PerfectMail
Setup Guide

Version: 3.7.6
November 14, 2013

Contents

Contents

1 Copyright Notice

2 Welcome to PerfectMail™

Welcome to the *PerfectMail™ Anti-Spam Solution*. PerfectMail is an *Edge Transport Server* product that filters e-mail *before* it reaches your Mail Server. We provide a flexible solution that works with all SMTP based e-mail products; including Microsoft Exchange™, Lotus Domino™, Novell GroupWise™, Sendmail™, QMail™, etc. PerfectMail™ is a complete server product that can be installed on most modern hardware and virtualized environments.

Our focus is on *business e-mail*. Our mantra is: **No False Positives**!

3 PerfectMail™ Setup Procedure

Congratulations and thank you for purchasing PerfectMail™. Setting up PerfectMail is fast and easy; it should take about 30 minutes. Before proceeding with the install, please read this entire document. The Setup process involves the following steps:

1. Learn about PerfectMail™
2. Build/Purchase either a Physical or Virtual Server
3. Install PerfectMail
4. Initial PerfectMail Configuration
5. PerfectMail Detailed Configuration
    i. Update General Configuration Settings
    ii. Configure Domains and Users
    iii. Configure Filter Settings
6. Perform Post Install tasks
    i. Redirect Incoming E-mail
    ii. Redirect Outgoing E-mail
    iii. Update firewall settings

3.1 Mail Server Compatibility

PerfectMail™ is **guaranteed** to be compatible with your mail server!

PerfectMail products are compatible with **all SMTP or ESMTP compliant mail servers** including:

- Microsoft Exchange™
- Lotus Domino™
- Novell GroupWise™
- IMail, QMail, Sendmail
- Communigate, Scalix
- MDaemon, eMailMan, MerakMail Server
- And about 1,000,000 other mail server products!

If your mail server program is not on our list, please Contact Us to verify compatibility.

3.2 PerfectMail Documentation

For detailed information on PerfectMail™ and it's user interface, please refer to the *PerfectMail™ Administrator's Guide*. If you do have any questions or problems, please contact our PerfectMail™ support team <support@perfectmail.com>.

To download the latest install image and get up-to-date documentation please visit our download site at http://www.perfectmail.com/download

A selection of documents are available from the web interface under the *Documentation* menu. Administrators should read the *Admin Guide*. Current documents include:

- Setup Guide
- Admin Guide
- User Guide
- License Agreement

We're always interested in improving our product and documentation, so all your comments and requests are highly valued.

4 Important PerfectMail Setup Notes

The PerfectMail™ Edge Transport Server is a complete *Operating System* and *Application* bundle. PerfectMail includes a highly customized and secured version of Linux. However, knowledge of Linux is not required. All administrative duties can be performed using our *web based user interface*.

WARNING: The Installation CD performs a complete system install. It will erase all existing software on the existing machine. Be sure this is what you want before you install PerfectMail.

PerfectMail acts as an *SMTP relay host*
It makes filter or forward decisions by examining many aspects of an e-mail, including message structure, content, reputation and verification.

PerfectMail does not replace your mail server
PerfectMail filters and forwards e-mail, but is separate from and does not replace your existing mail server. You must run your own mail server; e.g. MS Exchange, Lotus Domino, GroupWise, Sendmail, QMail, etc.

PerfectMail must be your MX Host!
PerfectMail *must* be the first point of contact with the Internet. PerfectMail *must act as a mail exchanger* for your domains (i.e. your DNS MX records will be pointing directly to PerfectMail). If e-mail is relayed through a proxy or intermediate e-mail host, critical information will be lost and PerfectMail's effectiveness will be significantly impaired.

The Firewall must *not* act as an e-mail proxy
Some firewalls can act as e-mail proxies, applying rudimentary e-mail filtering. This option must be disabled. *Only use port forwarding rules to PerfectMail.*

Configure PerfectMail to filter your domains
PerfectMail will only accept traffic for configured e-mail domains. Make sure all your domains are setup using PerfectMail's Web Interface.

Does your mail server do *SMTP Recipient Filtering*?
SMTP Recipient Filtering occurs when your mail server rejects e-mails sent to accounts that *don't exist*. Some mail servers, notably MS Exchange, have this turned off by default. *SMTP Recipient Filtering* is an important method whereby PerfectMail is able to *automatically* validate the existence of an e-mail address. For MS Exchange servers, refer to the section on *Enabling SMTP Recipient Filtering for MS Exchange*.

Relay outgoing e-mail through PerfectMail
Our e-mail reputation engine is a major strength of PerfectMail. This adaptive engine self-trains by watching both in-bound and out-bound e-mail traffic. For maximum effectiveness, PerfectMail needs to see both in-bound and out-bound e-mail. For MS Exchange servers, refer to the section on *Configuring a SmartHost for MS Exchange*.

DNS resolution *must work*!!!
Domain Name Service resolution *must work* for your PerfectMail server to function. PerfectMail *will not accept e-mail from unresolvable domains*! Similarly, the hostname you assign to your PerfectMail server must be fully resolvable in DNS (Example: perfectmail.mydomain.net). This server will be *visible* to the Internet; **an unresolvable hostname name may cause other mail servers to reject *your* e-mail**.

5 Build the Server

The *PerfectMail Install Image* is a self-installing CD that includes the entire PerfectMail software base and underlying operating system, ready to install on your hardware. PerfectMail on CD supports most popular hardware platforms and, because it includes the operating system, there is nothing else to buy.

PerfectMail works in both physical and virtual environments. We don't recommend particular brands of hardware; choose your preferred hardware vendor or build a white box. The only hardware requirement is that it must be compatible with **Red Hat Enterprise Linux version 6.4**.

In general we recommend deploying a virtualized environment. PerfectMail does not put a lot of strain on the server it runs on, which makes it perfect for virtualization.

For *virtual* servers we recommend starting with the minimum sizing as specified for your *PerfectMail Edition*, and increase the virtual resources as needed.

(This document does not describe setting up a virtual environment.)

5.1 PerfectMail Sizing and Limits

Size your server to match your selected *PerfectMail Edition*, described below. PerfectMail does not put a lot of strain on the server it runs on. However, for physical servers it's best to over-buy hardware (1Gb memory minimum) to minimize downtime if hardware upgrades are required.

For *virtual* servers we recommend starting with the minimum sizing as specified for your *PerfectMail Edition*, and increase the virtual resources as needed.

Most PerfectMail server issues concern under-provisioned hardware. If you are experiencing server problems it's best to check your resource usage. If in doubt, increase memory.

5.1.1 Minimum System Requirements

PerfectMail™ can run as either a physical or virtual server. At minimum, you need:

- P4/Athlon CPU
- 1 GB of memory
- 10 GB of disk space
- 10/100 or GB NIC
- keyboard and display

The more e-mail traffic PerfectMail™ server sees, the more resources it will need to function effectively.

Note: Physical hardware can function with 512Mb of memory. However we've found this small amount of memory to be insufficient for most mail loads.

5.1.2 Memory Usage

PerfectMail uses approximately 250Mb + 10Mb/thread of virtual memory. This value varies between machines but gives a good estimate.

5.1.3 Resource Requirements

PerfectMail Edition	Small Business	Standard	Advanced	Enterprise
Maximum recommended Users	1-75	250	1,000	5,000
Max disk space for message store	20Gb	50Gb	200Gb	All available disk Dynamically grow message store space
CPU	Single Core	Single Core	Dual Core	Quad Core
Memory	1Gb	1.5Gb	2.5Gb	4Gb
Maximum message store	7 days	30 days	90 days	180 days
Maximum concurrent messages	32	64	128	256
Maximum messages per day	250,000	500,000	1,000,000	2,000,000

5.2 Build a Physical Server

Building a physical solution is easy:

- Select *your preferred vendor hardware*
- Choose hardware that is compatible with **Red Hat Enterprise Linux version 6.4**
- Size your server to match the *PerfectMail Edition* you need

We have drivers for most hardware built into our distribution. For very recent hardware you may need to install vendor supplied drivers. We're very interested in ensuring the most commonly used drivers are delivered pre-installed in our product, so please let us know if you need to install drivers.

If you have questions, please contact our support staff at support@perfectmail.com.

5.3 Build a VMware™ Server

IMPORTANT: Please ensure the CD is installing under a VMware Guest and NOT the VMware Host server.

PerfectMail™ is developed on and designed to operate in a VMware environment. It is VMware aware and will automatically install VMware tools during the setup process.

5.3.1 Create a VMware VM for PerfectMail

If you are creating a VMware virtual machine, use the following settings:

- **Operating System:** *Linux operating system*: *RedHat Enterprise Linux 6* (32-bit), *CentOS 4/5/6* (32-bit), *Other 2.6x Linux* (32-bit), or *Other Linux* (32-bit) (In order of preference.)
- **Memory:** Minimum=*1024Mb*
- **Processors:** *1*
- **Capacity:** *10Gb* minimum (Use the BusLogic SCSI HBA controller, if available.)
- **CD/DVD Drive:** Use an ISO Image pointed to your *PM-x.x.x-x.x.iso* file.
  Configure the VM to have the CD/DVD Drive mounted.
- **Network adapter**: 1 NIC required. Choose the Flexible, E1000 or VMXNET3 adapter.
- Not required: *floppy drive or USB device*

Configure the VM to have the CD/DVD Drive mounted. When you boot the VM it will automatically begin **Installing PerfectMail** from the *CD ISO Image*.

5.3.2 Post Install Tasks for VMware

There are no post-install tasks for VMware. PerfectMail is VMware aware and will automatically install VMware tools during the setup process.

5.4 Build a Hyper-V™ Server

IMPORTANT: Please ensure the CD is installing under a Hyper-V Guest and NOT the Hyper-V Host server.

PerfectMail is a fully supported Hyper-V guest Operating System. (PerfectMail is based on Red Hat Enterprise Linux.) You simply create a new Hyper-V VM sized for your *PerfectMail Edition*, install PerfectMail from the *ISO Install Image*, and then install Microsoft's *Linux Integration Services* on the new VM.

PerfectMail™ is fully supported on the following Microsoft Hyper-V releases:

- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Microsoft Hyper-V Server 2008
- Microsoft Hyper-V Server 2008 R2
- Microsoft Hyper-V Server 2012

The Linux Integration Services provide:

- Driver support for network and storage controllers
- Timesync to keep the VM clock synchronized with the host clock
- Integrated Shutdown to facilitate VM shutdown by either the Hyper-V Manager or Virtual Machine Manager.
- Symmetric Multi-Processing Support to a maximum of 4 CPUs
- Also install the adjtimex RPM for more accurate time keeping in the virtual machine.

5.4.1 Create a Hyper-V VM for PerfectMail

Create a new virtual machine with the appropriate settings for your *PerfectMail Edition*.

1. Open the Hyper-V Manager: Click *start*, point to *Administrative Tools* and click *Hyper-V Manager*.
2. Create a new virtual machine with the appropriate settings for your *PerfectMail Edition*. In the Actions menu, click *New*, and then click *Virtual Machine*.
    - **Memory:** Minimum=*1024Mb*
    - **Processor:** *1 Virtual Processor*
    - **IDE Controller:** DVD Drive: *Use an ISO Image pointed to your PM-x.x.x-x.iso file*. Configure the VM to have the CD/DVD Drive mounted.
    - **SCSI Controller:** *10Gb* minimum. (We've had reports that on install, you need to use an IDE drive in setup, not SCSI. If you experience similar problems, please let us know.)
    - **Network Adapter:** *RMP_03_DLink*. Select a *Dynamic MAC Address*. (Our preference is for a *Static MAC Address*, but we have had reports that setting a Static MAC address causes errors in Hyper-V. Note: there can be license activation code issues if the MAC address changes during a VM server migration.)
    - Not required: *COM1, COM2, or Diskette Drive*
3. Ensure that the virtual network adapter has a static MAC address.
4. Ensure the *PerfectMail Install Media* is mounted on your VM. Right-click the virtual machine that you created, and then click Settings. In IDE Controller, specify one of the following:

- An image file in ISO format that contains the files required for installation; i.e. the ISO Image pointed to your PM-x.x.x-x.x.iso file.
- A physical CD/DVD drive that contains the installation media.

5. Turn on the virtual machine: Right-click the *virtual machine* that you created, and then click *Connect*.

Configure the VM to have the CD/DVD Drive mounted. When you boot the VM it will automatically begin **Installing PerfectMail** from the *CD ISO Image*.

5.5 Build a XenServer™ VM

IMPORTANT: Please ensure the CD is installing under a XenServer™ Guest and NOT the Host server.

PerfectMail is a fully supported XenServer™ guest Operating System. (PerfectMail is based on Red Hat Enterprise Linux.) You simply create a new XenServer™ VM sized for your *PerfectMail Edition*, install PerfectMail from the *ISO Install Image*.

5.5.1 Create a XenServer VM for PerfectMail

With XenServer™ VMs are created from Templates. A Template is a "gold image" that contains all the various configuration settings to instantiate a specific VM. XenServer ships with a base set of Templates, which range from generic "raw" VMs that can boot an OS vendor installation CD (Windows) or run an installation from a network repository (Red Hat Enterprise Linux, Suse Linux Enterprise 10) to complete pre-configured OS instances (Debian Etch and Sarge).

However, PerfectMail has its own installation image that should be used to create the new VM. Follow the necessary steps to install from an ISO image or physical CD as required.

If you are creating a virtual machine, use the following settings:

- **Memory:** Minimum=*1024Mb*
- **Processors:** *1*
- **Capacity:** *10Gb* minimum
- **CD/DVD Drive:** Use an ISO Image pointed to your *PM-x.x.x-x.x.iso* file. Configure the VM to have the CD/DVD Drive mounted.
- **Network adapter**: 1 NIC required.
- Not required: *floppy drive or USB device*

5.5.2 Post Install Tasks for XenServer

Installing the Linux guest agent.

Although all the supported Linux distributions are natively paravirtualized (and thus do not need special drivers for full performance), XenServer includes a guest agent which provides additional information about the VM to the host. This additional information includes:

- Linux distribution name and version (major, minor revision).
- Kernel version (uname).
- IP address of each Ethernet interface.
- Total and free memory within the VM.

It is important to install this agent and keep it up-to-date as you upgrade your XenServer host.

To install the guest agent:

1. The files required are present on the built-in xs-tools.iso CD image, or alternatively by using the "Install Tools" option in XenCenter.
2. Mount the image into the guest via:

   ```
   mount /dev/xvdd /mnt
   ```

3. Execute the installation script as the root user:

   ```
   /mnt/Linux/install.sh
   ```

Note: CD-ROM drives and ISOs attached to Linux Virtual Machines appear as /dev/xvdd instead of as /dev/cdrom. They are not "true" CD-ROM devices, but normal devices. When the CD is ejected by either XenCenter or the CLI, it hot-unplugs the device from the VM and the device disappears. This is different from Windows Virtual Machines, where the CD remains in the VM in an empty state.

6 BIOS Settings

It is very important to ensure that the machine will power-up automatically after a power failure. The machine must also boot successfully, even without a keyboard, mouse, or monitor connected, as is the case in many data centers.

The power button should be set to only turn the machine off after a 4-second delay. This prevents accidental shut-off of the PerfectMail box.

The reset button should be disabled if it may accidentally be touched. If the button is fairly well-protected (eg. button is flush with case, so it wouldn't be hit accidentally), then the reset button may be enabled.

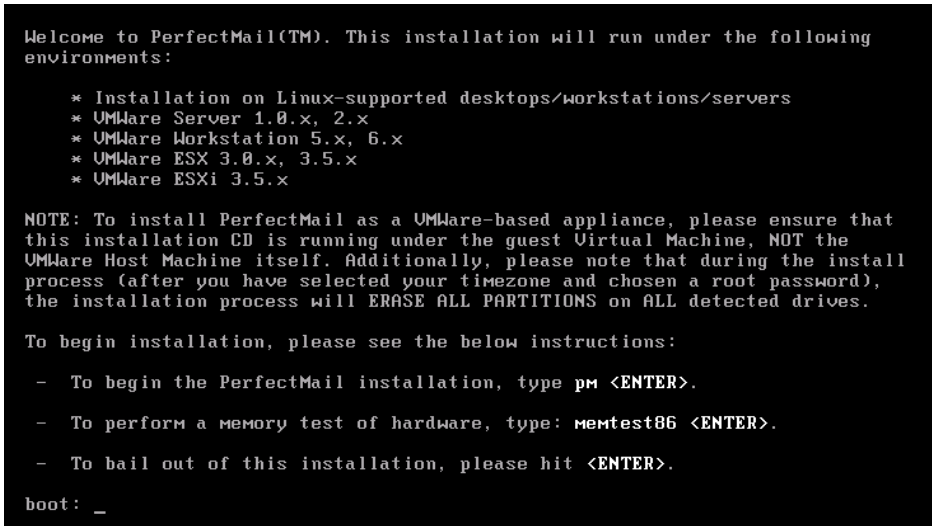
INSTALL NOTE: Ensure the hard drive is the **First Boot Device**. If after the initial install you see the PerfectMail Installation Boot screen then the CD/DVD drive probably has boot priority over the hard drive.

Halt on:	No errors
Soft-Off by Power Button:	Delay 4 Sec
AC Loss Auto Restart:	Former State
First Boot Device:	Hard Drive
Onboard LAN Boot ROM:	Disabled

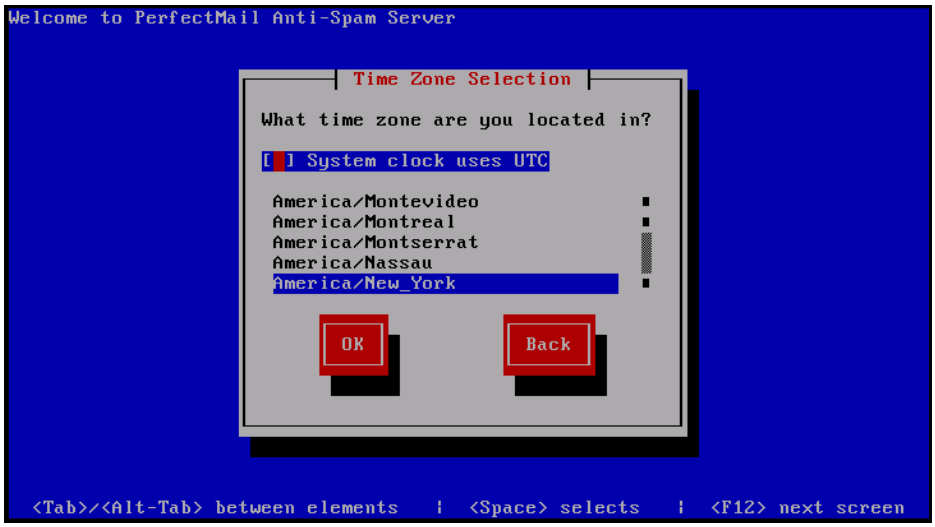
7 Install PerfectMail

Follow the following steps to install PerfectMail™ on your new physical or virtual server.

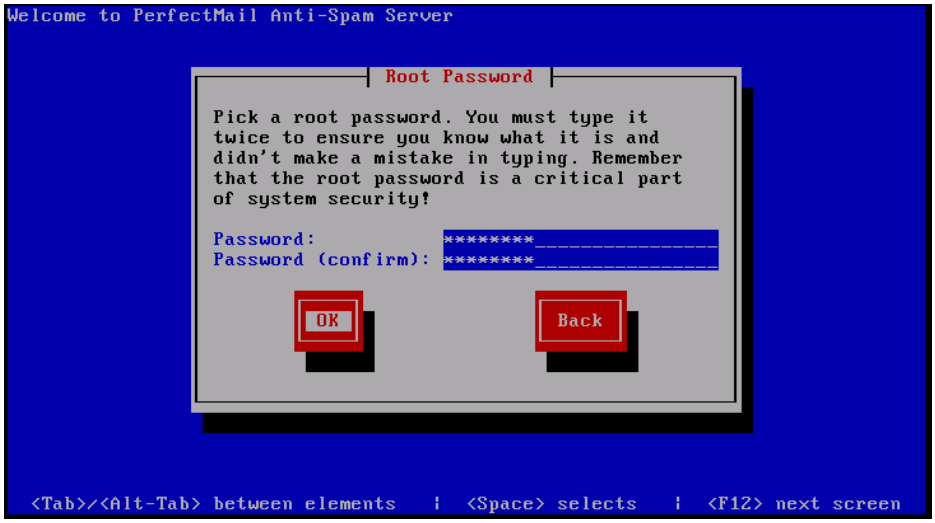
1. *Boot from the installation Media (CD or ISO image).*
2. At the "boot:" prompt, type "**pm**" and hit enter to start the install process.
   Installing PerfectMail™ will erase all existing software and data from the target server, so make sure this is what you want to do.



3. *Time Zone Selection.* Select the nearest city to your location. Use the arrow, enter and tab keys to navigate the "text-base" install interface.



4. *Set the **root password**.* Set the **root** password for this server. **It is extremely important to record this password! Do not lose it!** The *root* account on a Linux based server is like an *Administrator* account on a Microsoft server. It will be needed for accessing the server console, if needed. If you are not familiar with Linux don't worry about this - most tasks can be performed using the web interface; however, keep a record of the password in case it is needed.



5. *Installation process.* The installer will now automatically:
    - Check software package dependencies
    - Format the server file systems
    - Transfer an installer image to hard drive
    - Install required software packages to the hard drive
    - Run post-install scripts
    - Restart the server
6. **First Boot of PerfectMail.** During the *first boot* the server will automatically detect the presence of a VMware hosted system and install of VMware Tools (if necessary). The actual PerfectMail server application will be installed and configured; as well as miscellaneous configuration items. The server will reboot again. **NOTE:** If a DHCP server is not available the server may be slow to boot; please be patient. If this is the case, make sure you follow the steps specified in *Configure Basic Network Settings* below.
7. **Login Prompt.** PerfectMail™ is now installed and ready to be configured using your web browser. The console screen shows you which URL to point your web browser at. **However**, the initial network configuration is dependent on DHCP. If a DHCP server is not available or if you want to specify specific network settings you will need to *Configure Basic Network Settings* as described in the next section.

8. At this point perform any **Post Install** tasks required for your installation platform. For example, Hyper-V requires you to install the latest *Linux Integration Services*.

7.1 Configure Basic Network Settings

If the PerfectMail server does not have access to a DHCP server or if you want to specify specific network settings you need to *Configure the basic network settings.* Please take care and ensure these settings are functional.

To update the basic settings log into the Linux console. At the *login* prompt, login with the following credentials:

```
Login: netconfig
Password: (the password you set as the root password)
```

You will now be asked to supply basic network settings for your server. You will have an opportunity to update these settings later using the web interface. Please take care and ensure these settings are functional:

- *Host Name* - Must be a fully qualified host name (E.g myhost.mydomain.com). This should be a name that is resolvable using DNS. Remember, this server will be *visible* to the Internet; giving it an unresolvable host name may cause other mail servers to reject *your* e-mail.
- *IP Address* - The static IP address of this server using standard 4-octet notation: (E.g. 192.168.1.100)
- *Netmask* - The netmask of this server using standard 4-octet notation: (E.g. 255.255.255.0)
- *Default Gateway* - The default gateway for this network segment.
- *Primary DNS Server* - Remember, DNS resolution *must work* for your PerfectMail™ server to function. PerfectMail™ *will not accept e-mail from unresolvable domains*!

After changing network settings you will need to reboot the server. This can easily be done from the console using the Ctrl-Alt-Del keystroke.

8 Initial PerfectMail Configuration

Continue configuration via the **Web-based User Interface**. Point a web browser at the new server to continue configuring it. Login in with the following credentials (case sensitive):

```
User ID: admin
Password: admin
```

and continue configuring your PerfectMail™ server.

1. *Change the admin password and keep it safe.*
2. *Update your network settings.* It is critical that your server have appropriate network settings. PerfectMail is a network appliance and is dependent on Internet connectivity for both installation and operation. If the network settings are not correct and functional this product will not operate. Please review and update the following as needed:
   - *Hostname* - Please set this to a **resolvable fully qualified domain name** - e.g. myhost.mydomain.com.
   - *IP Address* - We strongly recommend using statically defined network settings.
   - *Default Gateway* - Make sure this works - we need to get to the Internet to both send/receive e-mail and get updates!
   - *Domain Name Services* - **THIS MUST WORK** - E-mail is tightly bound to DNS. If DNS is not functioning, e-mail will not be delivered.

   Note: If the network interface is configured for DHCP and a DHCP server is not available the network interface *will not start*! Check to make sure the network interface is configured correctly. You may need to log in to the system console with userid: **root** and password: **admin** to reconfigure an interface that will not start.
3. *Register your copy of PerfectMail.* Please register by filling out the registration form. This information is used to brand your server and generate a self signed certificate for secure connections. This information may also be used to notify you if, by either the PerfectMail support staff or the server itself, if there are any issues with the server. Your registration information must be correct and it will be validated. If you do not provide a valid e-mail address, you will not receive your extended demonstration license. Your information is used strictly for branding and registration purposes. It will not be shared with any third party.

4. *Review and accept our license agreement.*
5. *Acquire a Demo License.* Your server will register with PerfectMail and attempt to get a 10-Day Demo License. PerfectMail support staff will review your registration information and contact you with an activation key for a longer Demo period. If your PerfectMail server is unable to get a demonstration license over the Internet, please contact our support staff for assistance. Without an appropriate license, your PerfectMail server will run in *Demo Mode*, where it will not filter e-mail.
6. *Reboot!*

9 PerfectMail Detailed Configuration

Your PerfectMail™ server has an easy to use web interface allowing you to configure all aspects of the server and e-mail filtering. Review all the server settings to define your protected domains and ensure your server is correctly configured.

Refer to the *PerfectMail Administrator's Guide* for detailed information on working with the Web Interface. Included here are instructions for the most important setup tasks.

Point a web browser at the new server to continue configuring it. Login in with the following credentials (case sensitive):

```
User ID: admin
Password: your-new-admin-password
```

and continue configuring your PerfectMail™ server.

Important items to review include:

1. Create new PerfectMail administrator accounts as needed.
2. Review and update your network settings.
3. Review and update your licensing/registration information.
4. Add records for each protected Domain, specifying the domain name and where the *back end mail server* is located.
5. Create e-mail address lists as needed. PerfectMail can auto-learn e-mail addresses in most situations, but they may have to be added to the interface.
6. Define any known e-mail relay servers, including webservers that send e-mail, secondary MX'rs, etc.
7. Adjust your e-mail filter settings and make any changes to black/white lists or content filtering lists (subject and body lists)

For filtering, the default settings are good for most servers; however these settings should be reviewed and adjusted as necessary.

9.1 General Server Configuration

Included here are instructions for configuring important aspects of your PerfectMail server. Please review each configuration screen and make changes as needed.

9.1.1 Server Admin > Users

PerfectMail™ User Interface Accounts.

This page allows you to configure user access to the User Interface. Click on a *user name* to edit or remove existing users or click *Create User* to create a new user. User names should be relatively short (about 8 characters) and must not contain spaces or punctuation.

It's important to ensure you fill out all of the fields on this form. The user's e-mail name and e-mail address may be used for sending reports, e-mail blasting and reporting issues with your PerfectMail server.

Permissions:
There are three account types:

- **Administrator** - Administrators have full access to all aspects of the user interface.
- **User** - Users are able to view information and perform queries, but are generally unable to make changes. You can selectively assign server wide permissions to each user as is needed.
- **Web Service** - The *web service* interface allows external systems to interface with your PerfectMail server. Web services generally have very restricted rights. For more information on integrating servers using *web services*, contact our support staff.

Login Restriction:
You can restrict access to this *User Interface* to specific IP addresses or ranges.
Examples:

```
Unrestricted access...

IP Address: 0.0.0.0
   Netmask: 0.0.0.0

Restricted access via a single IP address...

IP Address: 192.168.100.13
   Netmask: 255.255.255.255

Restricted access via an IP address range...

IP Address: 192.168.100.0
   Netmask: 255.255.255.0
```

9.1.2 Server Admin > Network

Network settings configuration.

Use this screen to configure your servers network settings. Be aware that changing network settings may make the Web-UI unavailable, so use caution when making changes. Also note that *DNS Settings* can have a critical effect in the performance of this server. Refer to the *DNS Servers* below for more information.

DNS Settings and the Hostname:
It is important to maintain consistency between the *hostname* of this server and the DNS records referring to it. The hostname of your PerfectMail™ server is very important. Remote mail servers will attempt to verify this hostname against DNS records. If the hostname is not resolvable, most mail servers will reject any e-mail your server sends. Specifically anti-spam servers will check that:

- The *hostname* of your PerfectMail server is fully qualified and resolvable. (I.e. your domain name must be a part of the hostname and it must be a real, resolvable domain name. If this is not possible use the ".localdomain" domain.)
- There is an *A* record in DNS that resolves to the advertised IP address of this server.
- There is a *PTR* record in DNS resolving to the advertised IP address of your server.
- Anti-spam servers may check that the hostnames referred to by PerfectMail (the A and PTR records) all match.
- You should create a TXT record in DNS containing an SPF policy for each e-mail domain you host.

(Note: If the concepts above are new to you or if you have questions, contact our support staff for assistance.)

Host name:
The fully qualified hostname of this server. (e.g. myhost.mydomain.com) This should always be populated and fully qualified. **If the hostname is not fully qualified, your PerfectMail server will likely hang!!!**

Network Interface:
Choose either a *dynamic* or *static* configuration. As this is a mail server we strongly recommend a static configuration (in keeping with the hostname issues discussed above.) The *IP Address*, *Netmask*, and *Default Gateway* use standard 4-octet formatted IP addresses. Example:

```
     IP Address: 192.168.0.100
        Netmask: 255.255.255.0
Default Gateway: 192.168.0.1
```

DNS Servers:
IMPORTANT: *DNS resolution is a requirement for the proper operation of your PerfectMail server. Failure to perform DNS requests will result in a rejection of all e-mail delivery requests.* Enter the IP Addresses of up to 3 *DNS servers*, using the standard 4-octet formatting described above.

Alternate Ports:
If you have statically assigned your network configuration, you can configure alternate ports for receiving ssh or www traffic. This may be used as a workaround if you want to use non-standard ports for these services on the internet but your firewall doesn't give the option of port-forwarding from one port to another.

9.1.3 Server Admin > License

Server registration and licensing page.

It is important that you record accurate contact information and register your PerfectMail™ product. Information from this page will be used to generate a self-signed certificate for your PerfectMail™ product. Contact information from this page will be used by your server to contact you if there is ever a problem with your server. You may be contacted by PerfectMail staff or the server may automatically send you a notification e-mail if it finds a problem.

The *license number* and *activation code* are provided by PerfectMail staff. When your server is licensed you may need to provide your *Machine ID*.

NOTE: You must read and accept the *license agreement* available via a link at the bottom of this page. Otherwise, your PerfectMail server will run in demo mode and not filter spam.

If you have any questions, contact our PerfectMail support staff.

9.2 Configure Domains and Users

Login to the web user interface and go to the *Domain Admin* menu. This menu manages your filtered domains and users. The most important screen to configure is the *Add Domains* web page. (Short-hand: *Domain Admin => Add Domains*.)

PerfectMail™ will only accept traffic for configured e-mail domains. Make sure all your domains are setup using this page.

9.2.1 Domain Admin > Domains

Configuring Domains Protected by PerfectMail™

All e-mail domains you wish to protect with PerfectMail™ *must be listed* in the Domains table. The number of domains that may be administered at any one time is dependent on which edition you are using. Incoming e-mail to any domain *not listed in the Domains table will be rejected*. The only exceptions to this are for the servers listed as *Outgoing Relay*

Servers.

This page provides summary information for all of the domains being protected by PerfectMail™. The table is organized as follows:

- **Domains:** The number of administered domains and the name of each domain;
- **Tag:** The spam score at which an e-mail is suspected of being spam. An e-mail with a spam score in the range of Tag <= spam score < Reject results in the text [SPAM?] being prepended to the subject line. See the Filter Settings section below for more details;
- **Reject:** The level at which the e-mail is judged to be spam, this results in the message being quarantined, rejected, or refused;
- **Mail Host:** The IP address of the internal mail host, typically this is not the same as the Mail Exchanger IP address;
- **Status:** The status of the e-mail domain (e.g. OK, Filtering off).

From this page, you can:

- **Add Domain(s):** By clicking on the *Create New Domains* button. When adding domains enter one domain per line in the *domains* box. Each domain will get the settings defined on the Mail Host and Filter Settings' tabs.
- **Modify Domain Settings:** You can selected domains to be modified in one of two ways. You can left-click on the domain or you can check off multiple check boxes and click "Update Selected Domains" to make uniform changes to all of the selected domains.
- **Delete Domain(s):** One or more domains can be deleted by checking their check-box and clicking the *Delete Selected Domains* button.

Use the the Domains table **Search** field to display a subset of all of your managed e-mail domains. Then you can select them all and update the settings for all similar domains at once instead of having to apply the same settings to each domain one at a time. The text you enter in the Search field is used to match domain names and mail host IP addresses.

9.2.1.1 Domain Maintenance - Mail Host Tab

Delivery Hosts:
The *Internal Mail Host* holds the *IP address* of the internal mail server that mail for this domain should be delivered to.

E-mail Validation:

- **SMTP Recipient Filtering** - A validation technique where PerfectMail queries an internal mail server for e-mail addresses. If your mail server accepts all e-mail addresses your PerfectMail™ product will become swamped with bogus information. If this is the case, *turn off SMTP Validation*
- **Locally Defined Addresses** - PerfectMail always validates e-mail addresses against the *Valid Addresses* table.
- **Reject Unknown Addresses** - Reject any e-mail where the recipient address has not been validated using one of the above methods.

NOTE: You must know whether your mail server is giving proper SMTP recipient filtering responses. For example, Microsoft Exchange servers often accept all messages. If this is the case, please turn on SMTP recipient filtering. For Microsoft Exchange systems see *Enabling Recipient Filtering for MS Exchange* in this manual. If SMTP recipient filtering isn't configured properly and you aren't populating the *Valid Addresses* table, then you *must* turn off *Reject non-validated email*.

If you aren't sure if your mail server is giving proper SMTP recipient filter responses, contact PerfectMail support for

assistance.

9.2.1.2 Domain Maintenance - Filter Settings Tab

Basic Settings:

- **Filter** - Perform anti-spam filtering on this domain. If filtering is turned off, or if your license is expired e-mail will still be delivered through your server.

Tag and Reject Thresholds:
When an e-mail message arrives at your PerfectMail server it is subject to numerous validation and verification tests. The cumulative value of these tests becomes the *spam score* of the message. The base score is "0". The more *spammy* a message is, the higher the *spam score*. The message is then treated in one of three ways:

ACCEPT
: Messages scoring below the *tag threshold* are accepted. (Accept)

REJECT
: Messages scoring over the *reject threshold* are rejected (Content-Block). A value **26** or slightly higher is a good starting point. A long term default for **Reject** would be **22**.

TAG
: Messages scoring between the *tag* and *reject* thresholds have an uncertain disposition. We "Tag" the subject line of the message [SPAM?] and deliver it to the recipient. The user does not need to check a quarantine. An initial value of **16** or slightly higher is a good starting point and will ensure that very few legitimate messages are tagged. A long term default for **Tag** would be **12**.

Reject Dangerous Attachments:
Enable the blocking of *dangerous attachments* to this domain. Dangerous attachments are defined in the "Filters > Filter Settings Menu". The list of attachments generally consists of things like .exe, .com, .bat, etc.

Only Accept TLS Connections:
For this domain, only accept incoming connections where the transport is encrypted via SSL/TLS.

9.2.1.3 Domain Maintenance - Standard Mail Trailer Tab

Standard Message Trailer/Disclaimer:
Create a standard outgoing message trailer/disclaimer for this domain. This disclaimer will be appended to all outgoing e-mails from this domain.

9.2.2 Domain Admin > E-mail Addresses

Use these tables to explicitly configure e-mail addresses for all domains. It's important to ensure PerfectMail™ can identify which e-mail addresses are valid on your servers, so it can avoid loading your servers with unnecessary e-mail traffic and avoid overloading your mail server with *Delivery Status Notification* messages for bogus senders.

PerfectMail uses two methods of e-mail address validation, which work together to identify e-mail address hosted by your server:

1. **SMTP Validation** - A validation technique that directly queries your mail server via SMTP queries. For this option to work you must ensure that *SMTP Recipient Filtering* is enabled in your mail server; otherwise PerfectMail may become swamped with bogus information. If this is the case, turn off *SMTP Validation*. If *SMTP Validation* is turned off PerfectMail will build it's own table of addresses by watching your outgoing e-mail. *SMTP Validation* can be enabled via the *Domain Admin* page.

2. The **E-mail Addresses** tables - to explicitly define e-mail addresses. These tables can work in conjunction with *SMTP Validation* or on their own. The available tables are described below.

Table Format:
For each table, list one e-mail address per line. For example:

```
user@mydomain.com
user@myotherdomain.com
```

"Valid" Addresses:
Use this table to create a global list of **valid** e-mail addresses hosted by this PerfectMail server. Use this table in combination with your *SMTP Validation* as a set for each domain.

"No Filter" Addresses:
Use this table to explicitly list e-mail addresses that are valid, but should receive **no anti-spam filtering**.

"No Filter Attachment" Addresses:
Use this table to explicitly list e-mail addresses that are valid, but should receive **no attachment filtering**. Most users do not need to receive potentially dangerous e-mail attachments (e.g. executable code), but some users need such files as part of their regular communications. You can turn on dangerous attachment filtering for your user population, but still allow specific e-mail addresses to receive potentially dangerous files.

"No Deliver" Addresses:
Use this table to explicitly list valid e-mail addresses that we *should not* accept messages for. Sometimes internal e-mail addresses, including distribution lists, are identified by spammers. This table helps to keep your private address private.

"No Store" Addresses:
Use this table to explicitly list valid e-mail addresses that we should not store **message content** for. Use this table to avoid storing e-mail for particularly security conscious users.

9.3 Configure Additional Relay Servers

Domain Admin => Relay Servers

Login to the web user interface and go to the *Domain Admin* menu, then the *Relay Servers* web page. (Short-hand: *Domain Admin => Relay Servers*.)

Create entries for additional e-mail servers that should be permitted to relay e-mail through this PerfectMail™ server. *Incoming Relay Servers* are not checked against RBL, SPF, and other black lists. *Outgoing Relay Servers* receive no filtering at all.

E-mail will only be accepted or relayed for domains and servers configured in the *Domain Admin* and *Relay Servers* pages.

9.3.1 Domain Admin > Relay Servers

Relay Servers are known e-mail servers that are allowed to relay e-mail through your PerfectMail™ server.

Incoming Relay Servers, such as secondary mail exchangers, do not receive any server checks (RBL and SPF for instance). The e-mail messages originating from these servers are still filtered using all of the non-server anti-spam

tests.

Outgoing Relay Servers are considered known and trusted, just like your mail server. No filtering will be performed on e-mail originating from these servers.

Anti-virus checking is performed on all e-mail for Incoming and Outgoing relay servers.

Entries in this table use the following format:

- **IP Address:** *X.X.X.X* or *X.X.X.X/Y* - to specify an IP address or net block.

Example:

```
192.168.0.7
10.3.16.1/32
207.219.44.0/24
```

9.4 Configure Filter Settings

Login to the web user interface and go to the *Filtering* menu. This menu contains configuration files that affect how PerfectMail™ filters e-mail on a server-wide basis.

Configure the filtering settings for your PerfectMail server. The default settings are good for most servers; however these settings should be reviewed and adjusted as necessary. The *Filtering* menu contains additional configuration pages that can be used for managing *Incoming Sender Settings (Black/White Lists)*, *Word Lists* for scoring and blocking words and phrases for both the message subject and body, etc.

9.4.1 Filters > Filter Settings

Filer Settings: General

Demo Mode - In demo mode your PerfectMail™ server will perform *no actual e-mail filtering*. The user interface will report the decisions PerfectMail *would have taken*, but *no actual filtering will take place*.

Grey Listing - Grey Listing is a technique where e-mail servers are *temporarily rejected* the first few times they try to send e-mail. Legitimate e-mail servers will always resend the message. A great deal of *spam* comes from compromised PC's and industrial spammers, which will likely not resend messages. Grey listing may also occur in specific circumstances that highly indicate spam. When grey-listing occurs, senders receive a temporary reject until one of the following occurs:

- **3** minutes has passed
- more than **3** messages have been sent
- a message scores more than the *tag threshold*
- or, *Grey Listing* is turned off

Grey list data miners - A mail server is considered to be a "data miner" when it regularly attempts to send e-mail to non-existant e-mail addresses within your domain.

Delay new address queries - Upon initial installation, all of the e-mail addresses in your domain(s) are new to PerfectMail™. This option should be left off during the first month of operation so that the software can learn who are the valid recipients within each domain your are administering. After the first month, you can turn this option on to help

deflect data miners. New employees should be asked to send an initial e-mail to an external address so that the system can recognise a valid, new e-mail address.

Strict check vulnerable domains - For certain domains which are primary targets of phishing e-mails, PerfectMail™ performs an extra set of validation checks.

Block Missing PTR - Best e-mail practices include ensuring your e-mail server has a *reverse DNS record* (PTR record). Many compromised computers do not have this, so it is a good way of identifying spam sources. Unfortunately, there are quite a number of mail servers that don't follow *best practices* so there is a potential for false positives. Use with caution.

Reserved Percentage - Let's say your license allows you to have 100 simultaneous e-mail connections and you have reserved 10% for e-mail servers you have exchanged e-mail with before (they are "known"). If your server is handling 80 simultaneous connections with known e-mail servers, 10 will be left available for new e-mail messages from known e-mail servers, and the remaining 10 will be used for handling e-mail traffic from unknown e-mail servers.

Filter Settings: Attachments

- **Block Attachments** - Any attachment with executable commands can possibly damage/infect the recipients computer. Block e-mails containing dangerous e-mail attachments.
- **Zipped Attachments** - Block zip files containing dangerous file types.
- **Attachment List** - A scrollable list of the file types you wish to block. New file types can be added to the list, one file type per line.
- **Score links to dangerous attachments** - Increase the spam score of an e-mail if a link to a dangerous file type is present.
- **Dangerous link score** - The amount to add to the total spam score of the e-mail when a link to a dangerous file type is present.
- **Attachment List** - A scrollable list of the file types you wish to block links to. New file types can be added to the list, one file type per line.

Filter Settings: Reputation

Sender Policy Framework (SPF)

Sender Policy Framework is an open standard specifying a technical method to prevent sender address forgery. It allows the owner of a domain to specify their mail sending policy (which mail servers they use to send mail from their domain). If a message comes from an unknown server, it can be considered a fake and rejected. Since policies like *SPF* are relatively new, organizations may incorrectly structure their *SPF* records, blocking their own mail from being delivered to remote sites. If this is an issue for your organization, you can disable *SPF Filtering*. For more information on *Sender Policy Framework* please visit http://www.openspf.org.

- **Enable SPF Scoring**: If you are experiencing major problems with SPF filtering you can disable it here. If you have problems with specific domains try adding them to the **No Server Checks** table on the **Incoming Sender Settings** page.
- **SPF soft fail score**: The administrator for the senders domain says the sender is **probably** not from their organization. Score this amount.
- **SPF hard fail score**: The administrator for the senders domain says the sender is **definitely** not from their organization. Score this amount.
- **Peer status over-rides RBL/SBL** - At some point a mail server that you have a long history of exchanging e-mail with will become black listed. Enabling this option results in the history overriding the sudden appearance on a black list. This will allow e-mail to continue to flow from the listed server. All e-mail content will still be analyzed to see if it is spam.

RBL Lists - Real-time Block Lists. *These options should always be turned on.* Real-time database of IP addresses of verified spam sources and spam operations (including spammers, spam gangs and spam support services). We use the following services:

- **SWL List** - Enable the Spamhaus White List. This is an active, validated list of known good e-mail servers. Mail server IP addresses listed here are given a bonus score.
- **RBL** - Miscellaneous RBL Lists: Various RBL lists that are not yet classified into categories in the PerfectMail interface.
- **SBL** - Spamhaus Block List: This table is maintained by a dedicated international team based in eight countries, working 24 hours a day, 7 days a week.
- **PBL** - Policy Block List: A list of end-user IP address ranges which should not be delivering unauthenticated e-mail to any Internet mail server.
- **XBL** - Exploits Block List: A real-time database of IP addresses of illegal 3rd party exploits, including open proxies (HTTP, socks, AnalogX, Wingate, etc), worms/viruses with built-in spam engines, and other types of Trojan-horse exploits.
- **CBL** - Composite Block List: The CBL takes its source data from very large spam traps/mail infrastructures, and only lists IPs exhibiting characteristics which are specific to open proxies of various sorts (HTTP, socks, AnalogX, Wingate etc) which have been abused to send spam, worms/viruses that do their own direct mail transmission, or some types of Trojan-horse or "stealth" spam ware, without doing open proxy tests of any kind. (cbl.abuseat.org)
- **CSS** - Snowshoe spammers frequently use many fictitious business names (DBAs), false names and identities, concealed anonymous domains and frequently changing postal dropboxes and voicemail drops to prevent others from connecting snowshoe spam operations to one another and recognizing who is behind the operations and the spam they send.
- **NJABL** - Open Proxy IPs List: This service performs automated open relay and open proxy tests against any system that connects to any of the SMTP servers on networks that contribute relay data to the list. (www.njabl.org)

Additional RBL Service

PerfectMail automatically makes use of a number of RBL services, including the Spamhaus RBL services. You can add an additional service here:

- **RBL Host** - The host name used for performing RBL look-ups. The RBL look-up will be performed using current conventions. For example, looking up address 1.2.3.4 on the RBL host *lookup.myrbl.com* will generate a DNS look-up of *4.3.2.1.lookup.myrbl.com*. If PerfectMail receives a response of *127.0.0.?* (where ? is any value), the message will be deemed RBL listed.
- **RBL Reject Message** - This text will be returned to the message sender. It's a good idea to direct the sender to a website that will describe why their message was rejected. To make this possible you can use the **{ADDR}** macro to insert the sender's IP Address in your message.

Filter Settings: Spoofing

Domain Spoofing Filter

Often spammers will send messages that reportedly come from a domain you host. This section allows you to filter e-mail originating from the outside, which contains one of your domain names in the *from* e-mail address. Options are to:

- **Verify e-mail address.** Verify the existence of the sender address. The sender address must exist on the local server.
- **Block self sent e-mail.** That is, e-mail originating from the outside world, where the from and to address are

the same, will be blocked.
- **Block all.** All e-mail that reportedly comes from one of your hosted domains, but originates from the outside world, will be rejected.

Filter Settings: Content

E-mail content is compared against the list of scored words in both the subject and body word lists as well as the Bayesian filter.

Use system word list - Use the word list provided by PerfectMail™. You can view the word list at "Filters > Content > System Word List".

Use local word list - Use the word list that you can edit. You can edit/view this word list at "Filters > Content > Local Word List".

Maximum word score - subject - This is the maximum amount that will be added to the total spam score of the message based on the content of the subject line. So if the spam score of the subject line exceeds the maximum, only the maximum value will be added to the total spam score of the e-mail. Words and phrases that have a spam score of 99 in the system and local word lists are not affected by this limit. The value 99 is special, it indicates automatic rejection. Default value for this field is 16.

Maximum word score - body - This is the same as maximum word score - subject except it applies to the actual message body. Default value for this field is 16.

Bayesian filter - Enable the Bayesian filter subsystem. Bayesian filtering is a technique that uses statistical analysis to calculate the probability of an e-mail being spam; based on past history. PerfectMail constantly examines messages and self trains to ensure the Bayesian database is updated as spam changes.

Maximum Bayesian score - Default value for this field is 16.

Maximum Bayesian bonus - This is the maximum value that the total spam score of the message can be REDUCED if it's Bayesian score indicates that it is a good e-mail. Default value for this field is 3.

Content profiling - Enable the spam profiling subsystem. Default, checked.

Maximum profiling score - Default value for this field is 16.

Spamvertizers are industrial spammers who send seemingly legitimate advertising. They send large volumes of spam from ever changing server IP's, domain names and company names.

Enable Spamvertizer analysis - Default, checked.

Maximum Spamvertizer score - This maximum works in the same way as Maximum word score - subject. The value you enter should result in messages being rejected. Default value for this field is 16.

Phishing is the act of spoofing a legitimate site to try and gain personal information such as userid's, passwords, banking information, etc. Financial institutions are often the targets of phishing attacks.

Phishing Analysis - Default, checked.

Phishing score - This score should reject messages. Default value for this field is 16.

Filter Settings: Websites

PerfectMail extracts web site addresses (URLs) from e-mail messages and checks them against known spam sources and compromised servers and networks. As part of e-mail analysis, some websites may be examined to determine what sort of content they host. During the analysis process portions of the website may be downloaded to PerfectMail and cached.

Be aware that some web probes may contain hashed or encoded versions of your users e-mail addresses. We take reasonable steps to avoid any links that may include e-mail addresses or cause specific user based behavior (e.g. subscribe, unsubscribe). However, due to URL obfuscation methods we can not be completely accurate in eliminating all such links.

URLs extracted from the website, including website redirects are checked against various known spam site databases and scored against various lists to the specified maximum website URL score:

- **RBL** - Domains listed on the RBL lists.
- **DBL** - Domains listed on the domain block list.
- **SURBL** - Domains listed on the SURBL list.

Enable website probing - Results in the structure of the referenced website being tested for suspicious behaviour. For instance, if the URL points to a website which redirects you to a second website which redirects you a third website, etc. This would be an instance where we would consider the URL to have a malicious / spammy intent.

Website content analysis - The contents of the website are analyzed with the same tests used to determine if an e-mail is spam.

Maximum web score - It should be noted that this maximum score represents the sum of the *Maximum website URL score* plus any additional spam points from *Enable website probing* and *Website content analysis*.

URL history size - The number of website URLs to be kept in history.

Google Safe Browsing - Uses Google's list of suspected Phishing and Malware pages.

Filter Settings: Outbound

This feature allows you to filter your organization's outgoing e-mail.

Filter outbound recipients - uses the Black and White lists on **Filters > Sender** to block recipients for outbound e-mail. The black list will normally prevent a specific domain or address from sending to your server; this switch allows you to block traffic destined for those senders as well.

Filter outbound senders - restricts which domain names a *sender* may use for *outgoing* e-mail. Restricting outgoing e-mails can help prevent infected computers inside your network from sending spam, viruses and worms to the Internet. You can specify three types of filtering:

- **No filtering**
- **Allow sub domains of configured domains** - E-mail may be sent by configured domains and their sub domains. For example, if *mydomain.com* is configured in PerfectMail then outgoing e-mail such as *myname@myhost.mydomain.com* will be allowed.
- **Allow only configured domains** - Only allow e-mail from configured domains. All outgoing e-mail *must* be from a configured domain.

Other outbound sender domains - You can use this list to specify other, non-PerfectMail configured, domains to be e-mail senders.

Content filtering - applies the subject and body content reject filters to your outgoing e-mail. You can specify three types of filtering:

- **No filtering**
- **Partial content filtering** - blocks e-mail if it contains words and/or phrases that score 99 in the *reject words* list.
- **Full content filtering** - analyzes the outgoing message in its entirety. If it scores above the *Reject Threshold*, then the e-mail is blocked.

Exempt recipients - Used to specify recipients that do not require e-mail filtering. Enter domain names / IP addresses into this list, one per line. (Example: Use this for forwarding e-mail to blackberry.net.)

Filter Settings: Actions

If PerfectMail is uncertain about an e-mail, the subject line is *tagged* with the text defined here. The default setting is **[Spam?]**. Administrators should monitor their *tagged* messages. If the number of legitimate messages being tagged is high, the spam thresholds may need to be adjusted. *Our goal is to reduce the number of tag messages received to zero.*

- **Tag messages** - Enable subject tagging of uncertain e-mails.
- **Spam tag** - Define the spam tag. Default: [Spam?]
- **Remove outgoing tags** - Remove tag messages from outgoing e-mails, specifically replies to tagged messages.

Rejecting Spam

By default, PerfectMail will reject any message found to be spam. It returns a failure code, the reason for the failure and the text contained in the *reject message*. You can also choose to not *reject spam*; instead making use of the *mail headers* to filter e-mail at the mail client. (However, we recommend filtering e-mail at the server.)

In most instances the text in the **Reject Message** edit box will be forwarded to the person who sent the rejected e-mail. If a message is falsely rejected, this is the message the sender will see. It's a good idea to describe a method of contacting your e-mail support staff.

Mail Headers

All e-mail messages have headers which are typically not shown by your e-mail client program. E_mail headers include the From:, CC:, and Subject: fields you normally see when processing your e-mail. The message headers section of an e-mail contains extra information, such as the actual sender of the message which, when dealing with spam, is almost always different than the name stated in your From: field.

PerfectMail can be configured to add spam info headers to your e-mail messages. Your can use these headers to filter e-mail right at your e-mail client (e.g. Microsoft Outlook).

- **Spam score header** - This creates the *X-PM-Score* message header. This message header displays the numeric *spam score* of the message. Example: X-PM-Score: 15
- **Spam flag header** - This creates the *X-Spam-Flag* message header. This message header displays *YES (or NO)* if the message is spam (or not). Example: X-Spam-Flag: YES
- **Spam level header** - This creates the *X-Spam-Level* message header. This message header displays a

graphic representation of the *level of spaminess* using *'s (each * represents 4 points of *spam score*). Example: X-PM-Score: ****
- **Outgoing mail headers** - Suppress adding the above e-mail headers to outgoing messages.

Strip outbound DKIM - Strip inbound DKIM - At this point in time, PerfectMail™ does not make use of DKIM headers.

9.4.2 Filters > Sender

Formerly Black/White List

The following tables adjust filtering for mailhosts, domains and e-mail addresses. Using these tables it is possible to block content for whole countries. The following tables are availabe:

- **White List** - Mail servers, sending domains and e-mail addresses listed here will not be blocked by the spam filter, unless the e-mail contains a virus. List known good servers here to ensure important e-mail does not get blocked. Web servers and other production servers may send e-mail notifications, but these servers are often poorly configured as mail servers, making them good candidates for white listing.
- **Black List** - Mail originating from servers and domains listed here will be rejected.
- **Discard List** - Mail originating from servers and domains listed here will be quietly discarded. Note: this does not affect filtering or scoring decisions, which will occur as is normal. However, regardless of the result of the filtering system, the message will be quietly discarded.
- **No Reject List** - Similar to the *Discard List*, this table lists servers and domains what should not receive reject messages. This is especially important for newsgroup services such as *Yahoo Groups* which may react negatively to anti-spam software. For example, if messages forwarded from *Yahoo Groups* are rejected, *Yahoo Groups* may stop forwarding messages to the protected e-mail address. Listing such servers here allows you to quietly discard spam without affecting the delivery of future messages.
- **No Server Checks List** - Servers listed here, either explicitly by hostname or IP address, or implicitly as members of some domain, will not receive any server based validation or reputation checks, including SPF and RBL lookups. Servers that become black listed by RBL lists or have SPF configuration problems are good candidates for adding to this list, allowing you to accept e-mail from such servers and domains regardless of their disposition on such lists.

Table Format:
Each table accepts entries using the following formats. Certain format types may not make sense for all tables; please refer to the appropriate table description below for more information. The following formats are supported:

- **IP Address:** *X.X.X.X* or *X.X.X.X/Y* - to specify an IP address or net block. For example:

```
192.168.1.3
192.168.2.0/24
```

- **Host Name:** Specify the Fully Qualified Domain Name (FQDN) of a specific host. For example:

```
myhost.domain.com
yourhost.yourdomain.com
```

- **Domain:** Specify a complete domain, including sub domains. Each portion of the domain name must be specified fully; wild cards are not supported. For example:

```
newyork.customer.com
company.com
```

- **E-mail Address:** Specify complete e-mail addresses. This is particularly useful for domains that commonly send spam. For example:

```
user@domain.com
```

- **User:** Specify the user portion of an e-mail address. This is useful for specifying commonly used e-mail addresses, across multiple domains. For example:

```
sales@
webmaster@
```

9.4.3 Filtering > Subject

Subject Filter

The subject line of each message is checked for the listed words and phrases. The word list is case-insensitive and treats all punctuation as spacing. Your words will be automatically converted to the simplest version our filter can handle, including character case conversion and stripping of punctuation. Our anti-obfuscation engine is quite effective but should be used with caution.

Subject word categories:

- **Reject words** - Words and phrases contained on this list (one per line) cause the e-mail to be rejected.
- **Scored words** - Words and phrases contained on this list are given a score as specified in the *score field* just below the word list boxes.
- **System words** - These words and phrases are maintained by PerfectMail™.

Anti-obfuscation is a technique that identifies attempts to disguise words. For example:
Anti-Obfuscation maps `\/ 1 @ g r @` to `viagra`, `><@n@x` to `Xanax`, etc. The word score is scaled to match the measure of obfuscation. This technique is very successful, but it can sometimes give erroneous results if the listed word is similar to other non-offensive words; use with care. In particular try to avoid very simple words that may appear in messages; for example a word such as "aaaa" would be a very bad word choice.

Note: Only use alpha characters in the words and phrases. Do not use punctuation or special characters because the anti-obfuscation engine skip past these characters. Similarly, avoid accented characters.

To avoid false rejects, take special care when selecting words for these lists.

9.4.4 Filtering > Body

Body Filter

Use this filter to identify messages containing content and language that is not acceptable to your organization. When adding entries to this table, please take some time to consider the various instances where these phrases may be used; and may trigger false positives.

The body of each message is checked for the listed words and phrases. PerfectMail™ uses a custom content analyzer that utilizes a restricted alphabet to efficiently parse out words. All phrases are case-insensitive and all punctuation are treated as spaces.

Your words will be automatically converted to the simplest version our filter can handle, including character case conversion and stripping of punctuation. Our anti-obfuscation engine is quite effective but should be used with caution.

Body word categories:

- **Reject words** - Words and phrases contained on this list (one per line) cause the e-mail to be rejected.
- **Scored words** - Words and phrases contained on this list are given a score as specified in the *score field* just below the word list boxes.
- **System words** - These words and phrases are maintained by PerfectMail™.

Anti-obfuscation is a technique that identifies attempts to disguise words. For example:
Anti-Obfuscation maps `\/ 1 @ g r @` to `viagra`, `><@n@x` to `xanax`, etc. The word score is scaled to match the measure of obfuscation. This technique is very successful, but it can sometimes give erroneous results if the listed word is similar to other non-offensive words; use with care. In particular try to avoid very simple words that may appear in messages; for example a word such as "aaaa" would be a very bad word choice.

Note: Only use alpha characters in the words and phrases. Do not use punctuation or special characters because the anti-obfuscation engine skip past these characters. Similarly, avoid accented characters.

To avoid false rejects, take special care when selecting words for these lists.

10 Post Install Tasks

To make the most of your PerfectMail™ server it's best to configure PerfectMail™ to handle both incoming and outgoing e-mail.

10.1 Redirect Incoming E-mail to PerfectMail™

Direct inbound e-mail traffic to PerfectMail™. If your infrastructure is behind a firewall simply redirect SMTP (port 25) traffic to the PerfectMail™ appliance. Making updates to DNS involves a large time lag as DNS records propagate through the Internet, so firewall redirection is the preferred method.

TEST! You can review e-mail traffic on the web interface using the following menu items:

- *Activity => Raw Log* - To view raw MTA Logs. This is the best way to watch e-mail traffic at a low level
- *Activity => Mail Log* - To view recorded e-mail activity and spam filtering decisions

10.2 Redirect Outgoing E-mail through PerfectMail™

Direct outbound e-mail traffic from your mail server through PerfectMail™. Configure your PerfectMail™ server as an outbound relay or *smarthost* on your mail server. For MS Exchange users, please refer to *Configuring a Smarthost for MS Exchange*.

TEST! You can review e-mail traffic on the web interface using the following menu items:

- *E-mail => Transmission Log* - To view raw MTA Logs. This is the best way to watch e-mail traffic at a low level
- *E-mail => Mail Log* - To view recorded e-mail activity and spam filtering decisions

10.3 Firewall Settings

Port 25 (SMTP) traffic should be forwarded to your PerfectMail product.

It is best to create a one-to-one NAT mapping port 25 on the Internet facing IP address and your PerfectMail product. Problems can arise when the incoming SMTP IP address and the outgoing SMTP IP address do not match. In this situation incoming SMTP traffic is properly configured, however the outgoing SMTP traffic is sent on an unexpected port (usually the default outgoing IP address is used).

When sending e-mail to the Internet remote anti-spam servers will verify the domain name, hostname and reverse address of the sending IP address against your DNS records. Often the DNS records are not configured to support the default outbound IP address.

Anti-spam servers will compare the name reported by the server itself (i.e. the hostname), the address record (A record) from DNS and the reverse DNS record (PTR record). Anti-spam servers will score and possibly even reject messages for discrepencies between these records. This is further complicated by firewall port forwarding issues. The best way is if you have a 1-1 NAT for your e-mail so both incoming and outgoing mail use the same IP number. Failing that the names should all match up on the outgoing side of things.

We strongly recommend updating your firewall to restrict all outgoing SMTP (port 25) traffic. Only PerfectMail and other mail servers should be able to send e-mail directly to the Internet. PC's compromised by viruses, Trojans, etc. may send e-mail directly to the Internet which may result in your entire organization being blacklisted by RBL sites such as Spamhaus. (Especially if you have only one Internet facing IP address.)

Following are two examples of how to configure PerfectMail within your firewalled infrastructure.

10.3.1 Firewall Configuration: Green Zone + Internet

If you have a simple firewall configuration, with your internal network (Green Zone) being protected from the Internet, place your PerfectMail product in the internal network (Green Zone) and configure your firewall to allow the following network traffic.

Incoming Ports:

Port	Type	Protocol	Description
25	TCP	SMTP	Port forward to Perfectmail for incoming e-mail
443	TCP	HTTPS	Port forward to Perfectmail for remote secure web access (optional)
22	TCP	SSH	Port forward to Perfectmail for technical support (optional)

[Note: Using non-standard ports for support access (i.e. SSH and HTTPS) is acceptable as long as these are port forwarded to the appropriate ports on the PerfectMail server.]

Outgoing Ports:

Port	Type	Protocol	Description
25	TCP	SMTP	For outgoing e-mail
53	TCP/UDP	DNS/BIND	For DNS look-ups and testing
80	TCP	HTTP	For website probing
123	UDP	NTP	For remote Network Time Protocol look-ups

443	TCP	HTTPS	For website probing
43, 4321	TCP	whois, rwhois	For WhoIs queries

10.3.2 Firewall Configuration: Green Zone + DMZ + Internet

For the configuration you described with PM in the DMZ and your Mail Server and DNS in a Green Zone (protected network). The following ports are required for PerfectMail to function:

If you have a firewall configuration that includes a DMZ, with your internal network (Green Zone) being protected from the Internet, place your PerfectMail product in the DMZ network and configure your firewall to allow the following network traffic.

Between Internet and the DMZ - Incoming Ports:

Port	Type	Protocol	Description
25	TCP	SMTP	Port forward to Perfectmail for incoming e-mail
443	TCP	HTTPS	Port forward to Perfectmail for remote secure web access (optional)
22	TCP	SSH	Port forward to Perfectmail for technical support (optional)

[Note: Using non-standard ports for support access (i.e. SSH and HTTPS) is acceptable as long as these are port forwarded to the appropriate ports on the PerfectMail server.]

Between Internet and the DMZ - Outgoing Ports:

Port	Type	Protocol	Description
25	TCP	SMTP	For outgoing e-mail
53	TCP/UDP	DNS/BIND	For DNS look-ups and testing
80	TCP	HTTP	For website probing
123	UDP	NTP	For remote Network Time Protocol look-ups
443	TCP	HTTPS	For website probing
43, 4321	TCP	whois, rwhois	For WhoIs queries

Between the DMZ and the Green Zone - Incoming Ports, to Green Zone:

Port	Type	Protocol	Description
25	TCP	SMTP	Port forward to mail server for incoming e-mail
53	TCP/UDP	DNS/BIND	For DNS look-ups and testing (unless DNS server is in DMZ)
123	UDP	NTP	For Network Time Protocol (unless time server is in DMZ)

Between the DMZ and the Green Zone - Outgoing Ports, from Green Zone:

Port	Type	Protocol	Description
25	TCP	SMTP	For outgoing e-mail
443	TCP	HTTPS	For PerfectMail Web-UI secure access

80	TCP	HTTP	For PerfectMail Web-UI access (optional)

11 Active Directory

Active Directory (AD) can be a problem for third party tools. AD integration/configuration is not necessarily consistent and we've had reports from third party vendors who are very experienced with AD but still encounter quirky behavior; AD can require a bit of finesse. However, with *SMTP Recipient Filtering* enabled we simply do not need AD as we can authenticate e-mail addresses directly with Exchange.

By default Exchange will accept all e-mail, regardless of the recipient. SMTP Recipient Filtering is a feature where Exchange will only accept e-mail that it can either route or deliver. PerfectMail uses an algorithm to interactively query Exchange using the SMTP protocol to validate e-mail addresses rather than relying on AD. The implementation is very straightforward and works flawlessly.

12 PerfectMail™ Updates and Upgrades

PerfectMail is an actively developed product with regular releases to rules, signatures, block-lists and code updates.

Updates: Updates to *PerfectMail* occur on a regular and ongoing basis. Your server will check for updates to its spam and virus settings every 10 to 15 minutes to quickly adjust how it reacts to spam threats.

Upgrades: Periodic code releases are made to add more tools or make improvements to our anti-spam engine.

12.1 The Upgrade Process

We provide a 72 hour post install support availability window, where staff must be available to deal with any upgrade issues.

The upgrades themselves occur seamlessly on your PerfectMail™ server. The latest upgrade is downloaded to your server; after which mail services are suspended and the upgrade is applied. The total downtime is usually about 30 seconds, with no loss of e-mail.

After the upgrade is finished your PerfectMail™ server will send you an e-mail notification.

12.2 Staggered Upgrade Scheme

We have a staggered upgrade release schedule to minimize any disruption to your Mail Server. Prior to general release PerfectMail is tested on our Development, Alpha and Beta sites. After successful deployments through these three server groups it becomes available for general release, being pushed to upgrade groups: 'A', 'B' and 'C' in a progressive release schedule.

'A' sites receive their updates on the Monday of the general release; 'B' and 'C' sites receive their upgrades later in the week, or even in the following week.

At any time, if there are any reported issues they are assessed and appropriate actions are taken.

13 Trouble Shooting E-mail and Spam

13.1 Not Accepting Mail

PerfectMail™ may stop accepting e-mail for a number of reasons. Fortunately, PerfectMail runs a periodic validation script that checks for the most likely reasons and displays error messages and warnings on the *PerfectMail Dashboard*. It there is a problem with e-mail delivery, check the dashboard first.

13.1.1 Resolvable Hostname Issues

A server's *hostname is the name that it knows itself as. This is different than naming in DNS or any other mechanism. It is the locally defined name.*

Your PerfectMail product **must** have a *resolvable, fully qualified hostname*; e.g. `perfectmail.mydomain.com`. There **must** be a domain portion to the *hostname* of your PerfectMail server.

This *hostname* must be resolvable in DNS. Mail servers will look-up server names in DNS as a validation mechanism. Not having a resolvable *hostname* can cause problems.

If this is not possible to use resolvable DNS names you can use the `.localdomain` domain; e.g. `perfectmail.localdomain`.

The PerfectMail configuration scripts try to mitigate the creation of partial hostnames by appending all single word hostnames (e.g. "myhost") with the ".localdomain" top-level-domain (e.g. "myhost.localdomain"). The ".localdomain" top-level-domain is "known" and will not be validated against DNS.

13.1.2 Unique Hostname Issue

Your PerfectMail *hostname* must be unique. Often, mail servers will refuse to relay e-mail through mail servers with the same *hostname*. This is done to prevent endless e-mail delivery loops.

13.1.3 DNS Issues

PerfectMail absolutely needs to be able to perform DNS resolution. PerfectMail will refuse to accept e-mail from domain names that do not exist in the DNS space. If DNS is not resolvable then e-mail will not flow.

DNS is also used for a number of validation tests including look-ups on many RBL sites. Not having the ability to perform DNS look-ups severely impairs PerfectMail's ability to filter e-mail.

13.1.4 Server Resources

Memory constraints are the most likely cause of server problems. PerfectMail must have sufficient resources (i.e. memory, CPU and disk) to run. If the server uses all memory and swaps to disk the system performance will slow down significantly. If your server appears to be running slow, check the memory usage and add memory as appropriate.

If the hard disk becomes full PerfectMail will stop accepting e-mail. A nightly script prunes old data to ensure a safe amount of free disk to prevent this from happening.

When the "load average" of the server is greater than 12 (i.e. 12 processes waiting for the CPU) our Mail Tranpsort

Agent (MTA) will stop accepting new e-mail connections. This behavior prevents the PerfectMail server from crashing. With a high server load your server is not realistically able to process mail in any case as pushing the load average past 12 can put the server in an unresponsive state.

In any case, if your server is performing sub-optimally, you will likely need to review your resource usage and increase resources as appropriate. PerfectMail provides reports on its web interface to assist you with this assessment. Please refer to the following reports:

- "Reports > E-mail Activity"
- "Reports > Resource Usage"
- "Server Admin > Archive"

13.2 Why does an e-mail get *Deferred*

E-mail deferral occurs when a message (usually outgoing) cannot be immediately handed off to the next relay host. It is quite common to have messages queued as "deferred" as remote mail servers may not be available for any number of reasons: network traffic congestion, service outages, server load, DNS hiccups, grey-listing, etc.

Sometimes *spam* and *delivery notification messages* will get stuck in the queue as well. Spammers send a lot of e-mail, but rarely accept return e-mail, including bounce messages. These messages can get stuck in the queue. PerfectMail™ has automated processes that clean out such messages on an hourly basis.

13.3 DHCP Issues

If the network interface is configured for DHCP and a DHCP server is not available the network interface *will not start*! Check to make sure the network interface is configured correctly. You may need to log in to the system console with userid: **root** and password: **admin** to reconfigure an interface that will not start.

14 Reference

14.1 Resetting Network Settings

If it is not possible to reconfigure the network settings using the web user interface you can reset the settings via the server console. You must login on the console in order to perform this task. Login to the console with the following credentials:

Userid: netconfig
Password: *(The password for your "root" account.)*

You can now reset the basic network settings for this server. Please take care and ensure these settings are functional:

- Host Name - Must be a fully qualified host name (E.g myhost.mydomain.com). This should be a name that is resolvable using DNS. Remember, this server will be visible to the Internet; giving it an unresolvable host name may cause other mail servers to reject your e-mail.
- IP Address - The static IP address of this server using standard 4-octet notation: (E.g. 192.168.1.100)
- Netmask - The netmask of this server using standard 4-octet notation: (E.g. 255.255.255.0)
- Default Gateway - The default gateway for this network segment.
- Primary DNS Server - Remember, DNS resolution must work for your PerfectMail server to function. PerfectMail will not accept e-mail from unresolvable domains!

14.2 Microsoft Exchange™

14.2.1 Configuring a SmartHost for Microsoft Exchange™

14.2.1.1 Microsoft Exchange™ 2003

In Exchange 2003, it's possible to configure a smart host on the Default SMTP Virtual Server, but if you do it this way you can only set a single smart host. The preferred method, therefore, is to use an SMTP Connector for your outgoing emails which does allow multiple smart hosts to be specified.

Following are the steps to have Microsoft Exchange 2003™ System deliver outbound mail via a Smart Host:

1. Open up the Microsoft Exchange System Manager (Start > Programs > Microsoft Exchange > System Manager);
2. Expand "Administrative Group", <Your Groupname>, you may have more than one, "Servers", <SERVER NAME>, "Protocols", "SMTP", "Default SMTP Virtual Server";
3. Right-click on "Default SMTP Virtual Server" and select Properties;
4. Click on "Delivery" tab and select the "Advanced" button;
5. Enter the Address of the hosting PM for the "Smart Host" field. You can specify the IP Address e.g.. [192.168.3.44] (using the square brackets) or use a FQDN "yourhost.yourdomain.com" (without the quotes);
6. Click on "Apply", then "OK" for all cascading windows.

These changes should take place on the fly, there is no need to restart the Exchange services.

Note that the above procedures assumes that you have a straight-forward Exchange system in place with pre-defined Exchange Routing Groups in place and that there is only one Exchange system within your organization. If you have an Exchange environment consisting of a Front-End system and a Back-End system, then the above needs to be applied on the Back-End system only.

Alternatively, you may decide to use a connector which routes email, rather than an SMTP virtual server:

1. Open up the Microsoft Exchange System Manager (Start > Programs > Microsoft Exchange > System Manager);
2. Right-click on {Your Exchange Server} and select Properties;
3. Make sure the checkbox Display routing groups is checked;
4. Right Click "First Organization";
5. Locate the folder: Administrative Groups/{Your_Administrative_Group}/Routing Groups/{Your_Routing_Group}/Connectors;
6. Right-click Connectors, select New, and then click SMTP Connector;
7. Fill in the Name field;
8. In the Smart host box, type the hostname or IP address (wrapped in square brackets [ ]) of the smart host server and select the local bridgehead (usually your mail server);
9. Select the Address Space tab, typical settings are "SMTP" and select (*).

If the above procedures do not work for you and you have restarted the Exchange services (or rebooted the Exchange Server) then there is a possibility that you may have a custom Routing group defined with a custom SMTP connector for all SMTP Address Spaces and SMTP connector configurations within the Routing Group section take precedence over the default virtual SMTP protocol configurations within the Protocols section.

14.2.1.2 Microsoft Exchange™ 2007/2010

For Exchange 2007/2010 configure a default relay host (smarhost) by creating a Send Connector. With Exchange 2007/2010, Microsoft has separated the mail server roles. The Hub Transport role is responsible for sending and receiving external email. In a single Exchange server environment, the same server will perform all roles.

1. Open the Exchange Management Console;
2. Expand the Organization Configuration (click on the "+" next to Organization Configuration);
3. Select Hub Transport, then the Send Connectors tab;
4. Right-click on the existing Send Connector;
5. Select Properties, then the Network tab;
6. Select "Route mail through the following smart hosts:" and click Add;
7. Enter the internal IP address of your smarthost relay server.
8. Click OK.

Once you click OK the changes will take effect immediately.

Enabling SMTP Recipient Filtering for Microsoft Exchange™

Following are the steps to enable **recipient filtering** to allow PerfectMail™ to validate e-mail users for Microsoft Exchange™.

When recipient filtering functionality is enabled, it filters all messages that come through all Receive connectors on that computer. By default, recipient filtering is enabled on the computer that has the Edge Transport server role installed for inbound messages that come from the Internet but aren't authenticated. These messages are handled as external messages. If this feature is turned off **all e-mail addresses will be accepted** by both Exchange and PerfectMail™.

Please ensure you have the appropriate permissions to perform this task.

14.2.1.3 Microsoft Exchange 2003™

Please enable **recipient filtering** by doing the following:

1. Open Up Exchange System Manager.
2. Expand "Global Settings".
3. Right-click on "Message Delivery" and select "Properties".
4. Select the "Recipient Filtering" tab.
5. Check "Filter recipients who are not in the Directory" and click on "Apply".
6. A big warning message will come up regarding manually enabling filtering on specific SMTP virtual server. Click "OK".
7. Click "OK" to close "Message Delivery Properties".
8. You should now be back at the Exchange System Manager screen at this point. Expand "Administrative Group".
9. Expand the Information Store group. (There may be more than one within your organization.)
10. Expand "Servers", then <your server name>, then "Protocols".
11. Highlight "SMTP" and you should see the SMTP server configuration. (Default name is "Default SMTP Virtual Server".)
12. Right click "Default SMTP Virtual Server" and select "Properties".
13. The "General" tab will be open. Click on "Advanced" beside the "IP Address field".
14. An advanced window will pop up. Leave the default selection as is.
15. Click "Edit" and that will bring up the Identification window.
16. Check to enable "Apply Recipient Filter" and click "OK" and then "OK" again.
17. Click on "Apply", then "OK".
18. Repeat steps 12-17 for each SMTP protocol.
19. Repeat steps 9-17 for multiple store groups (if applicable).
20. There is no need to restart any Exchange services. Changes may take a few minutes to take effect as it may be replicated.

14.2.1.4 Microsoft Exchange 2007/2010™

With Exchange 2007/2010, Microsoft has separated the mail server roles. The Edge Transport role is responsible for recipient filtering. In a single Exchange server environment, the same server will perform all roles.

Use the Exchange Management Console to enable or disable recipient filtering:

1. Open the Exchange Management Console on the Edge Transport server.
2. In the console tree, click Edge Transport.
3. In the work pane, click the Anti-spam tab, and then select Recipient Filtering.
4. In the action pane, click Enable or Disable as appropriate.

Use the Shell to enable or disable recipient filtering:

1. Set-RecipientFilterConfig -Enabled $true

For detailed syntax and parameter information, see Set-RecipientFilterConfig.

14.3 Enabling Mail Headers in PerfectMail

To use Distributed Filtering you must enable specific mail headers in PerfectMail. Using your web browser, log into the PerfectMail administrative interface and go to the "Filtering > Filter Settings" page. At the bottom of this page you will find a section on "Mail Headers". Ensure the "Spam flag header" and "Spam level header" settings are checked.

14.4 Enabling Mail Header Filtering in Your E-mail Client

You can create filter rules on your local e-mail client (e.g. Microsoft Outlook™) to automatically file messages in your "Spam" or "Junk" folder. For sites that are particularly concerned about loosing e-mail, or even for specific users, you can have PerfectMail not reject any e-mail and use these filtering rules to filter messages on your local e-mail client.

This section describes how to implement Distributed Filtering for several popular e-mail clients. The steps for other e-mail clients are likely very similar to those presented here.

14.4.1 Microsoft Outlook Express™ Filters

1. Go to Tools->Message Rules->Mail...
2. Check 'Where the Message Body contains specific words'
3. Select 'Where the Message Body contains specific words '.
4. Click on 'contains specific words'.
5. Type in: X-Spam-Flag: Yes (one space between the : and the Yes)
6. Click 'Add'.
7. Click 'Ok'.
8. Select 'Move it to the specified folder'.
9. Click on 'specified'.
10. Highlight an existing folder, or create a new one.
11. Click 'Ok'.
12. Give the rule a name. (The default is New Mail Rule #1.)
13. Click 'Apply Now'. (You may or may not want to Apply Rule Now)
14. Click 'OK'.

14.4.2 Microsoft Outlook™ Filters

1. Go to Tools->Rules Wizard...
2. Click 'New...' (On the top right)
3. Choose 'Check messages when they arrive'
4. Click 'Next'.
5. Check 'With specific words in the message header'.
6. Click on 'specific words'.
7. Type in: X-Spam-Flag: Yes (one space between the : and the Yes)
8. Click 'Ok'.
9. Click 'Next'.
10. Check 'Move it to the specified folder'.
11. Click on 'specified'.
12. Highlight an existing folder, or create a new one.
13. Click 'Ok'.
14. Click 'Next'.
15. Click 'Next'. (Again, unless you want to add exceptions.)
16. Give the rule a name. (The default is what you typed for "specific words", above.)
17. Check 'Turn on this rule'. (You may or may not want to check 'Run this rule on my Inbox now'.)
18. Click 'Finish'.

14.4.3 Microsoft Outlook 2002™ Filters

Microsoft Outlook 2002™ does not have the ability to filter spam itself, but it has filtering "rules" that we can use. The Rules Wizard will only appear in the Tools menu when the Inbox is selected, so choose the Inbox before you try to

add a filter.

1. Select "Inbox" in the Folder List.
2. Click "Tools" and select "Rules Wizard".
3. Click "New" to create a new rule.
4. Check "Start from a blank rule" and select "Check messages when they arrive". Click "Next".
5. Check "with specific words in the message header".
6. In the rule description, click "specific words".
7. Under Specify a word or phrase to search for in the message header, enter "X-Spam-Flag: YES" to put spam into your "Spam" folder". Click "Add", then "OK", and finally "Next".
8. Under "What do you want to do with the message?", check "move it to the specified folder".
9. In the rule description, click "specified".
10. Under Choose a folder, click "New".
11. Enter "Spam" as the name and click "OK"
12. Select "Spam" under Personal Folders (click the plus sign to open Personal Folders if necessary) and click "OK", then click "Next" twice.
13. Click "Finish".

14.4.4 Microsoft Outlook 2003™ Filters

Microsoft Outlook 2003™ includes spam filtering. Outlook will filter messages based on its own concept of spam, but you can also have it put spam messages identified by PerfectMail in your "Junk" folder.

1. Select "Inbox" in the Folder List.
2. Select "Tools" and then "Rules and Alerts".
3. View the E-mail Rules tab.
4. Click "New Rule..."
5. Check "Start from a blank rule" and select "Check messages when they arrive". Click "Next".
6. Check "with specific words in the message header".
7. In the rule description, click "specific words".
8. Under Specify a word or phrase to search for in the message header, enter X-Spam-Flag: YES to put spam in your "Junk" folder. Click "Add", then "OK", and finally "Next".
9. Under "What do you want to do with the message?", check "move it to the specified folder".
10. In the rule description, click "specified".
11. Under Choose a folder, select "Junk E-mail" and click "OK".
12. Click "Finish".

14.4.5 Macintosh OS X™ Filters

Macintosh OS X™'s built-in Mail program can create filters based on custom headers.

1. In the menu bar, click 'Mailbox' then 'New Mailbox' and create the mailbox you want the Spam to end up in.
2. In the menu bar, click 'Mail' then 'Preferences...'
3. Click 'Rules' then 'Create Rule'.
4. Add a description of the rule, then click the 'From' Criteria, then click 'Expert...'
5. In the Header: field enter 'X-Spam-Flag', click 'Add Header' and 'OK'
6. Now click 'From' and select 'X-Spam-Flag'. Select 'Contains' in the next box and enter 'Yes' in the third Criteria box.
7. In the Action section, check 'Transfer to mailbox' and select the desired mailbox. Click 'OK'.
8. Adjust the rule priorities if you want, and dismiss the Mail Preferences dialog box.
9. The next time you check your mail, check to see if any messages were automatically filtered into your Spam mailbox!

14.4.6 Outlook Express™ for Macintosh™

The instructions are the same as for Outlook Express 4.5 and 5.x for Mac, but the menu item under Tools is called "Mail Rules" in version 4.5 and "Rules" in version 5.x. Also, there's no choice between POP/IMAP. Note: if you are sending messages found by this rule to a special mail folder, you must already have created the destination folder before you create the rule.

1. From the menu bar, choose Tools; then "Rules" or "Mail Rules" depending on your Outlook Express Version (5.x and 4.5 respectively.
2. Select POP, and then hit "new" for a new rule.
3. Under the section marked "If", choose "specific header" and then type or paste in the name of the header, which is "X-Spam-Flag".
4. Under "Contains:" type in Yes.
5. In the section marked "Then", specify an action -- move to a new folder, change its status or color, as you see fit. Note that we do not recommend simply deleting messages found by this rule.
6. The Enabled box needs to be checked in order for this rule to be active - it will be checked by default.

14.4.7 Netscape™ Filtering

Netscape 6.2.1 does not allow you to create custom filters, so users of this version are unable to take advantage of the special headers used in their mail client software at this time.

Netscape 4.7.8 allows you to create a custom filter. You can supply the special x-header information to Netscape 4.7.8 by doing the following:

1. In the pull-down bar at the top of your Netscape 4.78 window, go to "Edit: Message Filters". A new window will open.
2. Click "New". Click "Advanced". A new window will open.
3. Enter "X-Spam-Flag", click "Add", and click "OK". The latest new window will close.
4. In the pull-down list, select "X-Spam-Flag".
5. In the "contains" box, enter "X-Spam-Flag: Yes".
6. In the "Perform this action" pull-down list, select "move to folder".
7. Click "new folder" and create a Spam folder. It should then be selected in the pulldown list of your folders.
8. Click OK.
9. The next time you check your mail, check to see if any messages were automatically filtered into your Spam folder!

14.4.8 Evolution™ Filters

Ximian Evolution™ is an email client for Linux similar to Microsoft Outlook™. It is installed by many Linux™ distributions including Red Hat™, Fedora™, and SuSE Linux™. Evolution™ has the ability to filter on an arbitrary header as well as on the send and receive addresses.

1. Click "Inbox" to display the Inbox.
2. Click "Edit" and select "Message Filters". (Sometimes "Filters is located under "Tools".)
3. In the Filters window, click "Add".
4. Enter a name for the filter under "Rule name".
5. Under "Find items that meet the following conditions", choose "Specific header" in the leftmost button menu; in the field to the right of "Specific header", enter "X-Spam-Flag"; change the button beside this to read "is"; and enter "YES" in the last field.
6. Under "Then", choose "Move to Folder".
7. Click "click here to select a folder".

8. Click "New", enter SPAM as the folder name, select "Local Folders", and then click "OK" for each window until you get back to the main window..

15 PerfectMail™ License Agreement

PerfectMail™ License Terms and Conditions

PerfectMail™ IS WILLING TO LICENSE THE SOFTWARE YOU ARE ABOUT TO USE ONLY UPON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS CONTAINED IN THIS END USER LICENSE AGREEMENT AND SUPPLEMENTAL LICENSE TERMS (COLLECTIVELY "AGREEMENT"). PLEASE READ THE AGREEMENT CAREFULLY. THIS IS A BINDING AGREEMENT BETWEEN YOU (THE "CUSTOMER") AND PerfectMail&trade. YOU MUST AGREE TO BE BOUND BY THE TERMS OF THIS AGREEMENT IN ORDER TO USE THE SOFTWARE OR SUBSCRIBE (EITHER AS A PURCHASER OR FOR A TRIAL PERIOD) TO PerfectMail™ SERVICES. BY PROCEEDING TO RUN THIS SOFTWARE, YOU ACCEPT THE TERMS OF THE AGREEMENT. INDICATE ACCEPTANCE BY SELECTING THE "I AGREE" LINK AT THE BOTTOM OF THE AGREEMENT OR BY SIMPLY USING THE PRODUCT. IF YOU ARE NOT WILLING TO BE BOUND BY ALL THE TERMS, RETURN THE PRODUCT TO THE PLACE OF PURCHASE.

1. DEFINITIONS

In this Agreement,

1.1. *Company* means PerfectMail™, the developer of Product. A legal entity officially known as 789852 Ontario Inc. incorporated in the Province of Ontario, Canada.

1.2. *Software* means the object code version of the computer software licensed by Customer under this Agreement.

1.3. *Documentation* means such manuals, documentation and any other supporting materials relating to the Licensed Software as are currently maintained by PerfectMail™ and generally provided to its licensee.

1.4. *Product(s)* means hardware, Software, documentation, accessories, supplies, parts and upgrades that are determined by PerfectMail™ to be available from PerfectMail™ upon receipt of Customer's order.

1.5. *Reseller* means a dealer Licensed by PerfectMail™ to sell its products.

1.6. *Customer* Any licensee of PerfectMail™ products including, but not limited to, PerfectMail™. This term will also be used for organizations who wish to or are currently evaluating Product regardless of their ultimate decision to acquire a License or purchase Product.

1.7. *Access* Any direct or indirect computer/electronic access to any physical appliance, virtual appliance, customer server or managed service running Product. This includes, but is not limited to secure command line, web, graphics user interface, e-mail or other direct or indirect access.

1.8. *Customer Agreement* means the agreement between the Customer and the Reseller and/or PerfectMail™ setting out the type of License and License Fee for the products and/or services provided.

1.9. *License* means the Software and Support License or Evaluation License granted for the appropriate number of Terminals, License Fee and Term of Validity as set out in any accompanying Customer Agreement

1.10. *License Fee* means the fee or fees designated by PerfectMail™ or the Reseller for Software and Support. Different License Fees apply depending on the type of License, the duration of the License, and the nature of the support.

1.11. *Term of Validity* means the period set out in the accompanying Customer Agreement throughout which Customer may use the software either on the basis of an Evaluation License or a Software and Support License.

2. LICENSE TERMS

2.1. Software is owned and copyrighted by PerfectMail™ and/or by third party suppliers. Customer's Software and Support License confers no title or ownership and is not a sale of any rights in the Software. Third party suppliers shall have the rights to protect its own proprietary rights to the Software in the event of any infringement.

2.2. Unless otherwise permitted by PerfectMail™, Customer may only make copies of the Software for archival purposes or when copying is an essential step in the authorized use of the Software on a backup device, provided that copies are used in no other manner and provided that the use on the backup device is discontinued when the original or replacement device becomes operable.

2.3. Customer may not use more appliances than stipulated in the License, nor may the software be used if it is not within the Term of Validity of the most recent License or Support Agreement with the Customer.

2.4. Customer will not modify, disassemble or decompile the Software without PerfectMail's prior written consent. Where Customer has other rights under statute, Customer will provide PerfectMail™ with reasonably detailed information regarding any intended disassembly or decompilation. Customer will not decrypt the Software unless necessary for legitimate use of the Software. In addition Customer will take all reasonable steps to ensure that users of PerfectMail's software in Customer's possession do none of the aforementioned.

2.5. Customer will not remove any product identification, copyright notices, or other notices or proprietary restrictions from the Software unless this option is provided as a configuration option by the Software.

2.6. Customer will not disclose results of any benchmark tests of the Software to any third party without PerfectMail's prior written approval;

2.7. Customer will not install or use demo, demonstration or evaluation licenses for any purpose other than for evaluation purposes;

2.8. Customer will not sell, transfer, lease or otherwise assign free licenses to any other party.

2.9. If Customer does not renew a license agreement with PerfectMail™ by the termination date, customer agrees that the Product will no longer be supported, that updates will not be provided, that signature files will not be updated and that customer will not be entitled to bug fixes, defect repairs, feature enhancements or other benefits.

2.10. PerfectMail™ may terminate Customer's License upon notice for failure to comply with any applicable License terms.

3. LICENSE GRANT

3.1. Subject to timely payment of the products and/or License Fees and the terms and conditions of this Agreement, PerfectMail™ grants Customer a non-exclusive and non-transferable license to use the Software embedded within our products during the Term of Validity of the License in conformance with:

3.1.1. The terms set forth herein;

3.1.2. Use restrictions and authorizations for the Software specified in the Customer Agreement;

3.2. Some of the Software Programs included in PerfectMail's software are distributed under the terms of agreements with Third Parties ("Third Party Agreements") that may expand or limit Customer's rights to use certain Software Programs as set forth in Section 2. Certain Software Programs may be licensed (or sub-licensed) to Customer under the GNU General Public License and other similar open source license agreements ("OSLAs") which, among other

rights, permit Customer to copy, modify and redistribute certain Software Programs, or portions thereof, and have access to the source code of certain Software Programs, or portions thereof. In addition, certain Software Programs, or portions thereof, may be licensed (or sub-licensed) to Customer under terms stricter than those set forth in Section 2.

3.3. Unless the Customer is a PerfectMail™ authorized reseller, Customer may not sub-license the Software unless otherwise agreed to by PerfectMail™ in writing.

4. LIMITED WARRANTY

4.1. PerfectMail™ warrants that the Software will perform substantially in accordance with administrator manual or readme file of the Licensed Product during the Term of Validity of the most recent License.

4.2. PerfectMail's and its licensor's' entire liability and Customer's exclusive remedy shall be, at PerfectMail's option, either:

4.2.1. Return the prorated License Fees for the current period, or

4.2.2. Replacement of Software that does not meet PerfectMail's Limited Warranty. This Limited Warranty is void if failure of the Software has resulted from accident, abuse, or misapplications.

4.3. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, PerfectMail™ AND ITS LICENSORS DISCLAIM ALL OTHER WARRANTIES, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR PARTICULAR PURPOSE, WITH REGARD TO THE SOFTWARE AND THE ACCOMPANYING ITEMS.

5. FEES AND TAXES

5.1. All fees payable to PerfectMail™ are due at the commencement of the License Period. Customer agrees to pay any sales, value-added or similar taxes imposed by applicable law that PerfectMail™ must pay based on the services that Customer ordered.

6. INDEMNIFICATION

6.1. PerfectMail™ shall defend, at its sole discretion, or settle any action, claim or demand brought against Customer on the basis of infringement of any copyright, trademark, trade secret or patent (the "Intellectual property Rights") by the Software or use thereof. PerfectMail™ shall pay any final judgment entered into against Customer in such action provided that PerfectMail™ has the sole control of the defense and/or settlement and Customer promptly notifies in writing of such claim and provides all information known to the Customer relating thereto, and Customer cooperates with PerfectMail™ in the defense and/or settlement. Should the Software become or in PerfectMail's opinion may become the subject of infringement of any Intellectual Property Rights, PerfectMail™ may, at its expense do one of the following:

6.1.1. Replace the Software or affected part with non-infringing programs;

6.1.2. Modify the Software or affected part to make it non-infringing;

6.1.3. Procure for Customer the right to use the Software; or

6.1.4. If none of the alternatives are commercially reasonable, PerfectMail™ may refund the prorated License Fees received from Customer for the current Term of Validity.

6.2. PerfectMail™ shall have no indemnification obligation to the extent a claim is based upon:

6.2.1. The combination, operation or use of the Software with any products or services not provided by PerfectMail™; or

6.2.2. The use of the Software in a manner not authorized by this Agreement.

6.3. THIS SECTION PROVIDES THE ENTIRE OBLIGATION OF PerfectMail™ AND EXCLUSIVE REMEDY OF CUSTOMER WITH RESPECT TO THE INFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS.

7. Indemnification by Customer

7.1. Customer agrees that it shall fully indemnify and completely save harmless PerfectMail™ and any of its directors, officers, employees, agents, representatives of and from any and all liabilities, claims, expenses, damages including reasonable legal fees and disbursements arising out of any claims or suits for damage or injury to person in connection with, directly or indirectly, in whole or in part, (i) any negligent act or omission of the Customer's employees, agents, contractors, directors, officers or any person for whom it has a legal responsibility or (ii) the failure of Customer to comply with any municipal, provincial or federal law or (iii) any act or omission which is, or can be determined to be, a breach of any term or condition of this Agreement.

8. NON-DISCLOSURE OF PERFECTMAIL INFORMATION

8.1. The Software and other proprietary information provided by PerfectMail™ hereunder contain and constitute trade secrets, information and data proprietary to copyright by PerfectMail™. Customer shall use a reasonable degree of care to protect the confidentiality of the Software and shall not cause or permit such confidential information or data to be disclosed to third parties or duplicated except as permitted in this Agreement. Customer acknowledges and agrees that unauthorized disclosure, use or copying of the Software may cause PerfectMail™ irreparable injury. Accordingly, in the event of any unauthorized disclosure, use or copying of the Software, Customer agrees that PerfectMail™ shall have the right to seek injunctive or other equitable relief. Each party will not disclose or use any business and/or technical information of the other designated in writing or orally (and promptly confirmed in writing) as *Confidential* ("Confidential Information") without the prior written consent of the other party. Such restrictions do not extend to any item of information which:

8.1.1. Is or becomes available in the public domain without the fault of the receiving party;

8.1.2. Is disclosed or made available to the receiving party by a third party without restriction and without breach of any relationship of confidentiality;

8.1.3. Is independently developed by the receiving party without access to the disclosing party's Confidential Information,

8.1.4. Is known to the recipient at the time of disclosure, or

8.1.5. Is produced in compliance with applicable law or court order, provided that the disclosing party is given reasonable notice of such law or order and an opportunity to attempt to preclude or limit such production.

9. NON-DISCLOSURE OF CUSTOMER INFORMATION

PerfectMail™ acknowledges that the information retained on Product or otherwise received or generated, directly or indirectly, while working with Customer is highly confidential in nature and must be treated with the utmost discretion. As such, the following conditions are reasonable. Therefore, PerfectMail™ hereby agrees as follows:

9.1. PerfectMail™ will ensure that all officers, employees, contractors or associates who have direct or indirect access to Customer Product, data or information will be covered under individual Non-Disclosure Agreements.

9.2. PerfectMail™ will access Customer Product only while providing support and/or updating Product. Company will seek from Customer prior consent for any access outside of support and update.

9.3. Customer shall have the option to provide Company with blanket consent or consent on an incident by incident basis. Customer shall retain the option of changing consent at any time. PerfectMail™ must be provided notice before changes to consent take effect.

9.4. PerfectMail™, its officers, employees, contractors or associates will hold any information viewed while working on Customer Product in the strictest confidence. This includes, but is not limited to Product configuration information, the contents of any log or archive information viewed while working on Product or any other information that could be reasonably deemed to not be in the Public Domain.

9.5. For back up and recovery purposes or to improve Customer experience with Product, PerfectMail™ may retain copies of Customer Product configuration information on PerfectMail's servers.

9.6. PerfectMail™ will not duplicate, transfer, retain or otherwise copy Customer Product e-mail archive or e-mail contents from Product without prior consent of Customer.

9.7. PerfectMail™ normally receives aggregate performance data from Customer Product as part of our Product health and performance monitoring capabilities. No personal information is included in this performance data.

9.8. To ensure compliance with purchased license limits or to ensure accurate billing, PerfectMail™ may, from time to time, review reported resources from Product.

9.9. PerfectMail™ will not provide confidential Customer information to third parties without prior written consent from Customer, unless compelled by law.

9.10. PerfectMail™ will not use Customer information for any purpose other than as indicated in this agreement without first seeking Customer's prior written consent.

9.11. At the end of any contracts or agreements, and when Customer's obligations to PerfectMail™ are fully discharged, Customer may request that PerfectMail™ destroy all technical records relating to the support of Product. Alternatively, PerfectMail™ may destroy all Customer data at the end of contract or agreement covering such data. PerfectMail™ is under no obligation to maintain backups or archives of Customer configuration information.

9.12. PerfectMail™ is governed by and will comply with all Privacy and Confidentiality laws for Canada and the Province of Ontario.

10. DATA COLLECTION AND NOTIFICATION

10.1. PerfectMail™ may collect statistical and status information from your server for support and analysis purposes. At no time is e-mail message content sent from the Software Product to PerfectMail™, except for any messages the Customer has reported as spam for analysis.

10.2. By default, data reporting options are enabled. It is Customer's responsibility to review the Data Disclosure document and Product Documentation for more information on data reporting, disclosure and privacy.

10.3. PerfectMail™ has provided options in the Product for the Customer to disable data collection functionality. It is the Customer's responsibility to disable any data collection or reporting functions.

10.4. PerfectMail™ maintains a list of e-mail addresses reported by the Customer for support and notification purposes. These e-mail addresses are used for sending server and product status notifications and product update messages. If Customer does not wish to receive notification messages they must contact PerfectMail™ staff and request removal from the mailing list for their PerfectMail™ server.

10.5. PerfectMail™ may from time to time, request that Customer provide PerfectMail™ with access to Product. Normally, we require access as part of its support and update obligations outlined in PerfectMail's current Support agreements. Other circumstances may also arise whereby PerfectMail™ may desire access to Product. All access is at Customer's discretion.

10.6. PerfectMail™ makes reasonable efforts to secure and keep private all Customer data including content, e-mail addresses, status and statistic information. Customer data, including e-mail addresses, will not be shared with any third party unless required by law.

11. LIMITATION OF LIABILITY

11.1. IN NO EVENT SHALL PerfectMail™ OR ITS LICENSORS BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION) ARISING OUT OF THE USE OF OR INABILITY TO USE SOFTWARE EVEN IF THE COMPANY OR ANY OF ITS LICENSORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

11.2. IN NO EVENT SHALL PerfectMail™ OR ITS LICENSORS BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, PUNITIVE OR CONSEQUENTIAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF BUSINESS OR PERSONAL PROFITS, BUSINESS OR PERSONAL INTERRUPTION, BUSINESS OR PERSONAL INVESTIGATION, LOSS OF BUSINESS OR PERSONAL INFORMATION, OR LOSS OF EMPLOYMENT) ARISING OUT OF THE ACCESS, DOWNLOADING, EXAMINATION, PROCESSING, LOGGING, FILTERING OR FAILURE TO FILTER ANY CONTENT (INCLUDING BUT NOT LIMITED TO E-MAIL AND WEB CONTENT) BY PerfectMail™.

11.3. Customer understands and agrees that E-mail may contain content that is offensive or illegal. Further, Customer understands and agrees that anti-spam functions may transfer content from remote sites to your PerfectMail™ server for analysis; this content may also be offensive or illegal. PerfectMail™ accepts no responsibility or liability for content from any source that may be encountered during anti-spam processes. Any action taken by Customer with respect to content accessed, downloaded, examined, logged, filtered or not filtered by PerfectMail™ is the customers total responsibility and liability.

11.4. Customer understands that PerfectMail™ may take actions in the process of analyzing e-mail from spam that may appear to processes and software that analyze network traffic to be the actions of user's e-mail addresses. PerfectMail™ takes reasonable steps to minimize such traffic, however Customer is reponsible for differentiating between PerfectMail automated anti-spam processes and the actions of other systems and users on their network. PerfectMail™ accepts no responsibility or liability for any intrepretation, misinterpretation or actions which may or not be taken based on network traffic, content analysis or logging or any other computer or business process or system.

11.5. Any action against PerfectMail™ must be brought within twelve (12) months after the cause of action arises. For purposes of this Section, "PerfectMail™" includes its directors, officers, employees, subcontractors, agents and suppliers.

12. TERM AND TERMINATION

12.1. The Software and Support License is subject to renewal at the end of the License Period. Unless renewed under an extension of the Customer Agreement, the License to use the Software will terminate.

12.2. This Agreement may be terminated if either party fails to perform any of its duties or obligations hereunder and fails to substantially cure such default within ten (10) days after written notice is given to the defaulting party. Upon an event of default, the non-defaulting party may terminate this Agreement by providing written notice of termination to the defaulting party, reserving unto the non-defaulting party all other rights and remedies it may have under this Agreement. If Customer is in default, PerfectMail™ reserves the right, in addition to all other rights and remedies it may have, to withhold further performance of its obligations under this Agreement and may repossess the Software and Documentation.

12.3. Upon termination of any license granted hereunder, Customer will promptly remove all Software from all memory locations, and destroy or return all copies of the Software and Documentation to PerfectMail™.

13. GENERAL

13.1. Customer may not assign any rights or obligations hereunder without prior written consent of PerfectMail™, which consent can be unreasonably withheld.

13.2. Customer who exports, re-exports or imports PerfectMail™ Hardware and Licensed Software, technology or technical data purchased hereunder, assumes responsibility for complying with applicable laws and regulations and for obtaining required export and import authorizations. PerfectMail™ may suspend performance if Customer is in violation of any applicable laws or regulations.

13.3. If any term or provision herein is determined to be illegal or unenforceable, the validity or enforceability of the remainder of the terms or provisions herein will remain in full force and effect.

13.4. Except as specifically provided in Section 3.1.2, these PerfectMail™ Software and Support License Terms supersede any previous communications, representations or agreements between the parties, whether oral or written, regarding transactions hereunder. Customer's additional or different terms and conditions will not apply. These PerfectMail™ Software and Support License Terms may not be changed except by an amendment signed by an authorized representative of each party.

13.5 This license does not obligate PerfectMail™ to provide support for products licensed under free or trial licenses.

14. GOVERNING LAW

14.1. This Agreement shall be governed by and interpreted in accordance with the laws of Ontario, Canada, without reference to conflict of law principles. Customer and PerfectMail™ agree to the exclusive jurisdiction of the courts located in Brampton, Ontario, Canada.

15. PARTIAL INVALIDITY.

15.1. Both parties to this Agreement hereby acknowledge that neither of them intends to violate any public policy, statutory or common laws, rules, regulations, treaties, or decisions of any government agency or executive body of any country or community or association of countries.

16 Data Collection Disclosure

Introduction
Following is a full disclosure of all data reported to PerfectMail™ from a PerfectMail™ product. PerfectMail™ is a *high touch* product giving the following benefits:

- *Statistical Reporting* gives us clear & early warning of developing spam trends.
- *Server Monitoring* ensures early notification of problems.
- *Quick & Effective* customer support.
- *Off-site Backups* provide additional peace of mind. If needed we can quickly provide assistance or build a *fully configured* replacement machine.

Automatic Server Updates
The following updates occur automatically. To disable automatic updates, update the related settings on the *Security Settings* page.

- *Anti-virus Update:* Virus update checks are performed every 10 minutes. If an update is available, it will be installed automatically.
- *Anti-spam Update:* Anti-spam update checks are performed once a day. If an update is available, it will be installed automatically.
- *Software Update:* Software updates are performed by PerfectMail™ staff, when available; and only if access is granted.

Server Support Data
The following data elements are normally reported back to PerfectMail™ for support and analysis purposes. To disable any of these reporting features update the *Server Admin=>Server Settings* page on the *Web Interface*. If support & reporting features are disabled your PerfectMail™ product will still send notification that these features are disabled. **No e-mail message content is ever sent to PerfectMail™; except for those messages the client wishes to have examined for spam content.**

- Statistical Reporting: This hourly report consists of statistical information regarding the effectiveness of the anti-spam software. E.g. number of rejects, tags, accepts, RBL's, mining attempts, spam traps, etc.
- Report Spam: The client user or administrator forwards a spam e-mail to PerfectMail™ for review. Included with the reported spam e-mail are the PerfectMail™ server name and the name of the submitting user.
- Server Monitoring: Hourly health reports allow us to see if there are any issues with the product as a whole, and databases in particular. These messages describe the state of the databases, but do not include any elements of their content. If there is an issue with a database, a notification message containing the machine name and data table name is sent to PerfectMail™ for further attention. (PerfectMail™ is able to self-fix its databases. Administrator intervention is rarely required.) Additionally, in the event of a process crash, a core file (describing what the program was doing the issue occurred) may be sent for analysis.
- False Positive Investigation: For each false positive release, a message is sent to PerfectMail™. If the client has requested *false positive investigation*, we may examine the message to determine what the problem may be. In practice PerfectMail™ will contact the client for permission to perform such actions.

17 Support

If you have any issues at all, please contact our support team. You can reach us between 9:00am and 6:00pm EST, Monday to Friday. The best way to get support is to file a Support Incident on our website: http://www.perfectmail.com/support.

If you discover a PM bug, then your support incident incurrs no charge. Support incidents are intended to help customers do things more quickly and effectively or to help gather information or identify e-mail issues.

Support incidents are included in the price of the product (excluding the free version). Support packs are also available to bump this if needed. With support, if the issue is with our software or some deficiency on our part, including unclear documentation, or for customer feedback support is free. For other issues we burn or charge for a support incident.

E-mail Addresses:
Sales: sales@perfectmail.com
Support: support@perfectmail.com

Phone Numbers:
Office: +1 905 451 9488
Toll Free: +1 888 451 3131
Facsimile: +1 905 451 7823

Mailing Address:
PerfectMail™
15 Claypine Trail
Brampton, Ontario
Canada L6V 3L8

Web Site:
http://www.perfectmail.com