



Installation and Deployment

Help Documentation

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

Copyright (c) 2018 SmarterTools Inc.

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 coexist with multiple applications on the same server based on the following minimum requirements:

- Windows 7*, Windows 8*, Windows Server 2003 or higher, including Windows Server 2012***
- SmarterMail Web server included with product
- Microsoft .NET 4.0 Framework
- A dedicated IP address to ensure proper functionality

However, SmarterTools strongly recommends using the following for maximum efficiency:

- Windows Server 2008 R2 or higher***
- 64-bit version of Windows Server

- Microsoft IIS 7.5**
- Microsoft .NET 4.0 Framework
- 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.

*Understand that Microsoft's non-server based operating systems limit the maximum number of inbound connections, which could impact performance. For more information regarding this issue, refer to the Microsoft Software EULA .

**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 7.0/7.5 in place of the SmarterMail Web server for increased performance and security. For more information, see [Running SmarterMail as an IIS Site](#) .

***Only the most current versions of SmarterMail (10.5 or higher) were tested on Windows Server 2012. Previous versions may install on Windows Server 2012 and run as well. However, some work arounds may be necessary to get them to run well. See the SmarterTools knowledge base for more information.

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.

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 may need to be reactivated.

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

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

[Return to Getting Started](#)

Upgrading SmarterMail

Because the SmarterMail 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-NetLBClusterNodeNetworkInterface . 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
- Commtouch Premium Antispam
- Commtouch Zero-hour Antivirus

Microsoft Exchange ActiveSync

Microsoft Exchange ActiveSync is a data synchronization protocol that enables over-the-air access to email, calendars, tasks and notes from most mobile devices, including 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.

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

Exchange Web Services

Exchange Web Services (EWS) is a newer data synchronization protocol that seamlessly syncs SmarterMail messages, contacts, calendars and tasks to third-party email clients for Apple products, specifically Microsoft Outlook 2011 for Mac and Apple Mail. 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 [How To Activate Exchange Web Services](#)

Commtouch Premium Antispam

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

For step-by-step instructions on how to activate and enable the Commtouch add-on, please refer to the

KB articles [How To Activate Commtouch Premium Antispam](#) and [How To Enable Commtouch Premium Antispam](#) .

Commtouch Zero-hour Antivirus

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

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

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.

Commtouch Premium Antispam

When coupled with SmarterMail, Commtouch Premium Spam protection delivers upwards of 99.5% spam protection. Commtouch technology complements SmarterMail's out-of-the-box antispam features by adding email transmission pattern recognition. The Commtouch Premium Antispam solution is available as an optional add-on to SmarterMail from the SmarterTools website and authorized SmarterTools resellers.

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

Commtouch Zero-hour Antivirus

The Commtouch 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 Commtouch 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.

- [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.

Helm (part of the Parallels 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](#)

Parallels Automation

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

- [Learn more](#)

Parallels 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](#)

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 to manage 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 highly recommended)
- 7200 RPM SATA drive

Email Virtualization: SmarterMail in Virtual Server (VPS) Environments

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

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

Recommended Spam Protection Measures

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

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

CommTouch Premium Antispam

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

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

SpamAssassin-based Pattern Matching Engine

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

Greylisting

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

Other Built-in Antispam Measures

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

Remote SpamAssassin

SmarterMail includes support for SpamAssassin, an open source spam filtering program. When implemented, SmarterMail will pass an incoming message to SpamAssassin. SpamAssassin returns

the message 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.

CommTouch Zero-hour Antivirus

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

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

SmarterMail in Small to Medium-sized Business Deployments

Who Should Use This Document

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

Determining the Required Architecture

It is not unusual for a business to generate upwards of 50 legitimate mail messages, per employee, per day on average 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:

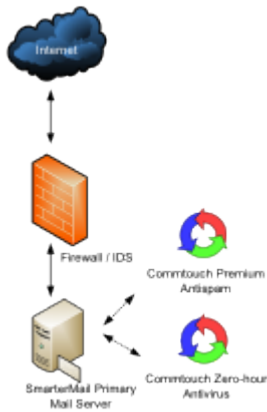
- Individuals and micro-businesses shall be defined as mail environments with average email volumes of up to 25,000 messages per day (12,500 in/12,500 out). This infers a maximum of 100 mailboxes. Information regarding these architectures is available in this SmarterTools document. Information regarding 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 highly recommended)
- 7200 RPM SATA drive (minimum)
- RAID 10 3

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

Email Virtualization: SmarterMail in Virtual Server (VPS) Environments

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

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

the virtual machines. By allowing the SmarterMail virtual machine a dedicated physical connection, this risk can be eliminated.

Recommended Spam Protection Measures

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

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

Commtouch Premium Antispam

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

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

SpamAssassin-based Pattern Matching Engine

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

Greylisting

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

Other Built-in Antispam Measures

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

Distributed SpamAssassin Servers

SmarterMail 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>.

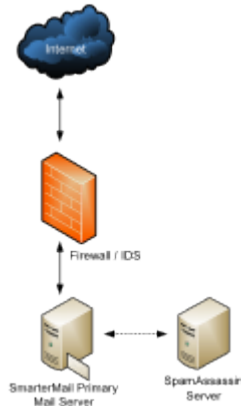
SmarterTools recommends the following hardware for stand-alone, distributed SpamAssassin servers:

- 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.

CommTouch Zero-hour Antivirus

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

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

Extending Capacity via Outbound Gateways

Outbound gateways are used for handling the delivery of remote mail to reduce the load on the primary mail server(s). An outbound gateway does not perform the tasks of storage and/or retrieval of

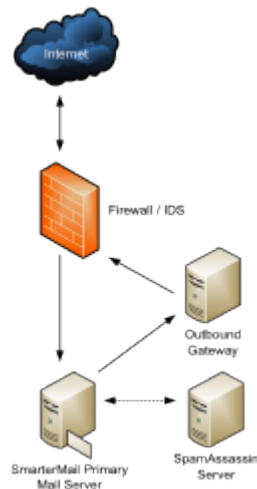
end users' mail, freeing it to process many times more outgoing messages than a primary server could be expected to handle effectively.

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

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

General Architecture with an Outbound Gateway

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



SmarterMail Outbound Gateway Servers

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

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

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

Using Third-party Solutions with SmarterMail

Inbound Gateways

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

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

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

- Barracuda: www.barracudanetworks.com
- 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.

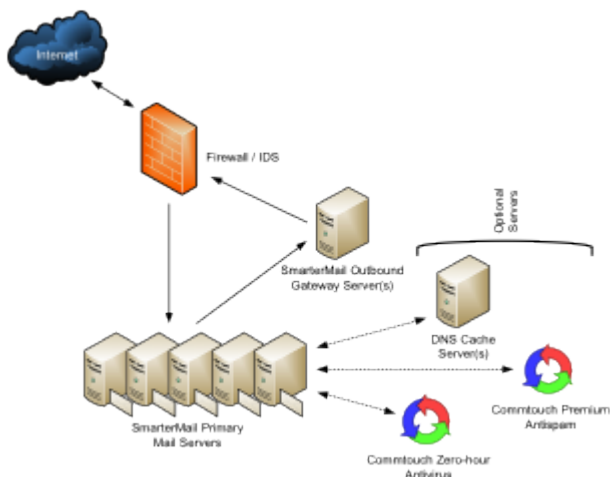
SmarterMail is built around a fully scalable model, so moving from one architecture recommendation to another requires relatively simple enhancements or modifications that can yield significant increases in performance and volume capacity.

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 space³—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.

CommTouch Premium Antispam

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

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

SpamAssassin-based Pattern Matching Engine

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

Greylisting

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

Other Built-in Antispam Measures

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

Recommended Virus Protection Measures

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

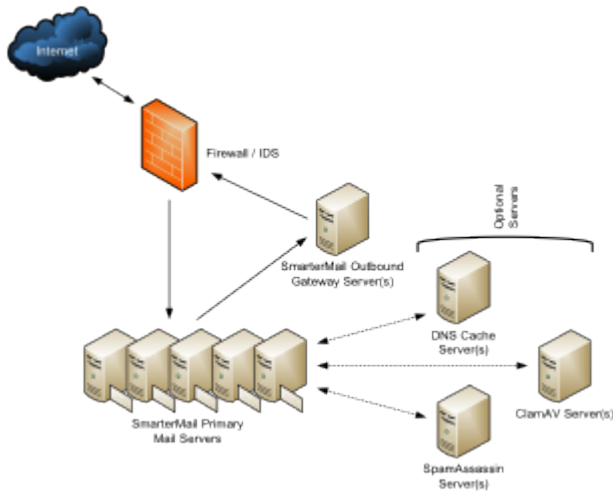
Commtouch Zero-hour Antivirus

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

For more information about the Commtouch Zero-hour 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

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.

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.
- 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(s)://your_WHMCS_hostname.com/admin/configaddonmods.php`
- Click "Activate" next to the SmarterMail Provisioning Module
- Go back to `http(s)://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(s)://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/configaddnmods.php?module=smartermail](http(s)://your_WHMCS_hostname.com/admin/configaddnmods.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

Parallels 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 for as the mail server of choice for Parallels 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.