoming gateway, or messages were manually dropped into the spool with sender addresses that don't exist locally. In these instances, the Manage User and Disable User actions cannot be performed.

Top Inbound Recipients

This section displays the top 10 users (local user accounts) who have received the highest number of incoming messages (for the time intervals specified). Both local and remote deliveries are included in the message count. This allows administrators to know which accounts on the server are receiving the most mail. The following actions can be performed on each user included in the table:

- Manage User - Select this option to impersonate the primary domain administrator that manages the user's email account. When clicked, a new window will load (logged in as the domain admin) and the user's settings will be displayed.
- Delete Messages - Select this option to permanently delete all of the inbound messages sent to the user that are currently in the spool. Note: This will only delete messages that are CURRENTLY being held in the spool.
- Move Messages - Select this option to move a user's inbound messages that are currently held in the spool to another folder on the server. Use the default path provided or enter any folder path on the server. Moving the .eml files to their own folder on the server is useful by allowing an administrator to review the messages before taking actions against them.

Top Inbound Senders

This section displays the top 10 email addresses that have sent the highest number of messages to users on the server (for the time intervals specified). The following actions can be performed on each email address included in the table:

- Block Inbound SMTP - Select this option to block all incoming mail sent from the email address. This action utilizes SMTP Blocking found in the Advanced Settings of the Security section. When an email address is blocked within the Spool Dashboard, an entry will be added to the SMTP Blocked list for incoming email and the entry will be denoted as having been blocked from the spool dashboard. Unblocking an email address in the Spool Dashboard will remove the SMTP Blocked entry and vice versa.
- Delete Messages - Select this option to permanently delete all inbound messages sent from the email address that are currently in the spool. Note: This will only delete messages that are CURRENTLY being held in the spool.
- Move Messages - Select this option to move all the inbound messages sent from the email address that are currently held in the spool to another folder on the server. Use the default path provided or enter any folder path on the server. Moving the .eml files to their own folder on the

server is useful by allowing an administrator to review the messages before taking actions against them.

Top Inbound IP Addresses

This section displays the top 10 IP addresses that have sent the highest number of messages to users on the server (for the time intervals specified). The following actions can be performed on each IP address included in the table:

- Blacklist IP - Select this option to block the IP address from sending messages to the server. When an IP address is blacklisted within the Spool Dashboard, an entry will be added to the Blacklist found in the Security section. The IP address will be blocked on SMTP only, and the entry will be denoted as having been blocked from the spool dashboard. Unblocking an IP address in the Spool Dashboard will remove the Blacklist entry in Security settings and vice versa.
- Delete Messages - Select this option to permanently delete all inbound messages sent from the IP address that are currently in the spool. Note: This will only delete messages that are CURRENTLY being held in the spool.
- Move Messages - Select this option to move all the inbound messages sent from the IP address that are currently held in the spool to another folder on the server. Use the default path provided or enter any folder path on the server. Moving the .eml files to their own folder on the server is useful by allowing an administrator to review the messages before taking actions against them.

Top Outbound IP Addresses

This section displays the top 10 IP addresses that have sent the highest number of outbound, remote deliveries (for the time intervals specified). The following actions can be performed on each IP address included in the table:

- Blacklist IP - Select this option to block the IP address from sending messages to the server. When an IP address is blacklisted within the Spool Dashboard, an entry will be added to the Blacklist found in the Security section. The IP address will be blocked on SMTP only, and the entry will be denoted as having been blocked from the spool dashboard. Unblocking an IP address in the Spool Dashboard will remove the Blacklist entry in Security settings and vice versa.
- Delete Messages - Select this option to permanently delete all outbound messages sent from the IP address that are currently in the spool. Note: This will only delete messages that are CURRENTLY being held in the spool.
- Move Messages - Select this option to move all the outbound messages sent from the IP address that are currently held in the spool to another folder on the server. Use the default path

provided or enter any folder path on the server. Moving the .eml files to their own folder on the server is useful by allowing an administrator to review the messages before taking actions against them.

Top Inbound Domains

This section displays the top 10 domains that have sent the highest number of messages to users on the server (for the time intervals specified). The following actions can be performed on each domain included in the table:

- Block Inbound SMTP - Select this option to block all incoming mail sent from the domain. This action utilizes SMTP Blocking found in the Advanced Settings of the Security section. When an domain is blocked within the Spool Dashboard, an entry will be added to the SMTP Blocked list for incoming email, and the entry will be denoted as having been blocked from the spool dashboard. Note: This action does not block on the EHLO Domain. Instead, it uses the Email Address field and enters only the domain. Unblocking a domain in the Spool Dashboard will remove the SMTP Blocked entry and vice versa.
- Delete Messages - Select this option to permanently delete all inbound messages sent from the domain that are currently in the spool. Note: This will only delete messages that are CURRENTLY being held in the spool.
- Move Messages - Select this option to move all the inbound messages sent from the domain that are currently held in the spool to another folder on the server. Use the default path provided or enter any folder path on the server. Moving the .eml files to their own folder on the server is useful by allowing an administrator to review the messages before taking actions against them.

Spam Quarantine

System administrators can quarantine outgoing messages that have been flagged as spam by SmarterMail's spam checks for a maximum of 30 days. Quarantining such messages allows administrators to investigate why certain messages are blocked as spam and make appropriate adjustments, if necessary. In addition, system administrators can easily resend any outgoing messages that should not have been quarantined.

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

- Checkbox - Use these boxes to select multiple messages. Messages must be selected before choosing an action from the content pane toolbar.
- File Name - The filename on the hard disk.
- Date - The date the message was flagged for quarantine.
- Sender - The email address that initially sent the email.
- Recipients - The total number of recipients.
- Size - The total size of the message on the hard drive, in kilobytes.
- Time In Quarantine - The amount of time the message has been quarantined.
- Time of Removal - The amount of time until the message is automatically removed from quarantine and permanently deleted.

The following actions are available from the content pane toolbar:

- Actions - Click this button and select the appropriate option to resend a quarantined message.
- Resend - Moves the selected message(s) to the spool for delivery to its intended recipients.
- View - Click this button and select the appropriate option to view the text of a selected message or to see the list of recipients for the selected message.
- Message - Displays the text of the selected message in a new window.
- Recipients - Allows the system administrator to see who the message was sent to.
- Delete - Clicking this button will allow the system administrator to delete messages from quarantine.
- Refresh - Clicking this button will allow the system administrator to update the page with the most recent quarantined spam messages.

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

Virus Quarantine

System administrators can quarantine outgoing messages that have been flagged as containing viruses by SmarterMail's ClamAV or the Cyren Zero-hour Antivirus add-on for a maximum of 30 days.

Quarantining such messages allows administrators to investigate false positives and make appropriate adjustments or notify the developer of the virus scanner, if necessary.

To view a list of quarantined virus messages, click the manage icon and expand the Spool folder in the navigation pane. Then click Virus Quarantine . A list of messages currently under quarantine because

they were flagged for a virus by SmarterMail antivirus measures will load in the content pane and the following columns will be available:

- Checkbox - Use these boxes to select multiple messages. Messages must be selected before choosing an action from the content pane toolbar.
- File Name - The filename on the hard disk.
- Date - The date the message was flagged for quarantine.
- Sender - The email address that initially sent the email.
- Recipients - The total number of recipients.
- Size - The total size of the message on the hard drive, in kilobytes.
- Time In Quarantine - The amount of time the message has been quarantined.
- Time of Removal - The amount of time until the message is automatically removed from quarantine and permanently deleted.

The following actions are available from the content pane toolbar:

- View - Click this button and select the appropriate option to view the text of a selected message or to see the list of recipients for the selected message.
- Message - Displays the text of the selected message in a new window.
- Recipients - Allows the system administrator to see who the message was sent to.
- Delete - Clicking this button will allow the system administrator to delete messages from quarantine.
- Refresh - Clicking this button will allow the system administrator to update the page with the most recent quarantined virus messages.

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

User Activity

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

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

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

- User - The name of the user.
- Type - The connection type. For example, IMAP or webmail.

- IP Address - This will tell the IP address of the user.
- Start Date - The start date and time of the connection.
- Duration - The length of the connection.

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

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

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

Inactive Users

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

Viewing inactive users is a good way to clean out users for a domain that are no longer needed.

Perhaps these users and their mailboxes can be archived or copied and moved to another location to recover some disk space.

Current Migrations

Use this section to manage the mailbox migrations currently taking place.

Current Migrations

SmarterMail's Mailbox Migration tool makes it easy for users to switch email providers by giving them the ability to import emails, contacts, calendars, tasks, and notes to SmarterMail from most third-party mail servers.

That being said, users can do this on their own, with little input from a SmarterMail system administrator. While this normally is not an issue, there are times when a system administrator may need to help a migration along - or even stop it altogether. That's where the Current Migrations page comes in.

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

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

- User - The name of the user performing the migration.
- Status - The status of the migration being performed. The status displayed will be one of the following:
 - Queued - The migration was initiated and is waiting to start.
 - In Progress - The migration was started and is currently processing.
 - Completed - The migration is finished for that user.

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

- End Session - End the selected user's migration. The migration will be stopped, regardless of where it is in process. As mailbox migrations are an "all or nothing" proposition, if a migration is stopped in the middle, none of the migration steps will be finalized unless the migration shows as "Completed."
- Refresh - Refreshes the list of current mailbox migrations and their status.

Current Connections

SmarterMail will monitor the server and see who is connecting via the different syncing protocols, including SMTP, IMAP, POP, XMPP and ActiveSync. System administrators can then use this section to blacklist a certain user if they believe too many connections are being made. Current connections can be viewed all at once or separated by protocol.

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

Regarding connections that appear to last longer than they should, this could be due to a number of reasons. For example, SMTP connections that stay active for hours could be due to multiple people connecting from behind a firewall. These people all appear to connect from a single IP, but they're actually individual connections, one for each user. The firewall simply portrays the connections as being from a single source. Another thing to note is an "anonymous" connection. An "anonymous" user is someone who has created a session without logging in. For instance, if they hit the login page and don't actually log in, that will create a new session marked as anonymous. You can get a large number of these if a search engine attempts to index your site or if you have an uptime service monitoring your login page.

Current IDS Blocks

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

SMTP, IMAP, POP, LDAP, XMPP, Webmail or for potential email harvesting abuse. System admins can view a list of blocked IPs by abuse type or view all blocked connections at one time.

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

Mass Messaging

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

Send Email

To send a mass email, click the manage icon . Then expand Mass Messaging in the navigation pane and click Send Email . The mass messaging options will load in the content pane and the following fields should be completed:

- From - The individual sending the email message. "System Administrator" will be entered as a default.
- To - Select the message recipients from the list. Note: If All Users on a Domain is chosen, you will then be asked to enter the domain name. If you choose Specific User you will be asked to enter a Specific User's email address.
- To Friendly Name - This is a friendly name or description for the recipients that will appear in conjunction with their email address in the To field. For example, if you're sending an email to all users of the domain example.com you could use something like "Example.com User - "
- Subject - The subject of the email.
- Message - Type the text of the message in this field. Messages can be in plain text or stylized with HTML formatting.

Once you complete all the fields, click the Send in the content pane toolbar to send the message.

Send Reminder

Reminders are a quick and easy way to send a follow-up to a previous, more detailed and stylized mass message. For example, if you send a message to all users of a domain about some upcoming

maintenance work on the mail server, you can use use Send Reminder to do a quick follow up reminding the users of the scheduled work.

To send a reminder, click the manage icon . Then expand Mass Messaging in the navigation pane and click Send Reminder . The mass messaging options will load in the content pane and the following fields should be completed:

- To - Select the message recipients from the list. Note: If All Users on a Domain is chosen, you will then be asked to enter the domain name. If you choose Specific User you will be asked to enter a Specific User's email address.
- Subject - The subject of the email.
- Message - Type the text of the message in this field.

Once you complete all the fields, click the Send in the content pane toolbar to send the message.

Services

System administrators can use this section to enable and/or disable specific services on the mail server. Generally, all of these services should be enabled. However, there are cases where a system administrator will want to disable one or more. For example, a web host or ISP may want to limit users' access to incoming mail to POP only when they connect with an email client in order to conserve disk space on the mail server. In this case, the system administrator would want to stop the IMAP services. Another example would be a mail administrator for a large corporation who doesn't want users to add multiple email accounts and therefore read and reply to email from personal accounts as well as their corporate accounts. In this case, the administrator would want to disable the IMAP Retrieval and POP Retrieval services.

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

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

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

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

Services

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

- IMAP - A client/server protocol in which email is received and held by the mail server. IMAP requires continual access to the client during the time that it is working with the mail server.
- IMAP Retrieval - With IMAP retrieval, mail is retrieved from external IMAP servers (e.g., another mail server like GMail) and saved in a mailbox on the mail server.
- Indexing - Indexes messages, contacts, calendars, tasks and notes so that users can search for specific mailbox items via the Web interface.
- LDAP (Enterprise Edition Only) - A communication protocol for accessing online directory services. Programs like Outlook and Thunderbird use LDAP to retrieve contact lists from SmarterMail. SmarterMail will validate email addresses for user accounts, aliases, and mailing lists.
- POP - An email protocol in which mail is saved in a mailbox on the mail server. When the end user reads the mail, it is immediately downloaded to the client computer and is no longer maintained on the mail server.
- POP Retrieval - Similar to IMAP Retrieval, with POP retrieval, mail is retrieved from external POP3 servers and saved in a mailbox on the mail server.
- SMTP - A TCP/IP (Internet) protocol used for sending and receiving e-mail. However, since it's limited in its ability to queue messages at the receiving end, it's usually used with one of two other protocols, POP or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP or IMAP for receiving messages from their local server.
- Spool - The internal message queue used to deliver messages locally and to remote services.
- SyncML - An open synchronization technology that is most commonly used to synchronize mail account data (calendars, contacts, etc.) between a mail server and a mobile device.
- XMPP (Enterprise Edition Only) - An open-source IM protocol designed to allow interoperability between different IM client programs. SmarterMail uses this protocol to power its chat functionality in the Web interface and/or third-party chat clients.

View Logs

System administrators can use this section to quickly view the server's log files. Viewing a server's log files, especially when it's possible to narrow down the type of server action or protocol that is being viewed, allows system administrators to look for any specific errors that could cause reliability issues on the server or narrow down reasons why a specific behavior is being seen. For example, system

administrators can review SMTP logs to see if an email was delivered or check ActiveSync logs to see if they can narrow down synchronization issues between a specific user's mailbox and their mobile device.

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

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

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

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

Message Archive Search

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

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

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

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

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

For more information on archiving, see [Message Archiving](#).

Impersonate

There are times when you will need to access domain or user specific information. SmarterMail uses impersonation to accomplish this goal, causing a separate window to login automatically as the domain administrator or a user. This can be a useful method to examine settings or diagnose a problem.

To impersonate a user, click the Manage icon and then click Impersonate in the navigation pane. A modal window will display asking for the email address that you would like to impersonate. Clicking OK will open a new tab in which you will be impersonating the user. From there, you may edit user settings, content filters, or whatever other part of the account that needs to be changed. Closing the tab will end the impersonation. In addition, when managing/impersonating a domain, an Impersonate button is available within the Users grid for quick impersonation. (To impersonate a domain, enter the domain administrator's email address. Alternatively, you can impersonate a domain by clicking the Domains icon, selecting the domain in the navigation pane and choosing to Manage the domain.)

Indexing Status

SmarterMail Search Indexing allows users to instantly find any files -- including messages, attachments, appointments, contacts, tasks, or notes -- in their mailbox. Following the initial scan of the server, SmarterMail continually monitors each user's mailbox for changes and updates the index accordingly. This method of indexing reduces server utilization while increasing the speed with which search results are returned.

System administrators can use this section to view the status of SmarterMail Search Indexing. Viewing the status of indexing can be beneficial when troubleshooting a problem. For example, if the mail service seems to be using a large amount of CPU, the system administrator can check to see if the cause of the temporary increase in CPU usage is due to indexing.

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

Password Policy Compliance

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

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

- Checkbox - Use these boxes to select multiple users. Users must be selected before choosing an action from the content pane toolbar.
- User - The username that is non-compliant.
- Domain - The domain on which the user exists.
- Name - The display name of the user that is non-compliant.
- Violations - The number of password requirements that are not being met.
- Auto Block SMTP Status - This column is used to display the SMTP status of the user. It will show “Blocked” if the user’s SMTP has already been blocked or a date of when the user will be blocked. At times, “N/A” may appear if the block has not yet been determined as this is processed once per day. Note: This column will only display if the “Disable outgoing SMTP when auto-block grace period ends” setting is enabled.

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

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

Restore

System administrators can use the Restore page to restore a user’s emails, email folders or their entire user account. This can be extremely useful if a folder or email is mistakenly deleted or if there is corruption within the mailbox.

To restore user data, click the Manage icon then Restore in the navigation pane. The following options will be available in the content pane:

- Type - Select the type of restore that you would like to perform:

- Attach User - Select this option to attach a user that is on disk but not in the domain. In other words, to restore an entire user's account. Note: The user's folder needs to be correctly placed in the domain folder on the server prior to performing this action.
- Attach Folder - Select this option to attach a folder that is on disk but not in the account. In other words, to restore a user's email folder.
- Rebuild Folder - Select this option to copy .grp files or .eml files into an existing user's folder and have SmarterMail re-build that folder to include the new .grp and .eml files. In other words, to restore a user's emails.
- Email Address - The full email address of the user account being restored.
- Folder Path - The path of the folder within the Web interface that will be used to rebuild or restore an email folder. For example, if you're restoring a subfolder that was created under the Inbox, the folder path would look like: Inbox\Example Folder.
- Recursive - Check this box to attach any subfolders that are found within a folder that is being attached or rebuilt.

Note: There could be a UID conflict issue if you restore .grp files into an existing folder with existing .grp files. If you are only restoring email messages, it is recommended that you create a new folder within the SmarterMail interface and copy the .grp and/or .eml files to that new folder. Then use the Rebuild Folder function. This issue would not occur when restoring .eml files into an existing folder with existing email.

Reports

Reports Overview

System administrators, domain administrators, and individual users can use real-time mail server statistics, historical summary reporting, and detailed trend analysis at the system, domain, and user levels to understand the performance of their systems. With dozens of pre-defined reports, SmarterMail provides critical statistics that help system and domain administrators monitor their systems.

For more information, see the Reports folder of the Help for Users section of the online help.

Settings

General Settings

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

Server Info

Use this tab to specify the following server settings:

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

Login Display

Small businesses using SmarterMail on their own servers, or even companies using SmarterMail from their hosting provider, will benefit from the ability to customize the SmarterMail login page to add a company logo, provide additional branding text, or simply adjust the default "Log into SmarterMail" text to be more in line with an overall brand message. Note: System Administrators can allow Domain Administrators to override the custom login screen by editing the Domain, clicking on the Features tab and checking Login Display Customization.

Use this tab to adjust the SmarterMail login display settings:

- Custom Help URL - Entering a full URL in this field will add a custom button to the Help menu that users can access in the SmarterMail interface. Administrators can link to a variety of things, including server-specific instructions for syncing, help resources, contact information, etc.
- Enabled - Check this box to enable the custom help URL in the Help menu.
- Custom Help Text - The hyperlink text for the custom URL in the Help menu.
- Custom Login Text - Use this field to adjust the default "Log into SmarterMail" text with something more in line with an overall brand message.

- Enabled - Check this box to enable the Custom Login Text.
- Company Logo - Upload a company logo by dragging and dropping a file in the highlighted area or clicking to browse for a file (max file size of 3mb). Uploading a logo using this upload control will host the image publicly on the server and enter the tag in the HTML section. Note: Uploading an image here alone will NOT display the image on the login screen. The HTML must remain in the Login Page HTML section. This upload control can be used by those who don't have their logo publicly hosted or who wish the image source to point back to their mail server. Furthermore, regardless of the image uploaded, the image's source URL will remain the same; only one image may be hosted at a time.
- Favicon - A favicon is an icon that is associated with a URL and displayed in a browser's address bar or next to the site name in a bookmark list. Upload a favicon by dragging and dropping a file in the highlighted area or clicking to browse for a file. Click Save and refresh the page to view the favicon that has been uploaded. Note: Recommended sizes for a favicon are 32x32, 64x64 or 128x128 pixels. On upload, the image will be converted to a 32x32 .ico image.
- Enable custom login page HTML - Check this box to enable the ability to use HTML to further modify the login screen to add additional text or adjust the layout. This is used in conjunction with the Login Page HTML section below.
- Login Page HTML - Enter the custom HTML that will be used to further modify the login screen (in-line custom CSS can be used as well). Note: To include white space around the company logo, the div id "companyinfo" must be included.

The following options are available in the content pane toolbar:

- Save - Saves the custom login display settings.
- Preview - Opens a new popup window displaying what the current settings render on the login screen. If this window remains open, live changes can be seen as settings are adjusted.

Spool

Use this tab to specify the following spool settings:

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

secondary service to interact with the message. By default, the delivery delay is 1 second.

- **Retry Intervals** - When the mail server is unable to contact the receiving server, the email attempting to be sent is held for a period of time before the mail server attempts to resend it. This is the time between retries. Users can specify multiple retry attempts to resend emails before it is bounced. By default, this is set to 4 attempts - at 15 min, 30 min, 60 min, and 90 min intervals.
- **Bounce DNS errors after** - The maximum number of attempts SmarterMail should make before the message is bounced due to a DNS error. The most common cause of a DNS error is a misspelled domain. Limiting the number of attempts before DNS errors are bounced is beneficial because messages will not sit in the queue for long periods of time taking up processing on the mail server and possibly slowing the system down. This will be helpful to users because messages will be bounced sooner and will give users the opportunity to fix any mistakes and get a message resent. By default, the server will make 2 attempts. Note: Setting this at 1 retry can be dangerous if the DNS server fails or if there is a loss of Internet connectivity. To disable this feature, set the number of bounces equal to the number of retry intervals.
- **Notify senders of delay after** - Sets the number of delivery attempts before the sender is notified that the email delivery is delayed. This can be beneficial as it lets the sender know that the mail server is still attempting to deliver the message but that the recipient has not received it yet. (Default value is 0.)
- **Command-Line File** - Enable this and enter the full path to an executable you wish to use to process incoming messages. Use %filepath as an argument to pass the path of the email file to the executable. It is allowable for the executable to delete the message to prevent delivery. Example: If you set this field to "c:\program files\myexe.exe %filepath", the program myexe.exe will be launched with the full path to the spool file as its first argument. Note: The command will not be executed if the Enabled box is not checked.
- **Command-Line Timeout** - The number of seconds that the server will wait for information from the remote server. By default, the timeout is set to 5 seconds.

Reports

Use this tab to specify the following settings:

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

Indexing

Use this tab to specify the following settings:

- Max Threads - The maximum number of threads to use for search indexing. Increasing this value will cause SmarterMail to use more CPU, but will allow the system to simultaneously index more users. (Default value is 1.)
- Segment Count Before Optimizing - The number of segment counts in an index before the index is reorganized. Increasing this number will increase file counts per mailbox, but will use less CPU. (Default value is 20.)
- Items Before Garbage Collection - The number of indexed items across the server before freeing as much memory as possible. Increasing this number will increase memory usage and lower CPU usage. (Default value is 5000.)
- Items to Index Per Pass - The number of items to index per user per index attempt. Increasing this number will increase memory usage and decrease the time it takes to index one user. However, it will increase the length of time it takes to index many small users if there are a few large users. (Default value is 2500.)
- Seconds In Queue Before Indexing - The amount of time a user must be in the indexing queue before being indexed. This setting provides a buffer for many changes to a mailbox to ensure the same user is not indexed multiple times. Increasing this number will cause search results to be delayed further, but will result in indexing heavier users less frequently. (Default value is 5.)
- Deleted Items Before Optimizing - The number of items that will be removed from the index before an optimization will occur. Increasing this number will slow search results. Decreasing this number will increase CPU and disk usage, but will increase search result speed. (Default value is 1000.)

System Administrators

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

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

Creating New System Administrators

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

Options

Use this tab to specify the following settings:

- Username - The identifier used to login to SmarterMail.
- New Password - The password used to login to Smartermail.
- Confirm Password - Re-type the password used to login to Smartermail.
- Description - A brief description of the administrator. For example, "for support department".
- Enable login access by IP address - Select this option to only allow system administrators to login from certain IP addresses.
- Allow Impersonation and Domain Management - There are times when an administrator may need to access domain or user specific information. SmarterMail uses impersonation to accomplish this goal, causing a separate window to login automatically as the domain administrator or user. Select this option to allow secondary system administrators the ability to impersonate user accounts and domains.

Login Access

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

Protocol Settings

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

POP

Use this tab to specify the following POP settings:

- POP Banner - The text that is displayed when initially connecting to the port. The banner supports the use of the following variables, which will be replaced with their corresponding values:
 - #HostName# - The hostname of the IP address to which the connection is made.
 - #ConnectedIP# - The IP address of the remote computer.
 - #Time# - The system's local time.

- #TimeUTC# - The time in UTC.
- #UnixTime# - The number of seconds since January 1, 1970.
- Command Timeout - If the server receives a command that sends large amounts of data but the data stops coming in for this number of minutes, the command will be aborted. By default, the command times out after 5 minutes.
- Max Bad Commands - After this many unrecognized or improper commands, a connection will be automatically terminated. By default, the maximum number of bad commands is 8.
- Max Connections - Some protocols in SmarterMail allow you to specify the maximum number of connections. Increasing this value allows SmarterMail to handle more connections of that type at once, but results in higher CPU and memory utilization. By default, the maximum number of connections is 500.
- POP Retrieval Download Path - The path in which mail is stored from POP accounts until it is read.
- Max POP Retrieval Threads - SmarterMail is multi-threaded, meaning it can do more than one thing at a time. This setting is for the maximum number of threads you want SmarterMail to work on concurrently for retrieving mail using the POP protocol. By default, the maximum number of POP retrieval threads is 10.
- POP Retrieval Interval - The frequency by which SmarterMail checks for new POP messages. By default, the POP retrieval interval is 1 minute.
- Autodiscover Host - The URL of the mail server (e.g., mail.domain.com) to be returned by an auto discover query.
- Autodiscover Port - The port to autodiscover uses to communicate with the mail server.
- SSL - Check this box to enable autodiscover to use SSL. NOTE: Autodiscover generally requires the use of SSL, especially when used with Microsoft Outlook.

IMAP

Use this tab to specify the following IMAP settings:

- IMAP Banner - The text that is displayed when initially connecting to the port. The banner supports the use of the following variables, which will be replaced with their corresponding values:
 - #HostName# - The hostname of the IP address to which the connection is made.
 - #ConnectedIP# - The IP address of the remote computer.
 - #Time# - The system's local time.
 - #TimeUTC# - The time in UTC.
 - #UnixTime# - The number of seconds since January 1, 1970.
- Command Timeout - If the server receives a command that sends large amounts of data but the

data stops coming in for this number of minutes, the command will be aborted. By default, the command times out after 15 minutes.

- Max Bad Commands - After this many unrecognized or improper commands, a connection will be automatically terminated. By default, the maximum number of bad commands is 8.
- Max Connections - Some protocols in SmarterMail allow you to specify the maximum number of connections. Increasing this value allows SmarterMail to handle more connections of that type at once, but results in higher CPU and memory utilization. By default, the maximum number of connections is 1000.
- IMAP Retrieval Download Path - The path in which mail is stored from IMAP accounts until it is read.
- Max IMAP Retrieval Threads - The maximum number of threads you want SmarterMail to work on concurrently. By default, the maximum number of POP retrieval threads is 10.
- IMAP Retrieval Interval - The frequency by which SmarterMail checks for new IMAP messages. By default, the IMAP retrieval interval is 10 minutes.
- Autodiscover Host - The URL of the mail server (e.g., mail.domain.com) to be returned by an auto discover query.
- Autodiscover Port - The IMAP port returned when autodiscover communicates with the mail server. System administrators can modify this port as needed to accommodate firewall settings, etc.
- SSL - Check this box to enable autodiscover to use SSL. NOTE: Autodiscover generally requires the use of SSL
- Enable IDLE Command - Select this checkbox to enable IMAP IDLE. IMAP idle is an extension of the IMAP protocol that allows a mail server to send status updates in real time. Through IMAP IDLE, users can maintain a connection with the mail server via any mail client that supports IMAP IDLE, allowing them to be instantly aware of any changes or updates. When enabled, SmarterMail will inform any connecting IMAP client that it accepts the IDLE command. Note: IMAP clients that do not fully support IMAP IDLE, like Microsoft Outlook, may use the command in such a way that it actually hinders performance.

LDAP

Use this tab to specify the following LDAP settings:

- Session Timeout - After a connection fails to respond or issue new commands for this number of seconds, the connection will be closed. By default, the session times out after 300 seconds.
- Command Timeout - If the server receives a command that sends large amounts of data and the data stops coming in for this number of seconds, the command will be aborted. By default, the command times out after 120 seconds.

SMTP In

Use this tab to specify the following incoming SMTP settings:

- **SMTP Banner** - The text that is displayed when initially connecting to the port. The banner supports the use of the following variables, which will be replaced with their corresponding values:
 - #HostName# - The hostname of the IP address to which the connection is made.
 - #ConnectedIP# - The IP address of the remote computer.
 - #Time# - The system's local time.
 - #TimeUTC# - The time in UTC.
 - #UnixTime# - The number of seconds since January 1, 1970.
- **Allow Relay** - If you are concerned about spam mailers using the relay function to send mail through your server or do not want any other mail server to use your SMTP server as a gateway, set this to Nobody (recommended). However, you can set the type of relays you will allow, should you so desire.
 - Nobody - Restricts sent mail to only work via SMTP authentication and with accounts on the local SmarterMail Server (except for IPs on the White List).
 - Only Local Users - Limits relay access to users (email accounts) for a valid domain on your SmarterMail Server.
 - Only Local Domains - Limits relay access only to mail hosts (domains) on your SmarterMail Server.
 - Anyone - Allows any other mail server to pass messages through your mail server, increasing the chances of your mail server being used for sending large volumes of messages with domains not associated with your local mail server. Selecting this option turns off statistics for all domains, due to the high amount of messages that are passed through the mail server with an open relay.
- **Session Timeout** - After a connection fails to respond or issue new commands for this number of seconds, the connection will be closed. By default, the session times out after 15 minutes.
- **Enabled** - Select this checkbox to enable the session timeout setting.
- **Command Timeout** - If the server receives a command that sends large amounts of data but the data stops coming in for this number of seconds, the command will be aborted. By default, the command times out after 120 seconds.
- **Max Bad Commands** - After this many unrecognized or improper commands, a connection will be automatically terminated. By default, the maximum number of bad commands is 8.
- **Max Connections** - Some protocols in SmarterMail allow you to specify the maximum number of connections. Increasing this value allows SmarterMail to handle more connections of that

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

- Max Hop Count - After a message gets delivered through this many mail servers, it is aborted by the software. This prevents looping due to DNS problems or misconfigurations. By default the max hop count is 20.
- Max Message Size - Messages greater than this size will be rejected by the mail server. By default, the max message size is 0 (unlimited).
- Max Bad Recipients - At times, spammers will hammer a domain with a dictionary harvesting attack. This means that software is used to send messages to many of the most common mailbox addresses (e.g., admin, user, contact, etc.) or username variations (e.g., alan@, alana@, alanb@, etc.) in order to find valid email addresses. Setting the max bad recipients means that after this many bad recipients (those that don't exist for the domain), the SMTP session will be terminated. This setting allows you to better protect yourself against email harvesting attacks. A value of 20 is recommended in most cases.
- Append Received Line - Select the option for appending the received line for all messages, only for SMTP Authenticated messages or for no messages at all.
- Require Auth Match - Select this to force a user's From: address to match their SMTP authenticated address, either by matching the entire email address or by matching just the domain - or not requiring it at all. This setting helps keep senders from spoofing email addresses through email clients.
- Max Messages Per Session - The maximum number of messages that can be sent in one session. This is useful in handling cases where spammers will make one connection and then send a large amount of messages with that connection.
- Autodiscover Host - The URL of the mail server (e.g., mail.domain.com) to be returned by an auto discover query.
- Autodiscover Port - The SMTP In port returned when autodiscover communicates with the mail server. System administrators can modify this port as needed to accommodate firewall settings, SMTP restrictions by ISPs, etc.
- SSL - Check this box to enable autodiscover to use SSL. Note: Autodiscover generally requires the use of SSL.
- Enable VRFY command - Select this checkbox to allow others (including other mail servers) to verify an email address on the server. Note: Some people believe enabling VRFY commands is a security risk, so be sure to research the possible ramifications before enabling this feature.
- Enable EXPN command - Select this checkbox to allow others to list all users associated with an alias or list. Note: Some people believe enabling EXPN commands is a security risk, so be sure to research the possible ramifications before enabling this feature.
- Allow relay for authenticated users - Select this checkbox to enable the "Allow Relay" setting

from above when users are required to use SMTP Authentication for sending messages.

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

SMTP Out

Use this tab to specify the following outgoing SMTP settings:

- Outbound IPv4 - The IPv4 address used to connect to external SMTP servers when a message is sent by the domain. If multiple IPv4 IPs are on the server, they will be listed in the dropdown.
- Outbound IPv6 - The IPv6 address used to connect to external SMTP servers when a message is sent by the domain. If multiple IPv6 IPs are on the server, they will be listed in the dropdown.
- Enable Primary IP on failure - Select this checkbox to have SmarterMail automatically fall back to the primary IP when a failure has occurred. SmarterMail will only attempt to connect once if this option is enabled.
- Command Timeout - If the server receives a command that sends large amounts of data but the data stops coming in for this number of seconds, the command will be aborted. By default, the command times out after 60 seconds.
- Max Spam Check Threads - The maximum number of messages that can be spam checked at one time. By default, the maximum spam check threads is 30.
- Max Delivery Threads - The maximum number of messages that can be sent at one time to email addresses that are not on the local server. If a message cannot be sent, the SmarterMail server's multi-threading capabilities will move on to the next message and eventually get back to the one it skipped. This action can save tremendous amounts of time when compared to some other mail servers that stall the spool if a message cannot be sent right away. By default, the max delivery threads is 50.
- Enable DNS Caching - Select this checkbox to cache the results of DNS calls in SmarterMail. This can help speed up delivery of messages.
- Enable TLS if supported by the remote server - Select this checkbox to use TLS (SSL encryption) if the server you are connected to supports it.
- Append authenticated as header for outgoing messages - Checking this box means that outgoing messages will have a new line item in the message header called "x-smartermail-authenticatedas" that demonstrates that the message sender was verified using SMTP

authentication. This header can then be used by anti-spam services for validation.

- Enable Remote Bounces - Select this checkbox to enable bounce messages from all senders.

When unchecked, bounce messages are restricted to only internal senders. Note: This setting is enabled by default.

XMPP

Use this tab to specify the following XMPP settings:

- Max Connections - Some protocols in SmarterMail allow you to specify the maximum number of connections. Increasing this value allows SmarterMail to handle more connections of that type at once, but results in higher CPU and memory utilization. By default, the maximum number of connections is 1000.
- Web Chat URL Listeners - The URLs that XMPP services should listen to in order to ensure live chat connections are made. Examples include "http://+:80/http-bind/" or "https://+:443/http-bind"

EWS

- Modification Auto Clean - SmarterMail records when an account syncs using Exchange Web Services and stores those sync sessions in a file. This setting tells SmarterMail how long to keep those sync sessions before they are automatically purged from the file.
- Autodiscover Host - The URL of the mail server (e.g., mail.domain.com) to be returned by an auto discover query when Exchange Web Services are enabled.

EAS

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

Log Settings

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

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

Log Files

Use this tab to specify the following settings:

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

- Compress Log Files After - The number of days after which log files are automatically compressed. This preserves existing log files but also saves server space.
- Enabled - Select this option to allow log files to be compressed after a specific number of days.
- Delete Log Files After - The number of days after which log files are automatically deleted.
- Enabled - Select this option to allow log files to be deleted after a specific number of days.

Log Detail Levels

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

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

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

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

- ActiveSync - The log level for Exchange ActiveSync connections.
- Administrative - The log level for for any changes and/or modifications made by system administrator accounts.
- Delivery - The log level for message delivery and spool operations.
- Events - The log level for event sessions.
- EWS - The log level for Exchange Web Services sessions.
- IMAP - The log level for IMAP sessions.
- IMAP Retrieval - The log level for IMAP retrieval sessions.
- Indexing - The log level for SmarterMail indexing.
- LDAP - The log level for LDAP sessions.
- Mailbox Importing - The log level for data imported during mailbox migrations.
- Maintenance - The log level for maintenance tasks performed by SmarterMail.
- Message-ID - The log level for logging Message-ID's of all messages sent to mailing lists.
- POP - The log level for POP sessions.
- POP Retrieval - The log level for POP retrieval sessions.
- SMTP - The log level for SMTP sessions.
- SyncML - The log level for SyncML sessions.
- WebDAV - The log level for CalDav and CardDav sessions.

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

ActiveSync Mailboxes

This feature is only available in SmarterMail Enterprise.

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

System administrators will use this section to enable and disable the EAS add-on for mailboxes across all domains on the SmarterMail server. Domain administrators will use this page to manage the EAS add-on for their particular domain. Note: Before an administrator can configure a mailbox to sync using ActiveSync, the add-on needs to be activated and available for users of the domain. For more information, please refer to the KB article [Activate Microsoft Exchange ActiveSync](#). Furthermore, domain administrators will only see this section available when the system administrator has enabled ActiveSync User Management for their domain.

To access this section as the System Administrator, click the Settings icon and click ActiveSync Mailboxes in the navigation pane. To access this section as the Domain Administrator, click the Settings icon , expand the Domain Settings folder and click ActiveSync Mailboxes in the navigation pane. A list of accounts for which the Exchange ActiveSync add-on is enabled will load in the content pane.

In general, the following columns are available:

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

The following options are available from the actions toolbar:

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

Personalization

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

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

Settings

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

- Use default settings - Selecting this will use as the default personalization settings.
- Override Settings - Selecting this activates the Colors and Custom CSS tabs and allows users to customize those settings.
- Enable users to override - This is a domain administrator only setting. Selecting this option will allow end users to modify the custom CSS and general color scheme for their webmail login.
- Skin - This dropdown will list any skins developed for SmarterMail. In general, the Default skin will always be available, but others may appear in this list as well.

Colors

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

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

Custom CSS

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

To modify a style, you should first use a Web browser like Chrome to inspect the element that you want to modify. (Using FireFox's Firebug plug-in will work as well). By inspecting the element you will see the class used and any styles associated with the class. You can then create a version of that

style yourself, and then paste it in the box to override the default. Realize this will happen wherever that style is used, so changing one style can affect several pages within the interface. To enable the custom styles, simply check the Enabled box on the Custom CSS tab.

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

System Messages

SmarterMail sends a variety of automated email messages for certain actions within SmarterMail. For example, system messages are sent to users when their password has expired or is in violation. Administrators can modify certain messages sent out from the server to make them match a company's voice and style, add extra information or add a standard From address.

To access this section, click the Settings icon and click System Messages in the navigation pane. A list of adjustable system messages will load in the content pane.

In general, the following columns are available:

- Name - The friendly name of the system message.
- Subject - The subject of the email.
- Display Name - The friendly name or description of the sender that will appear in conjunction with the From address (if included) in the From field of the email.
- From Address - By default, system messages send from "System Administrator" without a From address. Administrators can add a From address to allow users to respond to system messages or to decrease the likelihood a message will be caught by spam filters.

The following option is available from the actions toolbar:

- Edit - Select this option to edit the selected system message.

Events

Events Overview

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

Notification Profiles

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

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

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

The following columns are available:

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

The following options are available from the content pane toolbar:

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

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

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

Bindings

IP Addresses

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

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

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

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

Note: The IP Addresses listed in this section are pulled from the server and can only be removed from SmarterMail by removing the IP Address from the Network Interface Card (NIC).

Ports

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

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

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

Creating New Ports

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

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

Hostnames

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

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

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

Defaults

Domain Defaults

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

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

Technical

Use this tab to specify the following technical settings:

- Folder Path - The directory in which all information (XML files, mail statistics, alias information, etc.) pertaining to the domain is saved. By default this is C:\SmarterMail. However, it can be modified as needed.
- Auto-Responder Exclusions - To prevent SmarterMail from sending automated messages, such as out-of-office replies, to addresses based on the spam level of the original message, select the appropriate option from the list.
- Forwarding Exclusions - To prevent the system from forwarding messages based on the spam level of the message, select the appropriate option from the list.
- TLS - To enable or disable TLS (SSL encryption) for outgoing mail, select the appropriate option from the list.
- SRS - To enable or disable SRS (the ability for the mail server to re-write the senders email address so that forwarded messages pass SPF checks) for mail, select the appropriate option from the list.
- Calendar Auto Clean - Use this to set a time frame that SmarterMail will use to automatically remove legacy calendar items from users' calendars. This setting can also be managed by domain administrators.
- Require SMTP Authentication - Select this option to require SMTP authentication when sending email. Note: If this option is enabled, users must provide an email address and password to send email from their account. SmarterMail supports cram-md5 and login authentication methods.
- Restrict auto-responders to once per day per sender - Select this option to limit how frequently an auto-responder is sent. Continually sending something like an out-of-office reply to the same address every time an email comes in can cause abuse issues. Therefore, it is recommended that this be set for all domains.
- Disable greylisting - Select this option to disable the greylisting anti-spam option for the domain. Greylisting, though effective, can lead to a delay in email delivery for a domain.
- Allow users to opt out of LDAP listings - Select this option to allow users to remove themselves from the Global Address List.
- Exclude IP from received line - Select this option to remove the client's IP address from the received header on messages received through SMTP. Note: Removing the IP address from the

received header is not recommended because it violates RFC.

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

Features

Use this tab to enable or disable the following features:

- ActiveSync Remote Wipe - Select this to allow users with the Exchange ActiveSync add-on to have access to SmarterMail's remote wipe functionality.
- ActiveSync User Management - Select this to allow domain administrators add and delete mailboxes that can use the Exchange ActiveSync add-on. Note: The option to limit the number of ActiveSync mailboxes allotted for the domain can be found on the Limits tab.
- Calendar - Select this option to allow users to use the calendar feature.
- Catch-All Alias - Select this option to allow users to create catch-all email addresses. When enabled, this setting can be managed by domain administrators as well.
- Connected Services - Select this option to allow users to connect different services to their SmarterMail accounts to facilitate actions like attaching links to shared files.
- Contacts - Select this option to allow users to use the contacts feature. When enabled, this setting can be managed by domain administrators as well.
- Content Filtering - Select this option to allow users to use content filtering. When enabled, this setting can be managed by domain administrators as well.
- Control of Service Access - Select this option to give domain administrators the ability to manage access to POP, IMAP, SMTP and webmail services for users.
- Disposable Addresses - Select this option to allow users to create a temporary, disposable address independent of their email address.
- Domain Aliases - Select this option to allow domain administrator to create domain aliases. When enabled, this setting can be managed by domain administrators as well.
- Domain Chat History View - Select this option to allow domain administrators to be able to search through all chat history for any and all users of a domain.
- Domain Reports - Select this option to provide additional reports for domain administrators.
- Enable spam filtering - Select this option to show or hide the spam filter settings for domain administrators. Hiding the spam filter settings will prevent domain administrators from changing the weights set by the system administrator for spam checks.
- Email Reports - Select this option to provide the ability to email reports.
- Exchange Web Services (EWS) - Select this option to enable users on the domain to synchronize SmarterMail with supported email clients using Exchange Web Services. Note: For domains that will support inboxes with large volumes of email, IMAP is encouraged as the primary protocol as EWS does not perform well with large amounts of email.

- File Storage - Select this option to allow users to use the file storage feature. When enabled, this setting can be managed by domain administrators as well.
- IMAP Retrieval - Select this option to allow users to download IMAP email from third-party mail servers. When enabled, this setting can be managed by domain administrators as well.
- Live Chat (XMPP) - Select this option to allow users on the domain to chat with each other via the Web interface or any XMPP-compatible chat client. When enabled, this setting can be managed by domain administrators as well.
- Login Display Customization - Select this option to allow domain administrators to customize the login screen to add a company logo, provide additional branding text, or adjust the default “Login to SmarterMail” text.
- Mailing Lists Select this option to allow domain administrators to create and use mailing lists to send mass emails. When enabled, this setting can be managed by domain administrators as well.
- Mail Signing - Select this option to enable email verification via mail signing using DKIM. When enabled, this setting can be managed by domain administrators as well.
- Notes - Select this option to allow users to use the notes feature. When enabled, this setting can be managed by domain administrators as well.
- POP Retrieval - Select this option to allow users to download POP email from third-party mail servers. When enabled, this setting can be managed by domain administrators as well.
- SMTP Accounts - Select this option to allow users to send email from a third-party mail server account right from within SmarterMail. When enabled, this setting can be managed by domain administrators as well.
- SyncML - Select this option to allow users to sync SmarterMail with Outlook, Thunderbird and most smartphones using SyncML.
- Tasks - Select this option to allow users to use the tasks feature. When enabled, this setting can be managed by domain administrators as well.
- User Reports - Select this option to provide reports for users.

Limits

Use this tab to specify the following limits:

- Disk Space - The maximum number of megabytes allocated for the domain. By default, the domain is allocated 500 MB of disk space. This disk space limit also includes file storage for users. Note: When this limit is reached, SmarterMail will send a warning to the domain administrator and mailboxes on the domain will not be able to receive new mail.
- Domain Aliases - The maximum number of domain aliases allowed for the domain. A domain alias acts as a secondary domain that users can use for sending and receiving emails. By default, domains are limited to two domain aliases.

- Users - The maximum number of mailboxes allowed for the domain. By default, domains are limited to 100 users. Note: If your SmarterMail license limits the number of mailboxes allowed on the domain, your license level will override this setting.
- User Aliases - The maximum number of alias email accounts (forwarded to a true email account) allowed for the domain. By default, domains are limited to 1,000 user aliases.
- Mailing Lists - The maximum number of mailing lists allowed for the domain. By default, this setting is unlimited.
- Mailing List Max Message Size - The maximum size message that can be sent to a mailing list. By default, the maximum message size is unlimited.
- Enable domain to override - Check this option to allow domain administrators to specify the maximum size for mailing list messages.
- POP Retrieval Accounts - The maximum number of POP email accounts a user can set up in SmarterMail. By default, users can receive download messages for 10 POP email accounts.
- IMAP Retrieval Accounts - The maximum number of IMAP email accounts a user can set up in SmarterMail. By default, users can receive download messages for 10 IMAP email accounts.
- Max Message Size - The maximum size email a user can send. By default, the max message size is 10,000 KB. Note: This number includes text, HTML, images and attachments.
- Recipients per Message - The maximum number of recipients a message can have. By default, users can send messages to 200 email addresses.
- ActiveSync Accounts - Sets the maximum number of Microsoft Exchange ActiveSync accounts a domain can have set up. Note: This setting is used in conjunction with the ActiveSync User Management setting on the Features tab.

Sharing

This tab is only available in SmarterMail Enterprise edition.

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

- Global Address List - Select this option to allow users on a domain to see all user profiles on the domain and participate in LDAP queries against the domain. When enabled, domain administrators can manage this feature as well.
- Shared Calendars - Select this option to allow calendars to be shared with other users on the domain. When enabled, domain administrators can manage this feature as well.
- Shared Contacts - Select this option to allow contact lists to be shared with other users on the domain. When enabled, domain administrators can manage this feature as well.
- Shared Folders - Select this option to allow email folders to be shared with other users on the domain. When enabled, domain administrators can manage this feature as well.
- Shared Notes - Select this option to allow notes to be shared with other users on the domain.

When enabled, domain administrators can manage this feature as well.

- Shared Tasks - Select this option to allow task lists to be shared with other users on the domain. When enabled, domain administrators can manage this feature as well.

Priority

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

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

- Standard Messages - The priority level for messages that don't have another priority affecting it, as detailed below.
- Mailing Lists - The priority level for messages sent to a mailing list.
- Priority When Over Size - The priority level for messages that exceed the message size threshold. For example, system administrators may want to lower the priority of large messages to avoid slowing down the spool.
- Message Size Threshold - The maximum size a message can be without triggering the Priority When Over Size rule.
- Auto-Responders - The priority level for auto-responder messages, such as out-of-office responses.
- Bounces - The priority level for non-delivery receipts.
- Email Reports - The priority level for email reports.
- Appointment Reminders - The priority level for messages reminding users of upcoming appointments, meetings or events.
- Priority After Attempt 1 - The priority level for messages that were not successfully sent after the specified number of tries.
- Attempt 1 Threshold - The number of retry attempts the system should make before the priority set in Priority After Attempt 1 is assigned to the message.
- Priority After Attempt 2 - The priority level for messages that were not successfully sent after the specified number of tries.
- Attempt 2 Threshold - The number of retry attempts the system should make before the priority set in Priority After Attempt 2 is assigned to the message.

Throttling

This tab is only available in SmarterMail Enterprise edition.

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

Use this tab to edit the following throttling settings:

- Outgoing Messages per Hour - The number of messages sent by the domain per hour. By default, the number of outgoing messages is 5,000.
- Message Throttling Action - The action SmarterMail should take when the message throttling threshold is reached.
- Outgoing Bandwidth per Hour - The total number of MBs sent by the domain per hour. By default, the outgoing bandwidth is 100.
- Bandwidth Throttling Action - The action SmarterMail should take when the bandwidth throttling threshold is reached.
- Bounces Received per Hour - The number of non-delivery receipts a domain can receive per hour. By default, a domain can receive 1,000 bounces per hour.
- Bounces Throttling Action - The action SmarterMail should take when the bounces throttling threshold is reached.

Event Restrictions

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

Alias

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

Collaboration

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

Email

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

type.

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

Mailing List

- Enable Mailing List Added event - Select this option to enable the Mailing List Added event type.
- Enable Mailing List Deleted event - Select this option to enable the Mailing List Deleted event type.
- Enable Message Sent to Mailing List event - Select this option to enable the Message Sent to Mailing List event type.
- Enable Mailing List Bounce Removal event - Select this option to enable the Mailing List Bounce Removal event type.
- Enable Mailing List Subscribe event - Select this option to enable the Mailing List Subscribe event type.
- Enable Mailing List Unsubscribe event - Select this option to enable the Mailing List Unsubscribe event type.

Throttling

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

User

- Enable User Added Event - Select this option to enable an event type for when a new user is added to a domain.
- Enable User Deleted event - Select this option to enable an event type for when a new user is deleted from a domain.
- Enable User Changed Password event - Select this option to enable an event type for instances where users change their passwords.
- Enable User Changed Forward event - Select this option to enable an event type for instances where users change the forwarding address they have set up for their account.
- Enable User Disk Space Used event - Select this option to enable an event to fire when a user approaches a certain amount of disk space usage.

Domain Propagation

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

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

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

User Defaults

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

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

User Propagation

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

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

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

Routing

Forwarding Blacklist

The Forwarding Blacklist is a useful tool for preventing issues with companies that have extremely strict spam policies. For example, AOL and Comcast do not differentiate between the sending server and the server that forwarded a spam message, and as such, they commonly blacklist legitimate domains for forwarding spam. Because it's impossible to prevent ALL spam messages from being forwarded when a user has automated forwarding enabled, administrators may prefer to blacklist email forwarding to those strict domains.

Note: The Forwarding Blacklist only prevents the automated forwarding of email, which is configured in the user's general settings. Any messages that are manually forwarded from the Email section itself will bypass this blacklist.

To access the Forwarding Blacklist, click the Settings Icon . Then expand the Routing folder and click Forwarding Blacklist in the navigation pane. A list of blacklists will load in the content pane.

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

- Domain Name - Enter the name of the domain that should be blocked from automated email forwarding. When a domain is included in this list, users will see the following notification when they attempt to save a forwarding address with that domain: "Forwards to the following address(es) are not allowed: _____. Note: Users will still be able to manually forward emails to users on that domain.

Outgoing Gateway

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

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

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

Options

Use this tab to specify the following settings:

- Server Address - The IP address of the gateway server.
- Port - The port used to connect to the gateway server. By default, the port is 25.
- Auth Username - The username of the gateway server given to you by your ISP.
- Auth Password - The password for your gateway server.
- Encryption - Select the type of encryption from the list.
- Priority Range - The priority range for this server. System administrators can use gateway

servers to only send mails with a certain priority level. For example, gateways can be used only for lower priority messages, such as newsletters or messages over a certain size, to reduce load and free up processing on the primary mail server. Note: This feature is only available in SmarterMail Enterprise.

- Enable SmarterMail gateway mode - Select this option to indicate that the outgoing gateway server is another SmarterMail server.
- Description - A friendly name or brief description of the gateway.

SmarterMail Gateway

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

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

Incoming Gateways

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

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

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

Options

Use this tab to specify the following settings:

- Gateway Mode - The function that the incoming gateway will perform. If the incoming gateway is set to backup MX, it will only receive messages when your primary server is down. If the incoming gateway server is set to domain forwarding, it will receive all messages and forward them to your primary server.
- IP Address / IP Range - The IP address, or range of IP addresses, of the primary mail server.
- User Verification - The method used by the incoming gateway to determine if a user is valid or

not. Note: If none is selected, the incoming gateway server will accept all email addresses for the domain. If Web service is selected, the incoming gateway will check with the primary mail server for a list of valid email addresses.

- Enable SmarterMail Gateway Mode - Select this option to indicate that the incoming gateway server is another SmarterMail server.
- Disable Greylisting - Select this option to disable greylisting for the domain.

Domains

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

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

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

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

Spam

Use this tab to specify the following spam checks:

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

SmarterMail Gateway

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

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

Sender Priority Overrides

This feature is only available in SmarterMail Enterprise.

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

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

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

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

Storage

File Storage

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

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

Options

Use this tab to specify the following settings:

- Max File Size - The maximum size a file can be in order to be uploaded to the server.
- Root URL - The base URL of any file stored and shared in file storage. By default, the base

URL corresponds to the domain the mail server is set up on (i.e., <http://mail.example.com>). If SmarterMail is configured on an external IP that allows a network address translation (NAT) to an external IP, the system administrator may need to modify the root URL.

Extension Blacklist

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

Folder Auto-clean

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

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

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

Options

Use this tab to specify the following options:

- Allow domains to override auto-clean settings - Select this option to allow domain administrators to create their own auto-clean policies.
- Allow users to auto-clean inbox - Select this option to allow users to create auto-clean policies on the Inbox folder.

Rules

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

These options will be visible if size is chosen:

- Folder Size Before Auto-clean - The maximum size of the folder. Once the folder reaches this size, the auto-clean process is started and older messages (messages that were received the longest time ago) are deleted.
- Folder Size After Auto-clean - The goal size of the folder. When auto-cleaning, SmarterMail will delete older messages until the folder reaches this size. Note: This number should always be

lower than the "before" number.

- Enable auto-clean for this folder - Select this box to activate auto-cleaning of the selected folder.

These options will be visible if date is chosen:

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

Message Archiving

This feature is only available in SmarterMail Enterprise edition.

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

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

When archiving is set up, messages are automatically archived as soon as they hit the spool and before they are handled by any spam and/or content filters. This means that all messages are archived, not simply those that are delivered to a user's mailbox. (The exception to this rule is messages rejected due to SMTP Blocking. If a message is rejected due to SMTP Spam blocking, it will never hit the spool and, therefore, will not be archived.) On a nightly basis, SmarterMail zips up archived messages and stores them to conserve disk space on the mail server. However, zipped messages are still searchable.

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

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

- Domain - The domain on the SmarterMail server to be archived.
- Archive Path - The directory on the hard drive in which archived messages are saved.

- Rule - Choose to save none of your messages, all messages, only incoming messages or only outgoing messages.

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

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

Advanced Settings

Configuring SmarterMail for Failover

Who Should Use This

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

Failover Overview

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

Understanding How Failover Works

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

If the primary server fails, SmarterMail can be configured to automatically enable the secondary server. When this occurs, the secondary server takes over responsibility for processing background

threads and supporting all email functionality. This server will remain in active status until another failure occurs or the primary mail server comes back online.

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

Minimal System Requirements

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

Adding Network Load Balancing to Your Servers

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

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

Configuring the Load Balanced Cluster for Use with Failover

- Navigate to Start -> Administrative Tools -> Network Load Balancing Manager
 - Click the Cluster menu item and select New
 - In the New Cluster: Connect window, type the IP of your primary server in the Host: text box and select New
 - When the Interface Name and Interface IP appear, select the Interface Name and click Next
 - Since this is the primary node, ensure the host Priority is set to 1
 - In the New Cluster: Host Parameters window, confirm the IP address and Subnet mask are correct and change the initial host state to Stopped . This is to prevent any issues with connectivity if a machine randomly reboots or suffers from a hardware failure. If all nodes are set to Started for their initial host state, traffic will be split between the two (or more) machines.
- Note: Monitoring software can be used to execute scripts that will start and stop hot standbys in

the event of a failure and recovery. If you are not executing scripts via monitoring software then all failover will need to be handled manually.

- Click Next
- In the New Cluster: Cluster IP Addresses window, click Add and enter in your cluster IP address and the same subnet mask as in Step 6
- Select Next
- In the New Cluster: Cluster Parameters window, confirm the IP address and subnet mask, then enter a Full Internet Name , though this is optional
- Ensure the cluster operation mode is set to Multicast
- Click Next
- In the New Cluster: Port Rules window, click Edit
 - If you want you can restrict the cluster IP to work on an individual port or across a port range. You can also simply allow the cluster IP to work across all ports on the server
- Ensure your port rules are set to Single Host in the Filtering Mode section
- Click OK
- Verify your settings and click Finish to complete the setup

Joining Additional Nodes to the Cluster

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

rules, click Edit . Otherwise, click Finish to complete the setup

- Wait for the nodes to converge and, if necessary, stop the secondary sever by right clicking the second server's name, select Control Host -> Stop

Configure a Shared Service Directory

- Using Network File Sharing (NFS) or Samba (SMB), create a shared directory named SmarterMail , preferably on a NAS or SAN. NOTE: We recommend that this shared directory be hosted on a server that utilizes a RAID 10 configuration for the data.
 - Inside that new SmarterMail folder, create a Service folder
 - Configure your permissions accordingly. If special permissions are required, configure the SmarterMail service to run with the proper credentials within the Windows Services console.
- Note: When performing updates to the software, the credentials will need to be re-applied to the service

Configuring a Fresh Installation of SmarterMail for Failover

- Install SmarterMail Enterprise on a server. This will be your hot standby. Leave all setup information as the default settings and after setup is complete, configure SmarterMail as an IIS site.
- Stop the SmarterMail service on the hot standby
- Edit the failoverConfig.xml file in the primary server's Service folder as follows:

 - SharedSystemFilePath - Set to the shared network shared system folder
 - FailoverIPAddress - Set this to the IP address of the Network Load Balancer
 - IsEnabled - Set this to True
 - Save this file, then copy it to the hot standby's Service folder and replace the existing failoverConfig.xml
 - Copy over all folders, DAT and XML files from C:\Program Files (x86)\SmarterTools\SmarterMail\Service to the Service folder in the shared service directory you created
 - Start the service on the hot standby server and verify that the paths are pointing to the network shared paths
 - Activate your Enterprise key on the hot standby by logging into SmarterMail's management interface as the system admin and going to Settings -> Activation -> Licensing , then stop the SmarterMail service on the server
 - Start the service on the primary server, then reactivate your Enterprise license key in the SmarterMail management interface
 - After re-activating the license, go to Settings -> Bindings -> IP Address and bind all the ports to the load balancer's IP address and make sure no other IPs have any ports bound to them

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

Adding Failover to an Existing Installation of SmarterMail

Note: You will need to configure both servers for Network Load Balancing and set up a shared service directory. See the steps outlined in the Adding Network Load Balancing to Your Servers , Configuring the Load Balanced Cluster for Use with Failover , Joining Additional Nodes to the Cluster and Configure a Shared Service Directory sections earlier in this document for more information.

- Ensure the primary server is running the latest version of SmarterMail and that it is also configured as an IIS site. Ensure the IIS binding is pointing to your cluster IP address
- Install SmarterMail on a hot standby and configure it as an IIS site. Ensure the cluster node is stopped on the hot standby and ensure the IIS binding is also pointing to the cluster IP
- Stop the SmarterMail service on the hot standby
- Copy all of your mail data (located in C:\SmarterMail\ by default) to your shared service directory. If possible, use robocopy to do this because it will not result in any downtime for the mail service
- Once robocopy finishes, run it one more time. This second pass will only copy any new data
- Stop the SmarterMail service on the primary server
- Edit the failoverConfig.xml file in the primary server's Service folder as follows:
 - SharedSystemFilePath - Set to the shared network shared system folder
 - FailoverIPAddress - Set this to the IP address of the Network Load Balancer
 - IsEnabled - Set this to True
- Run the robocopy one more time to copy over any modified files and remaining spool e-mails
- Copy over all folders, DAT and XML files from C:\Program Files (x86)\SmarterTools\SmarterMail\Service to the Service folder in the shared service directory you created
- Edit the domainlist.xml file in the shared Service folder and change the path of your domains to match the new NFS\SMB path. (For example, \\NAS01\SmarterMail\Domains\mydomain.com)
- Edit the mailconfig.xml file and replace any instances of the old physical path's with your new network location for SmarterMail. (For example, if all of your data was hosted on E:\Smartermail, you would then perform a find and replace for all instances of E:\Smartermail to \\NAS01\Smartermail).
- On the primary server, go to Start -> Administrative Tools -> Network Load Balancing Manager and stop the cluster node, then start the NLB on the secondary node

- Start the SmarterMail service on the hot standby
- Access SmarterMail's web interface at the cluster IP and sign in as the system admin
- Activate your Enterprise key on the hot standby by going to Settings -> Activation -> Licensing
- Verify that the data and settings are being picked up from the shared Service directory
- Stop the SmarterMail service on the hot standby and stop the secondary cluster node
- Start the cluster node and the SmarterMail service on the primary server
- Sign into the web interface on the primary server and re-activate the Enterprise license key by going to Settings -> Activation -> Licensing
- Verify mail data and settings are being accessed from the shared service directory

Scripting Failover

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

Prepping PowerShell on the Servers

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

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

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

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

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

$StartSecondary = New-PSSession -ComputerName Server02 Invoke-Command -Session $StartSecondary -ScriptBlock { Import-Module NetworkLoadBalancingClusters ; Start-nlbclusternode -HostName Server02 -InterfaceName "WAN" ; set-service -computerName Server02 -name mailservice
```

```
-status running ; import-module WebAdministration ; start-webapppool
SmarterMail ; remove-psession Server02 }
```

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

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

```
$StopSecondary = New-PSSession -ComputerName Server02 Invoke-Command -
Session $StopSecondary -ScriptBlock { Import-Module
NetworkLoadBalancingClusters ; Stop-nlbclusternode -HostName Server02 -
InterfaceName "WAN" ; import-module WebAdministration ; stop-webapppool
SmarterMail; set-service -computerName Server02 -name mailservice -status
stopped ; remove-psession Server02}

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

Message Footer

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

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

Options

Use this tab to specify the following settings:

- Enable footer for all messages - Select this option to turn on the message footer for all incoming and outgoing messages.
- Apply to mailing lists - Select this option to append the message footer to mailinglist messages. Note: Mailing lists have their own configurable footers, so enabling this option will append a second footer at the end of each message. Because this may be confusing for mailing

list moderators and recipients, most administrators will choose to keep this option disabled.

- Enable domains to override footer settings - Select this option to allow domain administrators to configure their own message footer for the domain.

Footer

Use this tab to create the message footer text. Admins can use the HTML-based editor to create footers that seamlessly fit into any email message. Note: The message footer does not support the use of variables.

Automation with Web Services

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

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

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

Activation

Licensing

System administrators can use this area to view licensing information,

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

The following options are available from the content pane toolbar:

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

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

SmarterMail Self Diagnostic

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

Security

Antispam Administration

SmarterMail comes equipped with a number of antispam features and functions that allow you to be as aggressive as you want when combatting spam. Initial antispam settings were configured during installation, but these settings can be modified at any time. Without having to add any third-party measures, SmarterMail's antispam features can rid mail servers of up to 97% of all spam just using the standard configuration when it's installed.

Due to the flexible nature of SmarterMail's antispam setup, spam checks can influence the spam decision as much or little as you want. When spam protection runs on a particular email, all enabled spam checks are performed on the email. The total weight of all failed tests is what comprises the spam weight for the email. A spam probability level is then assigned to the email using the settings in the Filtering tab and an action is taken on that message based on its total spam weight.

An added benefit to SmarterMail's Antispam Administration is the ability to combat both incoming and outgoing spam messages. Most mail servers only allow system administrators to keep spam from entering the mail server. SmarterMail helps protect mail users from incoming spam but also includes

the added benefit of keeping mail servers from actually sending spam, thereby helping to protect the mail servers from being blacklisted.

To view the antispam settings for your server, click the Security icon and then click Antispam Administration in the navigation pane. The antispam settings will load in the content pane and the following tabs will be available:

Spam Checks

Use this tab to select the spam options that you want to enable for filtering (a point-based weighting system for filtering spam) and for blocking at the SMTP level. Weights can also be edited for the various checks from this tab. Note: Only enabled spam checks are used when calculating spam weight. To enable or disable a check, select the appropriate spam check by checking the box next to it and click Save .

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

- Save - Select this option to preserve any changes made to the spam check.
- Actions - Select an appropriate action from the list:
 - Wizard - Select this option to open the Getting Started Wizard in a new tab for quick spam setting adjustments. Note: Only the Spam Profiles and Security options will be displayed.
 - Import Spam Settings - Select this option to import the spamConfig.xml file for quick spam setting adjustments. This option allows administrators to easily share spam configurations across all installations within their infrastructure. Note that when importing spam configurations, all existing rules will be replaced with the rules in the imported XML.
 - Export Spam Settings - Select this option to export the spamConfig.xml file from the server files. This option allows administrators to easily share spam configurations across all installations within their infrastructure.
- Add RBL - Select this option to create an RBL spam check.
- Add URIBL - Select this option to create a URIBL spam check.
- Edit - Checkmark a spam check from the list and select this option to adjust its settings.
- Delete - Select this option to permanently remove the spam check.

The following columns are available for each spam check:

- Spam Check - The name of the spam check available.
- Avg. Time - The average time, in milliseconds, that the spam check takes to process.
- Weight - The weight range available for the spam check.
- Enable for Filtering - When checked, the weight assigned for the spam check is added to the message and used as part of its overall spam score. SmarterMail then handles the message based

on the spam settings created for a domain.

- Enable for Incoming SMTP blocking - Checking this box enables the spam check for SMTP blocking of incoming emails. If N/A is listed, then that particular spam check relies on content filtering and does not offer SMTP blocking. As SMTP blocks are done at the IP level and not based on message content, some spam checks do not offer SMTP blocking.
- Enable for Outgoing SMTP blocking - Checking this box enables the spam check for SMTP blocking of outgoing emails. If N/A is listed, then that particular spam check relies on content filtering and does not offer SMTP blocking. As SMTP blocks are done at the IP level and not based on message content, some spam checks do not offer SMTP blocking.

The following types of spam checks are available by default. In most cases, selecting the desired spam check and clicking Edit will allow you to set any properties associated with the check.

Custom Rules

Email can be assigned spam weights based on the header, body text or raw content of a message. For example, the system administrator can create a rule that assigns a specific spam weight to all messages containing the word "viagra" in the body text. To configure weights for custom body rules, complete the following fields:

- Rule Name - The name of the rule.
- Rule Source - What you want the rule to be based on: a message's header, body text or raw content. Note: If you select Header you will need to supply header details separately from the Rule Text .
- Rule Type - The type of rule you use to evaluate the text for a match. Rule types are contains, wildcard or regular expression.
- Weight - The amount to add to the email message's spam weight.
- Rule Text - The text that triggers the custom body rule.

Cyren Premium Antispam

The Cyren Premium Antispam add-on uses Recurrent Pattern Detection 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 Cyren Detection Center analyzes large volumes of Internet traffic in real time, recognizing and protecting against new spam outbreaks the moment they emerge. For more information, or to purchase this add-on, visit the SmarterTools website .

- Confirmed Weight - The weight that will be assigned if the Cyren Detection Center determines the message as coming from known spam sources.
- Bulk Weight - The weight that will be assigned if the Cyren Detection Center determines the message as sent in bulk. Note: Newsletters or mailing list messages may be included in this

classification.

- Suspect Weight - The weight that will be assigned if the Cyren Detection Center suspects the message may be spam because it was sent to a slightly larger than average distribution.
- Unknown Weight - The weight that will be assigned if the Cyren Detection Center is unable to determine the spam probability of a message. This should be treated similarly to a None Weight.
- None Weight - The weight that will be assigned if the Cyren Detection Center deems the message as not spam.

Declude

Declude integration allows you to use Declude products in conjunction with the SmarterMail weighting system. Declude addresses the major threats facing networks, and are handled by a multi-layered defense. Configuration of Declude is done through the Declude product, so all you need to do in SmarterMail is enable the spam check and the Declude score will be included when calculating the total spam weight of a message. For more information, visit www.declude.com.

- Low Spam Weight - The weight that will be assigned if Declude determines a low probability of spam.
- Medium Spam Weight - The weight that will be assigned if Declude determines a medium probability of spam.
- High Spam Weight - The weight that will be assigned if Declude determines a high probability of spam.

DomainKeys and DKIM

DomainKeys and DKIM are an email authentication system designed to verify the DNS domain of an email sender and the authenticity of a message. While a possible source for determining whether an email is spam or not, neither is universally adopted so any weights assigned for failing these checks should be minimal. In addition, because the DomainKey method has become obsolete; we recommend utilizing DKIM instead.

- Pass Weight - Indicates that the email sender and message integrity were successfully verified (less likely spam). The weight you set may be 0 (for no effect) or a negative number, thereby reducing the spam rating.
- Fail Weight - Indicates that the email sender and message integrity verifications failed (most likely spam). Set this to a relatively high weight, as the probability that the email was spoofed is very high.
- None Weight - Indicates that there was not a valid DomainKey/DKIM signature found to validate the sender and message integrity. Except in very special circumstances, leave this set to 0.

- Max message size to sign - The maximum outgoing message size you want the mail server to sign. By default this is set to 0, meaning all outgoing messages are signed.
- Max message size to verify - The maximum incoming message size you want the mail server to verify.
- Max key size allowed - Select the level of security you want used to sign each message. Default is set to 1024 bits. Setting this value higher may increase the CPU load on your mail server.

Message Sniffer

The Message Sniffer add-on is an intelligent antispam scanner that uses advanced pattern recognition and collaborative learning technologies to accurately identify spam, scams, viruses, and other email borne malware before it gets to a user's mailbox. For more information, or to purchase this add-on, visit the SmarterTools website .

- Confirmed Weight - The weight that will be assigned if Message Sniffer determines the message as coming from known spam sources.
- None Weight - The weight that will be assigned if Message Sniffer deems the message is not spam.

RBL Lists (Real-Time Blacklists)

RBL lists (also known as IP4R Lists) and URIBL lists are publicly accessible lists of known spammer IP addresses. These lists can be a very important part of spam protection. To attach a list click either Add RBL or Add URIBL in the content pane toolbar. Dependent on the list you're adding, the following settings are available:

- Name - A friendly name for the list that will help you and your customers identify it.
- Description - This field allows you to store additional information about the list.
- Weight - The default weight for this spam check. If an email sender is listed with the spam list, this is the value that will be added to the message's total spam weight.
- Max Weight - The maximum weight that a single URIBL check can add to the message.
- Hostname - The hostname of the RBL.
- Required Lookup Value(s) - The expected value(s) returned from an RBL if the sender's IP is listed with the RBL provider. Note: Multiple lookup values may be entered, separated by a comma.
- Enable bitmap checking - Select this checkbox if the RBL supports bitmapping. Bitmap checking can be used for RBLs and URIBLs that support this kind of spam check. For example, SURBL utilizes a multi-blacklist check. For more information and documentation on the appropriate usage, please visit www.surbl.org/lists .

Remote SpamAssassin

SpamAssassin itself is a powerful, third party open source mail filter used to identify spam that can be easily used alongside SmarterMail. It utilizes a wide array of tools to identify and report spam. By default, SpamAssassin will run on 127.0.0.1:783. For more information, or to download SpamAssassin, visit spamassassin.apache.org.

SmarterMail can use SpamAssassin with its weighting system:

- Low Spam Weight - The weight that will be assigned if SpamAssassin determines a low probability of spam.
- Medium Spam Weight - The weight that will be assigned if SpamAssassin determines a medium probability of spam.
- High Spam Weight - The weight that will be assigned if SpamAssassin determines a high probability of spam.
- Client Timeout - The timeout that SmarterMail will impose on a server if it cannot connect.
- Max Attempts per Message - The number of times SmarterMail will attempt to acquire a SpamAssassin score for an email.
- Failures Before Disable - The number of times a remote SpamAssassin server can fail before it is disabled.
- Disable Time - The length of time before the SpamAssassin server is re-enabled.
- Header Log Level - The amount of information SpamAssassin inserts into the header of the message

Reverse DNS (Domain Name Server)

Reverse DNS checks to make sure that the IP address used to send the email has a friendly name associated with it.

- Weight - The default weight for this spam check. If an email sender does not have a reverse DNS entry, this is the value that will be added to the message's total spam weight.

SmarterMail's SpamAssassin-Based Pattern Matching

SmarterMail includes a proprietary pattern matching engine built upon the SpamAssassin technology as part of the default installation of the product. It includes a number of spam detection techniques, including DNS-based and fuzzy-checksum-based spam detection, Bayesian filtering and more.

- Low Spam Weight - The weight that will be assigned if the pattern matching engine determines a low probability of spam.
- Medium Spam Weight - The weight that will be assigned if the pattern matching engine determines a medium probability of spam.

- High Spam Weight - The weight that will be assigned if the pattern matching engine determines a high probability of spam.
- Header Log Level - The amount of information the pattern matching engine inserts into the header of the message.

SPF (Sender Policy Framework)

SPF is a method of verifying that the sender of an email message went through the appropriate email server when sending. As more and more companies add SPF information to their domain DNS records, this check will prevent spoofing at an increasing rate.

- Pass Weight - Indicates that the email was sent from the server specified by the SPF record (more likely good mail). The weight you set may be 0 (for no effect) or a negative number, thereby reducing the spam rating.
- Fail Weight - Indicates that the email was sent from a server prohibited by the SPF record (highly likely spam). Set this to a relatively high weight, as the probability that the email was spoofed is very high.
- SoftFail Weight - Indicates that the email was sent by a server that is questionable in the SPF record. This should either be set to 0 or a low spam weight.
- Neutral Weight - Indicates that the SPF record makes no statement for or against the server that sent the email. Except in very special circumstances, leave this set to 0.
- PermError Weight - Indicates that there is a syntax error in the SPF record. Since SPF is relatively new, some domains have published improperly formatted SPF records. It is recommended that you leave this at 0 until SPF becomes more widely adopted.
- None Weight - Indicates that the domain has no published SPF record. Since SPF is relatively new, many legitimate domains do not have SPF records. It is recommended that you leave this at 0 until SPF becomes more widely adopted.

Filtering

Emails are filtered into one of three categories based on their total weight: Low Probability, Medium Probability and High Probability. If a weight is equal to or higher than a certain category, then it is assigned that probability of being spam. Use the Default Action option to define the weight thresholds and the default actions at each level. Note: Users can override these settings if you permit them to.

- Weight Threshold - The email is sorted into probability levels based on the weight threshold values.
- Default Action - The action to take when a message ends up with this probability.
- Text to Add - This is the text that will be displayed when a message reaches a particular level of spam.

SMTP Blocking

This tab allows you to set up extra spam checks that block emails at delivery if a certain amount of spam checks fail. Use the Enabled checkbox to enable a particular SMTP block. Note: Messages rejected due to SMTP blocking do not hit the spool and, therefore, will not be included in the message archive, if enabled.

- Incoming Weight Threshold - Enable this and an incoming email must score this value or higher in order to be blocked. The score is established by the settings on the Spam Checks tab. (Default is 30)
- Greylist Weight Threshold - Enable this and an incoming email must score this value or higher to be greylisted. (Default is 30)
- Outgoing Weight Threshold - Enable this and an outgoing email must score this value or higher in order to be blocked. The score is established by the settings on the Spam Checks tab. (Default is 30)
- Outgoing Quarantine - The amount of time to quarantine blocked SMTP messages.

Options

This tab contains options relating to the processing of spam and the ability for individual domains to override system-level settings.

- Auto Responders - Allows you to restrict what types of automated responses are permitted for the system. Certain anti-spam organizations are starting to block those servers that auto-respond to spam traps. To reduce the possibility of this occurring, set the auto-respond option to be as restrictive as your clients will permit.
- Content Filter Bouncing - As with auto-responses, certain anti-spam organizations also blacklist those servers that send bounce messages back to spam trap accounts. SmarterTools recommends setting this option to be as restrictive as your clients will allow.
- Max message size to content scan - The maximum message size for which content-based spam checks will run. Content-based spam checks include the SpamAssassin-based Pattern Matching Engine, remote SpamAssassin, Cyren Premium Antispam, and custom rules. Note: Increasing this number will also increase the mail server's memory usage.
- Allow domains to override filter weights and actions - Many domain administrators have their own opinions on what spam checks work best for their domain. Enable this to allow them to override the spam options if they wish.
- Enable bounces for outgoing SMTP blocking - Enable this to give a user a notification when a mail message has not been sent due to spam.
- Enable spool proc folder - Enable this to have SmarterMail place messages into this folder to

be analyzed in the background. While the messages are in the Spool Proc folder, .hdr can manipulate elements of the message, such as edit, write, and add headers. Once the scan has been completed, the message will be placed back into the spool and handled by SmarterMail from that point on.

- Disable spam filtering on SMTP whitelisted IP addresses - Disables antispam processing and zeroes the spam weight on whitelisted IPs.
 - Enable catch-all accounts to send auto-responders and bounce messages - Enable this if you rely on auto-responders being sent when a message comes in through a catch-all. In general, this is a bad idea, so it should be left unchecked unless your situation specifically requires it.
 - Enable SRS when forwarding messages - Enable this to allow the mail server to re-email (as opposed to "forward") an email message so that it passes any SPF checks on the recipient's end.
 - Enable DMARC policy compliance check - Enable this to allow the mail server to check messages against the DMARC policy standard. For more information, see the DMARC website
- .

Bypass Gateways

This tab gives administrators the ability to enter an IP Address or an IP Range of an incoming gateway. SmarterMail will analyze the .EML file and pull the most recent IP Address from the header which will usually be an organizations incoming gateway. By inputting that IP Address on this page will allow SmarterMail to analyze the IP of the originating server rather than focusing on the gateway that SmarterMail received the message from. This is important because the majority of the time an organizations incoming gateway will not be listed on any RBL lists, but the originating server may be.

To add an IP Address or IP Range, click the Add IP icon from the Actions toolbar.

Antivirus Administration

SmarterMail's default installation includes, at no additional cost, effective and self-updating antivirus protection with ClamAV. In addition, SmarterMail can support additional third-party solutions that include a quarantine directory as well as support for command-line antivirus solutions. SmarterMail has the ability to check the quarantine directory and respond to users that attempted to send an email containing a virus.

To view the antivirus settings for your server, click the security icon and then click Antivirus Administration in the navigation pane. The antivirus settings will load in the content pane and the following tabs will be available:

Options

- Virus Quarantine - Allows you to specify the amount of time you want to quarantine any detected viruses.
- Enable ClamAV - Select this checkbox to enable ClamAV.
- Enable real-time AV - Select this checkbox to enable virus checking in real-time.
- Enable command-line AV - Select this checkbox to enable a command-line virus scanner.
- Enable Cyren zero-hour antivirus - Select this checkbox to enable the Cyren Zero-hour Antivirus add-on.

ClamAV

Clam AntiVirus is a third-party open source antivirus toolkit, designed especially for scanning email on mail gateways. ClamAV is included at no additional cost in the default installation of SmarterMail. For more information on ClamAV, visit: www.clamav.com

- IP Address - The IP address of the ClamAV server to use.
- Port - The port that the ClamAV server is listening on.
- Remote Server - Select this checkbox if the server is a remote server.
- Timeout - The maximum number of seconds SmarterMail should wait for ClamAV to respond before moving on to the next message. By default, the timeout is 10 seconds.
- Failures Before Disable - The maximum number of ClamAV timeouts allowed before it is disabled. By default, ClamAv is limited to 5 failures.
- Virus Definitions - The date and time the virus definitions were last updated. The definitions are updated whenever the service starts and every 6 hours thereafter.

Command-line AV

- Command Line - The command that you want to execute. %FILEPATH will be replaced with the path to the file to be scanned.

Cyren Zero-hour Antivirus

The Cyren Zero-hour Antivirus add-on uses Recurrent Pattern Detection technology to identify 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.

Cyren evaluates each message and determines the probability that the message contains a virus. System administrators can choose the default action taken on a message when Cyren determines the it

has a medium, high, or definite probability of containing a virus. For more information, or to purchase this add-on, visit the SmarterTools website .

Greylisting

What is Greylisting and how does it work?

Greylisting has proven itself to be an effective method of spam prevention. When enabled, the system will keep track of the sending IP address, sending email address and recipient's email address for every message received. If an incoming message has a combination of a sending IP, sending address and recipient address that has not previously been seen, it will return a temporary failure to the sending server, effectively saying, □Try again later.□Valid servers will retry the email a short time later, which would be permitted. Spammers, on the other hand, typically create scripts that bombard your server with emails, and they rarely retry on temporary failures. When these messages are bounced back because of greylisting, they are typically not retried, therefore reducing the amount of spam that your customers receive. (Emails sent from whitelisted and authenticated□senders□will automatically bypass greylisting and are delivered directly to the spool.)

For those messages that are sent from valid email servers, the sending server should retry at least four times. If the first retry is beyond the block period (default 15 minutes) and within the pass period (default 6 hours), the message is passed to the spool and it goes through its normal processing without a delay. A record is also created that says this is a valid email address from that server to the given recipient and keeps it for 36 days (default). If another email from the same email address is received from the same server to the same recipient within the 36 days, the clock is reset for an additional 36 days and delivered directly to the spool.

Why use Greylisting?

Greylisting is a very effective method of spam blocking that comes at a minimal price in terms of performance. Most of the actual processing that needs to be done for Greylisting takes place on the sender's server. It has been shown to block upwards of 95% of incoming spam simply because so many spammers don't use a standard mail server. As such, spam servers generally only attempt a single delivery of a spam message and don't reply to the "try again later" request.

How do I set up Greylisting?

Note: You must be a system administrator to change greylisting settings.

In order to set up Greylisting, click the security icon and click Greylisting in the navigation pane. The greylisting settings will load in the content pane and the following tabs will be available:

Options

Use this tab to specify the following settings:

- Block Period - The period of time (in minutes) that mail will not be accepted (default 15 minutes).
- Pass Period - The period of time (in minutes) in which the sender's mail server has to retry sending the message (default 360 minutes).
- Record Expiration - The period of time(in days) that the sender will remain immune from greylisting once it has passed (default 36 days).
- Apply To - Select who greylisting applies to.
- Enable greylisting - Select this option to enable greylisting.
- Enable users to override greylisting - Select this option to allow users to selectively turn off greylisting (useful if you have an account that receives time sensitive mail).
- Greylist if the country for the IP address is unknown - Select this option to greylist messages when the country cannot be identified for the IP address. System administrators should note that the following cases are exempt from greylisting:
 - Whitelisted IPs for SMTP or Greylisting
 - Anyone who authenticates (includes SMTP Auth Bypass list)
 - Trusted senders
 - Anyone who has already sent you an email. Note: This list generates only after greylisting has been enabled.
 - Any IP in the greylistBypass.xml file

Filters

If you set the grelisting "Apply To" setting to "Everyone except specified countries / IP addresses" then you are able to add filters based on the countries or IP addresses you want to exclude from being greylisted.

Disadvantages of Greylisting

The biggest disadvantage of Greylisting is the delay of legitimate e-mail from servers not yet verified. This is especially apparent when a server attempts to verify a new user's identity by sending them a confirmation email.

Some e-mail servers will not attempt to re-deliver email or the re-delivery window is too short. Whitelisting can help resolve this.

Blacklist / Whitelist

System administrators are able to control the IP addresses that are blacklisted or whitelisted from accessing mail services. Blacklisting an IP address prevents it from making incoming connections, while whitelisting an IP address adds the IP as a trusted source, allowing connections to bypass relay restrictions that may be imposed. Exercise caution when granting whitelist status to a server, and be sure that you know what services on that server may send mail through your own.

To manage the blacklist or whitelist, click the Security icon and then click Blacklist or Whitelist in the navigation pane.

To create a new entry in the blacklist or whitelist, click New in the content pane toolbar. To edit an entry, click Edit in the content pane toolbar. The blacklist or whitelist settings will load in a popup window and the following options will be available:

- IP Address - Enter a single IP address in dotted quad notation (X.X.X.X) in this box if you want to add only a single IP (ex: 192.168.1.26).
- IP Range - Enter a range of IP addresses in the two boxes, and all IP addresses that are contained in the range will be added (ex: 192.168.1.1 - 192.168.1.255).
- Protocol - Check the boxes for the protocols you wish to include in the blacklist or whitelist entry. The available options are: SMTP, POP, IMAP, XMPP and Disable greylisting. (Disabling greylisting is only available when whitelisting an IP address, and, if checked, the whitelisted IP will not be greylisted.)
- Description - Use this field to enter optional notes for understanding the various whitelist / blacklist entries.

Note: SmarterMail runs a check against the IPs listed in whitelist, blacklist and authentication bypass settings. This check looks at the number of IPs listed and will display a warning if the IPs listed represent a significant number. (E.g., a range greater than a /24.) While the warning does not affect the ability to save the settings, it is an indication that the administrator may want to review the settings prior to adding the IP range.

Blacklist / Whitelist

System administrators are able to control the IP addresses that are blacklisted or whitelisted from accessing mail services. Blacklisting an IP address prevents it from making incoming connections, while whitelisting an IP address adds the IP as a trusted source, allowing connections to bypass relay restrictions that may be imposed. Exercise caution when granting whitelist status to a server, and be sure that you know what services on that server may send mail through your own.

To manage the blacklist or whitelist, click the Security icon and then click Blacklist or Whitelist in the navigation pane.

To create a new entry in the blacklist or whitelist, click New in the content pane toolbar. To edit an entry, click Edit in the content pane toolbar. The blacklist or whitelist settings will load in a popup window and the following options will be available:

- IP Address - Enter a single IP address in dotted quad notation (X.X.X.X) in this box if you want to add only a single IP (ex: 192.168.1.26).
- IP Range - Enter a range of IP addresses in the two boxes, and all IP addresses that are contained in the range will be added (ex: 192.168.1.1 - 192.168.1.255).
- Protocol - Check the boxes for the protocols you wish to include in the blacklist or whitelist entry. The available options are: SMTP, POP, IMAP, XMPP and Disable greylisting. (Disabling greylisting is only available when whitelisting an IP address, and, if checked, the whitelisted IP will not be greylisted.)
- Description - Use this field to enter optional notes for understanding the various whitelist / blacklist entries.

Note: SmarterMail runs a check against the IPs listed in whitelist, blacklist and authentication bypass settings. This check looks at the number of IPs listed and will display a warning if the IPs listed represent a significant number. (E.g., a range greater than a /24.) While the warning does not affect the ability to save the settings, it is an indication that the administrator may want to review the settings prior to adding the IP range.

SMTP Authentication Bypass

SMTP Authentication is a security measure that can be very beneficial in the fight against spam and unauthorized email as it forces the sender to authenticate their username and password before an email is sent through the mail server.

Unfortunately, some applications do not have support for SMTP authentication when sending mail. Most often, these are web sites that have automated mail sending mechanisms. The solution is to add the IP addresses of these servers/sites to SmarterMail's SMTP Authentication Bypass. Any IP address entered into this page will not be asked to provide an SMTP Authentication login. In this list you can see all IP addresses that are bypassing SMTP Authentication.

To get started, click the security icon and click SMTP Authentication Bypass in the navigation pane. A list of bypasses IP addresses will load in the content pane and the following options will be available in the content pane toolbar:

- New - Adds a new IP address or IP Address Range to bypass.
- Edit - Edits the selected IP address.
- Delete - Permanently removes the IP address from the SMTP authentication bypass list.

Trusted Senders

This section allows system administrators to exempt specific email addresses (such as `jsmith@example.com`) or domains (such as `example.com`) from SmarterMail's spam filtering. This can prevent mail from friends, business associates and mailing lists from being blocked and lets the system know that these messages come from a trusted source.

To view the trusted senders list for the server, click the security icon and click Trusted Senders in the navigation pane. A list of trusted senders will load in the content pane and the following options will be available in the content pane toolbar:

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

Server Blacklist Checker

Knowing when a mail server is listed by one of the realtime black lists (RBL) SmarterMail incorporates into its various spam checks used to mean system administrators would have to log in to various websites and perform manual checks of their domains and/or IP addresses. However, with the Server Blacklist Check, these checks are performed automatically for all IP addresses added to a SmarterMail server so system administrators know if a server is actively blacklisted. Once a day, SmarterMail checks all of the RBLs available by default for any server IP addresses (besides `localhost`), regardless of whether the RBL is actively being used as a spam check. If the RBLs come back showing an IP as blacklisted, it changes that IP's blacklist status from `False` to `True` on the Server Blacklist page. System administrators are advised to set up Blacklist Status Changed system events that will immediately notify them if a server becomes listed by a RBL.

To access the Server Blacklist Check, click the Security icon and then click Server Blacklist Check . A list of IP addresses on the server will load in the content pane and the following columns will appear in the content pane:

- IP Address - The IP address used for a domain, or for several domains, on that mail server.
- Spam Check - The name of the RBL or URIBL that is being used.
- Blocked - If the IP is blocked by the specific spam check, this column will say True . If the IP

address is NOT blocked, this will say False .

- Change - The last date and time the IP was checked against the specific list.

Advanced Settings

Abuse Detection

SmarterMail has several methods of preventing abuse and denial of service (DoS) attacks. The ones that can be configured are explained below. Any number of detection methods can be added.

To view the configurable abuse detection settings, click the security icon . Then expand the Advanced Settings folder and click Abuse Detection in the navigation pane. A list of abuse detection rules will load in the content pane and the following options will be available in the content pane toolbar:

- New - Creates a new abuse detection rule.
- Edit - Edits the selected abuse detection rule.
- Delete - Permanently deletes the selected abuse detection rule(s).
- Wizard - Displays the Abuse Detection section of the SmarterMail setup wizard, which offers the following preset security options:
 - Do not change abuse detection settings
 - Relaxed abuse detection (Includes: DoS, SMTP Brute Force)
 - Strict abuse detection (Includes: DoS, SMTP Brute Force, Email Harvesting, Internal Spammer Notifications, Bounces Indicate Spammer)

To create a new abuse detection rule, click New in the content pane toolbar. The abuse detection settings will load in the content pane and the following options will be available:

Denial of Service (DoS) - Too many connections from a single IP address can indicate a Denial of Service (DoS) attack. Enable this option to block IPs that are connecting too often to the server. It is recommended that you whitelist any trusted IP addresses that may send out large mailing lists or make many connections if you enable this option.

- Service - Select the service that will be monitored for this type of attack (SMTP/IMAP/POP/XMPP/LDAP).
- Time Frame - The period of time in the past that is examined to determine if an IP address should be blocked. Too many connections in this period of time, and a block will be initiated.
- Connections Before Block - The number of connections before a block is placed. It is common for several connections to be open at once from an IP address. Set this to a relatively high value so that you can catch DoS attacks while not impacting legitimate customers.
- Time to Block - The number of minutes that a block will be placed once an IP address hits the

threshold.

- Description - A friendly name or brief description of the rule.

Bad SMTP Sessions (Harvesting) - A bad session is any connection that ends without successfully sending a message. Many bad sessions usually indicate spamming or email harvesting. Leaving all of these options set to 0 (zero) will disable this type of abuse detection. Note: It is recommended that you whitelist any trusted IP addresses that may send out large mailing lists if you enable this option.

- Time Frame - The period of time in the past that is examined to determine if an IP address should be blocked. Too many bad sessions in this period of time, and a block will be initiated.
- Bad Sessions Before Block - The number of bad sessions before a block is placed. A few bad sessions happen once in a while, for instance when a person sends an email to an email account that does not exist. It is not these people that you are targeting, but rather those that are attempting to compromise or harass your customers.
- Time to Block - The number of minutes that a block will be placed once an IP address hits the threshold.
- Description - A friendly name or brief description of the rule.

Internal Spammer - Enabling this rule in SmarterMail will block or quarantine an account from sending mail, as well as alert an administrator, whenever multiple emails from a single sender are received on the server during a specified time frame.

- Action - Choose whether to send a notification email only, block messages from the sender or quarantine messages from the sender.
- Time Frame - The period of time in the past that is examined to determine if the rule triggers. Too many emails from a single sender in this period of time, and the email notification is sent and the Action chosen is performed.
- Messages Before Notify - After this many messages are received within the time period specified, the email notification is sent and the Action chosen is performed.
- Time to Block - The number of minutes that a block will be placed once an IP address hits the threshold.
- Email to Notify - The email address of the administrator account to which the notification will be sent.
- Description - A friendly name or brief description of the rule.

Password Brute Force by Protocol - A common ploy by spammers and hackers is attempting to guess passwords for users. Many times this entails continual log in attempts to an account using different passwords, each a bit different than the one before it. This thereby brute forcing the password.

- Service - Select the service that will be monitored for this type of attack (SMTP/IMAP/POP/XMPP/LDAP).
- Time Frame - The period of time in the past that is examined to determine if an login attempt is a brute force attempt. Too many connections in this period of time, and a block will be initiated.
- Connections Before Block - The number of failed login attempts before the IP is blocked.
- Time to Block - The number of minutes that a block will be placed once an IP address hits the threshold.
- Description - A friendly name or brief description of the rule.

Bounces Indicate Spammer - Enabling this rule in SmarterMail will block or quarantine an account from sending out mail, as well as alert an administrator, after receiving a certain number of bounce messages in the specified time frame.

- Action - Choose whether to send a notification email only, block messages from the sender or quarantine messages from the sender.
- Time Frame - The period of time in the past that is examined to determine if the rule triggers. Too many emails from a single sender in this period of time, and the email notification is sent and the Action chosen is performed.
- Bounce Threshold - After this many bounce messages are received within the time period specified, the email notification is sent and the Action chosen is performed.
- Time to Block - The number of minutes that a block will be placed once an IP address hits the threshold.
- Email to Notify - The email address of the administrator account to which the notification will be sent.
- Description - A friendly name or brief description of the rule.

Password Requirements

To ensure the security of the mail server and its mailboxes, system administrators can specify minimum requirements for user passwords. To access the password requirements settings, click the security icon . Then expand the Advanced Settings folder and click Password Requirements in the navigation pane. The password requirement settings will load in the content pane and the following options will be available:

- Minimum Password Length - The minimum number of characters the password must have.
- Password Expiration - The number of months that a password is valid. After the specified time, a user's outgoing SMTP will be disabled and a password change will be forced upon Web interface login. Check the Enabled box to enable this setting. Note: If a user's 'Disable password

changes' setting is enabled, their password will not expire.

- Auto-block Grace Period - The number of days a user can wait to update their account password before outgoing SMTP is disabled due to password policy violation. Note: This setting only applies if the "Disable outgoing SMTP when auto-block grace period ends" setting is checked.
- User Notification Timing - The interval(s) used to notify users of when their password will expire or when their auto-block grace period will end and, subsequently, their outgoing SMTP will be disabled. The default values are 28, 14, 7, 3, 2, 1 days. This means SmarterMail will send out warning messages to the user to change their password 28 days, 14 days, 7 days, 3 days, 2 days and 1 day before their password officially expires or the grace period ends if their password violates the requirements. Note: SmarterMail will send one, single notification for all missed intervals. For example, imagine "Auto-block Grace Period" is set for 30 days and the "User Notification Timing" is set at 60, 45, 25, 10, 2, 1. When a user is in violation, SmarterMail will send a single notification for the 60 and 45 day intervals then continue as normal at the 25 day interval.
- Require a number in the password - Select this option to force users to include a number in the password.
- Require a capital letter in the password - Select this option to force users to include a capital letter in the password.
- Require a lower case letter in the password - Select this option to force users to include a lowercase letter in the password.
- Require a symbol in the password - Select this option to force users to include a symbol in the password.
- Require password does not match username - Select this option to ensure that the username and password do not match.
- Disable password strength for existing passwords - Select this option to allow changes to the password requirements to only affect new users or new passwords.
- Enable password retrieval - Select this option to allow users to reset their password if they forgot it. Note: In order for users to utilize password retrieval, they must have a backup email address configured in their account settings.
- Prevent commonly used passwords - Select this option to prevent users from configuring passwords that are included in the list of commonly used, insecure passwords. Note: The default location of the list of commonly used passwords is: C:\Program Files (x86)\SmarterTools\SmarterMail\Service\Common_Passwords.xml.
- Prevent user□s previous passwords from being used - Select this option to prevent users from using previously used passwords when changing their account password. Note: This setting prohibits old passwords from being used indefinitely. It is not based on a time interval.

- Disable outgoing SMTP when auto-block grace period ends - Select this option to disable outgoing SMTP after the auto-block grace period ends when a user's password does not meet the password requirements.

SMTP Blocking

The SMTP Blocked Sender list is an effective method for temporarily canceling a domain or individual user's ability to send email on the server. For example, if a particular account is sending an abnormal amount of email, you can add their address to Blocked Senders and they will be unable to send email until you remove them from the Blocked Senders list. Users and/or domains can be left on the list for whatever time you deem appropriate, and can be an effective stop-gap versus actually deleting the user and/or domain from the server.

To view blocked senders, click on the security icon . Then expand the Advanced Settings folder and click SMTP Blocked Senders in the navigation pane. A list of blocked senders will load in the content pane and the following options will be available from the content pane toolbar:

- New - Adds a new SMTP blocked sender.
- Edit - Edits the selected blocked sender.
- Delete - Permanently removes the email or domain from the blocked senders list.

Adding a New SMTP Blocking Rule

To add a new SMTP blocking rule, simply click the New button. You are presented with the following options:

- Block Type - Options are set as either Email Address or EHLO Domain.
- Email Address - The complete email address to set up for the block.
- EHLO Domain - This is the return value given when SmarterMail sends the EHLO or HELO command. A standard EHLO domain is the fully qualified domain name set up for the mail server you're wanting to block. (E.g., mail.smartertools.com). However, it IS possible that it will be something different based on whether the command is sent by the SmarterMail Web interface or an email client. For example, it may be the local IP address of the sending machine.

Therefore, there is no well-established rule for what should be entered until some testing is done by the system administrator.

- Blocked Address - Enter either the full email address or the EHLO Domain, based on the Block Type that was selected.
- Direction - Specify whether to block either incoming SMTP, outgoing SMTP or both.
- Description - Friendly description for the block.

NOTE: SMTP blocking does NOT occur immediately when the EHLO command is given. Instead, a "soft" block is used and SmarterMail will fail any authentication attempts or RCPT TO commands. This is because if the failure occurs right after the EHLO command, any person attempting to spam from a mail server could figure out what the problem is and change the domain given with the command on each send. A "soft" failure should, instead, make the spammer believe he is using an incorrect password.

SpamAssassin

SpamAssassin is a powerful, free mail filter used to identify spam. It utilizes a wide array of tools to identify and report spam. These include:

- Header and text analysis
- Bayesian filtering
- DNS blocklists
- Collaborative filtering databases

To view a list of servers currently set up to run SpamAssassin checks, click the security icon / Then expand the Advanced Settings folder and click SpamAssassin Servers . A list of SpamAssassin servers will load in the content pane and the following columns will be available:

- Name - The name of the SpamAssassin server.
- Status - The status of the SpamAssassin server.
- IP Address - The IP address of the server running SpamAssassin. By default, the port is 783.
- Port - The port on which the SpamAssassin server should listen.

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

- New - Adds a new SpamAssassin server. Administrators will need to provide the server's IP address and the port on which SpamAssassin should listen.
- Edit - Modifies the SpamAssassin server settings.
- Delete - Permanently deletes the SpamAssassin server.

For more information on SpamAssassin, please visit <http://spamassassin.apache.org> .

Reserved Domain Names

System administrators can prevent certain domains names from being added to SmarterMail. For example, domains that are already used for free email services, like gmail.com or yahoo.com, are ideal additions to the reserve list as allowing administrators to add such domains to SmarterMail could

affect message delivery. Similarly, domains that are traditionally reserved for testing and documentation, such as test.com or example.com are also ideal candidates for the reserve list.

To view a list of reserved domains, click the security icon and expand the Advanced Settings folder in the navigation pane. Then click Reserved Domain Names . A list of reserved domains will load in the content pane and the following options will be available from the content pane toolbar:

- New - Adds a domain to the reserve list.
- Edit - Edits the selected domain.
- Delete - Deletes the selected domain(s) from the reserve list.

Additional Help Topics

Automating LogIn to SmarterMail

The HTML code below demonstrates how you can make a text link (e.g. "Log into your mail") that automatically logs a user in to the SmarterMail application. By putting a hidden form on a simple web page, you can fill in the "Email Address", and "Password" information either via hard coding the data or through a scripting language like ASP, ASP.Net, or ColdFusion.

For the example code listed below, we have the form values set to generic text (e.g. "Actual_Email_Address_Here") to show where you would hard code values that are submitted to the login.aspx page. You could also dynamically generate these values using a scripting language like ASP or ColdFusion (a sample ASP script would substitute value="Actual_Email_Address_Here" with value=<% =email %>). The form action shown (<http://127.0.0.1:9998/smartermail/login.aspx>) uses the default location of the Smartermail Web Interface. If you have created a separate web site for Smartermail, or assign a different IP address for Smartermail within IIS, this action would have to be altered to reflect this change. This example demonstrates how easy and powerful the Smartermail application is in allowing companies to automate entry into the mail application.

<html>

```
<head> <meta http-equiv= "Content-Language" content= "en-us" > <meta http-equiv= "Content-Type" content= "text/html; charset=windows-1252 "> <title>Smartermail Login</title> </head>
```

```
<SCRIPT LANGUAGE= "JavaScript" > function GoToMail() { document.mailform.submit(); } </SCRIPT>
```

```
<body>
```

```
<form name= "mailform" action= "http://127.0.0.1:9998/Login.aspx" method= "post" > <input type= "hidden" name= "shortcutLink" value= "autologin" id= "shortcutLink" > <input type= "hidden" name= "email" id= "email" value= "Actual_Email_Address_Here" > <input type= "hidden" name= "password" id= "password" value= "Actual_Password_Here" > </form>

<p><a href= "JavaScript:GoToMail()" > Log into your mail </a></p>
```

```
</body>
```

```
</html>
```

Gateways and Other Server Roles

Please note that SmarterMail was designed to support one server in several of these roles. For instance, one server could act as an Incoming Gateway, Outgoing Gateway, or Backup MX.

SmarterMail can also take on one of these roles when placed together with a competing mail server product. For example, using SmarterMail as an outgoing gateway on a server other than your primary mail server may help to resolve problems with stability of other mail server software products.

Primary mail server

- Use for storing email for defined users.
- Accessible through POP, SMTP, IMAP, and over the web.
- To configure:
 - Follow instructions in online help

Backup MX Server

- Use as a backup for mail delivery in case of short amounts of downtime or delivery problems on your primary mail server.
- To configure:
 - Add a placeholder domain (called "example.com") to open up the port to listen on.
 - Configure SmartHosting by adding the IP addresses to which delivery should be allowed.
 - In general settings, change the delivery retry times to 10, 10, 10, and 1440.

- In DNS, add secondary MX records pointing to the new server's IP. Set the preference value higher than the main MX record.

Incoming Gateway server

The FREE, one-domain version will suffice for virtually all environments.

- Use to host third party anti-virus and/or anti-spam software products in order to reduce load on primary server.
- Reduces load on primary server by managing all incoming sessions and performing abuse/intrusion detection.
- To configure:
 - Enable domain forwarding and add all destination IPs and domain names that will be forwarded.
 - Add a placeholder domain (called "example.com") to open up the port to listen on.
 - In DNS, change the MX records of your domains to reference the new gateway server.
 - Install and configure any third-party anti-virus or anti-spam products, such as Declude JunkMail or Declude Virus.

Outgoing Gateway server

The FREE, one-domain version will suffice for virtually all environments.

- Use as a delivery mechanism to reduce load on your primary servers.
- Also use as a method to combat blacklisting. If the server gets blacklisted, rotate the primary IP on the network card to a different one to send out on the new IP.
- To configure:
 - Add a placeholder domain (called "example.com") to open up the port to listen on.
 - Set relay option in General Settings to "nobody".
 - Add the primary mail server's IP addresses to the IP Whitelist for SMTP.
 - In your primary mail server's General Settings page, set the IP address of the gateway server and enable gatewaying.

SmartGateway server

The FREE, one-domain version will suffice for virtually all environments.

- Use as a delivery mechanism to balance the load on your gateway servers.
- To configure:
 - Add a placeholder domain (called "example.com") to open up the port to listen on.
 - Set relay option in General Settings to "nobody".

- Add the primary mail server's IP addresses to the IP Whitelist for SMTP.
- In your primary mail server's General Settings page, set the IP address of the gateway server and enable gatewaying.

Backup MX Servers

A Backup MX Server is a mail server that will store (spool) your incoming email if your primary mail server becomes unavailable. A mail server can become unavailable to receive incoming mail for a number of reasons. For example:

- Hardware or software failure
- Very busy and unable to receive new incoming connections, or emails
- Network connection is down or saturated
- Network routing issues can also cause your mail server to become unavailable

Case 1 - No Backup MX

If you do not have a Backup MX Server, the following conditions may occur:

- Email will be bounced (Returned to Sender).
- Your (inbound) email will cause a backup in the originating mail server's spool.
- Service Timeout. Depending on the Retry attempts by the originating mail server, your mailboxes may never receive their incoming email.
- Users do not understand bounce messages. To most users, bounce messages are unreadable, so when they can't send an email, they do not try to resend.

Case 2 - With a Backup MX

How Email works when a Backup MX Server is involved:

- User sends an email to 'user@example.com' (a mailbox hosted by your SmarterMail Server)
- Their mail server looks up the MX Records for 'example.com' and finds two:
 - IP: x.x.x.x Weight: 10
 - IP: y.y.y.y Weight: 20
- Their mail server first attempts to connect to: x.x.x.x
- Connection fails, which could be caused by any of the above conditions
- They try to connect to the secondary MX record: y.y.y.y
- They successfully connect to this server.
- Email transmission begins, and the Backup MX Server receives the email into its spool.
- Since there are no existing local domains on this server, SmarterMail stores this email in its spool.

- Based off of the Retry Attempts, SmarterMail will continue to try and make connections to your Primary Mail Server.
- SmarterMail will only make 4 retry attempts. It is recommended that you set the last attempt to a longer timeframe, i.e., 24 hours (1440 minutes)
- This way SmarterMail does not send a Bounce Message to the originator saying that it could not deliver the message, before your Primary Server is back online.
- If your Primary Mail Server comes back online before the final Retry Attempt, you can reset the Retry Counts on all messages in the spool. This will force the Backup MX Server to try forwarding all existing mail in the spool back to your Primary Mail Server.

Configuring a Backup MX Server

- Add a placeholder domain (called "example.com") to open up the port to listen on.
- Configure SmartHosting by adding the IP addresses to which delivery should be allowed.
- In general settings, change the delivery retry times to 10, 10, 10, and 1440.
- In DNS, add secondary MX records pointing to the new server's IP. Set the preference value higher than the main MX record.

Locking Down Your Server

Security is an ever-growing concern to business small and large. Because email servers are constantly under attack, SmarterMail has many features built into it to protect you. This topic explains steps you can take to protect yourself, your users, and your investment.

What is Security for a Mail Server?

The word security has many meanings. SmarterTools' opinion is that mail server security is comprised of several types of protection:

- Protecting your data
- Protecting your users
- Protecting your service availability
- Protecting others on the internet

Below are some "Best Practices" for maintaining a locked-down server, one that can withstand the constant abuse that mail servers are subject to.

- Update SmarterMail regularly
- Disable catch-all accounts
- Restrict bounces and auto-responders

- Require SMTP authentication
- Encourage the adoption of SPF

Update SmarterMail Regularly

SmarterTools is constantly working to improve SmarterMail and make it even more resistant to attacks. It is recommended that you keep your copy of SmarterMail up to date in order to stay protected.

Major and minor SmarterMail version releases are announced on our social media pages as well as the News items on the Support Portal . Email notices are sent to SmarterMail customers who are subscribed to receive these notifications. You can manage your mailing list subscriptions at My Account .

Disable Catch-All Accounts

Catch-all accounts were popular in the past because of the flexibility they offer to a domain administrator. All an administrator had to do was add a catch-all account, and any mail that was mis-delivered would drop right into his mailbox. When catch-alls were most popular, spamming methods were not as sophisticated, and email harvesting attacks were not so prevalent.

Today, however, mail servers get attacked every minute of every day. Spammers assault email domains with thousands of spam messages sent to different email accounts in the hope that they will strike a hit to verify that the email account exists and to deliver another spam email.

In addition, if the catch-all user has an auto-responder enabled, the problem can be doubly harmful. Spammers rarely use their real email address, so if your user auto-responds to each of the thousands of messages above, and they happen to go to a large email provider, you will likely end up getting blacklisted as a spammer yourself.

As you can see, allowing the use of catch-all accounts exposes you to many types of abuse. SmarterMail allows catch-alls because it is expected in a mail server, but to lock down your server, we recommend the following procedure that will disable catch-alls:

- Alert your users that catch-alls are being disabled.
- Click on the Domains icon and edit the desired domain.
- Click on the Features tab.
- Uncheck Catch-All Alias .
- Click Save .

Restrict Bounces and Auto-Responders

Email Bouncing occurs when delivery failures occur or a mailbox is full. A brief explanation of the error is sent back to the original sender of the message. Before spam became such a problem, this was usually not an issue. Today, however, spammers will sometimes spoof known spam trap accounts at places like SpamCop as the sender of the message. Thus, when your mail server bounces the message, the bounce ends up in the spam trap. Enough of these, and you'll be blacklisted.

The exact same is true for auto-responders that reply back to spoofed spam email.

SmarterMail allows you to restrict bounces and auto-responders to only those accounts that pass SPF checks, or to disable them entirely. SPF verifies that an email is not spoofed, and most of the serious spam trap accounts out there have SPF set up. To require SPF for bounces and auto-responders, do the following:

- Alert your users of the new policies being put into place.
- Click on the Security icon .
- Click on Antispam Administration in the navigation pane and then the Options tab.
- Change Auto-Responders to either Disabled or Require message passed SPF .
- Change Content Filter Bouncing to either Disabled or Require message passed SPF .
- Click Save in the content pane toolbar.

Require SMTP Authentication

SMTP Authentication is an unspoken requirement of domains on modern mail servers. Any domain that does not have Authentication enabled is at a serious risk of being a relay for spam. Spammers will try thousands of email accounts until they find one to send through, and if Authentication is not enabled, they will be able to use up your bandwidth and system resources to send mail.

Enabling SMTP Authentication ensures that users must supply credentials to send email from your server. This requires a change in their email clients so that the account information gets passed in SMTP, so there is often a bit of a learning curve. This process is necessary and important to protect your server, however, and without you are open for abuse.

To require SMTP Authentication for a domain, do the following:

- Alert your users of the change they will need to make to their email client. Due to the nature of this change, it is wise to give them a fair amount of warning.
- Click on the Domains icon and edit the desired domain.
- Click on the Technical tab.

- Check Require SMTP Authentication .
- Click Save .

It is also recommended that you update this setting in the default domain settings so that all new domains will require SMTP Authentication. In addition, to further secure the use of SMTP Authentication, you should ensure that "Require Auth Match" is set to Domain or Email Address for all domains. This means that a sender's "From" address must match the SMTP authentication address or domain, making it more difficult for users to spoof addresses. This can be done under the SMTP In tab of the Protocol Settings.

To apply this setting to all domains on your server at once, use the Domain Propagation page in the Settings menu.

Encourage the Adoption of SPF

SPF is an excellent method of preventing email spoofing, protecting your users from having their domain show up on spam throughout the world. SPF, however, is only as effective as you make it, as it requires changes to your DNS servers for each domain you host email for.

It is in the best interest of all email users everywhere that domain administrators add SPF records to their domain that indicate what servers are authorized to send email for their domain. Encouraging your domain administrators to adopt SPF protects them from being the victims of spoofing, and reduces the spam threat on not only your server, but others throughout the world as well.

More information can be found at: <http://www.openspf.net/>

Proper DNS Settings for Email

There are several major things to set up on your DNS server for each site you add to SmarterMail. How you set these up is dependent upon both who hosts your DNS and what DNS software is used. Check your DNS server documentation for instructions on how to set up the following records (replace example.com with the proper domain name).

Also, please bear in mind that your DNS may need to be set up differently. This is only a guideline that is recommended for most installations.

- WebMail URL - Add an A or CNAME record for mail.example.com that points to the IP address of the webmail interface. This will allow users of that domain to access the webmail by typing in <http://mail.example.com> or <http://mail.example.com:9998> in their web browser (depending on whether you use the included web server or IIS).
- Mail Pointer (MX) - Add an MX record for the domain that points to mail.example.com. This will allow other email servers to locate your mail server.

- Reverse DNS Record - Add a reverse DNS record for IP addresses assigned on the server to provide extra assurance to other mail servers. Also, it is recommended that the primary IP address of the server also have a reverse DNS record.
- Sender Policy Framework - Some large email providers like Hotmail and AOL are starting to require specially formatted TXT records to be added to your DNS. This special format is known as SPF (Sender Policy Framework). Information about how these records should be formatted can be found at <http://spf.pobox.com>. Please keep in mind that the owners of the domains may have significant input on what goes into these records.

Changing the System Administrator Login

By default, the login for the system administrator for SmarterMail is admin/admin . While this is easy to remember, it is also fairly easy to guess. When installing SmarterMail for the first time, you will be required to change this password during the setup wizard. Here are instructions in the manner you would want to change the system administrator password again.

Instructions

- Login as the administrator with the current login.
- Click the Settings icon .
- Choose System Administrators in the navigation pane.
- Click on the Options tab and double-click on the Primary Administrator or right-click and choose Edit.
- Enter the current password for verification.
- Enter a new and password (If changing the username as well, avoid using an email address for the username).
- Click on Save .

Resetting an Unknown Login

For instructions on how to reset an administrator login when the current login is unknown, please see the KB article [How To Reset an Administrator Username and Password](#) .

Troubleshooting a Domain

There are times when you will need to access domain specific information. SmarterMail uses impersonation to accomplish this goal, causing a separate window to login automatically as the domain administrator. This can be a useful method to examine domain settings or configure settings.

To impersonate a domain, click the Domains icon . Then select the desired domain in the navigation pane, right-click and choose Manage . Alternatively, you can select the domain in the navigation pane

and click Manage in the content pane toolbar. A new window will pop up, and you will be logged in as the domain administrator. From there, you may edit user accounts, content filters, or whatever other part of the domain that needs to be changed.

For instructions on troubleshooting specific user accounts on a domain, please see the topic Troubleshooting an Email Account .

Modifying Scoring for the SpamAssassin-based Pattern Matching Engine

System administrators can modify the scoring for the SpamAssassin-based pattern matching engine using the local.cf file. However, this feature is only recommended for experienced system administrators.

The local.cf file is placed in the service's SAData folder. It is used to override existing tests or to create new tests supported by SmarterMail. Note: Any modifications to the local.cf file will not be overwritten when installing a new version.

Overriding an Existing Test's Score

The most common modification to the local.cf file will be to override an existing test's score. For example, if a system administrator he notices a lot of spam messages getting into his users' mailboxes that are failing a particular test, he may want to override a that test's score.

To do so, the server administrator would add something like:

```
score TEST_I_WANT_TO_OVERRIDE 1.3
```

Here score is the keyword used by the engine, TEST_I_WANT_TO_OVERRIDE corresponds to the existing test they want to override and 1.3 is the new score.

Creating a New Test

If a system administrator notices a noticed a new pattern appearing in spam messages that isn't covered by the default files, he may want to create a new test. This would look something like this:

```
body NEW_TEST /test/ #look for the word test in the body of the email score NEW_TEST 10.3
```

Here body is the keyword for determining the type of test, NEW_TEST is the name of the new test, /test/ is the perl style regular expression that will be used while scanning the email, and everything after the pound-sign is a comment.

The system administrator will also need to score the new rule so that it has some affect on the final weight.

Glossary

Below is an alphabetized list of the various terms and phrases used in the SmarterMail Product.

Account - An account consists of an email address and a password, used to log into a mail server to retrieve or send mail.

Administrator - The person or company that purchased and installed SmarterMail Professional Edition on a server with abilities to set global configurations and create and delete email domains and end users.

Alias - An email address representing another address that only forwards received mail to another address or group of addresses. For example, if your email address is you@example.com and you wanted to make an account for purchases without actually having separate inboxes to check, simply create the email Alias purchases@example.com and the mail for purchases will be redirected to your original mailbox.

APOP - APOP stands for Authenticated Post Office Protocol. Every mail connection made sends your username and password across the network in clear text (no encryption). With APOP, your password is encrypted while being transmitted over the Internet.

Auto Responder - A preconfigured message immediately sent back to anyone you receive an email from.

Black List - Block email from email addresses and domains added to this list.

Content Filtering - Content Filtering allows a user to search incoming messages for certain words or string of words. Messages containing the filtered items can be acted upon, for example deleting them so it never reaches its final destination, or moving them to a separate folder away from the main inbox.

DNS Server - A DNS Server is a computer designated to holding a list of domain names and their corresponding IP addresses. For the purposes of SmarterMail, some Domain Name Servers hold a list of domain names and IP addresses associated with mass spam mail outs. SmarterMail makes it possible for Administrators to enter the URL and take advantage of these Domain Name Servers to filter out mail from known spammers.

Domain - A domain is the name associated with the last half of an email address, it resides after the @ symbol (e.g. in support@example.com, example.com is the domain).

Domain Administrator - The owner of a particular domain responsible for adding and deleting email accounts and setting configurations associated with that domain. The domain administrator account also functions like a standard user account in that it can send and receive mail, manage contacts, etc.

Domain Alias - An additional domain that forwards received mail to another address or group of addresses. For example, you may have two email addresses with different domain names, to combine their inboxes, add one email address to the Domain Alias List.

End User - A person who uses SmarterMail to send and receive mail, or to manage a domain consisting of other end user email accounts.

Folder Auto-Clean - Automatic deletion of older messages when a folder reaches a certain size. Used to keep folders like Junk E-Mail under control.

Forward - To redirect a received email to another email address.

IMAP / IMAP4 - Internet Message Access Protocol (IMAP) is a standard protocol for accessing e-mail from your local server. IMAP (the latest version is IMAP4) is a client/server protocol in which e-mail is received and held for you by your Internet server. IMAP requires continual access to the server during the time that you are working with your mail.

IP Address - Internet Protocol address is the numeric physical address of any computer. Therefore, you can access a computer by entering either the domain name or the IP address for the domain (e.g. 127.0.0.1).

IP Bypass - Pardon IP addresses from SMTP authentication enabled on any domain. This is often used to allow clients who have applications that do not support SMTP authentication to bypass this check.

IP4R / RBL List - A DNS lookup that attempts to determine if a mail server is likely to be sending spam. You take the IP address of the mail server, turn it around, and query a "DNS zone", to come up with something like "2.0.0.127.relays.example.com". If the mail server is listed in the spam database you queried, it will return an answer indicating that the mail server is listed.

Kill List - A list of domains that are denied access to the mail server.

LDAP - Lightweight Directory Access Protocol (LDAP) is a communication protocol for accessing online directory services. Programs like Outlook and Thunderbird use LDAP to retrieve contact lists from SmarterMail.

List Server - A list server (mailing list server) is a program, or a feature in a program, that handles subscription requests for a mailing list and distributes new messages, newsletters, or other postings from the list's members to the entire list of subscribers as they occur or are scheduled. Note: A list server should not be confused with a mail server, which handles incoming and outgoing e-mail for Internet users.

Mailbox - A folder that contains messages.

Mailing List - A mailing list is a list of people who subscribe to a periodic mailing distribution on a particular topic. Mailing lists include each person's e-mail address. Mailing lists have become a popular way for Internet users to keep up with topics they're interested in. Many software producers and other vendors are now using them as a way to keep in touch with customers.

POP / POP3 - With Post Office Protocol version 3 (POP3) your mail is saved for you in your mail box on the mail server. When you read your mail, all of it is immediately downloaded to your computer and no longer maintained on the mail server.

Postmaster - A required default email account for a domain. In order to receive email from the postmaster account, it has to be forwarded to another email address.

Relay - Allows an SMTP server to accept any email destined for other hosts and re-deliver that mail to the proper host, much like a field and track relay race where the SMTP servers are the runners and the email message is the baton.

SMTP - Simple Mail Transfer Protocol is a TCP/IP (Internet) protocol used in sending and receiving e-mail. However, since it's limited in its ability to queue messages at the receiving end, it's usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending e-mail and either POP3 or IMAP for receiving messages that have been received for them at their local server.

SMTP Authentication - When the mail server requires an email address and password that matches an account in order to send mail, as opposed to requiring just an email address.

Spam Check - A resource used for checking the validity of an email sender.

Spam List - Some Domain Name Servers (DNS) on the Internet contain a list of addresses from mail servers that are solely used for email spam. Therefore, the Spam List is a editable list of DNS's so you can compare your incoming mail to those known spam email servers and filter them out accordingly (An example of an "anti-spam" DNS is opm.blitzed.org).

Spam Weight - The weight is a value assigned to a spam check according to its validity and competency. Generally, the higher the weight, the more likely an email message is spam.

Spool - A directory on the mail server that holds emails before they are viewed or downloaded from a client.

Stats - The overall calculations about email from a domain including total messages and bandwidth.

URL - The Uniform Resource Locator is an address that links to a web page or web server that is usually entered into the top of a browser.

User - A client with an email account.

Web Interface - The point of access for administrators and end users to the Mail Server via browser.

Web Mail - An interface for sending and receiving email through the use of a browser (e.g. Internet Explorer or Netscape) instead of an email program (e.g. Outlook). Configuring client side email is as simple as hyper linking to the correct URL and Logging in with a user name and password.

Web Service - A Web Service is a remote application interface that a program can connect to to obtain information or execute commands through standard internet ports (typically port 80, the same port used by a typical web browser)

White List - Add an email address to this list to accept all mail from the sender, regardless of Black List restrictions.

SMARTERTOOLS END USER LICENSE AGREEMENT

SmarterTools, Inc. Software License Terms

This End User License Agreement ("EULA") is between SmarterTools, Inc. ("SmarterTools") and the License holder ("You") of the software product this EULA accompanies ("Software"). It is important to read and understand all of the terms, limitations, and conditions contained in this EULA prior to installing and using the Software because they affect how You may use the Software and Your rights under this License. By explicitly accepting this EULA, or by installing, copying, downloading, accessing, or otherwise using the Software, You agree to be bound by the terms of this EULA. If, prior to using or installing the Software, You decide that You are unable or unwilling to agree to the terms of this EULA, promptly and completely uninstall and destroy any electronic copies of the Software and accompanying items in your possession.

This EULA shall apply to:

- * This Software
- * Future Versions of this Software
- * Updates, add-ons, and plug-ins to this Software, as may be made available by SmarterTools from time to time, including but not limited to language packs, dictionaries, and skins (collectively "Updates")
- * Features selection(s), including, but not limited to, "Professional," "Enterprise", and "Free" editions of the Software, and maximum allowed numbers of users, profiles, devices, email addresses domains, web sites, or agents ("level");
- * Services, support, advice, and recommendations related to this Software that may be made available by SmarterTools on the Internet, in the Software documentation, or by telephone
- * Any and all Technical Support Services offered in connection with the Software

DEFINITIONS

The following definitions shall apply for the purposes of this EULA:

- * "Dedicated Hosting" shall refer to an individual, group, or organization ("Dedicated Host") that maintains a physical server device that is wholly or, in the case of Virtual Private Servers ("VPS"), a dedicated portion of a physical server device that is sold, leased, or otherwise made available to a third party; whether or not a fee or other compensation is exchanged; and in which the third party has authorization and/or access to the activation areas of the software and/or to system administration functions.

- * "Effective Date" shall be the date upon which this EULA was accepted by You.
 - * "Elastic Computing" shall refer to a user's ability to install software, create websites or instantiate a database on one or more Workers that can then be given incremental CPU cycles or percentages, memory (RAM) allocations, and/or physical disk space and bandwidth allocations that can all, then, be managed (increased or decreased) separately and on an as needed basis.
 - * "Failover" is the ability of a system to automatically switch to a second, standby system should the primary system fail or is temporarily shut down.
 - * "License" shall refer to the revocable, non-exclusive, non-transferable license to use the Software ("License") in accordance with the terms and conditions of this EULA. The term License applies to purchased and non-purchased Licenses, including but not limited to the object code, source code, and any accompanying alphanumeric combinations used to enable and/or activate the software or certain Features Selection(s) in the Software (collectively, "License Keys").
 - * "License Key" shall apply to the alphanumeric combination entered/applied upon installation and used to access Feature Selections. License Keys are delivered to the owners of purchased (paid for) Licenses and to those who may receive authorized promotional or trial Licenses, if applicable (pursuant to this EULA). SmarterTools may create and provide certain Levels, Editions, and/or Versions of the Software that do not require entry or use of a License Key for promotional or other purposes. This EULA remains in full force and effect whether or not a License Key is required or provided by SmarterTools.
 - * "Load Balancing" is a networking methodology whereby processing and workload is distributed evenly among a group of independent machines (e.g., servers) so that no single device is overwhelmed and so that there is no single point of failure.
- "Multi-tenancy" and "Multi-tenant license(s)" shall refer to the ability of any single license to support multiple separate and unique client organizations, particularly when offering a single license in a Software as a Service (SaaS) capacity. For the purposes of this EULA, only SmarterStats and SmarterMail are multi-tenant licenses.
- * "Periodic License" shall be a License with a defined temporal component (start and end date) whether or not such License is subject to renewal, automatically renews, effectively terminates, or is extended (e.g., Monthly/Lease Licenses, Trial Licenses, Development Licenses). Periodic Licenses may be governed by additional terms and conditions in a separate written agreement.
 - * "Third Party Providers" shall be any other software, application, plug-in, add-on, utility, tool, device, or methodology by any individual, group, organization, affiliation, company, or other entity that connects, modifies, links, and/or integrates to/with the Software for any purpose whatsoever.

* "Shared Hosting" shall refer to an individual, group, or organization ("Shared Host") that maintains a physical server device upon which software and/or tools are owned and installed by the Shared Host and made available to third parties for access or use; whether or not a fee or other compensation is exchanged; and in which the third parties do not have authorization or access to the activation areas of the Software and/or do not have authorization or access to system administration functions.

* "Worker(s)" shall be the location where software, websites or databases are installed in an Elastic Computing environment. A Worker can then have CPU cycles, disk space and RAM allocations and bandwidth modified (i.e., increased or decreased) on an as needed basis to accommodate shifts in traffic and usage. Also known as a worker process.

1. License.

A. Grant of License.

Upon the Effective Date, SmarterTools hereby grants You a revocable, non-exclusive, non-transferable license to use the Software ("License") in accordance with the terms and conditions of this EULA. This License shall commence on the Effective Date of this EULA and shall remain in effect until terminated in accordance with the terms of this EULA or superseded by another end user license agreement pursuant to installation of an Update or changes in Features Selection. SmarterTools, together with any third party content providers whose software code is incorporated in the Software or distributed with it, retains all right, title, and interest to the Software, including, but not limited to, copyrights, trademarks, proprietary methods, and trade secrets incorporated into the Software.

This License is subject to any restrictions SmarterTools, in its sole discretion, may impose in this EULA or imposed as a condition of purchase, including but not limited to the particular Features Selection You chose at the time of purchase. Updates and Features Selection are subject to the terms and conditions of this EULA, or any other end user license agreement provided with such Update or Features Selection at the time of receipt or purchase, which shall supersede this EULA.

This License to use the Software is conditioned upon You paying all related charges and fees imposed by SmarterTools for purchase of the Software, monthly-license of the Software, or for the authorized delivery of the Software as a service (SaaS). SmarterTools may, in its sole discretion, terminate this License if You fail to pay such charges or fees within the time allowed by SmarterTools.

B. Use of the Software.

You shall use the Software for Your own personal or internal business purposes. Personal or internal business purposes shall include the installation of the Software and activation of only one License on any single personal computer or server; one instance of a Virtual Private Server; or in the case of Elastic Computing, on any single Worker for Your own use or use by Your Customer(s) pursuant to

the terms of section 1.C. below. Should SmarterTools designate that a specific license can be used for Failover, then You may install that license on a second machine that matches the exact specifications of the initial installation machine, and use that second machine as a Hot Standby. Should SmarterTools designate that a license can be used for Load Balancing, then You may install that license on as many similarly-configured machines as necessary to meet any Load Balancing requirements.

C. Sublicense, Resale, Lease, Sub-lease ,or Transfer

You may sublicense this License to a third party(ies) ("Customer") only pursuant to a Shared Hosting agreement and the terms and conditions of this EULA, if applicable. You represent and warrant that each Customer has accepted this EULA prior to allowing the Customer access to or utilization of the Software and You shall promptly provide confirmation of each Customer(s)'s acceptance of the EULA upon request by SmarterTools. You shall indemnify, defend, and hold SmarterTools harmless against any claims asserted by or against You by any of Your Customer(s) or by any third party related to Your Customer(s)'s use of the Software, including but not limited to claims of infringement of the intellectual property rights of any third party and the additional warranty, liability, and indemnification provisions found in Sections 3 and 5.

Certain authorized parties ("SmarterTools Authorized Reseller") may Resell, Lease, Sub-lease, or Transfer this License (collectively, "Transfer") to any third party subject and pursuant to a separate authorizing agreement in writing with SmarterTools (e.g., Master Partner Agreement). For the purposes of this EULA, Transfer shall refer to any transaction whereby sole use, management, ownership, and/or control of the software is assigned to any third-party for that party's benefit, pursuant to the terms and conditions of this EULA, whether or not a fee or other compensation is charged and whether or not such Transfer is permanent or temporary. Transfers by or between any party(ies) other than SmarterTools or a SmarterTools Authorized Reseller must be approved by SmarterTools in advance and in writing.

You may install and maintain the Software on behalf of a third party; however, all SmarterTools Licenses in such circumstances must be purchased by the third party directly through SmarterTools or through a SmarterTools Authorized Reseller and the Software must be activated under the name of the related third party; thereby, the related third party assumes full ownership of the License subject to the terms and conditions of this EULA.

D. Limitations on Use of the Software and License Keys

You shall not modify, reverse engineer, reverse assemble, decompile, disassemble, decrypt, reflect, or use reflection on the Software, or otherwise attempt to discover or obtain the source code or structure, sequence, or organization of the software in whole or in part, except as provided in Section 9 of this

EULA. You may distribute copies of the software code in the same format that you received it, pursuant to the terms of this EULA, so long as You do not modify the Software in any way and so long as all copyright, trademark, and other notices contained in the Software remain intact.

The Software may periodically and automatically contact SmarterTools pursuant to Section 10 of this EULA. This contact may occur without any notice to You of such contact, and You hereby consent to such contact with SmarterTools. You shall not disable, delay, dismantle, disrupt, or otherwise interfere with the ability of the Software to contact or communicate with SmarterTools or the authentication of License Keys. Further, You shall not attempt to bypass, circumvent, disable, design around, or obviate the License Keys for any reason, including but not limited to attempts to access features, capacity, or capabilities in the Software not included in your Features Selection. Further, other than pursuant to Section 1.C. of this EULA, You shall not disclose or disseminate any License Keys associated or distributed with the Software, publicly or to any third party, nor shall You allow anyone else to use any such License Keys.

You may reassign/migrate this Software to a different device owned, leased, or rented by You subject to SmarterTools' approval in its sole discretion, provided that You completely uninstall or delete the Software from any personal computer, server, Virtual Private Server, Elastic Computing Worker or other device on which the Software was previously installed. SmarterTools reserves the right to require, in its sole discretion, reauthorization, re-registration, or another form of authentication at no additional charge to enable reassignment of the Software, and may disable the related License Key and/or access to the Software at any time if it determines, in its sole discretion, that such reassignment is prohibited by the terms of this EULA or constitutes fraud.

You shall not use the Software to harm third parties, disseminate unsolicited communications (emails, etc.), requests, or harmful data or programs including but not limited to malicious scripts and viruses. You shall not use the Software to disseminate pornography, child pornography, or other harmful or illegal materials, or in any way that may disparage or bring disrepute to SmarterTools.

2. Term and Termination.

This EULA is effective as of the date You install or use the Software, or as of the date You accept this EULA, whichever is sooner. You may terminate this EULA by completely deleting and wholly destroying any copies of the Software and documentation in Your possession or control. SmarterTools may terminate and/or disable the License or EULA if, in its sole discretion, SmarterTools determines that You have breached any of the terms and conditions of this EULA, with or without notice to You of such termination.

Sections 1.B., 1.C., 1.D., 3, 5, 6, 7, 8, 9, 10, 11, 12, and 13 shall survive termination of this EULA.

3. Limited Warranty and Limitation of Liability.

A. No Warranties

SmarterTools does not warrant that the Software will meet Your requirements, that the operation of the Software will be uninterrupted or error-free; that any data supplied by the Software will be accurate; or that the Software will work with any 3rd-party or supplemental software or hardware furnished with or accompanying the Software. Further, SmarterTools does not warrant the efficacy, functionality, or operation of such Accompanying Software or Hardware. **ALL HARDWARE, SOFTWARE, OR OTHER PRODUCTS OR SERVICES PROVIDED BY SMARTERTOOLS UNDER THIS EULA ARE PROVIDED AS-IS, AND SMARTERTOOLS EXPRESSLY DISCLAIMS ALL WARRANTIES, INCLUDING BUT NOT LIMITED TO WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.**

B. No Liability for Damages

SmarterTools shall not be liable for any damages under this EULA, including but not limited to consequential, statutory, punitive, incidental, or indirect damages, including but not limited to any loss of data, loss of profits, loss of savings, loss of time or convenience, or additional cost arising out of the use of or inability to use the Software, documentation, support, or any 3rd-party or accompanying software or hardware; even if SmarterTools has been advised of the possibility of such damages. Further, SmarterTools shall not be liable for nor bound by any claims, representations, promises, assertions, or other statements made by anyone other than SmarterTools employees or officers, including but not limited to resellers and sales representatives. SmarterTools shall not be liable for any damages or inconvenience resulting from errant data or misreporting of data, nor failures to relay information that may be deemed important by the user, any errant or substantial mistranslation of language or information, and/or for any damages arising from events listed in Section 5 of this EULA.

C. Third Party Providers and Web Services

The Software is designed to integrate and/or to be used in conjunction with Third Party Providers through Web services. SmarterTools assumes no liability and makes no warranty or guarantee regarding the applicability of effectiveness of this Software when used in conjunction with these products or whether or not such integration or use might interfere with the operation therein. You agree to hold SmarterTools harmless in all matters resulting from the integration or use with Third Party Providers.

D. Limitation of Liability

Your sole remedy under this Agreement shall be limited to replacement of the Software.

4. Technical Support

Currently, SmarterTools provides technical support for the Software via SmarterTools personnel, documentation, and Internet resources. Depending on Your Features Selection, including but not limited to pricing, volume, Software version, and the number of licenses You purchased, a certain amount of technical support may be included at no additional charge. Otherwise, technical support may be available for an additional charge on a per ticket, per call, or per time-frame basis or in other support packages. The amount of these charges may vary from time to time. Technical support is provided AS-IS, and the provisions of section 3.A., 3.B., and 3.C. apply to technical support.

SmarterTools provides no guarantee, expressed or implied, regarding the efficacy or continuation of technical or other support for this Software or particular version of this Software for any length of time and SmarterTools may choose to discontinue such support at any time and for any reason.

5. Indemnification.

You shall defend, indemnify, and hold harmless SmarterTools and its suppliers, licensors, successors, affiliates, agents, employees, executives, and assigns (hereafter "SmarterTools Indemnified Parties") from any claims, damages, losses, or expenses (including without limitation attorney fees and costs) incurred in connection with any and all damages, losses, claims, suits, judgments, or causes of action asserted against SmarterTools Indemnified Parties by third parties or Your Customers related to:

- * Any claims arising from or related to Your use of the Software or use of the Software by Your Customers or any portion thereof, including but not limited to claims of infringement of patents, copyrights, or other intellectual property or proprietary rights arising from your use of the Software or from use of the Software or any portion thereof in combination with any other software, hardware, device, system, or service;
- * Damages arising from Your breach or Your Customer's breach of this EULA;
- * Any loss, misdirection, or inaccuracy of any and all data, message, and/or information (partial or complete) by or directed to You, Your Affiliates, Your Customers, Your vendors, Your assignees, or any related third party and from any action, inaction, or consequence arising out of such loss, misdirection, or inaccuracy of any data, message, or information;
- * Any misuse, abuse, hostile transmission, fraud, or unlawful action arising from or related to the use of the Software or any portion thereof by or directed at You, Your affiliates, Your Customers, Your vendors, Your assignees, and/or any related third party;
- * Any claim, damage, loss, or expense related to the installation, quality, use, operation, functionality, transfer, or de-installation of the Software to You, Your Customer(s), or third parties.

* Any charges imposed by You or third parties on You or Your Customers related to Your or Your Customer(s)'s use of the Software, including but not limited to charges for data transmission and bandwidth, regardless of whether you have followed any recommendations provided with the Software or Software documentation.

6. Transfers

The rights under the License may be sublicensed under the terms of Section 1.C. or transferred to any of Your successors, heirs, or assigns. Any other attempt to sublicense, assign, or transfer any of the rights, duties, or obligations hereunder is void unless You have a separate written agreement with SmarterTools allowing for such transfer(s).

7. Jurisdiction.

This Agreement shall be governed in all respects by the laws of the United States and the State of Arizona, except for conflict of law's provisions. The parties agree that for any dispute, controversy, or claim arising out of or in connection with this Agreement, venue and personal jurisdiction shall be in the federal, state, or local court with competent jurisdiction located in Maricopa County, Arizona. The prevailing party will be entitled to an award of reasonable attorney's fees.

In the case that You are an agency or entity of the United States Government, the following additional terms apply:

* The Software qualifies as Restricted Computer Software, as defined in the Rights in Data-General clause at Federal Acquisition Regulations 52.227-14.

* Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013.

8. Payments.

You shall pay the total fee(s) for the Software imposed by SmarterTools at the time of purchase. You shall pay all invoices rendered by SmarterTools within thirty (30) calendar days after the invoice date, or within another time frame set forth by SmarterTools in writing in a separate agreement. All payments shall be made in United States Dollars (\$). If You fail to pay any amount due within the above timeframe, SmarterTools may impose late charges equal to the lesser of 1.5% per month or the highest interest rate allowable by applicable law, together with all related expenses and collection costs, including reasonable attorneys' fees, incurred by SmarterTools collecting any amounts owed under this EULA. Further, You shall reimburse SmarterTools for any out-of-pocket expenses incurred in connection with duties performed by SmarterTools hereunder. Upon request by You, SmarterTools

shall provide You with reasonable documentation evidencing the out-of-pocket expenses incurred by SmarterTools.

SmarterTools may disable License Keys for invoices that are not paid within a reasonable timeframe as determined by SmarterTools in its sole discretion. Licenses purchases that are made fraudulently, deceptively, or that result in a charge-back or disputed charge are considered to be not paid and are subject to disablement at the sole discretion of SmarterTools.

9. Limitations to Customization.

Should You choose to alter the appearance and/or user interface of the Software (the "Skin") by using the custom style or Skin options included in certain versions of the Software or by using a third-party process to alter the appearance or interface of the Software, the following requirement must be met:

- * You shall maintain and not remove any copyright notices within the comments and headers of Software files.

10. Transmission of Information and Communication.

At purchase of the Software and at other times during the term of this EULA You will be required to supply certain information including, but not limited to, email address(es), password(s), personal and/or company information, payment information (e.g. credit card information), and/or other personally identifiable and potentially valuable information. Acceptance of this Agreement indicates Your willingness to provide this information and have it transmitted to SmarterTools via internet, phone, facsimile, verbally, or otherwise and Your assumption of the incumbent risks associated with such transfers. SmarterTools takes the privacy and security of data very seriously and will make efforts to protect data in accordance with our privacy policy. A copy of the SmarterTools privacy policy is available by request. In any event, SmarterTools and its suppliers, licensors, successors, affiliates, agents, employees, executives, and assigns shall not be liable for any stolen, misdirected, or otherwise mishandled information pursuant to this EULA.

From time to time SmarterTools may contact You at any address, including any email address(es), You have provided to SmarterTools regarding the Software, available Updates or Features Selection for the Software, or for promotional purposes. You hereby expressly consent to such communications. If you do not wish to receive further notices, you may notify SmarterTools of your preferences.

From time to time the Software may cause computers, servers, and/or other electronic devices on which You install and operate this Software to use the internet or other means to exchange data with computers, servers, or other electronic devices owned by SmarterTools in order to maintain licenses, communicate updates or instructions, track the location and install base of the Software, gauge performance, enforce SmarterTools' rights with regard to licensing and this EULA, or other

information as is needed to properly maintain, protect, or update the Software. Acceptance of this Agreement indicates Your acceptance of this communication and Your assumption of the incumbent risks associated with such communication. Any attempt to prevent, preclude, disrupt, or modify this communication is not allowed under this EULA and may result in the disablement of the Software and license key.

11. Third-party Correspondence, Interaction, Purchase, Service, or Promotion

During use of the Software, You may enter into correspondence with, purchase goods and/or services from, or participate in promotions of third party advertisers or sponsors displaying goods and/or services through the Software. Any such activity, and any terms, conditions, warranties, or representations associated with such activity, is solely between You and the applicable third party. SmarterTools shall have no liability, obligation, or responsibility for any such correspondence, interaction, purchase, service or promotion between You and any such third-party including, but not limited to, translations, mapping, sharing, or any other service or transfer, even if such third-party correspondence, interaction, purchase, service, or promotion is listed as a benefit or feature of the Software. SmarterTools explicitly disclaims any liability, obligation or responsibility for the continuation, viability, quality, reliability, or availability of any such third party provided correspondence, interaction, purchase, service, or promotion.

SmarterTools does not endorse any sites on the Internet that are linked through the Software. SmarterTools provides these links to You only as a matter of convenience, and in no event shall SmarterTools or its licensors be responsible for any content, products, or other materials on or available from such sites. SmarterTools provides the Software to You pursuant to the terms and conditions of this Agreement. You recognize, however, that certain third-party providers of ancillary software, hardware, or services may require Your agreement to additional or different licenses agreements or other terms prior to Your use of or access to such software, hardware, or services.

In all events, conditions, and circumstances the provisions and limitations of Sections 3, 5, and 7 shall apply.

12. Severability.

The provisions of this Agreement will be deemed severable and the invalidity or unenforceability of any provision(s) will not affect the validity or enforceability of any other provision(s) herein.

13. Entire Agreement.

This EULA constitutes and expresses the entire agreement and understanding between the parties hereto with respect to the subject matter, all revisions discussions, promises, representation, and

understanding relative thereto, if any, being herein merged. This Agreement replaces and supersedes any prior agreement entered into between the parties hereto with respect to the subject matter herein.

Thank You for choosing SmarterTools Software.

Rev. 20150416

All materials copyright SmarterTools Inc.