# SmarterMail in Small to Medium

Help Documentation

# 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

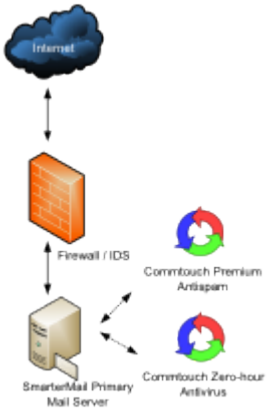
enterprise organizations with average email volumes numbering in the millions. This infers organizations with many thousands of mailboxes. Information regarding these architectures can be found in SmarterMail in High-Volume Deployments , which is available for download on the SmarterTools website.

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

**Distributed SpamAssassin Servers**

SmarterMail 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

that 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 .

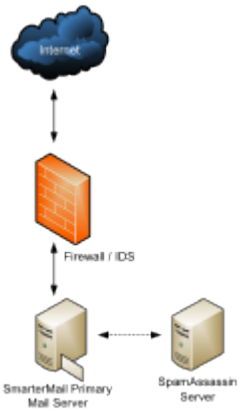
SmarterTools recommends the following hardware for stand-alone, distributed SpamAssassin servers:

- 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

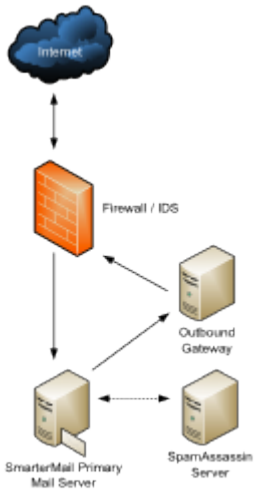
Outbound gateways are used for handling the delivery of remote mail to reduce the load on the primary mail server(s). An outbound gateway does not perform the tasks of storage and/or retrieval of end users' mail, freeing it to process many times more outgoing messages than a primary server could be expected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