Installation and Deployment

Help Documentation

Installation and Deployment

Browser Requirements

Desktop

SmarterMail is fully supported by any modern and updated desktop browser. Minimum versions supported:

- Google Chrome
- FireFox
- Microsoft Edge
- Safari
- Opera

Note: Any browser you use with SmarterMail should also support WebRTC to ensure video conferencing works for you and any participants. In addition, using any versions of the above browsers that are over a year old may lead to poor performance of the webmail interface.

Team Workspaces

Just as with SmarterMail in general, Team Workspaces was built to accommodate any modern, up-to-date browser. The reason for this is due to the requirements for audio, video and screen sharing available with Team Workspaces and the WebRTC protocols used on the back end. WebRTC makes real-time communciation possible within applications and is used by virtually all of the most popular web-based conferencing solutions on the market. As such, any recent browser will support Team Workspaces, and in many cases at least one or two previous versions of browsers are supported as well. That said, there are some limitations:

- Chrome and Firefox on iOS do not support WebRTC at this time. (Safari does.)
- WebRTC support was introducted in Safari 11. Previous versions are not supported.
- Legacy versions of Microsoft Edge may support WebRTC. However, the newer Chromium-based Edge browser definitely supports WebRTC so an upgrade to this version is strongly recommended for the best experience.

Mobile

In addition to working with most mobile email clients, not to mention third-party calendar and/or contact apps, SmarterMail offers the same robust webmail experience on mobile as it does on the desktop. As long as the mobile browser you use supports CSS, JavaScript and other modern scripting platforms, accessing the SmarterMail webmail interface is not a problem.

SmarterMail System Requirements

SmarterMail was designed to operate efficiently with multiple applications on the same server. Below are the minimum system requirements solely for SmarterMail. If SmarterMail is running on a server with other applications, those need to be taken into consideration and may add to the requirements listed below. In addition, high-load / high-volume servers may need to adjust the requirements as needed:

- Windows Server 2012 R2 64-bit or higher
- Microsoft .NET 4.7 Framework
- 4GB RAM
- 2-core CPU
- 1GB disk space for installation, not including mail data, file storage, etc.
- Dedicated IP address
- Active internet connection
- Microsoft Internet Information Server (IIS)

Minimal IIS Settings

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

App Pool Settings

Below are the settings for the App Pool that are typically recommended for the best web interface and EAS/EWS/MAPI performance. These settings keep the app pool running 24/7 and only do a nightly recycle at 2am server time. these are JUST the settings that are changed from the defaults:

- .NET CLR Version: v4.0
- Managed Pipeline Mode: Integrated
- Name: SmarterMail -- we generally recommend naming the App Pool the same as your SmarterMail site as this helps troubleshoot issues.
- Start Mode: AlwaysRunning
- Identity: NetworkService
- Idle Time-out (minutes): 0
- Load User Profile: False
- Specific Times: TimeSpan[] Array

Can SmarterMail Be Installed "In the Cloud"? (I.e., on Azure, Amazon AWS, etc.)

To put it simply, yes. However, the question really is "Should SmarterMail Be Installed In the Cloud" using one of the various cloud-based virtualization platforms?

Services like Azure and Amazon's EC2 platform, as well as other cloud providers, have some things to consider when determining how well any mail server will run. For example, some cloud services don't offer static IP addresses, instead rotating the IP addresses that are used. This 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. These issues can be overcome, but generally only when subscribing to high-end plans that are offered, and these can run into the thousands of dollars a month.

Therefore, while you can install SmarterMail on a cloud service such as Amazon's EC2, it is not necessarily the best solution. Using a VM with proper RAID configuration, either hosted on-premise or with a hosting provider, is generally the best, and most cost-effective, solution.

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, CPUs and/or CPU cores, 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.

Installation and Upgrade

SmarterMail comes as a single installation file that contains everything necessary to run the product and get it set up on your server, regardless of the Edition that you intend to use. The features available are based on the license used during the activation process; if no license is entered, the Free Version will be installed. SmarterMail installers -- both the .EXE and an .MSI -- are available on the SmarterMail Downloads page of our website.

Jump to:

Installing SmarterMail for the First Time

Installation

Once you've downloaded the installation file from the SmarterTools website, it's time to actually install the product. SmarterMail starts by installing it's mail service. This includes setting up all folders and directories needed to run SmarterMail. Therefore, it's just like any standard program installation:

- On the first page, you select the path for the installation and accept the license terms.
- Next, you'll input any licensing and activation information:

- Free Edition - Select this if you're going to test out SmarterMail. The Free Edition is essentially SmarterMail Enterprise (with some limitations) and works for a single domain and up to 10 email accounts.
- Enter a license key - If you have purchased SmarterMail, select this: you'll then be prompted to enter the license key so the product can be activated.
- Manual activation provided by support - In some systems, those locked behind strict network security policies for example, SmarterMail is used for internal purposes only. In these cases a "manual activation" of the product is necessary. These are provided by the SmarterTools support team.
- Once the activation information is provided, you'll see an overview of the SmarterMail version and mailbox allocation.
- Next, you provide some information about how SmarterMail appears in IIS: the Site Name, a

Hostname, IP and Port (if these are needed -- by default, SmarterMail binds to localhost on all IPs over port 9998). You can also change where SmarterMail installs by modifying the default File Path. (NOTE: IF installing SmarterMail on new hardware with the intention of migrating domains and users from another SmarterMail server, it's best to ensure you're installing using the same File Path as your previous server to ensure migrated data and settings are preserved.)

• Finally, you're given an overall summary of the installation. Clicking Install will install SmarterMail.

• On new systems, that haven't had SmarterMail installed, the installation process takes care of any additional set up and configuration that's necessary: setting up SmarterMail in IIS with an application pool and website, setting the proper permissions on both, etc.

• After the installation completes, you'll be presented with the "Welcome to SmarterMail" screen.

Welcome to SmarterMail

After SmarterMail is installed, a window opens in your default browser that takes you to the web interface for your installation. The URL used will match what was configured during the setup process, and if nothing was changed (e.g., no changes to the hostname or port), your browser will open localhost:9998/interface/setup#/.

On this Welcome page, you'll set up a few pieces of information to get started using SmarterMail:

• You'll create the primary System Administrator account

• You'll set the default base path for storing all SmarterMail data. This includes domain data, spool, log files, and POP and IMAP retrieval data, etc. By default, this path is C:\SmarterMail\

Once you have set up this information, you will redirected to the webmail interface and automatically logged in to SmarterMail using the System Administrator you created. From there, you can add in your first domain , then add users to that domain , you can modify your default domain template , adjust the security settings as needed, and more.

Manually Installing SmarterMail

Some SmarterMail administrators, specifically those who work for web hosting companies or ISPs, prefer to manually install SmarterMail. This is especially true for those administrators who have automated the installation process using SmarterMail's APIs and their own internal systems. Regardless of how you do it, SmarterTools offers a .MSI for those customers who want to manually install SmarterMail. To do this:

• Identify the server(s) on which you want to manually install SmarterMail.

• Download the .MSI from the SmarterMail Downloads page of our website. This .MSI should

be downloaded or moved to the server where SmarterMail will be installed.

• Unzip the manual installer inside the default installation path for SmarterMail, which is C:\Program Files\SmarterTools\SmarterMail.

• Register the SmarterMail service in Windows by opening a command prompt and entering the appropriate command under the folder that the unzipped files were saved to. For 64-bit, enter this command is:

```
c:\windows\microsoft.net\framework64\v4.0.30319\installutil.exe /i
mailservice.exe
• Start the mail service using Service Snap-in or by entering the following
command:

net start mailservice
• To ensure access to the webmail interface, set up an application pool for
SmarterMail, then a stie for SmarterMail in IIS site.
• Once completed, you should be able to navigate to the SmarterMail URL
using a browser and continue setting up the installation.
```

Upgrading SmarterMail

Upgrading SmarterMail is a very simple process: you simply uninstall SmarterMail using Add Remove Programs, then run the installer you download from the SmarterTools website. Yep, it's really that simple. For those worried about uninstalling first, when you use Add Remove Programs, only SmarterMail's program files are removed: NONE of the data files are touched. So all of your users, domains, settings -- all of it -- is perfectly preserved and ready to use after you install the new version you want to run.

Important Notes

While the installation of SmarterMail is quick and easy, there are a few things to be aware of, especially if you're upgrading from a Legacy version of SmarterMail (SmarterMail 16.x or earlier) to a new Build:

• Due to significant back end changes, it is not possible to roll back to a legacy version (SmarterMail 16.x or earlier) after upgrading to any current Build.

• When performing an upgrade from a legacy version to the most recent current Build, all domains will go through a conversion process and all users will be re-indexed . The re-indexing of users is handled in batches, so it can take time to complete, especially if you have a lot of users on the server.

• This conversion process should go smoothly, and it can be tracked by going to https://your-smartermail-domain/interface/convert-status. You will need to log in with the System

Admininstrator account, but that page will list every domain on the server and it's status as the conversion happens.

• If you run into errors at any point during the conversion process, please contact the SmarterTools Support Department. Be sure to provide a screenshot of the errors you're seeing in the SmarterMail interface as well as the conversion.log file from your SmarterMail Logs folder. (The default path is c:\SmarterMail\Logs.) Please send the full log file or copy and paste the snippet of text containing the domains showing an error.

• Legacy Versions of any product can be downloaded from your Account area. Simply log in to your account, and from the Account dropdown icon, select "Legacy Versions". Here you'll have access to any current Build plus the most recent release of any Legacy product.

• The Release Notes for all major and minor versions of SmarterMail, as well as Release Notes for all current Builds, are available on the SmarterMail Release Notes page of our website . It's a great idea to familiarize yourself with all the changes that have been made to SmarterMail between the version you're on and the version you'll BE on once you've upgraded.

• To ensure that the upgrade maintains the integrity of your data, settings, users, file structure, etc. it's important to keep any default settings "as is" during the installation of the upgrade. Only change default settings if they were changed for the version you're upgrading from. File paths, etc. should match exactly. For reference, the default installation file path for SmarterMail is C:\Program Files (x86)\SmarterTools\SmarterMail.

• If you are upgrading an installation that utilizes a license key, you WILL need to re-activate that key once the upgrade completes. Please be aware that license keys pertain to the version of SmarterMail you're running as well as the maximum version of SmarterMail you CAN run -- you cannot activate a key on a more recent version of SmarterMail if your key does not support that version. However, all license keys are retroactive for previous versions.

• Choose to use the same IIS site that was used previously. If IIS was not previously configured, create a new site. (NOTE: An IIS site is required in order to access the SmarterMail web interface. An IIS site can be configured after installation; however, you will not be able to access the setup wizard or web interface in the meantime. If you choose to configure the site later, you can access the IIS Configuration Tool by navigating to its default location at C:\Program Files (x86)\SmarterTools\SmarterMail\IIS Tool.)

• If you are running SmarterMail as an IIS site, IF NEEDED, change the .NET version of the Application Pool to .NET 4.0 and restart IIS.

Steps for Upgrading Legacy Versions

When upgrading a legacy version of SmarterMail, such as SmarterMail 15.x or earlier, it's very important to understand the current version and how much different it will be than the version you're upgrading from. SmarterMail has not only improved greatly from legacy versions, but it's gone

through a few interface changes along the way. This is especially noticeable if you're upgrading from particularly older versions of SmarterMail to a current Build.

In addition, we've previously recommended that customers upgrade in steps when coming from SmarterMail 14.x or earlier. However, this is no longer the case: the latest installers accommodate for all of the back end changes we've made since those versions, so it's no longer necessary to step up to SmarterMail 7.x, then SmarterMail 15.x, then on to the latest Build. In fact, it's NOT a good idea to upgrade in steps as you can carry forward any types of corruption or issues you may be having -- even if you don't notice them. There can be back end file issues that you don't see, but that break an installation if you step through upgrades. Doing a standard upgrade to the latest Build should account for any of those issues and account for them in some way: either by fixing the issues or preventing those issues from corrupting any domains or users once the upgrade is complete.

That said, if you're at a point where you're upgrading from SmarterMail 15.x or earlier, we'd be happy to help you out: simply contact our Sales or Support Department and we can help test the upgrade for you, BEFORE you actually start through the process. Doing this will allow us to troubleshoot any issues you may encounter during the upgrade, and either fix them for you or help set your expectations of what you'll see once the upgrade completes.

Upgrade Process

To upgrade SmarterMail, do the following:

- First, back up your current SmarterMail installation or take a snapshot of your VM. This will give you something to fall back on should something happen during the upgrade.
- Stop the SmarterMail website and associated Application Pool in IIS.
- Next, download the latest version of SmarterMail from our website .
- Uninstall the current version using Add or Remove Programs . This will only remove the SmarterMail program files -- no data or system files are touched. This is an important step and should not be skipped, especially if you're upgrading from an older version. Newer versions may not require this step, but it doesn't hurt.
- Run the installer.
- Upgrading is essentially like installing for the first time. The difference is that most fields will simply carry over based on your existing installation. So you'll walk through the installation just as you did when first installing the product but things like your paths, etc. will already be filled in. The upgrade process even finds the existing SmarterMail site in IIS!
- After the upgrade finishes, you're taken right to the SmarterMail login page where you can log in with your existing System Admininstrator account.

Upgrading Failover Servers

For organizations running SmarterMail Enterprise in a failover configuration -- that is, 2 SmarterMail front ends that share the domain, user and data via a network share or NAS -- the upgrade process is a bit more complex. This is because the SmarterMail installer itself generally doesn't have access to the shared drive or NAS device. Therefore, it's not possible to make any modifications to the folders and/or data that is shared on those types of storage solutions. Whlie an upgrade may not need to change any of those pieces, SmarterMail's upgrade process does still need access to them. Therefore, each server needs to be upgraded separately, with some files and folders moved temporarily during the upgrade.

Upgrading the Primary Server

For the purposes of this upgrade process, the "Primary Server" acts as the default SmarterMail server and manages the licensing of the server cluster whereas the other is considered the "Secondary Server" that remains connected to the cluster and is available as a "hot standby".

- Stop the SmarterMail Service on both the Primary and Secondary servers. The rest of these actions should be performed on the Primary Server.
- Uninstall the old version of SmarterMail via Add/Remove Programs.
- Install the new version of SmarterMail.
- Stop the SmarterMail Service again. (It will restart after the installation).
- Right-click on the SmarterMail Service and go to the Log On tab. Make sure the account being used has the proper permissions/credentials for accessing the shared directory.
- Start the SmarterMail Service. The old "failoverConfig.xml" on the shared drive should be converted to failover.json, which is saved in the Service\Settings directory.
- Verify that the domains loaded properly.

Upgrading the Secondary Server

Upgrading the Secondary Servers is a bit easier as you don't need to move files between the two servers.

- Stop the SmarterMail Service on both the Primary and Secondary servers. The rest of these actions should be performed on the Primary Server.
- Uninstall the old version of SmarterMail via Add/Remove Programs.
- Install the new version of SmarterMail.
- Stop the SmarterMail Service again. (It will restart after the installation).
- Right-click on the SmarterMail Service and go to the Log On tab. Make sure the account being used has the proper permissions/credentials for accessing the shared directory.
- Start the SmarterMail Service. The old "failoverConfig.xml" on the shared drive should be

converted to failover.json, which is saved in the Service\Settings directory.

- Stop the SmarterMail Service one more time.
- Edit the failover.json file to match the failover.json on the Primary Mail Server.
- Start the mailservice on BOTH the Primary and Secondary Servers.
- Verify that the domains loaded on the Secondary Server match the Primary Server.

After both servers have been upgraded, it's best to perform some tests to ensure that the failover acts as expected and that any backups being performed are working.

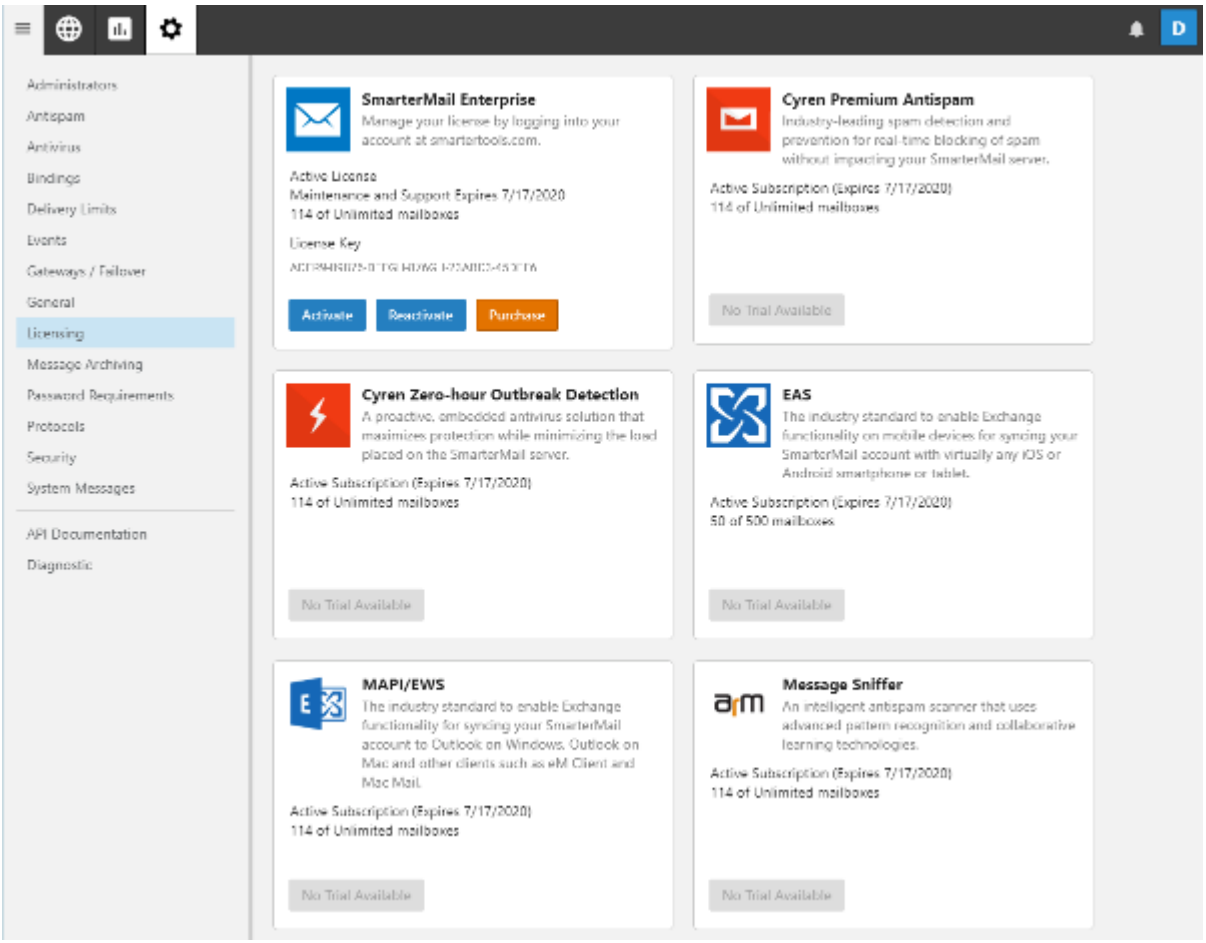
Licensing and Activation

During the installation process for SmarterMail, you're asked to input a license key, which defines the Edition and mailbox count that is activated once the installation completes. If you so desire, you can install SmarterMail as the Free Edition, which is good for use with 1 domain and up to 10 mailboxes.

To upgrade to a paid version and unlock additional mailboxes and/or gain access to use purchased SmarterMail Add-ons , a license key must be activated. Furthermore, if the SmarterMail installation is moved to another server or upgraded to a different version or product level, the product will need to be activated again. System Administrators can use the Licensing section to activate SmarterMail or view current licensing information and limits.

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. If the server cannot connect for security reasons or due to internet connectivity, please contact sales@smartertools.com to request steps for a manual activation. A manual activation requires the server's hostname, which can be found by entering 'hostname' into the server's command prompt.

To access the Licensing section, log into SmarterMail as a System Administrator and click on the Settings icon. From there, click on Licensing in the navigation pane. The current licensing details for SmarterMail and its add-ons will be displayed, including the license key, license level information, status of the license or subscriptions, the number of items used out of the total limit, and an indication of whether an add-on trial is available.



The following actions can be taken:

- Activate - Select this option to activate a new SmarterMail license key. Activating a paid license requires authentication by verifying the SmarterTools account login credentials. Trial license keys do not require authentication to be activated.
- Reactivate - Select this option to refresh the limits of the SmarterMail installation. This will cause SmarterMail to callback to the SmarterTools servers to refresh the limits of the license key and should be used after purchasing an add-on, upgrading to the Enterprise edition or increasing the mailbox limit. Reactivating is immediate and does not require authentication with the SmarterTools account credentials.
- Purchase - Select this option to be taken to the SmarterTools website where you can purchase a new license key or add-on.
- Start Trial - If an add-on trial is available, a Start Trial button will appear on its card. This allows the system administrator to test the functionality for up to 30 days. A trial can only be activated one time. To continue using the service after the trial, the add-on must be purchased. In addition, trials are not availble on Free Editions of SmarterMail. Note: The ActiveSync trial is limited to 25 Mailboxes.

Note: If you are running a trial version of SmarterMail, it will automatically revert to SmarterMail Free when the trial expires.

Configuring SmarterMail for Failover

This feature is only available in SmarterMail Enterprise.

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.

To review the Failover Servers configured for an installation, log into SmarterMail as a System Administrator and click on Gateways / Failover in the navigation pane. Then click on Failover Servers tab .

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 2012 R2 64-bit or higher. (Windows Server Core is not currently supported).
- Three IP addresses
- Both servers must have their server times synchronized
- A domain account or local system User or Group account with bi-directional authentication. (NOTE: SmarterMail can NOT be run using Local System, Local Service or Network Service in a failover configuration.)
- 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 Settings folder
• Configure your permissions accordingly. The SmarterMail service needs to run as a domain account or a local account with bi-directional authentication. You can configure this within the Windows Services console. When running SmarterMail with failover, Local System, Local Service and Network Service users are not allowed. 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

• Manually install and configure a primary SmarterMail server using the .MSI file available from the SmarterMail downloads page . Then, stop the service on this primary installation.
• Manually install another SmarterMail Enterprise instance on a second server. This new installation 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 failover.json file in the primary server's Settings folder as follows. (Default location is C:\Program Files (x86)\SmarterTools\SmarterMail\Service\Settings.)

• FailoverIPAddress - Set this to the IP address of the Network Load Balancer
• IsEnabled - Set this to True
• SharedSystemFilesPath - Set to the shared network shared system folder

A sample failover.json would look like this:

```
{ "NodeId": "a51eba87-c8c6-49e3-812f-84e46ab617e7", "FailoverIPAddress": "122.32.55.241", "IsEnabled": true, "SharedSystemFilesPath": "\\\\serverName\\SmarterMail\\Service\\Settings" } NOTE: The code should look like the above: casing, proper escaping of paths, etc. in order for the JSON to be read properly.
• Save this file, then copy it to the hot standby's Settings folder, replacing the existing failover.json
• Copy over all folders and files from C:\Program Files (x86)\SmarterTools\SmarterMail\Service\Settings to the Settings 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 Administrator and going to the activation section. 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 IP Addresses 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, log into the primary server as the System Administrator and go to Gateways / Failover . The servers that are part of the failover cluster will be displayed on the Failover Servers tab.

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 failover.json file in the primary server's Settings folder as follows:

• FailoverIPAddress - Set this to the IP address of the Network Load Balancer
• IsEnabled - Set this to True
• SharedSystemFilesPath - Set to the shared network shared system folder

A sample failover.json would look like this:

```
{ "NodeId": "a51eba87-c8c6-49e3-812f-84e46ab617e7", "FailoverIPAddress":
"122.32.55.241", "IsEnabled": true, "SharedSystemFilesPath":
```

"\\\\serverName\\SmarterMail\\Service\\Settings" } NOTE: The code should look like the above: casing, proper escaping of paths, etc. in order for the JSON to be read properly. Also, due to size limitations, in the sample above the SharedSystemFilesPath is split across 2 lines -- that should be ONE line.

• Copy that failover.json file, after you've edited it, and move it to the same location on the hot standby. You should replace the file on the hot standby, if it already exists.

• Run the robocopy one more time to copy over any modified files and remaining spool emails

• Copy over all folders and files from C:\Program Files (x86)\SmarterTools\SmarterMail\Service\Settings to the Settings folder in the shared service directory you created

• Edit the domains.json file in the shared Settings folder and change the path of your domains to match the new NFS\SMB path. (For example, \\NAS01\SmarterMail\Domains\mydomain.com)

• Edit the settings.json 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 Administrator

• Activate your Enterprise key on the hot standby by logging into SmarterMail's management interface as the System Administrator and going to the Licensing section.

• 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 the Licensing section.

• Verify mail data and settings are being accessed from the shared service directory

Scripting Failover

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

Prepping PowerShell on the Servers

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

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

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

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

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

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

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

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

```
$StopSecondary = New-PSSession -ComputerName Server02 Invoke-Command -
Session $StopSecondary -ScriptBlock { Import-Module
NetworkLoadBalancingClusters ; Stop-nlbclusternode -HostName Server02 -
InterfaceName "WAN" ; import-module WebAdministration ; stop-webapppool
```

```
SmarterMail; set-service -computerName Server02 -name mailservice -status
stopped ; remove-pssession Server02}

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

SmarterMail Add-ons

SmarterTools' add-on licensing system allows users to enhance the functionality of SmarterTools products. Information about the add-ons available for your installation, purchasing and/or activating add-ons can be found on the Licensing and Activate page of this online help.

The following add-ons are available for SmarterMail:

- EAS (Microsoft Exchange ActiveSync)
- MAPI (Messaging Application Programming Interface)/EWS (Exchange Web Services)
- Message Sniffer
- Cyren Premium Antispam
- Cyren Zero-hour Antivirus

EAS

EAS 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, EAS enables SmarterMail users to have access to their email, calendars, tasks, and notes while working offline. Finally, Windows Mail, People and Calendar all support EAS for syncing mail, contacts and calendars.

MAPI/EWS

MAPI provides users with native Microsoft Outlook synchronization and functionality at the server level. Available for Outlook 2016 and above, MAPI offers standard functionality such as syncing emails, calendars, contacts, tasks and notes, but also additional functionlity that is available when connecting Outlook to Microsoft Exchange.

EWS seamlessly syncs SmarterMail messages, contacts, calendars and tasks to third-party email clients, including Apple Mail for MacOS and eM Client for Windows. EWS allows for fast communication between an email client and the mail server.

Message Sniffer

Message Sniffer complements SmarterMail’s built-in antispam and antivirus features and accurately captures more spam, viruses, and malware when combined with SmaterMail's "out of the box" protection. 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.

Cyren Premium Antispam

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

Cyren Zero-hour Outbreak Detection

The Cyren Zero-hour Outbreak Detection add-on is a service that identifies new, "zero hour" 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.

Antispam and Antivirus Integration

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

Message Sniffer

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

new spam and malware attacks. The Message Sniffer solution is available as an integrated add-on to SmarterMail from the SmarterTools website and authorized SmarterTools resellers.

- Learn more
- Buy now

Cyren Premium Antispam

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

- Learn more
- Buy now

Cyren Zero-hour Outbreak Detection

The Cyren Zero-hour Outbreak Detection uses Recurrent Pattern Detection to identify viruses based on their unique distribution patterns and provides a complementary shield to conventional AV technology. Cyren Zero-hour Outbreak Detection 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 .

- Lean more

Declude

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

- Learn more

F-Prot

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

- Learn more

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.

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

- Learn more --%>

Plesk (7.5 or higher)

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

- Learn more

WebSitePanel

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

- Learn more

WHMCS

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

- Learn more

HostingController

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

- Learn more

Automation with Web Services

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

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

Note: Web services are intended for use by high-volume and automated business environments, and hosting companies as they develop procedures to manage their SmarterMail system and workflow. 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 our Small to Medium-sized Business guide.
- High-volume deployments shall include ISPs, hosting companies, large businesses, and

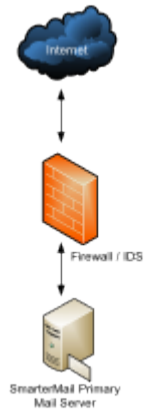
enterprise organizations with average email volumes numbering in the millions. This infers organizations with many thousands of mailboxes. Information regarding these architectures is available in our High Volume Deployments guide.

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

Small businesses generally have a single SmarterMail server that processes all mail for all users. This includes webmail client logins, antispam and antivirus protection, syncing of contacts, calendars, tasks and notes using a syncing protocol, and it can even include archiving, if necessary. Just remember: the more you add, the more you need in terms of processing power and memory. In addition, if the server processes large amounts of email, it may be necessary to add a larger hard drive, or even move from standard hard drive configuration, such as a SATA drive, to using a SSD. Here is what a standard Small Business Deployment looks like:



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:

- Dual-core processor
- 2+ GB of RAM
- Windows Server 2012 R2, 64-bit is required
- 250GB SSD for your Operating System and data (NOTE: size is dependent on the number of

users, data to store, etc.)

• 250GB 7200 RPM SATA drive for your Spool

A Note on the Spool

Nothing taxes hard drives more than an email server. Due to the nature of what a mail server does, i/o is a HUGE mitigating factor in terms of performance. This is because, generally, so many files are written to, and read from, the hard drive. As a result, even on small installations it's a good idea to keep your Spool -- the primary location where ALL messages go when they're sent or received -- on a drive that's separate from your operating system. The Spool folder, while crucial to a mail server working properly, can be relatively transitory -- moved, renamed and re-created, etc. as needed. However, your OS drive is not. In addition, as so many files are written to the Spool, the drive where the Spool is located should be defragged regulary.

Email Virtualization: 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). The most important factor of performance in a shared environment is the design and implementation of the storage network to ensure SmarterMail has enough IOP availability to the storage pool. Leveraging iSCSI with IO Multipathing is recommended over standard 1Gbe connections if fiber channel, or 10Gbe is unavailable.

SmarterMail in the Cloud

SmarterMail has been tested in Amazon EC2, Google Cloud, as well as Azure and functions as expected. One thing to take into consideration here is ordering the proper instance with adequate storage IOPS.

Please take into consideration, most cloud providers also restrict SMTP traffic.

With Amazon, you'll need to fill out a request form to remove e-mail sending limitations. This can be found here: https://aws.amazon.com/forms/ec2-email-limit-rdns-request?catalog=true&isauthcode=true

With Google Cloud, you'll need to leverage an Outbound gateway such as SendGrid. More information can be found here: https://cloud.google.com/compute/docs/tutorials/sending-mail/

Windows Azure does not place such restrictions when it comes to sending out over port 25 but do place restrictions on overall outgoing traffic and implement bandwidth throttling based on the size of your VM.

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.

Securing an Email Server for Small Business

SmarterMail's included antispam and antivirus measures will work perfectly fine for most small business installations. That said, they may need monitoring and scores adjusted as needed to ensure that the majority of spam your mail server receives is handled appropriately. In addition, it's recommended that greylisting is used. While this can impact the delivery of messages, it's a good way to prevent one-off spam messages from getting through. The unfortunate thing about spam is that there is no silver bullet: spam protection takes some time and diligence. However, having multiple layers of spam protection, like using the included antispam measures, greylisting and potentially adding in another antispam measure, is the best approach to keeping inboxes free from the clutter of unwanted email.

The nice thing is, if additional services are needed, they can be easily integrated into SmarterMail. That includes Cyren Premium Antispam and Zero-hour Antivirus, as well as any third-party services a business wants to implement. (E.g., SpamExperts.) In addition, SmarterMail runs well if other antivirus products are used on the server, such as AVG or Eset.

Regarding security, the default security settings will be fine for most small businesses. However, it's never a bad idea to implement good password policies and have IDS in place to ensure your mail server is at least protected. Other things, like throttling and more, can be put in place to ensure your mail server remains unaffected should issues occur, such as a mailbox becomes compromised. In these instances, throttling can keep that compromised account from blasting out emails that could get your mail server blacklisted.

Then there's putting things in place to help offer proof that an email is originating from the server it says it's coming from. These include DKIM, SPF and DMARC, which are all supported by SmarterMail. These, PLUS requiring SMTP authentication for your users, can help prevent mail from being blocked at the recipient's mail server.

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 can be found in our Individual and Micro-business Deployments guide.
- 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 this guide.
- 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 our High Volume Deployments guide.

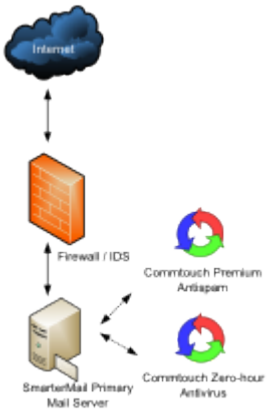
1 Intel presentation, “IT Business Value”, 9-16-2005.

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

Medium-sized businesses generally still have a single SmarterMail server that processes all mail for all users. The difference is in the number of users and the amount of daily message traffic. Medium businesses will almost always move beyond webmail usage and have syncing in place for mobile devices using technologies like EAS and/or EWS. Based on the amount of email they process, medium businesses will also have multiple antispam measures in place, such as Cyren Premium Antispam. Depending on the business, they may also require email archiving.

As with ANY SmarterMail installation, the more you add, the more you need in terms of processing power and memory. In addition, if the server processes large amounts of email, it may be necessary to add a larger hard drive, or even move from standard hard drive configuration, such as a SATA drive, to using a SSD. Here is what a standard Medium Business Deployment looks like:



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
- 6 GB of RAM
- Windows Server 2012 R2, 64-bit is required
- 4 x 7200 RPM SATA drive (minimum) for OS and data (NOTE: SSDs can be used as needed

or as budget allows)

• RAID 10 3

• 500GB 7200 RPM SATA drive for the Spool

3 Regarding the RAID 10 recommendation, we realize that some companies have policies in place that require the use of alternate RAID configurations. This is perfectly acceptable, except RAID 1 is NOT recommended. Using RAID 1 arrays will likely result in significant reductions in hard drive performance -- up to a 50% loss vs. a single drive and up to 8x slower than a 4-drive RAID 10 implementation. Estimated i/o usage for a medium-sized deployment can range between .5 - 3 MBps or between 128 and 758 IOPS.

A Note on the Spool

Nothing taxes hard drives more than an email server. Due to the nature of what a mail server does, i/o is a HUGE mitigating factor in terms of performance. This is because, generally, so many files are written to, and read from, the hard drive. As a result, even on small installations it's a good idea to keep your Spool -- the primary location where ALL messages go when they're sent or received -- on a drive that's separate from your operating system. The Spool folder, while crucial to a mail server working properly, can be relatively transitory -- moved, renamed and re-created, etc. as needed. However, your OS drive is not. In addition, as so many files are written to the Spool, the drive where the Spool is located should be defragged regulary.

Email Virtualization: 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). The most important factor of performance in a shared environment is the design and implementation of the storage network to ensure SmarterMail has enough IOP availability to the storage pool. Leveraging iSCSI with IO Multipathing is recommended over standard 1Gbe connections if fiber channel, or 10Gbe is unavailable.

SmarterMail in the Cloud

SmarterMail has been tested in Amazon EC2, Google Cloud, as well as Azure and functions as expected. One thing to take into consideration here is ordering the proper instance with adequate storage IOPS.

Please take into consideration, most cloud providers also restrict SMTP traffic.

With Amazon, you'll need to fill out a request form to remove e-mail sending limitations. This can be

found here: https://aws.amazon.com/forms/ec2-email-limit-rdns-request?catalog=true&isauthcode=true

With Google Cloud, you'll need to leverage an Outbound gateway such as SendGrid. More information can be found here: https://cloud.google.com/compute/docs/tutorials/sending-mail/

Windows Azure does not place such restrictions when it comes to sending out over port 25 but do place restrictions on overall outgoing traffic and implement bandwidth throttling based on the size of your VM.

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

Recommended Spam Protection Measures

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

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

Message Sniffer

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

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

Cyren Premium Antispam

Available as an optional add-on for SmarterMail, Cyren Premium Antispam uses recurrent pattern detection (RPD) technology to protect against spam outbreaks in real time. Rather than evaluating the content of messages, the Cyren Detection Center analyzes large volumes of Internet traffic in real

time, recognizing and protecting against new spam outbreaks the moment they emerge. When combined with SmarterMail's out-of-the box antispam measures, the Cyren Premium Antispam add-on can effectively block 99% of spam from users' inboxes.

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

SpamAssassin-based Pattern Matching Engine

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

Greylisting

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

Other Built-in Antispam Measures

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

Distributed SpamAssassin Servers

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

The Windows version is limited to processing a single message at a time, effectively handling approximately 25,000 spam messages per day and is usually more than adequate to the needs of individual and micro-business environments. However, the Linux version of SpamAssassin can process multiple spam messages simultaneously, allowing it to process significantly more messages

than its Windows counterpart. Therefore, SmarterTools recommends the stand-alone Linux version of SpamAssassin for small to medium-sized business environments (see Figure 2).

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

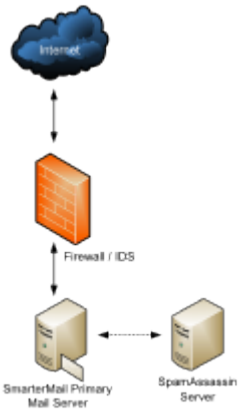
SmarterTools recommends the following hardware for stand-alone, distributed SpamAssassin servers:

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

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

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

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



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

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

Recommended Virus Protection Measures

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

Cyren Zero-hour Outbreak Detection

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

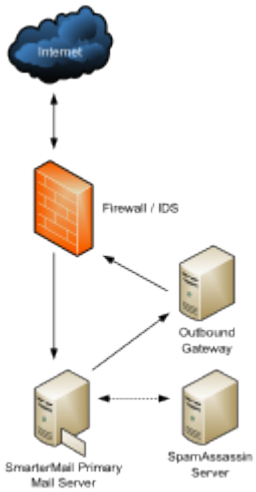
Outbound gateways are used for handling the delivery of remote mail to reduce the load on the primary mail server(s). An outbound gateway does not perform the tasks of storage and/or retrieval of end users' mail, freeing it to process many times more outgoing messages than a primary server could be expected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

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. In higher volume environment's it's also important to realize how end users synchronize mail to various mail clients and mobile devices (using POP, IMAP, EAS, EWS, MAPI, or a variety of all of these) and how this can impact resource availability such as drive i/o.

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.

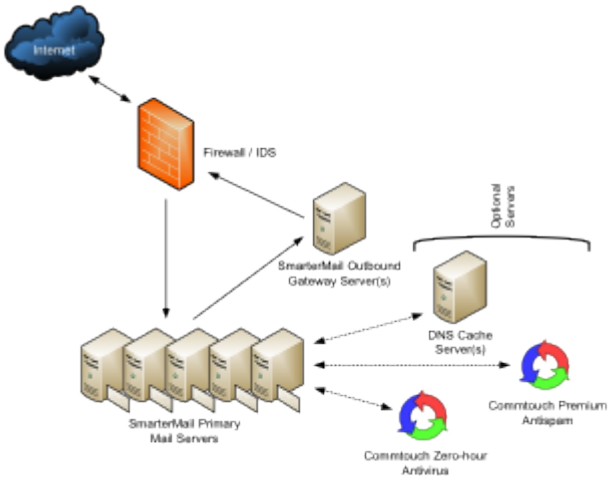
That said, the authors have chosen to divide their recommendations into three categories: individual and micro-business architectures, small to medium-sized business architectures, and high-volume deployment architectures. For the purposes of these recommendations:

- 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 our Individual and Micro-business Deployments guide.
- 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 our Small to Medium-sized Business Deployments guide.
- 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

This server is the central data processor and repository of your client's email. Users connect to this server using POP, IMAP, EAS, EWS or MAPI 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. Users can also synchronize their contacts, and calendar across several different methods. A SmarterMail network may contain one or more mail servers. Under normal activity—and assuming sufficient disk space 3 —each server should be able to handle up to 40,000 users per server (1 million messages per day).

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

- Dual-core, server-grade processors
- 8 - 16 GB of RAM, depending on the sycn technologies used
- RAID 1 array for the operating system and program files
- One single SSD drive or RAID 0 array for the email spool
- RAID 10 4 array to store user data and email (8 disk minimum when using platter drives, even SAS 10 and 15k drives.) If a Hybrid setup can take place with SSD Cache on a RAID10, even better. The administrator will want to configure their storage to optimize random 4k reads\writes. SmarterMail is very heavy on random Reads\Writes on small sectors. Estimated IOPS usage for a high volume deployment = 10-20 MBps with heavy random 4k reads\writes,

which breaks down to 5,000 - 10,000 IOPS.

• Windows Server 2012 R2 or higher, 64-bit is required

• Virtual machines are not recommended for large deployments as restrictions on disk i/o can seriously impact performance. (Though this is not a factor when leveraging properly designed storage networks with adequate i/o availability)

Email Virtualization: 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). The most important factor of performance in a shared environment is the design and implementation of the storage network to ensure SmarterMail has enough IOP availability to the storage pool. Leveraging iSCSI with IO Multipathing is recommended over standard 1Gbe connections if fiber channel, or 10Gbe is unavailable.

SmarterMail in the Cloud

SmarterMail has been tested in Amazon EC2, Google Cloud, as well as Azure and functions as expected. One thing to take into consideration here is ordering the proper instance with adequate storage IOPS.

Please take into consideration, most cloud providers also restrict SMTP traffic.

With Amazon, you'll need to fill out a request form to remove e-mail sending limitations. This can be found here: https://aws.amazon.com/forms/ec2-email-limit-rdns-request?catalog=true&isauthcode=true

With Google Cloud, you'll need to leverage an Outbound gateway such as SendGrid. More information can be found here: https://cloud.google.com/compute/docs/tutorials/sending-mail/

Windows Azure does not place such restrictions when it comes to sending out over port 25 but do place restrictions on overall outgoing traffic and implement bandwidth throttling based on the size of your VM.

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.

SmarterMail Outbound Gateway Servers

SmarterTools recommends the following hardware for SmarterMail outbound gateways:

- Dual-core processor
- 1 GB of RAM
- SSD drive for dedicated spool, though SATA can be used for lower volume

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

Configuring SmarterMail for Failover

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

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

Recommended Spam Protection Measures

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

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

Message Sniffer

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

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

Cyren Premium Antispam

Available as an optional add-on for SmarterMail, Cyren Premium Antispam uses Recurrent Pattern Detection (RPD) technology to protect against spam outbreaks in real time. Rather than evaluating the content of messages, the Cyren Detection Center analyzes large volumes of Internet traffic in real time, recognizing and protecting against new spam outbreaks the moment they emerge. When combined with SmarterMail's out-of-the box antispam measures, the Cyren Premium Antispam add-on can effectively block 99% of spam from users' inboxes.

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

Greylisting

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

Other Built-in Antispam Measures

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

Recommended Virus Protection Measures

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

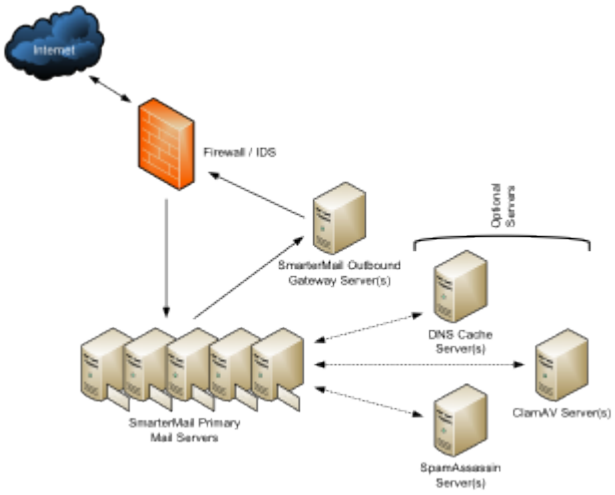
Cyren Zero-hour Outbreak Detection

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 Outbreak Detection 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 Outbreak Detection 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 that 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
- 2 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. Instead, the load should be passed to third-party products.

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 inbound gateway when using a third-party inbound gateway solution.

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

Summary

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

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

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

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

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

Integrations

Base WHMCS SmarterMail Provisioning Module

Package Description

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

Package Goals

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

The package provides the following services:

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

Prerequisites

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

Installing the SmarterMail Module

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

- Extract the SmarterMail module
- Place contents in your WHMCS directory under "..modules/addons/smartermail"
- Navigate to http(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/configaddonmods.php?module=smartermail
• Here, you're presented with the SmarterMail server interface. This is where you create, suspend, set max domain counts and delete SmarterMail servers
• Click "New Server"
• Fill in the following settings:

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

WHMCS Product/Service Module

Package Description

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

Package Goals

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

The package also provides the following services:

Admin Area Features

• Create Domain
• Suspend Domain

- Unsuspend Domain
- Terminate Domain
- Change Package
- Change Password

Client Area Features

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

Prerequisites

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

Installing the SmarterMail Server Module

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

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

Configure WHMCS to Access and Group SmarterMail Servers

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

- Login to WHMCS as a System Administrator
- Click Setup → Products\Services → Servers
- Click add new server across the top

- Enter Server information for the SmarterMail server to be added
- Under Server Details, select the Type of ‘smartermail’ and enter System Administrator credentials
- Save your changes

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

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

Configure Your Product/Service

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

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

WHMCS Client Area

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

Client Area To access SmarterMail through the client area:

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

Add User To add a user:

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

Edit User To edit a user:

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

Add Alias To add an alias:

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

Edit Alias To edit an alias:

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

Odin APS (Automated Provisioning System) Package for SmarterMail

Package Description

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

Package Goals

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

- Domain Services

- Add / Remove Domains
- Add / Edit / Remove Domain Aliases
- Add / Edit / Remove User Aliases
- Domain Disk Space Reporting
- Mailbox Services

- Add / Edit / Remove Mailboxes
- Configure Email Forwarding Settings
- Configure Auto-responder Settings
- Mail List Services

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

Prerequisites

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

- Existing installation of Parallels Operations Automation (PoA)
- Existing, licensed installation of SmarterMail 9.x or above
- Required knowledge in the following areas:

- Application Manager

- APS catalog
- Importing packages
- Provisioning Manager

- Resource templates
- Service templates
- Customer Manager

- Creating of customers
- System director

- Task manager

Installation

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

• Applications

• Expand Service Director
• Expand Application Manager
• Select Applications
• Click on “Import Package”
• Select “local file” option and click “Choose File”
• Provide the path to the SmarterMail APS
• Check “Enabled” option
• Finally click “Submit” and the package will be scheduled for importing
• APS Catalog

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

Configuration

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

Resource Types

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

• General package settings
• Global settings
• Default settings
• Services

Creating an Application

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

• Expand Service Director
• Expand Application Manager
• Select Applications

• Select the “Application” field and search for ‘SmarterMail*’
• The results should yield the ‘SmarterMailAPS’ package that was installed prior (where applicable)
• Select the ‘SmarterMailAPS’ package
• Click the “Resource Type” tab
• Click “Create”

• Select Application from the Resource Class list
• Give it a name (Ex: SmarterMail App) & Description, click “Next”
• Fill in the following fields under the “Global application settings” section:

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

Creating an Application Service

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

• Navigate to the “Resource Types” section of the SmarterMail APS package. Follow the same steps when creating an application resource to get to this section.
• Click "Create"

• Select Application Service from the Resource Class List
• Give it a name (Ex: SmarterMail App Domain Service) & Description, click “Next”
• Select from the list of services the application service will be (Ex: SmarterMail Domain Service)
• Provide default values for this resource, then click “Next”
• Priority can be any number, so let’s go with 1, Click “Next”
• Click “Finish”

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

Service Templates

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

Creating a Service Template

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

- Provide a name & description
- Uncheck “Autoprovisioning”
- Set “Type” to Custom
- Click “Next”
- A list of available Resources will be shown

- Select the Resource Application that was created earlier as well as any of the Resource Application Services that were just created. For example, "SmarterMail App" and "SmarterMail App Domain Service"
- Click "Next"
- Set the limits of the service template

- Check Unlimited for the Resource Application (Ex: SmarterMail App), Application Backup and Application User
- Resource Application Services (Ex: SmarterMail App Domain Service) can be either set to unlimited or can have a limit applied to them
- Home Visibility is an optional field that can be checked, if desired, that provides usage information for the user when they log in
- Click "Next"
- Review your settings, then click "Finish"

Subscriptions

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

Creating a Subscription

- Expand Service Director
- Expand Provisioning Manager
- Select Service Templates

• Select the “Service Template” field and search for, then select, the service that was created prior
• Click “Activate” under the General section of the service template (the service template must be activated prior to adding a subscription)
• Click “Subscriptions” tab
• Click “Create New Subscription”
• Select the “Company” field and search for the company that will be subscribing to this template, then select the company from the search results
• Set additional resource limits for the subscription if desired (subscriptions will inherit the values from the service template by default)
• Click “Next”
• Review the settings and click “Finish”

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

Package Setup and Usage

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

Setup

Creating a Domain

• Expand Operations Director
• Expand Customer Manager
• Select Customers
• Select the "Company" field and search for a company, then select the company from the search results
• Click the Resources tab
• Click "Add New Domain"

• Provide a domain name (e.g., example.com)
• Check "Set Registrar Status to Ready"
• Select the SmarterMail APS subscription from the "Subscription" dropdown
• Click "Next"
• Click "Next" again
• Review the settings and click "Finish"

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

Usage

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

Login

- Expand Operations Director
- Expand Customer Manager
- Select Customers
- Select the “Company” field and search for the company, then select the company from the search results
- Click “General” tab
- Click “Staff Members” and a list of staff members will be shown
- Click “Login as Customer”

Configure

- Click the “SmarterMailAPS” link towards the bottom of the page
- Click “Add New”
- Fill in the following fields:

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

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

Website Panel Module for SmarterMail

Package Description

WebsitePanel is a multi-tenant, enterprise hosting automation tool with support for private cloud servers. It enables you to centralize the management of your hosting infrastructure and share resources

across multiple customer accounts. This product can be used with SmarterMail and SmarterStats to deploy users and domains\sites from a single interface.

Package Goals

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

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

Prerequisites

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

Configuration

Once all of the prerequisites are met, configuring the modules is fairly straightforward. The steps below cover adding a new server to your environment, creating a hosting plan, and creating a customer account to utlize 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 email 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.