SpamTitan On-Premise

TitanHQ SpamTitan

ADMINISTRATORS GUIDE v6.10

www.titanhq.com/spamtitan

COPYRIGHT

The product described in this document is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

TitanHQ gives no condition, warranty, expressed or implied about the fitness or quality of this manual or the accompanying product. TitanHQ reserves the right to make changes to this manual or the accompanying product, without notice to any person or company. TitanHQ shall not be liable for any indirect, incidental, special, or consequential damages, loss of profits, loss of goodwill, loss of reputation or economic loss resulting from the use of this manual or the accompanying product whether caused through TitanHQ negligence or otherwise and based on contract, tort, strict liability or otherwise, even if TitanHQ or any of its suppliers has been advised of the possibility of damages.

Printed in Ireland.

Part Number: ST-AG-610

CONTACTING TITANHQ CUSTOMER SUPPORT

Telephone:	+1 201 984-3271
Email:	helpdesk@spamtitan.com
Forum:	http://helpdesk.spamtitan.com/support/home
Web:	www.titanhq.com

TITANHQ WELCOMES YOUR COMMENTS

We want to know about any corrections or clarifications that you would find useful in our documentation, which will help us improve future versions. Include the following information:

- Version of the manual that you are using
- Section and page number
- Your suggestions about the manual

Send your comments and suggestions to us at the following email address: docinfo@titanhq.com

Preface

The SpamTitan Administrator Guide is designed to help mail system administrators in the operation of the SpamTitan. This guide provides an overview of the key product features, along with instructions for setting up, administrating, and monitoring SpamTitan. These instructions are intended for an experienced system administrator with knowledge of networking and email administration.

Table of Contents

1 Introduction 7

2 Setup and Installation 8

2.1 Installation Planning 8

2.2 Preparing for Setup 8

2.3 System Requirements 9

2.4 Installation Instructions 9

2.5 Basic Configuration 9

2.6 The SpamTitan Graphical User Interface (GUI) 9

2.7 Setup 10

2.7.1 Network Configuration 10

2.7.2 Mail Relay Setup 11

2.8 Licensing 12

2.9 System Time 12

3 Network 14

3.1 IP Configuration 14

3.2 DNS Settings 15

3.3 HTTP Proxy 16

3.4 Static Routes 16

3.5 Port Forwarding 17

3.6 Alias IP Addresses 18

3.7 Outbound Delivery Pools 18

3.8 IPv6 19

4 Mail Relay 21

4.1 Domains 21

4.2 IP Controls 24

4.3 Sender Controls 25

4.4 Outbound Settings 26

4.5 General Settings 29

4.6 SMTP Controls 30

4.7 Greylisting 32

4.8 Advanced Routing 33

5 Rate Controls 35

5.1 Rate Control Policies 35

5.2 SMTP Limits 38

6 Managing System Updates 40

7 Shutting Down the Appliance ... 42
8 Clustering ... 43
8.1 Setting up a SpamTitan Cluster ... 43
8.2 Restrictions and Considerations ... 43
9 Content Filtering ... 44
9.1 Virus Filtering ... 44
9.1.1 Clam Anti-Virus ... 44
9.1.2 Kaspersky Anti-Virus ... 44
9.1.3 Enabling Virus Scanning and Configuring Global Settings ... 44
9.1.4 Managing Virus Definition Updates ... 45
9.2 Spam Filtering ... 47
9.2.1 Enabling Spam Scanning and Configuring Global Settings ... 47
9.2.2 Spam Rule Updates ... 48
9.3 Attachment Filtering ... 49
9.3.1 Extension Filters ... 49
9.3.2 File Name Filters ... 50
9.3.3 File Type Filters ... 50
9.3.4 Mime Type Filters ... 51
9.3.5 Compressed Archive File Scanning ... 51
9.3.6 Password Protected Archives ... 51
9.3.7 Configuration ... 52
9.4 Content Filtering ... 53
9.4.1 Predefined Filters ... 55
9.4.2 Using Regular Expressions ... 56
9.4.3 Regular Expression Examples ... 56
10 Anti-Spam Engine - Settings ... 58
10.1 Network Testing ... 58
10.2 Internal Networks ... 58
10.3 Bayesian Database ... 59
10.4 Penpals Soft Whitelisting ... 61
10.5 Optical Character Recognition ... 61
10.6 Botnet Analysis ... 62
10.7 Passive OS Fingerprinting ... 62
10.8 Performance Tuning ... 62
10.9 Language Options ... 63
11 Anti-Spam Engine – Policies ... 64

11.1 Domain Policies ... 64
11.2 User Policies ... 67
11.3 Roles and Permissions ... 68
11.4 Admins ... 69
11.5 Domain Groups ... 70
12 Settings ... 72
12.1 Changing the Password ... 72
12.2 Interface Settings ... 72
12.3 SSL Certificate Management ... 74
12.4 TLS Encryption ... 75
12.5 Access Authentication: Configuring HTTP/HTTPS ... 76
12.6 Access Authentication: Web Access ... 77
12.7 Access Authentication: Web Authentication Settings ... 77
12.8 Backing up and Importing System Configuration ... 82
12.9 Notification Templates ... 83
12.10 Remote Syslog ... 85
12.11 Configuring Outbound Disclaimers ... 86
12.12 SNMP Management ... 87
13 Filter Rules ... 89
13.1 Configuring the Global Email Blacklist ... 89
13.2 Configuring the Global Email Whitelist ... 90
13.3 Pattern Filtering ... 90
14 Quarantine ... 93
14.1 Manage Quarantine ... 93
14.2 Quarantine Reports ... 95
14.3 Quarantine Report Settings ... 96
14.4 Aliases ... 98
15 Reporting ... 100
15.1 System Information ... 100
15.2 Graphs ... 103
15.3 Administration ... 104
15.4 History ... 105
15.5 Reports ... 109
15.6 Today's On-Demand Reports ... 111
15.7 Scheduled Reports ... 112
15.8 Archived Reports ... 113

16 Logging 114
17 Outlook Add-In 116
18 Remote Management 117
19 Firewall Information 118

1 Introduction

This chapter provides an overview of SpamTitan.

SpamTitan is high-performance mail filtering security suite that provides the necessary email infrastructure to meet the needs of the most demanding enterprises. SpamTitan combines a hardened operating system and an assortment of software applications and services to produce a mail firewall appliance that eliminates spam and viruses and enforces corporate email policy.

Anti-Spam defenses on the appliance ensure through a multi-layered approach that over 99% of all spam is detected.

Anti-Virus protection is provided through the use of two industry leading anti-virus scanning engines: Clam AV and Kaspersky anti-virus.

Message filtering capabilities allows you to enforce corporate email policy on inbound and/or outbound messages. Filter rules allow you to block banned attachments or add disclaimers. These rules can be performed on a domain and/or per-user basis to provide fine-grained control.

Mail monitoring features ensures that you have complete visibility of all mail that passes through the appliance with the ability to generate automated reports and/or on demand reports.

2 Setup and Installation

This chapter guides you through the process of configuring SpamTitan for email delivery. When you have completed this chapter, SpamTitan will be able to send and receive SMTP email over the Internet and within your network.

2.1 Installation Planning

SpamTitan will normally be installed on a server in your network between your firewall and mail server(s). This requires a rule change to your firewall to direct incoming email on Port 25 (SMTP) to the IP address of the SpamTitan server. If you are assigning a new MX record for the SpamTitan server while maintaining your existing MX records, you should be aware that spammers will target secondary or lower priority MX records. The latter is based on the assumption that secondary MX records will not be protected by spam filters. In this case any secondary MX record should be a backup mail server which will queue mail if the primary MX record is unavailable.

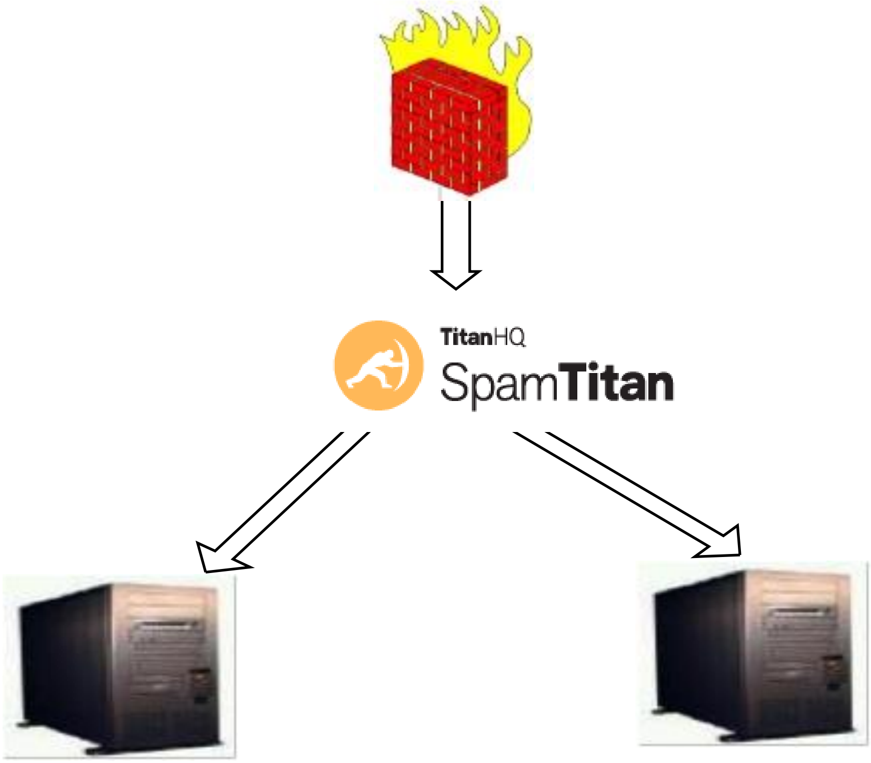


Figure 2-1 Typical Deployment

2.2 Preparing for Setup

To successfully setup SpamTitan in you environment, you must gather important network information from your network administrator about how you would like to connect SpamTitan to your network. SpamTitan is configured via a web interface.

The initial setup required for installing the SpamTitan appliance is performed through a console based-installation menu. The final configuration may be performed from your desktop through the web-based administrative interface.

2.3 System Requirements

The *minimum* hardware requirements for installing and using SpamTitan are as follows:

<500 users	<1000 users	<5000 users	>5000 users
Intel Pentium® 4 Processor with 2.5GHz (or equivalent)	Intel Xeon® Processor with 2.5GHz (or equivalent)	Intel Xeon® Dual Core Processor with 3GHz (or equivalent)	Please contact support.
1GB RAM	2GB RAM	4GB RAM	
40GB hard disk	40GB hard disk	40GB hard disk	
One or more PCI Ethernet network interface card	One or more PCI Ethernet network interface card	One or more PCI Ethernet network interface card	

Table 2-1 Minimum System Requirements

2.4 Installation Instructions

SpamTitan may be installed on *bare-metal* or as a VM appliance using the ISO, OVA or IMG files which are available for download. See the *SpamTitan Quick Start guide* and/or the Video guides on the SpamTitan solutions knowledgebase - https://helpdesk.spamtitan.com/support/solutions for more details on the initial installation process.

2.5 Basic Configuration

After deploying the SpamTitan software as either a VM or on bare metal, then the second step of the installation is performed through the web-based administrative interface of SpamTitan.

Connect a laptop or any computer with a web browser to the SpamTitan server via a cross over network cable. If your SpamTitan server has already been pre-configured for your environment you can the plug it directly into your network. To access the web interface type in the following URL to your browser:

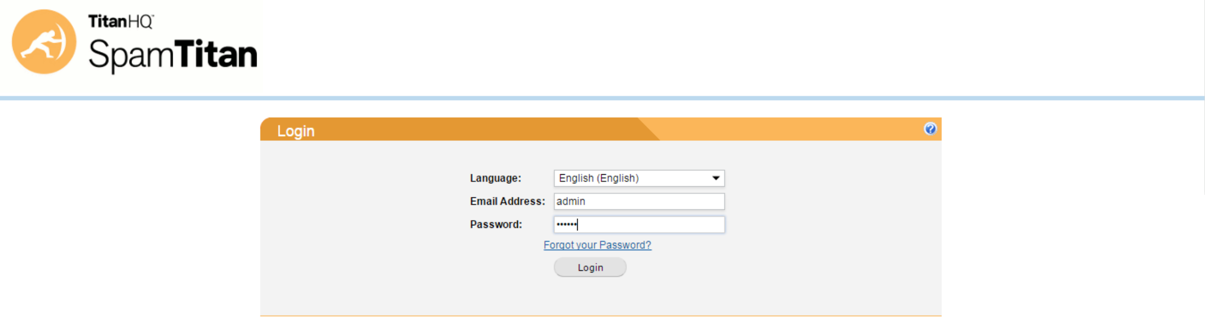
http://192.168.168.2/ or http://<preconfigured IPAddress>.

2.6 The SpamTitan Graphical User Interface (GUI)

The graphical user interface (GUI) enables you to manage and monitor the system using a web-based interface. Each page is laid out in an intuitive and consistent manner and includes numerous charts and tables detailing the current status of the system. The GUI can also be used to view real-time information on all mail flow history. Administrators can instantly report on any email users (local/remote) mail flow history and view mail statistics.

Note: To access the GUI, your browser must support and be enabled to accept JavaScript and cookies, and it must be able to render HTML pages using Cascading Style Sheets (CSS).

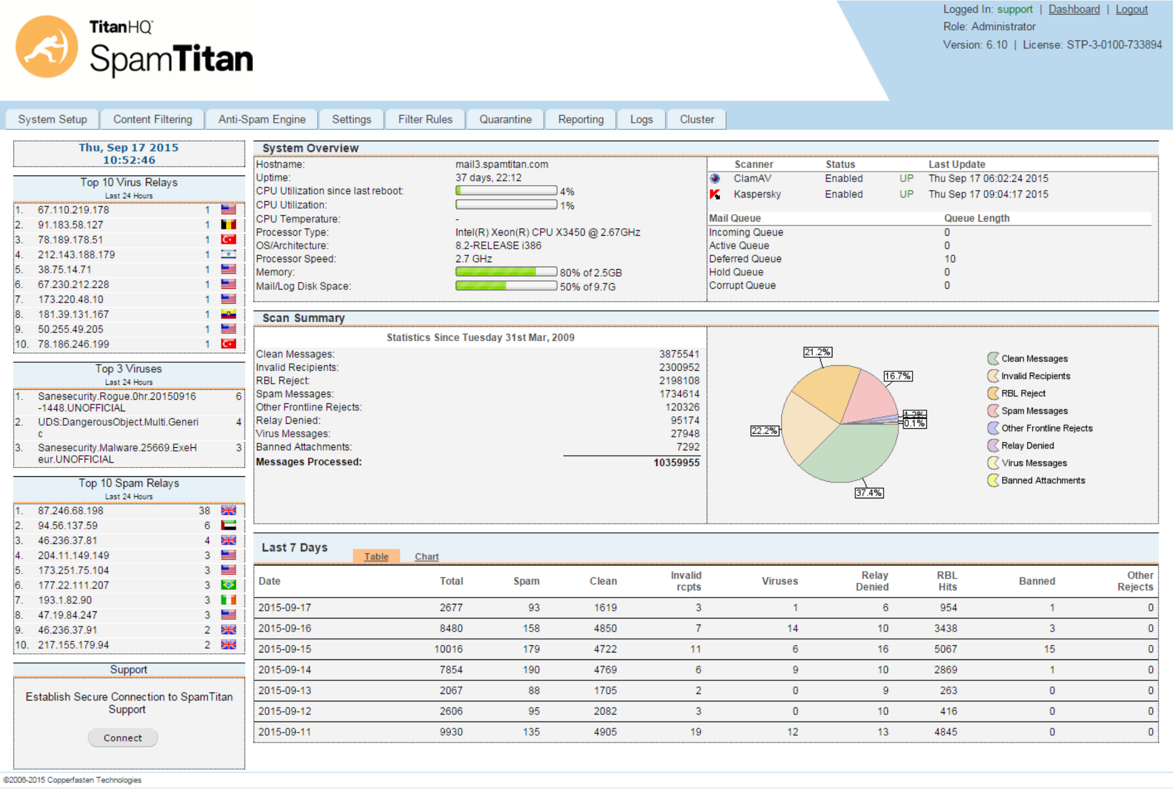
You can view the GUI by entering the IP address or hostname of the appliance as a URL. All users accessing the GUI must log in. Type your username and password, and then click Login to access the GUI. You can login with the **admin** account with password **hiadmin**. Make sure you change the admin password after logging in.



Language: English (English)
Email Address: admin
Password: ••••••
Forgot your Password?

Figure 2-2 Login Screen

After successfully logging in as the administrator, you are presented with the system dashboard. The dashboard provides an overview of the SpamTitan system at a glance.



Logged In: support | Dashboard | Logout
Role: Administrator
Version: 6.10 | License: STP-3-0100-733894

Thu, Sep 17 2015
10:52:46

Top 10 Virus Relays
Last 24 Hours

1.	67.110.219.178	1
2.	91.183.58.127	1
3.	78.189.178.51	1
4.	212.143.188.179	1
5.	38.75.14.71	1
6.	67.230.212.228	1
7.	173.220.48.10	1
8.	181.39.131.167	1
9.	50.255.49.205	1
10.	78.186.246.199	1

Top 3 Viruses
Last 24 Hours

1.	Sanesecurity.Rogue.0hr.20150916-1448.UNOFFICIAL	6
2.	UDS:DangerousObject.Multi.Generic	4
3.	Sanesecurity.Malware.25669.ExeHeur.UNOFFICIAL	3

Top 10 Spam Relays
Last 24 Hours

1.	87.246.68.198	38
2.	94.56.137.59	6
3.	46.236.37.81	4
4.	204.11.149.149	3
5.	173.251.75.104	3
6.	177.22.111.207	3
7.	193.1.82.90	3
8.	47.19.84.247	3
9.	46.236.37.91	2
10.	217.155.179.94	2

Support

Establish Secure Connection to SpamTitan Support

System Overview

Hostname:	mail3.spamtitan.com
Uptime:	37 days, 22:12
CPU Utilization since last reboot:	4%
CPU Utilization:	1%
CPU Temperature:	-
Processor Type:	Intel(R) Xeon(R) CPU X3450 @ 2.67GHz
OS/Architecture:	8.2-RELEASE i386
Processor Speed:	2.7 GHz
Memory:	80% of 2.5GB
Mail/Log Disk Space:	50% of 9.7G

Scanner	Status		Last Update
ClamAV	Enabled	UP	Thu Sep 17 06:02:24 2015
Kaspersky	Enabled	UP	Thu Sep 17 09:04:17 2015

Mail Queue	Queue Length
Incoming Queue	0
Active Queue	0
Deferred Queue	10
Hold Queue	0
Corrupt Queue	0

Scan Summary

Statistics Since Tuesday 31st Mar, 2009

Clean Messages:	3875541
Invalid Recipients:	2300952
RBL Reject:	2198108
Spam Messages:	1734614
Other Frontline Rejects:	120326
Relay Denied:	95174
Virus Messages:	27948
Banned Attachments:	7292
Messages Processed:	**10359955**

Last 7 Days

Date	Total	Spam	Clean	Invalid rcpts	Viruses	Relay Denied	RBL Hits	Banned	Other Rejects
2015-09-17	2677	93	1619	3	1	6	954	1	0
2015-09-16	8480	158	4850	7	14	10	3438	3	0
2015-09-15	10016	179	4722	11	6	16	5067	15	0
2015-09-14	7854	190	4769	6	9	10	2869	1	0
2015-09-13	2067	88	1705	2	0	9	263	0	0
2015-09-12	2606	95	2082	3	0	10	416	0	0
2015-09-11	9930	135	4905	19	12	13	4845	0	0

©2006-2015 Copperfasten Technologies

Figure 2-3 Dashboard

2.7 Setup

After connection and gaining access to the web interface, the rest of the configuration is performed using the web interface.

2.7.1 Network Configuration

1. Log in to the SpamTitan web interface using **admin** for the username and **hiadmin** for the password as described above. Select **System Setup > Network** to configure the **IP address** and **Default Route** to be assigned to the SpamTitan server including the Subnet Mask. See ‘Network Configuration’ for more information on configuring the system IP address.

2. **Note**: When you change the IP address you must reset the browser URL to the new IP address to continue with the configuration.

3. From the **System Setup > Network** page you can also set your Domain Name Server (DNS) settings for the network the appliance will be installed on. If you have secondary DNS servers add their IP address here. See "DNS Settings" on page 16 for more information on configuring DNS.

2.7.2 Mail Relay Setup

1. Select **System Setup** > **Mail Relay** and in the **General Settings** section enter:

   - Enter the Appliance hostname as a FQDN (fully qualified domain name)
   - If your mail server has a size limit on incoming email then select it via the "Max message size:" drop down menu
   - Press the "Save" button

2. Select **System Setup > Mail Relay** and in the **Domains** section enter the details for each domain that you manage:

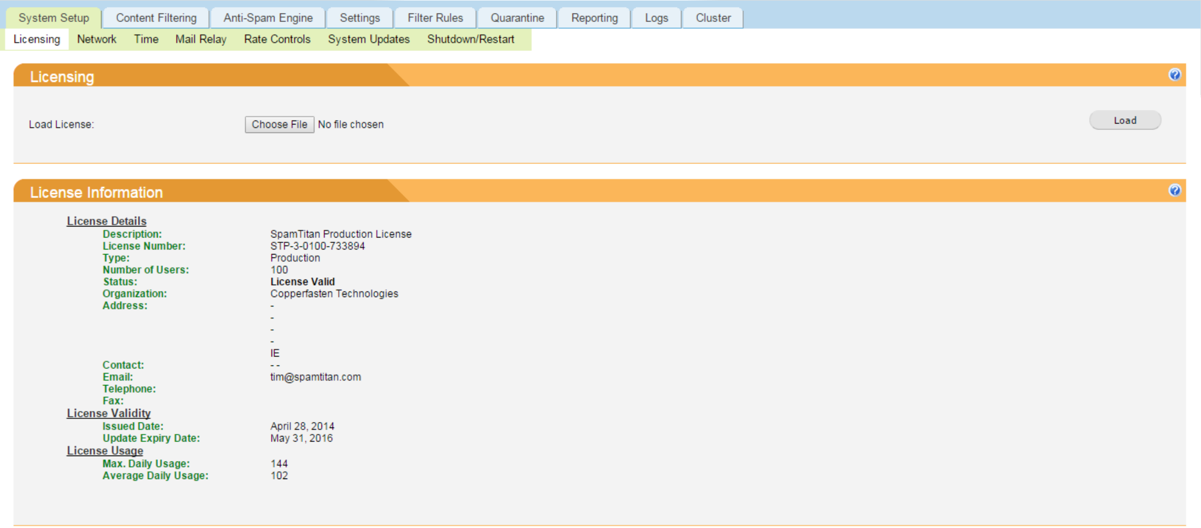
   - **Domain** as mydomain.com for example
   - The **FQDN** or **IP address** of your email sever for this domain
   - The **Destination port** for email defaults to 25
   - Press the **Add...** button
   - Repeat for all other domains you serve
   - All the domains you have added will appear in a list you can now test the email function by clicking the **Test** column

3. If **Recipient Verification** is supported by your mail server make sure it's set to **Dynamic Recipient Verification.** Microsoft Exchange 2003 and most email servers now support this feature. When enabled the appliance will check the address of incoming email with the mail server; if the intended recipient is unknown then the email is rejected with a DSN (Delivery Status Notification) message and no further processing is performed. If your mail server doesn't support Recipient Verification you can set this field to:

   - No Recipient Verification
   - LDAP Recipient Verification if you are running Active Directory
   - Specify Allowed Recipients. You can then enter a list of valid email address manually or import a list from a text file with one email address per line.

See **Mail Relay: Domains** for more information on managing domains and the recipient verification options. You have now completed the mandatory configuration steps that are required in order to receive mail for you organization. There are other settings that you may wish to change. Please review the default settings in each menu section. For an explanation of any setting press the help icon.

2.8 Licensing



Licensing

Load License: No file chosen

License Information

License Details

Description:	SpamTitan Production License
License Number:	STP-3-0100-733894
Type:	Production
Number of Users:	100
Status:	**License Valid**
Organization:	Copperfasten Technologies
Address:	- - - - IE
Contact:	- -
Email:	tim@spamtitan.com
Telephone:	
Fax:	

License Validity

Issued Date:	April 28, 2014
Update Expiry Date:	May 31, 2016

License Usage

Max. Daily Usage:	144
Average Daily Usage:	102

Figure 2-4 Licensing page

In order to license SpamTitan you need to obtain a valid license file from SpamTitan.

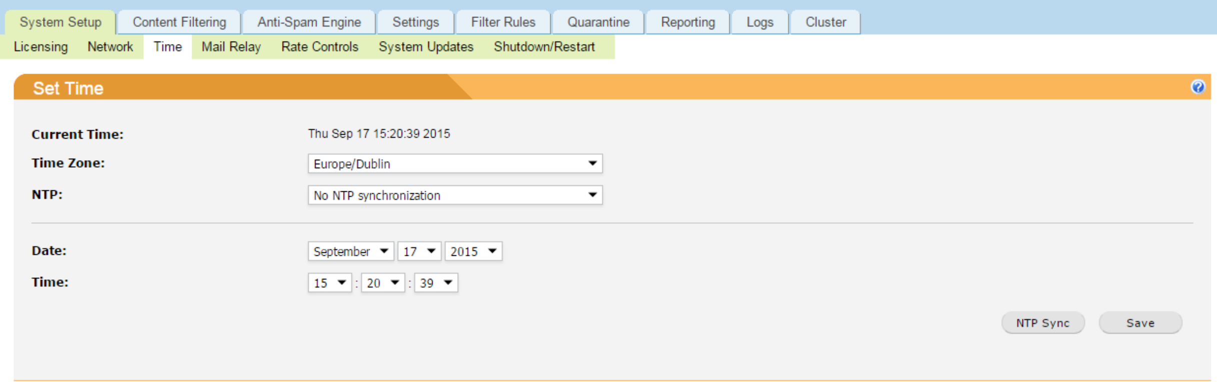
This license may then be imported through the **System Setup** > **Licensing** page. Click the Browse button, select the license file to upload and finally click the Load button.

After successful loading of the license, the License Information window will show details of your license. Without a valid license, access to the web interface will be restricted, as will access to spam, virus and system updates.

2.9 System Time

SpamTitan uses the time and date settings to time stamp log events, to automatically update anti-virus definition files and spam rule set files, and for other internal purposes.

Use the **System Setup > Time** page to set the time and date of the appliance.



Set Time

Current Time:	Thu Sep 17 15:20:39 2015
Time Zone:	Europe/Dublin
NTP:	No NTP synchronization
Date:	September 17 2015
Time:	15 : 20 : 39

Figure 2-5 Time setup

The date and time can be set manually with the help of the drop-down menu or can be automatically synchronized using NTP. Network Time Protocol (NTP) is a protocol used to synchronize computer clock times in a network of computers. NTP uses Coordinated Universal Time (UTC) to synchronize computer clock times to a millisecond, and sometimes to a fraction of a millisecond. By default, SpamTitan uses an internal list of public NTP servers to automatically update the time.

To select your time zone and automatically update the time, choose the time zone from the Time Zone menu.

Then choose **Use NTP to synchronize time** from the NTP Settings menu to use NTP to set the time automatically. You must specify at least 1 NTP server to use for time synchronization. Press the Reset button to reset the NTP servers to the CMFA default servers. These are several publicly available servers.

If you want to set the time manually, then select **No NTP Server** from the NTP Settings menu. Then enter the date in the Month, Day and Year fields and the time in the Hours, Minutes and Seconds fields. After selecting the time settings, click Save to update the date and time.

3 Network

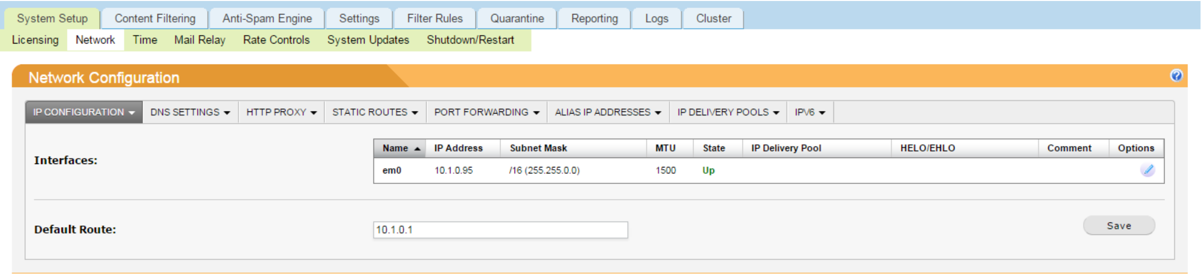
This chapter covers the basic networking setup tasks that are available from the **System Setup > Network** page. The following topics are included in this chapter:

- IP Configuration
- DNS Settings
- HTTP Proxy
- Static Routes
- Port Forwarding
- Alias IP Addresses
- Outbound Delivery Pools
- IPv6

3.1 IP Configuration

This section describes how to configure the network operation of SpamTitan.

The IP Configuration tab of the Network Configuration page allows you to configure the network properties for each network interface on the appliance, as well as the default gateway.



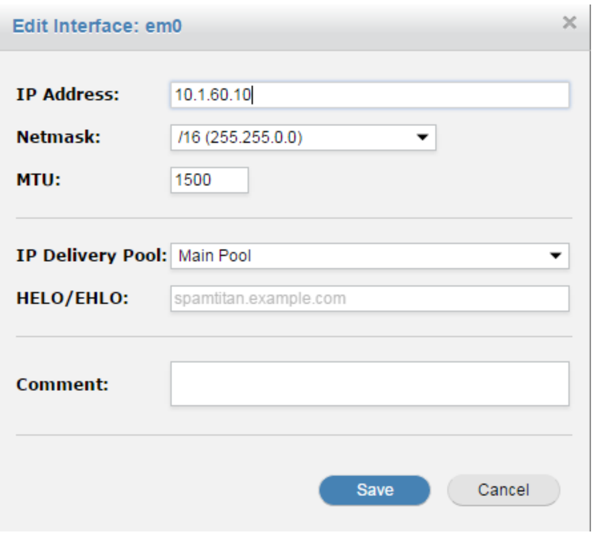
Interfaces:

Name	IP Address	Subnet Mask	MTU	State	IP Delivery Pool	HELO/EHLO	Comment	Options
em0	10.1.0.95	/16 (255.255.0.0)	1500	Up				

Default Route: 10.1.0.1

Figure 3-1 Networking: Interfaces page

Click the edit icon (✎) to edit the settings for each network interface. Most installation will require only one network interface. The Edit Interface dialog will be displayed:



IP Address: 10.1.60.10
Netmask: /16 (255.255.0.0)
MTU: 1500
IP Delivery Pool: Main Pool
HELO/EHLO: spamtitan.example.com
Comment:

Figure 3-2 Edit Interface Dialog

The settings on the Edit Interface dialog are as follows:

Setting	Description
IP Address	The current IP address of the interface
Netmask	Select a network mask
MTU	Enter the maximum transmission unit for the interface in bytes. In most circumstances the default MTU of 1500 bytes will be OK and should not be changed as entering incorrect values here could render the interface unusable.
IP Delivery Pool	Specify which IP Delivery Pool (if any) that this network interface is a member of.
HELO/EHLO	It's important that the DNS PTR record of your connecting IP addresses matches the hostname that is supplied in the HELO/EHLO command of the SMTP conversation, as otherwise recipient mail servers may reject the connection.
Comment	Optional comment

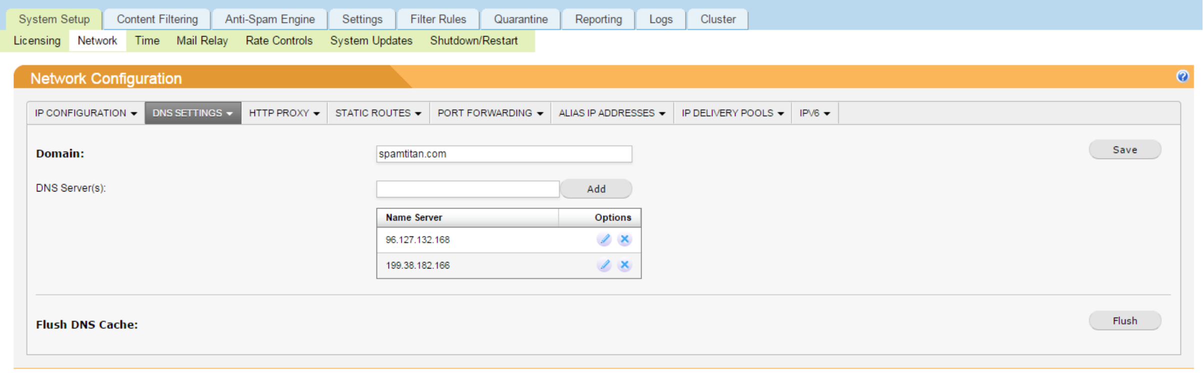
Table 3-1 Edit Interface Dialog Settings

Note: When you save the Network Configuration settings, you may be disconnected from the SpamTitan server if the IP address is changed. You will then have to access the SpamTitan server at its new IP address.

3.2 DNS Settings

The domain name system (DNS) is a distributed data base for the management of Internet name spaces. DNS allows you to either convert a hostname to an IP address or, alternately, convert the IP address to a name (reverse lookup).

The **System Setup > Network** page allows you to configure the DNS settings.



Domain: spamtitan.com

DNS Server(s):

Name Server	Options
96.127.132.168	
199.38.182.166	

Flush DNS Cache:

Figure 3-3 DNS Settings page

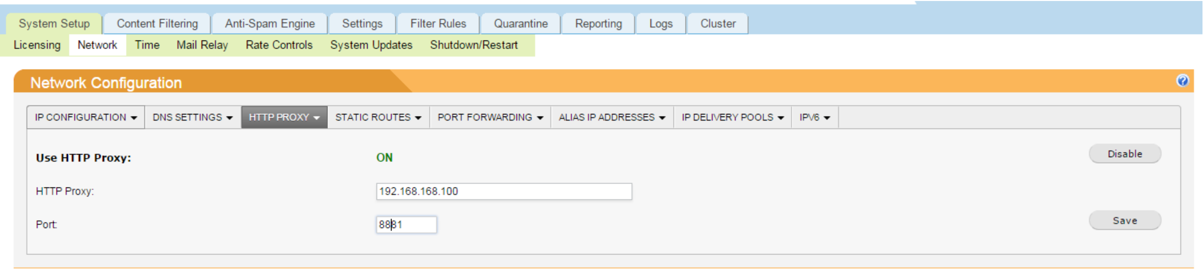
The following table describes the DNS settings:

Field	Description
Domain	This shows the primary domain for the appliance.
DNS Server(s)	This specifies the list of primary and secondary DNS name servers in Internet address (dot notation) format that the DNS resolver should query. Up to 3 name servers should be listed. If you specify more than 1 name server, then the resolver will query them in the order listed. Note: Certain features of SpamTitan, such as RBL and SURBL tests depend on DNS availability in order to correctly categorize messages.
Flush DNS Cache	Click the *Flush* button to clear the DNS cache.

Table 3-2 DNS Settings

3.3 HTTP Proxy

SpamTitan uses, by default, port 80 to retrieve Virus signature updates and spam rule updates. If you use an http proxy server in your organization then Enable the HTTP proxy setting on the **System Setup** > **Network** page, and specify the HTTP Proxy and HTTP Port. Incorrect proxy settings may cause your virus signature and spam rule updates to fail. HTTP proxy is disabled by default.



Use HTTP Proxy: ON

HTTP Proxy: 192.168.168.100

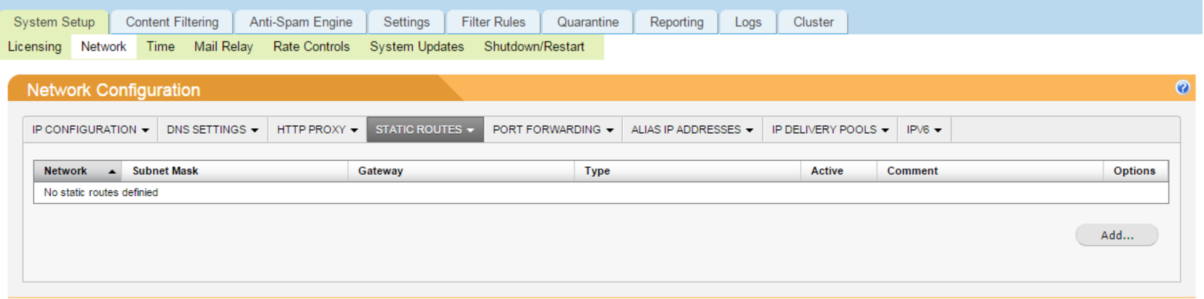
Port: 8881

Figure 3-4 Configure HTTP Proxy settings

3.4 Static Routes

If you have complex routing requirements, then you may need to manipulate the network routing tables by adding static routes.

The **System Setup > Network** page allows you to manipulate static routes.



Network ▲	Subnet Mask	Gateway	Type	Active	Comment	Options
No static routes defined						

Figure 3-5 Configure Static Routes

To add a static route enter the routing information and press the Add button. Use the following syntax when adding a route:

```
        [-net | -host] destination gateway [netmask]
```

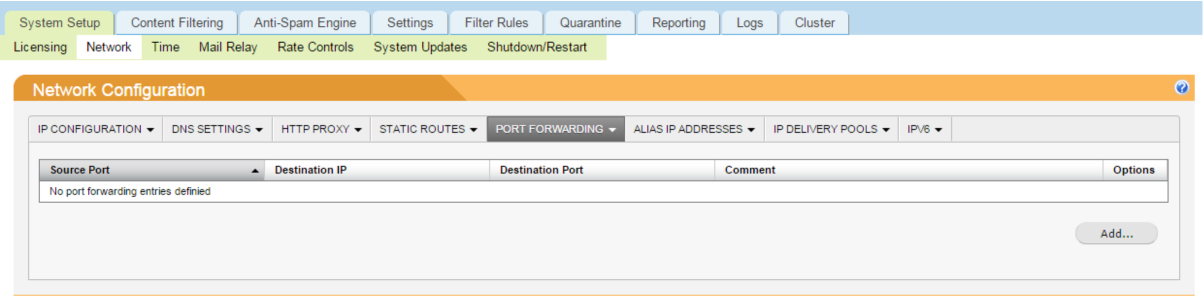
where destination is the destination host or network, gateway is the next-hop intermediary via which packets should be routed. Routes to a particular host may be distinguished from those to a network by interpreting the Internet address specified as the destination argument. The optional modifiers -net and -host force the destination to be interpreted as a network or a host, respectively. Otherwise, if the destination has a "local address part" of INADDR_ANY (0.0.0.0), or if the destination is the symbolic name of a network, then the route is assumed to be to a network; otherwise, it is presumed to be a route to a host. Optionally, the destination could also be specified in the net/bits format.

For example,

- 128.32 is interpreted as -host 128.0.0.32
- 128.32.130 is interpreted as –host 128.32.0.130
- -net 128.32 is interpreted as 128.32.0.0
- -net 128.32.130 is interpreted as 128.32.130.0
- 192.168.64/20 is interpreted as -net 192.168.64 –netmask 255.255.240.0.

3.5 Port Forwarding

Accessing the **Port Forwarding** section of **System Setup** > **Network** will let the user add a port forwarding entry:



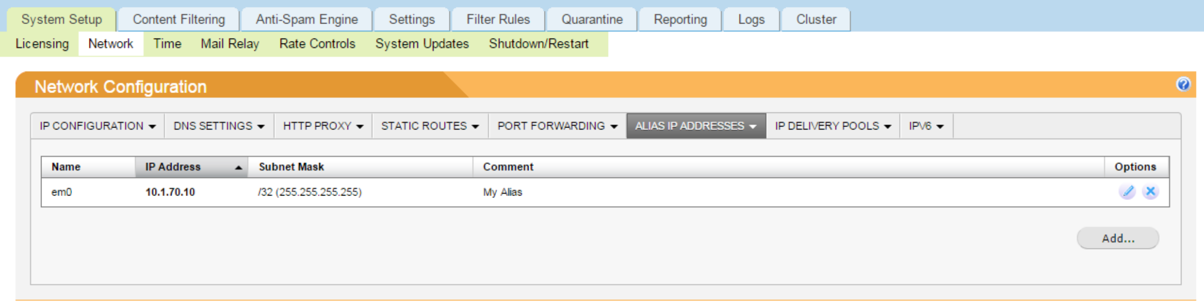
Source Port	Destination IP	Destination Port	Comment	Options
No port forwarding entries defined				

Figure 3-6 Configure Port Forwarding settings

Port forwarding allows rules to be set up that will transparently redirect traffic destined for non-used ports on the appliance to a port on a different system. In the **Source Port** field we specify an unused TCP port on the appliance. We then add the IP address of the destination server that packets will be forwarded to in the **Destination IP** field. In the **Destination Port** section we add a TCP port on the destination server.

3.6 Alias IP Addresses

Using the **Alias IP Addresses** section of **System Setup > Network** we can add details of any IP Aliases.



Name	IP Address	Subnet Mask	Comment	Options
em0	10.1.70.10	/32 (255.255.255.255)	My Alias	

Figure 3-7 Configure Alias IP Addresses

Additional IP addresses may be established for each network interface. This is sometimes useful when changing network numbers, and you wish to accept packets addressed to the old interface. If the address is on the same subnet as the first network address for this interface, all configured additional IP addresses will respond on the configured SMTP port as well as the configure UI port.

This is also used to configure extra alias IPs for IP Delivery Pools to deliver mail from.

To add a new IP Alias, click on the Add... button. The Add IP Alias dialog is displayed.

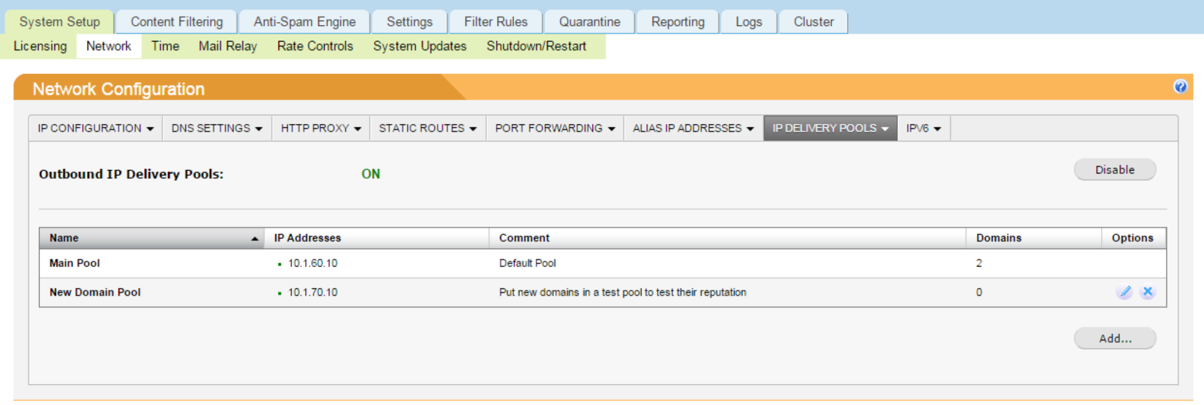
The entries on the Add/Edit IP Alias dialog are as follows:

Field	Description
IP/Network	IP address to add
Address Type	Specify if the address is an IPv4 or IPv6 address.
Physical Interface	The network interface card (NIC) that this address is being added to.
IP Delivery Pool	Select the pool you wish this alias to deliver mails from. You can configure these from the System Setup > Network > Alias IP address tab
Comment	Optional comment field.

Table 3-3 Add/Edit IP Alias dialog fields

3.7 Outbound Delivery Pools

By default, SpamTitan will use the primary IP address to deliver outbound messages to the MX records of the recipients. Some customers may wish to separate the outbound delivery IP from the inbound delivery IP. Also, to minimize the impact of potentially getting listed on RBL blacklists (for example, in the event of an internal spam outbreak), some users (ISPs typically) may prefer to use a pool of IP addresses which will be selected randomly to deliver the outbound mail. It's then easier for them to pull an IP if one of them gets listed on an RBL.



Outbound IP Delivery Pools: ON

Name	IP Addresses	Comment	Domains	Options
Main Pool	• 10.1.60.10	Default Pool	2	
New Domain Pool	• 10.1.70.10	Put new domains in a test pool to test their reputation	0	✎ ✕

Figure 3-8 Configure IP Delivery Pools

In addition, different IP Delivery Pools may be specified for different outbound sender domains. So, for instance when running in a multi-tenant environment, MSPs/ISPs may assign a private IP address pool to certain customers.

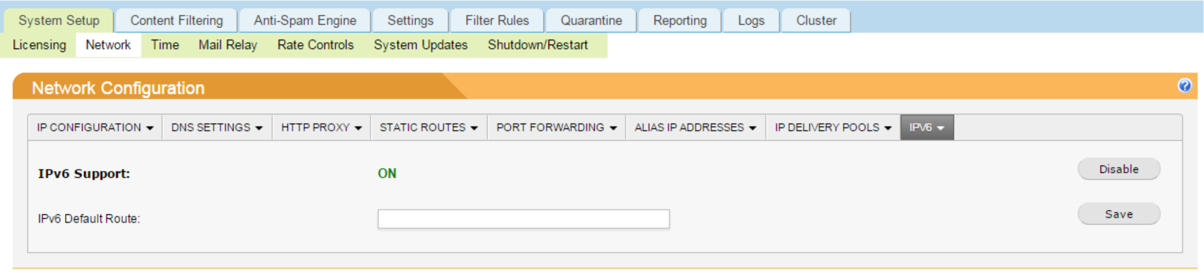
Once IP Delivery Pools are enabled, you can assign the appliances IP addresses to 1 or more IP Delivery pools. This can be done on the IP Configuration tab and the Alias IP Addresses tab.

It's important that the DNS PTR record of your connecting IP addresses matches the hostname that is supplied in the HELO/EHLO command of the SMTP conversation, as otherwise recipient mail servers may reject the connection. When adding an IP address to an IP Delivery pool, it's possible to set a custom HELO for the IP address in the HELO/EHLO field which defaults to the hostname of the appliance. This default is fine as long as the PTR record of the IP matches.

By default, all outbound mail will use the Main Pool if IP Delivery pools are enabled. To use a specific IP Delivery Pool for all mails from a specific (internal) domain, you must edit the domain on the System Setup -> Mail Relay -> Domains tab, and specify the IP Delivery Pool from the dropdown list.

3.8 IPv6

Using the IPV6 section of System Setup > Network we can alter IPV6 settings.



IPv6 Support: ON

IPv6 Default Route:

Figure 3-9 Configure IPv6 settings

When IPv6 networking is enabled, the appliance may send and receive email over IPv6 networks, and those messages will be scanned for viruses and spam. To enable IPv6 support, click on the **Enable** button and then specify the IPv6 default route. You can then specify an IPv6 address for an interface on the **Alias IP Addresses** tab, and an IPv6 name server entry may be specified on the **DNS settings** tab.

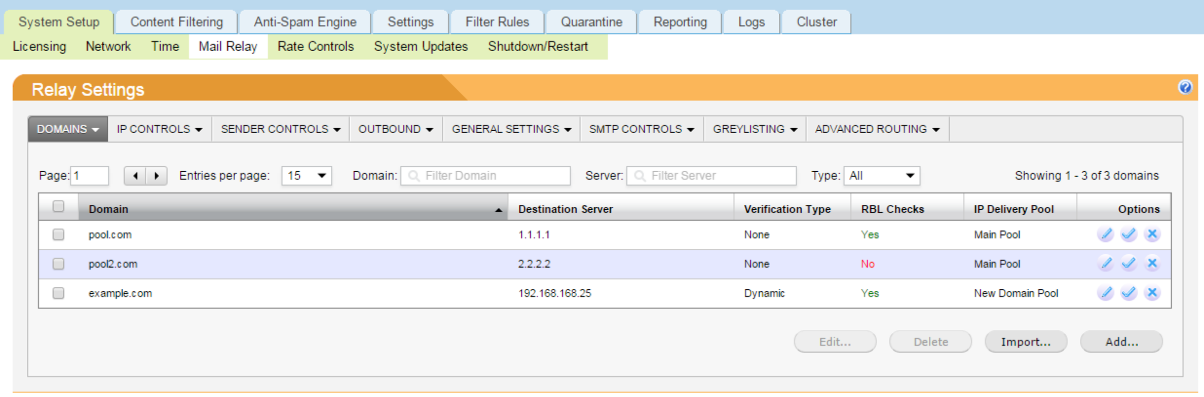
4 Mail Relay

This chapter describes how to configure basic mail relay settings of SpamTitan. The following topics are included in this chapter:

- Domains
- IP Controls
- Sender Controls
- Outbound Settings
- General Settings
- SMTP Controls
- Greylisting
- Advanced Routing

4.1 Domains

Use the **Domains s**ection of the **System Setup** > **Mail Relay** page to add or edit domains that your organization accepts mail:



Page: 1 Entries per page: 15 Domain: Filter Domain Server: Filter Server Type: All Showing 1 - 3 of 3 domains

□	Domain	Destination Server	Verification Type	RBL Checks	IP Delivery Pool	Options
□	pool.com	1.1.1.1	None	Yes	Main Pool	✎ ✓ ✕
□	pool2.com	2.2.2.2	None	No	Main Pool	✎ ✓ ✕
□	example.com	192.168.168.25	Dynamic	Yes	New Domain Pool	✎ ✓ ✕

Figure 4-1 Mail Relay: Domains

The following table describes each of the fields of the Add/Edit Domain dialog:

Field	Description
Domain	Describes the domain that will receive mail. If the resolved destination address matches one of the listed domains, or a sub-domain thereof, then the message will be accepted for processing. Otherwise the mail will be rejected as an unauthorized relay attempt.
Destination Server	This is the hostname or IP address of the mail server which will receive mail after been processed by SpamTitan. Typically the destination mail server would be your Microsoft Exchange Server, or alternative mail server on your local network. Multiple servers may be specified by adding additional entries to the field. They will behave differently

	depending on the separator: ▪ Comma ",": each server will be used in round-robin order. i.e. the load will be distributed evenly between them. ▪ Space " ": subsequent entries after the 1st entry will be treated as fallback servers which will only be used if the precending entries are unreachable. You must either use subsequent entries as fallbacks or round-robins, the functionality cannot be mixed.
Destination Port	This is the port number of the destination mail server. Default 25.
Enable MX Lookup	If checked, then mail will be relayed using the MX records for the server listed in Destination Server. If this setting is enabled, then you must enter a domain name for the Destination server field. Default: Off.
Recipient Verification	Recipient Verification provides a means of protecting against Dictionary Attacks. A *Dictionary Attack* is an email spamming technique in which a spammer sends out thousands of emails with randomly generated addresses using combinations of letters in the hopes of reaching a percentage of actual email addresses. This can add a significant burden to your email server and, depending on your servers configuration may result in a number of bounce messages. For instance, Microsoft Exchange attmepts to protect against Dictionary Attacks by accepting messages for all recipients rather than rejecting invalid recipients and letting a spammer know which accounts are valid. Unfortunately, this often leads to unnecessarily high Exchange server CPU loads because the server still attempts to send one or more non-delivery notifications for every invalid recipient. If Recipient Verification is enabled, then messages to unknown users are immediately rejected, before the message even arrives in your network. SpamTitan can use several methods to perform recipient verification depending on your environment. If your mail server supports recipient verification, then you should select **Dynamic Recipient Verification.** Most Unix based mail servers, Groupwise, and Exchange 2003 (off by default) support this option. In the **Verification Server** field specify the server that the verification probe should be sent to. Normally this will be the same as the Destination Server, but in some cases it may be a different server if required.

	For Exchange 2000 mail servers, or other mail servers that support LDAP directories, select **LDAP Recipient Verification** and enter in yout LDAP server details. This will query the LDAP server to check if the intended recipient(s) are valid or not. If none of the above options are available, then you can **Specify a list of Allowed Recipients** by manually entering all allowed email addresses, or Importing a flat text file of allowed addresses. Specify one email address per line.
RBL Checks	By default, all RBLs listed on the **System Setup > Mail Relay > IP Controls** page will apply to all domains. You can opt out this domain from RBL testing by setting RBL Checks to No. Default: Yes.
IP Delivery Pool	Outbound mail sent from a user in this domain will use an IP address from the specify IP Delivery Pool. If no IP Delivery Pool is specified, the mail will be sent from the Mail Pool which defaults to the IP address of the appliance.
Domain Group	If Domain Groups are in use, it is possible to assign this domain to a Domain Group using the field provided. At least one Domain Group must exist before this field appears. This field auto-completes, offering suggestions as you type. Assigning the domain to a domain group will allow one or more Domain Group Administrators to be created with access to the Domains within that Domain group. The exact functionality available to the Domain Group Administrator can be controlled by assigning them a role with specific permissions. Default: None.

Table 4-1 Add/Edit Domain dialog settings

Click on the icon to test your domain configuration settings. In the Send Test Email dialog, enter a valid email address for the selected domain and press the Send button. This will attempt to send a test message to that address using the destination server donfigured.

The **Import Domains** feature allows you to bulk import domains into SpamTitan from a csv file. You may prefer to use this if you have multiple domains to manage, rather than enter each domain individucally. To import domains in bulk click on the Import… button. The CSV file must have the following format:

- Domain Name (required)
- Destination Mail Server:Port (required)
- Recipient Verification type (none/dynamic/ldap) (required)

If dynamic recipient verification is choosen, then the following field must also be present:

- Verification Server

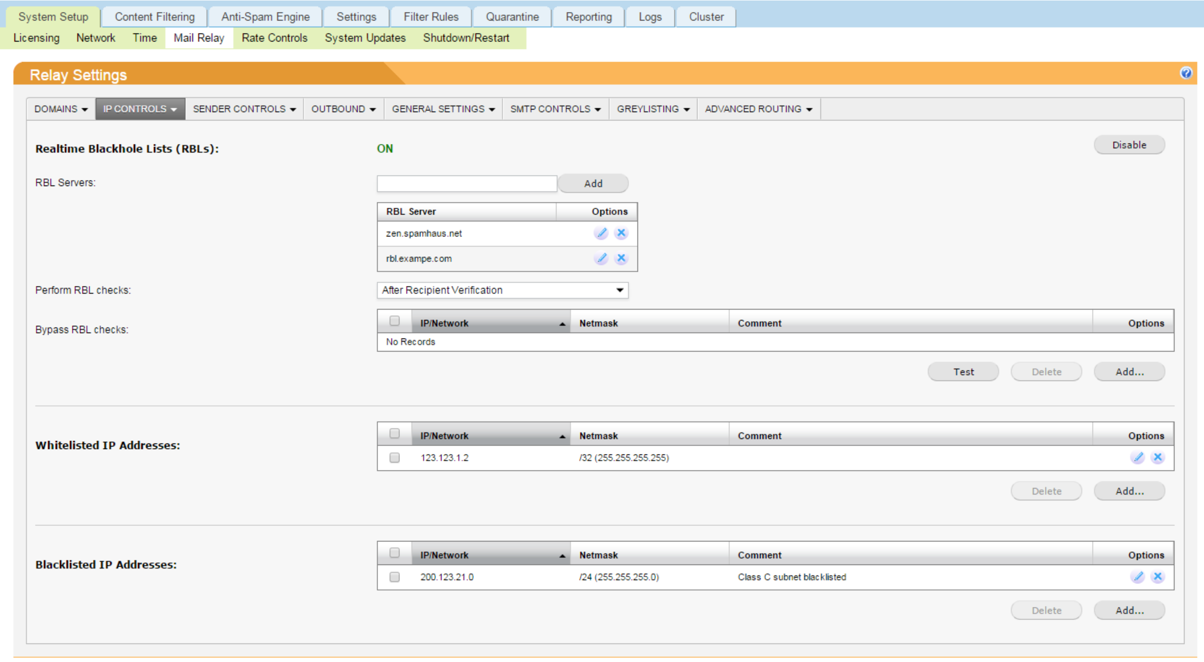
If ldap recipient verification is choosen, then the following fields must also be present:

- LDAP Server:Port
- LDAP Search User (if anonymous bind is allowed leave this blank)
- LDAP Search User Password (if anonymous bind is allowed leave this blank)
- LDAP Query Filter
- LDAP Search base
- LDAP result attribute

4.2 IP Controls

Use the **IP Controls** section of **System Setup > Mail Relay** to alter RBL as well as

Whitelisted IP Addresses and Blacklisted IP Addresses settings:



Realtime Blackhole Lists (RBLs): ON

RBL Servers:

RBL Server	Options
zen.spamhaus.net	
rbl.exampe.com	

Perform RBL checks: After Recipient Verification

Bypass RBL checks:

□	IP/Network	Netmask	Comment	Options
No Records				

Whitelisted IP Addresses:

□	IP/Network	Netmask	Comment	Options
□	123.123.1.2	/32 (255.255.255.255)		

Blacklisted IP Addresses:

□	IP/Network	Netmask	Comment	Options
□	200.123.21.0	/24 (255.255.255.0)	Class C subnet blacklisted	

Figure 4-2 IP Controls page

The following table describes each of the fields:

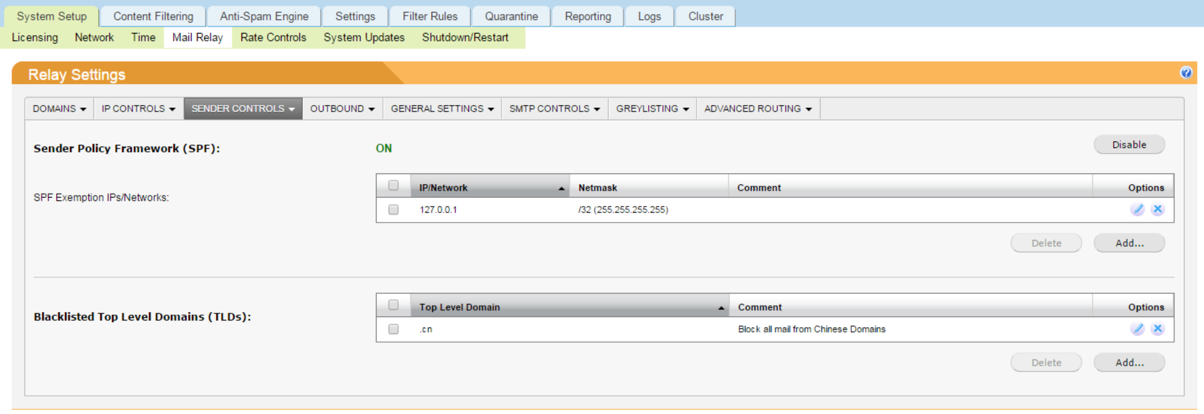
Field	Description
Realtime Blackhole Lists	Use this option to enable or disable the usage of Realtime Blackhole lists. The **Realtime Blackhole List** feature can be used to check external databases (DNSbl) for known spammer hosts or relays. A DNSbl (DNS blacklist) works for IP addresses only.
RBL Servers	To add an RBL to the list of **RBL Servers** enter the RBL and click the **Add** button.
Perform RBL checks	Use this to alter the settings of whether to perform RBL checks after recipient verification, when the message is confirmed to be deliverable, or before recipient verification.
Bypass RBL checks	The **Bypass RBL checks** is a list of IP addresses or CIDR addresses that will be accepted, even if they

	would fail an RBL test. This is to facilitate RBL false positives.
Whitelisted IP Addresses	The Whitelisted IP Addresses table lists IP addresses and networks that bypass spam scoring tests.
Blacklisted IP Addresses	The Blacklisted IP Addresses table lists IP addresses and networks that are rejected during the initial SMTP handshake and before the receipt of any of the message body.

Table 4-2 IP Controls settings

4.3 Sender Controls

Use the Sender Controls tab in the System Setup > Mail Relay page to alter SPF and blacklisted TLD settings.



Sender Policy Framework (SPF): ON

SPF Exemption IPs/Networks:

□	IP/Network	Netmask	Comment	Options
□	127.0.0.1	/32 (255.255.255.255)		

Blacklisted Top Level Domains (TLDs):

□	Top Level Domain	Comment	Options
□	.cn	Block all mail from Chinese Domains	

Figure 4-3 Sender Controls page

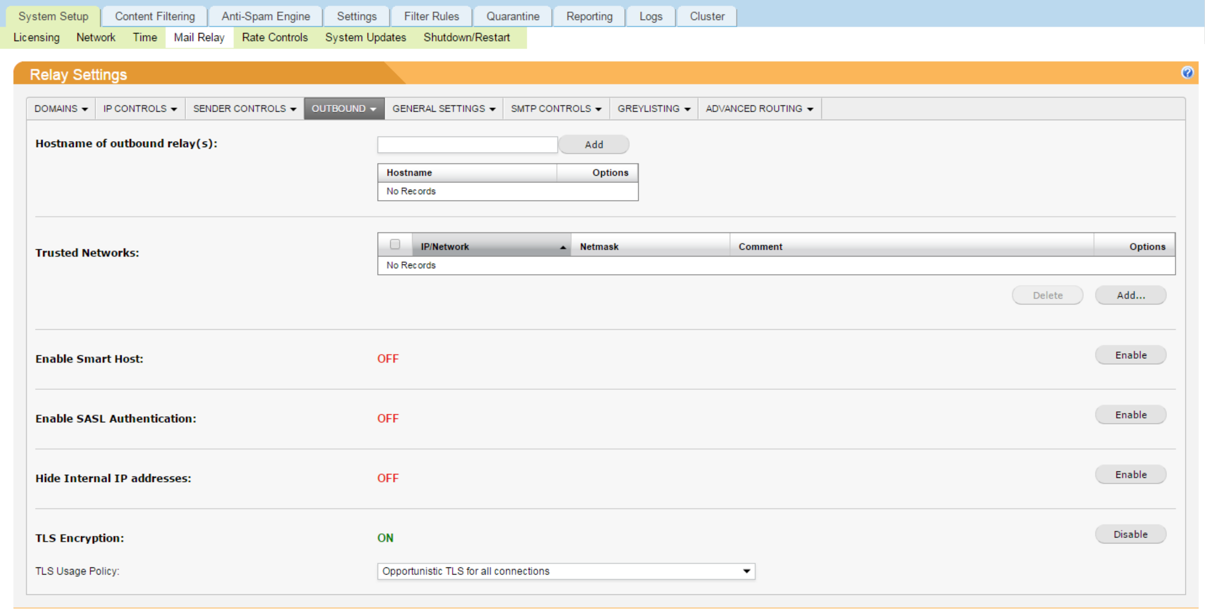
The following table describes each of the fields:

Field	Description
Sender Policy Framework	SPF allows the owner of a domain to use special DNS records to specify which machines are authorized to transmit e-mail for that domain. When receiving a message from a domain, the receiver can check the DNS records to make sure that the mail comes from locations that the domain authorized. When enabled, messages that fail the SPF test will be rejected. This option is *Disabled* by default as it can result in mail being rejected from domains with misconfigured SPF records.
SPF Exemption IPs/Network	Click 'Add' to enter the details of IPs/Networks that are exempt from SPF checks.
Blacklisted Top Level Domains	This section lists sender domains that are rejected during the initial SMTP connection. For example, use this section to block all mails from domains ending with *.info* or *.biz*.

Table 4-3 Sender Controls settings

4.4 Outbound Settings

Use the **Outbound** tab of the **System Setup > Mail Relay** page to alter the settings for outbound mail delivery.



Hostname of outbound relay(s):

Hostname	Options
No Records	

Trusted Networks:

□	IP/Network	Netmask	Comment	Options
No Records				

Enable Smart Host: OFF

Enable SASL Authentication: OFF

Hide Internal IP addresses: OFF

TLS Encryption: ON

TLS Usage Policy: Opportunistic TLS for all connections

Figure 4-4 Configuring Outbound mail

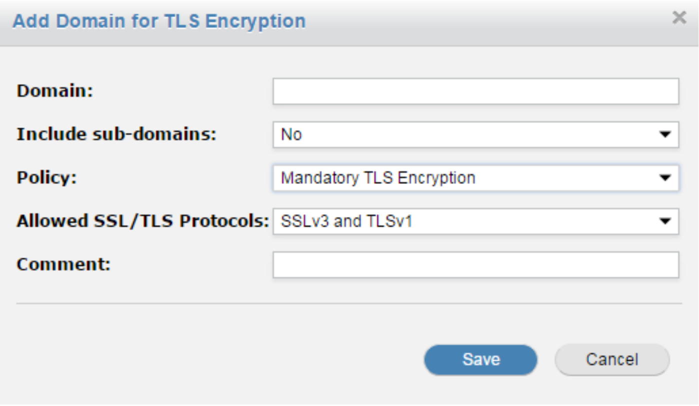
The following table describes the settings on the **Outbound** tab:

Field	Description
Hostname of outbound relay(s)	This lists the hostname of the relay(s) that you send your outbound mail through. This is used to 'rescue' legitimate bounce messages that were generated in response to mail you really did send. If a bounce messages is found, and it contains one of these hostnames in a *Received* header in the bounced message, it will not be marked as a blowback virus-bounce.
Trusted Networks	If you want to relay outgoing mail through SpamTitan you must specify the list of hosts and/or networks that are allowed to relay mail. The list of trusted networks is a list of network addresses or network/netmask patterns specified in CIDR (Classless Inter-Domain Routing) format. The list is matched from top to bottom, and the search stops on the first match. Specify the "!" character in the pattern to exclude an address or network block from the list.
Enable Smart Host	A **Smart Host** is a mail server which allows SpamTitan to send mail via an intermediate server instead of sending mail directly to recipients' servers. To enable a Smart Host click on the **Enable** button. It will then be possible to specify the Smart Host, Smart Host Port number, and authentication settings. Select

	Yes in the **Force TLS encryption** dropdown to ensure that all traffic between SpamTitan and the Smart host is encrypted.
Enable SASL Authentication	SMTP/SASL Authentication solves the problem of relaying messages from anywhere in the world via your SpamTitan server. If a mail client successfully authenticates itself providing username and password to SpamTitan, then that mail client will be permitted to relay mail. The credentials provided are compared against the users' credentials in a LDAP/Active Directory.
Hide Internal IP addresses	Enable this setting to strip **Received headers** with internal (trusted) IP addresses from outbound mail.
TLS Encryption	To use a secure TLS encrypted channel to send outbound mail from all domains, enable TLS Encryption. By default, this enables a TLS Usage Policy of opportunistic TLS encryption for all connections. SpamTitan advertises and negotiates an encrypted channel with the peer for the SMTP connection. The encrypted channel is only used when the peer also supports it – hence the term opportunistic.
TLS Usage Policy	The TLS Usage policy lets you choose between: ▪ Opportunistic TLS for all connections ▪ Use TLS only for specified domains ▪ Use TLS for specified domains and Opportunistic TLS for all other connections

Table 4-4 Outbound mail settings

Click on the Add button to create a TLS policy for a specific domain:



Add Domain for TLS Encryption

Domain:

Include sub-domains: No

Policy: Mandatory TLS Encryption

Allowed SSL/TLS Protocols: SSLv3 and TLSv1

Comment:

Figure 4-5 Add/Edit TLS Policy dialog

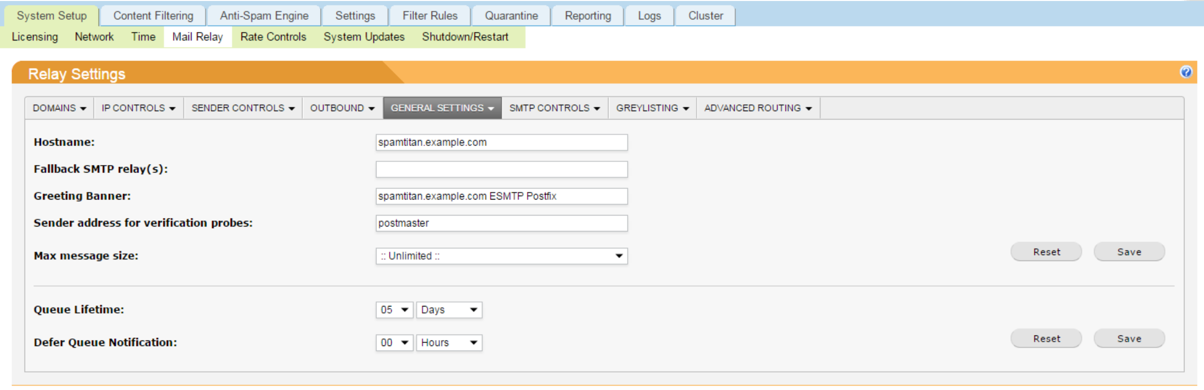
The entries on the **Add/Edit Domain for TLS Encryption** dialog are as follows:

Field	Description
Domain	Recipient domain of whom this TLS policy relates.
Include sub-domains	Weather the policy applies to sub-domains of the given domain.
Policy	The security levels in order of increasing security are: ▪ **Disable TLS** ▪ **Opportunistic TLS Encryption.** When opportunistic TLS handshake fails, SpamTitan retries the connection with TLS disabled. This allows mail delivery to sites with non-interoperable TLS implementations. ▪ **Mandatory TLS Encryption** Messages are sent only over TLS encrypted sessions. The SMTP transaction is aborted unless the STARTTLS ESMTP feature is supported by the remote SMTP server. If no suitable servers are found, the message will be deferred. Mandatory TLS encryption is not viable as a default security level for mail delivery to the public Internet as most MX hosts do not support TLS at all, and some of those that do have broken implementations. ▪ **Mandatory TLS Encryption with Verification** At the "verify" TLS security level, messages are sent only over TLS encrypted sessions if the remote SMTP server certificate is valid (not expired or revoked, and signed by a trusted certificate authority) and where the server certificate name matches a known pattern.
Allowed SSL/TLS Protocols	When mandatory TLS Encryption or higher is chosen, then you must specify the protocols that the SpamTitan SMTP client will use. By default "SSLv2 and TLSv1" are the chosen protocols.
Comment	Optional comment for this entry.

Table 4-5 Add/Edit TLS Policy settings

4.5 General Settings

The settings on the **General Settings** tab of the **System Setup > Mail Relay** page control the SpamTitan settings for the *postfix* mail relay.



Hostname: spamtitan.example.com

Fallback SMTP relay(s):

Greeting Banner: spamtitan.example.com ESMTP Postfix

Sender address for verification probes: postmaster

Max message size: :: Unlimited ::

Queue Lifetime: 05 Days

Defer Queue Notification: 00 Hours

Figure 4-6 Configuring General Mail Relay settings page

The following table describes the settings in the General Settings section:

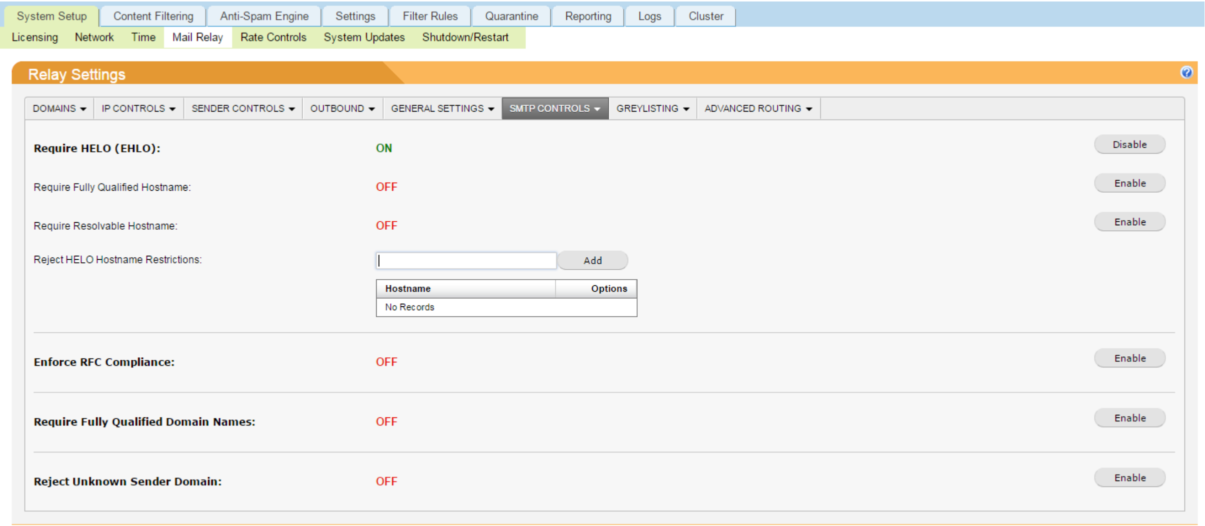
Setting	Description
Hostname	This describes the fully qualified hostname of SpamTitan
Fallback SMTP relay(s)	The Fallback SMTP relay(s) is an optional list of relay hosts for SMTP destinations that can't be found or that are unreachable. By default, mail is returned to the sender when a destination is not found, and delivery is deferred when a destination is unreachable. The Fallback relays must be SMTP destinations. If you specify multiple SMTP destinations, SpamTitan will try then in the specified order.
Greeting Banner	The Greeting Banner is the text that follows the 220 status code in the SMTP greeting banner. The default value is **$hostname ESMTP $mail_name** where $hostname expands to the fully qualified hostname of the appliance and $mail_name expands to **Postfix.**
Sender address for verification probes	This is the sender address to use in address verification probes (default: postmaster). Specify an empty value or <> if you want to use null sender address. Beware, some sites reject mail from <>, even though RFCs require that such addresses be accepted.
Max. message size	The **Maximum message size** setting applies to all incoming mails. If your backend server has a limitation on message sizes, you should set this to the same value or a lower limit here. A reasonable maximum setting would be 20 to 40MB.

Queue Lifetime	The **Queue Lifetime** if the maximal time a message is queued for delivery before it is sent back as undeliverable. The default value is 5 days.
Defer Queue Notification	**Defer Queue Notification** is the time after which the sender receives the message headers of mail that is still queued. Disable by entering 0 as value. This is the default value.

Table 4-6 General Mail Relay settings

4.6 SMTP Controls

The SMTP protocol has no built-in method for authenticating senders of emails, and as such spammers have employed a number of tactics for hiding their identities. Examples include spoofing the Envelope sender address on a message or using a forged HELO address. Some unsolicited commercial email (UCE) can be blocked here by applying strict SMTP checks. This will block some UCE software that violates the SMTP protocol.



Require HELO (EHLO): ON

Require Fully Qualified Hostname: OFF

Require Resolvable Hostname: OFF

Reject HELO Hostname Restrictions:

Hostname	Options
No Records	

Enforce RFC Compliance: OFF

Require Fully Qualified Domain Names: OFF

Reject Unknown Sender Domain: OFF

Figure 4-7 SMTP Controls page

The **SMTP Controls** section of the **System Setup > Mail Relay** page allows you to manage the SMTP controls that are used to reject messages based on SMTP properties of the connection, and the originating IP address of the connection.

These options allow you to screen messages before they have been downloaded to the appliance, thus saving on bandwidth and freeing the spam engine from processing messages, which could have already been identified as spam.

The following table describes the Frontline Content Control settings:

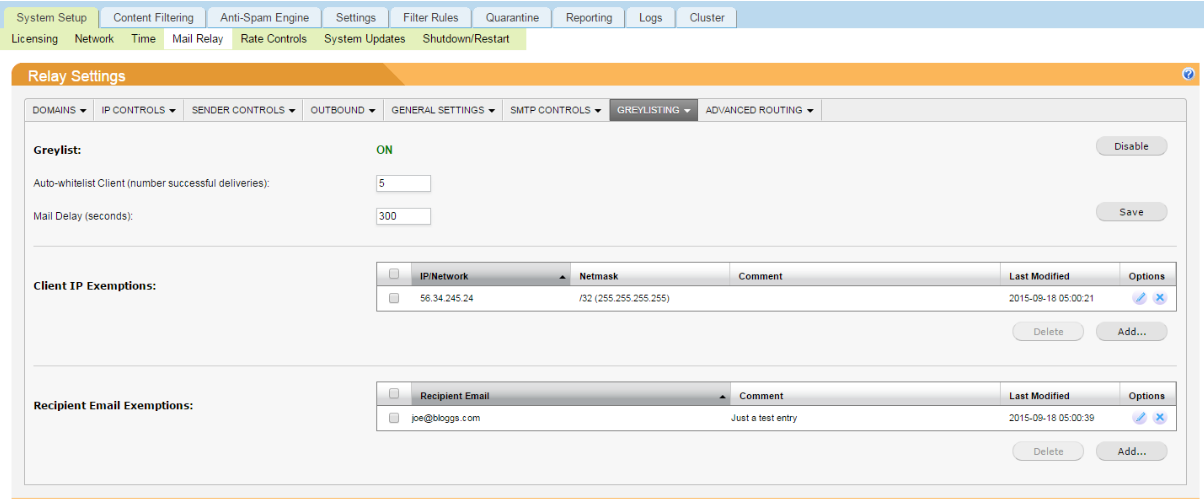
Setting	Description
Require HELO (EHLO)	Activate this option if you want SpamTitan to require that connecting clients send a HELO (or EHLO) command at the beginning of an SMTP session. Requiring this will stop some UCE software. Default: On

Require Fully Qualified Hostname	Activate this option to reject a SMTP connection when the hostname in the client HELO/EHLO command is not in fully-qualified domain form, as required by the RFC. Default: Off
Require Resolvable Hostname	Activate this setting to reject the request when the hostname in the client HELO/EHLO command has no DNS A or MX record. Default: Off
Reject HELO Hostname Restrictions	This allows you to list HELO hostname entries that will be rejected if used by the connecting client HELO (EHLO) command. For instance, nobody should HELO as *localhost* since we are localhost.
Allowed HELO Hostname Restrictions	This allows you to list HELO hostname entries that may be used by non-compliant (but legitimate) mail servers who do not adhere to the RFC. For instance, if you are checking for HELO Fully Qualified hostnames and/or resolvable HELO hostnames, and a particular connecting mail server does not meet these requirements, then you can enter the clients HELO entry here to allow the connection to be accepted. **Note:** The connection may still be rejected, if, for instance, the client fails an RBL check or recipient verification check.
Enforce RFC Compliance	Activate the Enforce RFC Compliance setting to control how tolerant SpamTitan is with respect to addresses given in the MAIL FROM or RCPT TO SMTP commands. If enabled, Postfix will require envelope addresses to be within angle brackets (<>) and without extraneous information as required by the RFC. Unfortunately, the Sendmail program tolerates lots of non-standard behaviour, so a lot of software expects to get away with it. As such, being strict to the RFC not only stops unwanted mail, it may also block legitimate mail from poorly written mail applications. Default: Off
Require FQDN	Activate this option to reject connections if the address in the client MAIL FROM command is not in fully-qualified domain form or if the address in the client RCPT TO command is not in fully-qualified domain form.
Reject Unknown Sender Domain	Activate this option to reject the connection when the sender mail address has no DNS A or MX record.

Table 4-7 SMTP Controls settings

4.7 Greylisting

Greylisting is an anti-spam technique which will initially not accept an email from an unknown source but after some time it will eventually be accepted. Mail is identified by its Triplet. A Triplet is the **CLIENT_IP / SENDER / RECIPIENT** of the sending mail.



Greylist: ON

Auto-whitelist Client (number successful deliveries): 5

Mail Delay (seconds): 300

Client IP Exemptions:

□	IP/Network	Netmask	Comment	Last Modified	Options
□	56.34.245.24	/32 (255.255.255.255)		2015-09-18 05:00:21	✎ ✕

Recipient Email Exemptions:

□	Recipient Email	Comment	Last Modified	Options
□	joe@bloggs.com	Just a test entry	2015-09-18 05:00:39	✎ ✕

Figure 4-8 Configuring Greylisting

The idea behind Greylisting is that Zombie networks used by spammers will not try to resend their spam messages once the messages are rejected.

If it is the first time that this triplet is seen or the time since the last triplet with the same details is less than the Mail Delay setting, then the email gets rejected with a temporary error. Spammers will not try again later, as it is however required per RFC regulations for genuine mail servers to re-send.

The following table describes the various Greylisting options:

Setting	Description
Greylist	You can enable or disable Greylisting by clicking the **Enable** button. Default: Disabled
Auto-whitelist Client	When this setting is enabled IPs that regularly send clean mail, can automatically get onto a whitelist that will bypass them from the greylisting test for all future mails. Note: Their mails will still be subject to all other spam tests that are enabled and Auto-whitelisted clients are not shown in the Client IP Exemptions table. The default auto whitelist counter is set to 5. This means SpamTitan must receive at least one clean mail from a different triplet over 5 different hours. You can change this number to anything from 1 and over, setting 0 will disable the auto-whitelist feature.
Mail Delay	This specifies the amount of time (in seconds) to wait until accepting the same triplet as valid mail. This is

	automatically set to 300 (five minutes) but can be set to any number between 1 and one hour (3,600 seconds).
Client IP Exemptions	The **Client IP Exemptions** table shows a list of Client IP addresses to bypass Greylisting. CIDR's are accepted.
Recipient Email Exemptions	The **Recipient Email Exemptions** table shows a list of Email addresses to bypass Greylisting. Domains are accepted, entered as e.g. 'test.com' without the at symbol.

Table 4-8 Greylisting settings

Example of a Client IP that is added to the auto-whitelist

Auto-whitelist setting is set to 2

Time	Client IP	Sender	Recipient
13:05	1.2.3.4	s1@example.com	r1@yourdomain.com
14:15	1.2.3.4	s2@example.com	r2@yourdomain.com

- Different hours (✓)
- Same IP address (✓)
- Different triplet (✓)
- **Result**: Client IP is added to the auto-whitelist.

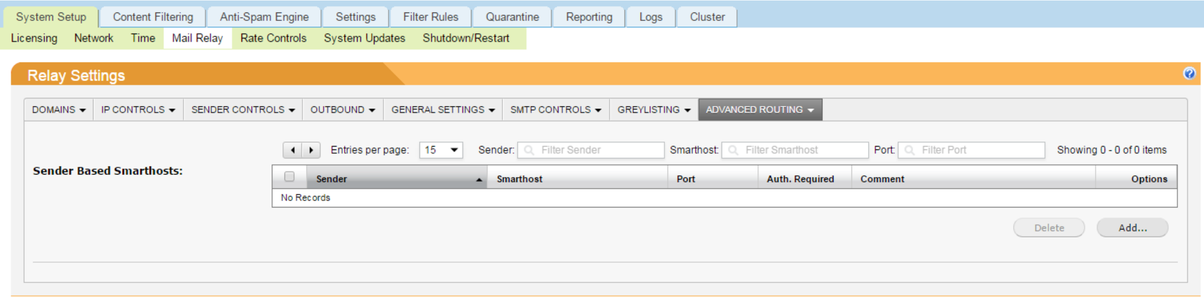
Time	Client IP	Sender	Recipient
17:27	1.2.3.4	s1@example.com	r1@yourdomain.com
17:54	1.2.3.4	s2@example.com	r2@yourdomain.com

- Different hours (✗)
- Same IP address (✓)
- Different triplet (✓)
- **Result**: Client IP is not auto-whitelisted as it did not satisfy all conditions.

4.8 Advanced Routing

Sender dependent smart-hosts provide the ability to relay mail *outbound* from a particular domain or email address through a specific relay/smart-host.

If you require ***all*** outbound mail to go through a particular email server, then specify those smart-host settings in the Smart Host section on the **System Setup > Mail Relay > Outbound** page. Sender based smart-host entries will override those settings for the specified domains or email addresses.



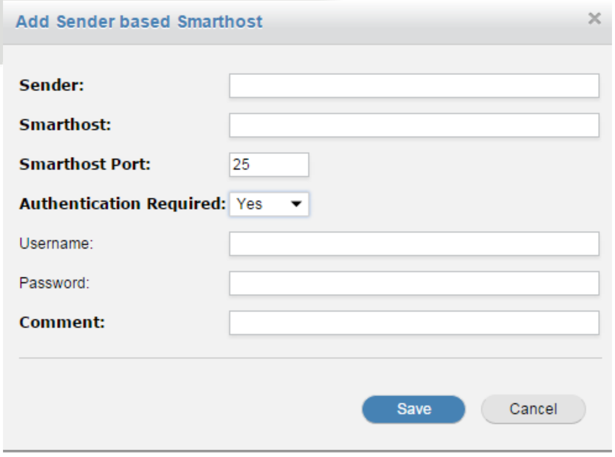
Sender Based Smarthosts:

Entries per page: 15 Sender: Filter Sender Smarthost: Filter Smarthost Port: Filter Port Showing 0 - 0 of 0 items

☐	Sender	Smarthost	Port	Auth. Required	Comment	Options
No Records						

Figure 4-9 Advanced Routing page

To add a new sender based smart-host, click on the **Add…** button. The **Add Sender based Smarthost** dialog is displayed.



Add Sender based Smarthost

Sender:

Smarthost:

Smarthost Port: 25

Authentication Required: Yes

Username:

Password:

Comment:

Figure 4-10 Add/Edit Sender based Smarthost dialog

The following are the entries on the Add/Edit Sender based Smarthost:

Field	Description
Sender	This specifies the envelope sender address or @domain to relay via the smarthost. Email addresses will have higher priority than domains. For instance, if you have entries for both *user@example.com* and *@example.com*, then messages from user@example.com will be relayed through the smarthost for that entry, while messages from all other senders in the example.com domain will be relayed through the smarthost for that domain.
Smarthost	The relay/smarthost to relay to.
Smarthost Port	The port for the smarthost. Default: 25
Authentication Required	Specifies if the smarthost requires authentication credentials to be sent when relaying mail. Default: No
Username	Username for authentication, if required.
Password	Password for authentication, if required.
Comment	Optional comment field.

Table 4-9 Add/Edit Sender based Smarthost dialog settings

5 Rate Controls

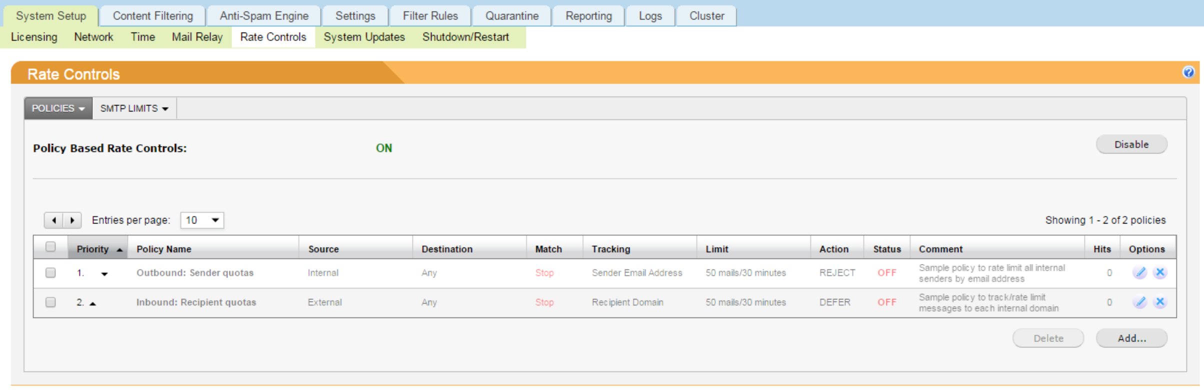
5.1 Rate Control Policies

The Rate Controls Policies feature in SpamTitan can be used to mitigate the effect of certain senders or sending servers from transmitting massive amounts of email due to possible malware infection.

This is particularly important for compromised internal systems which are relaying mail outbound through SpamTitan, as going undetected these outbreaks could lead to the appliance IP address ending up on RBL blacklists. In addition, it can also be used to ensure that a user, sending server or recipient domain remain within a specific limit of either messages or cumulative size of messages for a certain period of time.

Policies may be created to perform sender (based on envelope from address or IP address) or recipient based throttling on messages and/or cumulative message size per defined time unit. For instance, SpamTitan ships with sample policies (which are disabled by default) for rate limiting In-bound connections by tracking the number of connections from each external IP address, and rate limiting Outbound connections by tracking number of mails per sender email address during a 30 minute interval. If the threshold (default 50) is exceeded, then the message is deferred and logged in the History as Rate Controlled.

The policies are implemented by assigning a time-based quota for a specific period, with usage during this period calculated using a sliding/rolling window model.



Policy Based Rate Controls: ON

Entries per page: 10

Showing 1 - 2 of 2 policies

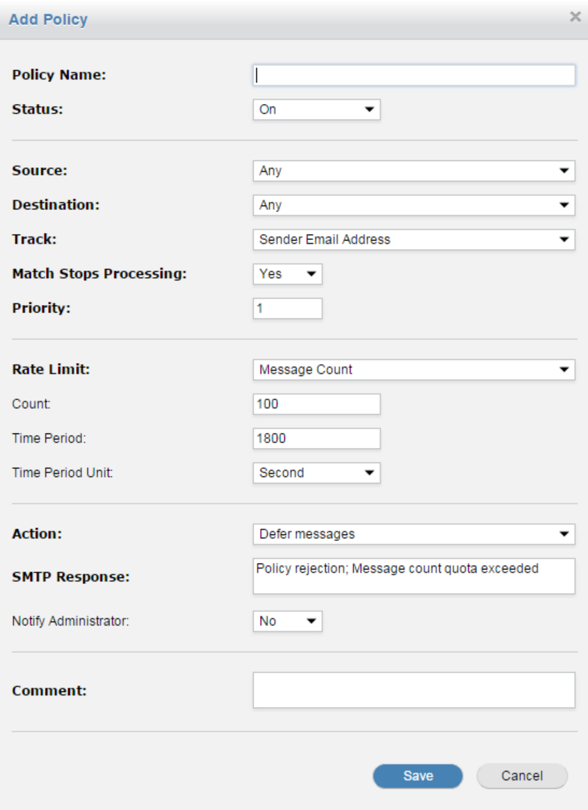
□	Priority	Policy Name	Source	Destination	Match	Tracking	Limit	Action	Status	Comment	Hits	Options
□	1. ▾	Outbound: Sender quotas	Internal	Any	Stop	Sender Email Address	50 mails/30 minutes	REJECT	OFF	Sample policy to rate limit all internal senders by email address	0	✎ ✕
□	2. ▴	Inbound: Recipient quotas	External	Any	Stop	Recipient Domain	50 mails/30 minutes	DEFER	OFF	Sample policy to track/rate limit messages to each internal domain	0	✎ ✕

Figure 5-1 Rate Control Policies page

To enable the Policy based Rate Controls, click on the Enable button. The existing policies will then be displayed in order of priority - with lower priority policies having higher precedence. A policy matches when both the sender/recipient attributes both the policy source/destination. If more than one policy matches, the all policies will be tracked until a policy has Match Stops Processing set to Yes.

To reorder the policies click the down (▾) or up (▴) arrow for the policy. Alternatively, you may reorder a policy rule, by setting its priority when you edit the policy.

To add a new policy, click on the **Add...** button. The Add Policy dialog is displayed.



Policy Name:

Status: On

Source: Any

Destination: Any

Track: Sender Email Address

Match Stops Processing: Yes

Priority: 1

Rate Limit: Message Count

Count: 100

Time Period: 1800

Time Period Unit: Second

Action: Defer messages

SMTP Response: Policy rejection; Message count quota exceeded

Notify Administrator: No

Comment:

Figure 5-2 Add/Edit Rate Control Policy dialog

The entries on the Add/Edit Policy dialog are as follows:

Field	Description
Policy Name	Descriptive name for the policy.
Status	Select ON or OFF to enable or disable this policy.
Source	Source indicates where the message originates. Source can be one of: ▪ **Any** ▪ **Internal**: Originating from an internal network (as defined under System Setup > Mail Relay > Outbound > Trusted Networks) ▪ **External**: Originating from an external network. ▪ **From a specific domain**: specify the sender domain that should match this rule ▪ **From a specific email address**: specify the sender email address that should match this rule ▪ **From a specific IP address/CIDR**: specify the sender IP address or CIDR address that should match this rule
Destination	Destination indicates where the message is destined to. Destination can be one of: ▪ **Any** ▪ **To a specific domain**: specify the recipient domain that should match this rule ▪ **To a specific email address**: specify the sender IP

	address or CIDR address that should match this rule
Track	Track specifies the attribute to maintain counters for. Track can be one of: ▪ **Sender IP Address**: If you select to track the sender IP address, you must specify a bitmask to apply to the sending servers' IP address, for instance /24. This will track the triplet through the entire /24 block. ▪ **Sender Email Address**: Each sender email address will be tracked separately ▪ **Sender Domain**: Each sender domain is tracked separately, and all email sent from these domains will be tracked and matched ▪ **Recipient Email Address**: Each recipient email address will be tracked separately ▪ **Recipient Domain**: Each recipient domain is tracked separately, and all email sent to these domains will be tracked and matched
Match Stops Processing	If set, when a policy matches, no further policy rules will be processed.
Priority	Priority to assign to the rule. All new policies default to the highest priority (1), with all other policies shifting down.
Rate Limit	This specifies if the policy applies to Message Counts or Cumulative Message Size.
Count	The message count threshold that the mails must exceed to trigger the rate control rule.
Size (kb)	The cumulative size of the messages the mails must exceed to trigger the rate control rule.
Time Period	If the rate limit threshold above is exceeded in the Time interval specified here, the message will be deferred or rejected. Otherwise, the rule passes and the tracking counters updated. The time period depends on the value selected below (seconds, minutes, or hours). For example, if you enter 10 as the Time Period and select Minutes from the Time Period Unit drop-down list below, the time period lasts 10 minutes.
Time Period Unit	The unit that the time period is measure in must be selected from the following options: Second, Minute, Hour. The value selected together with that entered above determines the time period.
Action	This specifies the action to be taken when a rule matches and the rate limit threshold has been exceeded in the time interval specified. Action can be one of: ▪ Defer Messages: Messages matching this rule will be deferred. The sender will receive a 4xx level error message instructing the mail server to retry after a predefined time interval. RFC compliant mail servers act upon the defer message and will try

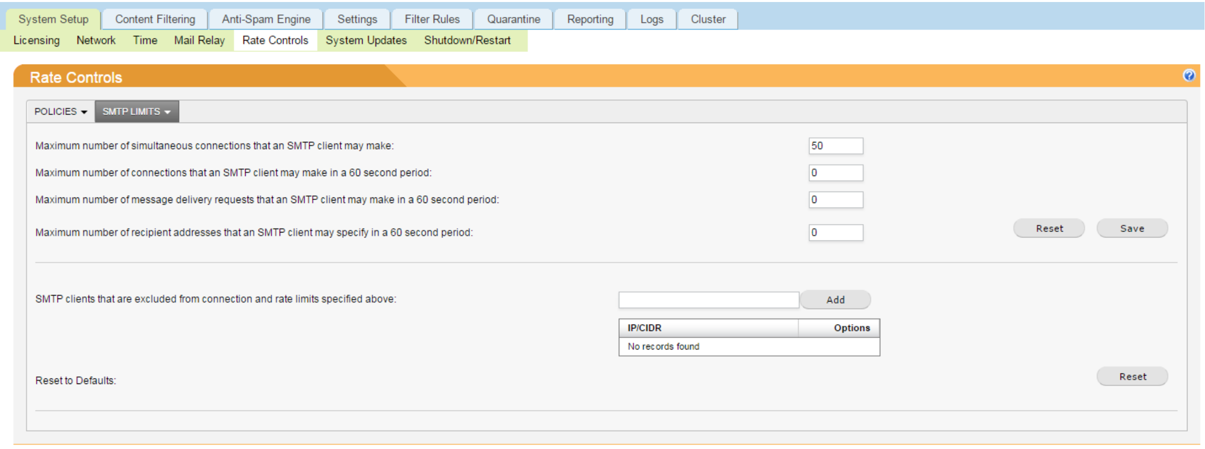
	sending the message again later, while email from spam bots will typically not retry sending the email again. ▪ Reject Messages: Messages matching this rule will be rejected. The sender will receive a 5xx level error instructing the mail server that delivery has permanently failed for that message.
SMTP Response	This is the response that is returned to the sender when a policy rule fires and a message is deferred or rejected.
Notify Administrator	Indicates if an administrator should be notified via email if this rule fires. If enabled, specify the email address of the administrator to receive the notifications.
Comment	Specify an optional comment to associate with this rule.

Table 5-1 Add/Edit Rate Control Policy settings

Note: In a cluster, policy tracking occurs separately on each node. For instance, if the policy is to rate limit senders to 50 mails/hour and you have a two node cluster, each sender could send 100 mails/hour if both nodes are receiving mail in a round-robin fashion.

5.2 SMTP Limits

The SpamTitan appliance Rate Control features provide protection against SMTP clients that make too many connections and/or too many connections in a small amount of time - for example during a spam storm from a spam-bot. The appliance can limit the number of simultaneous connections from the same SMTP client, as well as the connection rate and the rate of certain SMTP commands from the same client. If the limits are exceeded, then further connections are deferred from that client until such time that they fall again below the thresholds.



Maximum number of simultaneous connections that an SMTP client may make: 50

Maximum number of connections that an SMTP client may make in a 60 second period: 0

Maximum number of message delivery requests that an SMTP client may make in a 60 second period: 0

Maximum number of recipient addresses that an SMTP client may specify in a 60 second period: 0

SMTP clients that are excluded from connection and rate limits specified above:

IP/CIDR	Options
No records found	

Reset to Defaults:

Figure 5-3 SMTP Limits page

The Rate Control SMTP Limit settings are as follows:

Setting	Description
Maximum Number of simultaneous connections that an SMTP client may	Specify the maximum number of connections that an SMTP client may

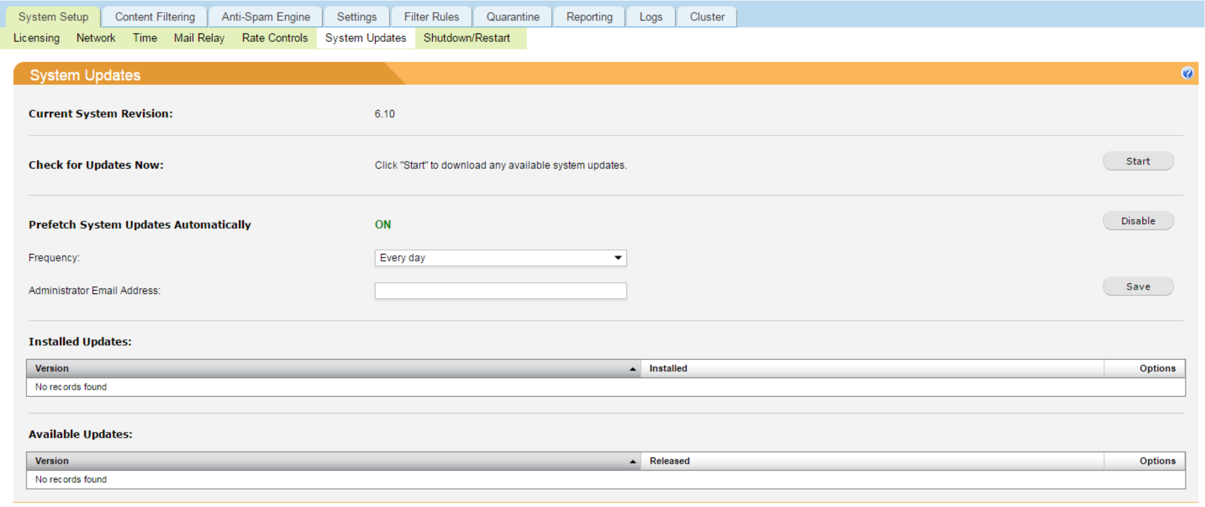
make	make. Default: 50. To disable this feature, specify a limit of 0.
Maximum number of connections that an SMTP client may make in a 60 second period	Specify the maximum number of connections that SMTP client may make in a 60 second period. Default: 0 (disabled - i.e. a client can make as many connections per 60 second time period as the appliance can accept).
Maximum Number of Message Delivery Requests that an SMTP Client may make in a 60 second period.	Specify the maximum number of message delivery requests that an SMTP client may make in a 60 second period. Default: 0 (no limit)
Maximum number of recipient addresses than an SMTP client may specify in a 60 second period	Specify the maximum number of recipient addresses that an SMTP client may specify in a 60 second period. Default: 0 (no limit)
SMTP clients that are excluded from connection and rate limits	Rate control exceptions allow you to specify SMTP clients that are excluded from connection and rate limits specified above. By default, clients in trusted networks are excluded. Specify a list of network blocks or IP/CIDR addresses.
Reset to Defaults	Click the Reset button to reset the rate controls to the default values.

Table 5-2 SMTP Limits settings

Note: These limits must not be used to regulate legitimate traffic: mail will suffer grotesque delays if you do so. The limits are designed to protect the appliance against abuse by out-of-control clients.

6 Managing System Updates

SpamTitan is continually striving to improve its products. **System Setup > System Updates** allows you to keep up to date with the latest patches and functionality enhancements.



Current System Revision: 6.10

Check for Updates Now: Click "Start" to download any available system updates.

Prefetch System Updates Automatically ON

Frequency: Every day

Administrator Email Address:

Installed Updates:

Version	Installed	Options
No records found		

Available Updates:

Version	Released	Options
No records found		

Figure 6-1 System Updates page

Periodic system updates are released from SpamTitan that may contain the following:

- New features
- Patches
- Spam and Virus engine updates
- Security updates

The following table describes the options on this page:

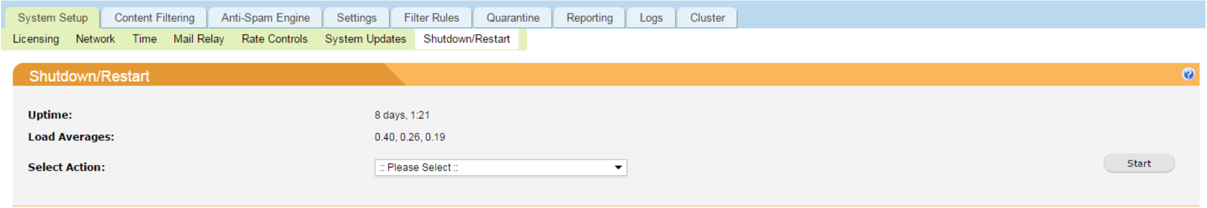
Field	Description
Current System Revision	This lists the currently installed version.
Check for Updates Now	Click **Start** to check for and download any available system updates. A popup window will show the progress of the task. The download (if any) may take a few minutes depending on the size of the update. Please ensure that any pop-up blocking software does not block this new window, so you can monitor the progress of the update process.
Prefetch System Updates Automatically	System Updates may also be automatically imported when they become available. Note that these imported update packages will not be immediately installed. They will be listed with other uninstalled updates under the Available Updates table
Frequency	This process can be run with a Frequency of hourly, daily (default), or weekly.

Administrator Email Address	Enter the email address of an administrator to be notified via email of new system updates that have automatically been pre-fetched.
Installed Updates	This lists all the updates that have been applied.
Available Updates	This lists all the updates that have been fetched, but which have not yet been installed. Always read the release notes before installing a new system update. To install an unapplied update, click the Install link for that update. Since System Updates must be applied in order, installing a package will also install lower-numbered (earlier revisions) packages automatically, if necessary. Note: System Updates uses FTP to retrieve packages. If SpamTitan is behind a firewall please ensure that FTP access is available. Note: Mail Processing is disabled while installing a system update. Therefore you should apply system updates during non-business hour

Table 6-1 System Update settings

7 Shutting Down the Appliance

The **System Setup > Shutdown Restart** page allows you to shut down or reboot the appliance.



Uptime: 8 days, 1:21

Load Averages: 0.40, 0.26, 0.19

Select Action: :: Please Select ::

Figure 7-1 Shutdown Restart page

The following table describes the fields on this page:

Field	Description
Uptime	The uptime shows how long the system has been running.
Load Averages	The load average shows the load average of the system over the last 1, 5 and 15 minutes respectively.
Select Action	▪ **Logout**: Log out of the user interface ▪ **Shutdown**: shutdown and power off the appliance. This process will take approximately 2 minutes. After the complete shutdown you can safely switch off the appliance. All settings and configuration are saved on shutdown and restart. ▪ **Restart**: Reboot the appliance Note: Access to the user interface will be terminated after Shutdown and during Restart.

Table 7-1 Shutdown Restart settings

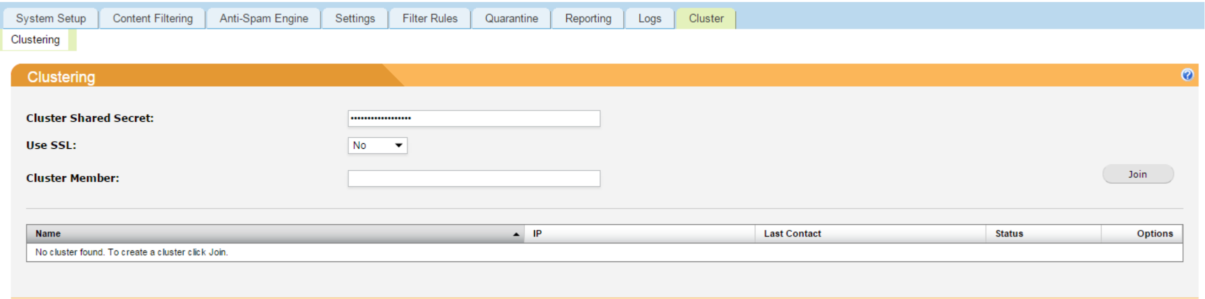
8 Clustering

8.1 Setting up a SpamTitan Cluster

SpamTitan appliances can be clustered to provide load balancing and failover. This chapter explains how to set up a SpamTitan cluster and run reports on a cluster. Note that all non-local settings are automatically replicated across every node in the cluster, but can be individually changed by an administrator.

To setup a cluster:

1. Install SpamTitan on each of the nodes that are to be included in the cluster.
2. Load a valid license on each node. Note: each license must be for an identical number of users (up to 100 users, for example). When using a Production License, the firs node in the cluster must have an STP license and the other nodes must have an STC license. Evaluation licenses may also be used.
3. On the first node, navigate to the **Cluster** menu and enter the **Shared Secret**. Leave the **Cluster Member** blank and click **Join**.



Cluster Shared Secret: ••••••••••••••••••

Use SSL: No

Cluster Member:

Name	IP	Last Contact	Status	Options
No cluster found. To create a cluster click Join.				

Figure 8-1 Cluster setup page

4. Via the **Cluster** menu on the next node to be added, enter the **Shared Secret** and then enter the IP address of the first or primary node into the **Cluster Member** box. Click **Join**.
5. Repeat the steps for each additional node to be added.

8.2 Restrictions and Considerations

The following restrictions and considerations should be noted prior to creating a cluster:

1. SpamTitan does not support geographically dispersed clusters.
2. Communication between nodes is via HTTP and, consequently, this should not be disabled on any of the appliances forming the cluster.
3. A minimum of 1 GB of memory per cluster node is recommended.
4. In the event that one or more nodes are unavailable, both quarantine reporting and cluster wide reporting will be paused until such time as all nodes are againavailable.

9 Content Filtering

This chapter covers the configuration of the Virus detection engines, the Spam engine, and the message attachment filter.

9.1 Virus Filtering

SpamTitan contains integrated virus scanning engines from Clam AV and Kaspersky. Virus scanning with Clam AV and Kaspersky Antivirus is enabled by default, with hourly checks for definition updates.

9.1.1 Clam Anti-Virus

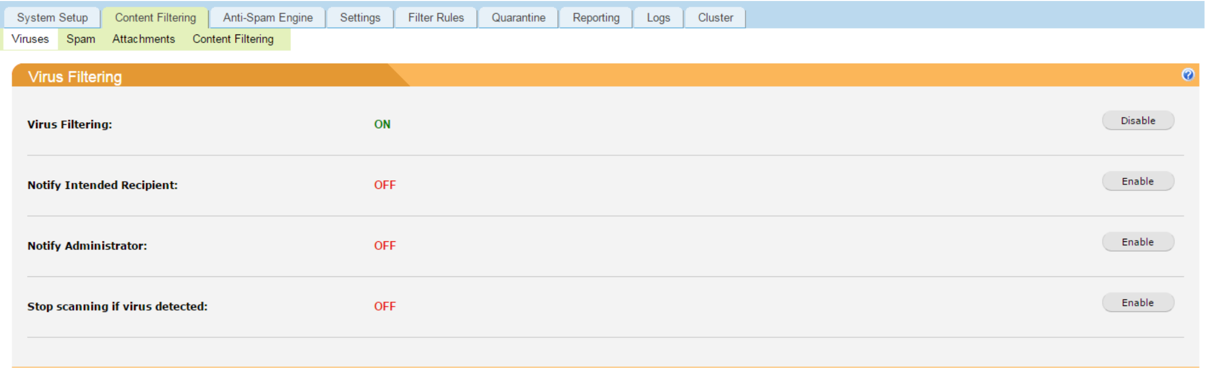
The Clam Antivirus is a powerful, fast, and most importantly accurate virus detection engine that uses a scalable multi-threaded daemon to scan for viruses and viruses. It has built in support for scanning within all archives and compressed files (and also protects against archive bombs).

9.1.2 Kaspersky Anti-Virus

SpamTitan ships with Kaspersky virus scanning engine. You activate the key when you enable Kaspersky on the **Content Filtering > Viruses** page. Once the Kaspersky virus scanner is enabled it will be used in parallel with the Clam Antivirus engine to detect viruses.

9.1.3 Enabling Virus Scanning and Configuring Global Settings

Use the **Content Filtering > Viruses** page to configure the appliance to scan messages for viruses and specify the virus notification settings. If enabled, virus scanning is performed prior to anti-spam scanning.



Virus Filtering: ON

Notify Intended Recipient: OFF

Notify Administrator: OFF

Stop scanning if virus detected: OFF

Figure 9-1 Virus Filtering general settings page

The table below describes the global filtering options:

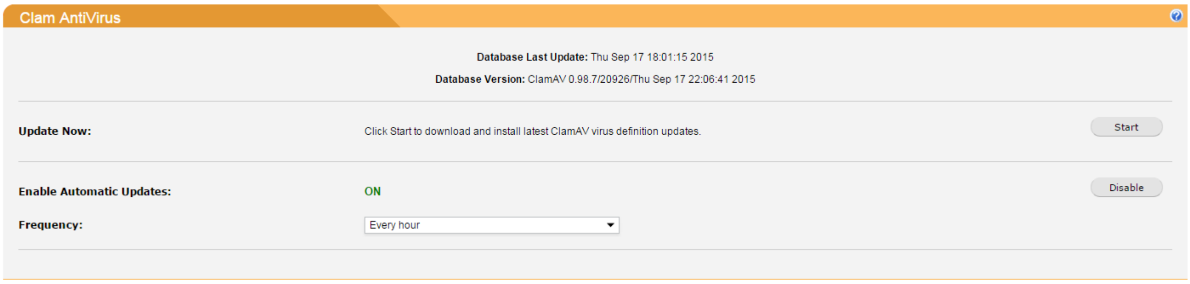
Virus Filtering Options	Description
Virus Filtering	When virus filtering is enabled, all emails are screened for unwanted content like viruses and Trojan horses. **Note**: You can enable/disable virus checking for individual users and/or domains by modifying the policy for that user/domain. Virus Filtering is enabled by default.
Notify Intended Recipient	Enable this option if you want to notify the intended

	Recipient of a virus infected message that their email was blocked via an email notification message. The recommended setting for this is disabled.
Notify Administrator	If you also want to notify an Administrator of a virus then enable this option and enter the email address of the administrator.
Stop scanning if virus detected	If both the Clam AV and Kaspersky Antivirus engines are scanning messages enabling this option will cause SpamTitan to not wait for the second (slower) engine to finish. This option is disabled by default.

Table 9-1 Virus Filtering General settings

9.1.4 Managing Virus Definition Updates

The **Clam** Antivirus engine is the default Antivirus engine for SpamTitan when virus checking is enabled.



Database Last Update: Thu Sep 17 18:01:15 2015

Database Version: ClamAV 0.98.7/20926/Thu Sep 17 22:06:41 2015

Update Now: Click Start to download and install latest ClamAV virus definition updates.

Enable Automatic Updates: ON

Frequency: Every hour

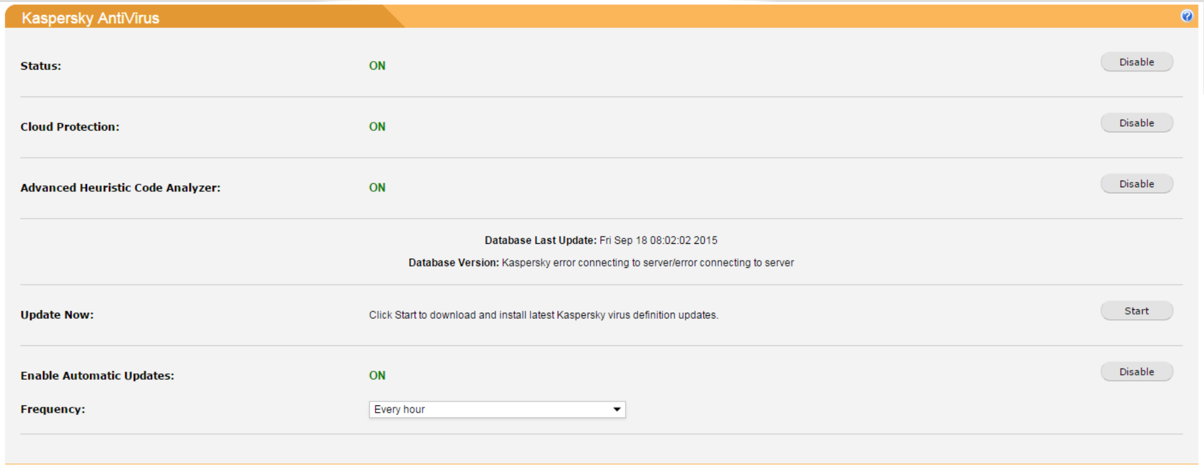
Figure 9-2 Configuring Clam AV settings

The following table describes the Clam Antivirus Update Settings:

Clam Anti-Virus Settings	Description
Database Last Update	Display when last Clam Update applied
Database Version	Displays the version of Clam that is currently running on SpamTitan together with the revision umber for the latest definitions and when these definitions were produced
Update Now	Click **Start** for retrieval and installation of the latest Clam AV virus definition file
Enable Automatic Updates	Determines whether Clam AV definitions are automatically retrieved and applied. Recommended Setting is **ON**. Click Disable to disable automatic updates.
Frequency	The frequency of checks for automatic updates

Table 9-2 Clam AV settings

The **Kaspersky** Antivirus engine is an optional virus scanner that may be run in parallel with Clam AV to provide dual-layer virus protection.



Kaspersky AntiVirus

Status: ON

Cloud Protection: ON

Advanced Heuristic Code Analyzer: ON

Database Last Update: Fri Sep 18 08:02:02 2015

Database Version: Kaspersky error connecting to server/error connecting to server

Update Now: Click Start to download and install latest Kaspersky virus definition updates.

Enable Automatic Updates: ON

Frequency: Every hour

Figure 9-3 Configuring Kaspersky settings

The following table describes the Kaspersky Antivirus Update Settings:

Kaspersky Anti-Virus Settings	Description
Status	Determines if Kaspersky antivirus is enabled or not
Cloud Protection	Enable this option for improved detection of day-zero viruses which utilize the Kaspersky Security Network (KSN) cloud based lookups.
Advanced Heuristic Code Analyser	Heuristic analysis is a method of virus detection which cannot be detected by AV definition files. It allows for the detection of messages, which are suspicious of being infected by unknown or modification of known viruses.
Database Last Update	Displays when SpamTitan last applied the Kaspersky definition updates.
Database Version	Displays the version of Kaspersky that is currently running on SpamTitan together with the revision number for the latest definitions.
Update Now	Click **Start** to check for, retrieve and install the latest Kaspersky virus definition file.
Enable Automatic Updates	Determines if Kaspersky virus definitions are automatically retrieved and applied. Recommended setting is **ON**. Click **Disable** to disable automatic virus updates.
Frequency	Determines the frequency with which SpamTitan will check for updates. Hourly is recommended.

Table 9-3 Kaspersky settings

9.2 Spam Filtering

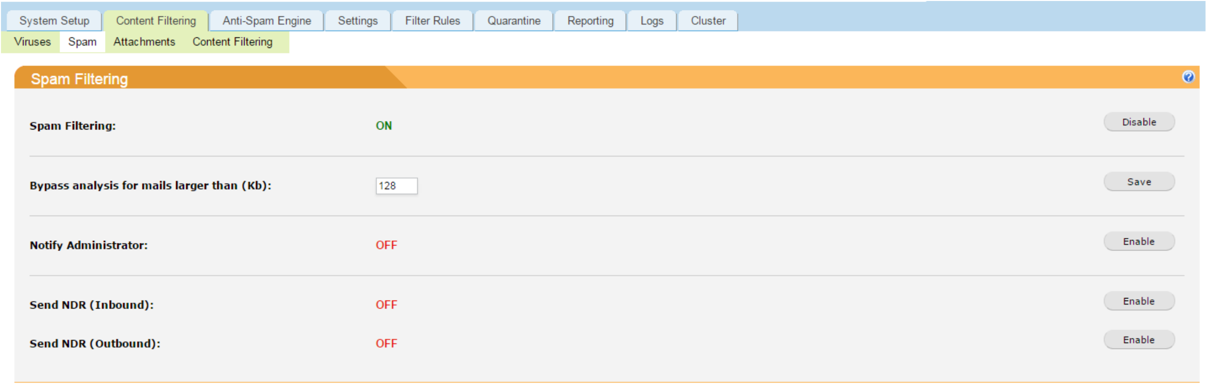
SpamTitan uses a multi-layered approach to eliminating spam at the email gateway. This cocktail approach of determining if a message is spam ensures that there are a minimum number of false positives (i.e. clean mail misclassified as spam). A spam score is assigned to each message which is calculated by combining the scoring from each layer of the message. The following tests are performed on each message:

- Harvesting/Dictionary attack protection
- Collaborative Spam Fingerprint checks
- RBL tests
- SURBL tests
- Bayesian Analysis
- Rule based spam scoring
- Whitelist/Blacklist filters

You can see a messages spam score in the Reporting message history page of the user interface. It can also be see in the X-Spam-Score and X-Spam-Status messages that are added to all inbound mail messages.

9.2.1 Enabling Spam Scanning and Configuring Global Settings

Use the **Content Filtering > Spam** page to configure the appliance to scan messages for spam and specify the spam notification settings.



Spam Filtering: ON

Bypass analysis for mails larger than (Kb): 128

Notify Administrator: OFF

Send NDR (Inbound): OFF

Send NDR (Outbound): OFF

Figure 9-4 Spam Filtering settings page

The following table describes the Spam Filtering options:

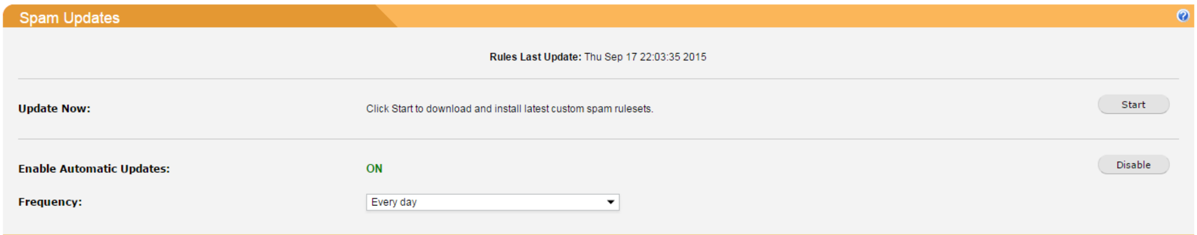
Spam Filtering Options	Description
Spam Filtering	When spam filtering is enabled, all emails are screened for spam. **Note**: You can enable/disable spam scanning for individual users and/or domains by modifying the policy for that user/domain. Spam Filtering is enabled by default.
Bypass analysis for mails larger than	Spam messages by their nature are typically small. To save on CPU resources there is no need to scan messages above a certain size. The spam scanning engine is not called when the message body is greater than 128kb (default).

Notify Administrator	If you want to notify an Administrator of a spam then enable this option and enter the email address of the administrator. This option is disabled by default.
Send NDR (Inbound)	Enable this option to send Non Delivery Reports (NDRs) to senders when the appliance blocks spam messages. This will send an NDR to external senders. As sender addresses are easily spoofed enabling these settings can lead to backscatter. Backscatter occurs when a bounce message is delivered to an innocent user from whom the spam message did not originate, and may lead to increased load on the appliance.
Send NDR (Outbound)	Enable this option to send Non Delivery Reports (NDRs) to senders when the appliance blocks spam messages. This will send an NDR to internal senders. As sender addresses are easily spoofed enabling these settings can lead to backscatter. Backscatter occurs when a bounce message is delivered to an innocent user from whom the spam message did not originate, and may lead to increased load on the appliance.

Table 9-4 Spam Filtering settings

9.2.2 Spam Rule Updates

Content Filtering > Spam > Spam Updates allows you to manually update the current spam definitions, as well as change the interval that SpamTitan checks for updates.



Spam Updates

Rules Last Update: Thu Sep 17 22:03:35 2015

Update Now: Click Start to download and install latest custom spam rulesets.

Enable Automatic Updates: ON

Frequency: Every day

Figure 9-5 Spam Update settings page

The following table describes the Spam Updates fields:

Spam Update Settings	Description
Rules Last Update	Displays when SpamTitan last updated the spam rule definitions.
Update Now	Click **Start** to check for, retrieve and install the latest SpamTitan anti-spam rule definitions.

Enable Automatic Updates	Determines if SpamTitan anti-spam rule definitions are automatically retrieved and applied. Recommended setting is **ON**. Click **Disable** to disable automatic spam rule updates.
Frequency	Determines the frequency with which SpamTitan will check for updates. The recommended setting is daily – ensuring that your appliance is always up-to-date with the latest spam rule definitions.

Table 9-5 Spam Update settings

9.3 Attachment Filtering

The Attachment filter facility can reject or quarantine mails which contain certain types of files based on their extensions (e.g. executable files) and/or their MIME types. If any mail part matches, the whole mail is rejected.

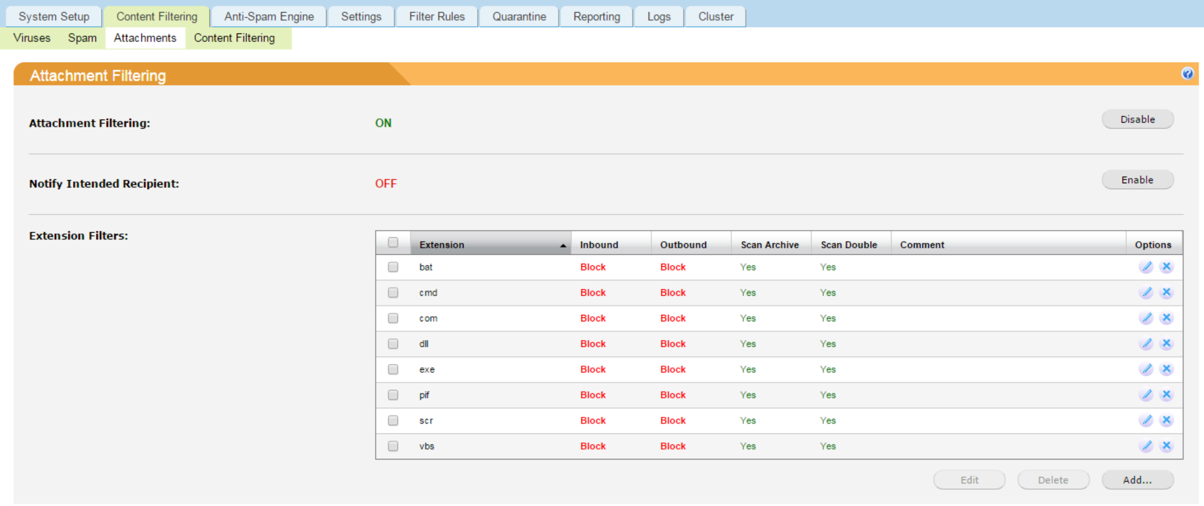
The Attachment filters can identify file attachments using a number of different methods, and also automatically scans compressed archive files.

9.3.1 Extension Filters

Using the messages MIME headers, the attachment filter can extract each file attachments extension, and apply filter decision based on the listed extensions.

This will not recognize files correctly if the sender modified the filename. For example, if a win32 executable has been renamed photo.jpg, an exe extension will not detect it. For cases like this it is necessary to also use the File Type Filters and/or MIME Type filters. You may also select the **Scan Double Extensions** to identify files which may have been renamed in an attempt to obfuscate their true identity. Double extensions are often used to trick users into opening malware. Often mail clients such as Outlook may hide the second extension so filename.gif.exe may appear as an ordinary filename.gif file.

Only alpha numeric characters are allowed for filename extensions.



Attachment Filtering: ON

Notify Intended Recipient: OFF

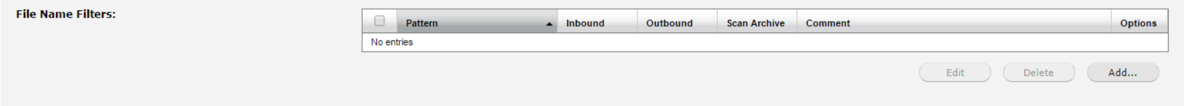
Extension Filters:

□	Extension	Inbound	Outbound	Scan Archive	Scan Double	Comment	Options
□	bat	Block	Block	Yes	Yes		✎ ✕
□	cmd	Block	Block	Yes	Yes		✎ ✕
□	com	Block	Block	Yes	Yes		✎ ✕
□	dll	Block	Block	Yes	Yes		✎ ✕
□	exe	Block	Block	Yes	Yes		✎ ✕
□	pif	Block	Block	Yes	Yes		✎ ✕
□	scr	Block	Block	Yes	Yes		✎ ✕
□	vbs	Block	Block	Yes	Yes		✎ ✕

Figure 9-6 Attachment Filtering page

9.3.2 File Name Filters

Using the messages MIME headers, the attachment filter can extract each file attachments filename, and apply the filter decision based on the listed filenames. Use the asterisk sign (*) to match zero or more characters; use the question mark sign (?) to match a single character. For instance, to filter all executable attachments that include the word sample, create a filter *sample*.exe.



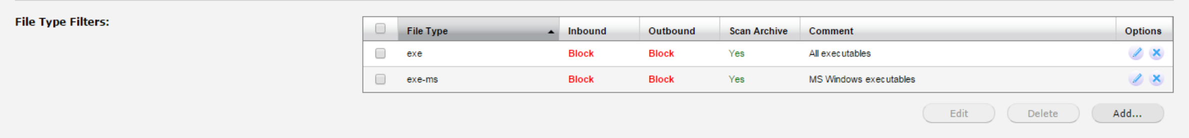
File Name Filters:

□	Pattern	Inbound	Outbound	Scan Archive	Comment	Options
No entries						

Figure 9-7 Attachment Filtering - File Name Filters

9.3.3 File Type Filters

SpamTitan will scan each attachment to determine its file type. If this matches any of those listed in the File Type Filters table, then the message will be filtered accordingly. This is useful in preventing users changing an attachments extension in order to try and circumvent the filters. For instance, an executable attachment will get blocked even if the file itself has a .txt extension.



File Type Filters:

□	File Type	Inbound	Outbound	Scan Archive	Comment	Options
□	exe	Block	Block	Yes	All executables	✎ ✕
□	exe-ms	Block	Block	Yes	MS Windows executables	✎ ✕

Figure 9-8 Attachment Filtering - File Type Filters

The following file types are recognized:

Miscellaneous	
txt	ASCII text file
pgp	PGP file
swf	Macromedia Flash file
uue	uuencoded file
hqx	binhex file
asc	ASCII file
Image Files	
pcx	PCX image file
bmp	PC bitmap file
jpg	JPEG image file
gif	GIF image file
png	PNG image file
tiff	TIFF image file
Audio Files	
mp2	MP2 file
mp3	MP3, MPEG ADTS, layer III file
m4a **m4b**	ISO Media, MPEG v4 system

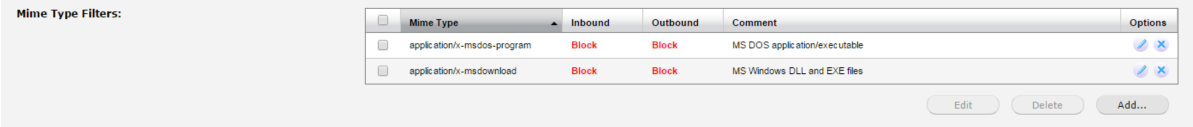
Compressed Archive Files	
zip	Zip archive
a	current ar archive
rar	RAR archive
lha	LHa archive
arc	ARC archive
arj	ARH archive
zoo	Zoo archive
tar	GNU/POSIX tar archive
cpio	ASCII cpio archive
tnef	Transport Neutral Encapsulation Format (TNEF) file
sit	StuffIt archive
deb	Debian binary package
cab	Microsoft cabinet file
F	frozen
gz	gzip compressed file
bz	bzip compressed file
bz2	bzip2 compressed file

flac	FLAC audio bitstream data
oga/ogg	Ogg data, FLAC audio
wav	WAVE audio
Executables	
exe-ms	MS-DOS or MS Windows executable
exe-unix	Unix (RISC, ELF, COFF) executable
exe-vms	VMS executable
exe	MS-DOS, MS Windows, VMS or Unix executable
Movie Files	
mpv	MPEG video stream data
mpg	MPEG system stream data
mkv	Matroska data
wmv	Microsoft ASF
avi	AVI file
ani	Animated cursor
xz	xz compressed file
lzma	lzma compressed file
lzo	lzop compressed file
Z	compressed file
7z	7-zip archive
Document Files	
ps	Postscript file
pdf	PDF file
rtf	Rich Text Format file
doc	Microsoft Office file
lat	LaTeX file
dvi	TeX DVI file
java	Compiled Java class file
html	HTML document
xml	XML document
sgml	exported SGML document

Table 9-6 Recognized File Types

9.3.4 Mime Type Filters

The Mime Type is the file type as reported in the MIME Content- Disposition and Content-Type headers, both in their raw (encoded) form and in rfc2047- decoded form if applicable. It consists of a general type and a specific type indicator; for instance image/png, video/avi or text/html.



Mime Type Filters:

□	Mime Type	Inbound	Outbound	Comment	Options
□	application/x-msdos-program	Block	Block	MS DOS application/executable	
□	application/x-msdownload	Block	Block	MS Windows DLL and EXE files	

Figure 9-9 Attachment Filtering - Mime Type Filters

9.3.5 Compressed Archive File Scanning

The attachment scanner will automatically scan files inside of compressed archive files such as .zip and .gz files. For each of the Extension, File Name, and File Type filters, you can specify if the filter should apply to files contain in archives or not using the Scan Archive setting.

9.3.6 Password Protected Archives

Password protected archives are archives (zip, bz2, tar, etc.) which require a password in order to open, and as such cannot be inspected for viruses. Specify to allow, block or quarantine password protected archives. If you choose to allow password protected archives, then you may prepend the subject with a tag containing the contents of the Modify Subject field. Leave empty to leave the subject unmodified. Note: Modification of the subject will only occur if the recipient is local.

9.3.7 Configuration

A mail containing attachments will only be blocked as containing a banned attachment if the attachment, or any of its decoded components, match the listed filters. Before creating filters, use the Attachment Filtering option, to enable filtering.

The creation of attachment filters is always performed at the global level; however domain and/or user policies can further control if attachment filtering should be applied for that domain or user, and what action to be performed if a banned attachment is discovered.

If you want to notify the intended Recipient of blocked mails due to banned attachment filtering then Enable the **Notify Intended Recipient** option.

To create a new attachment filter, click on the **Add...** button. The **Add Filter dialog** is displayed.

Each different filter type in this section has largely the same settings the differences will be mentioned in the below table.

Field	Description
Extension/File Name **File Type/Mime Type**	File extension, filename, file type or mime type
Inbound Action	The action to take for inbound messages that match this filter. Options available are: ▪ **Allow**: Allow the message. ▪ **Block**: Block the message. The domain or user policy will dictate if the message is quarantined. ▪ **Ignore**: Perform no filtering.
Outbound Action	The action to take for outbound messages that match this filter. Options available are: ▪ **Allow**: Allow the message. ▪ **Block**: Block the message. The domain or user policy will dictate if the message is quarantined. ▪ **Ignore**: Perform no filtering.
Scan Archives	Indicates if the filter should match files contained within compress archive files.
Scan Double Extensions	Indicates if the filter should match files containing multiple extensions. For instance, an attachment report.txt.exe or “image.png. exe” (note the spaces) would match an extension filter for exe if this option is enabled.
Comment	Optional comment field for filter

Figure 9-10 Add/Edit Filter dialog settings

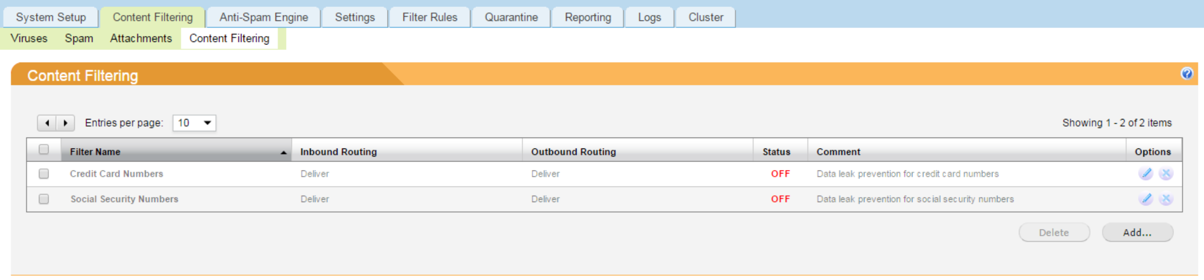
9.4 Content Filtering

The Content Filters feature in SpamTitan allows you to create custom content filters for both inbound and outbound email, and take an action on any messages that contains that content. For example, you can use the Content Filters to redirect all messages containing a particular pattern in the subject to an encryption server.

Note: Each message header or message body line is compared against the content filter rules line by line. When a match is found the corresponding action is executed, and the matching process is repeated for the next message header or message body line.

Note: Message headers are examined one logical header at a time, even when a message header spans multiple lines. Body lines are always examined one line at a time.

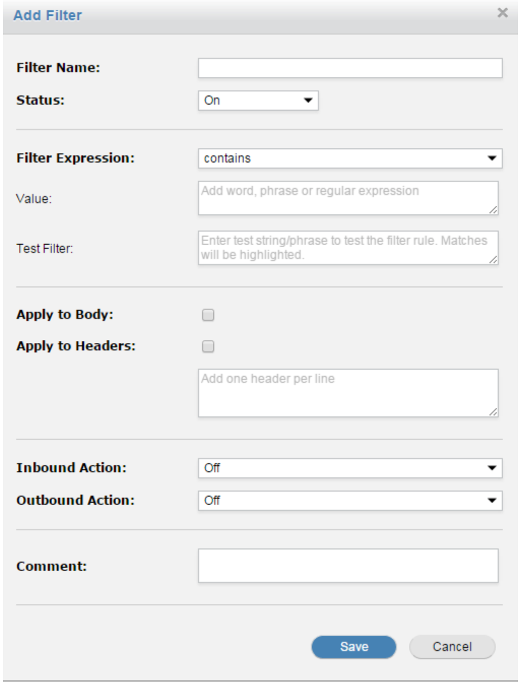
The Content Filtering page shows a list of all predefined and custom content filters that may have been created:



□	Filter Name	Inbound Routing	Outbound Routing	Status	Comment	Options
□	Credit Card Numbers	Deliver	Deliver	OFF	Data leak prevention for credit card numbers	
□	Social Security Numbers	Deliver	Deliver	OFF	Data leak prevention for social security numbers	

Figure 9-11 Content Filtering page

To create a new custom content filter, click on the **Add...** button. The Add Filter dialog is displayed.



Filter Name:	
Status:	On
Filter Expression:	contains
Value:	Add word, phrase or regular expression
Test Filter:	Enter test string/phrase to test the filter rule. Matches will be highlighted.
Apply to Body:	□
Apply to Headers:	□ Add one header per line
Inbound Action:	Off
Outbound Action:	Off
Comment:	

Figure 9-12 Add/Edit Content Filter dialog

The entries on the Add/Edit Filter dialog are as follows:

Field	Description
Filter Name	Descriptive name for the filter policy.
Status	Select ON or OFF to enable this filter policy.
Filter Expression	Create/edit a filter rule where the message content for the specified location: ▪ **starts with**: Begins with the specified value ▪ **ends with**: Ends with the specified value. ▪ **contains**: Contains the specified value. This option will match whole words and parts of words. For example, if the value specified is sex, and the rule is to be applied to the message body, if the body contains the word sex or unisex then the rule will match. To match messages with just the word sex, without matching unisex use the *matches any word* in or the *matches regular expression* filter options. ▪ **equals**: Contains only the specified value. For example, if the value specified is Free hotel rooms and the filter is to be applied to the Subject: header, then the filter will match only if the subject contains the text Free hotel rooms, and no other text. ▪ **matches any word in**: Contains any of the words listed in the specified value. Separate words with spaces. ▪ **matches regular expression**: Matches the specified regular expression value. See Using Regular Expressions below, for more information on writing regular expressions.
Value	Enter the content which should be scanned for in messages. If you selected a filter type of **starts with**, **ends with**, **contains** text, **equals** or **matches any word** in: ▪ The value must be a word or phrase. ▪ The value is not case sensitive. If you selected a filter type of matches regular expression: ▪ The value can be a regular expression. Use regular expressions to scan messages for text patterns rather than specific words or phrases. ▪ The regular expression syntax is validated as you type. If the syntax is invalid, then the Value field containing your regular expression will be highlighted in red. See **Using Regular Expressions** for more information

	on writing regular expressions.
Test Filter	Enter sample message text here to test if your filter expression is correct and matches. If the filter rule matches the text entered, then then Test Filter field will be highlighted in green.
Apply to Body	If you want the rule to apply to the body of the message, select this checkbox.
Apply to Headers	If you want the rule to apply to the message headers, select this checkbox and enter the headers that the rule should apply to. For instance, if you want the rule to apply to the Subject, enter *Subject*, or *Subject:*. The rule will match if it is found in any of the specified headers. If you want the filter rule to be applied to all headers, then leave this field blank.
Inbound/Outbound Action	The Inbound/Outbound action specifies the action to be taken on a message that matches the filter rule. You can specify different actions for both inbound and outbound messages. The following actions are available: ▪ **Delete**: Discards the message, with no notification to the sender or recipient. ▪ **Redirect to Relay**: Route/relay the message to a different SMTP relay host. For the Relay field, enter the fully qualified hostname or IP address of the relay host. Specify a domain, host, host:port, [host]:port, [address] or [address]:port; the form [host] turns off MX lookups. ▪ **Redirect to User**: Route/redirect the message to the specified email address. In the User field, enter the email address of the intended recipient. The message will be sent to this address instead of the intended recipient(s). Note: this action affects all recipients of the message. ▪ **Bounce**: Reject the message. Sender will receive a bounce message. ▪ **Whitelist**: Send the message to the intended recipient(s) bypassing all spam checking. ▪ **Quarantine**: Quarantine the message. The message will not be delivered. ▪ **Off**: Disable the rule.
Comment	Optional comment field

Table 9-7 Add/Edit Content Filter dialog settings

9.4.1 Predefined Filters

Two predefined content filters for Data Loss Prevention (DLP) are included:

- **Credit Card Numbers**: Use this filter to scan messages for content matching credit card numbers. Messages containing Visa, MasterCard, and Discovery, American Express or Diners Club card numbers will be subject to the chosen action.

- **Social Security Numbers**: Use this filter to scan messages for U.S. social security numbers. Messages containing social security numbers matching the pattern nnn-nn-nnnn will be subject to the chosen action. The pattern checks for valid social security numbers by ensuring that the pattern cannot contain a group of digits that are all 0s, such as in 000-11-1111, 111-00-1111, or 111-11-0000.

The filters are designed to match most formats for representing credit card numbers and social security numbers. However, since numbers can be formatted in multiple ways, the filter patterns may not catch all messages that contain credit card numbers or social security numbers. In addition, since the pattern looks for specific patterns of numbers, it is possible that numeric patterns that are not credit card numbers or social security numbers may be matched.

9.4.2 Using Regular Expressions

Regular expressions are a standard tool used in many scripting languages and provide a powerful pattern matching tool to allow creation of filters that can match patterns of text rather than only single words or phrases. Regular expressions consist of a combination of special characters called meta-characters and alphanumeric text characters.

The Content Filtering in SpamTitan uses Perl Compatible Regular Expression (PCRE) regular expressions. For more detailed information on syntax see:

- www.regular-expressions.info
- www.pcre.org

9.4.3 Regular Expression Examples

The following examples show the use of some simple regular expression constructs

Match email from a specific domain	
Match criteria	Match any email address from the domains example.com and example.net
Regular expression	(\W|^)[\w.+\-]{0,25}@example\.(com|net)(\W|$)
Details	▪ \W matches a non-alphanumeric character. It prevents the regular expression from matching characters before or after the email address. ▪ ^ matches the start of a line. ▪ $ matches the end of a line. ▪ [\w.+\-] matches any word character (in the range 0-9, A-Z and a-z), a period, a plus sign or a hyphen. ▪ The \ character escapes the period and the hyphen to indicate that these should not be treated as meta-characters. ▪ {2,30} matches when the preceding character occurs at least 2 times but not more than 30 times, for example, fo{1,2}bar will find fobar and foobar but not fooobar. ▪ The brackets group com and net, and the | that separates them indicates that they are conditional.

Table 9-8 Regular Expression examples 1

Match string containing IP addresses in the 192.168.1.0/24 netblock	
Match criteria	Match any IP address in 192.168.1.0/24 CIDT address (i.e. 192.168.1.0-192.168.1.255)
Regular expression	(\W|^)192\\.168\\.1\\.([1-9]|[1-9][0-9]|1([0-9][0-9])|2([0-4][0-9]|5[0-5]))(\W|$)
Details	▪ \W matches a non-alphanumeric character. It prevents the regular expression from matching characters before or after the IP address. ▪ ^ matches the start of a line. ▪ $ matches the end of a line. ▪ The \ before each period escapes the period, indicating that the period is not a regular expression meta-character. ▪ For the final octet of the IP address we must match 1-255; the | character separates the various options. • [1-9] • [1-9][0-9] • 1([0-9][0-9]) • 2([0-4][0-9]|5[0-5])

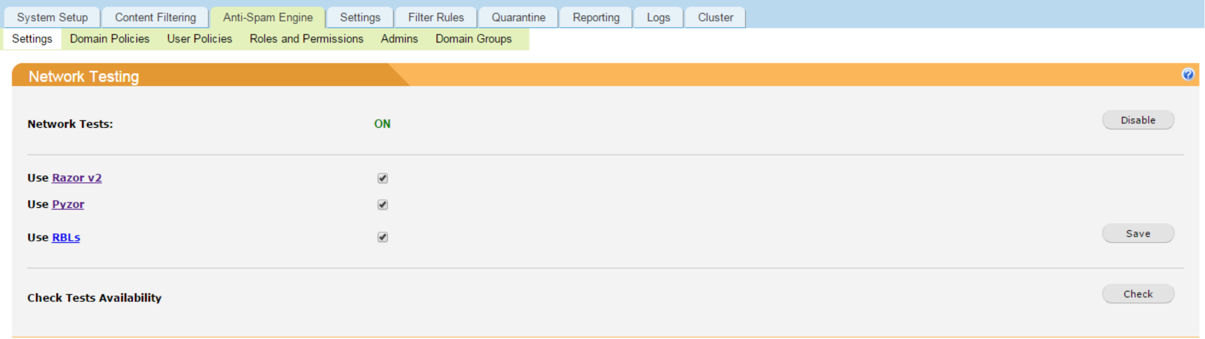
Table 9-9 Regular Expression examples 2

10 Anti-Spam Engine - Settings

The **Anti-Spam Engine > Settings** page allows you to manage the general settings for the anti-spam engine.

10.1 Network Testing

SpamTitan uses a number of network based tests when determining the spam score for a message.



Network Tests: ON

Use Razor v2 ☑

Use Pyzor ☑

Use RBLs ☑

Check Tests Availability

Figure 10-1 Network Settings page

Razor and **Pyzor** are distributed, collaborative, spam detection and filtering networks that uses statistical (e.g. volume of recipients) and randomized fuzzy checksums to efficiently spot mutating spam content. These databases are continuously updated with new spam messages. Both checks are enabled by default.

- Razor: requires outbound access to TCP port 2703.
- Pyzor: requires outbound access on TCP and UDP port 24441.

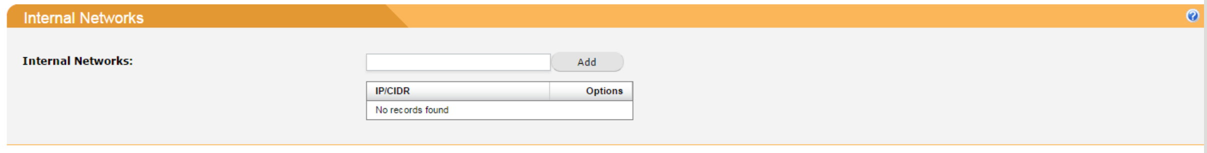
Realtime Blackhole Lists (RBLS) are used to check if an incoming message has passed through one or more machines which are blacklisted as spam sources or relays. These DNS blocklists are a common form of network-accessible database used in spam detection. Unlike the RBLs used by the MTA, the results of these checks simply contribute to the final spam score for a message. RBLs require DNS access which must be available.

Note: Network tests all require access to their servers through your firewall in order for these tests to operate. See Appendix A – Firewall Information for more information on what ports may need to be opened on your firewall for proper operation.

Click the Check button to check access to these network services. Note also that the remote Pyzor and Razor servers may be temporarily unavailable. If this happens and these tests are enabled then there will be a short delay in the processing of each message while these services timeout (10 seconds).

10.2 Internal Networks

The Spam engine will automatically attempt to figure out which Received: headers were inserted by trustworthy mail servers or relays, and which were not. This allows it to optimize RBL lookups, detect when mails never left a trusted network path, and increase spam scoring accuracy.



Internal Networks

Internal Networks:

IP/CIDR	Options
No records found	

Figure 10-2 Internal Networks page

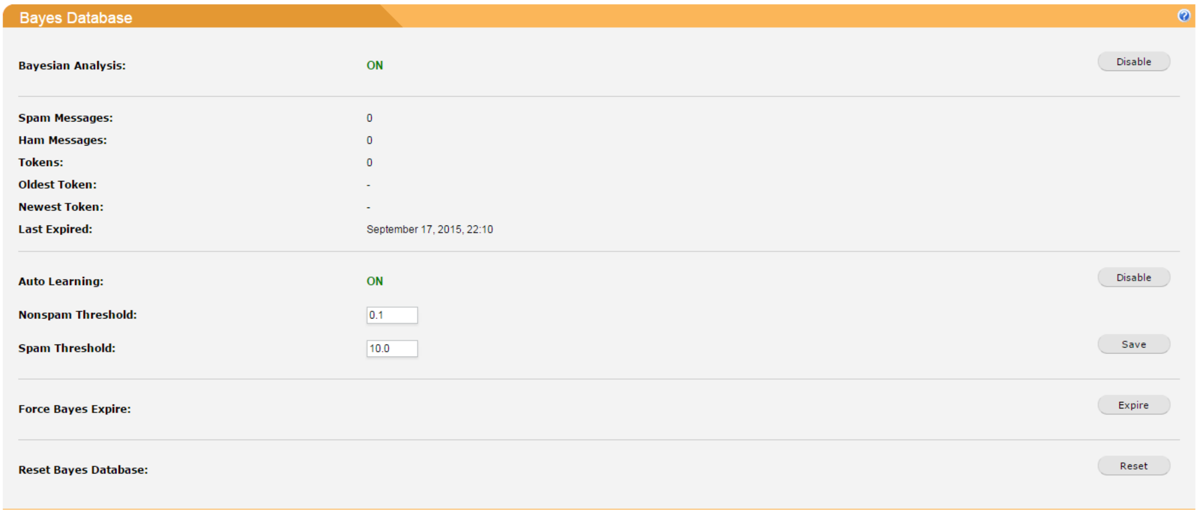
Internal Networks should include all hosts that act as an MX for your domains, or that may deliver mail internally in your organization. If SpamTitan is the MX for your organization then you may leave this as the default (127.0.0.1). For instance, if mail entering your organization is first processed by another server before being relayed to SpamTitan then it should appear in this list. Also if an internal mail server is relaying mail out of your organization then its IP address should appear in the list.

These settings will aid the spam engine in performing some tests better, increase accuracy, and reduce load.

Entries may be specified as a single host or as a network specified in CIDR (Classless Inter-Domain Routing) format.

10.3 Bayesian Database

SpamTitan contains a Bayesian classifier which tries to identify spam by looking at what are called tokens; words or short character sequences that are commonly found in spam or clean messages. For instance, if the Bayesian database has learned 100 messages with the phrase penis enlargement, the Bayesian code is pretty sure that a new message that contains that phrase is spam and as such raises the spam score of that message.



Bayes Database

Bayesian Analysis: ON

Spam Messages: 0
Ham Messages: 0
Tokens: 0
Oldest Token: -
Newest Token: -
Last Expired: September 17, 2015, 22:10

Auto Learning: ON
Nonspam Threshold: 0.1
Spam Threshold: 10.0

Force Bayes Expire:

Reset Bayes Database:

Figure 10-3 Bayesian Database page

The following table explains the various Bayesian Database settings that are found on the **Anti-Spam Engine > Settings** page:

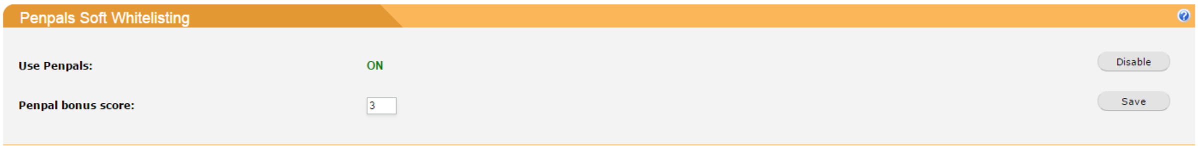
Bayesian Database Settings	Description
Bayesian Analysis	Shows if Bayesian analysis is enabled. Enabled by default.
Spam Messages	This field indicates the number of mail messages that have been learned as spam by the Bayesian classifier.
Ham Messages	This field indicates the number of mail messages that

	have been learned as clean messages by the Bayesian classifier.
Tokens	This is the total number of individual tokens that the Bayesian classifier has learnt.
Oldest Token	Indicates the date of the oldest token in the Bayesian database.
Newest Token	Indicates the date of the newest token in the Bayesian database.
Last Expired	Indicates when tokens were last expired from the database.
Auto Learning	If auto learning is enabled the anti-spam engine will automatically feed high-scoring (or low-scoring mails for non-spam) into the Bayesian classifier. If auto learning is disabled then messages will only be learned when users confirm spam from their quarantine reports or release messages (false positives). Auto Learning is Enabled by default.
Nonspam Threshold	This field indicates the score threshold below which a message has to score before the anti-spam engine will feed it into the Bayesian classifier as a clean message. Default is 0.1
Spam Threshold	This field indicates the score threshold above which a message must score before the anti-spam engine will feed it into the Bayesian classifier as a spam message. Default value is 10.0. Note: The spam engine requires that the message score at least 3 points from the message headers and 3 points from the message body to auto learn the message as spam. Therefore the minimum working value for this setting is 6.
Force Bayes Expire	In order to prevent the Bayesian database from growing too big, tokens are automatically expired from the database when certain criteria are met: ▪ The last expire was attempted at least 12 hours ago. ▪ The number of tokens in the database > 100,000 ▪ There is at least a 12 hour difference between the oldest and newest token times. Use this option to force an expiry attempt of the Bayesian database, regardless of whether it may be necessary or not. The above criteria will be used to decide if tokens are actually expired or not.
Reset Bayes Database	This option resets the Bayesian database and clears the database of all tokens.

Table 10-1 Bayesian Database settings

10.4 Penpals Soft Whitelisting

Penpals soft-whitelisting lowers the spam score of received replies to a message previously sent by a local user to this address. This can be useful in preventing potential false positives from email addresses that users are in frequent contact with.


Penpals Soft Whitelisting

Use Penpals: ON

Penpal bonus score: 3

Figure 10-4 Penpals page

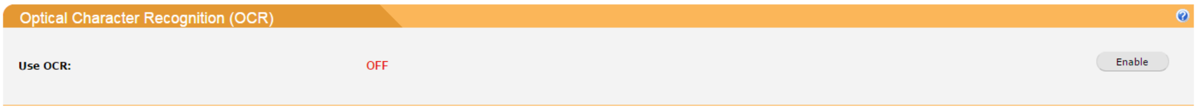
When a message is received, SpamTitan checks if a message was sent in the reverse direction, i.e. from a local user (which is now a recipient of the current mail) to the address that is now the sender of the message being processed. If any such message exists, then the age (seconds since the most recent message) is used to calculate an exponential decay score to be deducted from the spam engine score. The more recently the message has arrived the bigger the decay

Note that penpals soft-whitelisting aids incoming mail, and internal-to-internal mail, but has no effect on outgoing mail. The following table describes the Penpal settings:

Penpal settings	Description
Use Penpals	Indicates if penpals is enabled or not. Default is OFF. If you are using SpamTitan to process outbound email, then it is recommended to enable penpals.
Penpal bonus score	This field indicates the maximum score deducted when a message is received from a penpal (i.e. when the sender is known to have previously received mail from our local user from SpamTitan). A setting of zero (0) will disable the penpals feature. Default is 3.

Table 10-2 Penpals settings

10.5 Optical Character Recognition

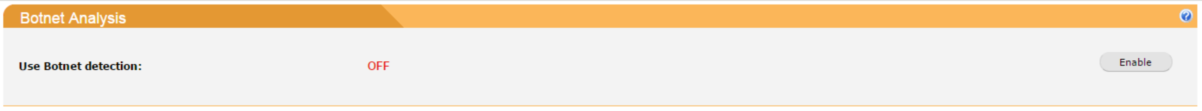

Optical Character Recognition (OCR)

Use OCR: OFF

Figure 10-5 OCR settings page

The use of Optical Character Recognition software allows SpamTitan to scan embedded images in email and protect from image-only based spam, which may otherwise go undetected. By using OCR, SpamTitan can use the text contained within an image to assign a spam score to the message. OCR scanning can be quite CPU intensive, and as such the use of OCR will add a couple of seconds to the processing time for each message which contains an embedded image. For busy servers with scarce system resources it may be desirable to disable OCR scanning.

10.6 Botnet Analysis



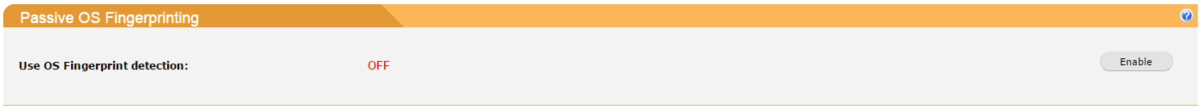
Botnet Analysis

Use Botnet detection: OFF

Figure 10-6 Botnet settings page

When enabled, DNS validation is performed on the first relay looking for signs of a potentially botnet infected host. For example, no reverse DNS, a hostname that would indicate an ISP client, or other hosts that aren't intended to be acting as a direct mail submitter outside of their own domain.

10.7 Passive OS Fingerprinting



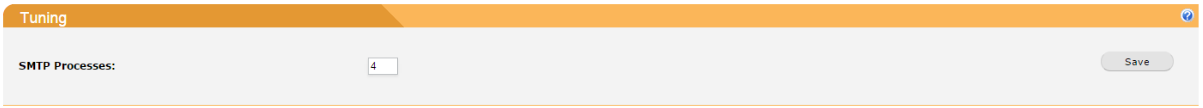
Passive OS Fingerprinting

Use OS Fingerprint detection: OFF

Figure 10-7 Passive OS Fingerprinting page

Passive OS Fingerprinting is a plug-in which allows SpamTitan to identify the operating system of the connecting SMTP client with reasonable accuracy. Most spam originates from the compromised Windows desktop systems. It is called passive since SpamTitan simply sniffs the network traffic as it goes by. This allows us to penalize Windows XP operating systems and reward UNIX operating systems. While OS fingerprinting can never be completely accurate, it does a very good job at identifying most Windows SP systems. Note, however that NAT routers and firewalls can make some systems unidentifiable. Also, SpamTitan will only be able to identify the OS of the last hop client- so if a spam message is relayed through one of your own relays before reaching SpamTitan, then the results would be those of the relay and not the originating SMTP spam client.

10.8 Performance Tuning



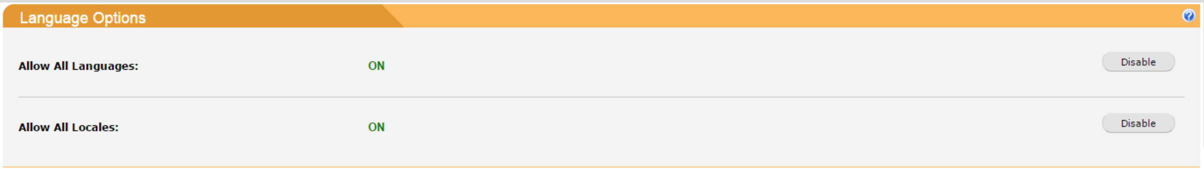
Tuning

SMTP Processes: 4

Figure 10-8 Performance Tuning page

The number of SMTP Processes determines how many parallel processes can be run to process mail. The default of 5 processes is suitable for most organizations, however for some organizations with a large throughput of email may need to increase this setting. Each process consumes quite a bit of memory, so the memory available can determine how may processes you can run before swapping occurs. If you increase this setting too high and the appliance starts swapping, or the load regularly goes beyond 3 then you should decrease this setting. Going beyond 10 usually brings no more improvement in overall-system throughput, it just wastes memory and could possibly degrade performance.

10.9 Language Options



Language Options

Allow All Languages: ON

Allow All Locales: ON

Figure 10-9 Language Options page

The language and locale settings on the **Anti- Spam Engine > Settings** page allows you to specify which languages and locales (country codes) are considered OK to receive mail from.

The following table describes the language options:

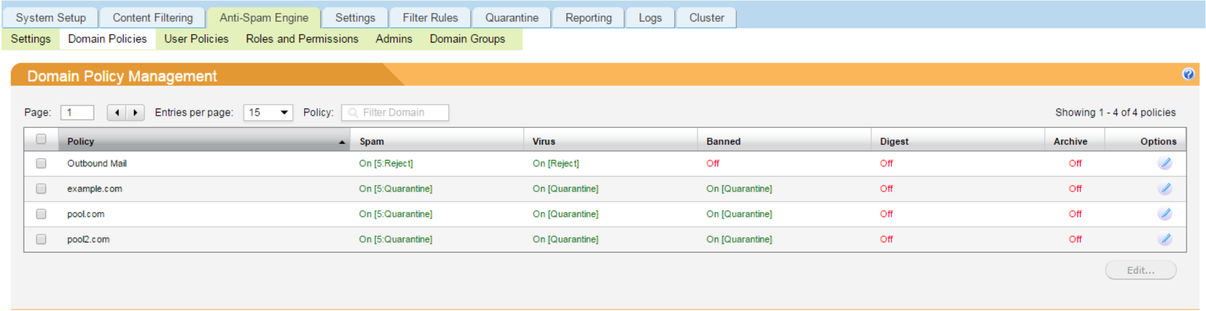
Field	Description
Allow All Languages	This field specifies which languages are considered OK to receive email from. Mail using character sets used by these languages will not be marked as possibly been spam in an undesired language. The default value is to allow all languages. **Note**: The language cannot always be recognized with sufficient confidence, in which case no score will be assigned to that test.
Allow All Locales	This field specifies which locales (country codes) are considered OK to receive email from. Mail using character sets used by languages in these countries, will not be marked as possibly being spam in a foreign language. If you receive lots of spam in foreign languages, and never get any non-spam in these languages, this may help. Note that all ISO-8859-* character sets, and Windows code page character sets are always permitted. The default value is to allow all locales.

Table 10-3 Language Options settings

11 Anti-Spam Engine – Policies

11.1 Domain Policies

SpamTitan contains extensive content scanning and message filtering capabilities that allows you to enforce corporate policies on all messages that enter or leave your organization on a per-domain or per-recipient basis.



Domain Policy Management

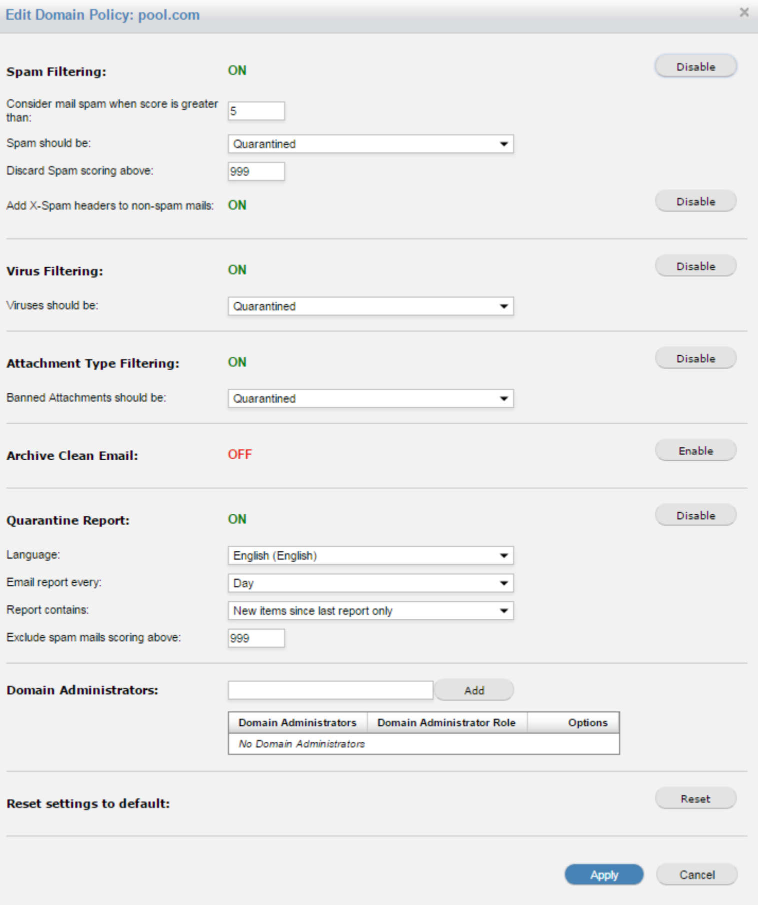
Page: 1 Entries per page: 15 Policy: Filter Domain Showing 1 - 4 of 4 policies

□	Policy	Spam	Virus	Banned	Digest	Archive	Options
□	Outbound Mail	On [5:Reject]	On [Reject]	Off	Off	Off	✎
□	example.com	On [5:Quarantine]	On [Quarantine]	On [Quarantine]	Off	Off	✎
□	pool.com	On [5:Quarantine]	On [Quarantine]	On [Quarantine]	Off	Off	✎
□	pool2.com	On [5:Quarantine]	On [Quarantine]	On [Quarantine]	Off	Off	✎

Figure 11-1 Domain Policies page

For each new domain that is added a default policy is automatically created. Therefore any mail to a user within that domain will use the policy for that domain; although a different user based policy may be created for users.

Anti-Spam Engine > Domain Policies allows you to manage the per-domain policy settings. These domain settings will be inherited by all users in those domains.



Edit Domain Policy: pool.com

Spam Filtering: ON

Consider mail spam when score is greater than: 5

Spam should be: Quarantined

Discard Spam scoring above: 999

Add X-Spam headers to non-spam mails: ON

Virus Filtering: ON

Viruses should be: Quarantined

Attachment Type Filtering: ON

Banned Attachments should be: Quarantined

Archive Clean Email: OFF

Quarantine Report: ON

Language: English (English)

Email report every: Day

Report contains: New items since last report only

Exclude spam mails scoring above: 999

Domain Administrators:

Domain Administrators	Domain Administrator Role	Options
No Domain Administrators		

Reset settings to default:

Figure 11-2 Edit Domain Policy dialog

The following table describes the settings on the **Edit Domain Policy** dialog:

Domain Policy Setting	Description
Spam Filtering	Specifies whether spam filtering is enabled for the selected domain.
Consider mail spam when score is greater than	This is the anti-spam engine scoring threshold above which mail is considered to be spam. Default: 5.
Spam should be	These are the actions that should be performed when a message is classified as spam: ▪ **Quarantined**: The message is accepted but quarantined. It will appear in the Quarantine Report of the recipient(s) and may be later released from the quarantine if it is deemed by the user to be a false positive. ▪ **Passed (Tagged):** The message is analysed as normal, but will be passed onto the end recipient(s) regardless. However, headers will be added to the message so that it will be possible to filter messages on the backend mail server and/or on the end-recipients Mail User Agent (MUA). You may also prepend text to the Subject header, indicating that the message has been identified as spam. Enable **Spam Modifies Subject** and specify an appropriate **Spam Subject Tag**. ▪ **Rejected**: The message will be rejected. The default action is to quarantine all messages that exceed the spam threshold.
Discard Spam scoring above	Messages scoring above the specified score will not be quarantined.
Add X-Spam headers to non-spam mails	Specifies if addition headers are added to the message indicating the result of the spam analysis. The headers added are: ▪ **X-Spam-Status**: This will show if the message exceeded the spam threshold and the score that it achieved. It will also list what rules were fired by the anti-spam engine. ▪ **X-Spam-Score**: This simply lists the spam score achieved. Note: These headers are only added to inbound messages. If you process out-bound messages then these headers will not be added.
Virus Filtering	Specifies whether virus filtering is enabled for the selected domain. Virus Filtering is enabled by default
Viruses should be	These are the actions that should be performed when a message is identified as containing a virus. See spam actions above for a description of these actions.
Attachment Type Filtering	Specifies whether the corporate message attachment policy will be applied to messages to recipient in the selected domain. See “Content Filtering” on page 49

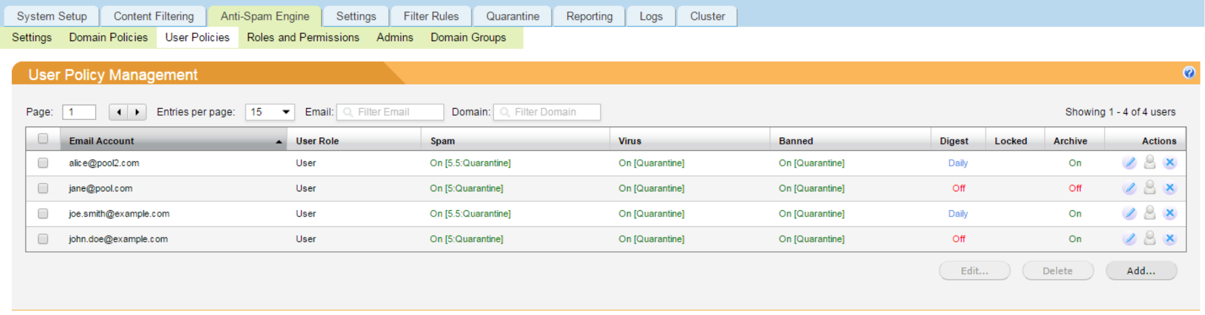
	for more details on scanning for banned attachments. Default is Enabled.
Banned Attachments should be	These are the actions that should be performed when a message is identified as containing a virus. See spam actions above for a description of these actions. Default action is Quarantine.
Archive Clean Email	Enable this setting to store all clean messages received by this domain in the history. By going to Reporting > History and viewing and clicking on a clean mail, you have the following options. Release, Whitelist sender, delete message, forward to quarantine administrator and mark message as spam.
Quarantine Report	This field specifies whether quarantine reports should be generated for recipient in this domain. A quarantine report will be generated for each recipient who has had messages quarantined.
Language	Select which language you would like your reports to be written in. Recipient may change the language of their report by logging into the UI and changing their preferences.
Email report every	Select the frequency of the quarantine reports. Reports may be generated every day, every weekday, every Friday, or every month. Recipient may change the frequency of their reports via the options section of the quarantine report, or by logging into the UI and changing their preferences.
Report contains	The quarantine report may contain a list of all items that are currently quarantined for each user or new quarantined items since the last report was generated (default) both of these can be viewed with or without virus infected emails included. Again, the user may change this via the options section of the quarantine report. If a user has no quarantined messages (or no new quarantined messages since last report) then no report will be delivered to them.
Exclude spam mails scoring above	Usually spam messages scoring above a certain score can be unequivocally be deemed spam and users are only interested in those messages that just fell above the spam threshold to look for false positives. If users get a significant amount of spam, then to keep the report size manageable you can exclude spam messages above, for example 30. This setting is set to 999 by default, meaning that no messages will be excluded (as a message cannot score that high).
Domain Administrators	Select administrators on a per-domain basis, enabling them to manage elements of their own email including license counts, mail usage and reporting.
Reset settings to default	Reset the policy to default values.

Table 11-1 Edit Domain Policy dialog settings

11.2 User Policies

By default, each recipient email address will inherit the policy as set for that domain. There are a number of circumstances where this policy can change however. For instance, if the domain policy for example.com specifies that quarantine reports are sent every weekday, then user@example.com could change their report preferences so that the quarantine report is only delivered weekly. A user can make this change either via their quarantine report or by logging into the web interface.

The **Anti-Spam > User Policies** page shows those addresses that have a specific policy that may be different from the domain policy.



Page: 1 Entries per page: 15 Email: Filter Email Domain: Filter Domain Showing 1 - 4 of 4 users

□	Email Account	User Role	Spam	Virus	Banned	Digest	Locked	Archive	Actions
□	alice@pool2.com	User	On [5.5:Quarantine]	On [Quarantine]	On [Quarantine]	Daily		On	✎ 👤 ✕
□	jane@pool.com	User	On [5:Quarantine]	On [Quarantine]	On [Quarantine]	Off		Off	✎ 👤 ✕
□	joe.smith@example.com	User	On [5.5:Quarantine]	On [Quarantine]	On [Quarantine]	Daily		On	✎ 👤 ✕
□	john.doe@example.com	User	On [5:Quarantine]	On [Quarantine]	On [Quarantine]	Off		On	✎ 👤 ✕

Figure 11-3 User Policies page

To create new user policies click the **Add…** button. To edit an existing user policy, click the ✎ icon in the options column. The Add/Edit User Policy dialog has the same settings as on the Add/Edit Domain Policy dialog apart from the following settings:

User Policy Settings	Description
Email Addresses	Specify one of more email addresses to create user policies for.
User Role	This dropdown allows you to select from the User Roles which are created on the Anti-Spam Engine > Roles and Permissions > User Roles tab. This allows you to specify the permissions such users will have when they log into the SpamTitan user interface. For instance, the Role may prevent users from modifying their own policy.
Lock Policy	If the Lock policy option is enabled and changes to the email address parent domain policy will *not* affect that user policy. For example, if the domain policy for example.com changes the spam score to 1, any user policy under example.com will also see that change appear on their policy unless it has been locked. A warning is issued to the Admin when editing a domain policy with locked users.

Figure 11-4 Add/Edit User Policies dialog settings

To impersonate a user, click on the 👤 icon in the options column. This will automatically log you into that users user interface with the same permissions as they would have.

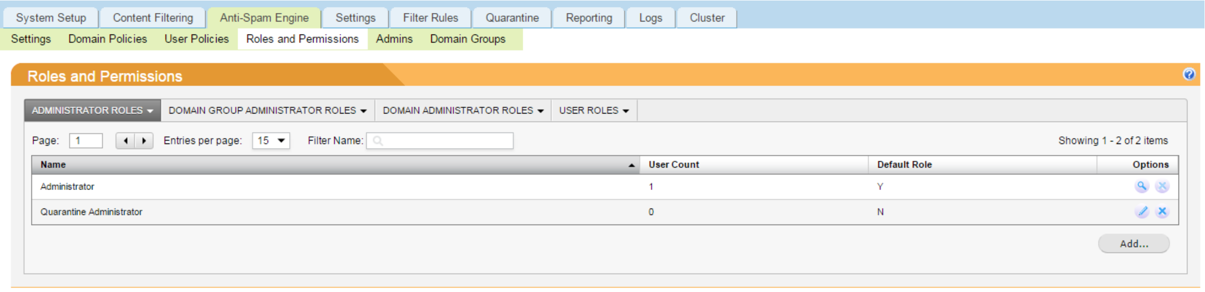
Note: By default, each recipient email address will inherit the policy as set for that domain. SpamTitan assigns a higher priority to user policies. When email arrives for a user who does not have a user policy, then the domain policy will be used. Likewise, if there is a policy associated with the email address then that will be used in preference to the domain policy.

User policies are automatically created when either:

1. A user logs into the UI for the first time.
2. A user whitelists a sender from their quarantine report.
3. An *existing* user (who has already sent or received email) requests their password using the **Forgot Password** link on the login page.

11.3 Roles and Permissions

From this section you can create and modify which pages administrators, domain administrators and users have access to when they log into the GUI; each sub section allows you to create varying roles for each of these types of users.

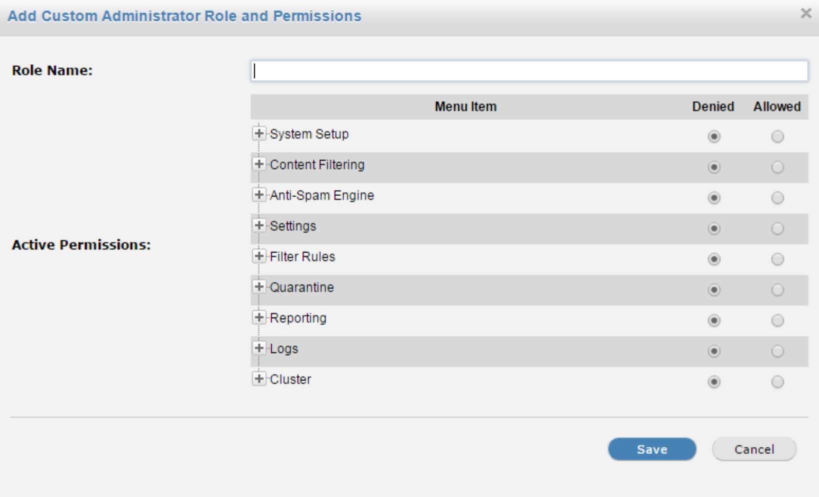


Name	User Count	Default Role	Options
Administrator	1	Y	
Quarantine Administrator	0	N	

Figure 11-5 Roles and Permissions

Click the **Add…** button to create a new Administrator role, Domain Group administrator role, Domain administrator role, or User role.

The Roles and Permissions dialog is displayed showing available options for each level of administrator.



Menu Item	Denied	Allowed
+ System Setup	●	○
+ Content Filtering	●	○
+ Anti-Spam Engine	●	○
+ Settings	●	○
+ Filter Rules	●	○
+ Quarantine	●	○
+ Reporting	●	○
+ Logs	●	○
+ Cluster	●	○

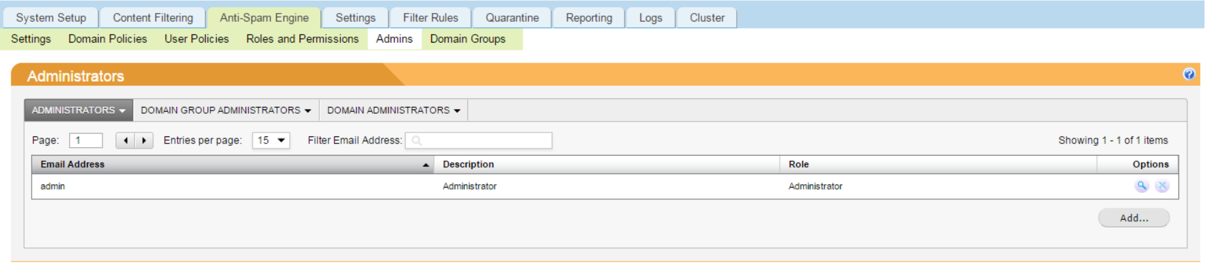
Figure 11-6 Roles and Permissions dialog

Click the **Allowed** or **Denied** checkbox beside a sections name to grant or block members of this role from accessing that section. You can allow and deny sub tabs by clicking on the (plus symbol) beside the section name to see the subsections within it. Each role must be allowed to access at least one page.

Administrators may be allowed access to the entire product. Domain administrators have fewer options and can only access pages for their own domains. Users can be allowed access to a more limited amount of pages still and only relating to their own user policy.

11.4 Admins

From here you can view and create as many custom administrators as you wish, the access rights of custom administrators are determined by the role applied to them.



Page: 1 Entries per page: 15 Filter Email Address: Showing 1 - 1 of 1 items

Email Address	Description	Role	Options
admin	Administrator	Administrator	

Figure 11-7 Administrators page

Any number of custom Administrator users may be created. The access rights of custom administrators are determined by the role applied to them.

There are 3 separate categories of custom administrator as follows:

Administrator Type	Description
Administrator	An Administrator is limited only by the role applied to them. The 'admin' user cannot be deleted.
Domain Group Administrator	A Domain Group Administrator can only access the Domain Group(s) to which they have been specifically granted access. If a Domain Group Administrator has access to more than one Domain Group, they will have multiple rows on the Domain Group Administrators table. A Domain Group is a group of domains, so the Domain Group Administrator will have access to make changes affecting only those domains which are part of their own Domain Group. A Domain Group can have any number of Domains, but each Domain can only belong to one Domain Group. Domain Group administrators are not necessary if no Domain Groups have been created. A Domain Group Administrator may be further limited by the role applied to them.
Domain Administrator	A Domain Administrator can only access the Domain(s) to which they have been specifically granted access. If a Domain Administrator has access to more than one Domain, they will have multiple rows on the Domain Administrators table. A Domain Administrator can only make changes affecting their own Domain(s).

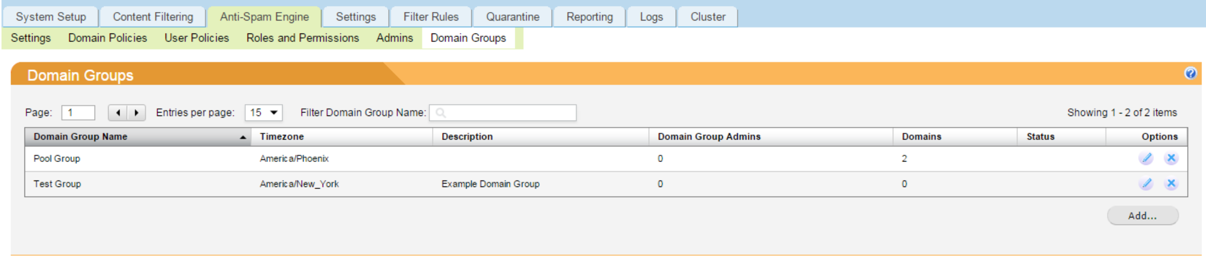
	Note that if Domain Groups are in use, a Domain administrator can have access to Domains that are in different domain groups. A Domain Administrator may be further limited by the role applied to them.

Table 11-2 Custom Administrator Categories

Note: Your ability to make changes in each of the above categories depends on your own access rights, so you may not see all three categories.

11.5 Domain Groups

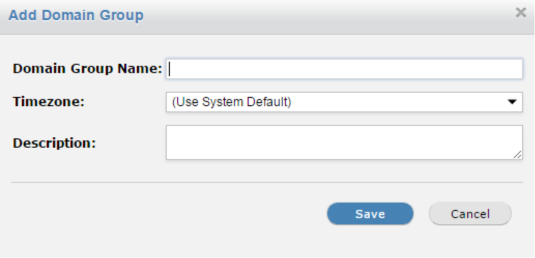
A Domain Group is a group of domains, for the convenience of controlling access to domains by Domain Group Administrators.



Domain Group Name	Timezone	Description	Domain Group Admins	Domains	Status	Options
Pool Group	America/Phoenix		0	2		
Test Group	America/New_York	Example Domain Group	0	0		

Figure 11-8 Domain Group Administrators

Click the **Add...** button to create a new Domain Group.



Domain Group Name:

Timezone: (Use System Default)

Description:

Figure 11-9 Add/Edit Domain Group dialog

The settings on the Add/Edit Domain Group dialog are as follows:

Setting	Description
Domain Group Name	Name for the Domain Group (required).
Time zone	If the Time zone is specified, any Domain Group Administrators accessing the SpamTitan interface will see times in the Domain Group's own local time. This also applies to any Domain Administrators accessing Domains within the Domain Group - they will see times adjusted for the time zone specific to the Domain Group.
Description	Option description/comment for the Domain Group.

Table 11-3 Add/Edit Domain Group dialog settings

You can create Domain Group Administrators with access to the Domain Group you have just created on the Admins page.

Once a Domain Group has been created, domains can be assigned to it on the **System Setup > Mail Relay** page. Domain Group Administrators can also assign domains to the Domain Group via their **Settings > Relay Settings** page.

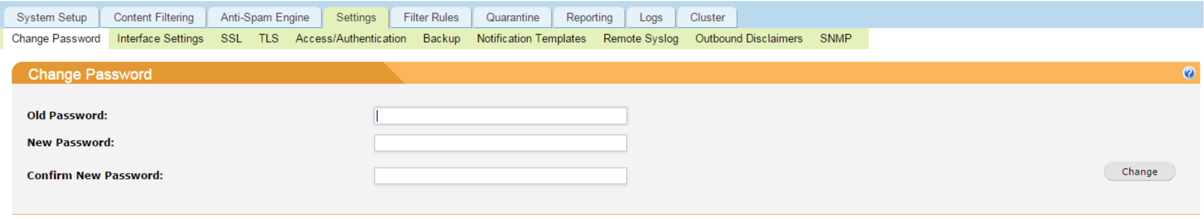
Full Administrators will always retain the ability to change any domain regardless of whether or not the domain belongs to a Domain Group.

12 Settings

This chapter covers basic administrative tasks that are available from the **Settings** page.

12.1 Changing the Password

The **Settings > Change Password** allows you to change the SpamTitan *Internal* password for the logged in user.



Change Password

Old Password:

New Password:

Confirm New Password:

Figure 12-1 Change Password page

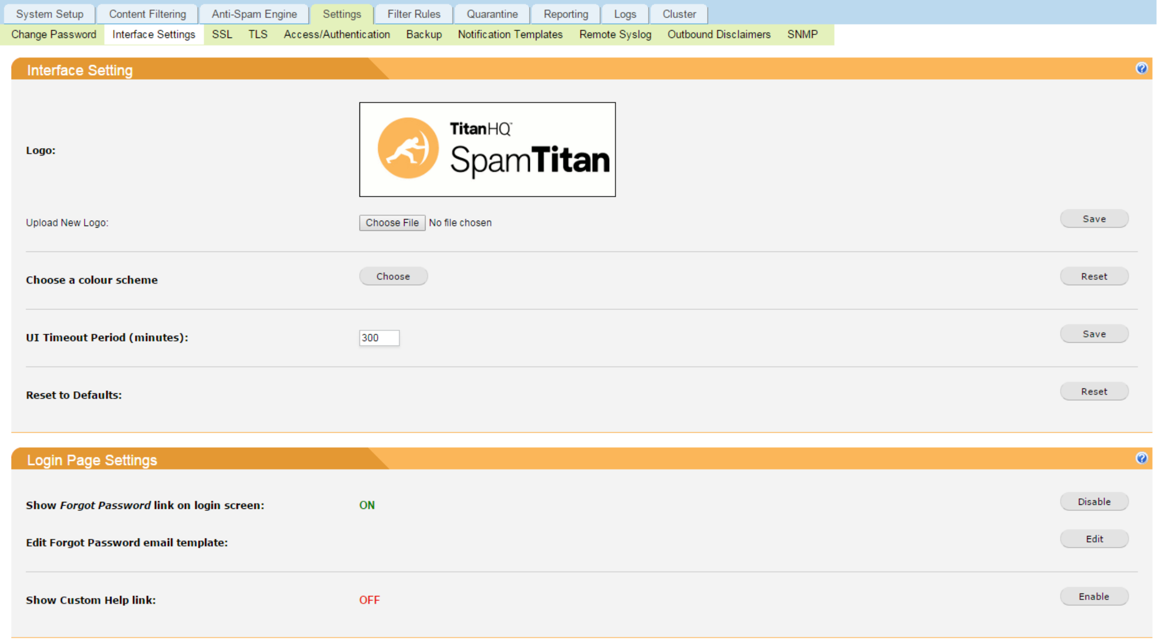
To change your password enter your current password in the **Old Password** field and then enter the new password you want to set in the **New Password** field and repeat it in the **Confirm New Password** field.

This password should be at least 6 characters long. A good password should contain a mix of uppercase and lowercase letters as well as numbers and punctuation. To prevent possible dictionary attacks it should not spell out any words found in the dictionary. Note that passwords are case sensitive.

If you are using an external password mechanism such as pop3, imap or ldap for end-user access authentication, then users will not be able to change those passwords.

12.2 Interface Settings

The **Settings > Interface Settings** contains settings that affect the appearance of the web interface, and allow you to 'white-label' the product.



Interface Setting

Logo:

Upload New Logo: No file chosen

Choose a colour scheme

UI Timeout Period (minutes): 300

Reset to Defaults:

Login Page Settings

Show *Forgot Password* link on login screen: ON

Edit Forgot Password email template:

Show Custom Help link: OFF

Figure 12-2 Interface Settings page

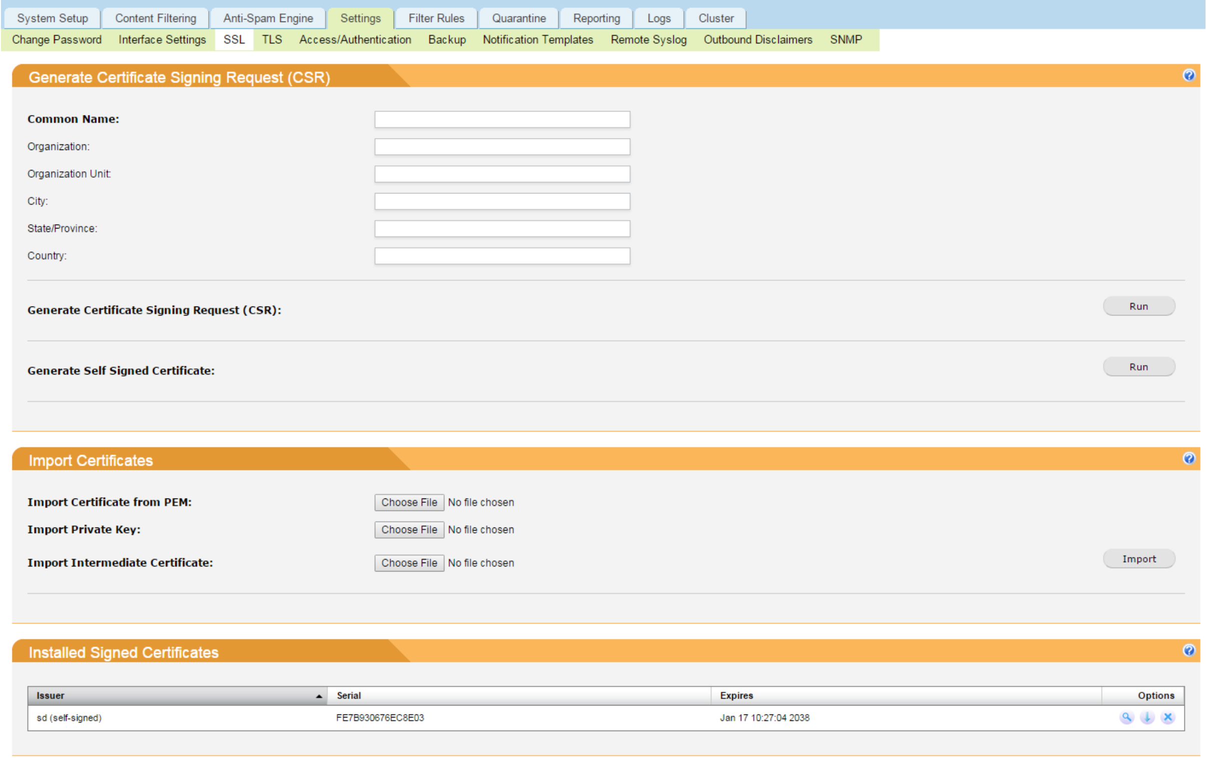
The following table describes the settings on the Interface Settings page:

Field	Description
Logo	This is the image that will be used on all pages in the graphical user interface.
Upload New Logo	Use the Upload New Logo option to replace default logo with your own custom logo. The image should be approximately the same size as the default logo (216x60 pixels) and must be of type jpg, png or gif.
Choose a colour scheme	Click the **Choose** button to open the Choose Colour Scheme dialog which allows you to customize the colours used in the GUI. Click the **Reset** to reset the colour scheme to the factory defaults.
UI Timeout Period	For security reasons the SpamTitan web interface time out after a specified period of inactivity. You can change this setting by changing the period (in minutes) and clicking the Save button. The default value is 30 minutes.
Reset to Defaults	If at any time you want to revert to the factory installed defaults for the interface appearance then click this button.
Show Forgot Password link on login screen	This option controls whether the login screen contains a link to the email password form. This feature should be disabled if the Web Authentication (see page 62) is set to something other than the default (Internal). This option may also be disabled if you do not want to allow users retrieve their login password and thus login to the interface. This option is enabled by default.
Edit Forgot Password email template	Enabling this allows editing of the email which is sent when the users click the Forgot Password link on the login page. This emails Subject, Sender Address and message body can be specified. The message body must contain the **%%PASSWORD%%** placeholder to work - this will get replaced with the users password. Note: The body of the messages may contain HTML formatted input.
Show Custom Help link	If you enable this option then the login screen will contain a **Login Help** link that can be redirected to your own web server that contains help for users on logging into and using the appliance. Use the **Login Help URL** field to specify the URL of your help page.

Table 12-1 Interface Settings

12.3 SSL Certificate Management

SSL management can be done on the **Settings > SSL** page. The use of SSL certificates ensures that all http communication to the SpamTitan UI is encrypted. Additionally, SSL certificates may be used for inbound TLS communication so that the mail connection between clients and the SpamTitan appliance is encrypted thus preventing eavesdropping and tampering.



Generate Certificate Signing Request (CSR)

Common Name:

Organization:

Organization Unit:

City:

State/Province:

Country:

Generate Certificate Signing Request (CSR):

Generate Self Signed Certificate:

Import Certificates

Import Certificate from PEM: No file chosen

Import Private Key: No file chosen

Import Intermediate Certificate: No file chosen

Installed Signed Certificates

Issuer	Serial	Expires	Options
sd (self-signed)	FE7B930676EC8E03	Jan 17 10:27:04 2038	

Figure 12-3 SSL Certificate Management

Each certificate generated contains the following information and will be available to all users who wish to view the certificate when viewing the SpamTitan UI:

Certificate Field	Description
Common Name	This is the fully qualified domain name that will be used in the URL to access the SpamTitan UI. It must match the server name exactly as otherwise you will get a warning dialog every time you visit the site. For example, spamtitan.example.com
Organization	This is the name of your company or organization.
Organization Unit	This is an optional filed to specify a specific department within your organization.
City	This is the name of the city or town where the organization is located.
State/Province	This is the full name of the state or province where the organization is located.
Country	This is the two-letter country code of the location of the organization e.g. US

Table 12-2 Certificate Information fields

To generate a **Certificate Signing Request (CSR)** enter the details above that will be included in the certificate and press the **Run** button. The Signing Request (CSR) that is generated will also contain the public key that will be included in your certificate. A **certificate authority** will use the CSR to create your signed SSL certificate. The signed certificate you receive back from the CA may be subsequently imported into SpamTitan via the **Import Certificate from PEM**. The system supports X.509 device certificates in PEM encode formats (file extensions include .cer, .crt and .pem). The PEM encoding is used for different types of X.509v3 files which contain ASCII (Base64) armored data prefixed with a '-- BEGIN ...' line.

SpamTitan allows you to generate private, self -signed certificates which provide the same security as certificates purchased from a certificate authority. However, in this case because the web browser will be unable to verify the authenticity of the certificate a warning message will be displayed to the user informing them of the unverified certificate. To generate a **Self-Signed Certificate** enter in the certificate details and run the **Generate Self-Signed Certificate** option.

You can avoid this problem by purchasing a trusted certificate from a trusted certificate signing authority. The certificate will be identifiable by all browsers, and so users will not be presented with the warning message.

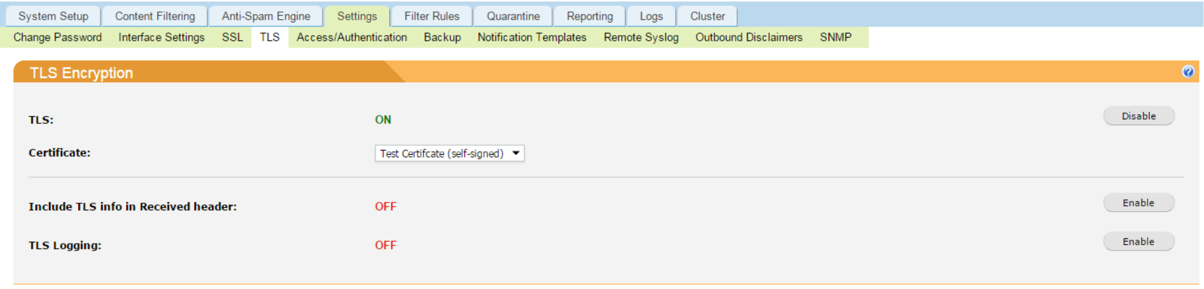
On the Settings>SSL page, when you receive the signed certificate back from the CA, use the **Import Certificate from PEM** option to import the certificate into SpamTitan.

When the certificate and key are contained in one file, you will only need to specify the certificate file. If the certificate and key files are in separate files, then you will also need to specify the private key. If an intermediate certificate is required, this may be specified using the **Import Intermediate Certificate** option.

The Installed Signed Certificates section shows all certificates generated and/or installed on the SpamTitan appliance, listing their **Serial Number** and **Expiration Date**. You also have the option to view the certificates details, to delete the certificate and download the private key associated with the certificate.

12.4 TLS Encryption

Transport Layer Security (TLS), located at Settings>TLS, provides a mechanism for certificate based authentication on encrypted sessions. If enabled, then SpamTitan will attempt to negotiate an encrypted session with the peer for the SMTP connection. If a TLS session cannot be negotiated (many clients/servers do not support TLS), then the session will fall back to plain text.



TLS: ON

Certificate: Test Certifcate (self-signed)

Include TLS info in Received header: OFF

TLS Logging: OFF

Figure 12-4 TLS Encryption page

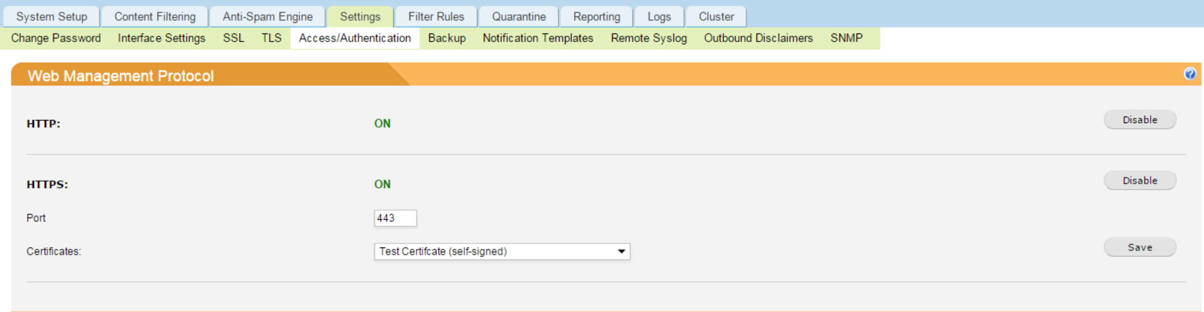
The settings on the TLS Encryption page are as follows:

Field	Description
TLS	Click the **Enable** button to enable TLS
Certificate	Choose an available certificate from the dropdown list. You can manage the certificated from the **Settings > SSL** page.
Include TLS info in Received header	To include information about the protocol and cipher used as well as the client and issuer CommonName into the Received: header, enable Include TLS info in Received header. The default is disabled, as the information is not necessarily authentic. Only the final destination is reliable, since the headers might have been changed in between.
TLS Logging	To get additional information during the TLS setup and negotiations you can enable TLS Logging. When enabled, start up and certificate information from the TLS subsystem will be logged to the SpamTitan maillog.

Table 12-3 TLS Encryption settings

12.5 Access Authentication: Configuring HTTP/HTTPS

SpamTitan can be managed via your web browser using HTTP or HTTPS.



HTTP: ON

HTTPS: ON

Port: 443

Certificates: Test Certifcate (self-signed)

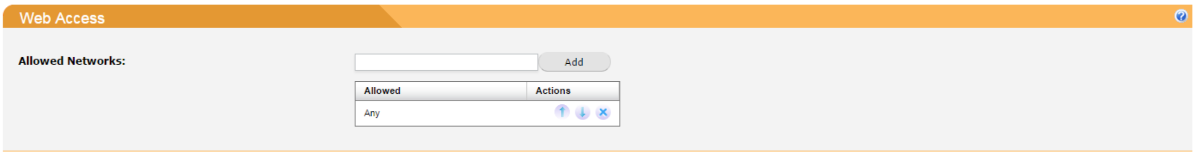
Figure 12-5Configuring HTTP/HTTPS page

By default HTTP is enabled. You can also enable management using HTTPS. The default Port for HTTPS is 443. You can add another layer of security for logging into SpamTitan by changing the default port. If you specify a port other than the default HTTPS port (443) then you will have to specify the port number as well as the hostname/IP address when logging in - e.g. https://192.168.10.10:789.

Note: The Certificate **Common Name** must match the site name exactly as otherwise you will get a warning dialog every time you visit the site. So if you access the UI using, for example, http://spamtitan.mydomain.com/ then you will need a common name of spamtitan.mydomain.com.

12.6 Access Authentication: Web Access

The **Allowed Networks** allows you to control the hosts and/or networks that should have access to the SpamTitan Interface. By default, all networks (**Any**) and all users are allowed access. It is recommended that this be changed to your internal network(s) to restrict access to just those users within your organization.



Web Access

Allowed Networks: Add

Allowed	Actions
Any	↑ ↓ ✕

Figure 12-6 Web Access settings

The list of allowed networks is a list of network addresses or network/netmask patterns specified in CIDR (Classless Inter-Domain Routing) format. The netmask specifies the number of bits in the network part of a host address.

Note: The list is matched from top to bottom, and the search stops on the first match. Specify the "!" character to a pattern to exclude an address or network block from the list.

You can also specify if a particular rule applies to a particular user or for everyone by appending a colon followed by the users email address ':user@example.com'. Example:

1. 192.168.0.101:admin
2. !Any:admin
3. !192.168.0.0/24:jsmith@example.com
4. 192.168.0.0/24

In this case *admin* can only connect to the web interface from 192.169.0.101. All other users can connect from the 192.168.0.0/24 network except for user *jsmith@example.com* who is not allowed access to the interface. It will not be possible to login from any other network. If no rule matches then access is denied.

A simpler example which specifies that access for all users is from any client on the 192.168.0.0/24 network would be:

192.168.0.0/24

Use the up (↑) and down (↓) arrow buttons to sort the rules according to your policy.

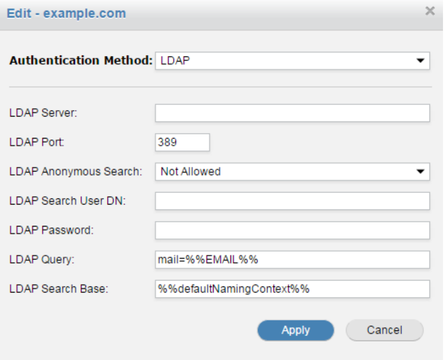
12.7 Access Authentication: Web Authentication Settings

The Web Authentication settings on the **Settings > Access/Authentication** page allows you to control for each internal domain what authentication method will be used when users attempt to login to the GUI to view their quarantine and/or user preferences. The following authentication methods are supported:

- **Internal** (default):
  SpamTitan will generate a unique password for each internal email address for which a policy exists. Individual user policies may be manually generated from the user interface, or when a user whitelists an email address from their

quarantine report. Users can receive their password via email if they click the '*Forgot your Password?*' link on the Login page and enter their email address. They can then change their password after logging in. If a policy does not already exist for the user, then one will be created.

- **LDAP:**
  LDAP Authentication allows you to specify an external LDAP-enabled directory to authenticate and authorize users on a per- domain basis. LDAP authentication for SpamTitan can be configured to support any LDAP compliant directory including Microsoft Active Directory, Lotus Domino, SunOne/iPlanet Directory Server and Novell eDirectory.



Edit - example.com

Authentication Method: LDAP

LDAP Server:

LDAP Port: 389

LDAP Anonymous Search: Not Allowed

LDAP Search User DN:

LDAP Password:

LDAP Query: mail=%%EMAIL%%

LDAP Search Base: %%defaultNamingContext%%

Figure 12-7 Configuring LDAP Authentication

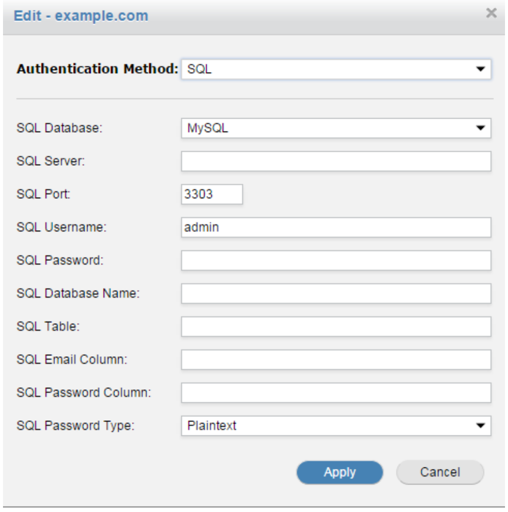
For users to authenticate with an external LDAP server specify LDAP as the Authentication Method for that domain and enter the LDAP server details. The following table describes the LDAP fields to be entered:

LDAP Settings	Description
LDAP Server	The name of the LDAP server that SpamTitan attempts to connect to for authentication purposes.
LDAP Port	The port SpamTitan uses to connect to the LDAP server for authentication purposes. Default port 389.
LDAP Anonymous Search	Some LDAP directories require that a valid user/password be provided to bind to the server in order to perform LDAP searches. Use this dropdown list to specify if Anonymous bind is allowed to the LDAP server.
LDAP Search User DN	If anonymous bind is not permitted then you must specify the DN of the user that will be used to bind to the Directory server specified in the LDAP server and port field as administrator. This is usually an email address or directory object of the form: cn=user,dc=company,dc=com.
LDAP Password	This field contains the password for the administrator profile specified in the LDAP Search User DN field.
LDAP Query	This field specifies the attribute that contains the username of the person authenticating. The default is mail=%%EMAIL%% where %%EMAIL%% will be

	replaced with the email of the person authenticating. For example, if the email address of the person authenticating is joe@domain.com then %EMAIL%% will be replaced with joe@domain.com. Similarly %%USER%% can be used to specify the left-hand side of the email address.
LDAP Search Base	This field specifies where in the directory the search will commence from. If the LDAP server is able to determine the defaultNamingContext (Active Directory only) then you can specify %%defaultNamingContext%% and the authentication module will determine this before doing the search.

Table 12-4 LDAP Authentication settings

- **SQL Server**
  SQL Authentication allows you to perform authentication against an external SQL server. Specify SQL as the Authentication Method and enter the credentials that the appliance will use to connect to the SQL server.



Edit - example.com

Authentication Method: SQL

SQL Database: MySQL

SQL Server:

SQL Port: 3303

SQL Username: admin

SQL Password:

SQL Database Name:

SQL Table:

SQL Email Column:

SQL Password Column:

SQL Password Type: Plaintext

Figure 12-8 Configuring SQL Authentication server

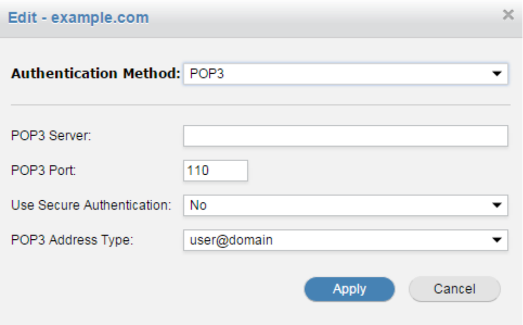
The following table describes the SQL authentication settings:

SQL Settings	Description
SQL Database	This field specifies the SQL database type been used.
SQL Server	The IP address or hostname of the SQL server that SpamTitan attempts to connect to for authentication purposes.
SQL Port	The port SpamTitan uses to connect to the SQL Server for authentication purposes. Default port 3306.
SQL Username	The username used to connect to the SQL server in order to perform the authentication.
SQL Password	The password associated with the username.

SQL Database Name	The field contains the name of the database containing the authentication tables.
SQL Table	The SQL table to be queried for the Authentication.
SQL Email Column	The column that contains the list of email addresses.
SQL Password Column	This field specifies the column that contains the password.
SQL Password Type	The password may be stored in plaintext format, or as a MD5 checksum, or encrypted.

Table 12-5 SQL Authentication settings

- **POP3**
  Authentication against a POP3 server is quite trivial. When this authentication method is enabled users attempting to login to the GUI will have their authentication credentials authenticated via a POP3 server.



Edit - example.com

Authentication Method: POP3

POP3 Server:

POP3 Port: 110

Use Secure Authentication: No

POP3 Address Type: user@domain

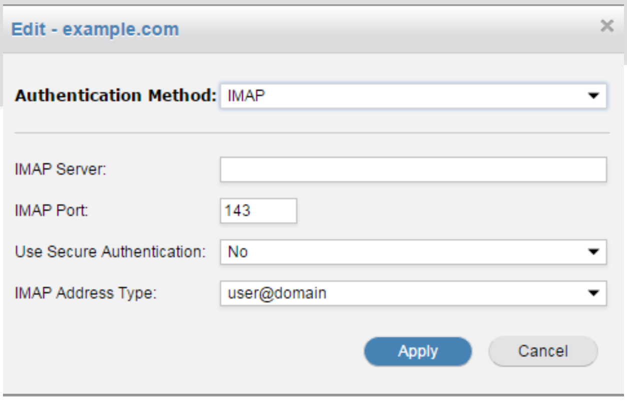
Figure 12-9 Configuring POP3 Authentication

The following table describes the POP3 authentication settings:

POP3 Settings	Description
POP3 Server	The IP address or hostname of the POP3 server that SpamTitan attempts to connect to for authentication purposes.
POP3 Port	The port SpamTitan uses to connect to the POP3 server for authentication purposes. Default port 110.
Use Secure Authentication	You can enable Secure Authentication if supported by the pop3 server.
POP3 Address Type	This is format required by your pop3 server for the username. If the pop3 server requires only the mailbox name for authentication, then select user. SpamTitan will then strip the domain name from the user supplied email.

Table 12-6 POP3 Authentication settings

- **IMAP**



Edit - example.com

Authentication Method: IMAP

IMAP Server:

IMAP Port: 143

Use Secure Authentication: No

IMAP Address Type: user@domain

Figure 12-10 Configuring IMAP Authentication

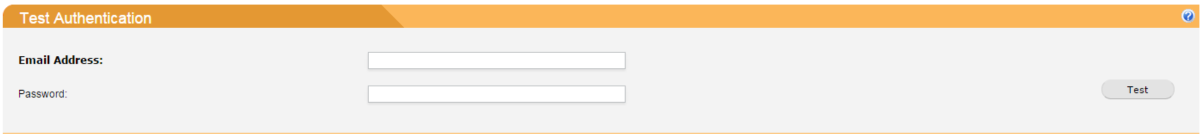
The following table specifies the IMAP fields to be entered if using IMAP as the authentication method for the GUI.

IMAP Settings	Description
IMAP Server	The IP address or hostname of the IMAP server that SpamTitan attempts to connect to for authentication purposes.
IMAP Port	The port SpamTitan uses to connect to the IMAP server for authentication purposes. Default port 143.
Use Secure Authentication	You can enable Secure Authentication if supported by the IMAP server.
IMAP Address Type	This field specifies the format expected by your IMAP server. Some IMAP servers require the credentials to be specified as an email address, while others require just the left-hand side of the email address (the username).

Table 12-7 IMAP Authentication settings

The support of external authentication modules ensures that when possible users won't have to remember multiple passwords. All login attempts will be directed to the appropriate authentication server for that domain.

You can use the **Test Authentication** feature on the **Settings > Access/Authentication** to ensure that your settings are correct. After saving your authentication settings, simply enter the **Email Address** and **Password** of a user to test. SpamTitan will determine the authentication method to use for that domain and validate the supplied password.



Test Authentication

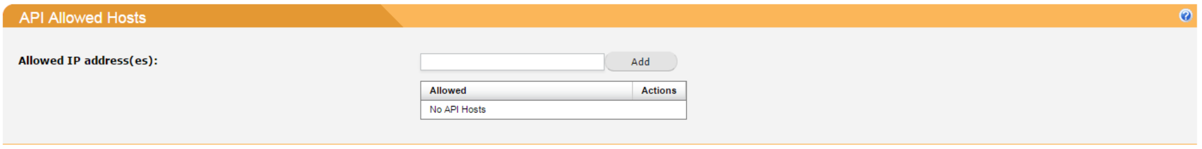
Email Address:

Password:

Figure 12-11 Test Authentication

The **SpamTitan API** is a set of Rest-based scripts that can be used to perform SpamTitan tasks from within your own environment. For instance, the bulk addition of a number of domains, or whitelists can be cumbersome using the user interface, but with the API can be achieved quite easily. Access to the API is restricted to the IP addresses listed in the

Allowed IP addresses section, located at **Settings > Access/Authentication**. See **Remote Management** for more details on the SpamTitan API.



API Allowed Hosts

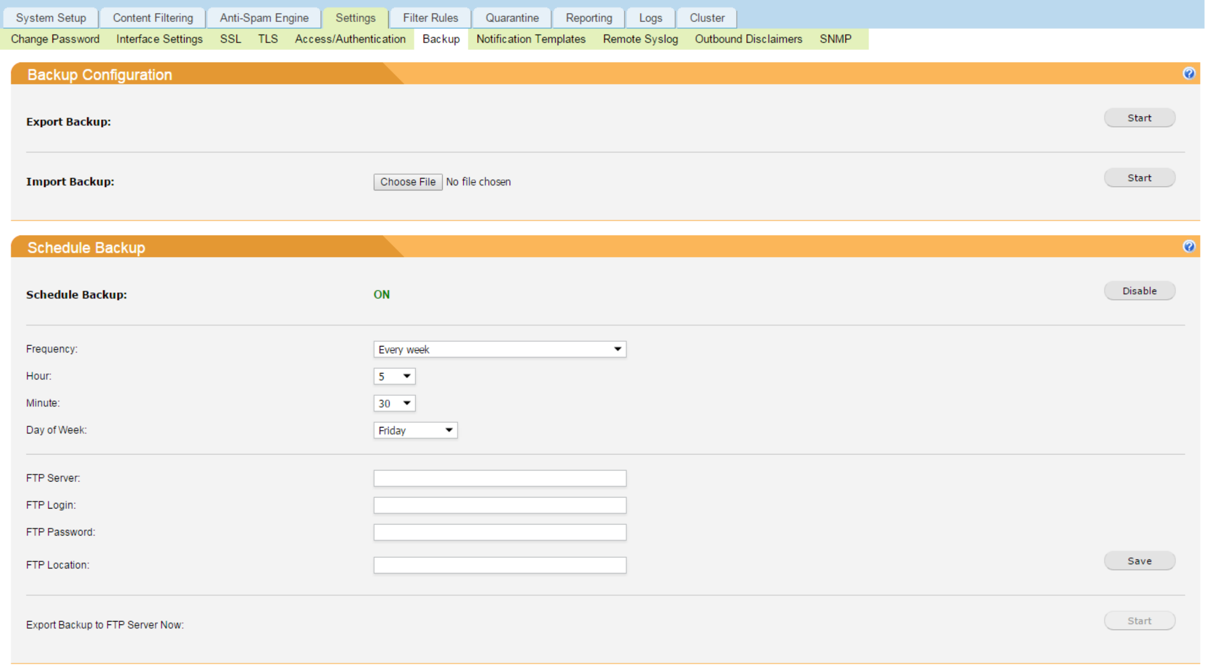
Allowed IP address(es): Add

Allowed	Actions
No API Hosts	

Figure 12-12 Configuring API Access controls

12.8 Backing up and Importing System Configuration

With the backup feature of SpamTitan the configuration of the software can be saved to a local data medium and can be restored if required. Settings saved include network settings, domains configured, user preferences and email whitelists and blacklists.



Backup Configuration

Export Backup: Start

Import Backup: Choose File No file chosen Start

Schedule Backup

Schedule Backup: ON Disable

Frequency: Every week

Hour: 5

Minute: 30

Day of Week: Friday

FTP Server:

FTP Login:

FTP Password:

FTP Location: Save

Export Backup to FTP Server Now: Start

Figure 12-13 Backup/Restore page

To create a backup of the system configuration, select **Settings > Backup** and press **Export Backup: Start** to create a backup file. If the backup has been created successfully you will be able to download the backup and save it to a folder of your choice.

To import a previously saved backup, select **Settings > Backup** and click **Choose File…** to find the backup file and click **Import Backup: Start**. If the uploaded file is a valid and version compatible backup then it will be restored.

To save you the work of backing up your configuration manually, the backup function supports automatic backup generation and FTP to a remote FTP server. To configure scheduled backups select **Settings > Backup** and configure the **Schedule Backup** panel settings.

The following table describes the schedule backup settings:

FTP Backup Settings	Description

Schedule Backup	Displays if scheduled backups are enabled.
Frequency	Specifies the backup to be performed daily, weekly or monthly.
Hour/Minute	The time of day to perform the backup.
Day of Week	If performing weekly backups, use this option to specify which day of the week to perform the scheduled backup.
FTP Server	The IP address of hostname of the FTP server.
FTP Login	The username that the appliance should use to log into the backup FTP server.
FTP Password	The password that the appliance should use to log into the backup FTP server.
FTP Location	The folder or path to store the backup files in on the backup server.
Export Backup to FTP Server Now	If you want to test that your FTP settings are correct you can Export Backup Now by pressing the Start button.

Figure 12-14 Scheduled FTP Backup settings

Note: It is only possible to restore backups that are at the same patch level as the currently installed system revision.

12.9 Notification Templates

Email Notification messages can be sent in response to virus, spam, or banned file attachment detection. Three types of messages are generated:

- Administrator notifications are sent to the administrator, if enabled.
- Sender (non) delivery notifications may be sent to the mail originator
- Recipient warnings may be sent to envelope recipients of the email containing a virus or banned attachment. These notifications are disabled by default since they are more of a nuisance than a benefit and contribute to unwanted backscatter on the Internet.

These Non-Delivery reports are only used if the appliance is configure to send them. See Content Filtering: Viruses, Content Filtering: Spam and Content Filtering: File Extensions to see if these notifications are enabled.

You can modify the templates for these notifications by editing the templates on the **Settings > Notification Templates** page. To reset to the system default templates press the **Reset to Default** button for the template that you would like to reset. Note that this will result in the loss of any custom changes.

The following table lists the various templates that can be modified:

Template	Description
Notify Virus Recipient	When a message is identified as containing a virus, then this message may be sent to the intended recipient of the email. This option can be specified on the **Content Filtering > Viruses** page.
Notify Virus Administrator	When a message is identified as containing a virus, then this message may be sent to the administrator of SpamTitan. This option can be specified on the **Content Filtering > Viruses** page

Notify Virus Sender	When a message is identified as containing a virus then this message may be sent to the sender of the email. This message will be sent if the recipient has a policy set that will reject viruses, rather than pass or quarantine it.
Notify Banned Recipient	When a message is identified as containing an attachment that is marked as banned then this message may be sent to the intended recipient of the email. This setting can be configured on the **Content Filtering > File Extensions** page.
Notify Banned Administrator	When a message is identified as containing an attachment that is marked as banned then this message may be sent to the administrator of SpamTitan.
Notify Banned Sender	When a message is identified as containing an attachment that is marked as banned then this message may be sent to the sender of the email.
Notify Spam Administrator	When a message is identified as spam then this message will be sent to the administrator of SpamTitan if spam admin notifications are enabled. See **Content Filtering > Spam** page.
Notify Spam Sender	When a message is identified as spam then this message may be sent to the sender of the email. This message will be sent if the recipient has a policy set that will reject spam, rather than pass or quarantine it.
Notification Emails Character	Select which alphabet you are writing your templates in here. This will ensure that when they are received the characters used will display correctly.

Table 12-8 Email Notification Templates

The following table describes the supported macros that may be used in the NDRs:

Macro	Description
%h	Hostname of this host
%d	Timestamp of message reception (RFC 2822 local date-time format)
%s	Original envelope sender, rfc2821-quoted and enclosed in angle brackets
%S	Address that will get sender notification. This is normally a one-entry list containing sender address (same as %s), but may be un-mangled/reconstructed in an attempt to undo the address forging done by some viruses.
%t	First entry in the 'Received' trace of the mail header
%a	Original SMTP session client IP address
%g	Original SMTP session client DNS name
%R	A list of original envelope recipients
%j	Subject header field body
%m	Message-ID header field body
[%H|]	A list of all header lines (field may be wrapped over more than one line). This does not include the 'Return- Path:' or 'Delivered-To:'

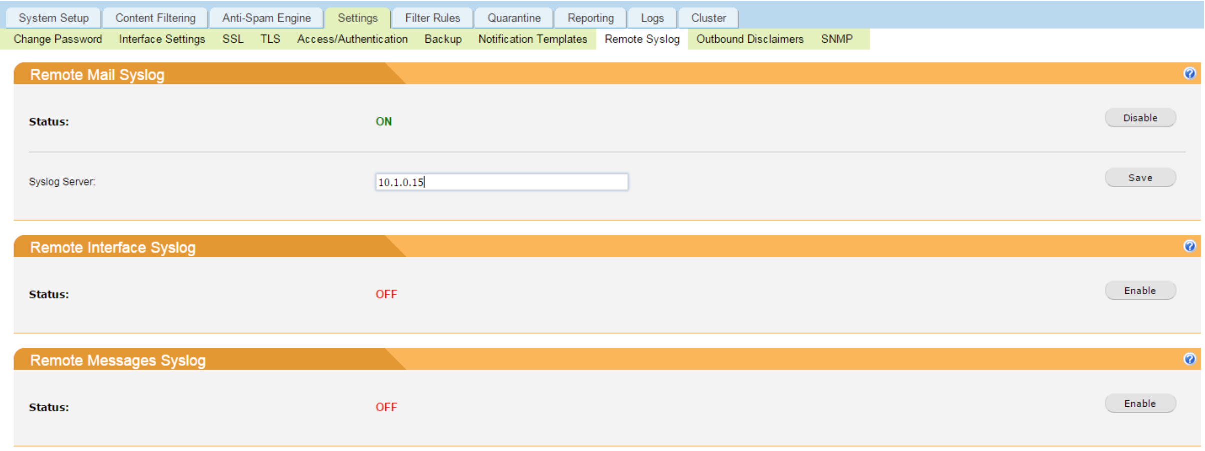
	headers, which would have been added (or will be added later) by the local delivery agent if mail would have been delivered to a mailbox.
%z	Original mail size (in bytes)
%v	Output of the (last) virus checking program
%V	A list of virus names found; contains at least one entry (possibly empty) if a virus was found, otherwise a null list
%F	A list of banned file names
%W	A list of AV scanner names detecting a virus
[%A|]	A list of the spam engines report lines

Table 12-9 Macros which may be used in templates

Note: If you want to use the '[' or ']' characters in the notification messages then to take away the special macro meanings of these characters they can be quoted by a backslash. E.g. \[or \].

12.10 Remote Syslog

All system logs are written to local log files on SpamTitan using syslog and may be viewed using the GUI. Syslog is the de facto standard for forwarding log messages in an IP network.



Remote Mail Syslog

Status: ON

Syslog Server: 10.1.0.15

Remote Interface Syslog

Status: OFF

Remote Messages Syslog

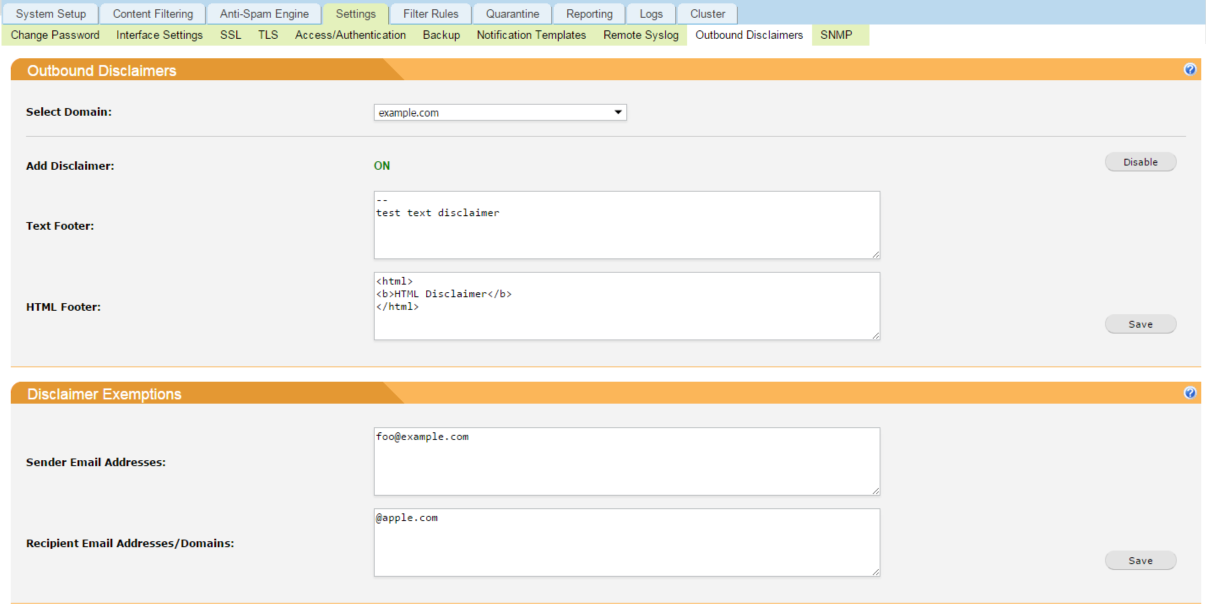
Status: OFF

Figure 12-15 Configuring Remote Syslog servers

The **Settings > Remote Syslog** page allows you to specify a server to which SpamTitan can send syslog files. The remote server defined must run a logging daemon compatible with the syslog protocol. You can specify a separate (or same) remote syslog server for each of the **Mail**, **Interface** and **Messages** log files.

12.11 Configuring Outbound Disclaimers

SpamTitan can append a default string to the footer of all messages delivered to external recipients.



Outbound Disclaimers

Select Domain: example.com

Add Disclaimer: ON

Text Footer:

```
--
test text disclaimer
```

HTML Footer:

```
<html>
<b>HTML Disclaimer</b>
</html>
```

Disclaimer Exemptions

Sender Email Addresses:

```
foo@example.com
```

Recipient Email Addresses/Domains:

```
@apple.com
```

Figure 12-16 Configuring Disclaimers

The Settings > Outbound Disclaimers page allows you to define disclaimers on a per-domain basis. Both text and HTML disclaimers are supported.

The following table describes the disclaimer settings that you can set for each sender domain:

Disclaimer Settings	Description
Select Domain	Select a domain to configure disclaimers for. This allows you to selectively add disclaimers from some domains only.
Add Disclaimer	Determines whether a disclaimer is attached to outgoing messages that are sent from the selected domain.
Text Footer	The disclaimer text that is attached to text-based messages
HTML Footer	The disclaimer text attached to HTML-based messages. When you have made the required changes press the Save button to save your changes

Table 12-10 Disclaimer settings

The Disclaimer Exceptions section allows you to exclude disclaimers from been added to certain messages to/from certain email addresses.

The following table describes the disclaimer exemption settings:

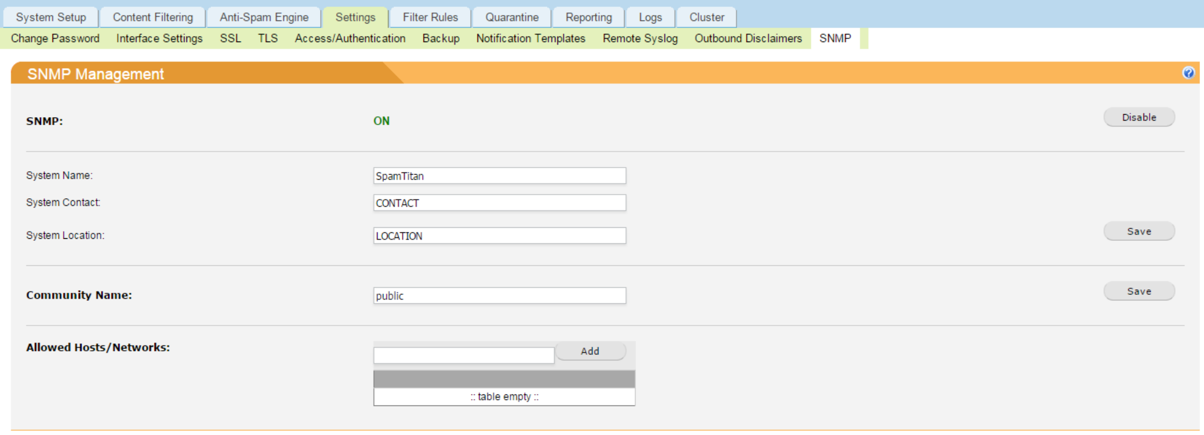
Disclaimer Exceptions	Description
Sender Email Addresses	List of sending email addresses that will not have a disclaimer added. Specify one email address per line.

Recipient Email Addresses/Domains	List of recipient email addresses or domains (e.g. @example.com) that will not have a disclaimer added. Specify one email address/domain per line.

Table 12-11 Disclaimer Exceptions settings

12.12 SNMP Management

SNMP (Simple Network Management Protocol) is a network protocol used over User Datagram Protocol (UDP) that allows network administrators to monitor the status of the SpamTitan appliance. SpamTitan replies to SNMP Get commands for MBIBII via any interface.



SNMP: ON

System Name: SpamTitan

System Contact: CONTACT

System Location: LOCATION

Community Name: public

Allowed Hosts/Networks:

:: table empty ::

Figure 12-17 Configuring SNMP

The following table describes the entries on the SNMP Management page:

SNMP Setting	Description
SNMP	Click the Enable\Disable button to turn the protocol on or off.
System Name	Enter the System Name. This could be for instance the hostname of the SpamTitan appliance.
System Contact	In this field, type in the name and/or email address of the network administrator for the SpamTitan appliance.
System Location	The System Location field may contain additional information such as the physical location of the appliance, an email address or a pager number.
Community Name	Create a name for a group or community of administrators who can view SNMP data and enter it in the Community Name field. You should use a community string which is used/known only at your site
Allowed Hosts/Networks	To restrict access further, enter the hostname, IP address or CIDR address of those systems/networks that are allowed to perform SNMP queries. Typically this will just be the IP address of your SNMP Management station. If no hostnames or addresses are specified then any system that provides the correct community string may request the

SNMP data.

Table 12-12 SNMP management settings

Note: SpamTitan supports most SNMP v1/v2c and relevant Management Information Base II (MIBII) groups which can provide a variety of information about your SpamTitan appliance. In addition the following OIDs provide information on the size of the mail queues:

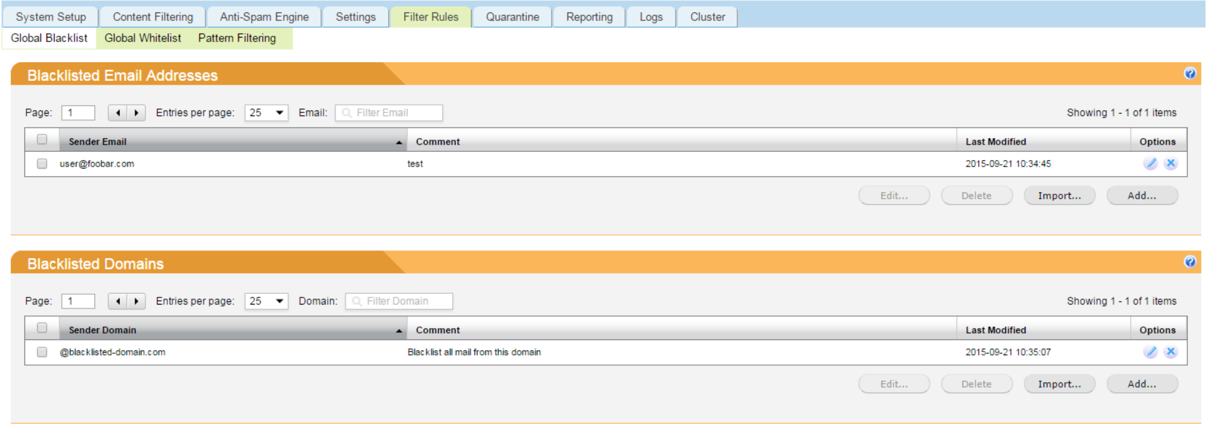
- .1.3.6.1.4.1.2021.8.1.101.1 - Active Queue
- .1.3.6.1.4.1.2021.8.1.101.2 - Incoming Queue
- .1.3.6.1.4.1.2021.8.1.101.3 - Deferred Queue
- .1.3.6.1.4.1.2021.8.1.101.4 - Corrupt Queue
- .1.3.6.1.4.1.2021.8.1.101.5 - Hold Queue

13 Filter Rules

This chapter covers the use of sender email filters and sender domain filters to allow you to blacklist or whitelist messages based on the senders email address.

13.1 Configuring the Global Email Blacklist

The **Filter Rules > Global Blacklist** page allows you to control which messages are always blocked by SpamTitan. Messages from these email addresses and/or domains will be automatically blacklisted, and the messages from those senders will not be scanned by the anti-spam engine.



Blacklisted Email Addresses

Page: 1 Entries per page: 25 Email: Filter Email Showing 1 - 1 of 1 items

☐	Sender Email	Comment	Last Modified	Options
☐	user@foobar.com	test	2015-09-21 10:34:45	✎ ✕

Blacklisted Domains

Page: 1 Entries per page: 25 Domain: Filter Domain Showing 1 - 1 of 1 items

☐	Sender Domain	Comment	Last Modified	Options
☐	@blacklisted-domain.com	Blacklist all mail from this domain	2015-09-21 10:35:07	✎ ✕

Figure 13-1 Configuring Global Blacklists

Click the **Add…** button to add a new blacklisted sender email address or domain, and the Add Blacklist entry dialog box will be displayed. Enter the email address or domain that you want to block, and then press the Save button. The address must be of the form *user@example.com* - which will block mail from that user to your account - or of the form *example.com* - which will block all email from that domain to your account.

To delete entries from the lists click the ✕ icon for that domain or email address.

Note: whitelisted/blacklisted sender testing is performed after a message is received. As such, front line controls may still apply. For instance, if the connecting client is on an RBL, then the message will be rejected (regardless whether the sender is on a whitelist). In such a situation, you will need to add the senders IP address to the 'Allowed RBL IP Addresses' which is on the System Setup -> Mail Relay -> IP Controls tab under RBLs.

Note: a sender may not be both white- and blacklisted at the same time. If you add a sender to the blacklist, then if that sender is on the whitelist, then that sender will be removed from the whitelist.

Note: The per-recipient white/black lists overrule the global white/blacklists for this domain.

To **Import** blacklists from a text file, create a text file will all the entries to blacklist, with one email address or domain (preceded by the '@' sign) per line.

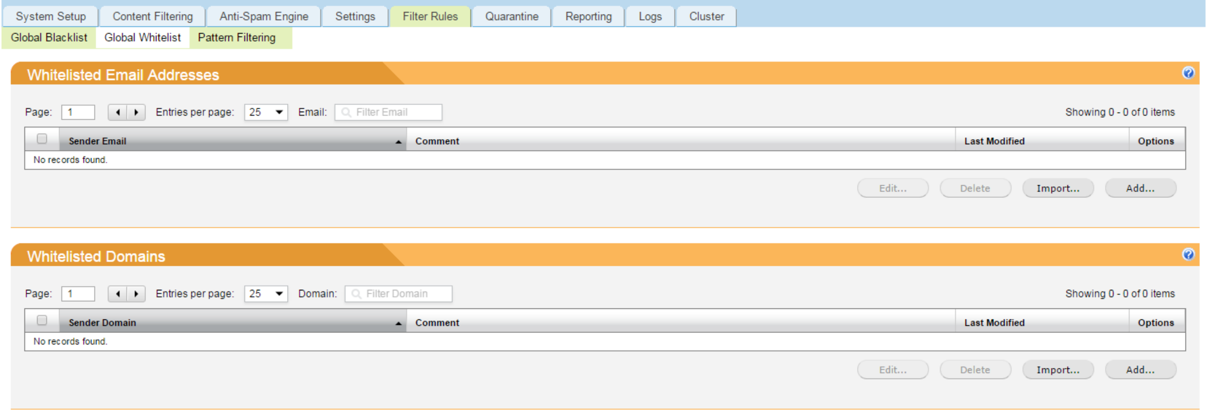
For example:

```
john@example.com
jane@example.com
@foobar.com
```

All lines starting with a '#' or ';' character will be treated as comments and ignored.

13.2 Configuring the Global Email Whitelist

The **Filter Rules > Global Whitelist** page allows you to control which messages are always allowed by SpamTitan. Messages from these email addresses and/or domains will be automatically whitelisted, and the messages from those senders will not be scanned by the anti-spam engine and be delivered to the intended recipient(s).



Whitelisted Email Addresses

Page: 1 Entries per page: 25 Email: Filter Email Showing 0 - 0 of 0 items

□	Sender Email	Comment	Last Modified	Options
No records found.				

Whitelisted Domains

Page: 1 Entries per page: 25 Domain: Filter Domain Showing 0 - 0 of 0 items

□	Sender Domain	Comment	Last Modified	Options
No records found.				

Figure 13-2 Configuring Global Whitelist

Click the **Add...** button to add a new whitelisted sender email address or domain, and the Add Whitelist entry dialog box will be displayed. Enter the email address or domain that you want to allow, and then press the Save button. The address must be of the form *user@example.com* - which will allow mail from that user to your account - or of the form *example.com* - which will allow all email from that domain to your account.

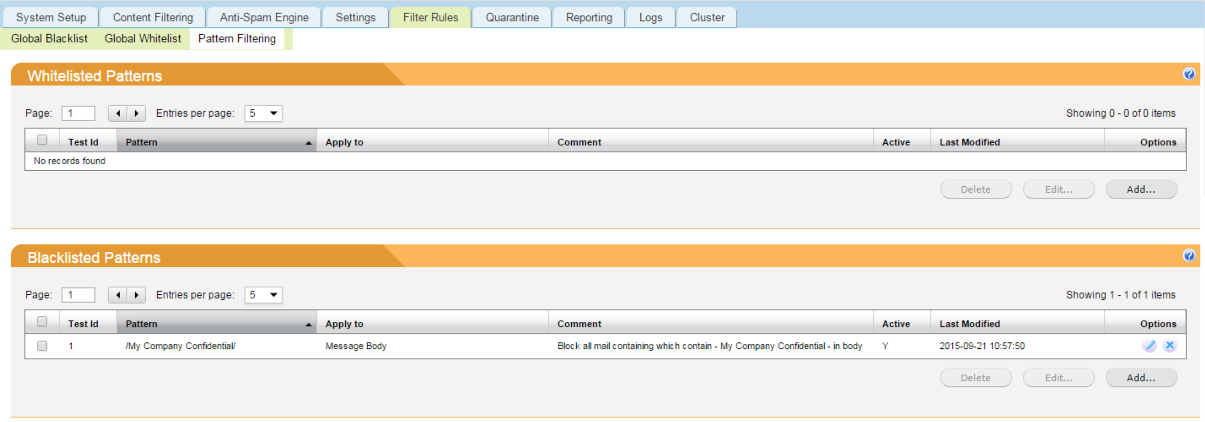
To delete entries from the lists click the ✕ icon for that domain or email address.

To **Import** whitelists from a text file, create a text file will all the entries to whitelist, with one email address or domain (preceded by the '@' sign) per line.

13.3 Pattern Filtering

Pattern Filtering provides the ability to block or accept messages based on filter rules applied to a message Subject, Headers or Body. In general, defining pattern filters should not be necessary and the vast majority of sites will correctly block or accept mail correctly without defining any filters here. Occasionally, it may be necessary to define filters that block or accept mails that are been incorrectly classified.

Additionally, Pattern Filters may be used to apply a Data Leak Prevention (DLP) policy for your organization to prevent, for instance, the leaking of credit card information from the organization.



Whitelisted Patterns

Page: 1 Entries per page: 5 Showing 0 - 0 of 0 items

□	Test Id	Pattern	Apply to	Comment	Active	Last Modified	Options
No records found							

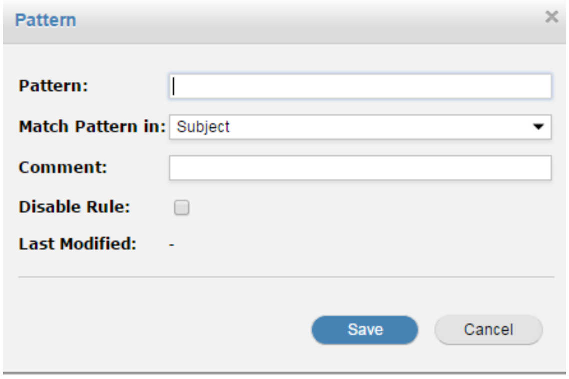
Blacklisted Patterns

Page: 1 Entries per page: 5 Showing 1 - 1 of 1 items

□	Test Id	Pattern	Apply to	Comment	Active	Last Modified	Options
□	1	/My Company Confidential/	Message Body	Block all mail containing which contain - My Company Confidential - in body	Y	2015-09-21 10:57:50	

Figure 13-3 Configuring Filter Rules

Click the **Add…** button to add a new pattern to whitelist or blacklist. The Pattern Dialog will be displayed.


Pattern

Pattern:

Match Pattern in: Subject

Comment:

Disable Rule: □

Last Modified: -

The fields on the Add/Edit Pattern dialog are as follows:

Field	Description
Pattern	The pattern to match. When creating filters you can use basic phrases or regular expressions. It is required that the pattern is enclosed by forward-slash (/) delimiter. In general, single word rules are poor filters as they don't take into account the context that the word is used in. For example, a filter /sex/ applied to a message subject does a simple case-sensitive search on the subject of the email for the string 'sex' and will block/accept the message if it finds it. However, this filter will also match 'unisex', 'sextuples' and others. In regular expressions a \b can be used to indicate where a word-break (anything that isn't an alphanumeric character or underscore) must exist for a match. The filter above can be made to not match 'unisex' or 'sextuples' by modifying it as follows: /\bsex\b/. Filters are case-insensitive.
Match Pattern in	Specify the part of the email message where the pattern should match. Possible values are: ▪ Subject ▪ Any Header ▪ Message body ▪ Subject or Message Body ▪ Any Header or Message Body

Comment	Optional comment field.
Disable Rule	Specifies if the rule is active or not.
Last Modified	Read-only field showing the last modified timestamp for this rule.

Table 13-1 Add/Edit Pattern dialog settings

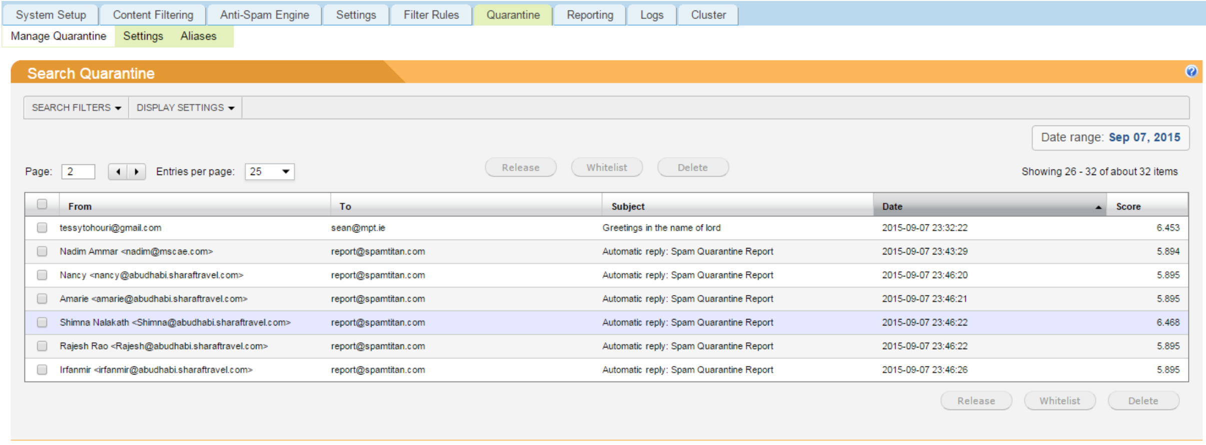
14 Quarantine

This chapter describes the quarantine management system, and how the administrator or end-user may review their quarantined messages. The chapter also describes the end-user quarantine reports, how they may be customized, and how users may set their own preferences as to when to receive the report.

14.1 Manage Quarantine

When evaluating messages for Spam SpamTitan applies hundreds of rules in order to arrive at an overall spam score for the message. By default, SpamTitan sets the spam threshold score at 5. If administrators find that this setting is too aggressive, or not aggressive enough then they can change the threshold on a per-domain or per-user basis. Any mail scoring above the threshold is considered spam and is quarantine (by default). All messages scoring below the threshold will be considered legitimate and passed onto the recipient(s).

The quarantine consists of a relational database which contains details on all messages that pass through the appliance and a reference to the quarantined file on disk.



Date range: **Sep 07, 2015**

Page: 2 Entries per page: 25

Showing 26 - 32 of about 32 items

☐	From	To	Subject	Date	Score
☐	tessytohouri@gmail.com	sean@mpt.ie	Greetings in the name of lord	2015-09-07 23:32:22	6.453
☐	Nadim Ammar <nadim@mscae.com>	report@spamtitan.com	Automatic reply: Spam Quarantine Report	2015-09-07 23:43:29	5.894
☐	Nancy <nancy@abudhabi.sharaftravel.com>	report@spamtitan.com	Automatic reply: Spam Quarantine Report	2015-09-07 23:46:20	5.895
☐	Amarie <amarie@abudhabi.sharaftravel.com>	report@spamtitan.com	Automatic reply: Spam Quarantine Report	2015-09-07 23:46:21	5.895
☐	Shimna Nalakath <Shimna@abudhabi.sharaftravel.com>	report@spamtitan.com	Automatic reply: Spam Quarantine Report	2015-09-07 23:46:22	6.468
☐	Rajesh Rao <Rajesh@abudhabi.sharaftravel.com>	report@spamtitan.com	Automatic reply: Spam Quarantine Report	2015-09-07 23:46:22	5.895
☐	Irfanmir <irfanmir@abudhabi.sharaftravel.com>	report@spamtitan.com	Automatic reply: Spam Quarantine Report	2015-09-07 23:46:26	5.895

Figure 14-1 Manage Quarantine page

The **Quarantine > Manage Quarantine** page allows the administrator to view all messages for all recipients that are in the quarantine. End users can access their own quarantine by logging into the User Interface using their own email address/password.

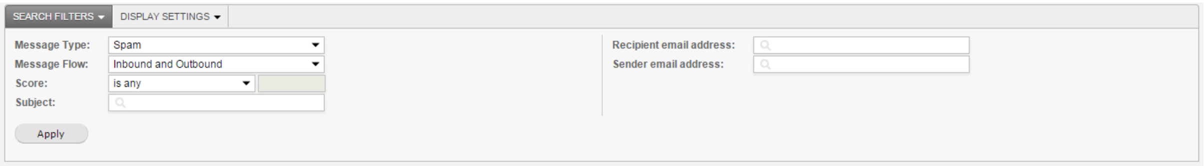
The following actions may be performed on messages in the Quarantine:

Quarantine Action	Description
View Message	To safely view a message that is in the quarantine click the From, To, or Subject of a particular quarantined message from the list of quarantined messages. This will open the message in a separate window. Note: All images in the message been reviewed will be blocked to prevent possible inappropriate content. If a message is subsequently to be released and delivered to your inbox then the original images will be present.
Release Message	Occasionally, there may be messages in the quarantine that

	are misidentified as spam (False positives). Users can redeliver the message to their inbox by clicking the **Deliver** link to the right of the message. The message will then be removed from the quarantine and the Bayesian database will be trained with the message so as to prevent this type of message from been blocked in the future.
Delete Message	Users can choose to delete messages one at a time, or in bulk by selecting the checkbox to the left of messages to delete. Deleting messages from the quarantine is in effect confirming that the message is spam. If the Bayesian database has not already learned this message as spam, then it will do so now. Note that if a message is deleted from the quarantine by the administrator then that message will not appear in the associated users' quarantine (or in their quarantine report).
Whitelist Sender	If the quarantine is been accessed by the administrator then this will add the sender of the selected message(s) to the global whitelist so that all future emails from this sender will bypass the SpamTitan antispam engine. They will still be scanned for viruses and banned attachments. Selecting this option will also Release the message from the quarantine. If the quarantine is been accessed by an end-user then the sender email address will be added to the users personal Whitelist. All future emails from this sender to this user will bypass the SpamTitan anti-spam engine. **Note**: The sender email address that is added to the Whitelist is the envelope email address. This is sometimes different from the address that appears in the From header of the message. You can see the message envelope sender email address by viewing the message.

Table 14-1 Actions which may be run against messages in Quarantine

The **Search Filters** allow the user to search for messages in the Quarantine based on a number of different criteria including message type, sender/recipient address, score, subject and message flow direction (inbound or outbound).



Message Type: Spam
Message Flow: Inbound and Outbound
Score: is any
Subject:
Recipient email address:
Sender email address:

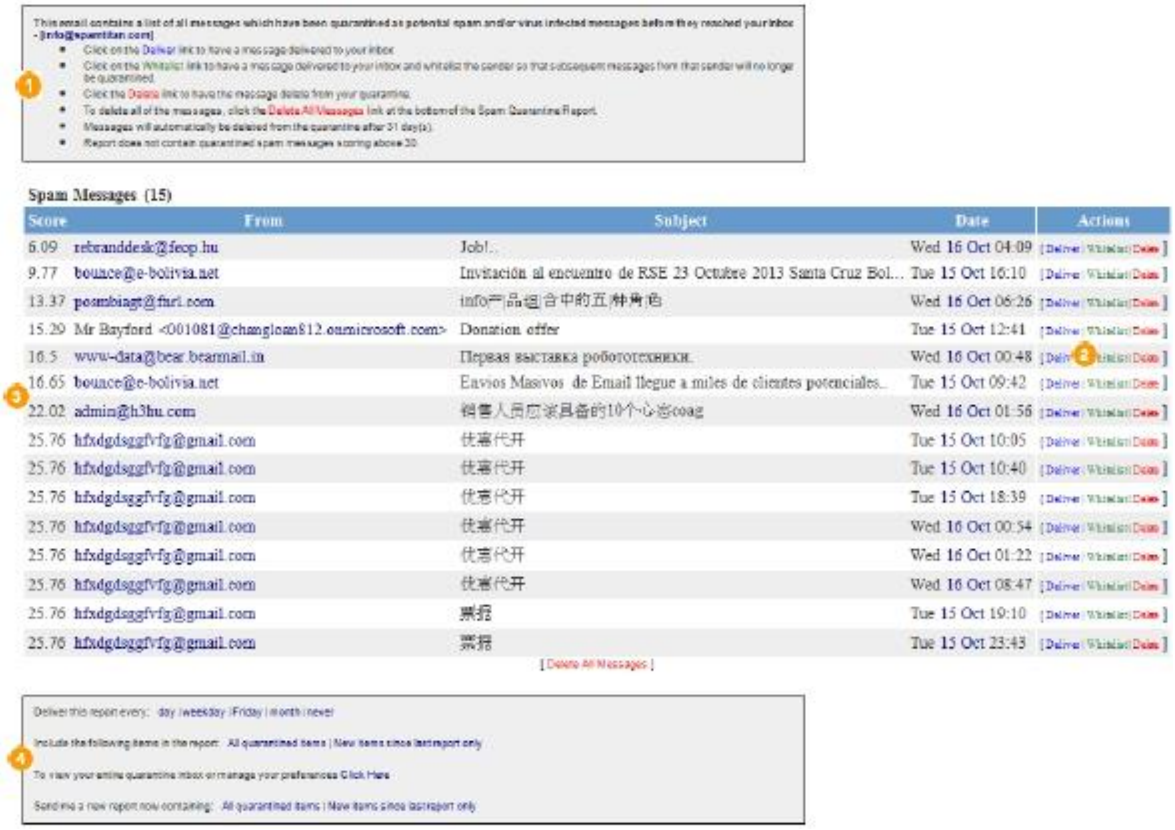
Figure 14-2 Quarantine Search Filters

14.2 Quarantine Reports

As well as being able to manage their quarantine from the web interface, end users may also manage their quarantined messages through the Quarantine Digest Reports that are automatically emailed to users on a periodic basic. The Quarantine Digest Report contains a list of email messages which have been caught and quarantined by the system, and provides links for users to interact and manage their quarantine.

SpamTitan will nightly generate the reports. For each user a report will only be generated if certain conditions are met:

- Today is a day for which the user requested a report in their preferences. E.g. if the user specified to receive reports on weekdays and today is Sunday then no report will be generated. Similarly if the user/admin specified that reports be sent weekly the report generation for that user will only occur on Fridays.
- The user must have quarantined messages.
- If the user/admin specified that the report should only contain details of quarantined messages since the last report and no such messages exist, then no report will be generated



This email contains a list of all messages which have been quarantined as potential spam and/or virus infected messages before they reached your inbox - [info@spamtitan.com]

- Click on the Deliver link to have a message delivered to your inbox.
- Click on the Whitelist link to have a message delivered to your inbox and whitelist the sender so that subsequent messages from that sender will no longer be quarantined.
- Click the Delete link to have the message delete from your quarantine.
- To delete all of the messages, click the Delete All Messages link at the bottom of the Spam Quarantine Report.
- Messages will automatically be deleted from the quarantine after 31 day(s).
- Report does not contain quarantined spam messages scoring above 30.

Spam Messages (15)

Score	From	Subject	Date	Actions
6.09	rebranddesk@feop.hu	Job!..	Wed 16 Oct 04:09	[Deliver | Whitelist | Delete]
9.77	bounce@e-bolivia.net	Invitación al encuentro de RSE 23 Octubre 2013 Santa Cruz Bol...	Tue 15 Oct 16:10	[Deliver | Whitelist | Delete]
13.37	poambiagt@furl.com	info产品组合中的五种角色	Wed 16 Oct 06:26	[Deliver | Whitelist | Delete]
15.29	Mr Bayford <001081@changloan812.onmicrosoft.com>	Donation offer	Tue 15 Oct 12:41	[Deliver | Whitelist | Delete]
16.5	www-data@bear.bearmail.in	Первая выставка робототехники.	Wed 16 Oct 00:48	[Deliver | Whitelist | Delete]
16.65	bounce@e-bolivia.net	Envios Masivos de Email llegue a miles de clientes potenciales..	Tue 15 Oct 09:42	[Deliver | Whitelist | Delete]
22.02	admin@h3hu.com	销售人员应该具备的10个心态coag	Wed 16 Oct 01:56	[Deliver | Whitelist | Delete]
25.76	hfxdgdsggfvfg@gmail.com	优惠代开	Tue 15 Oct 10:05	[Deliver | Whitelist | Delete]
25.76	hfxdgdsggfvfg@gmail.com	优惠代开	Tue 15 Oct 10:40	[Deliver | Whitelist | Delete]
25.76	hfxdgdsggfvfg@gmail.com	优惠代开	Tue 15 Oct 18:39	[Deliver | Whitelist | Delete]
25.76	hfxdgdsggfvfg@gmail.com	优惠代开	Wed 16 Oct 00:54	[Deliver | Whitelist | Delete]
25.76	hfxdgdsggfvfg@gmail.com	优惠代开	Wed 16 Oct 01:22	[Deliver | Whitelist | Delete]
25.76	hfxdgdsggfvfg@gmail.com	优惠代开	Wed 16 Oct 08:47	[Deliver | Whitelist | Delete]
25.76	hfxdgdsggfvfg@gmail.com	票据	Tue 15 Oct 19:10	[Deliver | Whitelist | Delete]
25.76	hfxdgdsggfvfg@gmail.com	票据	Tue 15 Oct 23:43	[Deliver | Whitelist | Delete]

[Delete All Messages]

Deliver this report every: day | weekday | Friday | month | never

Include the following items in the report: All quarantined items | New items since last report only

To view your entire quarantine inbox or manage your preferences Click Here

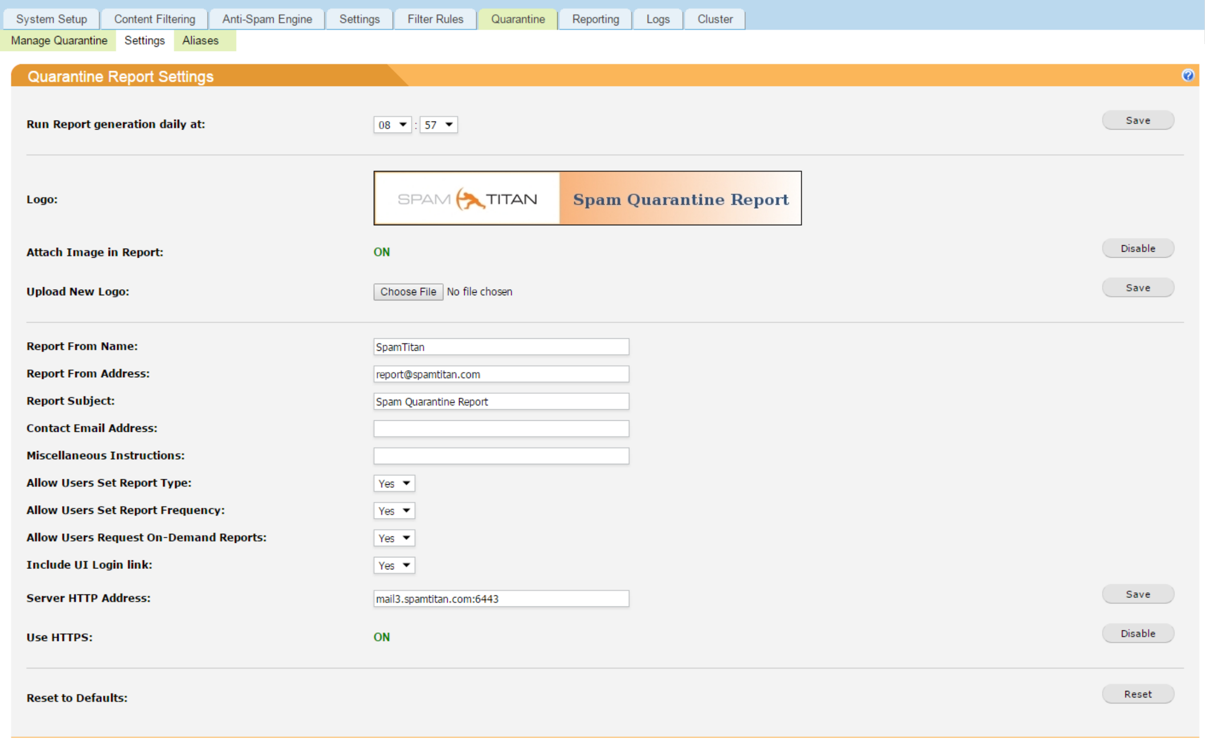
Send me a new report now containing: All quarantined items | New items since last report only

Figure 14-3 Email Quarantine Report

1. Custom Instructions
2. Message Actions to deliver, Whitelist or delete quarantined items
3. Quarantine Messages are sorted by Spam Score
4. User Report Preferences

14.3 Quarantine Report Settings

The **Quarantine > Settings** page allows you to configure settings for the users quarantine reports and customize the report with your own logo and instructions.



Run Report generation daily at: 08 : 57

Logo:

Attach Image in Report: ON

Upload New Logo: No file chosen

Report From Name: SpamTitan

Report From Address: report@spamtitan.com

Report Subject: Spam Quarantine Report

Contact Email Address:

Miscellaneous Instructions:

Allow Users Set Report Type: Yes

Allow Users Set Report Frequency: Yes

Allow Users Request On-Demand Reports: Yes

Include UI Login link: Yes

Server HTTP Address: mail3.spamtitan.com:6443

Use HTTPS: ON

Reset to Defaults:

Figure 14-4 Quarantine Report Settings page

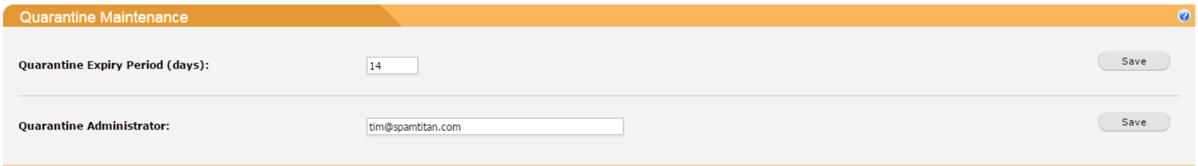
The following table describes the various settings that can be applied to the Quarantine reports:

Quarantine Report Settings	Description
Run Report generation daily at	Specifies the time that the overnight report generation script will be run daily. Click Save to save your changes.
Logo	You can change the appearance of the quarantine reports by changing the logo. This is the image that will be used in the quarantine digest report.
Attach image in Report	Specifies if the logo is displayed as the heading of a report. Default On.
Upload New Logo	Use the Upload New Logo option to replace the default logo with your own custom logo. The image should be approximately the same size as the default logo. Also ensure that the size of the image is appropriately small as it will be included in all reports that are generated.
Report From Name	This field specifies the descriptive name that will appear in the *From* address of the quarantine report. Default: SpamTitan Spam Appliance
Report From Address	This field specifies the email address that the quarantine report will appear to have come from. Default: noreply@SpamTitan.com. This should be

	changed to an address in your organization.
Report Subject	This field specifies the *Subject* for the quarantine report.
Contact Email Address	Optional contact email address that will appear in the instructions section of the quarantine report.
Miscellaneous Instructions	This field specifies optional instructions that can appear in the quarantine reports. This can be HTML formatted text e.g. it could contain a link to an internal webpage listing detailed user instructions.
Allow Users Set Report Type	Specifies if the report will contains links to allow the user change the report type that they receive. The report types are: ▪ All quarantine messages ▪ Quarantined messages since last report. This option is enabled by default.
Allow users Set Report Frequency	Specifies if the report will contain links to allow the user change when they can receive their reports. Option is enabled by default.
Allow users request on-demand Reports	Specifies if the report will contain a link to the web interface which allows the user to request an on demand report.
Include UI Login link	Specifies if the report will contain a link to the web interface so that the user can login directly to the web interface from the quarantine report.
Server HTTP Address	This specifies the IP address or fully qualified domain name of SpamTitan. All links in the quarantine report will use this reference.
Use HTTPS	Specifies if all links in the quarantine report use https or regular http.
Reset to Defaults	If at any time you want to revert to the factory installed defaults for the report appearance then click the Reset button.

Table 14-2 Quarantine Report settings

Messages that are stored in the quarantine that are not released or deleted must be purged at some time, as otherwise the quarantine will fill up and we will run out of disk space.



Quarantine Maintenance

Quarantine Expiry Period (days): 14

Quarantine Administrator: tim@spamtitan.com

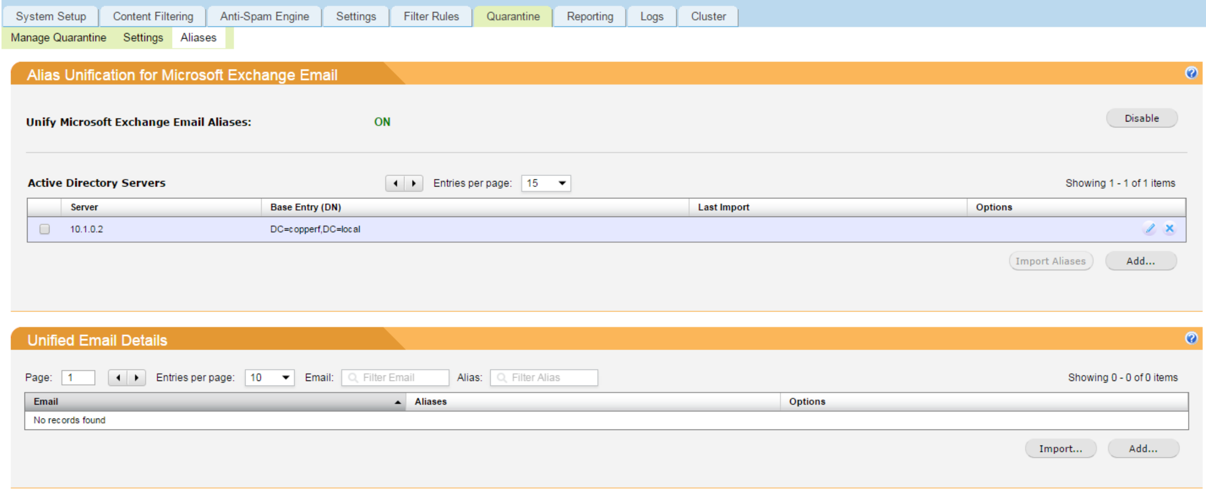
Figure 14-5 Quarantine Maintenance page

Enter the **Quarantine Expiry Period** specified in days and click the **Save** button. After this period, all mails that have not been released or deleted will be purged.

You may also specify a **Quarantine Administrator** by entering their email address here. This will give them access to the quarantine management tools.

14.4 Aliases

Alias unification provides the ability for users to see all their quarantined messages for all their alias email accounts when they receive a quarantine report, or when they login via the user interface.



Alias Unification for Microsoft Exchange Email

Unify Microsoft Exchange Email Aliases: ON

Active Directory Servers — Entries per page: 15 — Showing 1 - 1 of 1 items

	Server	Base Entry (DN)	Last Import	Options
□	10.1.0.2	DC=copperf,DC=local		

Unified Email Details

Page: 1 — Entries per page: 10 — Email: Filter Email — Alias: Filter Alias — Showing 0 - 0 of 0 items

Email	Aliases	Options
No records found		

Figure 14-6 Email Aliases

To add an Active Directory server to the list click on the **Add...** button. The **Add/Edit LDAP Server** dialog is displayed.

The entries on the Add/Edit LDAP Server dialog are as follows:

Setting	Description
LDAP server	The name of the LDAP server
Base entry (DN)	The base entry distinguished name (DN) as configured on the LDAP server. The base entry serves as the starting point of the LDAP directory search. For example, dc=example,dc=com. This field has an auto-complete function which will provide potential base entries.
Server login user	The username for accessing the LDAP server. £ is not permitted in the username.
Server login password	The password for accessing the LADP server. £ is not permitted in the password.
Import Frequency	Use this drop-down list to select the frequency at which you want to receive imports from the LDAP server.

Table 14-3 Add/Edit LDAP Server dialog settings

To automatically import user aliases from Active Directory, select one or more AD servers from the list and click on the **Import Aliases** button.

Imported aliases are displayed in the **Unified Email Details** list. This list may also be manually populated. To add aliases for an email address click on the **Add...** button. The **Add Alias dialog** is displayed.

The entries on the Add/Edit Alias dialog are as follows:

Field	Description
Delivery Address	Primary email address
Aliases	Enter additional names in the Aliases field that the user will receive email as. For example, if this account is for user john@example.com, you may also want to allow him to receive mail at john.doe@example.com

Table 14-4 Add/Edit Alias dialog settings

Note: It is recommended to add your primary address as an alias otherwise you will not be able to view your primary mail

Press the **Import** button to import a text file containing email addresses and their aliases. The text file must be in the following form:

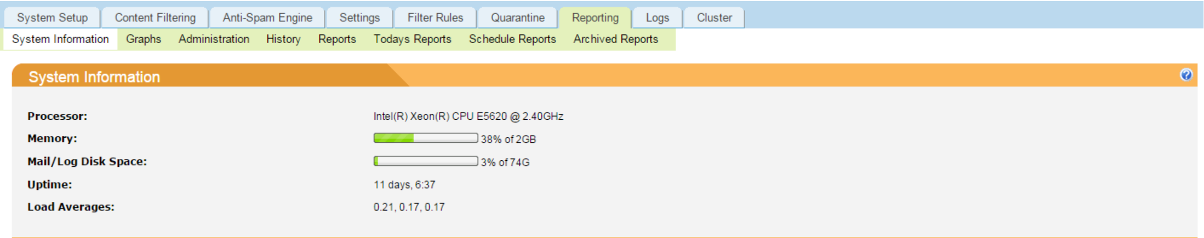
```
primary1 alias1 alias2 alias3
primary2 alias4 alias5
```

15 Reporting

This chapter describes the extensive reporting capabilities of SpamTitan.

15.1 System Information

The Reporting > System Information page provides an overview of the status of the SpamTitan appliance.



System Information

Processor:	Intel(R) Xeon(R) CPU E5620 @ 2.40GHz
Memory:	38% of 2GB
Mail/Log Disk Space:	3% of 74G
Uptime:	11 days, 6:37
Load Averages:	0.21, 0.17, 0.17

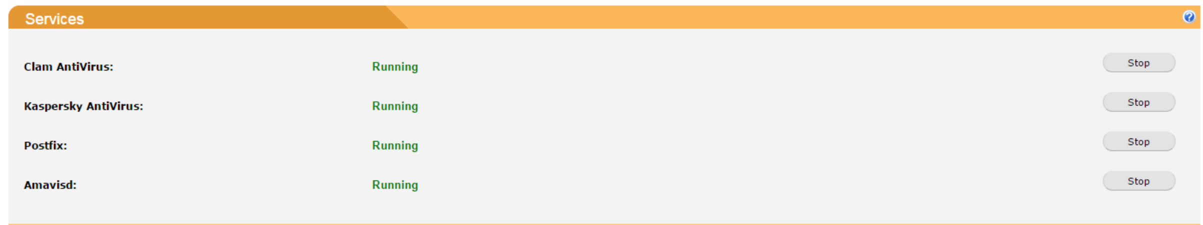
Figure 15-1 General System Information overview

The following table describes each of these settings:

Setting	Description
Processor	The processor that is installed in the SpamTitan server.
Memory	The total amount of memory that is available.
CPU Temperature	Indicates the current CPU temperature. If the CPU gets excessively hot (greater than 70C) then this may indicate a problem with the on-board fan.
Mail/Log Disk Space	Indicates how much disk space is available for the message quarantine and the system log files and how much of this disk space is currently in use.
Uptime	Shows how long the SpamTitan server has been running since the last reboot.
Load Averages	This indicates the current load on the SpamTitan server. It shows the number of running processes in the queue waiting for processor time. The numbers reflect the load average over the last minute, over the last 5 minutes and over the last 15 minutes respectively. A load average of 1 means that there was 1 process waiting for the CPU all the time. A process which is using 100% of the CPU only for a short time will result in a peak in the 1 minute average. A process hogging the CPU for a long time will raise the base level of the 15 minute average. Therefore, a high 15 minute average (>5) indicates low CPU power

Table 15-1 System Information fields

SpamTitan has a number of key daemons or **services** that must be always running to ensure correct operation of SpamTitan.



Services

Clam AntiVirus: Running

Kaspersky AntiVirus: Running

Postfix: Running

Amavisd: Running

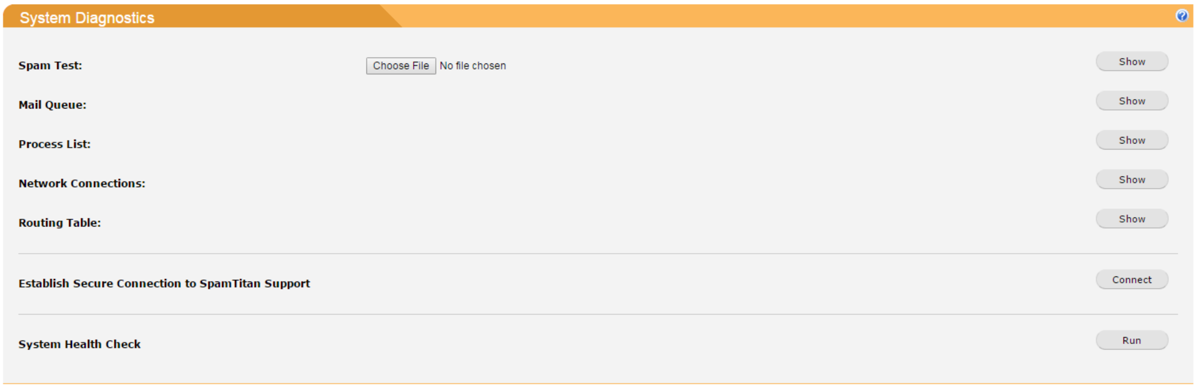
Figure 15-2 Manage SpamTitan services

These are:

- The Clam Antivirus service
- Kaspersky Antivirus (should only be running if Kaspersky is enabled)
- Postfix mail transfer agent
- Amavisd mail service
- Cluster Daemon (display only if running in a cluster)

If any of these services are not running, then restart them, checking the log files to ensure that they started OK.

The **System Diagnostics** section on the **Reporting > System Information** page allows you to run some troubleshooting commands on the appliance that you may then send to SpamTitan Support if required.



System Diagnostics

Spam Test: Choose File No file chosen

Mail Queue:

Process List:

Network Connections:

Routing Table:

Establish Secure Connection to SpamTitan Support

System Health Check

Figure 15-3 System Diagnostics

The following table illustrates the various tools that are available to you to troubleshoot problems with the system:

System Diagnostic	Description
Spam Test	You can use the Spam Test command to emulate how a message will be classified by the SpamTitan anti-spam engine. Use the Upload feature to upload a message to the appliance to test. The output of the test will be displayed in a popup window. You can see which rules fired on the particular message by viewing the Content analysis details at the end of the output.

Mail Queue	This command displays a summary of the mail messages that are queued for delivery. The **Queue ID** shows the internal identifier used on this system for the message along with a possible status character. The status characters are either * to indicate the job is being processed; X to indicate that the load is too high to process the job; and – to indicate that the job is too young to process. The **Size** indicates the size of the message in bytes. The **Arrival Time** indicates the time the message was accepted into the queue, and the **Sender/Recipient** indicates the envelope sender and recipient(s). If a message is retained in the queue then a second line will show the reason for the message to be retained. Click the auto refresh checkbox to have the display automatically refresh every 5 seconds.
Process List	The process list command displays information about all the processes that are running on the SpamTitan server.
Network Connections	This displays a list of all active network connections to and from the SpamTitan.
Routing Table	Displays the contents of the routing table on the system.
Establish Secure Connection to SpamTitan Support	If it is necessary for SpamTitan Support to troubleshoot any issues with the appliance, then you can press the Connect button to establish a secure tunnel with SpamTitan. This will allow SpamTitan Support to gain access to the appliance to diagnose and resolve the problem.
System Health Check	The System Health Check will perform a series of diagnostic checks on the system to ensure that it is configured correctly, and will highlight if there are any potential issues.

Table 15-2 System Diagnostic options

There are also standard **network trace tools** available under the **Tools** section which you can use to test network connectivity from the appliance to remote hosts.

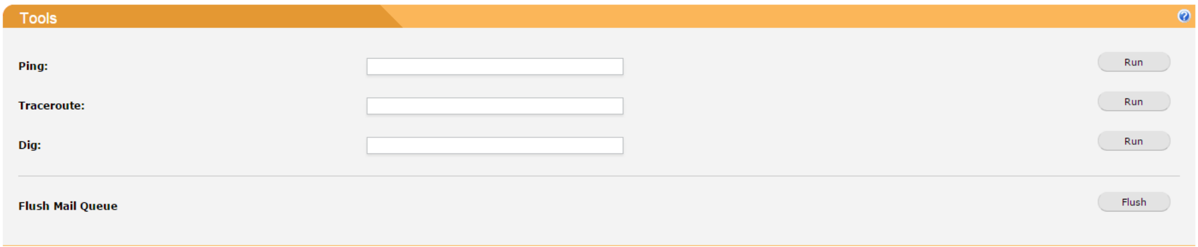


Figure 15-4 Using Network Trace tools

The following table describes the various tools that are available:

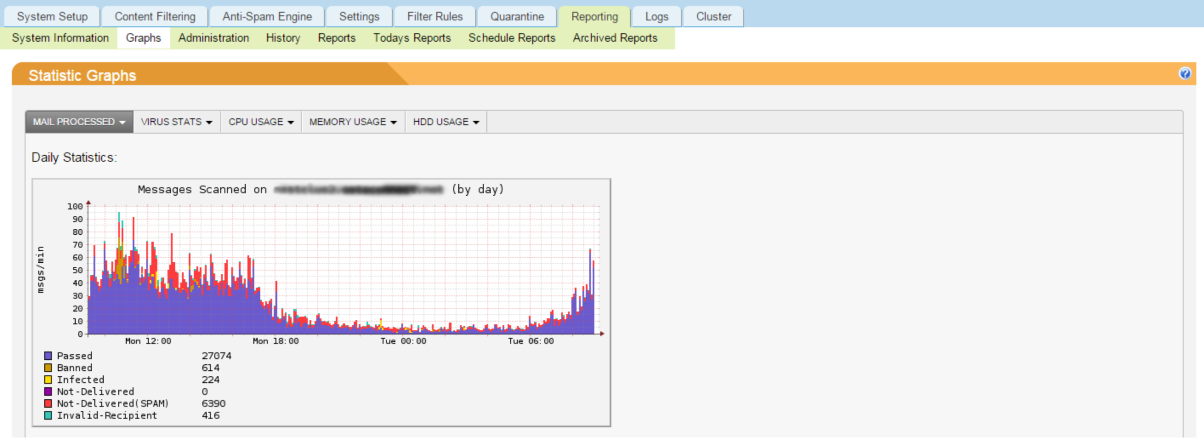
Tool	Description
Ping	This allows you to test the connection with a remote host on the IP level. Please note that the ping and traceroute

	tools require that ICMP is not blocked on your firewall if you are trying to contact an external host. The ping utility uses the ICMP protocol to elicit an ICMP response from a host or gateway.
Traceroute	The traceroute utility is similar to the ping utility except that it will display the route packets will take from SpamTitan to the remote host or gateway. This command can be useful for diagnosing routing problems.
Dig	Dig is a tool for interrogating DNS name servers. It performs DNS name lookups and displays the answers that are returned from the name server that are configured in the System Setup section. This is similar to *nslookup*, only more powerful. Enter the name of the host that you want to lookup followed by any optional dig arguments. For instance to lookup the MX records for spamtitan.com enter "spamtitan.com -t MX".
Flush Mail Queue	If items are retained in the mail queue, then the mail delivery agent (Postfix) will continue to try and deliver the mail for 4 days. Flushing the mail queue will attempt to deliver all those messages in the deferred mail queue. Normally, attempts to deliver delayed mail happen at regular intervals, the interval doubling after each failed attempt. **Warning**: flushing undeliverable mail frequently will result in poor delivery performance of other mail.

Table 15-3 Network Trace Tools

15.2 Graphs

The graphs on the **Reporting > Graphs** page show daily, weekly, monthly and yearly statistics on the number of email **messages processed**, marked as spam and containing viruses. Here we can also find graphs on **Virus Stats**, as well as **CPU**, **Memory** and **HDD Usage**.



Daily Statistics:

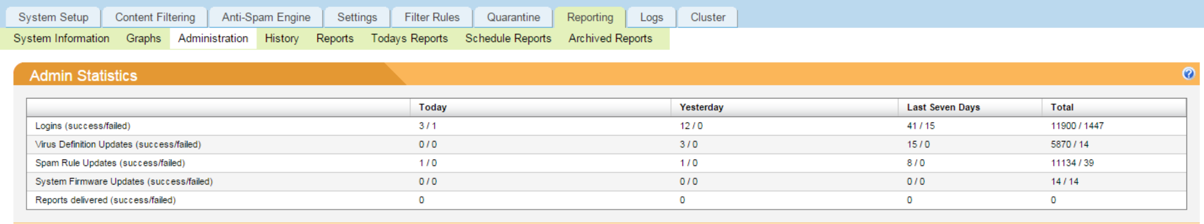
Messages Scanned on [redacted] (by day)

```
Passed                27074
Banned                614
Infected              224
Not-Delivered         0
Not-Delivered(SPAM)   6390
Invalid-Recipient     416
```

Figure 15-5 Reporting Graphs

15.3 Administration

The **Reporting > Administration** page provides an overview of administrative events over the last 30 days.



Admin Statistics

	Today	Yesterday	Last Seven Days	Total
Logins (success/failed)	3 / 1	12 / 0	41 / 15	11900 / 1447
Virus Definition Updates (success/failed)	0 / 0	3 / 0	15 / 0	5870 / 14
Spam Rule Updates (success/failed)	1 / 0	1 / 0	8 / 0	11134 / 39
System Firmware Updates (success/failed)	0 / 0	0 / 0	0 / 0	14 / 14
Reports delivered (success/failed)	0	0	0	0

Figure 15-6 Reporting Administration statistics

Each row has 4 columns showing a total for the number of the particular event that occurred today, yesterday, the last 7 days and in total. Data cells contain either 2 numbers (success/failed) or only one number showing the total amount for that event.

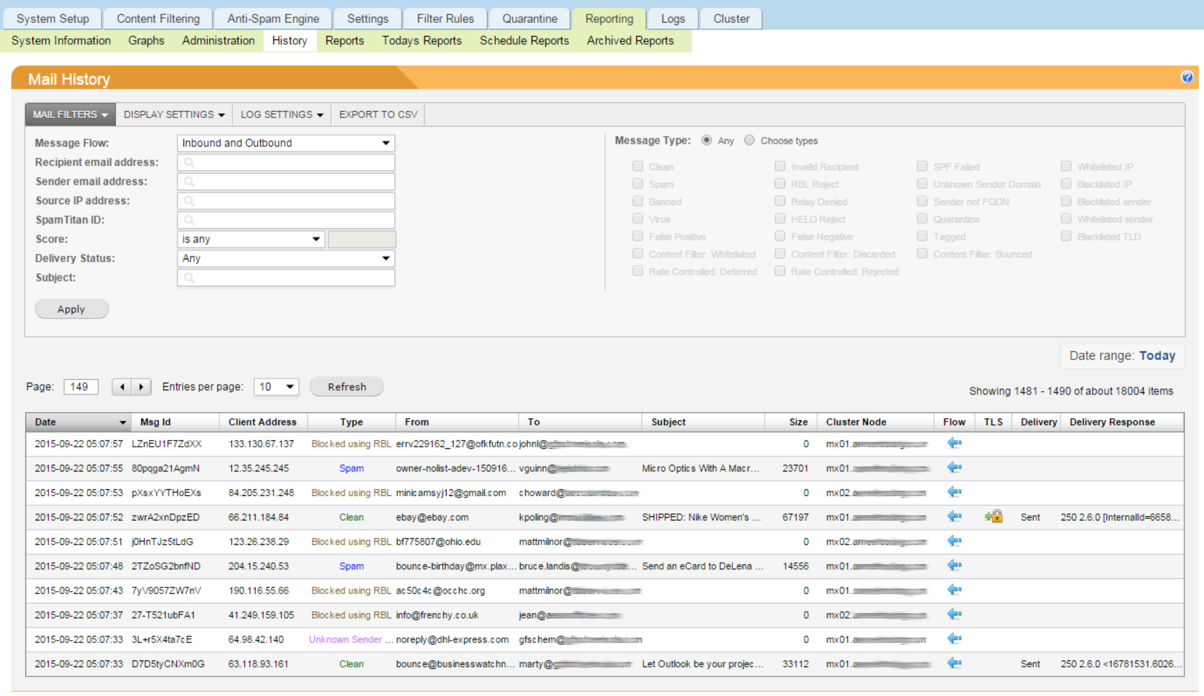
The following table describes each of the events recorded.

Event	Description
Logins (success/failed)	This shows the number of successful and unsuccessful login attempts to the web interface.
Virus Definition Updates	This field shows the virus definition updates that were made for the Clam Antivirus scanner. Success shows the number of successful updates of new virus definitions. The number does not reflect the number of checks for new definitions which by default are checked every hour.
Spam Rule Updates (success/failed)	This shows the number of successful and unsuccessful updates of the custom spam rules.
System Firmware Updates (success/failed)	This shows the number of successful and unsuccessful updates for system firmware update
Reports delivered	This shows the number of quarantine digest reports that were generated and successfully delivered.

Table 15-4 Reporting Administration entries

15.4 History

The **Reporting > History** page enables you to review all mail transactions that have passed through SpamTitan. The advanced search filters allow you to search based on specific criteria such as sender, recipient, IP source address etc.



Message Flow: Inbound and Outbound
Recipient email address:
Sender email address:
Source IP address:
SpamTitan ID:
Score: is any
Delivery Status: Any
Subject:

Message Type: ● Any ○ Choose types

□ Clean □ Invalid Recipient □ SPF Failed □ Whitelisted IP
□ Spam □ RBL Reject □ Unknown Sender Domain □ Blacklisted IP
□ Banned □ Relay Denied □ Sender not FQDN □ Blacklisted sender
□ Virus □ HELO Reject □ Quarantine □ Whitelisted sender
□ False Positive □ False Negative □ Tagged □ Blacklisted TLD
□ Content Filter: Whitelisted □ Content Filter: Discarded □ Content Filter: Bounced
□ Rate Controlled: Deferred □ Rate Controlled: Rejected

Date range: Today

Page: 149 Entries per page: 10

Showing 1481 - 1490 of about 18004 items

Date	Msg Id	Client Address	Type	From	To	Subject	Size	Cluster Node	Flow	TLS	Delivery	Delivery Response
2015-09-22 05:07:57	LZnEU1F7ZdXX	133.130.67.137	Blocked using RBL	errv229162_127@ofkfutn.co	johnl@[redacted]		0	mx01.[redacted]	←			
2015-09-22 05:07:55	80pqga21AgmN	12.35.245.245	Spam	owner-nolist-adev-150916...	vguinn@[redacted]	Micro Optics With A Macr...	23701	mx01.[redacted]	←			
2015-09-22 05:07:53	pXsxYYTHoEXs	84.205.231.248	Blocked using RBL	minicamsyj12@gmail.com	choward@[redacted]		0	mx02.[redacted]	←			
2015-09-22 05:07:52	zwrA2xnDpzED	66.211.184.84	Clean	ebay@ebay.com	kpoling@[redacted]	SHIPPED: Nike Women's ...	67197	mx01.[redacted]	←	🔒	Sent	250 2.6.0 [InternalId=6658...
2015-09-22 05:07:51	j0HnTJz5tLdG	123.26.238.29	Blocked using RBL	bf775807@ohio.edu	mattmilnor@[redacted]		0	mx02.[redacted]	←			
2015-09-22 05:07:48	2TZoSG2bnfND	204.15.240.53	Spam	bounce-birthday@mx.plax...	bruce.landis@[redacted]	Send an eCard to DeLena ...	14556	mx01.[redacted]	←			
2015-09-22 05:07:43	7yV9057ZW7nV	190.116.55.66	Blocked using RBL	ac50c4c@occhc.org	mattmilnor@[redacted]		0	mx01.[redacted]	←			
2015-09-22 05:07:37	27-T521ubFA1	41.249.159.105	Blocked using RBL	info@frenchy.co.uk	jean@[redacted]		0	mx02.[redacted]	←			
2015-09-22 05:07:33	3L+r5X4ta7cE	64.98.42.140	Unknown Sender ...	noreply@dhl-express.com	gfschem@[redacted]		0	mx01.[redacted]	←			
2015-09-22 05:07:33	D7D5tyCNXm0G	63.118.93.161	Clean	bounce@businesswatchn...	marty@[redacted]	Let Outlook be your projec...	33112	mx01.[redacted]	←		Sent	250 2.6.0 <16781531.6026...

Figure 15-7 History page

The following table describes the various **mail filters** that can be employed on the mail history logs. Note that the filters can be applied together to narrow the search.

Filter	Description
Message Flow	Indicates the message flow direction: Inbound or Outbound
Message Type	The message type filter allows you to filter messages based on how they were classified by SpamTitan. The following message type classifications are available: ▪ All Transactions (default) ▪ Clean messages ▪ Spam messages ▪ Banned Attachment messages ▪ Virus Infected messages ▪ False Positives (messages released from quarantine). ▪ Messages rejected to Invalid Recipients ▪ Messages rejected using RBL ▪ Messages rejected due to Relay attempt ▪ Message rejected with invalid HELO greeting ▪ False Negatives (messages incorrectly classified as clean) ▪ Messages rejected by SPF failure ▪ Messages with unknown sender domain ▪ Sender without a FQDN (Fully Qualified Domain

	Name) ▪ Quarantined messages ▪ Tagged Mail (Message identified as containing spam/virus/banned attachment, but recipient has a policy to pass) ▪ Messages with a Blacklisted Top Level Domain ▪ Messages from a Whitelisted/Blacklisted IP ▪ Messages from a Whitelisted/Blacklisted Sender ▪ Messages whitelisted by the Content Filter ▪ Messages discarded by the Content Filter ▪ Messages bounced by the Content Filter ▪ Rate Controlled messages deferred ▪ Rate Controlled messages rejected
Recipient email address	Filter results using the recipient email address. Use ‘*’ as a wildcard character e.g. to filter all messages to domain example.com enter **@example.com*
Sender email address	Filter results using the sender email address. Use ‘*’ as a wildcard character e.g. to filter all messages from the .co.uk domain enter *@*.co.uk
Source IP address	Filter results based on the connecting client IP address
SpamTitan ID	The internal SpamTitan ID which is assigned to every message.
Score	The SpamTitan spam score assigned to a message. Messages which are not analysed for spam are will have no score (e.g. rejected messages)
Delivery Status	The delivery status may be one of: ▪ Any ▪ Sent ▪ Deferred ▪ Bounced ▪ Expired Note that messages rejected or quarantined by SpamTitan will have no delivery status assigned to them as they have not been delivered.
Subject	Filter based on message subject. Use ‘*’ for wildcards.

Table 15-5 History mail filters

Press the **Apply** button after selecting your search filters to refresh the display.

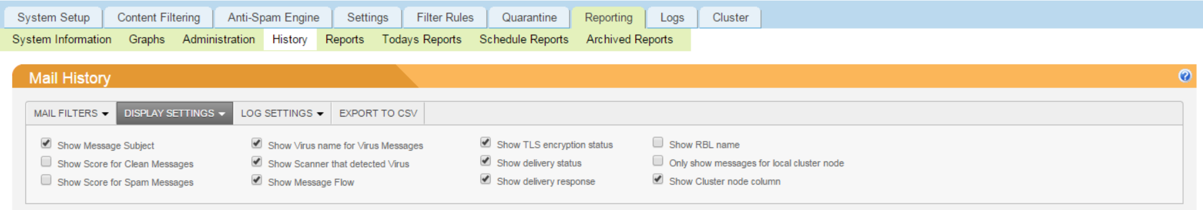
The following table describes each of the columns that are displayed in the mail transaction history table:

Column	Description
Date	Specifies the time and date that the message was processed.
Message Id	This is the internal message Id that SpamTitan has assigned to the message. Click the Message Id to view extended details on this particular message in a popup window.

Client Address	This is the source IP address of the host that sent the message to us. Note: If all your mail is relayed through an upstream mail relay before arriving at SpamTitan then this will contain the address of the upstream mail relay.
Type	The message type as classified by SpamTitan. See the History Filters table above for a description of the various message types.
From	The envelope sender address.
To	The envelope recipient address.
Subject	This is the subject header of the received message.
Size	The size of the message
Flow	The direction of the message ▪ Inbound ▪ Outbound ▪ Internal
TLS	Indicates if TLS was applied to the message. May be one of: ▪ Received over encrypted TLS channel ▪ Sent out over encrypted TLS channel ▪ Received and sent out over encrypted TLS channel
Delivery	Indicates the delivery status of the message. See filter table above for various values.
Delivery Response	This shows the SMTP response from the destination server. This can be useful to indicate, for instance, why a remote server rejected a message.

Table 15-6 History columns

The settings on the **Display Settings** tab allow you to control what columns and information are displayed in the mail history.



☑ Show Message Subject
☐ Show Score for Clean Messages
☐ Show Score for Spam Messages
☑ Show Virus name for Virus Messages
☑ Show Scanner that detected Virus
☑ Show Message Flow
☑ Show TLS encryption status
☑ Show delivery status
☑ Show delivery response
☐ Show RBL name
☐ Only show messages for local cluster node
☑ Show Cluster node column

Figure 15-8 Configuring History Display settings

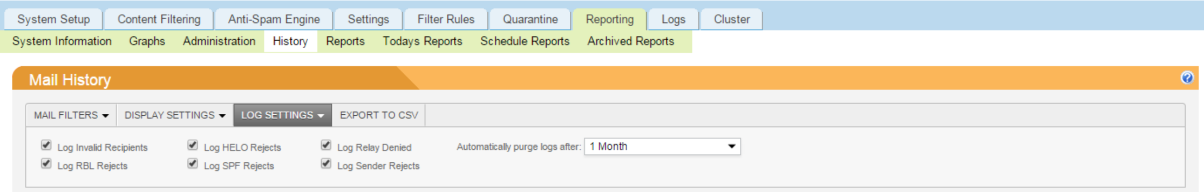
The following table describes the various Display Settings:

Display Setting	Description
Show Message Subject	Display the subject of the message
Show Score for Clean Messages	If enabled, the score assigned by SpamTitan will be displayed in the Type column of the history view for messages classified as Clean.
Show Score for Spam Messages	If enabled, the score assigned by SpamTitan will be displayed in the Type column of the history view for messages classified as Spam.
Show Virus name for Virus Messages	If enabled, then the name of the virus that the virus scanner detected will be displayed in the Type column of the history view for virus messages. Note: If more than 1 virus scanner is enabled then it is likely that the different virus scanners have different names for the virus. In this case the name of the virus as identified by the virus scanner which identified the virus first will be used.
Show Scanner that detected Virus	If enabled, then the name(s) of the virus scanner(s) that detected the virus will be display in the Type column of the history view for virus messages.
Show Message Flow	Show in which direction the Message is coming from and going to
Show TLS encryption status	Show the status of the Transport Layer Security (TLS)
Show delivery status	Show Delivery Status of the message.
Show delivery response	Show SMTP response from destination server.
Show RBL name	Show the name of the RBL that blocked the message
Only show messages for local cluster node	Clicking this option will ensure that only messages for the local cluster node are displayed.
Show Cluster node column	This will enable the user to see a cluster node column on the table displayed

Table 15-7 History display options

Settings will be remembered for next visit to this page.

The settings on the **Log Settings** tab allow you control various logging settings.



☑ Log Invalid Recipients
☑ Log RBL Rejects
☑ Log HELO Rejects
☑ Log SPF Rejects
☑ Log Relay Denied
☑ Log Sender Rejects
Automatically purge logs after: 1 Month

Figure 15-9 Configuring Log settings

The following table describes the various Log Settings:

Log Setting	Description
Log Invalid Recipients	If disabled, then messages from invalid recipients will not be logged in the database.
Log RBL Rejects	If disabled, then messages from RBL rejects will not be

	logged in the database.
Log HELO Rejects	If disabled, then messages from HELO rejects will not be logged in the database.
Log SPF Rejects	If disabled, then messages from SPF rejects will not be logged in the database.
Log Relay Denied	If disabled then massages whose relay is denied will not be logged in the database.
Log Sender Rejects	If disabled then messages from rejected senders will not be logged in the database.
Auto purge logs after	By default, messages are automatically purged from the database after 3 months. However on busy servers this may need to be lowered. **Note**: If the number of unique messages in the server exceeds 2 million then the oldest records (that are not quarantined) will be purged. For this reason, you may want to disable logging of the above messages. The aggregated total of each of these message types will be still be available on the dashboard and via the reports.

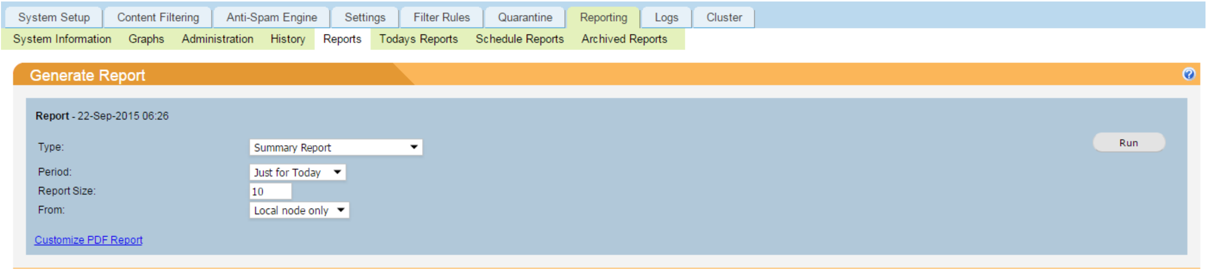
Table 15-8 History Log settings

The **Export to CSV** link allows you to download all transactions for the given search criteria to a Microsoft Excel spreadsheet.

Click the **Refresh** link to refresh the history view. Since the entire history is not shown on one page, use the links at the bottom of the page to jump to other pages.

15.5 Reports

The **Reporting > Reports** page allows you to generate a number of on-demand reports.



Report - 22-Sep-2015 06:26

Type: Summary Report

Period: Just for Today

Report Size: 10

From: Local node only

Figure 15-10 Generating Reports

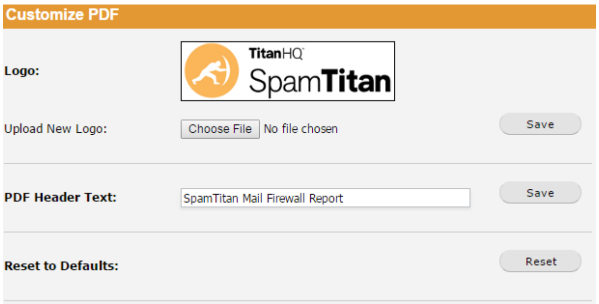
The following table describes the options available to you when generating on-demand reports:

Field	Description
Report	Date the report was generated.
Type	Select the report type from the following: ▪ Summary Report

	▪ Top Spam Relays ▪ Top Spam Recipient ▪ Top Virus Relays ▪ Top Virus Recipients ▪ Top Viruses ▪ Top Virus Scanners ▪ Top RBLs ▪ Top Invalid Recipient Relays ▪ Top HELO Rejected Relays ▪ Top Email Recipients (mails) ▪ Top Email Recipients (MB) ▪ Top Email Senders (mails) ▪ Top Email Senders (MB) ▪ Domain Summary Report ▪ Domain Group Summary Report ▪ License Usage Report
Period	This specifies the period for which the report will be generated. Options available are: ▪ Just for Today ▪ From Yesterday ▪ Last 7 Days ▪ All Note: a report period of All will generate a report based on all the records in the database. As records are automatically purged this may not include all records since the appliance was installed. See Mail History Log for more details.
Report Size	Indicates the number of items to include in the report (relevant only for top-ten type reports). Note: The pie chart will be limited to a maximum of 25 items.
From	Select whether to run reports on the Cluster, if applicable, or on individual nodes.

Table 15-9 Generate Reports options

Click the **Customize PDF Report** link to make customizations to your PDF reports.



Customize PDF

Logo:

Upload New Logo: Choose File No file chosen

PDF Header Text: SpamTitan Mail Firewall Report

Reset to Defaults:

Figure 15-11 Customize PDF Reports dialog

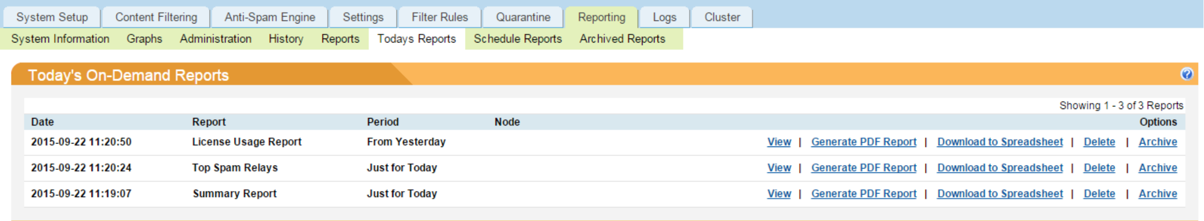
The following table describes the settings on the Customize PDF dialog

Setting	Description
Logo	The current logo in use for PDF reports
Upload New Logo	Click the *Choose File* button and choose a replacement logo to be used and then click *Save*. Note the logo size should be approx. 220x60px – otherwise the logo may be resized.
PDF Header Text	This text will be displayed in the Header of each PDF page.
Reset to Defaults	Reset the customized PDF report settings to the factory default.

Table 15-10 Customize PDF dialog settings

15.6 Today's On-Demand Reports

The **Reporting > Today's Reports** Tab shows the on-demand reports that were requested today. Reports are purged from here daily. If you wish to maintain the report for longer, then you can Archive it.



Today's On-Demand Reports

Showing 1 - 3 of 3 Reports

Date	Report	Period	Node	Options
2015-09-22 11:20:50	License Usage Report	From Yesterday		View | Generate PDF Report | Download to Spreadsheet | Delete | Archive
2015-09-22 11:20:24	Top Spam Relays	Just for Today		View | Generate PDF Report | Download to Spreadsheet | Delete | Archive
2015-09-22 11:19:07	Summary Report	Just for Today		View | Generate PDF Report | Download to Spreadsheet | Delete | Archive

Figure 15-12 Today's on-demand Reports

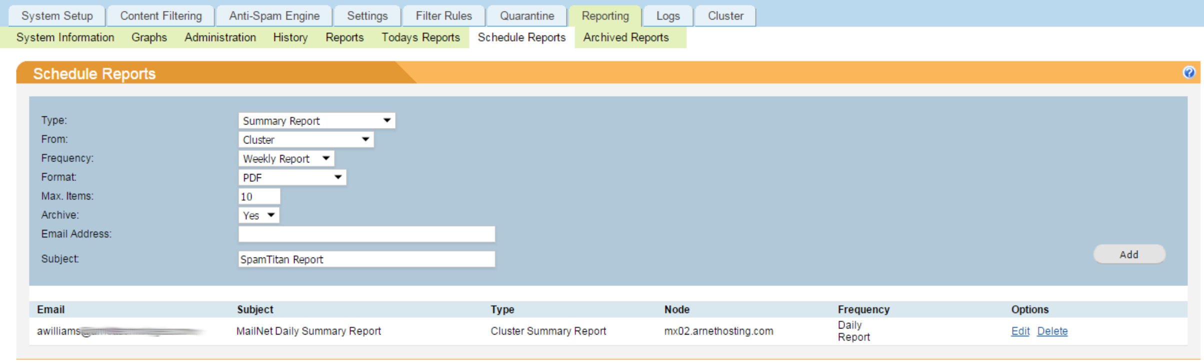
The Report displays the date, the type of report it is, the period of time over which it was run and on which node the information was collected from. The following options are then available for each report:

Option	Description
View	Click this link to view your generated report. It will display information depending on the type of report you have selected to run. It can be displayed in the form of a table and a pie chart. If your specified report settings return no information the following message will be returned: '*Report produced no data with supplied attributes*'.
Generate PDF Report	Click this link to generate a PDF version of the report.
Download to Spreadsheet	Click this link to download the report as a Microsoft Excel spreadsheet.
Delete	Delete the selected report.
Archive	Archive the selected report. It will now be viewable under the Reporting > Archived Reports tab.

Figure 15-13 On-demand report options

15.7 Scheduled Reports

SpamTitan provides the ability to schedule **Daily**, **Weekly** or **Monthly** reports to be generated and which can then be emailed to the specified distribution list and optionally archived on the appliance.



Type: Summary Report
From: Cluster
Frequency: Weekly Report
Format: PDF
Max. Items: 10
Archive: Yes
Email Address:
Subject: SpamTitan Report

Email	Subject	Type	Node	Frequency	Options
awilliams@[redacted]	MailNet Daily Summary Report	Cluster Summary Report	mx02.arnethosting.com	Daily Report	Edit Delete

Figure 15-14 Scheduled Reports

The following table specifies the various options for scheduling reports:

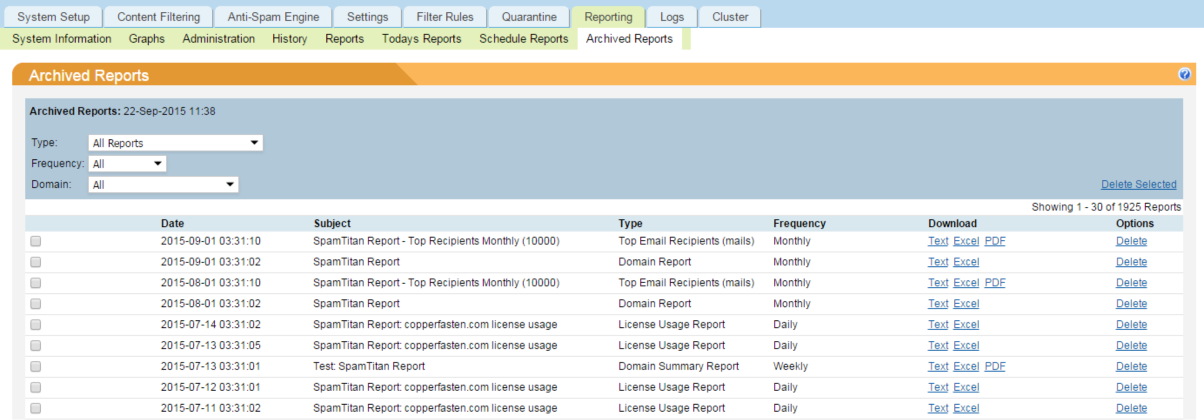
Option	Description
Type	The following reports may be scheduled: ▪ Summary Report ▪ Top Spam Relays ▪ Top Spam Recipients ▪ Top Virus Relays ▪ Top Virus Recipients ▪ Top Viruses ▪ Top RBLs ▪ Top Invalid Recipient Relays ▪ Top HELO Rejected Relays ▪ Top Email Recipients (messages) ▪ Top Email Recipients (bytes) ▪ Top Email Senders (mails) ▪ Top Email Senders (bytes) ▪ Domain Summary Report
From	Select whether to run reports on the Cluster, if applicable, or on individual nodes.
Frequency	▪ **Daily** reports will generate a report of the specified type for the previous day's activity. ▪ **Weekly** reports will be run each Monday and will produce a report of the specified type for the previous Monday-Sunday period. ▪ **Monthly** reports will be run on the 1st of the month and will produce a report for the previous month.
Format	Reports can be generated in as a **PDF** document, a **text** document, a Microsoft **Excel** spreadsheet or all three.
Max Items	The maximum number of items to display in the report.
Archive	Specifies if the report should be archived on the

	appliance.
Email Address	The report will be emailed to the addresses in this field. Separate email addresses with spaces.
Subject	The Subject to use for emailed reports.

Table 15-11 Scheduled Reports options

15.8 Archived Reports

The **Reporting > Archived** Reports page lists all the reports that have been archived on SpamTitan. These are the scheduled reports that are generated periodically.



Archived Reports: 22-Sep-2015 11:38

Type: All Reports

Frequency: All

Domain: All

Showing 1 - 30 of 1925 Reports

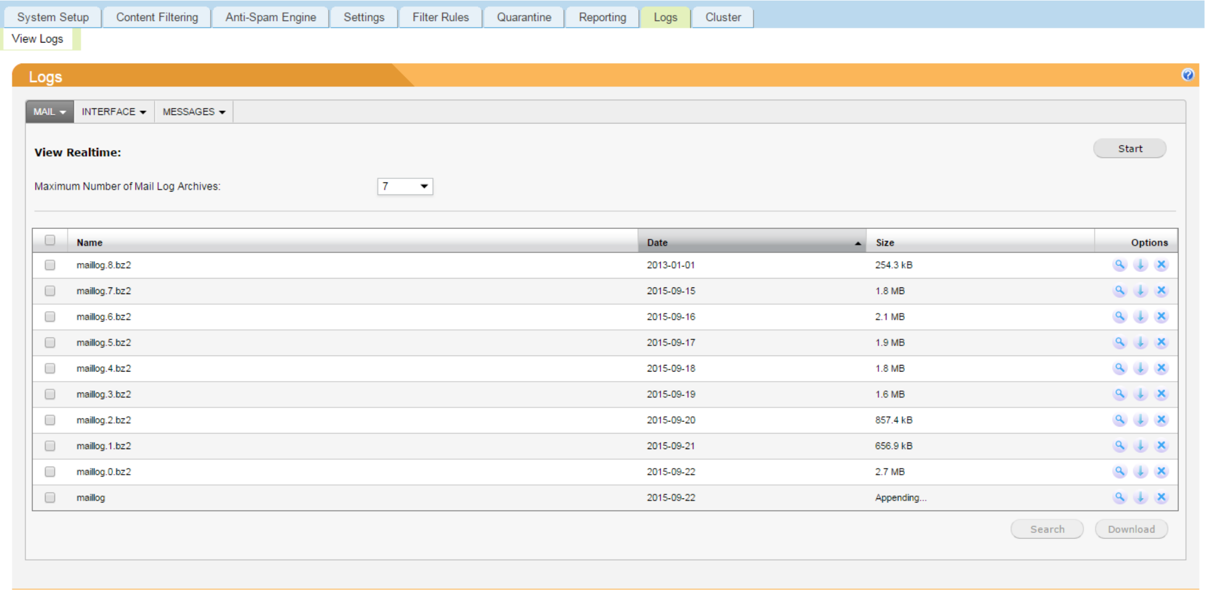
	Date	Subject	Type	Frequency	Download	Options
□	2015-09-01 03:31:10	SpamTitan Report - Top Recipients Monthly (10000)	Top Email Recipients (mails)	Monthly	Text Excel PDF	Delete
□	2015-09-01 03:31:02	SpamTitan Report	Domain Report	Monthly	Text Excel	Delete
□	2015-08-01 03:31:10	SpamTitan Report - Top Recipients Monthly (10000)	Top Email Recipients (mails)	Monthly	Text Excel PDF	Delete
□	2015-08-01 03:31:02	SpamTitan Report	Domain Report	Monthly	Text Excel	Delete
□	2015-07-14 03:31:02	SpamTitan Report: copperfasten.com license usage	License Usage Report	Daily	Text Excel	Delete
□	2015-07-13 03:31:05	SpamTitan Report: copperfasten.com license usage	License Usage Report	Daily	Text Excel	Delete
□	2015-07-13 03:31:01	Test: SpamTitan Report	Domain Summary Report	Weekly	Text Excel PDF	Delete
□	2015-07-12 03:31:01	SpamTitan Report: copperfasten.com license usage	License Usage Report	Daily	Text Excel	Delete
□	2015-07-11 03:31:02	SpamTitan Report: copperfasten.com license usage	License Usage Report	Daily	Text Excel	Delete

Figure 15-15 Archived Reports

Use the **Type** and **Frequency**, **Domain** and **From** settings to filter the display. The reports can be downloaded for viewing or deleted.

16 Logging

An important component in SpamTitan is its extensive logging capabilities. As well as the mail transaction log history which is stored in the database, log files also contain the records of regular operations and exceptions from various components of the system. These logs record information regarding all email activity and server management. This information can be valuable when monitoring your SpamTitan service as well as when troubleshooting or checking performance.



View Realtime:

Maximum Number of Mail Log Archives: 7

☐	Name	Date	Size	Options
☐	maillog.8.bz2	2013-01-01	254.3 kB	
☐	maillog.7.bz2	2015-09-15	1.8 MB	
☐	maillog.6.bz2	2015-09-16	2.1 MB	
☐	maillog.5.bz2	2015-09-17	1.9 MB	
☐	maillog.4.bz2	2015-09-18	1.8 MB	
☐	maillog.3.bz2	2015-09-19	1.6 MB	
☐	maillog.2.bz2	2015-09-20	857.4 kB	
☐	maillog.1.bz2	2015-09-21	656.9 kB	
☐	maillog.0.bz2	2015-09-22	2.7 MB	
☐	maillog	2015-09-22	Appending...	

Figure 16-1 Logging page

The log file pages allow you to view, search and download log files stored on SpamTitan.

The following table summarizes the log file types that are available:

Log File	Description
Mail Log	Contains *all* information regarding the email operations of SpamTitan. This includes all mail deliveries, bounces, failures or filtering events.
Interface Log	The Interface logs record all operations that are conducted via the web interface. It also provides details on appliance housekeeping activity and report generation – showing, for instance, all the users who receive quarantine reports.
Messages Log	This is the system log and records the following: boot information; DNS status information; spam, virus and system update attempts; disk issues; kernel issues. This log file is useful for troubleshooting general condition of the system.

Table 16-1 Available logs

The log files are recorded in plain text (ASCII) format and can be viewed via the User Interface from the Log Files page or download and viewed in your favorite editor. The log files are rotated on a daily basis at midnight and are retained on the system for the duration specified in the **Maximum Number of Mail Log Archives** setting. You can also have the log files written in real-time to a remote Syslog server. See **Settings > Remote Syslog** for more information.

To view the currently active log file, click on the **View Realtime Start** button. A new window with the last available log lines will be opened. The log will scroll automatically to display newly added lines.

To work with older log files, use the table listing all available log files for that category. You can perform an individual on a single file (**View**, **Download** or **Delete**) by clicking an Action type on the right of the table, or perform a global action (**Download** or **Search**) after selecting one or more files by checking their checkboxes on the left of the table.

The **Search Selected** function allows you search for strings in log files. Only lines containing the string will be displayed. You can perform case insensitive searches of the string by checking the **Case Insensitive** option. It is possible to search several files at once. If your search string returns no matches then an empty window will be displayed.

17 Outlook Add-In

The SpamTitan Outlook add-in v2.1 allows you to report spam back to the SpamTitan anti-spam appliance. When you send mail flagged as spam, you are sending the email message body to be trained by the SpamTitan Bayesian filter as a token, aka either spam or ham (legitimate mail). What this means is that the contents of the mail are learned by the filter and that any future emails containing these characteristics will have a greater probability of being classified correctly.

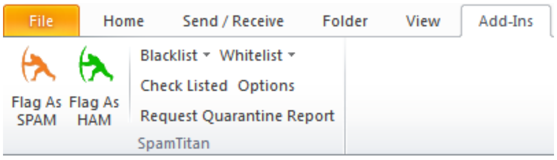
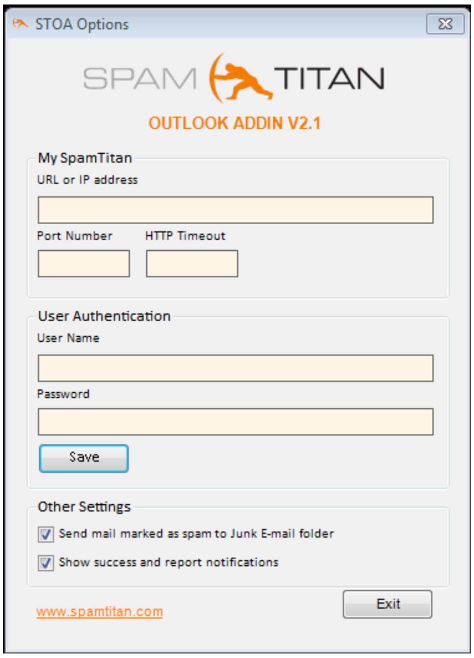


Figure 17-1 Outlook plugin ribbon



☑ Send mail marked as spam to Junk E-mail folder

☑ Show success and report notifications

Figure 17-2 Outlook plugin options dialog

REQUIREMENTS

1. NET Framework 3.5 SP1
2. Office 2007 Primary Interop Assemblies
3. Visual Studio 2010 tools for Office Runtime (x86, x64)
4. Outlook 2007 or 2010
5. Windows XP / Vista / 7

If the first three requirements are not found setup will download them and install. Please be patient as the .NET install may take a few minutes. Once installed the SpamTitan Outlook Add-in installer will run.

If you are interested you can download the SpamTitan Outlook Add-in .EXE file.

18 Remote Management

SpamTitan can be remotely managed via the SpamTitan API. The API enables administrators to remotely manage domains, users, policies, whitelists and blacklists.

Access to the API is limited to trusted IP address. To configure an IP address as trusted, go to the **Settings > Access/Authentication** page and enter the IP address that you wish to trust in API Allowed Hosts.

See the **SpamTitan API Users Guide** for more details on using the API.

19 Firewall Information

The following table lists the possible ports that may need to be opened for proper operation of SpamTitan.

Port	Protocol	In/Out	Description
20/21	TCP	Out	FTP out for retrieval of system updates
22	TCP	Out	SSH access to allow SpamTitan Technical support create a secure connection to the appliance for support.
25	TCP	Out	SMTP to send email
25	TCP	In	SMTP to receive email
80	TCP	In	HTTP access to the GUI for system management and monitoring, and quarantine management. Also the Clam and Kaspersky virus definition updates are retrieved via HTTP. This port need not be open if you have configured an alternative HTTP proxy port.
53	UDP	In and out	DNS
123	UDP	In and out	NTP if using time servers outside your firewall
443	TCP	In	Secure HTTP access to the GUI

Table 19-1 Firewall ports