

Help

DoubleCheck Quick Reference Table of Contents

System Section

- [System Preferences](#)
- [Configuration Import](#)
- [Configuration Export](#)
- [Date and Time Settings](#)
- [Network Information](#)
- [Restart Networking](#)
- [System Shutdown / Reboot](#)
- [Supervised Daemons](#)
- [Mysql](#)
- [User Functions](#)
- [User Manager](#)
- [License Manager](#)
- [System Monitoring](#)
- [Current Network Status](#)
- [Local System Monitoring](#)
- [Remote System Monitoring](#)
- [System Info](#)
- [Scanner Modules](#)
- [Module Configuration](#)
- [Setup Wizard - Step 1](#)
- [Setup Wizard - Step 2](#)
- [Setup Wizard - Step 3](#)
- [Setup Wizard - Step 4](#)
- [Setup Wizard - Step 5](#)
- [Setup Wizard - Step 6](#)
- [Setup Wizard - Step 7](#)
- [Setup Wizard - Step 8](#)
- [Setup Wizard - Step 9](#)
- [Setup Wizard - Step 10](#)
- [Setup Wizard - Step 11](#)
- [Setup Wizard - Step 12](#)
- [Setup Wizard - Step 13](#)

Logs Section

- [Log Display Settings](#)
- [Log Settings](#)
- [Quick Search](#)
- [Database Search](#)
- [Database Search Results](#)
- [Email Log](#)
- [Non-Spam Log](#)
- [Spam Log](#)
- [Policy Log](#)
- [Virus Log](#)
- [SMTP Denies Log](#)

- [RBL Deny Log](#)
- [SPF Deny Log](#)
- [SMTP Deny Log](#)
- [Quick Reports](#)
- [Management Report](#)
- [Overall Report](#)
- [Non-Spam Report](#)
- [Spam Report](#)
- [Policy Report](#)
- [Virus Report](#)
- [Trend Analysis](#)
- [Cost Savings Calculator](#)
- [MRTG Graphs](#)
- [Raw Logs](#)

Spam Section

- [Spam Preferences](#)
- [Customize Heuristic Scoring](#)
- [Custom Spam Rules](#)
- [Advanced Spam Preferences](#)
- [Database Settings for spamd](#)
- [Manual Spam Engine/Rules Update](#)
- [Restart Spam Daemon](#)

Policy Section

- [Default Policy Settings](#)
- [Queue Level Policies](#)
- [Add Policy Rule](#)

Virus Section

- [General Virus Configuration](#)
- [Install EXTRA.DAT file](#)
- [Anti-Virus Information](#)
- [Manual Virus Definition Update](#)

SMTP Section

- [SMTP General Settings](#)
- [Recipient Domains and Mail Routes](#)
- [Add Recipient Domains](#)
- [Recipient Verification Settings](#)
- [SMTP Authentication Settings](#)
- [SMTP Envelope Rules](#)
- [SPF \(Sender Policy Framework\) Settings](#)
- [RBLSMTPD Settings](#)
- [RBL Servers](#)
- [Host Access Rules](#)
- [Signature/Disclaimer Settings](#)

DoubleCheck Quick Reference

System Section

System Preferences

System Admin Name:

Name of System Admin. Used in automated emails to end-users.

System Admin Email:

Email of System Admin. Used as return address in automated emails to end-users.

Default Login Permission on New Users:

When adding new users to the system, this will be the default login permission.

Default SMTP Authentication Permission on New Users:

When adding new users to the system, this will be the default SMTP Authentication setting to enable/disable them from send authenticated email.

New User Signup Method:

Will specify whether to allow new users to confirm their accounts via email, or to require a sysadmin to confirm new accounts.

Remote Configuration Backup:

Enable or Disable Remote Configuration Backup to NMGI. This option is not available without Maintenance Contract.

Automatic Virus Definitions Updates:

Enable or Disable Automatic Virus Definition Updates. Enabled by Default. This automatic check is every half hour.

Notify Sysadmin on Virus Definition Updates:

Enable or Disable Notification when Definitions have been updated. Disabled by Default.

Automatic Spam Engine/Rules Updates:

Enable or Disable Automatic Spam Engine and Ruleset Updates. Enabled by Default. This automatic check is daily.

Notify Sysadmin on Spam Engine Updates:

Enable or Disable Notification when Spam Engine or Rulesets have been updated. Disabled by Default.

Identification Threshold Min/Max:

Allows you to define minimum and maximum values that a postmaster or user may set their Spam Identification threshold too.

Quarantine Threshold Min/Max:

Allows you to define minimum and maximum values that a postmaster or user may set their Spam Quarantine threshold too.

Delete Threshold Min/Max:

Allows you to define minimum and maximum values that a postmaster or user may set their Spam Delete threshold too.

Whitelist Score Min/Max:

Allows you to define minimum and maximum values that a postmaster or user may set their Whitelist score too.

Blacklist Score Min/Max:

Allows you to define minimum and maximum values that a postmaster or user may set their Blacklist score too.

Configuration Import

Configuration Import:

A Doublecheck configuration file can be Imported (restored) either via a local file upload, or via the remote restore options. The remote restore will not be available without Maintenance Contract. After configuration Import, it is recommended to restart the system for changes to fully take place.

Configuration Export

Configuration Export:

A Doublecheck configuration file can be Exported (backed up) either via a email, or via the remote backup options. The remote backup will not be available without Maintenance Contract. A remote Configuration Export must be performed before a remote Configuration Import, otherwise the import will fail. Nightly remote configuration exports happen automatically, so a remote configuration import will always get the system back to the last successful export.

Date and Time Settings

Set Time By:

Two methods are supported when settings the time: NTP and Manual. It is recommended that you set time via NTP to keep the system time accurate. If you have an internal time server, you may use that, otherwise use the external time source provided or change it to one that is close to you. NTP has nothing to do with what timezone you are in, that is solely for display purposes. Please change your timezone to match your location, even when using NTP. Note, NTP uses destination port 169/udp, so if your firewall limits outbound connections and you are using a remote time source, NTP may not work for you. In this case, setting the time manually, or using an internal time server would be recommended.

NTP Server:

The NTP Server is the time source you would like to sync your system clock with. You may use the remote time source provided, or change that to any other time source whether it is internal or external.

Set Timezone:

Setting the timezone will adjust the time displayed to your local time.

Manually Set Date:

Manually setting the date should only be done if you cannot connect to a remote time source via NTP.

Manually Set Time:

Manually setting the time should only be done if you cannot connect to a remote time source via NTP.

Network Information**Connection Status:**

The connection status interface will show you green lights when it is able to connect to the Service, and red when it cannot. Red lights in the Outbound column indicate no internet access or the ports are being filtered. The lights in the local column should always be green as those are local tests. See System->Control Service Daemons to manage the local daemons.

Devices:

Each Network Interface that is detected in the System will be displayed in Network Settings. Each Interface can be configured separately, and one be the Gateway Device, or they can be Multi-Homed, where both devices will have a gateway of their own. The device with the lowest weight preference will be the default gateway for new outbound connections. If the weight is the same, it will load-balance the connections. For incoming connections, the Multi-homed environment will send traffic back out which ever source it came in on.

Boot Protocol:

Static needs hard-coded TCP/IP information. DHCP will obtain information from a DHCP Server. If using DHCP, it is recommended that you use assign a static address to the machine via the DHCP server based on its MAC Address.

IP Address:

The IPv4 address you will be assigning to this machine. Internal IP addresses will be in the 10.x.x.x, 172.16-31.x.x, or 192.168.x.x format.

Subnet Mask:

The Subnet Mask (netmask) determines what subnet this machine will be on. A standard Class C subnet is 255.255.255.0.

Host Name:

Host Name is the name you want to assign to the machine. It has no bearing on SMTP services. To set the SMTP hostname, please see SMTP Hostname in the SMTP section.

Gateway:

The Gateway address is the upstream router or firewall that provides internet access to this device. If this machine has an internal IP address, the router or firewall must be NAT capable.

Gateway Device:

The Ethernet device that is attached to an upstream router. If set to Multi-Homed, you will be required to set Gateway Information on each device respectively.

DNS Nameservers:

DNS Nameservers accept up to 4 nameservers. The default nameserver will be 127.0.0.1, which is the box itself. Doublecheck runs its own BIND caching nameserver, which helps eliminate multiple RBL and DNS based lookups for the same hosts. This improves speed, performance, and saves cpu and bandwidth.

Restart Networking**Info:**

Restarting Networking will take down all ethernet devices and routing and bring them back up based on the current network settings

System Shutdown / Reboot**Restart:**

Restarting Doublecheck will perform a full linux reboot. All mail deliveries that occur while the box is down will tempfail.

Shutdown:

Shutting down Doublecheck will perform a full linux halt.

Supervised Daemons**send:**

The qmail-send daemon is responsible for delivery of mail.

smtpd:

The qmail-smtpd daemon is responsible for accepting of mail, and passing it onto the Anti-Virus and Spam scanners.

spamd:

The spam daemon is responsible for accepting mail and assigning it a score.

Mysql**mysql:**

The mysql daemon is responsible for doublecheck configuration, logging, and session state.

mysql tables :

The mysql tables for doublecheck will be listed, below the mysql status. You can check the tables for errors, repair the tables if errors are found, and optimize the tables in case of overhead.

User Functions

User Search:

The user search field can search for a supplied string and compare matches against the email address and name fields. You can also limit searches by specific user flags.

Adding New Users:

To add a new user, click the button labeled Click Here. Fill out the add user form for the new user and submit it. To add a user at a particular domain name, that domain must first be personalized. See SMTP->Recipient Domains and Mail Routes for personalizing domains.

User Manager**Display Users:**

User accounts will be displayed 25 at a time. You can limit your display to browsers, new users, users, postmasters or sysadmins using the Search User interface. The Search User interface can optionally take a value to search for. This value is compared against the First Name, Last Name, and Email Address, and will return case-insensitive matches containing that pattern.

User Roles:

There are 4 roles that a user can play. By default, all new users added have a single flag of U. The U flag gives them user permissions to log in and manager their own settings. The second flag is the P (Postmaster) flag. With this flag, a user can modify settings for their Domain. Third, the S (SysAdmin) flag. This flag allows the user to set Global options. The default admin account is the only user, and only SysAdmin by default. The last flag, B (Browser) is an add-on flag that can apply to any of the first 3 roles just discussed. If you add a B flag to a SysAdmin, that user can log in and look at everything a SysAdmin can look at, but that user cannot make any modifications to settings. Same goes for a PB (Postmaster/Browser). A PB can view logs and settings for his domain, but cannot make any changes. A UB (User/Browser) can view their own logs, but cannot make modifications to their settings.

Add New User:

In order to add a new users, you must have a SysAdmin flag, or be delegated as the Postmaster for your domain. Postmasters can only add new users or other postmasters at their domain. Those with only a User flag have no "Add New User" rights.

License Manager**License Information:**

To Activate Doublecheck, you must enter a valid License Number and Activation key. Activation Keys are specific to the DCID, and contain information about which features to unlock, as well as how many users and personalized domains are available. Also included in the key is information about Maintenance and Warranty. There is an update key feature if your need for users or domains change.

LIC #:

The License number.

MC #:

Maintenance Contract Status. Will show None if Maintenance Contract has expired.

EW #:

Extended Warranty Status. Will show None if warranty has expired or the hardware was not provided by NMGI.

Estimated / Licensed Users:

Estimated users are based on mail traffic by unique recipient addresses for domains tied to this license number. To get individual domain user estimates, see SMTP->Recipient Domains and Mail Routes. The Licensed Users number is the user level purchased.

Licensed Domains:

Licensed domains is the number of personalized domains available. However, you may have as many unpersonalized (global) domains on a single license as long as the total user count is within the licensed user limit.

System Monitoring**Current Network Status:**

The current network connectivity table shows basic network services provided by or utilized by DoubleCheck, and whether or not it can talk on those ports.

Local System Monitoring:

Local System monitoring are checks ran by the system itself to insure there are no problems with the spamd agent, sql tables, or message queue. A status report can also be scheduled here on a user-defined basis.

Remote System Monitoring:

To Activate remote monitoring, you must obtain an activation key. Once you have this key, you can activate the monitoring agent by typing in the key and pressing the Install button. Once the key is install, simply click the START link under Daemon Status.

Current Network Status**Mail Delivery:**

DoubleCheck use SMTP to send and accept mail on port 25/tcp.

Name Resolution:

By default, DoubleCheck uses itself as the primary nameserver for name resolution. This requires port 53/udp outbound to be open, otherwise name resolution will fail. If port 53/udp cannot be opened outbound, an internal DNS server with the ability to resolve queries will need to be used as the primary nameserver and the others removed.

Spam Updates:

Spam Updates use web requests, port 80/tcp, to pull necessary files to update the spam engine.

Virus Updates:

Virus Updates use ftp, port 21/tcp, to pull new virus definition files.

Local System Monitoring

System Status Report:

The system status report is a quick summary of system information such as virus and spam status, license information, and a quick breakdown of mail flow since last status report. This is intended to go to a system admin as a way to get a quick health report on the system without having to log in.

Spamd Child Monitor:

The spamd child monitor will watch spamd children and make sure they do not use too much CPU. When a child uses too much CPU, it is normally because there is a problem. Spamd children auto-spawn and respawn themselves after they process 25 messages each, so the CPU time on a single child is normally under 30 seconds. The default CPU time to alert on is 5 minutes, and it is recommended that Kill Long Processes is enabled to prevent excess utilization and potential denial of service.

Message Queue Monitor:

The message queue monitor watches number of messages in the queue. If the queue grows large, it normally indicates a delivery problem. Many times a growing queue will indicate a problem with the destination mail server not accepting the mail properly. The number of messages in queue to alert on depends on your mail traffic.

SQL Table Monitor:

The SQL Table monitor watches the SQL tables to make sure corruption does not occur. If it does, an Alert is sent. Optionally, you can have it automatically repaired, however this is not recommended for large or high traffic sites as the table will be locked for a couple minutes and will cause mail to back up.

Remote System Monitoring

Remote Monitoring Status:

When enabled, the status will show where the system is reporting to. You can start and stop the monitoring daemon here as well. When enabled, a process ID (pid) will appear. For https reporting to an N-Central Server, you will need to make sure port 443/tcp outbound is not blocked.

Install New Key:

An N-Able Activation key is needed to start the monitoring daemon. This key can be obtained from your N-Central Server if you have an N-Able monitoring solution, or a 3rd party that is Ready for N-Able. NMGI and DoubleCheck are Ready for N-Able.

System Info

Kernel Info:

Reports which kernel version is running

Users Currently Logged In:

Reports which users are logged in at the console level, or remote shell.

Current Memory Status:

Reports Physical and Swap memory usage

Current Process List:

Reports full process listing

Scanner Modules

Module Config for Specific Domain or User:

This allows you to configure scanners for a specific domain or user from the Sysadmin login.

Scan Order:

The Scan Order determines the order the modules are ran. You can either modify the Scan order on the left, or modify the module associated with that order number on the right. You cannot have duplicate scan orders. If you want to disable a module, set the Scan Order on that module to Disabled.

Modules for Global Configuration:

A drop down list of available modules will be available for each scan order. The list of available modules is determined by your license and activation key.

Module Configuration

Auto Definition Updates:

Turns auto-updates on or off for this module

Auto Update Check Frequency:

How often the updater should check for updates on this module.

Paths and Options:

Paths and arguments to runtime scanners can be modified here, but this is highly discouraged. Changing these options may cause scanners to fail!

Setup Wizard - Step 1

Begin Setup Wizard:

Step 1 simply prompts for you to walk through the setup wizard. Press Yes to continue, No to skip the wizard.

Setup Wizard - Step 2

Primary Domain Name:

Step 2 requires the primary domain name you want this system to accept mail for. Other domain names can be added later via SMTP->Recipient Domains and Mail Routes.

Setup Wizard - Step 3

Mail Server Location:

Step 3 is the mail server location for the primary domain name defined in step 2. It will automatically try to pull the IP address based on the MX record resolution. If the lookup results in 'nxdomain', please type the IP address of your Mail Server. If the lookup results in the external IP address and Doublecheck is placed behind the firewall, simply change the IP address to the internal address of the mail server.

Setup Wizard - Step 4

SMTP Hostname:

Step 4 sets the SMTP Hostname of Doublecheck. The SMTP Hostname for this server how this system speaks to other mail servers on the internet. The hostname you assign here should reside in your public DNS, and is recommended to be the same hostname you have defined as your MX record. It will automatically set this hostname based on an MX Record lookup for your primary domain name. If the hostname it detects is not correct, please modify it before pressing Continue.

Setup Wizard - Step 5

System Administrator Email Address:

Step 5 will set the admin email address. The admin contact address should be the person responsible for maintaining the system. This address may receive system alerts regarding updates or errors detected in the system. This admin email address is not for virus notifications.

Setup Wizard - Step 6

Available Antivirus Engines:

Step 6 will show which Anti-Virus engines are available for scanning email. To disable a scanner, simply uncheck the box beside it. By default, all AV Modules will be enabled.

Setup Wizard - Step 7

Antivirus Admin Email Address:

Step 7 sets the email address to whoever received virus notifications in your organization.

Setup Wizard - Step 8

Policy/Content Filter Engines:

Step 8 will show the available content filters. All content filters are enabled by default. To disable a scanner, check the box beside the module name.

Setup Wizard - Step 9

Anti-Spam Engines:

Step 9 will show the available anti-spam engines. All anti-spam engines are enabled by default. To disable a anti-spam scanner, check the box beside the module name.

Setup Wizard - Step 10

Spam Accuracy Level:

Step 10 sets the Global Spam Identification threshold. A setting of Very High is equal to an level 3, High is 4, Average is 5, Low is 6, and Very Low is 7. See Spam Section->Spam Preferences->Spam Identification Threshold for more details on scoring.

Setup Wizard - Step 11

Spam Message Handling:

Step 11 defines quarantine, reject, and delete thresholds. Multiple thresholds can be selected by holding the CONTROL key down while clicking. After you select which methods you want, you will set their threshold scores in Step 12.

Setup Wizard - Step 12

Spam Quarantine Level:

The Spam Quarantine Level corresponds to the numeric Spam Quarantine threshold, where the lower the number, the more spam is quarantined. A setting of Very High is equal to an level 5, High is 7, Average is 9, Low is 12, and Very Low is 15.

Spam Quarantine Email Address:

The email address to route quarantined mail to.

Spam Reject Level:

The Spam Reject Level corresponds to the numeric Spam Reject threshold, where the lower the number, the more spam is rejected. A setting of Very High is equal to an level 5, High is 7, Average is 9, Low is 12, and Very Low is 15.

Spam Delete Level:

The Spam Delete Level corresponds to the numeric Spam Delete threshold, where the lower the number, the more spam is deleted. A setting of Very High is equal to an level 5, High is 7, Average is 9, Low is 12, and Very Low is 15.

Setup Wizard - Step 13

Setup Complete:

Click Apply Settings to finalize your settings. If you need to modify a setting, use Go Back. If you want to discard the

configuration, chose Discard Settings.

Logs Section

Log Display Settings

Log Display Settings:

Display Settings control the number of rows to display for the top sender and recipient tables, found in the reports.

Log Settings

Log Settings:

Log Settings control where to log email information to, how long to keep the logged information, and how to email the purged logs to.

Quick Search

Quick Search:

The Quick Search feature allows you to see complete email flow by combining both log tables into a common log. Only mailfrom, rcptto, and remoteip are searchable fields in the Quick Search interface, and from there you have the ability to refine the search by Event and Type. Also, if you only want to see records from a certain table, you can select that table from the Search Logs drop down. By default it will show the 50 most recent records matching the criteria you specify, you can change the limit using the Records per Page dropdown.

Message Details:

To get more information on a particular record, click the details link on the left. This page will show you all relevant information pertaining to this connection or email message. If the message was archived, it will give you the ability to view the source, headers, text or html parts of the message. Regardless of Content-Type on virus infected email, HTML parts will not be available. Use Full Source view and copy+paste it out into your own application. The HTML View should be used with caution, as embedded script or object tags in bad email could make your browser perform bad things.

Resend Message:

If the message was archived and you need to resend this message, the resend button will allow you to do this. The resend button will not be available if there is no archived source.

Database Search

Search Tables:

A Database Search can be run on either the Email Log table, or the SMTP Deny table by changing the "Search Database Table" option.

Search Output:

After a search is performed, all clickable hyperlinks will perform new searches.

Search Groupings:

The Group By field allows you to group results based on unique entries in that field. For example, Show all results that contain Mail From: john@doe.com and Group By: Recipient. This will show all the unique people that john@doe.com has sent to, and produce a new column to the right containing the number of times he has emailed these users. After this query has run, you have the option of Sorting based on the Group Count column by running another query and selecting Group By: Group Count.

Database Search Results

Database Search Results:

Database searches return all hits matching the criteria supplied based on the amount of records currently in the email table. By default, the email table will keep up to 50,000 records, so if you get 1,000 emails a day, you will have 50 days worth of searchable data. If you need more than 50,000 records, that setting can be changed in Logs->General Settings.

Searchable Results:

All record fields have hyperlinkable data so you can follow other links without re-running database searches.

Email Log

Description:

The Email Log contains all non-purged email with full details, ordered by datetime so the newest email will be at the top by default. The amount of records in the email log will depend on your Log Purge settings in Logs->General Settings.

Non-Spam Log

Description:

The Non-Spam Log contains all non-purged non-spam emails with full details, ordered by datetime so the newest email will be at the top by default. The amount of records in the email log will depend on your Log Purge settings in Logs->General Settings.

Spam Log

Description:

The Spam Log contains all non-purged spam emails with full details, ordered by datetime so the newest email will be at the top by default. The amount of records in the email log will depend on your Log Purge settings in Logs->General Settings.

Policy Log**Description:**

The Policy Log contains all non-purged policy violation emails with full details, ordered by datetime so the newest email will be at the top by default. The amount of records in the email log will depend on your Log Purge settings in Logs->General Settings.

Virus Log**Description:**

The Virus Log contains all non-purged virus emails with full details, ordered by datetime so the newest email will be at the top by default. The amount of records in the email log will depend on your Log Purge settings in Logs->General Settings.

SMTP Denies Log**Description:**

The SMTP Denies Log contains all non-purged connections that have been denied at the SMTP level, ordered by datetime so the newest email will be at the top by default. The amount of records in the email log will depend on your Log Purge settings in Logs->General Settings. RBL Denies and SMTP Denies will comprise this log. SMTP Denies can be Bad Senders (Error Code 554), Bad Recipients (Error Code 555), Relay Attempts (Error Code 553), Invalid Sender Domain (Error Code 552), and others.

RBL Deny Log**Description:**

The RBL Deny Log contains all non-purged connections that have been denied at the SMTP level (Error Code 559 perm or 451 tempfail) due to RBL matches, ordered by datetime so the newest email will be at the top by default. The amount of records in the email log will depend on your Log Purge settings in Logs->General Settings.

SPF Deny Log**Description:**

The SPF Deny Log contains all non-purged connections that have been denied at the SMTP level due (Error Code 558) to Sender Policy Framework (SPF) failures, ordered by datetime so the newest email will be at the top by default. The amount of records in the email log will depend on your Log Purge settings in Logs->General Settings.

SMTP Deny Log**Description:**

The SMTP Denies Log contains all non-purged connections that have been denied at the SMTP level due to SMTP Rule matches, ordered by datetime so the newest email will be at the top by default. The amount of records in the email log will depend on your Log Purge settings in Logs->General Settings. Only SMTP Denies will comprise this log. SMTP Denies can be Bad Senders, Bad Recipients, Relay Attempts, Invalid Sender Domain, among others.

Quick Reports**Quick Reports:**

Quick Reports give you a snapshot of the top senders, recipients, or IP addresses in various categories. Quick Reports can be customized by start and stop date, and can show a custom number.

Management Report**Description:**

The Management Report combines various logging features from other reports in order to provide a single point of reference for administrators.

Date Selection:

A specified date range can be specified for producing a management report. However, the Management Report only runs on the email log data, so depending on your purge intervals, you may have between 1 to 90 days worth of data by default depending on your daily traffic. Specifying a date older than the oldest log entry will force the date to the oldest entry for you. Same goes for specifying a date in the future that is beyond your newest log entry. To gain more email data, you need to increase your record size in Logs->General Settings. The larger the number, the longer it will take to produce reports. This number should not exceed 250,000 records unless you have dedicated database hardware.

Outbound Email Classification:

Outbound email is determined based on the recipient address that the email was sent to. If the recipient address is not located in your recipient hosts file (SMTP->Recipient Domains and Mail Routes) then it is considered Outbound, since a remote connection would be needed to deliver the mail. Relay attempts may show as outbound mail on SMTP Denies.

Overall Report**Description:**

The Overall Report is a report on all email information, including RBL Denies, SMTP Denies, Spam and Viruses. This report will show overall policy information based on a user defined time period to present. Detailed information such as Top Senders or Recipients is limited to the amount of data in the email database, which is purged based on settings found in Logs->General Settings.

Non-Spam Report**Description:**

The Non-Spam Report is a report only on Non-Spam email. This report will show overall policy information based on a user defined time period to present. Detailed information such as Top Senders or Recipients is limited to the amount of data in the email database, which is purged based on settings found in Logs->General Settings.

Spam Report

Description:

The Spam Report is a report only on Spam email. This report will show overall policy information based on a user defined time period to present. Detailed information such as Top Senders or Recipients is limited to the amount of data in the email database, which is purged based on settings found in Logs->General Settings.

Policy Report

Description:

The Policy Report is a report only on Policy Violations. This report will show overall policy information based on a user defined time period to present. Detailed information such as Top Senders or Recipients is limited to the amount of data in the email database, which is purged based on settings found in Logs->General Settings.

Virus Report

Description:

The Non-Spam Report is a report only on Virus email. This report will show overall policy information based on a user defined time period to present. Detailed information such as Top Senders or Recipients is limited to the amount of data in the email database, which is purged based on settings found in Logs->General Settings.

Trend Analysis

Queue Distribution:

Breaks down email traffic that has entered the queue, based on the time period you specify.

Total Distribution:

Breaks down all email traffic, including SMTP/RBL Deny information based on the time period you specify.

Trend Charts:

Shows Clean, Spam, Virus, and SMTP Deny history over a time period you specify. Several Display methods available.

Spam Score Distribution:

Shows a spam histogram based on spam score of emails during a user defined time period to present. Can aide in determining various Spam thresholds.

Cost Savings Calculator

Description:

Cost Savings Calculator allows the administrator to plug in real numbers on live data to produce and Cost Savings.

MRTG Graphs

MRTG Graphs:

These graphs help show trends over time. Network, Memory, Disks, Load, Queue and SMTP are some of the categories that are monitoring. By watching these graphs, you can determine anomalies in your email traffic and detect possible system failure.

Raw Logs

Raw Log Files:

Raw Log files allow you to see low level system information. Low level delivery information is found in the qmail/ directory. Low level smtp connection information is found in the smtpd/ directory. The general DoubleCheck log file is doublecheck.log found in the main directory. Other standard linux log files provided by syslog are also found in this directory.

Downloading Large Log Files:

Any log file that is over 1MB in filesize will be offered as a compressed file download. You will need software on your computer to uncompress this gzip data file. Wizip and Winrar will both uncompress *.gz files.

Spam Section

Spam Preferences

Spam Identification Threshold:

By turning the Spam Identification threshold OFF, you effectively stop the spam engine from running. When it is set to ON, you must specify a value that you want to start identifying messages as spam at. The Default Threshold/Score is 5.0. A heuristic, weighted rule base of over 650 rules will determine what each message scores. The higher the score, the more spam content that is in that message. By raising your threshold, you will identify less spam, but there will be less chance of having a false-positive. By lowering your threshold, you will catch more spam, but will need to maintain a good whitelist for the false-positives.

Alter Subject:

When Subject Rewriting is turned ON, any message that scores over your Identification Threshold will be TAGGED (prepended) to the subject header. If Subject Rewriting is turned OFF, then this setting is unused, but messages that score over your threshold will still be logged as spam in your monitoring and report. This would allow you to keep a threshold at 5, and delete at 10, but everything that scores between 5 and 10 would deliver onto the end users untagged (but logged as spam).

Keywords for Subject Prepend:

HITS - Can be used to display the spam score in the subject line
REQD - Can be used to display required hits in the subject line

Quarantine Threshold:

The Quarantine Threshold is an independent threshold that allows you to quarantine message that score over the threshold you specify. For example, you could Identify Spam at 5.0, and Quarantine at 8.0. This would allow everything that scored from 5.0 to 8.0 to be tagged as spam and delivered onto the end user for filtering via inbox rules. The Quarantine Threshold should be greater than or equal to the Identification threshold, and can be greater than or less than the Delete Threshold, but not equal to the Delete Threshold.

Quarantine Address/Location:

When a message scores over the quarantine threshold, it can be sent to a quarantine email address, or a quarantine location. Currently, IMAP4 is the only supported quarantine location, and must be specified in the format `imap://user:pass@ip:folder`. So, to copy to a public folder on exchange, a setting like `imap://aduser:adpass@adserver:Public Folders/Quarantined Items` would work great, assuming there is a public folder called 'Quarantined Items'. Spaces are allowed.

Delete Threshold:

The Delete Threshold is an independent threshold that allows you to delete messages that score over the threshold you specify. Heuristics show, email that scores over 9.0 has a 0.01% chance of being a false-positive, and mail that scores over 12.0 has 0.00% chance of false positive so setting a level in that range should yield best results. The Delete Threshold can be higher or lower than the Quarantine Threshold, but not equal to the Quarantine Threshold if used. The Delete Threshold should also be greater than or equal to the Identification Threshold.

Reject Threshold:

The Reject Threshold is an independent threshold that allows you to reject messages that score over the threshold you specify. Rejecting spam will send an 554 SMTP Error code to the connecting mail server. Well behaving mail servers (ie legit senders) will turn this into a Mail-Daemon to the return path (mail from: envelope) if it is not null.

Message Handling:

When this option is set to On, an incoming message that is tagged as spam, instead of modifying the original message, the spam engine will create a new report message and attach the original message as a message/rfc822 MIME part (ensuring the original message is completely preserved, not easily opened, and easier to recover). If this option is set to Off, incoming spam is only modified by adding some headers and no changes will be made to the body.

Ok Languages:

Which languages are considered OK to receive mail in. The Spam Engine will try to detect the language used in the message text. Note that the language cannot always be recognized reliably. In that case, no points will be assigned.

Ok Locales:

Which locales (country codes) are considered OK to receive mail from. Mail using character sets used by languages in these countries, will not be marked as possibly being spam in a foreign language.

Use Auto Whitelist:

The Auto Whitelist (AWL) system tracks unique sender histories, and applies a factor to the average score for new mail from those senders. A unique sender is determined by the senders email plus the first to IP segments for each recipient. `user@hotmail.com:68.102` for `user@yourdomain.com` is considered different than `user@hotmail.com:24.225` for `user@yourdomain.com` and is tracked independently.

Use Bayesian Classification:

The Naive Bayesian-style classifier allows the spam engine to tokenize each message and compare against a database of tokens to determine spam probability. The database is verified against is created by turning Auto Learning on, otherwise you must supply your own databases. Bayes will not begin classifying email until it has at least 200 spam and 200 non-spam emails in its database. This is done to prevent inaccurate results from a low corpus. Bayes classification is on by default.

RBL Checking:

Real-time Black Hole list support is disabled in the spam engine by default. RBLSMTP is ran at the SMTP level to block RBL listed mail before it ever enters into the queue. You can enabled this here if you need to do second level RBL checks that go deeper than just the connecting IP address.

Customize Heuristic Scoring**Rule Category:**

Rules are grouped into one of six distinct categories: header, body, rawbody, uri, full and meta. The Header Rules category contains all tests that are applied against the message headers. The Body Rules category contains all tests that are ran against the body of the email. Non-textual MIME parts, HTML tags and line breaks will all be stripped, and the message will be decoded from quote-printable or base64 as necessary. Body tests also include the Subject line as the first line of body. Raw Body rules are those that are ran against the raw data in all textual parts of the email. Like Body Rules, Raw Body Rules will also be decoded from base64 and quote-printable, but HTML tags will remain intact. URI Rules are those which are applied against all URIs found in the body of the email. Full Rules will run against the entire email message, including headers, body and all MIME parts. Meta Rules are combined rules based on the results from other rules that the particular Meta Rule uses. Meta Rules return a boolean value (true or false).

Rule Name:

The name of the rule as defined within the heuristic engine.

Rule:

The code (regex,eval,meta) that is applied against the email for the specific category (header, body, rawbody, uri, full or meta).

Rule Description:

The description associated with the heuristic rule.

Default Scores:

The default scoring applied for message matching this heuristic rule. There are 4 score fields. Field 1 is the score applied when Bayes and Network tests are disabled. Field 2 score is used when Network tests are enabled and Bayes is disabled. Field 3 is used with Network tests are disabled and Bayes is enabled. Field 4 is used when Network test and Bayes are both enabled (default setting). When a score value is only present in Field 1, that score will be used in all situations.

Current Scores:

The current scoring applied for messages matching this heuristic rule. See Default Scores for a description of the 4 scoring fields.

Description:

An optional description to accompany changes to the default scoring of the heuristic rule. This is an optional field.

Custom Spam Rules**Whitelist From:**

Whitelist From allows you to specify certain senders or domains that you never want to tag as spam. The wildcard character * (asterisk) is supported for wildcard matching (ie *@domain.com matches anyuser@domain.com).

Whitelist To:

Whitelist To allows you to specify certain recipients or domains that you never want to tag as spam. The wildcard character * (asterisk) is supported for wildcard matching (ie *@domain.com matches anyuser@domain.com).

Blacklist From:

The Global Blacklist From allows you to specify certain SENDERS or SENDER DOMAINS that you always want to tag as spam. The wildcard character * (asterisk) is supported for wildcard matching (ie *@domain.com matches anyuser@domain.com). For administrators, there is SMTP Envelope Rules to prevent senders or domains at the SMTP level without the additional overhead.

Blacklist To:

Blacklist To allows you to specify certain recipients or domains that you always want to tag as spam. The wildcard character * (asterisk) is supported for wildcard matching (ie *@domain.com matches anyuser@domain.com). For administrators, there is SMTP Envelope Rules to prevent recipients or domains at the SMTP level without the additional overhead.

All Spam To:

All Spam To works the same as Whitelist To and More Spam To, but the score assigned to ALL_SPAM_TO will be applied to matches. See Customize Heuristic Scoring to alter the value applied to the ALL_SPAM_TO rule.

More Spam To:

More Spam To works the same as Whitelist To and All Spam To, but the score assigned to MORE_SPAM_TO will be applied to matches. See Customize Heuristic Scoring to alter the value applied to the MORE_SPAM_TO rule.

Advanced Spam Preferences**Description:**

Advanced Spam Preferences are only configurable in a global fashion.

Auto Learn Non-Spam Threshold:

The level in which all email scoring under this will be learned as ham.

Auto Learn Spam Threshold:

The level in which all email scoring over this will be learned as spam.

Minimum Non-Spam Learned before Classification:

How many messages must be auto-learned as Ham before Bayes will begin to classify email.

Minimum Spam Learned before Classification:

How many messages must be auto-learned as Spam before Bayes will begin to classify email.

Razor Timeout:

Network Timeout for Razor checking

Pyzor Timeout:

Network Timeout for Pyzor checking

DCC Timeout:

Network Timeout for DCC checking

RBL Timeout:

Network Timeout for RBL checking

Database Settings for spamd**Description:**

Database Settings for the Spam Engine tell where it should pull per-domain and per-user preferences from.

Database Type:

mysql, postgres, oracle, etc. Any db type that is supported by DBI. Note, you may need to have additional DBD drivers installed!

Database Host:

Hostname or IP address where database is located

Database Port:

Port number where database is listening for requests

Database Username:

Username to attach to database with.

Database Password:

Password to authenticate with.

Database Name:

Name of database to use.

Custom Query:

Select statement for pulling user prefs.

Manual Spam Engine/Rules Update**Description:**

Spam Engine and Rules are automatically ran via crontab daily. If you need to force an update, you can use this feature.

Firewall Access:

Update attempts connect on outbound port 80/tcp (HTTP) for configuration information, and pull down system files via port 21/tcp (FTP).

Disabling Auto Updates:

To disable automatic spam updates, see SYSTEM->System Preferences

Restart Spam Daemon**Description:**

Restarting the Spam Daemon will take the service down and bring it back up. While it is restarting, any mail you received into the queue will not be scanned for spam content.

Policy Section**Default Policy Settings****Policy Checking:**

Enables or Disables policy checking. Available to postmasters and users depending on the settings under Policy Control for Postmasters/Users.

Apply Policies on Zip Contents:

Whether or not to scan inside of compressed files for policy violations.

Notifications From Address:

What email address policy notification messages appear to come from.

Notifications From Name:

Who policy notification messages appear to come from.

Custom Notification Message:

The default message to include in all policy notification messages.

Policy Admin Email:

Policy Admin email determines who gets notified when Notification settings include 'Policy Admin'.

Default Policy Notifications Settings:

Default Notification settings define who gets alerted on policy violation detections.

Policy Handling:

Default setting to reject, quarantine or delete policy violations.

Default Quarantine Email Address:

Email Address to send policies violations to.

Allow Postmasters to create 'Accept' Policies:

domain accept policies override global policies. admin users can create 'accept' policies by domain without giving the control to the postmaster for that domain.

Allow Postmasters to turn off Policy Checking:

By enabling this, Domain Postmasters have the ability to turn off Policy checking for their entire domain.

Allow Users to create 'Accept' Policies:

user accept policies override all other policies. admin users, or postmasters for that users domain, can create 'accept' policies by user without giving the control to the user.

Allow Users to turn off Policy Checking:

By enabling this, Users have the ability to turn off Policy checking for themselves.

Queue Level Policies**Email Header Policies:**

Header policies define specific headers and what values to match for possible violations. Common headers used are 'Subject' and 'ALL' to match any header. Each header policy has the ability to override the notification settings, message handling, quarantine address, and policy description. Headers that exist multiple times will be appended (ie Received: headers) so you can match on any of them by using 'Received'.

Email Body Policies:

Body Policies defined specific words or phrases to match for possible violations. Each body policy has the ability to override the notification settings, message handling, quarantine address, and policy description. Body policies will only apply to the first 256kb of data in the body.

File Attachment Policies:

File Attachment Policies defined specific files or extensions (use ends with matching) to match for possible violations.

Each file policy has the ability to override the notification settings, message handling, quarantine address, and policy description. File policies also have the ability to restrict a certain file or extension based on file size.

Add Policy Rule

Policy Status:

Whether to enable or disable this policy.

Policy Name:

32-bytes max. The name of this policy will be selected in notifications, policy logs, and reports, so make it as accurate as possible for the content you are blocking.

Policy Description:

Setting this will override the default notification message.

Policy Type:

Options are Header, Body, or File

Policy Match Type:

Match types are Equals, Contains, Contains (safe), Starts with, Ends with or full regex. For full regex matches, the regex value is in the format /matchthis/ - Case insensitive full regexs use the 'i' flag, /matchthis/i - For more information on writing regular expressions, see <http://www.regular-expressions.info/>. Contains (safe) match types will match words or phrases by placing boundaries around them. So if you want to block the word 'sex' but not 'sexy', a Contains (safe) match will accomplish that. If you want to match the word 'sex' or 'sexy', a simple Contains match will work.

Email Header:

Email header that you want to match. Use 'ALL' to match any header.

Words/Phrases or Regex:

Each policy can now support multiple words or phrases. Each word or phrase should be placed on its own line within the textarea field. The Policy Match Type applies to all words and phrases within that policy. So if you create a Match Type of Contains (safe) and you have a wordlist containing the words 'dog' and 'cat', any email with the word dog or cat in it would be hit. If you use the phrase 'dog and cat', any email containing the phrase 'dog and cat' would hit this policy.

File Names or Regex:

File names or regex that you want to match. The match type determines how filenames are matched. To block file executables, one could write a Match type of 'Ends With' and a list of file extensions such as '.exe', '.bat', '.com', etc.

File Size Limit:

Whether or not to apply file size limitations on the file policy.

Case-Insensitive Match:

Whether or not to perform case-sensitive matches. This Does not apply to match type full regex, use the 'i' operator for case-insensitive regex matches.

Effected Scope:

Global, Domain, or User. See below.

Effected Username/Domain:

If Scope is not global, a Domain name or an email address can be specified here to only apply this policy to a certain domain or individual email address.

Notification Settings:

Who should be alerted when this policy matches.

Message Handling:

How this policy rule should be handled. Options are delete, reject, quarantine, copy to and deliver, and copy to and delete, copy to and delivery, and copy to and delete.. which will all override the default setting. The copy to and deliver method is to be used strictly for IMAP4 copies, and expects a quarantine address/location value of imap://user:pass@ip:folder.

Quarantine Address/Location:

When a message hits a policy where the message handling is set to quarantine, you have the option to quarantine to an email address, or a quarantine location. Currently, IMAP4 is the only supported quarantine location, and must be specified in the format imap://user:pass@ip:folder. So, to copy to a public folder on exchange, a setting like imap://aduser:adpass@adserver:Public Folders/Quarantined Items would work great, assuming there is a public folder called 'Quarantined Items'. Spaces are allowed.

Quarantine Address:

Only valid if message handling is set to 'quarantine', you can use this field to override the default quarantine address.

Opt-Out From List:

The Opt-out list checks the Remote IP, the mail from envelope, and the From email header for exceptions. Multiple values should be separated by newlines, space, or commas. Simple Wildcards (*) are accepted, as well as fixed space wildcards (see below).

Opt-Out To List:

The Opt-out list checks rcpt to envelope header as well as the To email header for exceptions. Multiple values should be separated by newlines, space, or commas. Simple Wildcards (*) are accepted, as well as fixed space wildcards (see below).

Fixed Space Wildcards:

A fixed space wildcard allows you to define how close words should be to trigger a match. 'meet {4} doe' would match the phrases 'meet john doe' and 'meet jane doe' but not 'meet thomas doe'. 'meet {4,6} doe' would match meet john, jane, and thomas doe because the second word can be 4 to 6 characters long. {4} and {4,} are considered equal.

Virus Section

General Virus Configuration

Virus Protection:

Enables or Disables virus protection.

Admin Email:

Alerts are sent to the administrative contact address specified here.

Virus Notifications Email/Name:

Name: Your companies Virus Admin contact.

Email: Your companies Virus Admin email.

When alerts are sent out to the sender of the virus, and the administrative contact, the Alerts From settings will be who the alert appears to be from.

Custom Virus Notification Message:

Custom Message that is added to all Virus Notifications.

Redundant Scanning:

When On (default), the scanner will unpack the email before the virus scan is ran, and it will leave the original copy of the message for the Virus scanner to unpack as well. When Off, the original copy of the message is not made available.

Unzip Attachments:

Whether or not to scan inside of ZIP files. If Unzip Attachments is Off there, Scanning for Policies inside of zip files will not be possible either.

Message Handling:

Whether to reject (SMTP Error Code), quarantine (to Virus Quarantine Address), or delete. If you want sender notifications on virus detections, you should use Message Handling 'reject' and not 'Sender' in Virus Notification. That way, the sender server delivers a Mailer-Daemon to a legit sender that is infected. Virus worms do not send Non-Deliverables when they encounter a 550 smtp error code.

Quarantine Address/Location:

When a message a virus and the message handling is set to quarantine, you have the option to quarantine to an email address, or a quarantine location. Currently, IMAP4 is the only supported quarantine location, and must be specified in the format imap://user:pass@ip:folder. So, to copy to a public folder on exchange, a setting like imap://aduser:adpass@adserver:Public Folders/Quarantined Items would work great, assuming there is a public folder called 'Quarantined Items'. Spaces are allowed.

Install EXTRA.DAT file

EXTRA.DAT:

This file contains virus definitions that allow you to stop newly discovered viruses before new definitions make it into the standard release. See <http://www.avertlabs.com> for information on obtaining an EXTRA.DAT file for a specific virus.

Anti-Virus Information

Virus Engine:

The name of the virus engine being used.

Engine Version:

The version of the engine above.

Definitions:

What virus definitions are currently installed for that particular engine. Status of definitions will be displayed to the right.

Manually Check for Update:

This will force a check for new definitions.

Configure Scanner Specific Settings:

This section will allow you to set auto-update intervals, timeouts, paths to binaries, and other scanner specific configuration items.

Manual Virus Definition Update

Manual Updates:

If the date shown on your virus definitions are out of date, you can try to perform a manual update. The manually update will give you a step by step report as it updates. If your updates are failing, this should tell you why. Outbound destination port 21/tcp must be open for virus definition updates.

SMTP Section

SMTP General Settings

SMTP Hostname:

The SMTP Hostname is the name that your mail server will HELO as to remote clients and mail servers. This should be the Full Qualified Domain Name that you list in your public DNS for your MX record (ie.. mail.yourdomain.com). If your MX record is simply yourdomain.com, create a new A record, and change your MX accordingly, as setting your SMTP Hostname to just your domain name may cause SMTP routing to fail as it will be considered a local delivery.

Reverse Lookups:

Enabling reverse lookups will allow DoubleCheck to record the TCPREMOTEHOST information from the client. DoubleCheck can then log it accordingly, and you will have the ability to create BadHost Rules, or Host Access Rules based on the hostname and not just the IP Address. When Reverse Lookup is enabled, and a host fails to Reverse properly, it will be recorded as 'unknown'. Therefore, to block any clients without reverse DNS, a BadHost rule for 'unknown' could be added. With Reverse Lookups turned off, all TCPREMOTEHOST information will be recorded as 'unknown'.

Received Header:

This option allows you to enable or disable adding received headers containing information of the sender. It is recommended to leave this enabled, and disable it per Host Access Rule as needed. If DoubleCheck is solely being used as a Smart Host, a Outbound Mail Gateway, or an Authenticated MX Relay, then disabling Received Headers globally here is okay. Disabling Received Headers prevents information leakage of IP addresses and Computer names of clients that may be sending email through the system.

Queue Lifetime:

Queue lifetime determines how long the system will hold a deferred message. You can force a delivery attempt on the entire queue by using Reschedule Queue for Delivery in Control Service Daemons.

Message Size Limit:

The maximum size of a message that can be delivered through DoubleCheck. This is NOT the maximal file attachment size. If you set this to 20MB, and someone sends 20 MB file attachments, the message would bounce back to them. Targeted towards ISPs that restrict overall message size limit.

NULL Sender Checks:

Takes one of three different values. Disabled means no NULL Sender prevention. Block Null Senders with Multi-Recips will only reject when a null sender issues multiple rcpt to's per SMTP Session. Block All NULL Senders will prevent anything coming in that does not have a specific email address in the mail from. By Blocking All NULL Senders, you will effectively remove all Mail-Daemons for bounces/NDAs, you will no longer receive vacation notices, and most like a number of other automated things. This can also be set per-host access rule.

MIME Signature Rules Check:

Globally Enables or Disables MIME Signature checks. The MIME Signatures are signatures that you specify based on the first 9-characters of base64 encoded attachment. More information will be available on this feature in the future. This can also be set per-host access rule.

Remote Host Rules Check:

Globally Enables or Disables Host Deny Rules you have defined in SMTP Envelope Rules. This can also be set per-host access rule.

Sender Rules Check:

Globally Enables or Disables Sender Deny rules you have defined in SMTP Envelope Rules. This can also be set per-host access rule.

Recipient Rules Check:

Globally Enables or Disables Recipient Deny rules you have defined in SMTP Envelope Rules. This can also be set per-host access rule.

Sender Domain DNS Check:

Globally Enables or Disables DNS Lookups on the Mail From domain for incoming email. This can also be set per-host access rule.

RBL Check:

Globally Enables or Disables RBLSMTPD Globally. See the RBLSMTPD Section for more information on RBL. This can also be set per-host access rule.

SPF Check:

Globally Enables or Disabled SPF Globally. See the SPF Section for more information on SPF. This can also be set per-host access rule.

Max 1-min Load Avg:

The Max 1 minute load average limit will prevent the system from working itself to death. An average linux load value for a single processor ranges from 0 to 2.0. Values above 2 indicate the system is under heavy load. Once the load surpasses the default value of 3.5, the system will defer incoming SMTP connections. Once loads have settled, SMTP will resume normal operation.

Max Incoming Concurrency:

The Incoming Concurrency is the maximum concurrent SMTP connections the system can handle. 20MB of memory is allocated per incoming connection, so this number should correspond to the amount of RAM in the machine, but not get so high that the CPU cannot process. The incoming connection is where the spam and virus filtering occurs, so it is the most resource intensive of the concurrencies. If an incoming concurrency over 25 is needed, multiple MTAs may be required to handle the load. When the 15 concurrent connections are in use, the 16th connection must wait until the 1st connection has finished. This can result in small delay before being presented with an SMTP banner. Message delivery standards are to wait 60 seconds for a banner before temporary failure occurs.

Max Concurrency by Class C:

See Max Incoming Concurrency for an explanation on how concurrencies work. This limit only operates on a per class C basis, so a single class C cannot take up all of your concurrencies. This value can be set on an individual basis using host access rules.

Max Concurrency by IP:

See Max Incoming Concurrency for an explanation on how concurrencies work. This limit only operates on a per IP basis, so a single host cannot take up all of your concurrencies. This value can be set on an individual basis using Host Access Rules.

Remote Concurrency:

The number of simultaneous remote deliveries allowed. Deliveries to domains listed in Mail Routes are considered Remote deliveries and this setting will impact those domains. On average, this settings is roughly twice of what your

incoming concurrency should be, in order to handle incoming and outgoing mail. Remote concurrencies over 25 may need additional hardware or MTAs to support the load.

Max Recipients per Session:

The Maximum number of RCPT TO: that can be specified in a single SMTP connection. Spam senders like to send to as many recipients as possible via one connection to save time and bandwidth costs on their end. This number is usually best set a half the number of mailboxes on the backend. So if you have 30 employee mailboxes, setting this to 15 would be a recommended starting point.

Max Bad Recipients per Session:

The Maximum number of failed RCPT TO: in a single SMTP connection. RCPT TO: failures can be caused by SMTP Envelope Rules defined for bad recipients, relaying attempts, and/or recipient verification failures. Once this value has been reached, a 557 SMTP error response will be sent back to the client.

Tarpitting:

Tarpitting is the act of slowing down an SMTP session when 'too many' RCPT TO: have been sent. Dictionary attacks are well known for sending many RCPT TO: in a single SMTP session. The tarpit seconds will create a pauses for every RCPT TO: it sees after the tarpit recipient limit has been reached.

Recipient Domains and Mail Routes**DCID:**

Domains are assigned to DCID's for licensing purposes. See System->Manage Licenses for more information on licensing.

Domain / Route:

A recipient domain is a domain in which you accept mail for. Domain names that are handled locally are entered here, and mail is commonly routed to the mail server using Mail Routes. If a mail route is not established, standard MX records are looked up via DNS, and delivery is attempted to the highest preference MX. If MX priority on the backend mail server or cluster is a priority, utilize an internal DNS server that handles the MX queries properly, and ignore the Mail Routing feature. If load balancing between a backend cluster of mail servers is needed, specifying a Mail Route as a hostname that resolves to multiple A records is preferred.

Personalized:

A personalized domain is a domain that allows postmasters and users to define domain-based or individual user settings that are different from the global settings. In order to add postmaster or user accounts at a particular domain, you must personalize the domain within Recipient Domains and Mail Routes.

Add Recipient Domains**DCID:**

Which license to associate the domain to.

Domain Name:

The domain name you want to accept email for (ie example.com).

Create Mail Route:

Whether or not this domain should be statically assigned a mail route. If set to No, MX records for this domain will be looked up and delivery will be attempted to the highest preference MX record.

Mail Server IP/Hostname:

The IP Address or Hostname of the Mail Server that handles mailboxes for this domain.

Enable Personalized Settings:

Allows Postmasters and Users to be added to this domain name so they can define per-domain or per-user settings.

Recipient Verification Settings**Configuration Scope:**

Recipient Verification Settings can be configured globally for all domains, as well as for individual personalized domains. For global domains (non-personalized), they will use the global verification settings.

Default Domain Name:

The Default domain name is used when the rcpt to is a username only.

Recipient Verification Method:

The Recipient Verification Method determines how the verification of the recipient is accomplished. The current methods available for recipient verification are SMTP Callout, Exchange/Active Directory, DoubleCheck, Amail, and Vpopmail.

SMTP - Recipient Callout:

Recipient Callout is compatible with nearly all mail server backends, as it issues the envelope to the backend server to see if the recipient exists or not. For this to function properly, your mail server must issue a 55x SMTP error response when an invalid rcpt to is issued in the SMTP envelope. Exchange 2003, by default, does not do this, so it may be necessary to alter the configuration for your mail server.

LDAP - Active Directory/Exchange:

Recipient Verification with Active Directory is accomplished via LDAP calls. The LDAP Server that you use to verify the recipients should be your active directory server. Usually all that is required is to edit the LDAP DN User and DN Password for a user that has browse access to the full tree. This doesnt necessarily need to be the administrator.

SQL - Amail:

Amail is a webmail server for unix/linux that has a backend MySQL server that contains information about the users on the system. This module will allow you to verify recipients in that backend atmail database.

SQL - Vpopmail:

Vpopmail is a virtual mail server for unix/linux that hosts multiple domains on a single mail system. The backend for vpopmail is normally a MySQL database, and this module will allow you to verify recipients against that server.

SQL - Doublecheck:

DoubleCheck Recipient Verification would require you to add all your users with DoubleCheck under SYSTEM->User Manager. SMTP Callout is recommended over DoubleCheck Recipient Verification to avoid having to manage user information in multiple locations.

SMTP Authentication Settings**Configuration Scope:**

SMTP Authentication Settings can be configured globally for all domains, as well as for individual personalized domains. For global domains (non-personalized), they will use the global verification settings. For personalized domains, SMTP Authentication attempts must include the domain name in the username, otherwise there is no way to designate the difference as SMTP Auth happens before MAIL FROM or RCPT TO is issued.

Default Domain Name:

The Default domain name is used when authenticating with usernames only. This only applies to the global scope.

Authentication Method:

The Authentication Method determines how to authenticate the username and password. The current methods available are Exchange/Active Directory, DoubleCheck, Atmail, and Vpopmail.

LDAP - Active Directory/Exchange:

Authentication against Active Directory is accomplished via LDAP calls. The LDAP Server that you use to verify the recipients should be your active directory server.

SQL - Atmail:

Atmail is a webmail server for unix/linux that has a backend MySQL server that contains information about the users on the system. This module will allow you to authenticate against that backend atmail database.

SQL - Vpopmail:

Vpopmail is a virtual mail server for unix/linux that hosts multiple domains on a single mail system. The backend for vpopmail is normally a MySQL database, and this module will allow you to authenticate against that backend vpopmail database..

SQL - Doublecheck:

DoubleCheck authentication allows you to authenticate as users added under the SYSTEM->User Manager.

SMTP Envelope Rules**Remote Host Rules:**

A Remote Host rule can be an IP Address or Hostname pattern. In order to use the reversed IP information to match hostnames, you must enable Reverse Lookups in SMTP -> General Settings. Example Remote Host rules are Deny 192.168.1.* and Deny *.spamdomain.com. Allow Host Rules give you the ability to override a Deny. For example, you Deny 192.168.1.*, but you want to Allow 192.168.1.3. For these rules to run, you must have Host Rule Checking enabled, either via a Host Access Rule that the connection is coming in on, or globally via SMTP -> General Settings.

Sender Rules:

Sender Rules allow you to drop connections at the SMTP side based on the mail from: envelope header. Sender Rules support full wildmat wildcard syntax. This include * (asterisk) for zero or many matching, ? for single char matching, and [] for range matching. See the wildmat documentation for more information, or consult your DoubleCheck User Guide. Allow Sender Rules give you the ability to override a Deny. For example, you deny *@spamdomain.com, but you want to allow user@spamdomain.com. For these rules to run, you must have Sender Rule Checking enabled, either via a Host Access Rule that the connection is coming in on, or globally via SMTP -> General Settings.

Recipient Rules:

Recipient Rules allow you to drop connections at the SMTP side based on the rcpt to: envelope header. Recipient Rules support full wildmat wildcard syntax. This include * (asterisk) for zero or many matching, ? for single char matching, and [] for range matching. See the wildmat documentation for more information, or consult your DoubleCheck User Guide. Allow Recipient Rules give you the ability to override a Deny. For example, you deny all email addresses at *@yourdomain.com, but you want to create an allowed list of emails.. user1@domain.com, user2@domain.com, etc. For these rules to run, you must have Recipient Rule Checking enabled, either via a Host Access Rule that the connection is coming in on, or globally via SMTP -> General Settings.

HELO Rules:

A HELO rule is a string to match the HELO/EHLO of the SMTP Session. A good practice here is do Deny the IP Address that your MX record resolves to in the HELO, as many spam clients will send HELO . Allow HELO Rules give you the ability to override a Deny. For example, you Deny *mail.com, but you want to Allow hotmail.com. For these rules to run, you must have HELO Rule Checking enabled, either via a Host Access Rule that the connection is coming in on, or globally via SMTP -> General Settings.

Skip DNS Lookup:

Skip DNS lookups allow you to specify a domain name that should not have DNS lookups ran on it during the Mail From Domain Exists phase of the SMTP Connection. For these rules to run, you must have DNS Rule Checking enabled, either via a Host Access Rule that the connection is coming in on, or globally via SMTP -> General Settings. If you do not want to do any DNS checking on mail from domain, that can be disabled via SMTP -> General Settings, then you would not need any Skip DNS rules.

Reject MIME Signature:

MIME Signatures are the first 9-characters of the base64 encoded file attachment. For these rules to run, you must have MIME Signature Rule Checking enabled, either via a Host Access Rule that the connection is coming in on, or globally via SMTP -> General Settings.

SPF (Sender Policy Framework) Settings**SPF Checking:**

Defines which level of SPF Checking you would like to apply. 0=disabled, 1 and 2=add headers, 3 and above will actually cause an SMTP Deny (Error Code 558) depending on the SPF result. The default setting is Level 3 and will only reject connections that fail the SPF query.

SPF Guess:

When incoming mail from a domain that does not publish an SPF zone, this string will be used to perform a 'spf guess'. The result of an SPF guess will never be Fail.

Local SPF Rules:

Local SPF rules allow you to define mechanisms prior to running the SPF queries. Adding trusted upstream MX record sources or known locations to result in SPF pass are common uses. See <http://spf.pobox.com/mechanisms.html> for mechanisms that can be used.

RBLSMTPD Settings**Use RBLSMTPD:**

RBLSMTPD is enabled by default. This allows Real-time Black Hole list checking at the SMTP Level. This differs from Queue Level RBL Checking found in Global Spam Preferences in that SMTP Level RBL checks only have access to the incoming Remote IP address. Using Queue level RBL checking will only add to the overall spam score of the message, but it will allow you to look at all the Received headers and match multi-hops against RBLs. If you have a Proxy or Firewall that hides the true source address from the outside, RBLSMTPD will have no effect and can be shut off. However, we highly recommend configuring your system to allow it access to the true remote IP, as RBL can stop 30-70% of unnecessary email traffic.

Log Denies to MySQL:

Whether or not to log RBL matches denied at the SMTP level to the SMTP Deny MySQL log. You may run a Database Search using the SMTP Deny as the search table to view this log, or run a Monitoring -> SMTP Report to get overall statistics.

Remote Timeout:

After an RBL match has been made, the SMTP server must connect back to the remote senders SMTP server and send a 451/559 error code. This timeout specifies how long it should take before it gives up.

RBL Servers**Order:**

Connections are checked against the RBL Servers in a specific order. You can move the RBL Servers up or down into the order you would like them to be checked. You can choose to disable a specific RBL by going to EDIT and updating it to disabled mode. RBL's that are in disabled mode will not be checked, regardless of the order they are in. You also have the options to Add or Delete any RBL servers you would like to have on the list.

Status:

The Status of the RBL Server tells you whether the connection will be checked against this specific server. You can disable an RBL by going to EDIT and updating it's preferences.

RBL Server:

The RBL Server is the hostname or IP address of the DNS Blacklist providing reverse ip lookup to determine if the connecting IP address is on their black list.

RBL Type:

The type can either be an RBL Source (standard) or an Anti-RBL Source. RBL Sources returns true if the IP is blacklisted, Anti-RBL Sources return true if the connecting IP is not blacklisted. Currently, RBL Sources that support A records instead of TXT records are not supported.

Connection Handling:

When a connecting IP address matches a blacklist, the mail is either deferred with a 451 Temporary Failure message, or bounced with a 559 You are listed on a RBL message. Temporary Failures will cause the offending server to retry at various times until the queuelifetime has expired on that message. This allows administrators to get their mail server unlisted, and not force all emails to be resent.

Fail Mode:

A fail mode of Fail Open allows connections as unlisted when an RBL cannot be reached. Fail Closed will assume they are listed if the RBL cannot be reached. The default is Fail Open and there should be a very good reason not to keep it this way.

Host Access Rules**Host Access Rules:**

Host Access Rules allow you to specify per-connection settings. You can prevent an IP or subnet from connecting the SMTP service, shut off RBL or Spam checking, set a max message size limit and more. Rules are checked from top to bottom. The first rule that matches is the rule that is used.

IP Address, Subnet, Range, or Host:

This field can take an IP Address, a partial address "always" ending in a period, a last segment IP Range, or a hostname. To block an entire Class A, you would enter the first IP segment followed by a period (10.). To block an entire Class B, you would enter the first two IP segments followed by a period (10.1.). To block an entire class C, you would enter the first three IP segments followed by a period (10.1.2.). To block a Class A, B, or C Range, you would use the following formats. 10-12. blocks 10., 11., and 12. Class A's. 10.1-3. blocks 10.1., 10.2., and 10.3. Class B's. 10.1.2-4. blocks 10.1.2., 10.1.3. and 10.1.4. Class C's. 10.1.2.3-5 blocks 10.1.2.3, 10.1.2.4, and 10.1.2.5 IP Addresses. Hostname blocking relies on reverse DNS to be enabled in SMTP->General Settings. With Reverse DNS turned on, you can block hostnames with Host Access Rules. By entering a hostname of 'hotmail.com', you would block all incoming mail from IP addresses that reverse lookup to 'hotmail.com' exactly. If 'hotmail.com' sends from subdomains like 'mx1.hotmail.com', placing a period in front of the hostname will block anything in that TLD, but not the TLD specifically. .hotmail.com would block mx1.hotmail.com, mx2.hotmail.com, but it would not block hotmail.com specifically. You would need two access rules to the domain name specifically, and all subdomains under it.

Access Rule:

The Access Rule will either "allow" the SMTP connection to take place, or "deny" the connection. Make sure your IP addresses or ranges are correct before you establish a deny, as this can cause Denial of Service if misconfigured.

Relay Client:

If you need to provide outbound SMTP in a relay fashion you may do so by setting this option to "Yes". Do not open relay up to any more IP addresses than you need to, or you stand the chance of getting listed on the Blacklists. Your Internal LAN subnet is usually a good addition to add as a Relay Client.

Email Signature Overrides:

Enabling Email Signatures can be done globally, per-domain, or per-user via the Signature Setup in the SMTP Section. To force a certain access rule to have signatures on or off, you can do that here. A custom signature for this host access rule may also be provided.

RBL Check:

RBL Check can be disabled on a individual basis. This will allow Blacklisted IP Addresses to still send mail to you. By default, RBL is enabled unless turned off in the DEFAULT rule.

DNS Check:

Disabling the DNS will prevent mail from being blocked from senders where the MAIL FROM: envelope header cannot be resolved. This is not a reverse lookup, do not get them confused. If an email was sent with the envelop header MAIL FROM: user@hotmail.ocm, it would be rejected because hotmail.ocm is not a valid domain. Enabled Disabled

SPF Check:

Disabling the SPF will prevent SPF queries from even being ran.

Queue Scan:

Disabling the Queue Scan will prevent the Virus Check, Policy Check, and Spam Check from occurring. Disabling this feature is not recommended! RBL and DNS Checks will still occur as they happen at the SMTP level, and not the queue level.

Spam Check:

By default, the Spam Check is always on even on relay clients. You must set this value to enable or disable spam checking per rule. If Spam Checking is disabled Globally under the Spam section, this will have no effect.

Virus Check:

By default, the Virus Check is always on unless disabled globally or here per Access Rule.

Policy Check:

By default, the Policy Check is always on unless disabled globally or here per Access Rule.

Max Message Size:

Max Message Size allows you to restrict the size of email messages based on the senders IP address. The value is added in bytes, and displayed to you in Megabytes on the View page. Setting this at zero will disable Max Message size and size will be unlimited.

Per-IP Connection Limit:

Prevents IPs within this access rule from using more connections than defined here. If not defined, the global setting found under SMTP -> General Settings will be used. If the access rule is for a specific IP address, The per-ip limit applies solely to that address.

Per-C Connection Limit:

Prevents Class Cs within this access rule from using more connection than defined here. If not defined, the global setting found under SMTP -> General Settings will be used. The access Rules scope must be larger than a single IP address for this setting to be usable.

Max Load Limit:

Prevents mail from hosts within this access rule when the system load is greater than defined here. If not defined, the global setting found under SMTP -> General Settings will be used.

Description:

Provide a reason for adding this rule. Limited to 256 chars.

Signature/Disclaimer Settings**Enable Signatures:**

Turns on or off signatures on outbound mail. Requires at least 1 ACTIVE signature to work.

Signature Method:

Determines which MIME Parts to sign. The default is Text and HTML, however this does require unpacking the message and repackaging it, so this does increase overhead. Signing the text part only is very low overhead as it only has to append to the message. Attaching the signature will create an RFC822 type attachment to the email. This involves unpacking and repacking the message just like signing HTML.

Sign Email Replies:

Enable or Disable signatures on replies. Default is On.

Sign Email Forwards:

Enable or Disable signatures on email forwards. Default is On.

Prevent Multiple Signatures:

Prevents multiple signatures from being added to an email thread when Email Replies are enabled. Default is On.

Line Breaks Before Signature:

The number of line breaks to insert before adding the signature. Applies to both TEXT and HTML. Default is 1.

Text Signature Separator:

The separator used to split the body content from the signature. Default is double-dash, which is read by many mail clients as a signature, and strips the signature when replying. To define a custom separator, use None and add your separator into the text signature.

HTML Signature Separator:

The separator used to split the body content from the HTML signature. Default is a Horizontal Rule. To define a custom

separator, use None and add your separator into your HTML signature.

Add New Signature:

The signature description is a short name used for display purposes only. To make the signature active, set Activate Signature to On and supply a Text Signature. The Text Signature will be automatically converted into HTML for you if you do not specify a HTML signature. To have a different HTML signature than what the Text Signature renders, you need to set Custom HTML Signature to On.

Viewing Signatures:

To view what a signature will look like when emailed, click on the name of the signature under the signature name column. If a custom HTML signature was not provided, the text signature will be rendered to HTML. URLs starting with <http://> will become hyperlinks.

Random Signatures:

To add a random signature you need to have more than 1 active signature. After adding 2 or more signature, make sure the light in the active column is GREEN. You can change an active status by simply clicking on the light!

Signature Scope:

The scope that signatures apply to work top down. If a Global signature is defined and signatures are enabled, all domains and users will inherit that global signature. To override the global signature for a particular domain, you need to either turn off Signatures at the domain level (requires personalization), or you need to add a new signature for that domain. Once you add a new signature, the Global signature will no longer be available to use unless all domain level signatures are deleted. Once you have established a domain level signature, all users under that domain will inherit that signature. To override the domain level signature, a user would need to turn off signatures (requires personalization and user account) or defined their own custom signature. Once a custom signature is defined, the domain level signature is no longer available, unless all personal signatures are deleted.