

# Tech Note

Release Notes

SonicWALL Email Security 5.0 Software Edition

SonicWALL, Inc.  
September 25, 2006

## Contents

---

This document includes the following sections:

- SYSTEM REQUIREMENTS
- KEY FEATURES
- KNOWN ISSUES
- RESOLVED KNOWN ISSUES

## System Requirements

---

SonicWALL Email Security 5.0 Software Edition supports:

### Operating Systems

- Windows 2000, SP4
- Windows 2003, SP1

### Hardware Requirements

- Intel Pentium: Celeron, P4 or compatible CPU
- 1 Gigabyte RAM minimum
- Hard Disk: 40GB minimum



# Tech Note

## Key Features

The following is a list of features introduced in the SonicWALL Email Security 5.0 Software Release:

### Compliance Module

The Compliance Module provides the following new features. These features are only available as part of the Compliance Module:

- **Predefined Dictionaries** – Email Security 5.0 provides pre-defined dictionaries of terms to use in filters. Users can use the pre-defined healthcare dictionaries to search for common health terms and diagnosis numbers. Users can modify the dictionaries to further suit their needs. The dictionaries are designed to help in building filters for categories like Financial Terms and medical Drug Names.

The predefined dictionaries are available on the **Policy & Compliance > Compliance Module > Dictionaries** page

SONICWALL  
EMAIL SECURITY  
MailFrontier

Sign off: admin

Server Configuration   Anti-Spam Anti-Phishing   Anti-Virus Techniques   Auditing   Policy & Compliance   User & Group Management   Junk Box   Reports & Monitoring

admin

**Policy & Compliance** [Help](#)

Build Policy dictionaries to be used within filter definitions.

Standard Module:  
[Filters](#)  
[Policy Groups](#)

Compliance Module:  
**Dictionaries**  
[Approval Boxes](#)  
[Encryption](#)  
[Record ID Definitions](#)  
[Archiving](#)

[Add New Dictionary](#)   [Import Dictionary](#)

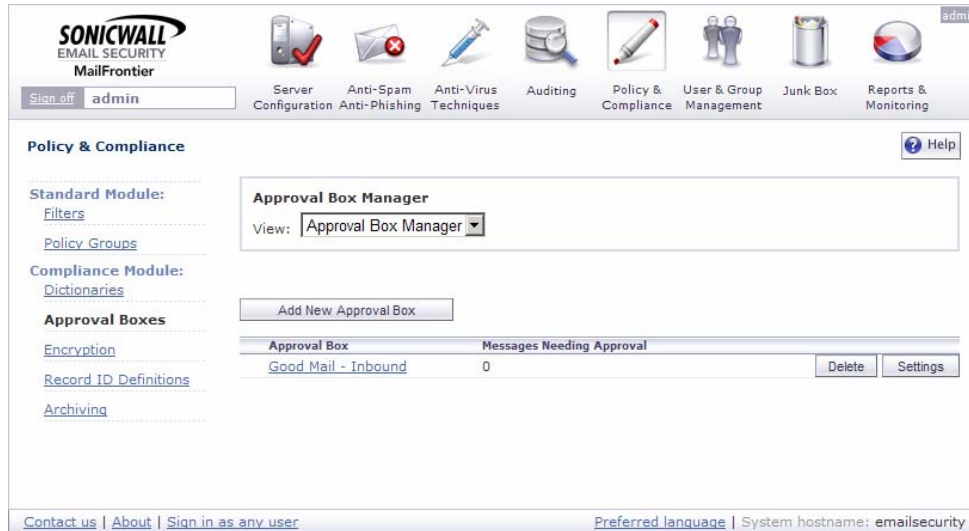
Dictionary	Term Count	Edit	Delete
Financial Terms (SonicWALL) - 1.0	3892	<a href="#">Edit</a>	<a href="#">Delete</a>
Medical Drug Names (SonicWALL) - 1.0	4996	<a href="#">Edit</a>	<a href="#">Delete</a>

[Contact us](#) | [About](#)   [Preferred language](#) | System hostname: bracham-desktop

© Copyright 2003-2006 SonicWALL, Inc.

# Tech Note

- **Approval Boxes** – In Email Security 5.0 Approval Boxes are now part of the Compliance Module.
  - For customers with existing Approval Boxes who purchase the Compliance Module, their Approval Boxes will now be available on the **Policy & Compliance > Approval Boxes** page.



- For customers with existing Approval Boxes who do not purchase the Compliance Module, the **Compliance Module** section in the **Policy & Compliance** menu on the left will be available. Only single choice, **Approval Boxes** will be available. All other **Compliance Module** features will not be available.



These customers will need to purchase the Compliance Module to continue using Approval Boxes after their current subscription expires.

## Tech Note

- **Encryption** – Email Security 5.0 allows you to route emails that match a specific policy to an encryption/decryption server in addition to using TLS (standards-based, free, gateway-to-gateway encryption) available in the base product. You specify the encryption server path on the **Policy & Compliance > Compliance Module > Encryption** page

The screenshot shows the SonicWall MailFrontier web interface. The top navigation bar includes icons for Server Configuration, Anti-Spam, Anti-Virus, Auditing, Policy & Compliance, User & Group Management, Junk Box, and Reports & Monitoring. The user is logged in as 'admin'. The main content area is titled 'Policy & Compliance' and contains a sidebar with links for Filters, Policy Groups, Compliance Module, Dictionaries, Approval Boxes, Encryption, Record ID Definitions, and Archiving. The main form area has two input fields: 'Name or IP address of SMTP server for Encryption:' with the value '10.100.12.34' and 'Name or IP address of SMTP server for Decryption:' with the value '10.100.12.35'. An 'Apply Changes' button is located at the bottom of the form. The footer includes 'Contact us | About', 'Preferred language', and 'System hostname: mfappwin1000'. Copyright information for 2003-2006 SonicWALL, Inc. is also present.

- **Record ID Match** – As part of privacy protection initiative such as HIPAA (Health Insurance Portability and Accountability Act of 1996), GLBA (Gramm-Leach-Bliley Act or Financial Services Modernization Act of 1999), and VISA CISP (Cardholder Information Security Program), there is a need to detect whether emails contain relevant record identifications. Some of the IDs to match are:

- ABA Bank Routing Number
- Canadian Social Security Number
- Credit Card Number (15 & 16 digits; AMEX, VISA, MASTERCARD, Diner Club, Discover, enRoute)
- Date
- Phone Number (US & International)
- Social Security Number (US)
- ZIP Code

Email Security 5.0 provides a Record ID Match feature that can identify this kind of information. The usage of this feature is exactly the same as current policy filter implementation. End users would create a new policy filter and simply select one of the Identification types specified above. Optionally users can also create a Custom ID or modify pre-loaded IDs.

Record ID Match is available on the **Policy & Compliance > Compliance Module > Record ID Definitions** page.

# Tech Note

The screenshot shows the SonicWall MailFrontier interface. The top navigation bar includes icons for Server Configuration, Anti-Spam Anti-Phishing, Anti-Virus Techniques, Auditing, Policy & Compliance, User & Group Management, Junk Box, and Reports & Monitoring. The user is logged in as 'admin'. The main content area is titled 'Policy & Compliance' and contains a 'Record ID Definitions' table. The table lists various identifiers with 'Edit' and 'Delete' buttons for each.

Record ID Definitions		
ABA Bank Routing Number	Edit	Delete
Canadian Social Insurance Number	Edit	Delete
Credit Card Number	Edit	Delete
Date	Edit	Delete
Phone Number	Edit	Delete
Social Security Number	Edit	Delete
Zip Code	Edit	Delete

- **Easy Archiving** – Email Security 5.0 provides a feature to efficiently archive email messages by sending a copy of the message via SMTP to an archive server. To use this feature, specify an archive server in the **Policy & Compliance > Compliance Module > Archiving** page.

The screenshot shows the 'Archiving' configuration page in the SonicWall MailFrontier interface. The 'External SMTP server' option is selected. The IP address of the archive server is set to 'archive@example.sonicwall.com'. The 'File system' option is unselected. The 'Keep archived emails for' dropdown is set to '30 Days'. An 'Apply Changes' button is visible at the bottom of the configuration area.

# Tech Note

- **Compliance Module Reports** – In addition to the new features in the Compliance Module, Email Security 5.0 provides reports for the new Compliance Module features. The following reports are available under **Reports and Monitoring > Compliance Reports**.

- Inbound Messages Decrypted

The screenshot shows the SonicWall MailFrontier interface. The top navigation bar includes icons for Server Configuration, Anti-Spam Anti-Phishing, Anti-Virus Techniques, Auditing, Policy & Compliance, User & Group Management, Junk Box, and Reports & Monitoring. The 'Reports & Monitoring' section is active, displaying the 'Inbound Messages Decrypted' report. The report is filtered for 'Hourly' data. The table shows the number of messages decrypted per day from 01/02/08 to 01/07/08.

Day	Number of Messages
01/07/08	0
01/06/08	0
01/05/08	0
01/04/08	0
01/03/08	0
01/02/08	0

- Inbound Messages Archived

The screenshot shows the SonicWall MailFrontier interface. The top navigation bar is the same as the previous screenshot. The 'Reports & Monitoring' section is active, displaying the 'Inbound Messages Archived' report. The report is filtered for 'Hourly' data. The table shows the number of messages archived per day from 01/07/08 to 01/07/08.

Day	Number of Messages
01/07/08	0
01/06/08	0
01/05/08	0
01/04/08	0
01/03/08	0
01/07/08	0

- Top Inbound Approval Boxes by Name

The screenshot shows the SonicWall MailFrontier interface. The top navigation bar is the same as the previous screenshots. The 'Reports & Monitoring' section is active, displaying the 'Top Inbound Approval Boxes by Name' report. The report is filtered for 'Today' data. The table shows the number of messages filtered for each approval box name in January.

Approval Box Name	Number of Messages Filtered
good mails - inbound	4

# Tech Note

- o Outbound Messages Encrypted

The screenshot shows the SonicWall MailFrontier interface. The top navigation bar includes icons for Server Configuration, Anti-Spam Anti-Phishing, Anti-Virus Techniques, Auditing, Policy & Compliance, User & Group Management, Junk Box, and Reports & Monitoring. The user is logged in as 'admin'. The 'Reports & Monitoring' section is active, with options for 'Customize', 'Schedule', 'Download Report', and 'Help'. On the left, there is a sidebar with links: Dashboard, System Status, Return on Investment, Bandwidth Savings, Inbound Good vs Junk, Outbound Good vs Junk, Inbound vs Outbound Email. The main content area displays the 'Outbound Messages Encrypted' report with tabs for 'Hourly', 'Daily', and 'Monthly'. The data table is as follows:

Day	Number of Messages
01/07/08	0
01/06/08	0
01/05/08	0
01/04/08	0
01/03/08	0
01/02/08	0

- o Outbound Messages Archived

The screenshot shows the SonicWall MailFrontier interface. The top navigation bar includes icons for Server Configuration, Anti-Spam Anti-Phishing, Anti-Virus Techniques, Auditing, Policy & Compliance, User & Group Management, Junk Box, and Reports & Monitoring. The user is logged in as 'admin'. The 'Reports & Monitoring' section is active, with options for 'Customize', 'Schedule', 'Download Report', and 'Help'. On the left, there is a sidebar with links: Dashboard, System Status, Return on Investment, Bandwidth Savings, Inbound Good vs Junk, Outbound Good vs Junk, Inbound vs Outbound Email. The main content area displays the 'Outbound Messages Archived' report with tabs for 'Hourly', 'Daily', and 'Monthly'. The data table is as follows:

Day	Number of Messages
01/07/08	0
01/06/08	0
01/05/08	0
01/04/08	0
01/03/08	0
01/02/08	0

- o Top Outbound Approval Boxes by Name

The screenshot shows the SonicWall MailFrontier interface. The top navigation bar includes icons for Server Configuration, Anti-Spam Anti-Phishing, Anti-Virus Techniques, Auditing, Policy & Compliance, User & Group Management, Junk Box, and Reports & Monitoring. The user is logged in as 'admin'. The 'Reports & Monitoring' section is active, with options for 'Customize', 'Schedule', 'Download Report', and 'Help'. On the left, there is a sidebar with links: Dashboard, System Status, Return on Investment, Bandwidth Savings, Inbound Good vs Junk, Outbound Good vs Junk, Inbound vs Outbound Email. The main content area displays the 'Top Outbound Approval Boxes by Name' report with tabs for 'Today', 'This Month', and 'This Year'. The data table is as follows:

Approval Box Name	Number of Messages
Filtered	
<b>January</b>	
No data is available	

# Tech Note

## Connection Management

Email Security 5.0 provides a Connection Management feature that can block attacks on a company's mail server. Denial of Service attacks and other high volume generators of mail can cause mail networks to grind to a halt. In addition to rapidly evaluating spam, phishing, and viruses, SonicWALL Email Security protects mail networks from Directory Harvest Attacks (DHAs), Denial of Service (DoS) attacks, and other connection-level impacts.

- **Denial of Service (DoS):** Anywhere from one computer to several thousand computers infected with a virus One or several computers are pummeling the mail server with junk mail addressed to random, invalid recipients in attempt to cripple the mail flow
- **DoS:** Several hundred (or thousand) machines around the world are infected by a virus which contains an SMTP engine and is programmed to bring down the mail infrastructure at example.com by sending messages to it as quickly as possible. The mail servers are overwhelmed trying to process the increased volume, run out of resources, and mail flow grinds to a halt.
- **Directory Harvest Attack (DHA):** A small number of computers connect to the mail server and try to guess valid user names by attempting a large number of addresses. These IP addresses send a disproportionately high percentage/number of messages with invalid recipients.

To protect the mail server from these attacks, the connection Manager performs the following:

- Distinguish between IP Addresses that need to be deferred temporarily (rate limited) and blocked indefinitely (known bad IP Addr)
- Identify offenders by the number of connections they have made
- View/Edit the current list of deferred/blocked IP Addresses
- Add a known good IP address to a "white list"
- Defer various IP addresses for different amounts of time such as "24 hours"
- Reporting on emails blocked by the feature
- Limit the number of connections from a given IP Address
- Limit the number of messages per connection/session
- Limit the number of recipients per message

## Enhanced Spam Effectiveness

Spam outbreaks have become increasingly devious, leveraging images and other tricks to get through spam filters. Supplementing the constant spam filter data updates received by all customers with a current subscription, the SonicWALL Email Security 5.0 introduces:

- **Image Spam Capture Improvements** – SonicWALL SMART Network now thumbprints images, enabling a 1 million user global community to instantly identify spam images



# Tech Note

## Known Issues

---

The following is a list of known issues in the SonicWALL Email Security 5.0 Software Release:

### Combined policy actions can allow delivery of unwanted email

The symptom or behavior exhibited by this issue is that Email Security routes and delivers email to the original destination, despite policy actions intended to change the routing or prevent delivery to the original downstream recipient or IP address.

This problem occurs when two policy actions are triggered for a single message where the actions are defined as follows:

- One action is a non-exclusive action
- One action is an exclusive action with the intent to change the original recipient or route for the email

These actions can occur within a single policy filter or as the combination of actions from several different policy filters.

A combination of any action in column one with any action in column two of the following table can trigger this issue:

Non-exclusive Actions	Exclusive Actions
Tag subject with	Route to
Strip all attachments	Route to IP
Append text to message	Permanently Delete
Issue email notification	Bounce back to sender
Add X-Header to message	Store in Junk Box
Remove X-Header from message	Store in Approval box
	Encrypt
	Decrypt

As an example of this issue, consider the case where an email message is processed and triggers a policy rule that has an action of "Tag subject with". The message also triggers a second policy rule that includes an action of "Store in Junk Box". You would expect that the message subject is tagged and stored in the Junk Box. However, due to this issue, the actual behavior is as follows:

- The message is tagged and stored in the Junk Box
- A copy of the message is delivered to the original recipient

The actual action is "Store in Junk Box and Deliver", which is not the expected behavior.

### Exception routing fails with specific email addresses

This issue can cause the Mail Transfer Agent (MTA) to fail to start. The problem can occur when you add a network path that uses the last MTA option, and configure it with specific email addresses. Even when you turn on the option **Route email using MX record routing with these exceptions**, the MTA does not start.

An example configuration of adding a network path that uses the last MTA option, and configuring it with a specific email address is as follows:

```
engr.example.com 10.1.1.2
sales.example.com 10.1.1.1
phread@example.com 10.1.1.3
```



# Tech Note

---

The workaround for this problem is to use the Address Rewriting functionality in the proxy to re-write the domain part of the address, then use Exception routing based on the domain.

## Administration

- **45012: Symptom:** Audit page shows Header From, but search is on Envelope RCPT TO. **Condition:** Occurs in messages where the Envelope MAIL FROM field does not match the Header From field.

## Installation

- **45011: Symptom:** When you launch an auto update over HTTPS w/a self signed cert, the Java applet that we run on your local machine will ask you if you want to trust the certificate. Then a second dialog appears asking if you want to proceed because the name on the self signed cert does not match the name in the URL for the server. You must answer Yes to both dialogs. **Condition:** Occurs when the certificate is not in the local keystore file for the JRE or JDK.

## Policy and Compliance

- **7822: Symptom:** Case sensitive and disguised text identification check box needs to be disabled from the adding filter UI when Record ID is used.

## Reports

- **44212: Symptom:** MTA Queued Detail Info UI (Show Details) displays items per recipient instead of per message. **Condition:** Occurs when the system is configured to use inbound MTA, and you send two messages with one recipient each, and one message with two recipients, resulting in queuing.

## Resolved Known Issues

---

The following is a list of resolved known issues between the SonicWALL Email Security 5.0 Software Release and the SonicWALL Email Security 4.7 Release:

### Administration

- **7874: Symptom:** Dictionary causing memory leak (HDR). **Condition:** Occurs when using the HDR policies and policy dictionaries with the emails extracted from HDR's "full history".

### Effectiveness

- **6585: Symptom:** RBL not working on Windows 4.1.0 & Linux 4.1.1 build. **Condition:** Occurs when you license and configure in all-in-one mode, then add an RBL and send mail using the IP addresses in the received headers that are listed in the RBL.

### Replication

- **43218 and 7330: Symptom:** The replicator has a memory leak. **Condition:** Occurs when CC and RA are combined.

Part number: 232-000697-00  
Revision: Rev B  
Last updated: November 10, 2006

