MailScan for Linux

MailScan for Linux is a powerful Real-Time mail scanning Software for Mail Servers running on Linux operating systems that offers a complete protection against Viruses, Worms, Trojans, Spammers, Phishers and Other malware. It provides a comprehensive Security Solution for e-communications at the Mail Gateway level.

How it works?

MailScan for Linux works on SMTP Port 25 and receives mails on behalf of the actual mail server. It thoroughly scans all mails for malware and spam and subsequently quarantines or deletes infected or spam mails. This ensures that MailScan protects the Mail Server in a proactive and preventive manner. MailScan for Linux acts as a Content-Security and Anti-Virus Software for your Corporate Mail Server. It scans and cleans e-mails.

MailScan for Linux

MailScan™

Key features

Real-time Anti-Virus at the Mail Gateway

MailScan features one of the fastest and most up-to-date antivirus systems, capable of detecting viruses, worms, Trojans, backdoors, rootkits, spyware, adware, bots, porn dialers, Trojan clickers, and other malwares directly before delivering to the User's mailbox.

Automated Threat Alerts

When an email containing malware or spam is identified and handled, a notification can be sent to the sender, intended recipient, or other specified individuals.

Comprehensive Reports

MailScan's reporting feature presents an overview of its activities over a defined period, categorized into various sections.

Enhanced Content Scanning Capabilities

MailScan's content control options enable you to define restricted words or phrases in emails for detection. Emails containing these terms in the subject, body, or tags are blocked or quarantined.

Anti-Spam and Anti-Phishing Protection

MailScan prevents spam and phishing attacks using a combination of technologies, including Gray Listing, Real-time Blacklist (RBL) and more.

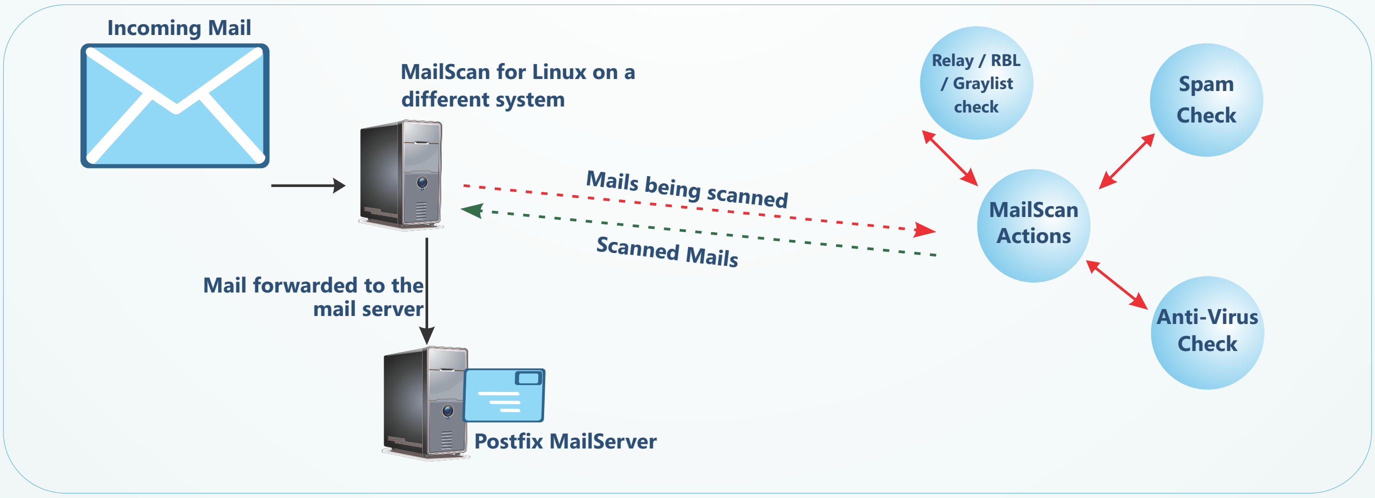
Self-Diagnosis / Troubleshooting

When MailScan experiences a functionality issue, the 'Send Debug Information' feature creates a debugs.zip file.

Various Deployment Scenarios

- Scenario I

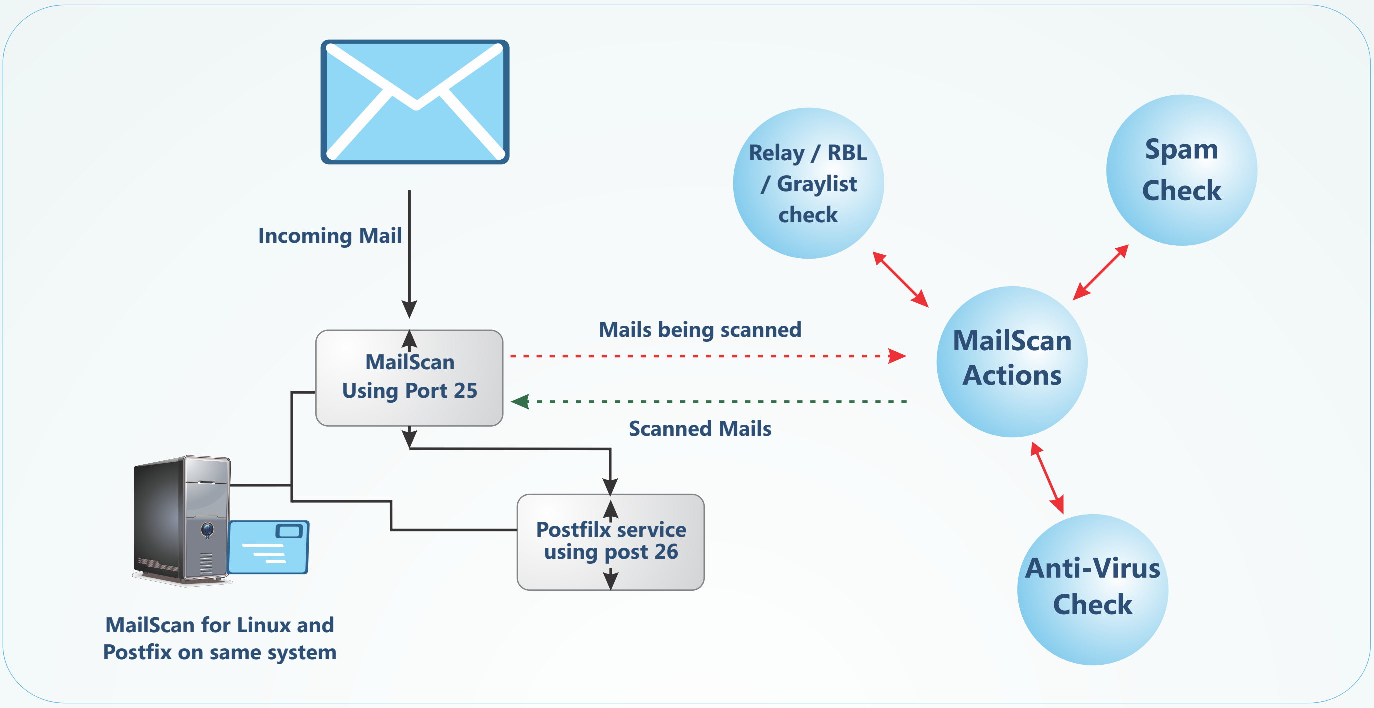
MailScan for Linux MailServer can functions as a Mail Gateway (Mail Transport Agent – MTA), allowing the MailServer to reside on a separate system. It scans all incoming and outgoing emails before forwarding them to the MailServer on the designated system.



Various Deployment Scenarios

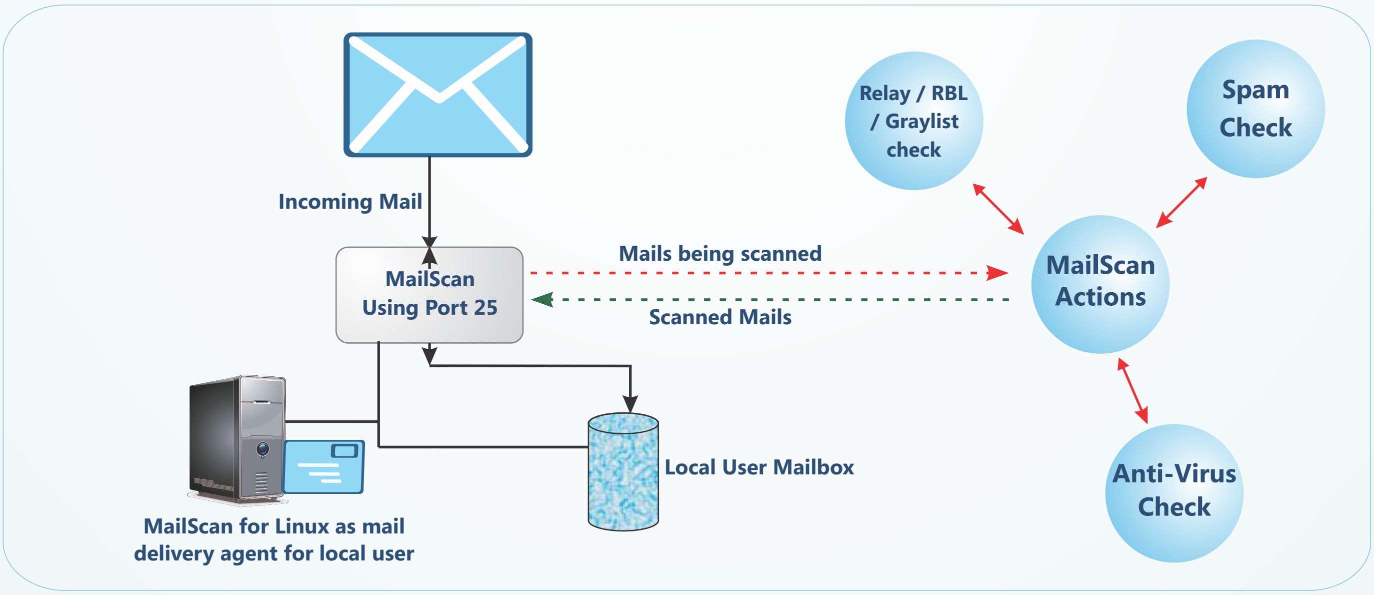
• Scenario II

MailScan for Linux MailServer can be deployed on the same system as the MailServer. It will listen on Port 25, while the Mail Server's SMTP service should be configured to operate on an unused port, such as Port 26. All incoming emails are received on Port 25, scanned by MailScan, and then relayed to the MailServer's SMTP service on Port 26 for final processing.



• Scenario III

MailScan for Linux Mail server can also act as a Mail Delivery Agent (MDA) for locally configured mail users



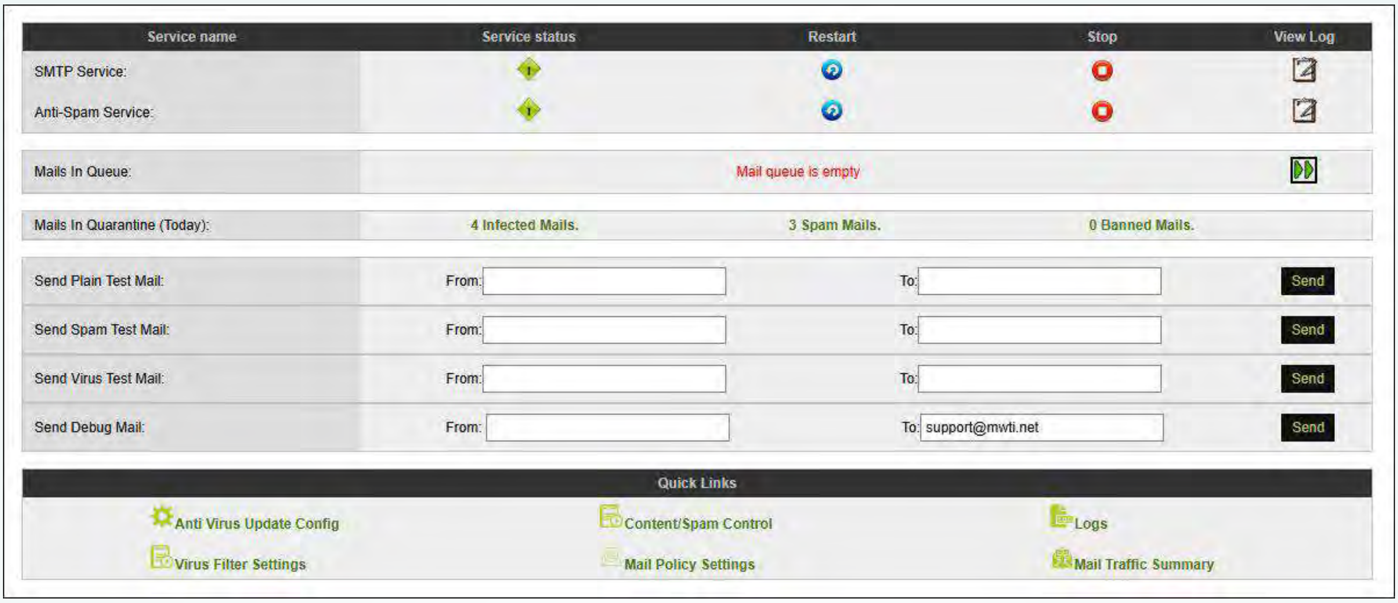
MailScan for Linux

MailScan

Other Features

• Administrator Web Console view of MailScan Server:

Displaying the server service status and other settings.



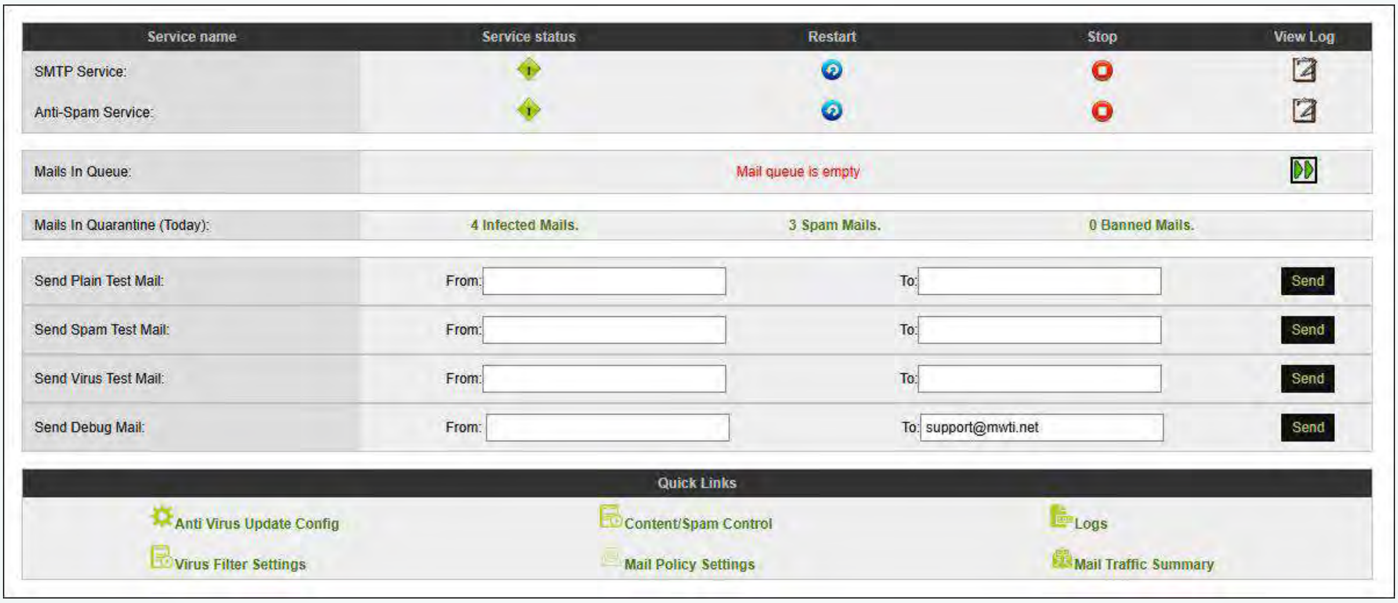
Service name	Service status	Restart	Stop	View Log
SMTP Service:	◆	↻	●	✎
Anti-Spam Service:	◆	↻	●	✎
Mails In Queue:	Mail queue is empty			⏩
Mails In Quarantine (Today):	4 Infected Mails.	3 Spam Mails.	0 Banned Mails.	
Send Plain Test Mail:	From:	To:		Send
Send Spam Test Mail:	From:	To:		Send
Send Virus Test Mail:	From:	To:		Send
Send Debug Mail:	From:	To: support@mwti.net		Send

Quick Links		
Anti Virus Update Config	Content/Spam Control	Logs
Virus Filter Settings	Mail Policy Settings	Mail Traffic Summary

• Server Control

MailScan for Linux displays a list of services, indicating whether they are running or stopped. You can restart any service as needed. The SMTP Service and Anti-Spam Service are essential components of MailScan for Linux and should always remain active.

On the screen, a running service is marked with a green flag, while a stopped service is indicated by a red flag. To restart a service, select the Blue. To stop a service, use the Red icon.



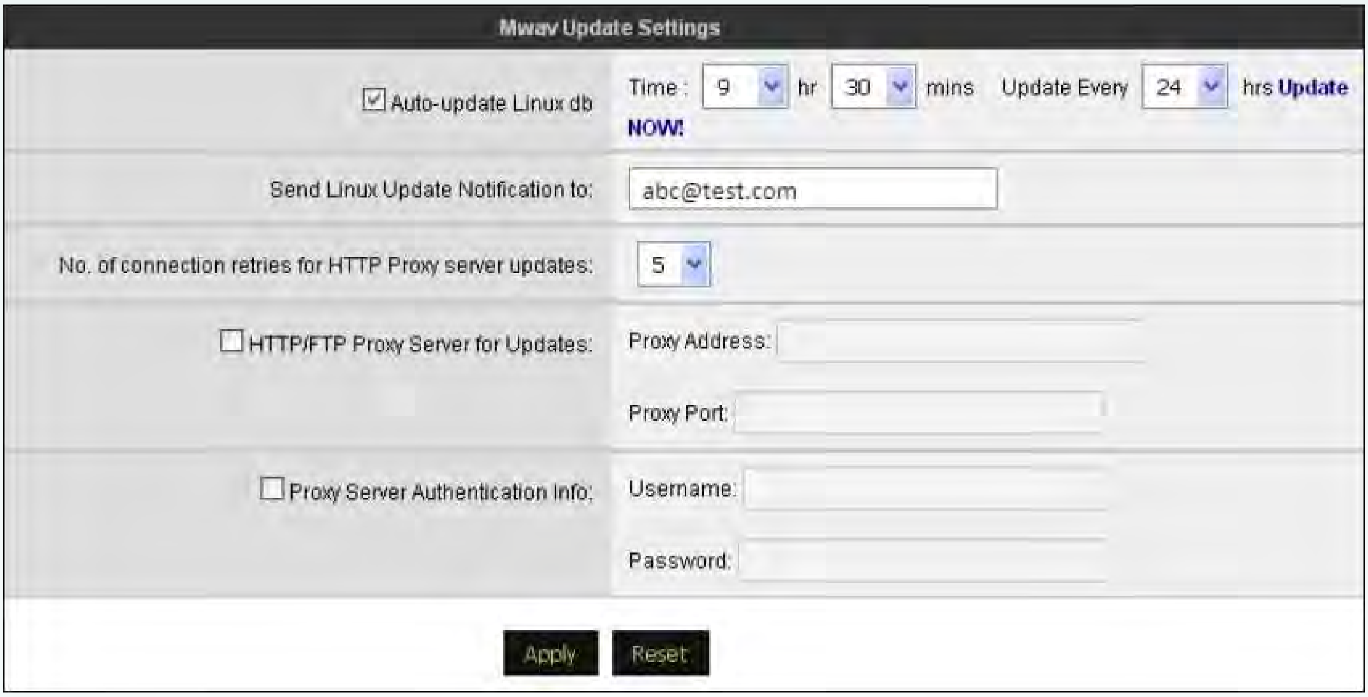
Service name	Service status	Restart	Stop	View Log
SMTP Service:	◆	↻	●	✎
Anti-Spam Service:	◆	↻	●	✎
Mails In Queue:	Mail queue is empty			⏩
Mails In Quarantine (Today):	4 Infected Mails.	3 Spam Mails.	0 Banned Mails.	
Send Plain Test Mail:	From:	To:		Send
Send Spam Test Mail:	From:	To:		Send
Send Virus Test Mail:	From:	To:		Send
Send Debug Mail:	From:	To: support@mwti.net		Send

Quick Links		
Anti Virus Update Config	Content/Spam Control	Logs
Virus Filter Settings	Mail Policy Settings	Mail Traffic Summary

MailScan for Linux

- **Anti-Virus Database update settings**

Settings for scheduling downloads of Anti-virus Signatures and other Settings.



Mwav Update Settings

☑ Auto-update Linux db — Time : 9 hr 30 mins Update Every 24 hrs **Update NOW!**

Send Linux Update Notification to: abc@test.com

No. of connection retries for HTTP Proxy server updates: 5

□ HTTP/FTP Proxy Server for Updates: Proxy Address: Proxy Port:

□ Proxy Server Authentication Info: Username: Password:

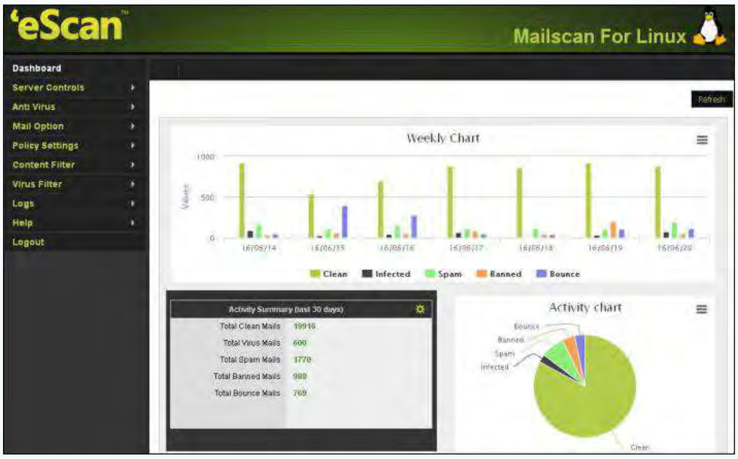
- **Web-Based Admin Console**

The MailScan for Linux administration console is accessible via a web browser, allowing centralized management and configuration.

To log in to the Web Administration panel, open a browser and visit:

http://ip-address-of-MailScan-Server:10443

MailScan performs real-time scanning of all inbound and outbound emails, detecting viruses, malware, malicious attachments, and offensive content. Its advanced content filtering engine identifies and blocks spam based on predefined keywords and patterns, preventing the transmission of irrelevant or harmful messages within the organization. By integrating both virus scanning and content analysis, MailScan ensures secure and compliant email delivery to the Mail Server.



Activity Summary (last 30 days)

Total Clean Mails	19916
Total Virus Mails	600
Total Spam Mails	1770
Total Banned Mails	988
Total Bounce Mails	769

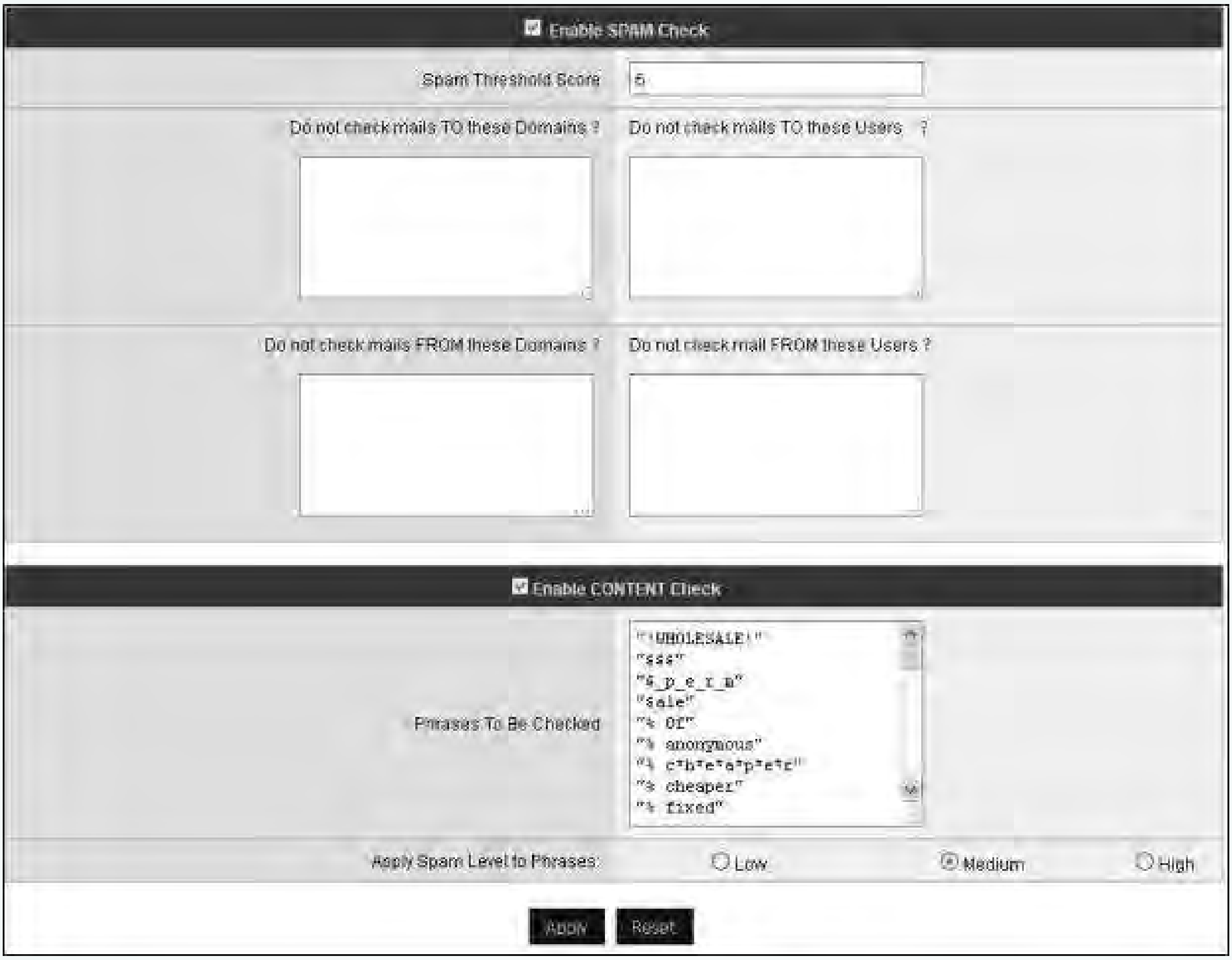
MailScan for Linux

• Content Filtering and Spam Control Settings

MailScan for Linux incorporates a robust spam detection engine that enables content-based filtering using predefined keyword patterns. For example, many spam emails contain characteristic phrases such as “chance of a lifetime” or “get rich.” By leveraging keyword-based scanning, MailScan effectively identifies and flags suspicious emails.

Additionally, MailScan supports configurable spam scoring, allowing administrators to assign weighted spam probability levels to specific phrases. This granular control enhances the accuracy of spam classification and reduces false positives.

For enhanced security and efficiency, MailScan provides customizable whitelisting and blacklisting mechanisms. The whitelist ensures that emails from trusted users and domains are always recognized as legitimate, while the blacklist blocks messages from known spam sources based on sender IPs, domains, and email addresses.



☑ Enable SPAM Check

Spam Threshold Score: 5

Do not check mails TO these Domains ?

Do not check mails TO these Users ?

Do not check mails FROM these Domains ?

Do not check mail FROM these Users ?

☑ Enable CONTENT Check

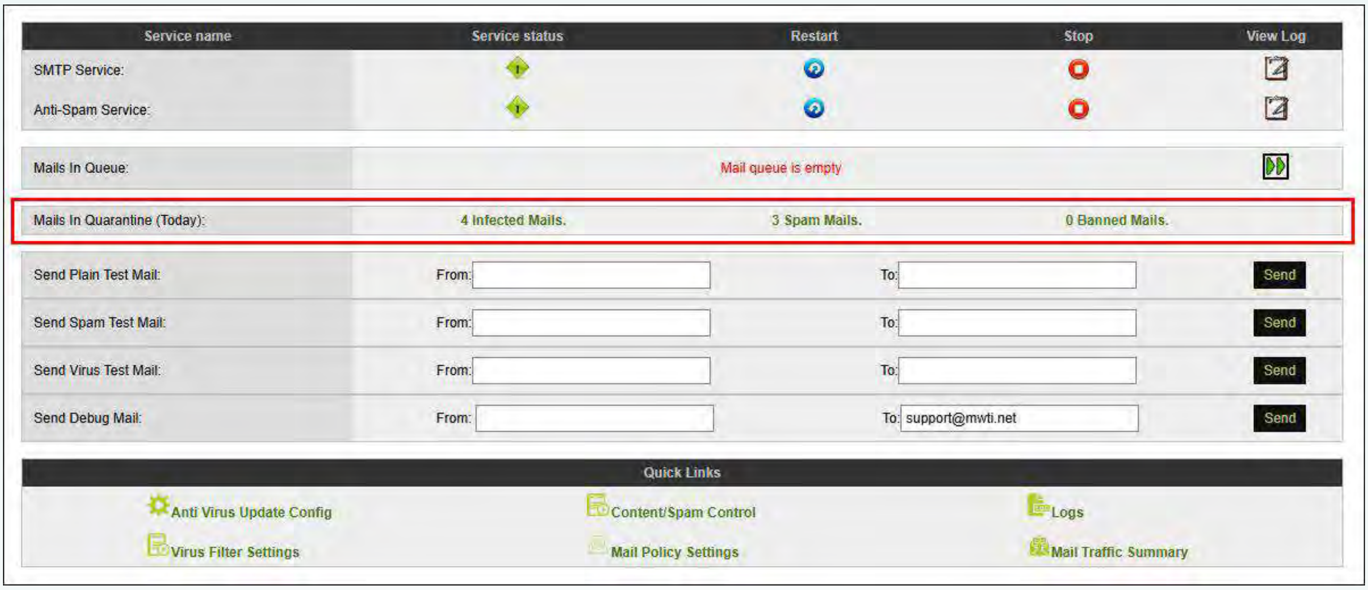
Phrases To Be Checked:

```
"!WHOLESALE!"
"$$$"
"s_p_e_r_m"
"sale"
"% off"
"% anonymous"
"% c*h*e*a*p*e*r"
"% cheaper"
"% fixed"
```

Apply Spam Level to Phrases: ○ Low ● Medium ○ High

• Manage Quarantined Mails

This section shows the count of emails classified as Spam, Infected, or Banned. Clicking on any category opens with detailed information about the corresponding emails.



Service name	Service status	Restart	Stop	View Log
SMTP Service:	◆	↻	●	✎
Anti-Spam Service:	◆	↻	●	✎

Mails In Queue:	Mail queue is empty			▶▶
Mails In Quarantine (Today):	4 Infected Mails.	3 Spam Mails.	0 Banned Mails.	

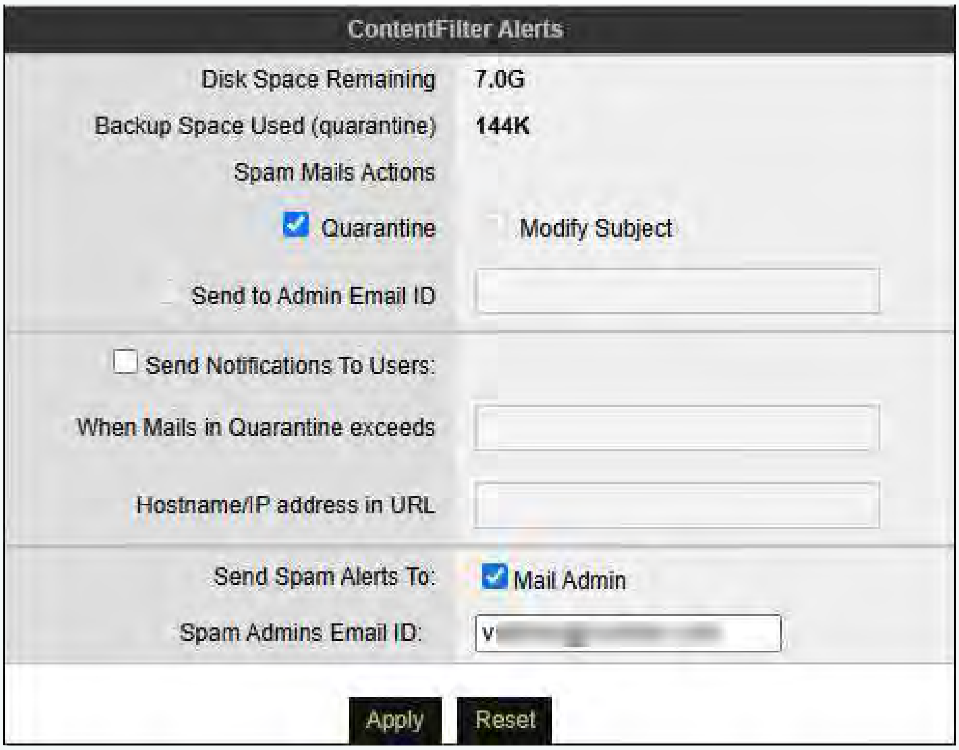
Send Plain Test Mail:	From:	To:	Send
Send Spam Test Mail:	From:	To:	Send
Send Virus Test Mail:	From:	To:	Send
Send Debug Mail:	From:	To: support@mwti.net	Send

Quick Links

Anti Virus Update Config	Content/Spam Control	Logs
Virus Filter Settings	Mail Policy Settings	Mail Traffic Summary

• Content Filter Alerts

This feature enables you to configure custom alerts that are triggered when any spam emails are detected in emails. Notification / Alerts can be sent to the sender, recipient, and administrator. Spam emails can either be quarantined and stored in a dedicated quarantine folder or redirected to a designated mailbox.



ContentFilter Alerts

Disk Space Remaining 7.0G

Backup Space Used (quarantine) 144K

Spam Mails Actions

☑ Quarantine □ Modify Subject

Send to Admin Email ID

□ Send Notifications To Users:

When Mails in Quarantine exceeds

Hostname/IP address in URL

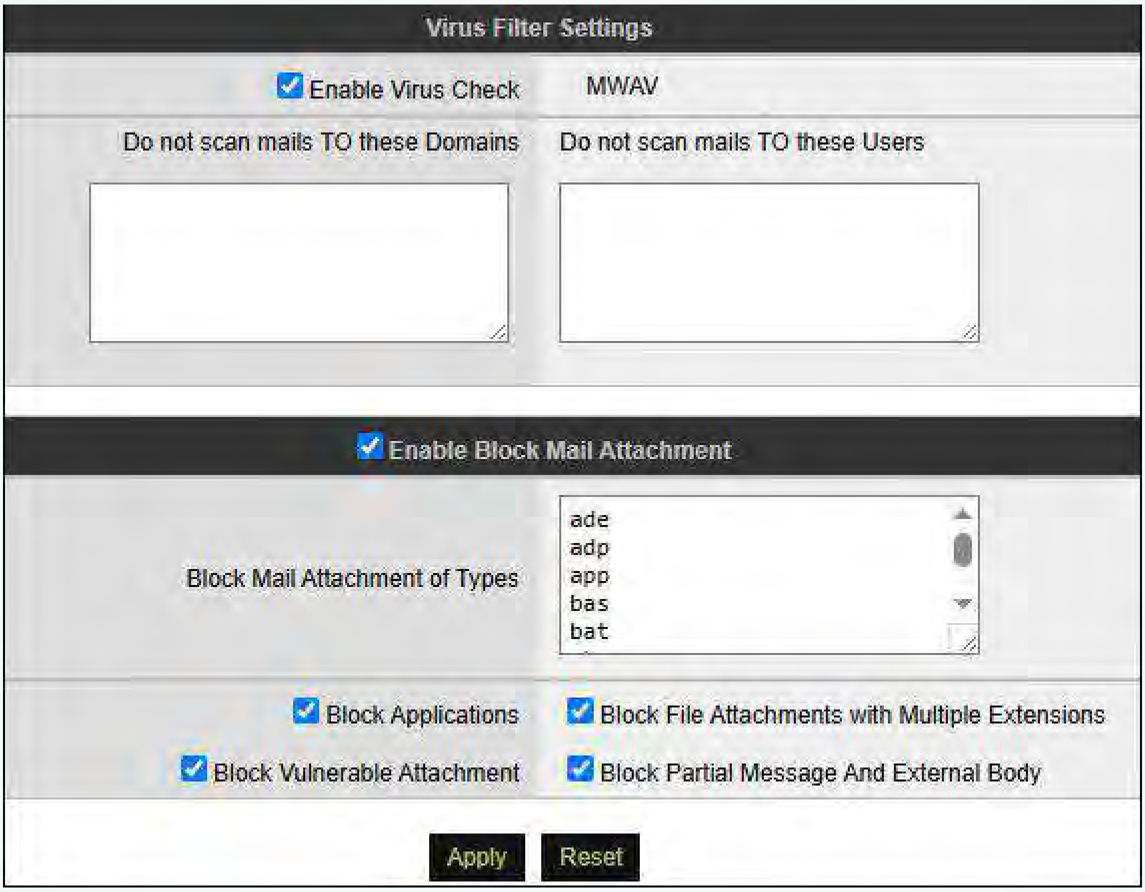
Send Spam Alerts To: ☑ Mail Admin

Spam Admins Email ID: v[redacted]

Apply Reset

- **Scan & Block Malicious Email Content**

  This module enhances email security by allowing the configuration of antivirus settings. Trusted domains and users can be designated as secure, while potentially harmful file types can be restricted from entering or leaving the server. Additionally, it helps prevent the unauthorized transmission of confidential information via email.



Virus Filter Settings

☑ Enable Virus Check MWAV

Do not scan mails TO these Domains

Do not scan mails TO these Users

☑ Enable Block Mail Attachment

Block Mail Attachment of Types: ade, adp, app, bas, bat

☑ Block Applications

☑ Block File Attachments with Multiple Extensions

☑ Block Vulnerable Attachment

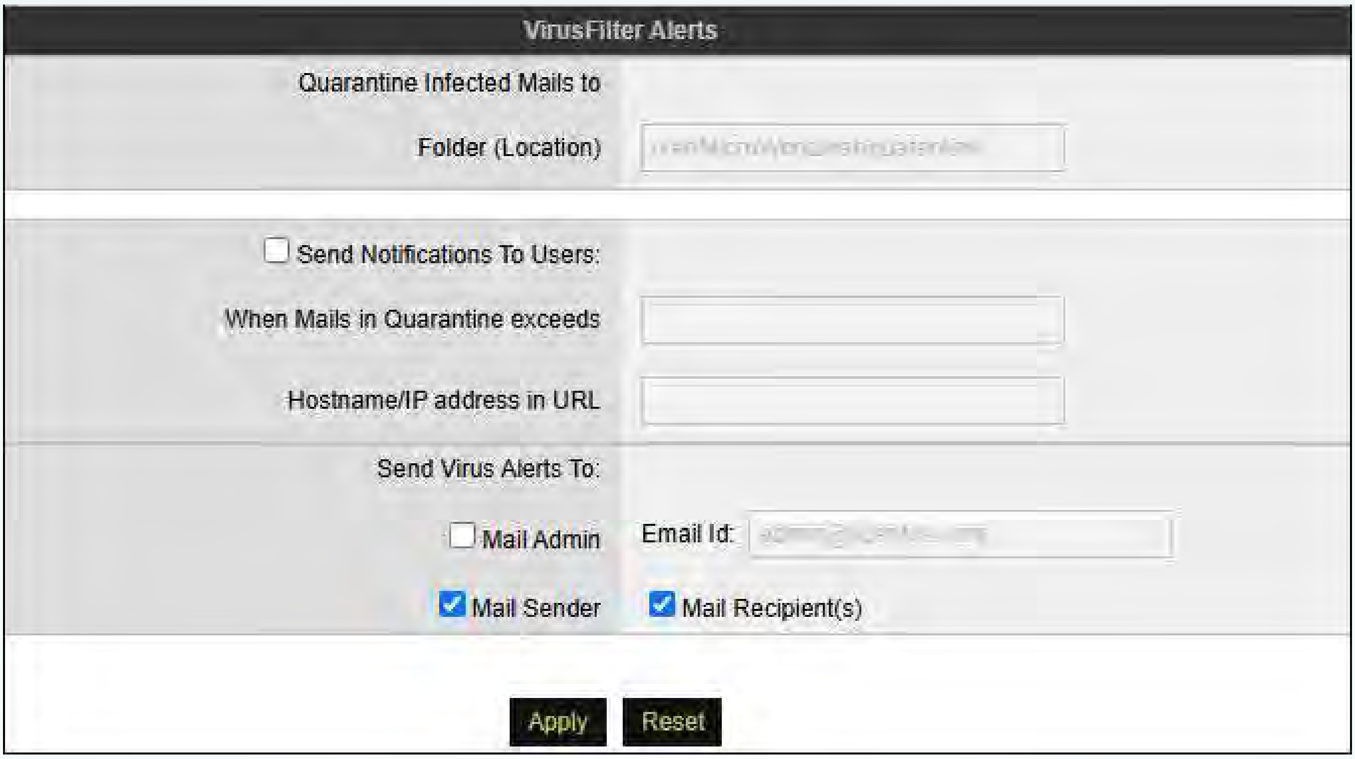
☑ Block Partial Message And External Body

MailScan for Linux

MailScan™

• Virus Filter Alert

This feature enables automated alerts when virus-infected emails are identified. Notifications are dispatched to the sender, recipient, and IT administrator, while infected emails are either quarantined in a dedicated folder or routed to a mailbox for further inspection.



VirusFilter Alerts

Quarantine Infected Mails to

Folder (Location) [illegible]

□ Send Notifications To Users:

When Mails in Quarantine exceeds

Hostname/IP address in URL

Send Virus Alerts To:

□ Mail Admin Email Id: [illegible]

☑ Mail Sender ☑ Mail Recipient(s)

• System Requirement

- CPU: 2GHz Intel™ Core™ Duo processor or equivalent.
- Memory: 2 GB & above

• Platforms Supported

- RHEL 4 & above (32 & 64 bit)
- CentOS 5.10 & above (32 & 64 bit)
- SLES 10 SP3 & above (32 & 64 bit)
- Debian 4.0 & above (32 & 64 bit)
- OpenSuSe 10.1 & above (32 & 64 bit)
- Fedora 5.0 & above (32 & 64 bit)
- Ubuntu 6.06 & above (32 & 64 bit)

eScan™

Enterprise Security

An ISO 27001 Certified Company

Toll Free No.: 1800 267 2900

www.escanav.com

MicroWorld Software Services Pvt. Ltd.
CIN No.: U72200MH2000PTC127055
Tel.: +91 22 6772 2900
email: sales@escanav.com

Awards

Partnerships

Comprehensive Protection for

SOHO • BUSINESS • CORPORATE • ENTERPRISE