Hosted Email Security Administrator's Guide

Notes, Cautions, and Warnings

NOTE: A NOTE indicates important information that helps you make better use of your system.

CAUTION: A CAUTION indicates potential damage to hardware or loss of data if instructions are not followed.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

© 2012 Dell Inc.

Trademarks: Dell™, the DELL logo, SonicWALL™, SonicWALL GMS™, SonicWALL ViewPoint™, Aventail™, Reassembly-Free Deep Packet Inspection™, Dynamic Security for the Global Network™, SonicWALL Aventail Advanced End Point Control™ (EPC™), SonicWALL Aventail Advanced Reporting™, SonicWALL Aventail Connect Mobile™, SonicWALL Aventail Connect™, SonicWALL Aventail Native Access Modules™, SonicWALL Aventail Policy Zones™, SonicWALL Aventail Smart Access™, SonicWALL Aventail Unified Policy™, SonicWALL Aventail™ Advanced EPC™, SonicWALL Clean VPN™, SonicWALL Clean Wireless™, SonicWALL Global Response Intelligent Defense (GRID) Network™, SonicWALL Mobile Connect™, SonicWALL SuperMassive™ E10000 Series, and all other SonicWALL product and service names and slogans are trademarks of Dell Inc.

2012 – 06 P/N 232-000884-00 Rev. A

Table of Contents

Pre-Configuration Tasks 7

- Introduction 7
- Initial Configuration 7
- Activating the Hosted Email Security Service 8
  - Adding MX Records 8
- Logging In 9

System 11

- Introduction 11
- License Management 11
  - Available Services 12
  - License Table 12
  - License Keys 13
- Administration 13
- Network Architecture 14
  - Server Configuration 14
  - Spooling 15
- LDAP Configuration 16
  - Configuring LDAP 17
  - LDAP Query Panel 18
  - Add LDAP Mappings 19
  - Configuring SonicWALL Email Security for Multiple LDAP Servers 20
- Junk Box Settings 21
  - General Settings 21
  - Action Settings 22
  - Miscellaneous Settings 22
- Junk Box Summary 23
- User View Setup 25
- Monitoring 27
  - Viewing Alerts 28

Anti-Spam Anti-Phishing Techniques 29

- SonicWALL Email Security and Mail Threats 29
- Managing Spam 30
  - Spam Identification 30
- Default Spam Management 31
- Address Books 33
- Anti-Spam Aggressiveness 35
  - Configuring GRID Network Aggressiveness 35

Configuring Adversarial Bayesian Aggressiveness Settings 35
Determining Amounts and Flavors of Spam 36
Languages 36
Miscategorized Email Messages 36
Anti-Phishing 37
What is Enterprise Phishing? 37
Preventing Phishing 38
Configuring Phishing Protection 38
Use SonicWALL Email Security's Community to Alert Others 39
Report Phishing and Other Enterprise Fraud to SonicWALL Email Security 39
Anti-Virus Techniques 41
How Virus Checking Works 41
Preventing Viruses and Likely Viruses in Email 42
Auditing 45
Email Auditing 45
Searching InboundEmails 45
Audit Simple Search 46
Audit Advanced View 46
Configure Auditing 48
Users, Groups, & Domains 49
Working with Users 49
Finding All Users 49
Sort 50
Signing In as a User 50
Resetting User Message Management Setting to Default 50
Edit User Rights 50
Import 51
Export 51
Adding a Non-LDAP User 52
Editing a Non-LDAP User 52
Removing a Non-LDAP User 53
Enabling Authentication for Non-LDAP Users 53
Working with Groups 53
About LDAP Groups 53
Add a New Group 54
Finding a Group 54
Removing a Group 54
Listing Group Members 55
Setting an LDAP Group Role 55
Setting Junk Blocking Options for LDAP Groups 56
User View Setup 57

Anti-Spam Aggressiveness 58
Languages 59
Junk Box Summary 60
Spam Management 61
Phishing Management 62
Virus Management 63
Forcing All Members to Group Settings 63
Working with Domains 64
SonicWALL Email Security Roles 64

Junk Box 65

Junk Box—Simple View 65
Junk Box—Advanced View 66
Working with Junk Box Messages 68
View 68
Unjunk 68
Managing Junk Summaries 68
Supported Search in Audit and Junkbox 69

Reports and Monitoring 71

Reporting in SonicWALL Email Security 71
Overview Reports 71
Reports Dashboard 72
Inbound Good vs Junk 73
Junk Email Breakdown Report 74
Anti-Spam Reports 75
Spam Caught 75
Top Spam Recipients 76
Anti-Phishing Reports 77
Phishing Messages 77
Anti-Virus Reports 78
Inbound Viruses Caught 78
Directory Protection 78
Number of Directory Harvest Attacks (DHA) 78
Scheduled Reports 79
Customize a Report 79
Add Scheduled Report 80
Download Report 81

Warranty and Licensing 1

Warranty and Licensing Agreement 1
Limited Warranty 1
End User Licensing Agreement 2

CHAPTER 1

Pre-Configuration Tasks

Introduction

This chapter describes pre-configuration information, such as purchasing and activating the SonicWALL Hosted Email Security solution.

This chapter contains the following sections:

- "Initial Configuration" on page 7
- "Activating the Hosted Email Security Service" on page 8
- "Logging In" on page 9

For installation and set up instructions for your Hosted Email Security solution, refer to the *Dell SonicWALL Hosted Email Security Quick Start Guide*.

Note For security purposes, the Hosted Email Security terminates your session if there is no activity for 10 minutes. You must log in again if this occurs.

Initial Configuration

To configure a SonicWALL Hosted Email Security solution, you must have a computer that meets or exceeds the following requirements:

- An Internet connection
- A Web browser supporting Java Script and HTTP uploads. Supported browsers include the following:

Accepted Browser	Browser Number Version
Internet Explorer	7.0 or higher
Firefox	3.0 or higher
Opera	9.10 or higher for Windows
Chrome	4.0 or higher
Safari	3.0 or higher for MacOS

Note Because many of the windows are pop-up windows, configure your Web browser's pop-up blockers to allow pop-ups from your organization's server before using SonicWALL Email Security.

Activating the Hosted Email Security Service

After purchasing the Hosted Email Security service, you are then directed to the activation screen.

Specify the following fields, then click **Activate Services**:

- **Domain Name**—The primary domain name that is associated with your SonicWALL Hosted Email Security solution.
- **Mail Server Host / IP Address**—The IP address of the mail server hosting your user mailbox(es).
- **Email Address / Login**—The email address or login name associated with your SonicWALL Hosted Email Security account.
- **Password**—The password associated with your SonicWALL Hosted Email Security account.

A message displays confirming successful activation and product registration. Click **Go to HES Console** to continue.

Adding MX Records

After activating your Hosted Email Security service, you may receive a message to replace your current MX records settings.

Mail eXchange (MX) records specify the delivery route for email messages sent to your newly specified SonicWALL Hosted Email Security domain name.The SonicWALL Data Center can then create an internal MX record so mail is correctly routed to the specified domain.

Multiple MX records are assigned to your domain name. Each MX record designates a priority to organize the way your domain's mail servers receive incoming email messages; the lower the number, the higher the priority. You should always set back-up priority numbers in case the primary mail server fails or is down.

For example, a customer wishes to activate the domain name *jumbo.com*. Since the SonicWALL Data Center hosts *snwlhosted.com*, the domain then becomes *jumbo.com.snwlhosted.com*. After an MX record is created, where the customer publishes *jumbo.com MX jumbo.com.snwlhosted.com*, SonicWALL then publishes an A record: *jumbo.com.snwlhosted.com A 173.240.21.100*, where *173.240.21.100* is the IP address that SonicWALL's Hosted analyzers use to route emails sent to the jumbo.com domain.

For more information regarding MX records, contact your ISP or refer to the Knowledge Base Article "Setting Up Your MX Record for Email Security Hosted Solution" located at: https://www.fuzeqna.com/sonicwallkb/consumer/kbdetail.asp?kbid=9670

Logging In

After completing the activation process, click the **Go to HES Console** button to be directed to the Hosted Email Security console. You can also open a new Web browser and navigate to: https://www.snwlhosted.com. Enter the User Name and Password you configured in the Activation process, then click **Log In**.

CHAPTER 2

System

Introduction

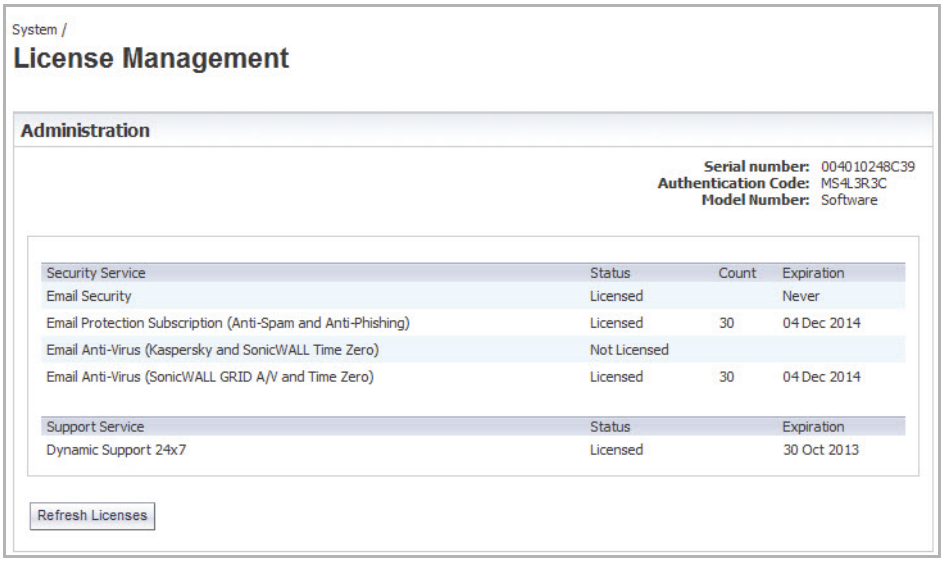
In this chapter, you will learn how to configure the system more extensively and learn more about additional system administration capabilities.

This chapter contains the following sections:

- “License Management” on page 11
- “Administration” on page 13
- “Network Architecture” on page 14
- “LDAP Configuration” on page 16
- “Junk Box Settings” on page 21
- “Junk Box Summary” on page 23
- “User View Setup” on page 25
- “Monitoring” on page 27

License Management

The License Management page allows you to view current Security and Support Services for your Hosted Email Security solution. To see more regarding the information on the License Management page, log in to your hosted.mysonicwall.com account.



Serial Number—The serial number of your Hosted Email Security solution.

Authentication Code—The code you entered upon purchasing/activating the Hosted Email Security solution.

Model Number—Since there is no physical appliance for the Hosted Email Security solution, the model number is listed as Software.

Available Services

SonicWALL Hosted Email Security comes with several services that must be licensed separately. For maximum effectiveness, all services are recommended. The following services available:

- **Email Security**—The standard license that comes with the service and enables basic components. This license allows the use of basic service features.
- **Email Protection Subscription (Anti-Spam and Anti-Phishing)**—This license protects against email spam and phishing attacks.
- **Email Anti-Virus (Kaspersky and SonicWALL Time Zero)**—Provides updates for Kaspersky anti-virus definitions and SonicWALL Time Zero technology for immediate protection from new virus outbreaks.
- **Email Anti-Virus (SonicWALL Grid A/V and SonicWALL Time Zero)**—Provides updates for SonicWALL Grid anti-virus definitions and SonicWALL Time Zero technology for immediate protection from new virus outbreaks.

License Table

The following table provides details about the different types of licenses:

Security Service	Name of the SonicWALL Hosted Email Security service.
Status	The status may be one of the following: Licensed: Services has a regular valid license. Free Trial: Service has been using the 14-day free trial license. Not Licensed: Service has not been licensed, neither through a regular license nor through a free trial license. Perpetual: The Base Key license comes with the purchase of the product and is perpetual. Note that the Base Key is the only perpetual license.
Free Trial	SonicWALL offers the opportunity to try out various services for a trial period of 14 days. Try: This link leads to information about the service, and allows you to sign up for a free trial license. If a free trial is accepted, the “Try” option is removed from this column, and the Status column is updated to “Free Trial”.
Count	Number of users to which the license applies.
Expiration	Expiration date of the service. Never: Indicates the license never expires. Date: A specific date on which the given service expires.

License Keys

Once the product is registered with hosted.mysonicwall.com, the Hosted Email Security obtains the purchased licenses. The License Management page displays a summary of the credentials that were received and stored on the Email Security server.

The **Refresh Licenses** button is used to synchronize the state of the licenses on the server with the hosted.mysonicwall.com website. Upon successfully synchronizing, the licenses on your appliance or software will automatically update to those of your online account. This button is used to update the license status of your product manually.

Note To manage licences, login to your hosted.mysonicwall.com/Login.aspx account.

Administration

The Administration page allows you to change the master account Username and Password. SonicWALL strongly recommends that you change the master account password.

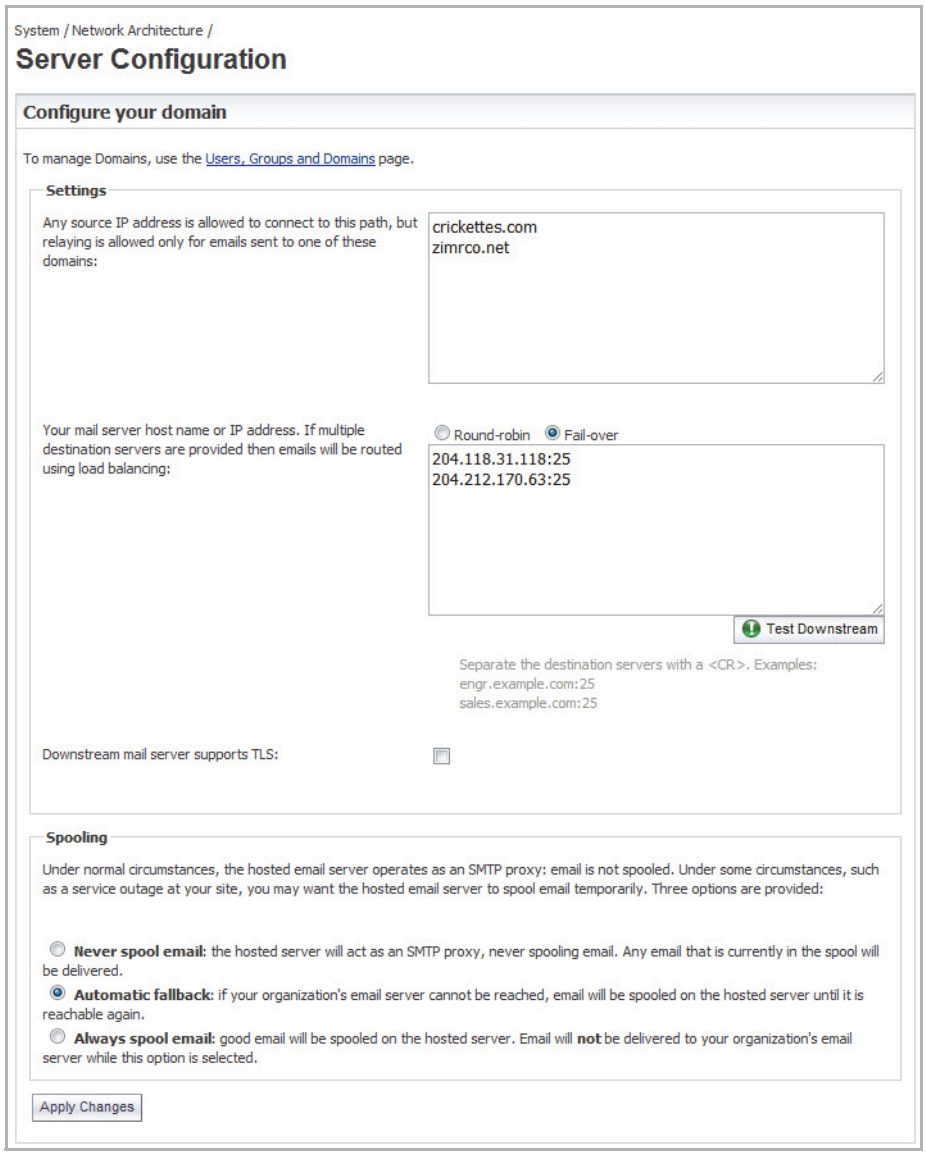
To change password, follow the procedures below:

1. The Username you originally registered with appears as the default Username (`admin@domain.com`)
2. Type a new password in the **Password** text box.
3. Type the same password in the **Confirm password** text box.
4. Click **Apply Changes**.

Network Architecture

Server Configuration

The **System > Network Architecture > Server Configuration** page allows you to configure the inbound destination server, which is the email server that will accept good email after SSonicWALL Hosted Email Security removes and quarantines junk mail. For example, this could be the IP address of a Microsoft Exchange server. The default port is 25.

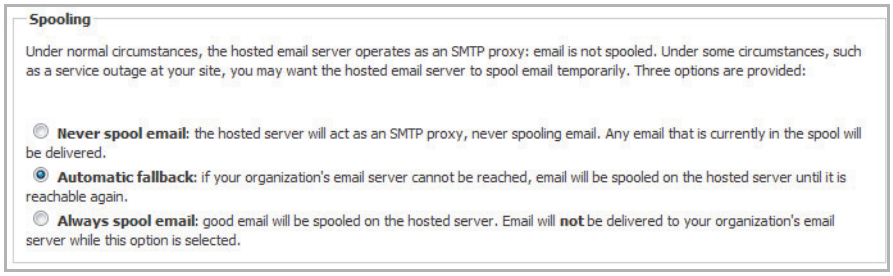


Any source IP address is allowed to this path, but relaying is allowed only for email sent to one of these domains	This field only displays domain name for emails to be relayed to. Note the default domain listed is the domain you initially activated the Hosted Email Security solution with. Navigate to the **Users, Groups & Domains > Domains** screen configure Domain settings.
Your mail server host name or IP address	Enter the mail server host name or IP address. Note the default IP address is the address you initially activated the Hosted Email Security solution with. If multiple destination servers are provided, emails will be routed using load balancing, in which you can also configure as either Round-robin or Fail-over. **Test Downstream:** Click this button to test connection to the specified mail server host name or address. A message displays, notifying you if the connection was successful or if the connection failed.
Downstream support TLS	Click this checkbox to enable Transport Layer Security (TLS) encryption for your downstream email messages.

Spooling

The Inbound Spooling feature available on the Hosted Email Security solution allows users to spool, or hold, mail when all the customer's receivers are unavailable. Inbound mail is then delivered when the receivers become available. The Hosted Email Security solution normally operates as an SMTP proxy, relaying email directly to your downstream receiver. However, it can also be configured to spool email when all of your organization's downstream receivers are unavailable.

When spooling is engaged, the proxy directs all good mail to the Email Security MTA for queuing and later delivery. When spooling is disengaged, the proxy resumes directly relaying mail to the receivers, and the MTA delivers the queued mail.



Choose the spooling option that best suits your needs:

- **Never Spool Email**—Select this option to never spool mail, regardless of the state of the downstream receivers. This is the default setting.
- **Automatic Fallback**—Select this option to spool mail if the downstream receivers unexpectedly go down or become unreachable. When configured to Automatic Fallback, spooling engages after the receiver farm has been unavailable for a period of time. Spooling then disengages when the receiver farm becomes available again.

- **Always Spool Email**—Select this option to leave the spooling feature engaged for all mail and to remain engaged until the mode is configured to **Never Spool Email** or **Automatic Fallback**. Note that manual spooling is intended for situations when the administrator knows the receivers will be down, such as a scheduled maintenance.

Note The Automatic Fallback feature initiates if the server becomes completely unresponsive. Because the feature may take a few moments to verify that the server is completely unresponsive, senders may see a transient error message.

LDAP Configuration

SonicWALL Email Security uses Lightweight Directory Access Protocol (LDAP) to integrate with your organization's email environment. LDAP is an Internet protocol that email programs use to look up users' contact information from a server. As users and email distribution lists are defined in your mail server, this information is automatically reflected in SonicWALL Email Security in real time.

Many enterprise networks use directory servers like Active Directory or Lotus Domino to manage user information. These directory servers support LDAP, and SonicWALL Email Security can automatically get user information from these directories using the LDAP. You can run SonicWALL Email Security without access to an LDAP server as well. If your organization does not use a directory server, users cannot access their Junk Boxes, and all inbound email is managed by the message-management settings defined by the administrator.

SonicWALL Email Security uses the following data from your mail environment.

- Login Name and Password: When a user attempts to log into the SonicWALL Email Security server, their login name and password are verified against the mail server using LDAP authentication. Therefore, changes made to the usernames and passwords are automatically uploaded to SonicWALL Email Security in real time.
- If your organization allows users to have multiple email aliases, SonicWALL Email Security ensures any individual settings defined for the user extends to all the user's email aliases. This means that junk sent to those aliases aggregates into the same folder.
- Email groups or distribution lists in your organization are imported into SonicWALL Email Security. You can manage the settings for the distribution list in the same way as a user's settings.

LDAP groups allow you to assign roles to user groups and set spam-blocking options for user groups.

Configuring LDAP

Use the LDAP Configuration screen to configure SonicWALL Email Security for username and password authentication for all employees in the enterprise.

SonicWALL recommends completing the LDAP configuration to get the complete list of users who are allowed to login to their Junk Box. If a user does not appear in the User list in the User & Group screen, their email will be filtered, but they cannot view their personal Junk Box or change default message management settings.

Enter the server information and login information to test the connection to the LDAP server.

1. Click the **Add Server** button to add a new LDAP Server. Configuring the LDAP server is essential to enabling per-user access and management. These settings are limited according to the preferences set in the User Management pane. See the "User View Setup" section on page 25 for details.

2. The following checkboxes appear under the **Settings** section:
   - **Show Enhanced LDAP Mappings fields:** Select this option for Enhanced LDAP, or LDAP Redundancy. You will have to specify the Secondary Server IP address and Port number.
   - **Auto-fill LDAP Query fields when saving configurations:** Select to automatically fill the LDAP Query fields upon saving.
3. Enter the following information under the **LDAP Server Configuration** section:
   - **Friendly Name:** The friendly name for your LDAP server.
   - **Primary Server Name or IP address:** The DNS name or IP address of your LDAP server. (Configuration checklist parameter M)
   - **Port number:** The TCP port running the LDAP service. The default LDAP port is 389. (Configuration checklist parameter N)
   - **LDAP server type:** Choose the appropriate type of LDAP server from the dropdown list.
   - **LDAP page size:** Specify the maximum page size to be queried. The default size is 100.
   - **Requires SSL:** Select this box if your server requires a secured connection.
   - **Allow LDAP referrals**: Leaving this option unchecked will disable LDAP referrals and speed up logins. You may select this option if your organization has multiple LDAP servers in which the LDAP server can delegate parts of a request for information to other LDAP servers that may have more information.
4. In the **Authentication Method** section, specify if the LDAP login method for your server is by **Anonymous Bind** or **Login**. Specify the **Login name** and **Password**. This may be a regular user on the network, and typically does not have to be a network administrator.

Note

Some LDAP servers allow any user to acquire a list of valid email addresses. This state of allowing full access to anybody who asks is called Anonymous Bind. In contrast to Anonymous Bind, most LDAP servers, such as Microsoft's Active Directory, require a valid username/password in order to get the list of valid email addresses. (Configuration checklist parameter O and P)

5. Click the **Test LDAP Login** button.

   A successful test indicates a simple connection was made to the LDAP server. If you are using anonymous bind access, be aware that even if the connection is successful, anonymous bind privileges might not be high enough to retrieve the data required by SonicWALL Email Security.

6. Click **Save Changes**.

LDAP Query Panel

To access the **LDAP Query Panel** settings window, click the Friendly Name link or the Edit button of the server you wish to configure. If the “Auto-fill LDAP Query Fields” checkbox is selected in the Settings section, the following fields will be automatically filled in with default values after the basic configuration steps are completed.

To configure Query Information for LDAP users, follow the procedures below:

1. Enter values for the following fields:
   - **Directory node to begin search:** The node of the LDAP directory to start a search for users. (Configuration checklist parameter Q).
   - **Filter:** The LDAP filter used to retrieve users from the directory.
   - **User login name attribute:** The LDAP attribute that corresponds to the user ID.
   - **Email alias attribute:** The LDAP attribute that corresponds to email aliases.
   - **Use SMTP addresses only:** Select the checkbox to enable the use of SMTP addresses.
2. Click the **Test User Query** button to verify that the configuration is correct.
3. Click **Save Changes** to save and apply all changes made.

Note Click the **Auto-fill User Fields** button to have SonicWALL Email Security automatically complete the remainder of this section.

To configure LDAP Settings for Groups, follow the procedures below:

1. Enter values for the following fields:
   - **Directory node to begin search:** The node of the LDAP directory to start a search for users. (Configuration checklist parameter Q).
   - **Filter:** the LDAP filter used to retrieve groups from the directory.
   - **Group name attribute:** the LDAP attribute that corresponds to group names.
   - **Group members attribute:** the LDAP attribute that corresponds to group members.
   - **User member attribute:** the LDAP attribute that specifies attribute inside each user's entry in LDAP that lists the groups or mailing lists that this user is a member of.
2. Click the **Test User Query** button to verify that the configuration is correct.
3. Click **Save Changes** to save and apply all changes made.

Note Click the **Auto-fill Group Fields** button to have SonicWALL Email Security automatically complete the remainder of this section. Note that if you have a large number of user mailboxes, applying these changes could take several minutes.

Add LDAP Mappings

On some LDAP servers, such as Lotus Domino, some valid addresses do not appear in LDAP. Use this section with LDAP servers that only store the “local” or “user” portion of the email addresses. Click the **View Rules** button. The LDAP Mappings screen displays:

Domain Mappings

- **Domain is:** Choose this option from the first dropdown menu to add additional mappings from one domain to another.
- **Replace with:** If this option is chosen from the second dropdown menu, then the domain is replaced. For example, if the *Domain is* “engr.corp.com” then *Replaced with* “corp.com”, then mail addressed to “anybody@engr.corp.com” is instead sent to “anybody@corp.com”.
- **Also add:** If this option is chosen from the second dropdown menu, then when the first domain is found, the second domain is added to the list of valid domains. For example, if “engr.corp.com” is the first domain and “sales.corps.com” is the second, then when the domain “engr.corp.com” is found in the list of valid LDAP domains, then “sales.corps.com” is also added to that list.

Character Substitutions

- **Left hand side character is:** Choose this option from the first dropdown menu to add character substitution mappings.
- **Replace with:** If this option is chosen from the second dropdown menu, then the character is replaced in all characters to the left of the “@” sign in the email address. For example, if the space character, “ ”, is the first character, and the “-” is the second character, then an email addressed to “Colin Brown@corp.com” would be sent to “Colin-Brown@corp.com”.
- **Also add:** If this option is chosen from the second dropdown menu, then a second email address is added to the list of valid email addresses. For example, if “-” is the first character, and “.” is the second character, then if “Obi-W-Kenobi@corp.com” is a valid email address, the address “Obi.W.Kenobi@corp.com” would also be considered a valid email address.

Note This screen does not make changes to your LDAP system or rewrite any email addresses; it only makes changes to the way SonicWALL Email Security interprets certain email addresses.

Configuring SonicWALL Email Security for Multiple LDAP Servers

The LDAP configuration page allows administrators to configure more than one LDAP server. All LDAP servers are listed. For each LDAP server, you can edit or delete it without affecting the connection of other LDAP servers.

To add an LDAP server, follow the procedures listed below:

1. Log in as the Email Security administrator.
2. Click **System** and then **LDAP Configuration**.
3. Click the **Add Server** button.
4. Fill in the connection information for the LDAP server you wish to add. Be sure to give it a unique friendly name so that you can easily identify it in the list of servers.
5. When you are finished, click **Save Changes**. Use the test button to confirm that the LDAP server is properly connected and configured.

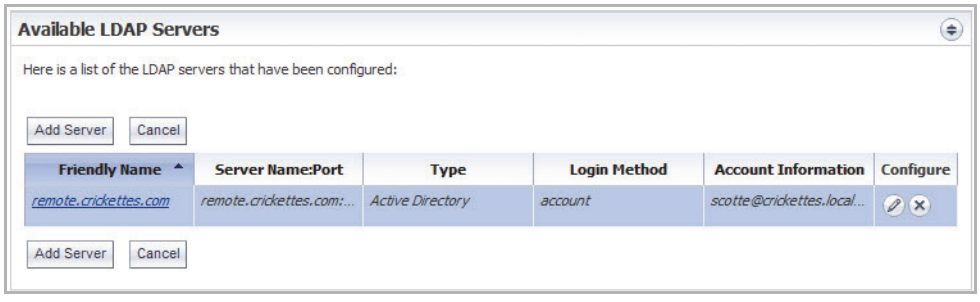
Administering Multi-LDAP Environments

Administrators must log into a specific domain unless they are the SonicWALL Email Security administrator. Once a domain administrator is logged in, she can modify the Email Security settings for her domain, including the anti-spam settings. The Email Security administrator can see all the LDAP servers attached to SonicWALL Email Security. The administrator logs in with no domain specified.

Editing LDAP Connection Information

The Email Security administrator configures the multiple domains. To change the settings of an existing LDAP server:

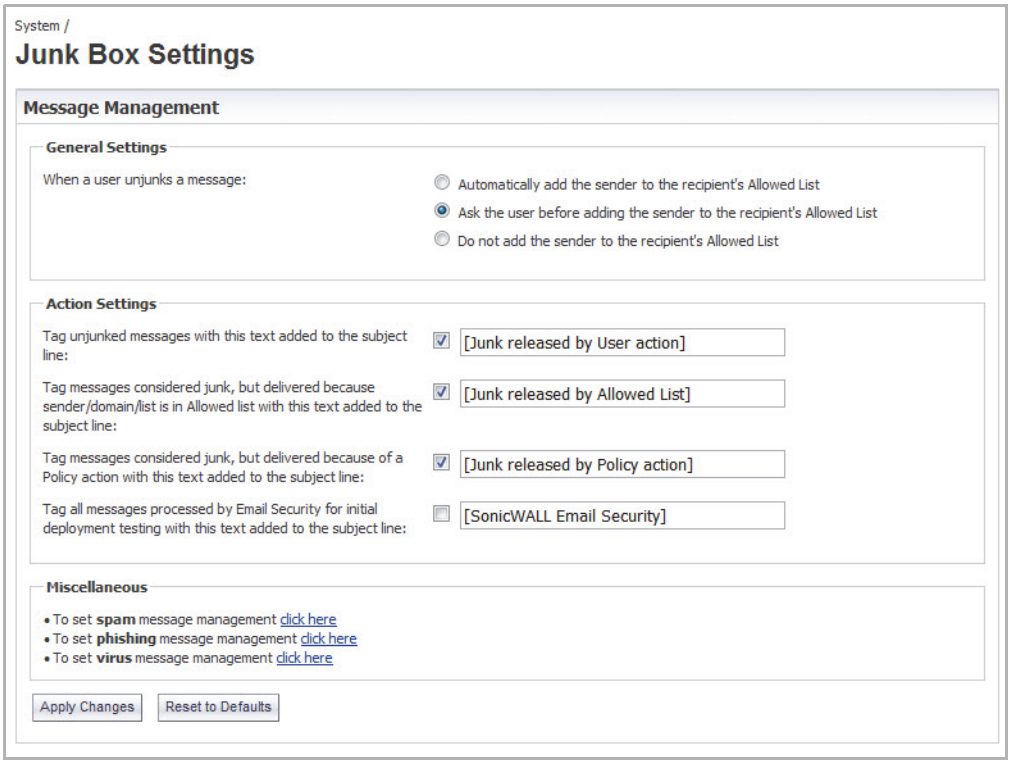
1. Log in as the Email Security administrator.
2. Navigate to the **System > LDAP Configuration** page.
3. Click the server name link or the Edit (pencil) button associated with the friendly name of the LDAP server you want to change.



4. Edit the details of the LDAP server using the information you have collected.
5. When you are done, click **Apply Changes** and use the test button to confirm that the LDAP server is properly connected and configured.

Junk Box Settings

The Junk Box Settings page allows you to configure Junk Box message management settings.



General Settings

Select the action the Hosted Email Securitywill take when a user unjunks a message:

- Automatically add the sender to the recipient's Allowed List
- Ask the user before adding the sender to the recipient's Allowed List
- Do not add the sender to the recipient's Allowed List

Action Settings

The following settings define conditions for tagging messages delivered to users' inboxes. The tags below will be prefixed to the subject line of the message:

- **Tag unjunked messages with this text added to the subject line**—Select this checkbox to tag unjunked messages. Specify the words to be used for tagging.
- **Tag messages considered junk, but delivered because sender/domain/list is in Allowed list with the text added to the subject line—**Select this checkbox to tag messages considered junk, but are to be delivered because either the sender, domain, or list is in the Allowed List. Specify the words to be used for tagging.
- **Tag messages considered junk, but delivered because of a Policy action with the text added to the subject line**—Select this checkbox to tag messages considered junk, but are to be delivered because of a Policy action. Specify the words to be used for tagging.
- **Tag all messages processed by Email Security for initial deployment testing with this text added to the subject line—**Note that this option is intended for use during initial deployment testing of a new Hosted Email Security installation. Select this option to tag all messages to be processed by the Hosted Email Security and specify the text to be tagged.

Miscellaneous Settings

Click on the following links to configure message management for available services:

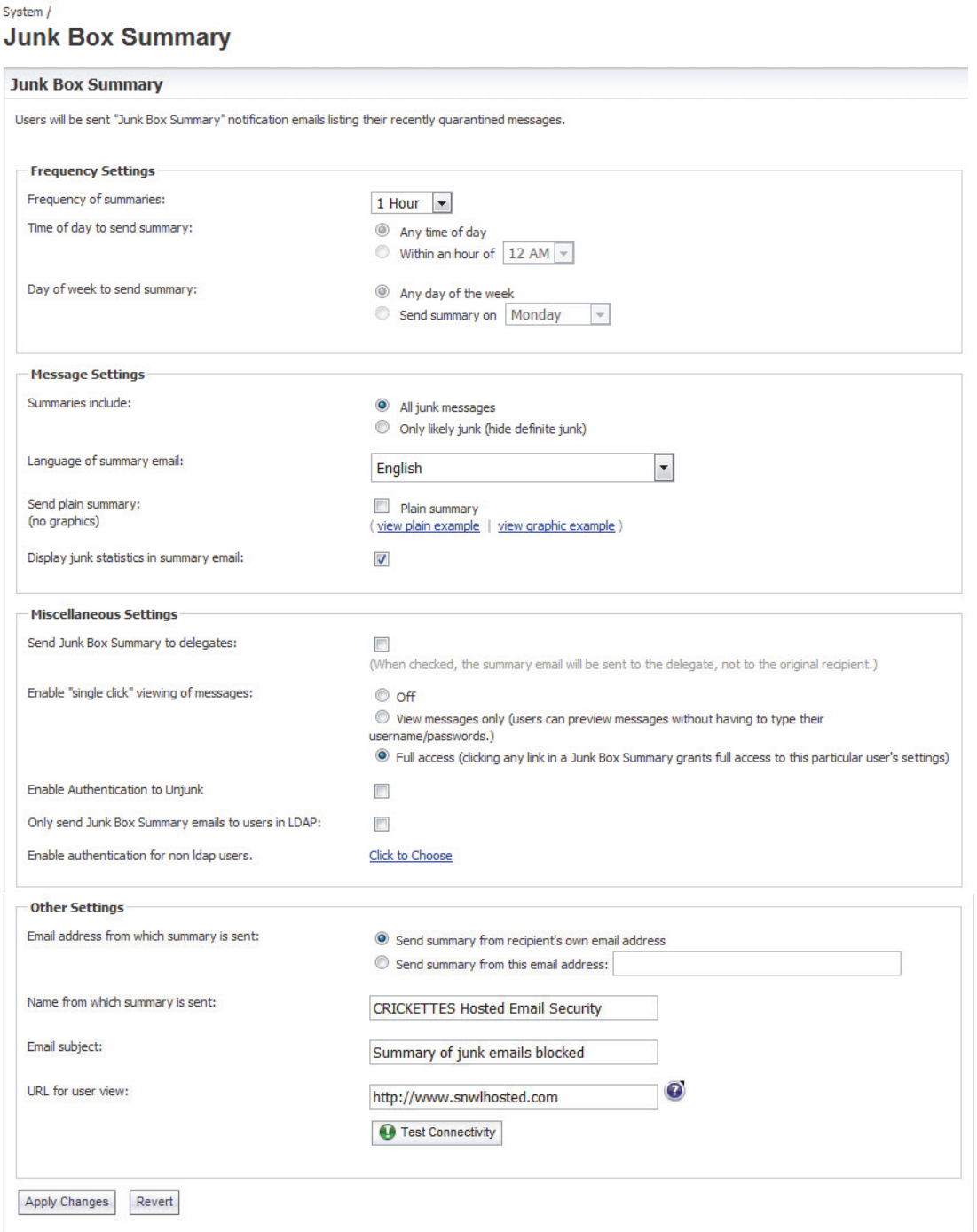
- **Spam**—Click this link to direct you to the Anti-Spam screen.
- **Phishing**—Click this link to direct you to the Anti-Phishing screen.
- **Virus—**Click this link to direct you to the Anti-Virus Techniques screen.

Junk Box Summary

SonicWALL Email Security sends an email message to users listing all the messages that have been placed in their Junk Box. The Junk Box Summary includes:

- Good vs Junk count (organization)
- Number of blocked messages (per user)

Users can unjunk items listed in the Junk Box Summary email by clicking links in the email. When unjunking there is an option not to add a sender to the Allowed list.



Frequency Settings

1. Select **Frequency of summaries** from the dropdown box.
2. Select the **Time of day to send summary** from the available options. Note that individual users can override these settings.
3. Select the **Day of the week to send summary** from the available options. Note that individual users can override these settings.

Message Settings

4. Choose whether to include in message summary **All junk messages** or **Only likely junk (hide definite junk)**.
   If **All junk messages** is selected, both *definite* and *likely* junk will be included.
   If **Only likely junk** is selected, only *likely* junk messages will be included in the message summary; messages determined *definite* junk will not be included.
5. Choose **Language of summary email** from the dropdown list.
6. Enable **Display junk statistics in summary email** by selecting the checkbox.

Miscellaneous Settings

7. Select the checkbox to **Send Junk Box Summary to delegates**. When selected, the summary email will be sent to the delegate, not to the original recipient.
8. To **Enable "single click" viewing of messages**, select from the following:
   - **Off**—Single click viewing messages is not enabled.
   - **View messages only—**Users can preview messages without having to log in with their username and password.
   - **Full access**—Clicking any link in the Junk Box Summary grants the user full access to messages without having to log in with their username and password.
9. Choose the **Enable Authentication to Unjunk** checkbox to make users authenticate when selecting messages to unjunk.
10. Choose to enable **Only Send Junk Box Summary emails to users in LDAP** by selecting the checkbox.
11. To **Enable Authentication for Non-LDAP Users**, click the **Click to Choose** link.

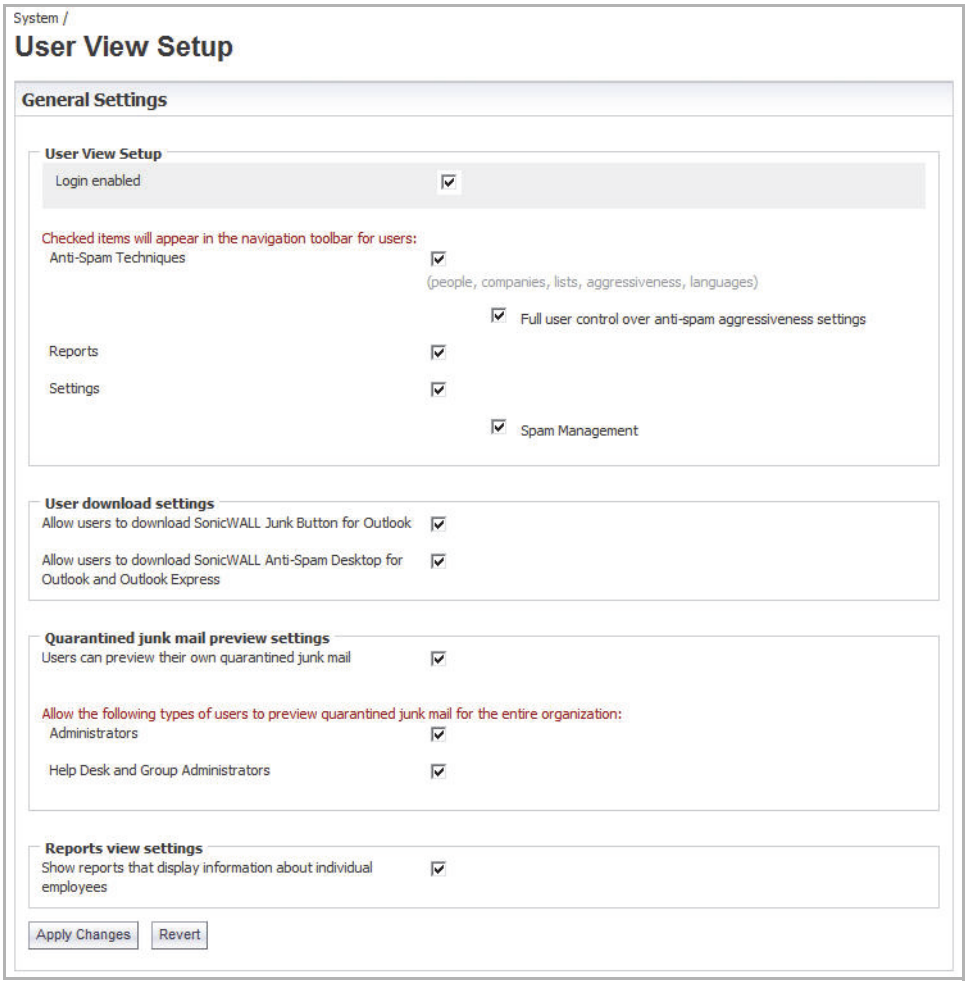
Other Settings

12. Choose the **Email address from which summary is sent**.
13. The message summary can come from the individual user or another email address, which you can enter in the space provided. Be aware that if summaries are sent because the address doesn't exist, the Junk Box Summary message will bounce as well.
14. Enter the **Name from which summary is sent**. This is the name that displays as the sender for summary messages. For example, *Company Name Junkbox*.
15. Enter the **Email Subject** for summary messages. For example, *Summary of junk emails blocked*.
16. The **URL for user view** is automatically filled in based on your server configuration, and is included in the Junk Box Summary email. Clicking on the email link in the message will allow users to unjunk messages.

17. Click the **Test Connectivity** button to test that the URL connects properly. If the test fails, check that the URL is correct.
18. Click the **Apply Changes** button.

User View Setup

Configure how the end users of the SonicWALL Email Security solution access the system and what capabilities of the solution are exposed to the end users.



To set up the User View settings, follow the procedures below:

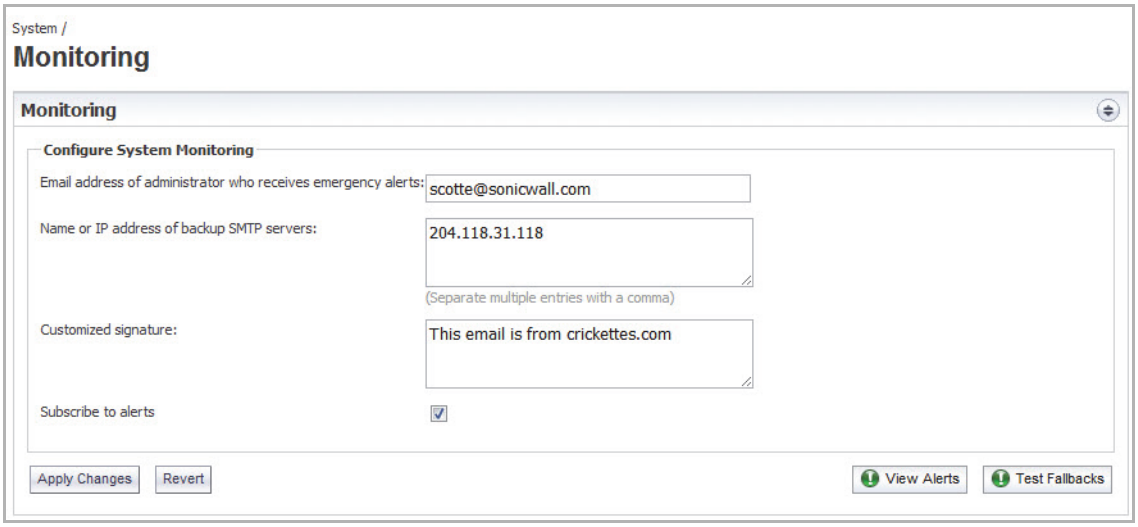
1. Select which items appear in the User Navigation Toolbar:
   - Select the **Login enabled** checkbox to allow users to access their junk boxes.
   - Allow users to log into SonicWALL Email Security and have access to their per-user Junk Box. If you disable this, mail will still be analyzed and quarantined, but users will not have access to their Junk Box.

- Select the **Anti-Spam Techniques** checkbox to include the user-configurable options available for blocking spam emails. Users can customize the categories People, Companies, and Lists into their personal Allowed and Blocked lists. You can choose to grant users full control over these settings by selecting the **Full user control over anti-spam aggressiveness settings** checkbox, or force them to accept the corporate aggressiveness defaults by leaving the checkbox empty.
- Select the **Reports** checkbox to provide junk email blocking information about your organization. Even if this option is checked, users may view only a small subset of the reports available to administrators.
- Select the **Settings** checkbox to provide options for management of the user's Junk Box, including individual junk summary reports and specifying delegates.

2. Determine the User Download Settings:
   - With the **Allow users to download SonicWALL Junk Button for Outlook** checkbox selected, users will be able to download the SonicWALL Email Security Junk Button for Outlook. The Junk Button is a lightweight plugin for Microsoft Outlook. It allows users to mark emails they receive as junk, but does not filter email.
   - With the **Allow users to download SonicWALL Anti-Spam Desktop for Outlook and Outlook Express** checkbox selected, users will be able to download the Anti-Spam Desktop. Anti-Spam desktop is a plugin for Microsoft Outlook and Outlook Express that filters spam and allows users to mark emails they receive as junk or good email. It is a complete anti-spam application.
3. Determine the settings for Quarantined Junk Mail Preview Settings:
   - Select the **Users can preview their own quarantined junk mail** checkbox to enable users to view their individual mail that is junked.
   - Choose which other types of users can preview quarantined junk mail. These roles are configured within SonicWALL Email Security.
4. Users are not usually shown reports which include information about users, such as email addresses. Select the **Reports view settings** checkbox to give user access to those reports.
5. Click **Apply Changes**.

Monitoring

Use the Monitoring page to configure system monitoring settings and alerts. Note that some of these fields may be pre-defined based on the information provided upon initial setup of the SonicWALL Email Security.



Email address of the administrator who receives emergency alerts—The email address of the mail server administrator. Enter the complete email address. For example, *user@example.com.*

Name or IP address of backup SMTP servers—Enter the name or IP address of one or more SMTP servers that can be used as fallback servers to send alerts to if the configured downstream email server(s) cannot be contacted. For example, *mail2.example.com* or *10.100.0.1.*

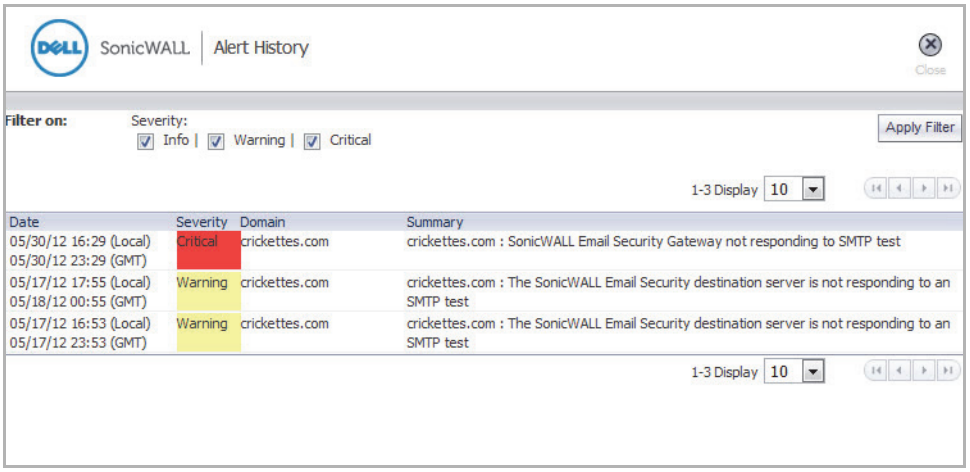
Customized Signature—Enter a signature to append at the end of your email messages.

Subscribe to alerts—Select the checkbox to receive alerts.

Test Fallbacks—Click this button to test the name or IP address(es) listed as backup SMTP servers.

Viewing Alerts

You can also click the View Alerts button to see the Alert history for a specific Host.



Alerts in SonicWALL Email Security provide the following details:

- A time stamp
  - In local time
  - In GMT
- The severity of the alert, which is one of the following:
  - Info
  - Warning
  - Critical
- The domain of which the alert applies
- A summary of the alert

You may apply a severity filter to better assist you in viewing the alerts. Select the checkbox(es) of which alerts you want to view, then click **Apply Filter**.

CHAPTER 3

Anti-Spam Anti-Phishing Techniques

This chapter contains the following sections:

- "SonicWALL Email Security and Mail Threats" on page 29
- "Managing Spam" on page 30
- "Default Spam Management" on page 31
- "Address Books" on page 33
- "Anti-Spam Aggressiveness" on page 35
- "Languages" on page 36
- "Anti-Phishing" on page 37

SonicWALL Email Security and Mail Threats

SonicWALL Email Security determines that an email fits *only one* of the following threats: Spam, Likely Spam, Phishing, Likely Phishing, Virus, Likely Virus, or Directory Harvest Attack (DHA). It uses the following precedence order when evaluating threats in email messages:

- Virus
- Likely Virus
- Policy Filters
- Phishing
- Likely Phishing
- Spam
- Likely Spam

For example, if a message is both a virus and a spam, the message will be categorized as a virus since virus is higher in precedence than spam.

If SonicWALL Email Security determines that the message is *not* any of the above threats, it is delivered to the destination server.

Managing Spam

SonicWALL Email Security uses multiple methods of detecting spam and other unwanted email. These include using specific Allowed and Blocked lists of people, domains, and mailing lists; patterns created by studying what other users mark as junk mail, and the ability to enable third-party blocked lists.

You can define multiple methods of identifying spam for your organization; users can specify their individual preferences to a lesser extent. In addition, SonicWALL Email Security provides updated lists and collaborative thumbprints to aid in identifying spam and junk messages.

Spam Identification

SonicWALL Email Security uses a multi-prong approach to identifying spam and other unwanted email. It is useful to understand the general operation so you can build your lists appropriately.

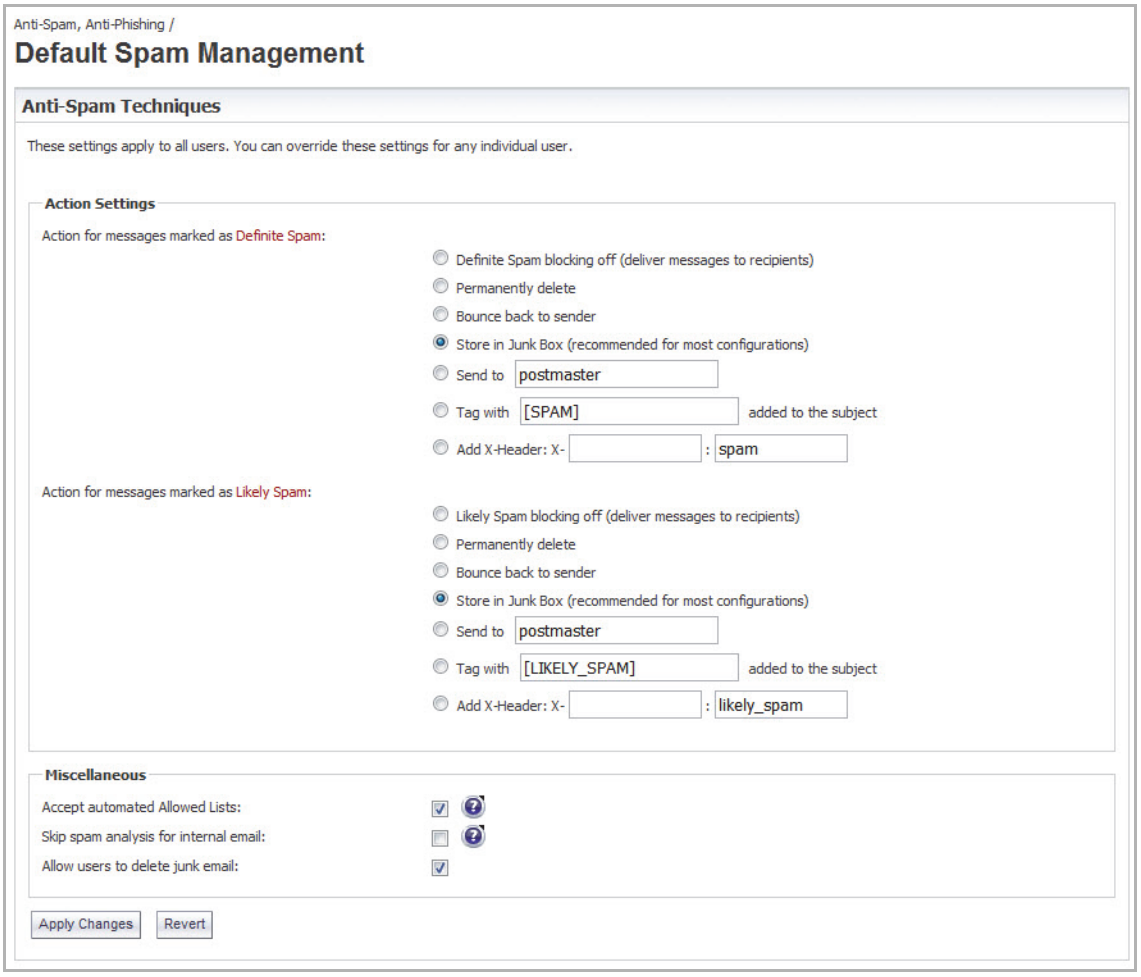
When an email comes in, the sender of the email is checked against the various allowed and blocked lists first, starting with the corporate list, then the recipient's list, and finally theSonicWALL Email Security-provided lists. If a specific sender is on the corporate blocked list but that same sender is on a user's allowed list, the message is blocked, as the corporate settings are a higher priority than a user's.

More detailed lists take precedence over the more general lists. For example, if a message is received from `aname@domain.com` and your organization's Blocked list includes domain.com but a user's Allowed list contains the specific email address `aname@domain.com`, the message is not blocked because the sender's full address is in an Allowed list.

After all the lists are checked, if the message has not been identified as junk based on the Allowed and Blocked lists, SonicWALL Email Security analyzes messages' headers and contents, and use collaborative thumbprinting to block email that contains junk.

Default Spam Management

Use the Default Spam Management window to select options for dealing with spam and likely spam. The default setting for spam and likely spam will quarantine the message in the user's junk box.



To manage messages marked as definite spam or likely spam, follow the procedures below:

1. Choose one of the following responses for messages marked as definite spam and likely spam:

Responses	Effect
Definite Spam filtering off	SonicWALL Email Security does not filter messages for spam. All messages are passed through to the recipient.
Permanently Delete	The email message is permanently deleted. CAUTION: If you select this option, your organization risks losing wanted email.
Bounce Back to Sender	The message is returned to sender with a message indicating that it was not deliverable.
Store in Junk Box (default setting)	The email message is stored in the Junk Box. It can be unjunked by users and administrators with appropriate permissions. This option is the recommended setting.
Send To	Enter the email address of the person to receive this email.

Responses	Effect
Tag With	This email is tagged with a term in the subject line, for example, [JUNK] or [Possible Junk?]. Selecting this option allows the user to have control of the email and can junk it if it is unwanted.
Add X-Header	This option adds an X-Header to the email with the key and value specified to the email message. The first text field defines the X-Header. The second text field is the value of the X-Header. For example, a header of type “X-EMSJudgedThisEmail” with value “DefiniteSpam” results in the email header as: “S-EMSJudged-ThisEmail:DefiniteSpam”.

Check the **Accept Automated Allowed List** checkbox to accept automated lists that are created by User Profilers. With this feature enabled, User Profilers analyze the recipients of emails from members of your organization and automatically added them to Allowed Lists.This helps reduce the false positives, which are good email messages judged as junk. This feature can be configured globally, for particular groups, or for specific users.

Note If this checkbox is unchecked in the Corporate, Group, or User windows, User Profilers have no effect.

2. Check the **Skip spam analysis for internal email checkbox** to exclude internal emails from spam analysis. If you are not routing internal email through SonicWALL Email Security, leave this checkbox unchecked.
3. Check the **Allow users to delete junk** checkbox to allow users to control the delete button on individual junk boxes.

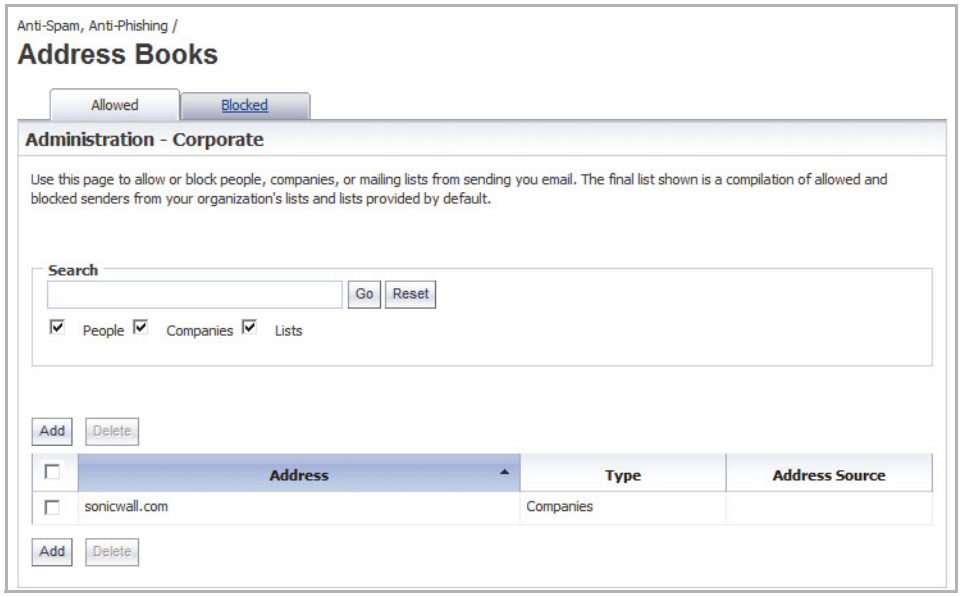
Note When you go on vacation or extended leave, deselect this box so that your vacation-response reply does not automatically place all recipients on your Allowed list.

4. Click **Apply Changes** to save.

Address Books

The Address Books page enables you to allow or block people, companies, or mailing lists from sending you email. The page shows a compilation of allowed and blocked senders from your organization's lists and lists provided by default.

If you attempt to add your own email address or your organization's domain, SonicWALL Email Security will display a warning. A user's email address is not automatically added to the allowed list because spammers sometimes use a recipient's own email address. Leaving the address off the allowed list does not prevent users from emailing themselves, but their emails are evaluated to determine if they are junk.

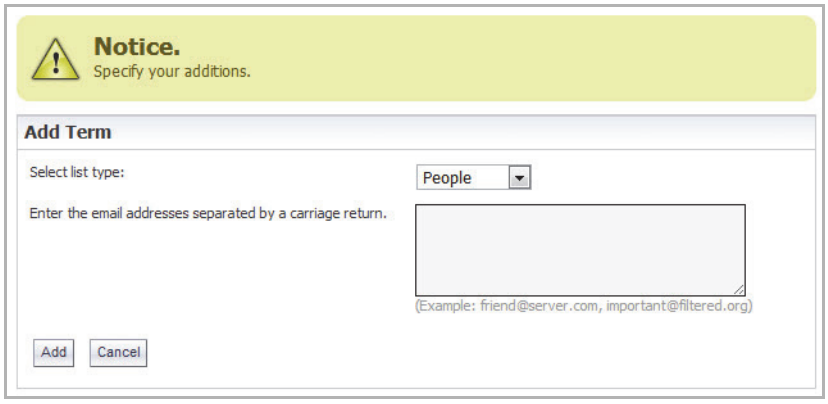


To search for an address, enter all or part of the email address in the Search field. For example, entering *sale* displays `sales@domain.com` as well as `forsale@domain.com`. Narrow your search by selecting the **People**, **Companies**, or **Lists** checkbox(es) below the Search field. Click **Go** to perform the search.

To add People, Companies, or Lists to the Allowed or Blocked lists, follow the procedures listed below:

1. Choose the Allowed or Blocked tab.
2. Click the **Add** button

3. Select the list type (People, Companies, Lists) from the dropdown menu. Enter one or more email addresses, separated by carriage returns, to add to the chosen list. Click **Add** to complete.



Note the following:

- You cannot put an address in both the Allowed and Blocked list simultaneously. If you add an address in one list that already exists on the other, it is removed from the first one.
- SonicWALL Email Security will warn you if you attempt to add your own email address or your own organization.
- Email addresses are not case-sensitive; SonicWALL Email Security converts the address to lowercase.
- SonicWALL Email Security will ignore any entries to the Allowed list if the sender-ID (SPF) check fails.
- You can allow and block email messages from entire domains. If you do business with certain domains regularly, you can add the domain to the Allowed list; SonicWALL Email Security allows all users from that domain to send email. Similarly, if you have a domain you want to block, enter it here and all users from that domain are blocked.
- SonicWALL Email Security does not support adding top-level domain names such as `.gov` or `.abc` to the Allowed and Blocked lists.
- Mailing list email messages are handled differently than individuals and domains because SonicWALL Email Security looks at the recipient's address rather than the sender's. Because many mailing list messages appear spam-like, entering mailing list addresses prevents misclassified messages.

To delete People, Companies, or Lists from the Allowed or Blocked lists:

1. Choose the Allowed or Blocked tab.
2. Select the checkbox next to the address(es) you want to delete.
3. Click the **Delete** button.

Anti-Spam Aggressiveness

The Anti-Spam Aggressiveness window allows you to tailor SonicWALL Email Security to your organization's preferences. Configuring this window is optional. SonicWALL Email Security recommends using the default setting of Medium unless you require different settings for specific types of spam blocking.

Configuring GRID Network Aggressiveness

The GRID Network Aggressiveness technique determines the degree to which you want to use the collaborative database. SonicWALL Email Security maintains a database of junk mail identified by the entire user community. You can customize the level of community input on your corporate spam blocking. Selecting a stronger setting makes SonicWALL Email Security more likely more responsive to other users who mark a message as spam.

Use these settings to specify how stringently SonicWALL Email Security evaluates messages.

- If you choose **Mildest**, you will receive a large amount of questionable email in your mailbox. This is the lightest level of Anti-Spam Aggressiveness.
- If you choose **Mild**, you are likely to receive more questionable email in your mailbox and receive less email in the Junk Box. This can cause you to spend more time weeding unwanted email from your personal mailbox.
- If you choose **Medium**, you accept SonicWALL Email Security's spam-blocking evaluation.
- If you choose **Strong**, SonicWALL Email Security rules out greater amounts of spam for you. This can create a slightly higher probability of good email messages in your Junk Box.
- If you choose **Strongest**, SonicWALL Email Security heavily filters out spam. This creates an even higher probability of good email messages in your Junk Box.

Configuring Adversarial Bayesian Aggressiveness Settings

The Adversarial Bayesian technique refers to SonicWALL Email Security's statistical engine that analyzes messages for many of the spam characteristics. This is the high-level setting for the Rules portion of spam blocking and lets you choose where you want to be in the continuum of choice and volume of email. This setting determines the threshold for how likely an email message is to be identified as junk email.

Use these settings to specify how stringently SonicWALL Email Security evaluates messages.

- If you choose **Mildest**, you will receive a large amount of questionable email in your mailbox. This is the lightest level of Anti-Spam Aggressiveness.
- If you choose **Mild**, you are likely to receive more questionable email in your mailbox and receive less email in the Junk Box. This can cause you to spend more time weeding unwanted email from your personal mailbox.
- If you choose **Medium**, you accept SonicWALL Email Security's spam-blocking evaluation.
- If you choose **Strong**, SonicWALL Email Security rules out greater amounts of spam for you. This can create a slightly higher probability of good email messages in your Junk Box.
- If you choose **Strongest**, SonicWALL Email Security heavily filters out spam. This creates an even higher probability of good email messages in your Junk Box.

Determining Amounts and Flavors of Spam

You can determine how aggressively to block particular types of spam, including sexual content, offensive language, get rich quick, gambling, advertisements, and images.

For each of the spam flavors:

- Choose **Mildest** to be able to view most of the emails that contain terms that relate to these topics.
- Choose **Mild** to be able to view email that contains terms that relate to these topics.
- Choose **Medium** to cause SonicWALL Email Security to tag this email as likely junk.
- Choose **Strong** to make it more likely that email with this content is junked.
- Choose **Strongest** to make it certain that email with this content is junked.

For example, the administrator has determined that they want to receive no email with sexual content by selecting Strong. They are less concerned about receiving advertisements, and selected Mild. You can also choose whether to allow users to unjunk specific flavors of spam.

Languages

You can allow, block, or enter no opinion on email messages in various languages. If you enter **No opinion**, SonicWALL Email Security judges the content of the email message based on the SonicWALL Email Security modules that are installed.

Note Some spam email messages are seen in English with a background encoded in different character sets such as Cyrillic, Baltic, or Turkish. This is done by spammers to bypass the anti-spam mechanism that only scans for words in English. In general, unless used, it is recommended to exclude these character sets. Common languages such as Spanish and German are normally not blocked.

Miscategorized Email Messages

The following happens when an email message is miscategorized:

- For false negatives, SonicWALL Email Security adds the sender address of the junked email to the user's Blocked List so that future email messages from this sender are blocked. (The original sender is blacklisted for the original recipient.)
- For false positives, SonicWALL Email Security adds the addresses of good email senders that were unjunked to the user's Allowed List. (The original sender is whitelisted for the original recipient.) If the sender email is the user's own email address, the address is not added to the allowed list, because spammers send email pretending to be from the user. Email sent to and from the same address will always be evaluated to determine if it is junk.
- These messages are sent to the global collaborative database. Good mail that was unjunked is analyzed to determine why it was categorized as junk.

Anti-Phishing

SonicWALL Email Security's Anti-Spam Anti-Phishing module protects organizations against email containing fraudulent content. There are two audiences for fraud: the consumer and enterprise users. SonicWALL Email Security focuses on preventing fraud that enters the enterprise via email. Email is an entry point for malicious hackers.

What is Enterprise Phishing?

There are numerous types of enterprise phishing.

- *Consumer phishers* try to con users into revealing personal information such as social security numbers, bank account information, credit card numbers, and driver's license identification. This is known as *identity theft.* Recouping from having a phisher steal your identity can take many hours and can cost consumers many dollars. Being phished can bring your life to a virtual standstill as you contact credit card companies, banks, state agencies, and others to regain your identity.
- *Enterprise phishers* attempt to trick users into revealing the organization's confidential information. This can cost thousands of executive and legal team hours and dollars. An organization's electronic-information life can stop abruptly if hackers deny services, disrupt email, or infiltrate sensitive databases.

Phishing aimed at the IT group in the organization can take the following forms:

- Email that appears to be from an enterprise service provider, such as a DNS server, can cause your organization's network to virtually disappear from the Web.
- Hacking into your web site can cause it to be shut down, altered, or defaced.
- Email might request passwords to highly sensitive databases, such as Human Resources or strategic marketing information. The email might take the form of bogus preventive maintenance.
- Other information inside the organization's firewall, such as Directory Harvest Attacks (DHA) to monitor your users.

Phishing can also take the form of malicious hackers spoofing your organization. Email is sent that appears to come from your organization can damage your community image and hurt your customers in the following ways:

- Spoofed email can ask customers to confirm their personal information.
- Spoofed email can ask customers to download new software releases, which are bogus and infected with viruses.

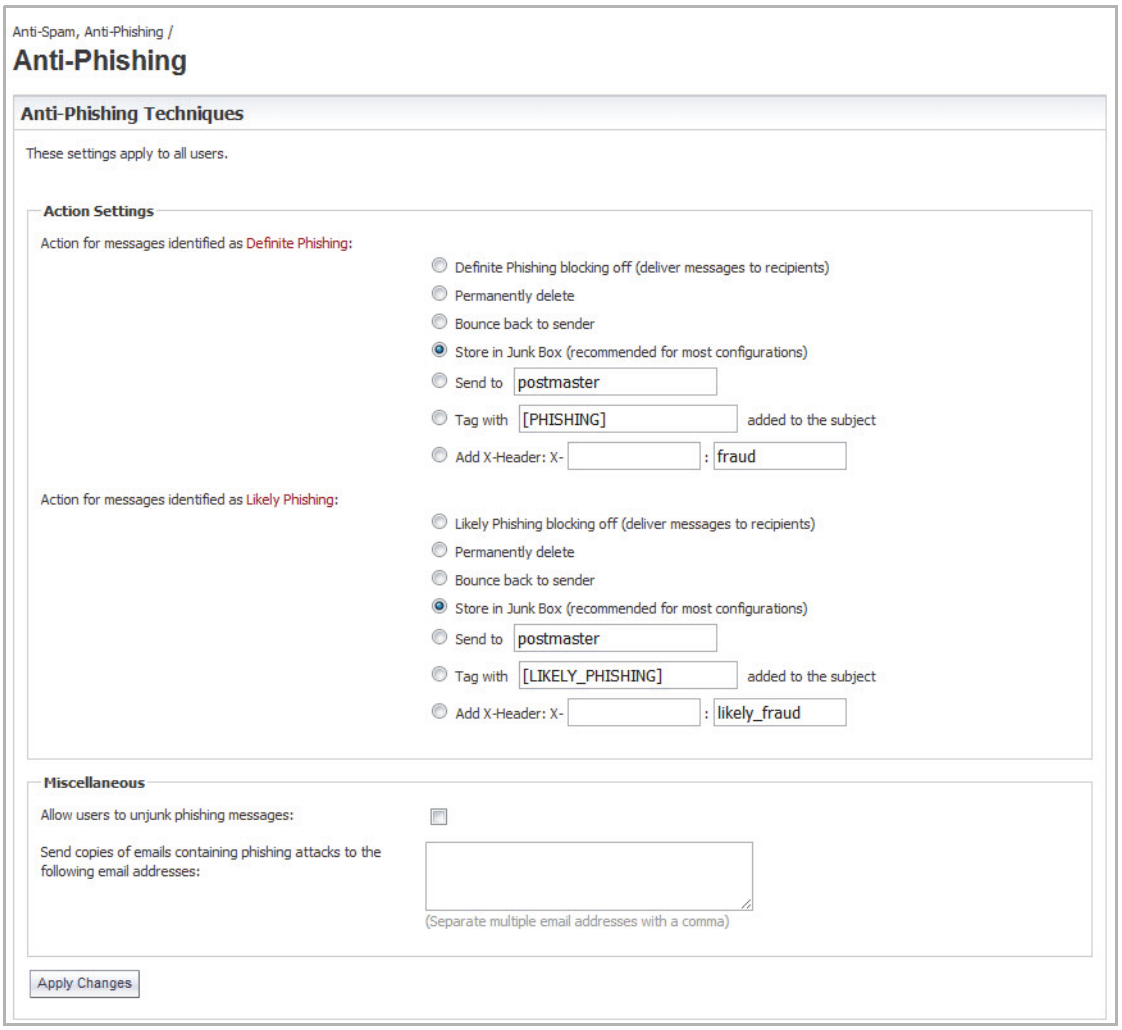
Preventing Phishing

Phishing harms organizations and consumers by raising the price of doing business, which raises the cost of goods and services. SonicWALL Email Security prevents phishing through:

Adapting SonicWALL Email Security's spam-fighting heuristics to phishing

- Divergence Detection™—ensures that all contact points are legitimate. Contact points include email addresses, URLs, phone numbers, and physical addresses.
- Sender ID or Sender Policy Framework (SPF)—a system that attempts to validate that a message is from the domain from which it purports to be. Sender ID authenticates that the domain from which the sender's message reports matches one of the IP addresses published by that domain. SonicWALL Email Security factors Sender ID pass or fail into its junk algorithm.

Configuring Phishing Protection



To configure SonicWALL Email Security to screen for phishing, complete the following procedures:

1. Navigate to the **Anti-Phishing** page.Click the radio button to choose which action to take for messages identified as **Definite Phishing**.
2. Click the radio button to choose which action to take for messages that contain **Likely Phishing**.
3. Check the **Allow users to unjunk phishing messages** checkbox if you want to allow users to unjunk fraudulent messages.
4. Enter one or more email addresses of people designated to receive **Copies of emails containing phishing attacks**.
5. To send copies of fraudulent email messages to a person or people designated to deal with them, enter the recipients' email addresses in the **Send copies of emails containing phishing attacks to the following email addresses** text box. \
6. Click **Apply Changes**.

Use SonicWALL Email Security's Community to Alert Others

Phishing is continuously evolving and adapting to weaknesses in the organization's network. Malicious hackers use any known weakness to infiltrate the corporate firewall. SonicWALL Email Security has tuned and enhanced their spam-management techniques to prevent phishing. SonicWALL Email Security also collects incidences of phishing and summarizes the email addresses, text, phone numbers, and domains of phishing perpetrators in a database, which stores the thumbprints of the phishing message.

Report Phishing and Other Enterprise Fraud to SonicWALL Email Security

SonicWALL Email Security alerts organizations to phishing attacks. SonicWALL Email Security needs you to report fraudulent email messages to mailto:fraud@sonicwall.com. Reporting phishing enables SonicWALL Email Security to alert other users to the phishing attacks you experienced.

CHAPTER 4

Anti-Virus Techniques

SonicWALL Email Security's Anti-Virus modules protect your organization from inbound email-borne viruses and prevent your employees from sending viruses with outbound email. Once SonicWALL Email Security has identified the email message or attachment that contains a virus or is likely to contain a virus, you choose how to manage the virus-infected email.

This chapter contains the following sections:

- "How Virus Checking Works" on page 41
- "Preventing Viruses and Likely Viruses in Email" on page 42

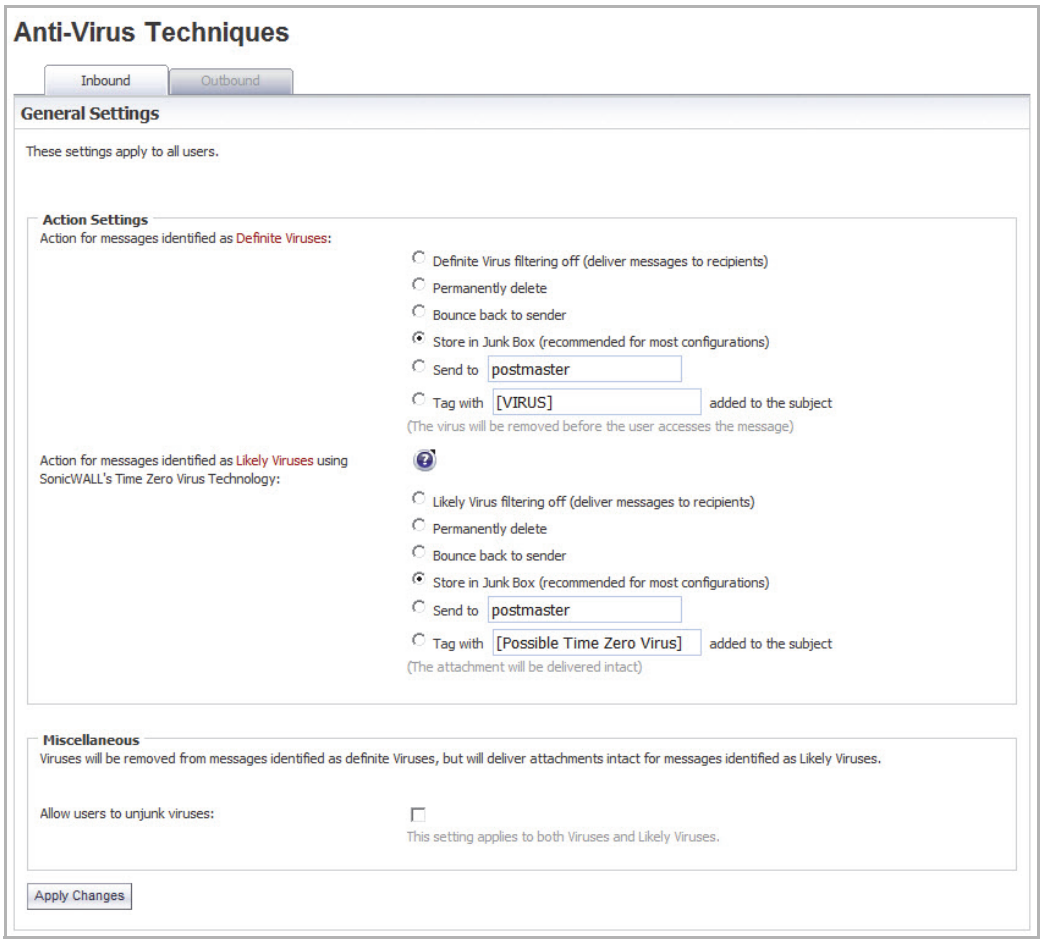
How Virus Checking Works

The Anti-Virus modules use virus-detection engines to scan email messages and attachments for viruses, Trojan horses, worms, and other types of malicious content. The virus-detection engines receive periodic updates to keep them current with the latest definitions of viruses. SonicWALL Email Security supports McAfee ® and Kaspersky virus-detection engines. You can choose to buy and deploy one or both virus-detection engines supported by SonicWALL Email Security. Messages determined to be dangerous by McAfee or Kaspersky engine are categorized as *Viruses*. SonicWALL Email Security also supports the SonicWALL GRID antivirus automatically. GRID virus-detection works in with the McAfee and Kaspersky virus-detection engines to improve your protection from virus payloads.

When any one of the virus-detection engines is activated, you also get the benefit of SonicWALL Email Security's **Time Zero Virus Technology**. This technology uses heuristic statistical methodology and virus outbreak responsive techniques to determine the probability that a message contains a virus. If the probability meets certain levels, the message is categorized as *Likely Virus*. This technology complements virus-detection engines and enabling this technology provides the greatest protection for *time zero viruses*, the first hours that a virus is released, when major anti-virus companies have not yet modified their virus definitions to catch it.

Preventing Viruses and Likely Viruses in Email

To configure Anti-Virus protection, navigate to the **Anti-Virus Techniques** page. If you have licensed more than one virus-detection engines, they will all work in tandem. Licensed virus-detection engines can be used on both inbound and outbound paths. Determine how to treat email messages that contain *Definite Viruses* or *Likely Viruses* and select the action to take.



See the table below for a description of the available actions:

Action	Consequences	Additional Information
Definite Virus Filtering Off	SonicWALL Email Security passes this email through to users without stripping the virus or likely virus.	This choice provides no screening for viruses or likely viruses. Messages are delivered to recipients.
Permanently Delete	SonicWALL Email Security permanently deletes this message.	This is a secure option for the enterprise because the virus or likely virus is permanently deleted. However, neither the receiver nor the sender knows that the email message contained a virus or likely virus. Once the message is deleted, you cannot retrieve it.

Action	Consequences	Additional Information
Bounce Back to Sender	SonicWALL Email Security bounces email back to the sender with the virus removed.	The sender is notified of the virus or likely virus in the email.
Store in Junk Box **(Default Setting)**	SonicWALL Email Security stores email in the Junk Box. If you click the Allow Users to Unjunk button, users can unjunk the message.	Mail is stored in Junk Box. If you click the **Allow Users To Unjunk** button users can receive the message, with the virus or likely virus removed. NOTE: SonicWALL Email Security recommends this option because you can retrieve the message after SonicWALL Email Security strips the virus.
Send To	SonicWALL Email Security sends email to a specified address field.	Option allows messages to be copied to a specific email address.
Tag with [VIRUS] or [LIKELY VIRUS]	SonicWALL Email Security delivers email to the addressee and strips the virus. The subject is tagged with [VIRUS], or [LIKELY VIRUS] or another administrator-specified term.	You can enter another tag in the text box or use the default [VIRUS] or [LIKELY VIRUS].

Click the **Allow Users to Unjunk Viruses** checkbox to allow users to view messages with viruses from Junk Box. The virus is removed before the user accesses the message. This setting allows both Viruses and Likely Viruses to be unjunked.

Click **Apply Changes**.

CHAPTER 5

Auditing

SonicWALL Email Security's Auditing module enables the user to monitor all emails, both inbound and outbound, that pass through SonicWALL Email Security. This allows the user to monitor where emails have filtered into or locate the destination of a particular email.

This chapter contains the following sections:

- "Email Auditing" on page 45
- "Searching InboundEmails" on page 45
- "Configure Auditing" on page 48

Email Auditing

The Email Auditing window can track the path of any message that passes through SonicWALL Email Security. The Email Auditing window contains a search display that the administrator uses to search inbound emails. SonicWALL now uses a search engine to search on audit and junk messages.

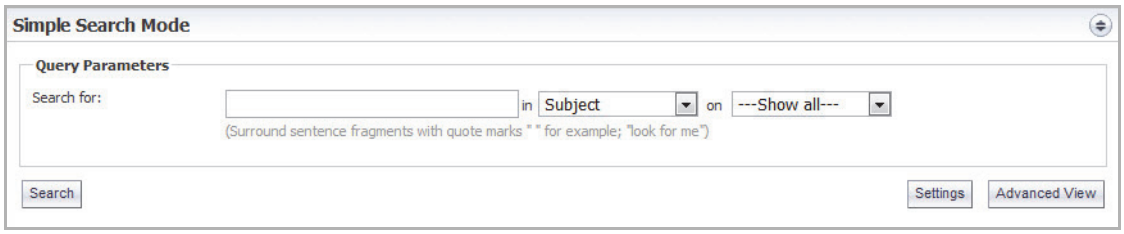
Searching InboundEmails

Inbound emails processed by SonicWALL Email Security are those that originate from outside of your organization including the total number of junk messages and good messages. Below the search section a list of emails is displayed with the following information:

- the recipient of the email
- where the email is located
- the type of threat the email is identified as
- notes about the email
- attachments from the email
- the subject heading of the email
- the sender of the email
- the timestamp of the email

Audit Simple Search

To use the Audit Simple Search Mode, follow the procedures below:

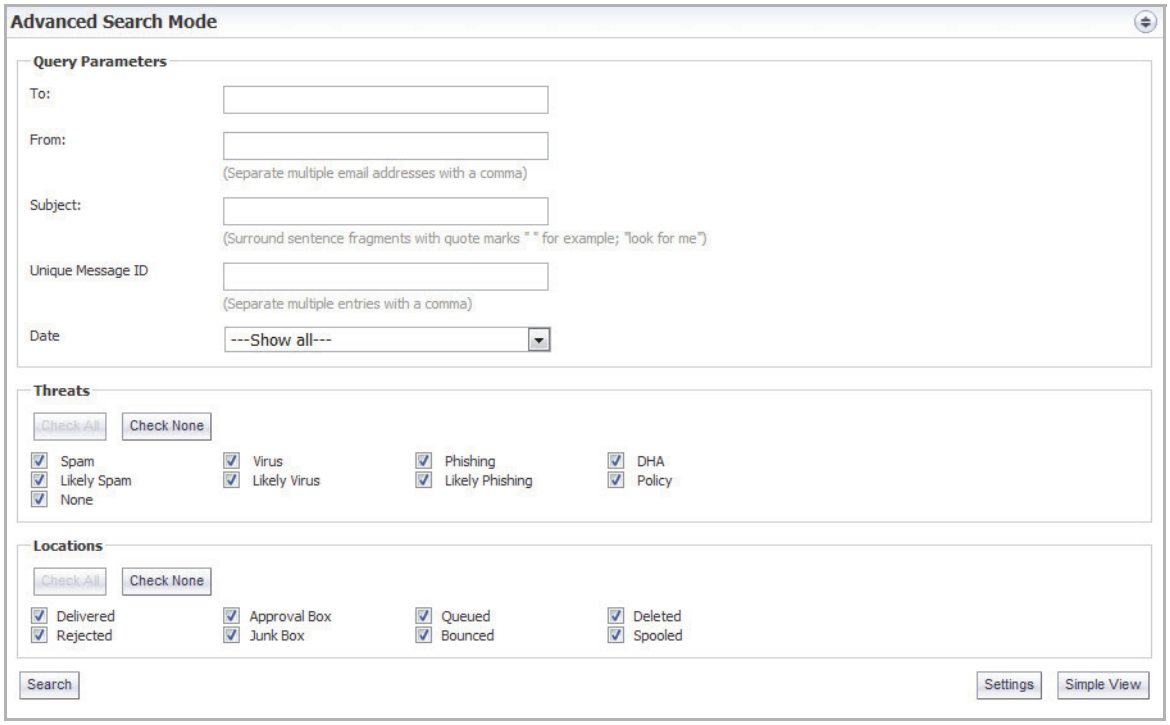


1. Search for messages by selecting specific strings from the dropdown list in the following fields: Subject, From, To, or Unique Message ID. Ensure sentence fragments are surrounded by quotation marks.
2. Select the specific date or **Show all** to search from the dropdown list.
3. Click **Search**.

Audit Advanced View

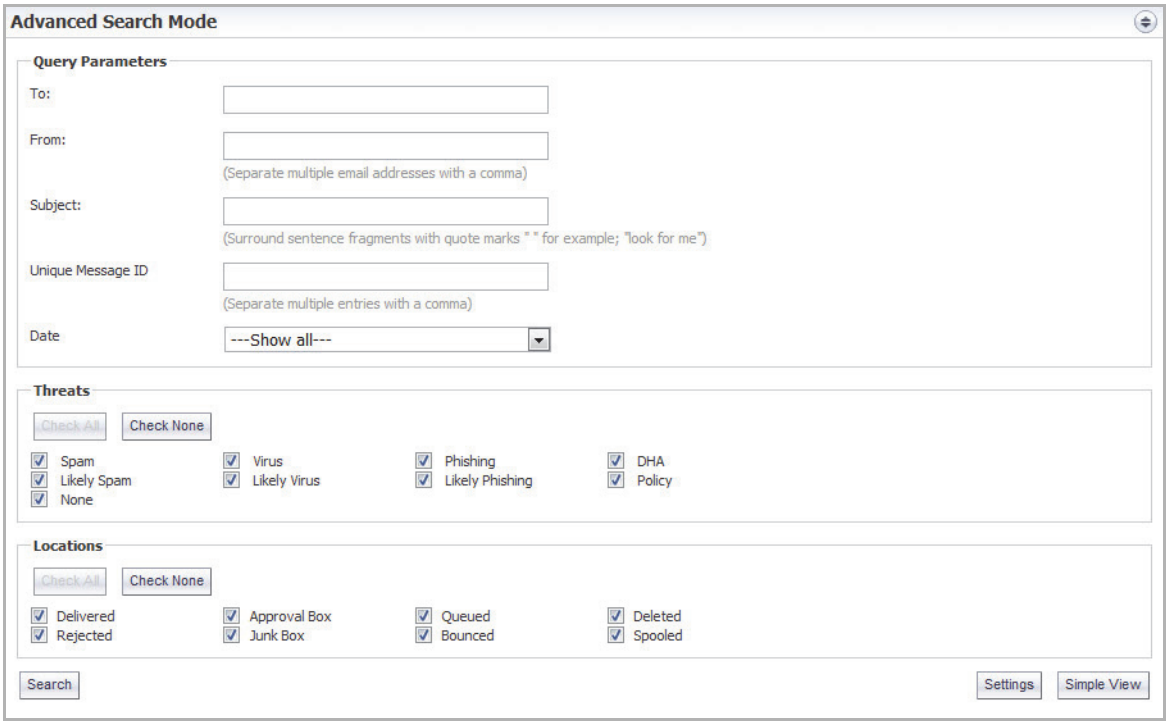
This view provides support to search on multiple fields to get the results in more granularity.

1. On the **Auditing** page, click the **Advanced View** button.



2. To search for specific email threat types or in specific mail locations, select the desired checkboxes.
3. Click **Search**.

Messages matching your search criteria are displayed. To move quickly through results pages, click in the field that says “Page 1 of 6435” and type the result page you want to view. You can also change the number of messages displayed on each page. As an example, suppose you wanted to see only messages that were Spam or Likely Spam. Clear all the checkboxes except the **Spam** and **Likely Spam** check boxes. Leave all the locations selected and click **Search**.

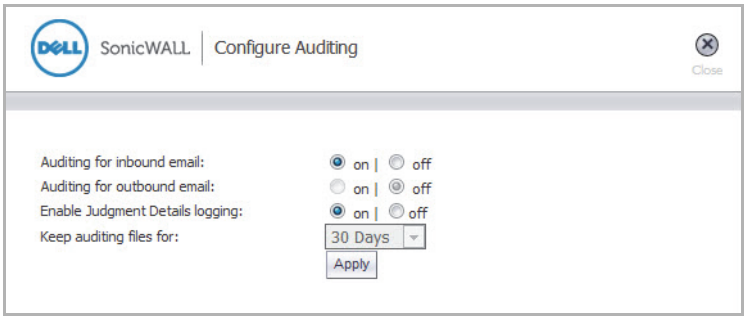


You can also **Send Copy To** or **Download** specific messages. To send a copy of specific email messages, select the checkbox next to the message, then click the **Send Copy To** button. Enter the email address, then click **Send**. To download specific messages, select the checkbox next to the message, then click the **Download** button. The message will download to your local drive.

Configure Auditing

The Configure Auditing window allows you to tailor SonicWALL Email Security to your organization's preferences for auditing emails. Configuration in this window is optional. SonicWALL Email Security sets the default in the **ON** positions with a default of 30 days for keeping auditing files. To configure Auditing:

1. From the **Auditing** page, click the **Settings** button.



2. Select the radio button(s) in the **On** position for the following:
   - Auditing for inbound email
   - Enable Judgment Details logging

The **Auditing for Outbound Email** option is automatically set to Off. Contact your Sales Representative for more information regarding upgrading your SonicWALL Email Security solution.

CHAPTER 6

Users, Groups, & Domains

The User and Group Management function allows you to manage the list of users who can log in to the SonicWALL Email Security, assign roles to individual users or groups of users, and set spam blocking options for groups users.

This chapter contains the following sections:

- "Working with Users" on page 49
- "Working with Groups" on page 53
- "Setting an LDAP Group Role" on page 55
- "Setting Junk Blocking Options for LDAP Groups" on page 56
- "Working with Domains" on page 64
- "SonicWALL Email Security Roles" on page 64

Note the following:

- To manage users and groups from within this module, you need to have configured your SonicWALL Email Security setup to synchronize with your organization's LDAP server. You can configure LDAP settings and queries on the **System > LDAP Configuration** page.
- SonicWALL Email Security queries your corporate LDAP server every hour to update users and groups. Changes made to some settings in this section may not be reflected immediately on SonicWALL Email Security, but are updated within an hour.

Working with Users

To manage users in SonicWALL Email Security, navigate to the **Users, Groups & Domains > Users** page. From this screen, you can sign in as any user, set their message management settings to corporate default, and edit their privileges in the system. Select the **Source** to use from the dropdown list, then click **Go**.

Finding All Users

If there are too many users to display in a window, you can conduct a search using the "Find all users in column" section.

1. Select from the dropdown list to do a search by **User Name** or **Primary Email**.
2. Next, select from the next dropdown list if the search parameter is **equal to**, **starts with**, or **contains**. Note that each of these fields determines the speed of the search, where equal to is the fastest type of search and contains is the slowest.
3. Select if you want the search to **Show LDAP entries** or **Show non-LDAP entries** by selecting the checkboxes next to either option.
4. Enter the search parameter in the blank field, and click **Go**.

Sort

To sort the list of users by that column, click the **User Name** or **Primary Email** heading.

Signing In as a User

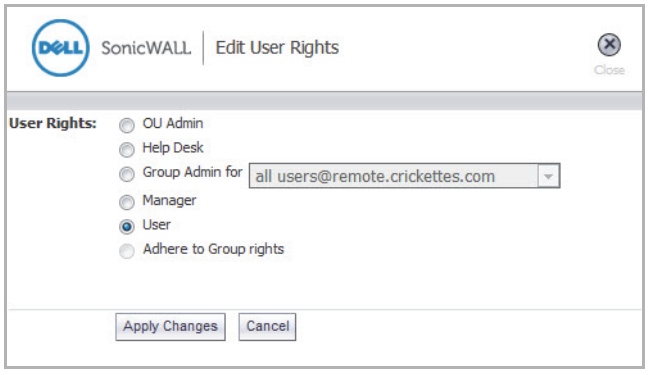
Administrators can sign in as any user, see their Junk Box, and change the settings for that user. In addition, you can sign in as a particular user to manage their delegates for them. Click the checkbox next to the User Name, then click the **Sign In as User** button.

Resetting User Message Management Setting to Default

Select one or more users and click **Set Message Management to Default** to restore all settings to the defaults. Be aware that this overrides all individual user preferences the user might have set.

Edit User Rights

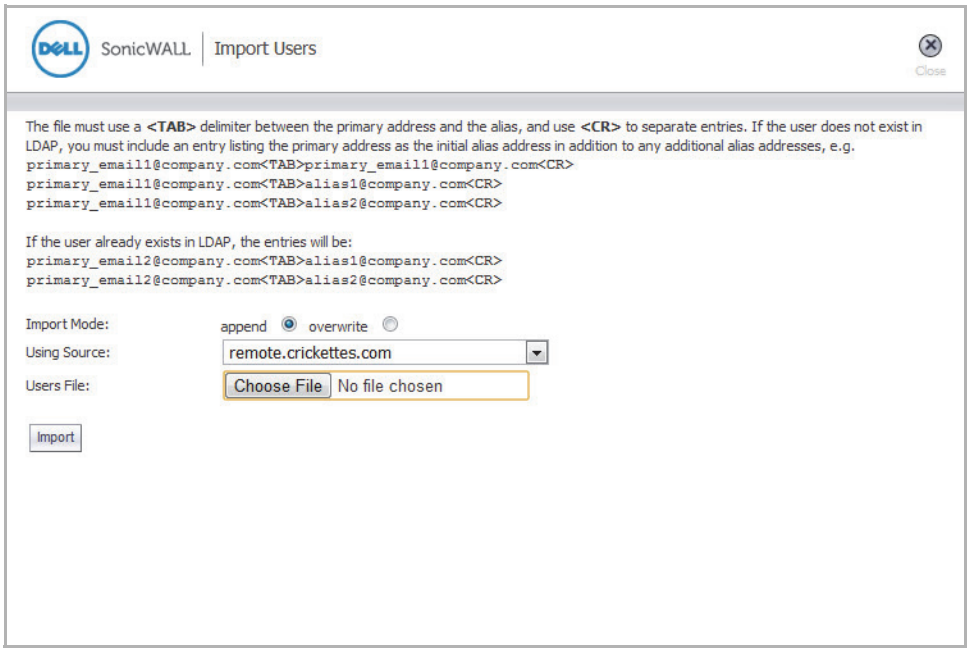
Administrators can assign different privileges to different users in the system by assigning them pre-defined roles. To assign a role to a user, select the user and click on **Edit User Rights** button. Select which rights to assign to a user, then click **Apply Changes**.



Note See “Setting an LDAP Group Role” on page 55 for more information.

Import

The administrator can add multiple non-LDAP users by importing a list of names. The list is made up of the primary addresses followed by the corresponding aliases of the users. The imported file can be appended to the existing names, or overwrite them. The format of the file is tab-delimited. One may use an Excel spreadsheet to generate a user list and save it as a tab-delimited file. To import the list, click the browse button to locate the file and click **Import**.

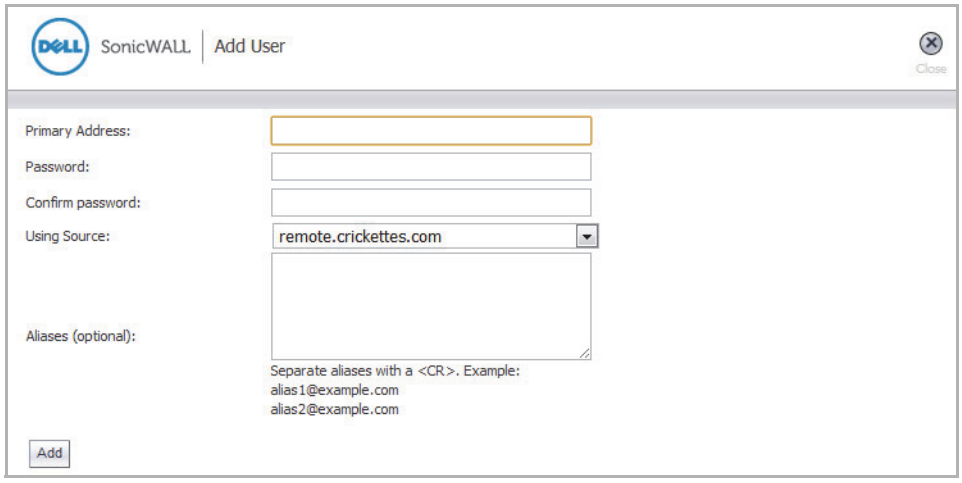


Export

The administrator can download a tab-delimited list by clicking this button. The file generated lists multiple non-LDAP users and can later be imported using the Import feature.

Adding a Non-LDAP User

The administrator can add or edit individual non-LDAP users. Click the **Add** button above the list of Users. Fill out the Primary Address, Password, and Alias fields, then click **Add**. Add an existing user with an alias and the user will have that alias added to them. This is not dependent on LDAP status.

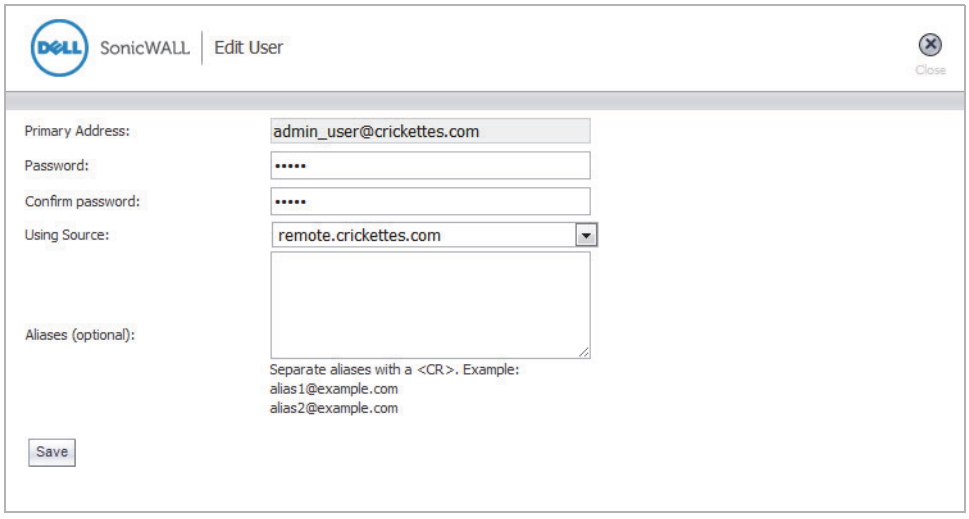


Note

Users added in this way remain non-LDAP users. Their User Rights cannot be changed. Their source will be listed as Admin. Users can edit their Junk Box setting only if the administrator sets the Junk Box setting: **Enable "Single Click" viewing of messages** to "Full Access" in the **System > Junk Box Summary** page.

Editing a Non-LDAP User

The administrator can edit individual non-LDAP users. First, select a non-LDAP user by using the checkbox in front of the name, then click the **Edit** button. The Edit User dialog box displays. Make changes to the available fields, then click **Save**.

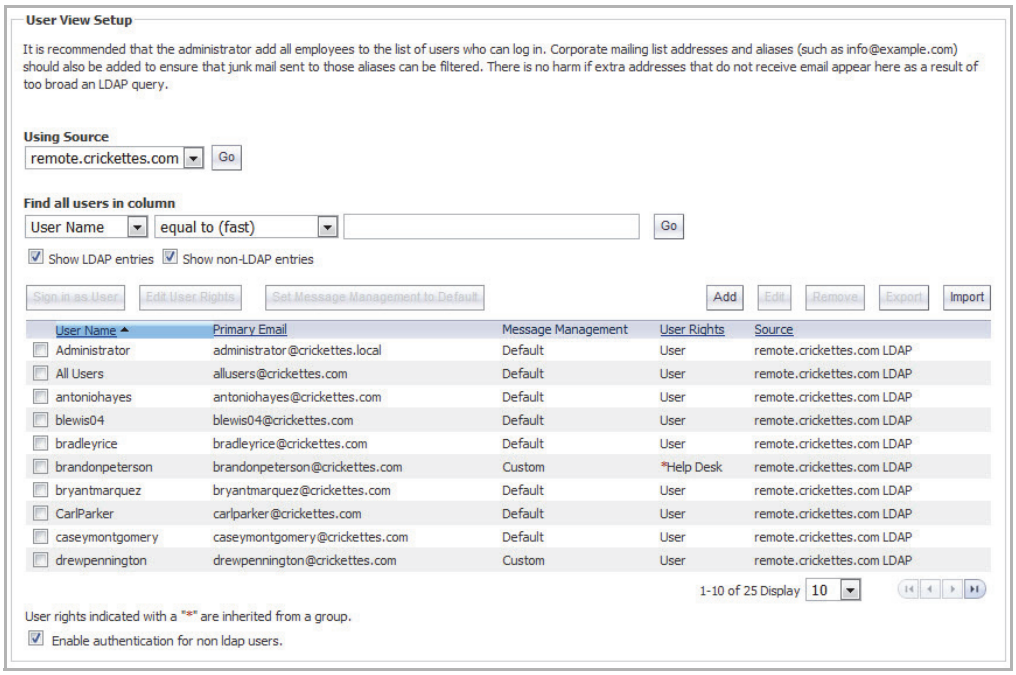


Removing a Non-LDAP User

The administrator can remove individual non-LDAP users. First, select a non-LDAP user by using the checkbox in front of the name, then click the **Remove** button to delete the name from the list.

Enabling Authentication for Non-LDAP Users

After adding non-LDAP users, navigate to the **Users, Groups & Domains > Users** page. Click the **Enable Authentication for Non-LDAP Users** checkbox towards the bottom of the screen.



Working with Groups

About LDAP Groups

This section describes how SonicWALL Email Security lets you query and configure groups of users managed by an LDAP server. Most organizations create LDAP groups on their Exchange server according to the group functions. For example, a group configured on their Exchange server called support represents the technical support groups in Exchange.

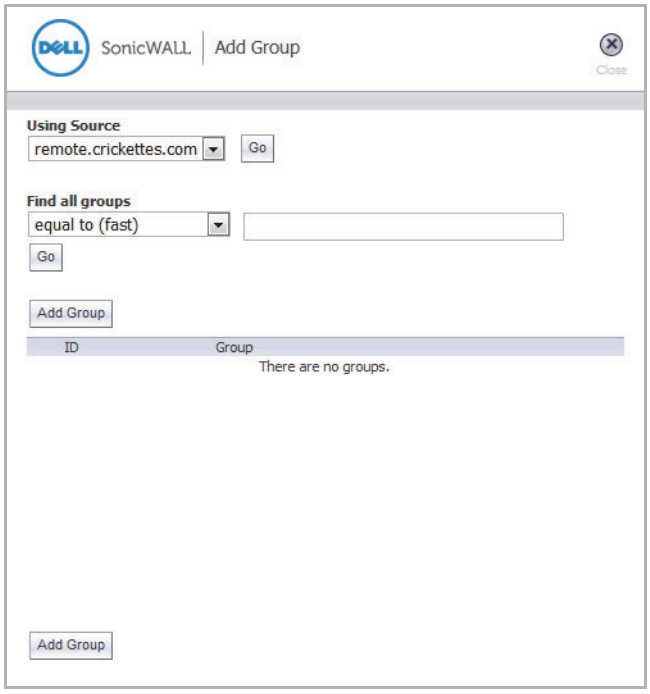
Configure LDAP groups on your corporate LDAP server before configuring the rights of users and groups on SonicWALL Email Security in the LDAP Configuration screen.

SonicWALL Email Security allows you to assign roles and set spam-blocking options for user groups. Though a user can be a member of multiple groups, SonicWALL Email Security assigns each user to the first group it finds when processing the groups. Each group can have unique settings for the aggressiveness for various spam prevention. You can configure each group to use the default settings or specify settings on a per-group basis.

Updates to groups settings in this section do not get reflected immediately. The changes will be reflected the next time SonicWALL Email Security synchronizes itself with your corporate LDAP server. If you want to force an update, click on the **Refresh Users & Groups** button.

Add a New Group

To add a new group, click the **Add New Group** button. The Add Group window appears with a list of all the groups to which you can assign roles. You can also add new groups in this window.



Finding a Group

1. From the Add Group screen, search for the group you want by entering the name in the text box. Choose the search mechanism and search speed: **equal to** (fast), **starts with** (medium), or **contains** (slow). Click **Go** to begin the search.

   OR

   Scroll through the list of groups to locate the group you want to add.
2. Click the checkbox to include the group.
3. Click **Add Group**.
   A message appears stating that the group was added successfully.

Removing a Group

1. Click the checkbox adjacent to the group(s) to remove.
2. Click the **Remove Group** button.
   A success message appears.

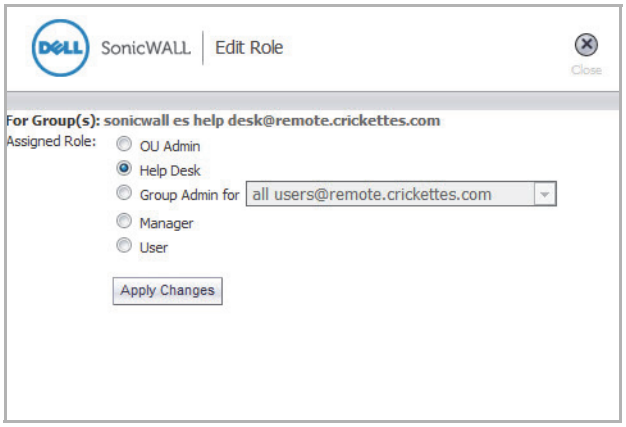
Listing Group Members

1. Click the checkbox adjacent to the group to list.
2. Click the **List Group Members** button.
   Users belonging to that group will be listed in a pop-up window.

Setting an LDAP Group Role

All members of a group are also given the role assigned to the group. To set the role of a group, follow the procedures listed below:

1. Click the checkbox adjacent to the group to edit.
2. Click **Edit Role**
   A window appears with the group's name and current role.
3. Click the radio button for the appropriate role that you want to assign to the group.
4. Click **Apply Changes**.
   A message appears stating that the group was changed successfully.



Setting Junk Blocking Options for LDAP Groups

All members of a group get the junk blocking options assigned to the group. To set spam blocking options for an LDAP group:

1. Click the checkbox adjacent to the group that you want to edit.
2. Click the **Edit Junk Blocking Options** button.
   The Junk Blocking Options for Group window appears.

Note

The **Adhere to Corporate Defaults** box is checked by default. By opening this screen, you are now editing the spam blocking options for this one group. There is an **Adhere to Corporate Defaults** checkbox at the very top of each sub-page in this dialog, this check box only applies to the values on one page and for the current group only. For example, you can adhere to the corporate defaults for the **User View Setup** and **Anti-Spam Aggressiveness** pages, but uncheck the box and set custom settings for the **Language** and **Spam Management** pages.

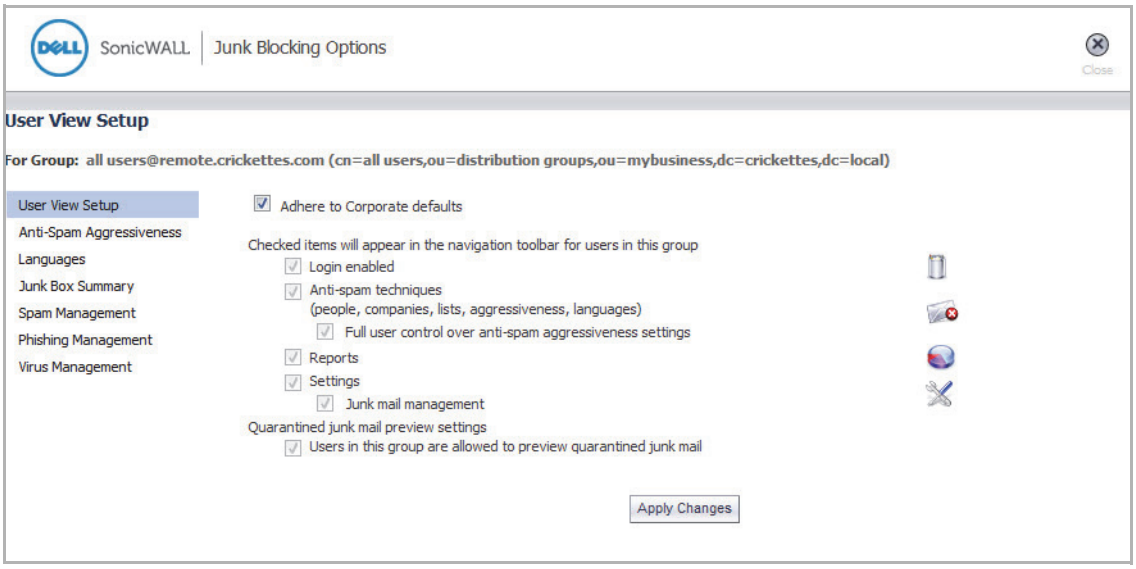
To enable the specified group to have special privileges, deselect the **Adhere to Corporate/ Group Defaults** box.

User View Setup

This controls what options are available to the users in this group when they login to server using their user name and password. You can change the settings on the following items:

- **Login Enabled**—Enables users in this group to log into their Junk Box.
- **Anti-Spam Techniques—**Allows or blocks specified people, companies, lists, aggressiveness, foreign languages.
  - **Full user control over anti-spam aggressiveness settings**—Allows users full access to configuring Anti-Spam aggressiveness settings.
- **Reports**—Allow users in this group to look at their Spam reports.
- **Settings**—Enables users in this group to view their settings.
  - **Junk mail management**—Allows users access to junk mail management settings.
- Quarantined Junk Mail Preview Settings—Click the **Users in this group are allowed to preview quarantined junk mail** checkbox to enable this setting for users.

Click **Apply Changes** to save and apply changes made to this section.

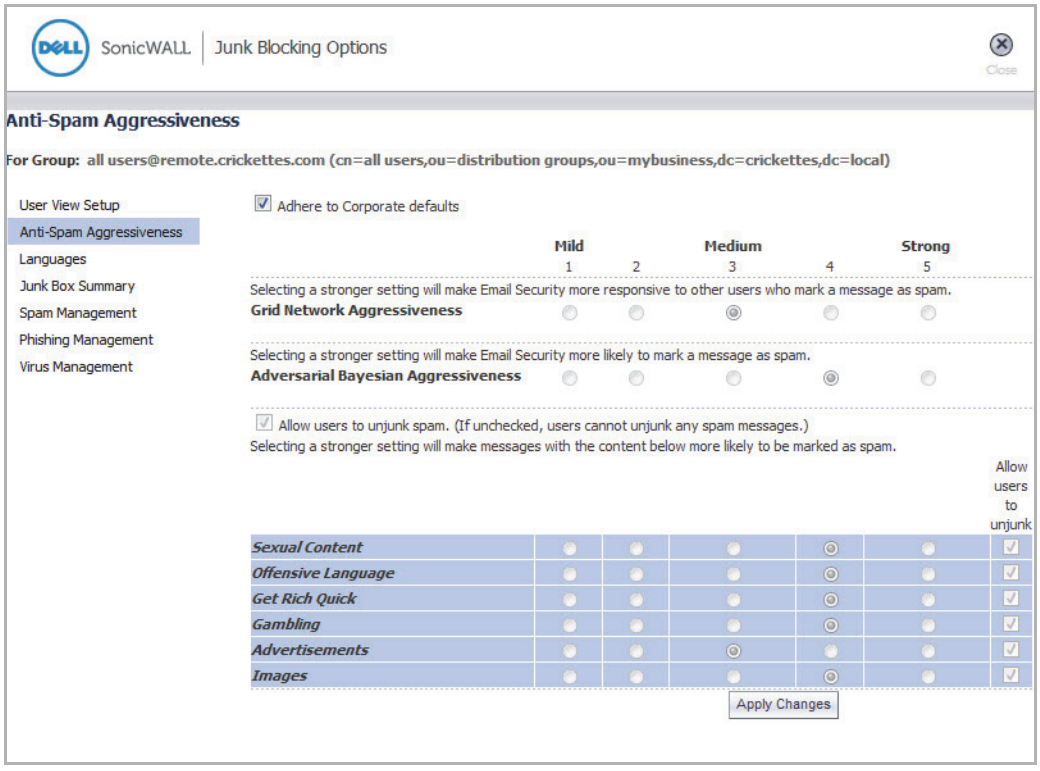


Anti-Spam Aggressiveness

You can configure Anti-Spam Aggressiveness settings for this group.

- Choose the appropriate **Grid Network Aggressiveness** level for this group. Note that selecting a stronger setting will make SonicWALL Email Security more responsive to other users who mark a message as spam.
- Choose the appropriate **Adversarial Bayesian Aggressiveness** level for this group. Note that selecting a stronger setting will make SonicWALL Email Security more likely to mark a message as spam.
- Select the checkbox to **Allow users to unjunk spam**. If the checkbox is unchecked, users are not able to unjunk spam messages.
- For each category of spam, determine level and whether members of the group are allowed to unjunk their Junk Boxes.

Click **Apply Changes** to save and apply changes made to this section.

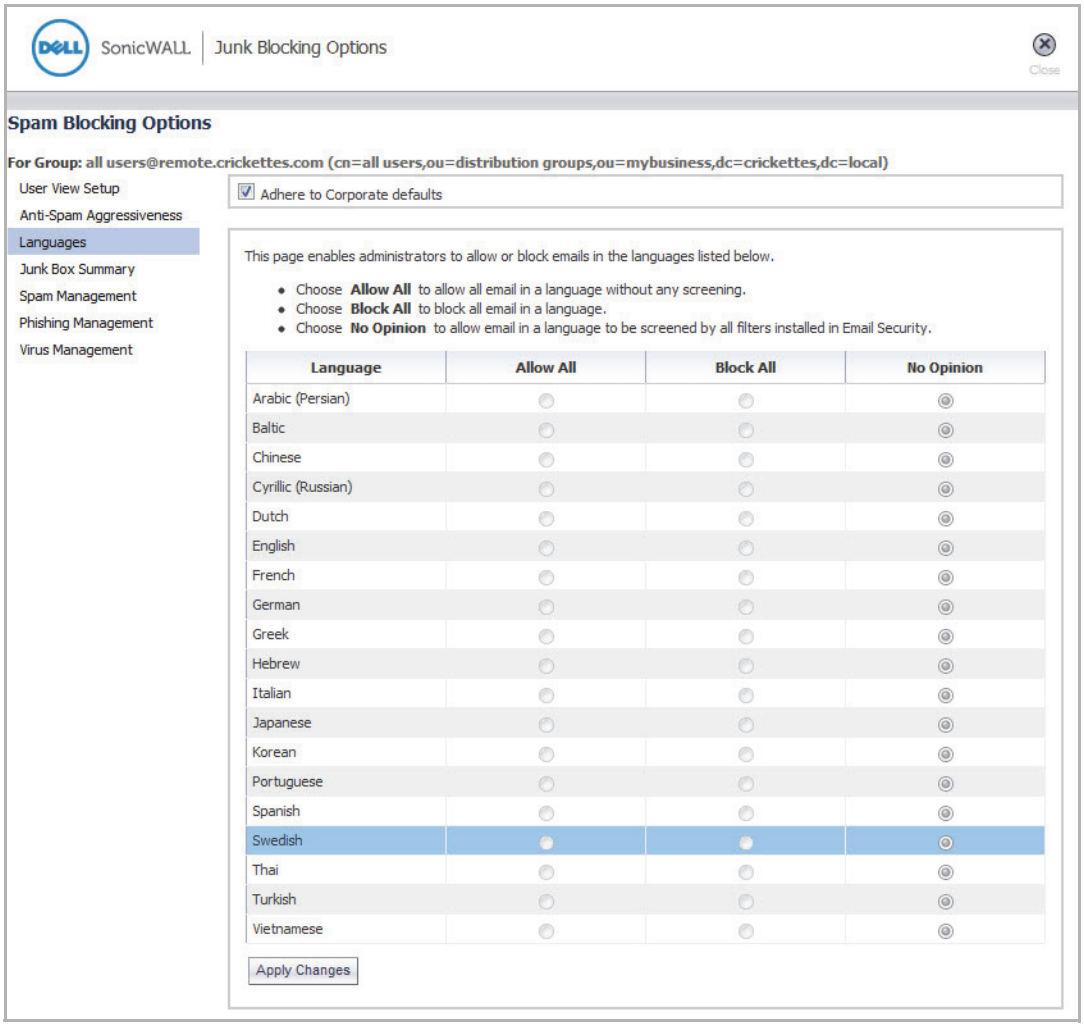


Languages

You can determine the foreign language emails that groups can receive.

- Select **Allow All** to allow all users in a group to receive email in the specified language.
- Select **Block All** to block all users in a group from receiving email in the specified language.
- Click **No opinion** to permit email to be subject to the spam and content filtering of SonicWALL Email Security.

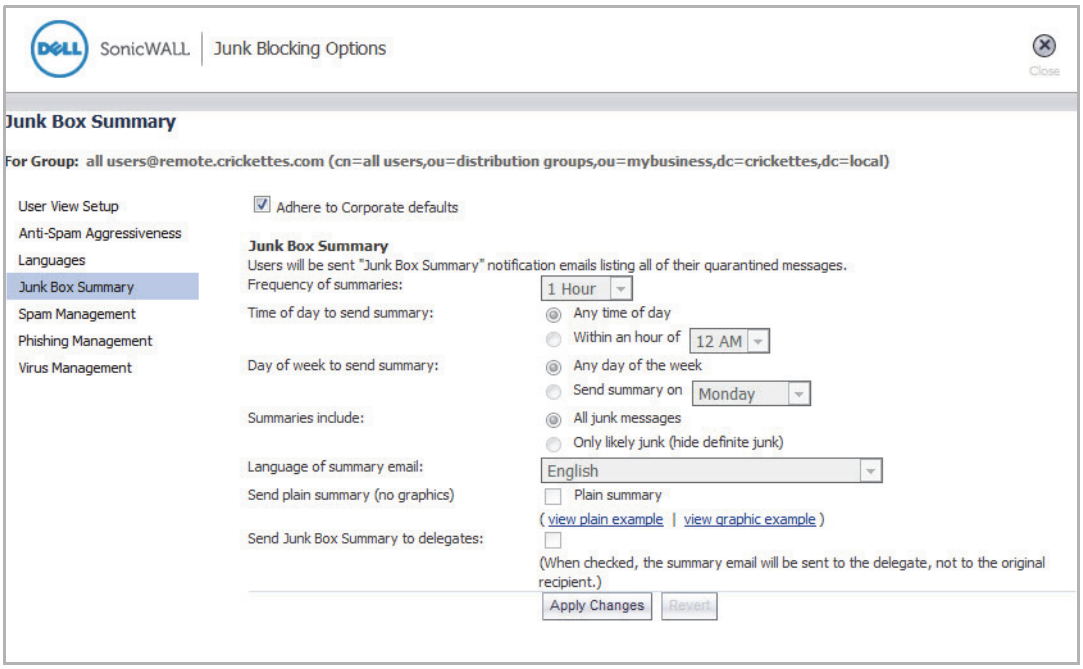
Click **Apply Changes** to save and apply changes made to this section.



Junk Box Summary

You can manage the way in which you receive the Junk Box summary of emails.

1. Select the **Frequency of Summaries** sent to users.
2. Select the **Time of Day** users receive junk summary emails.
3. Select the **Day of the Week** users receive junk summary emails.
4. Select if the Summaries include **All Junk Messages** or **Only Likely Junk**.
5. Select from the dropdown list the **Language of Summary Email**.
6. Choose to send **Plain Summary** or **Graphic Rich Summary**.
7. Select the checkbox to **Send Junk Box Summary to Delegates**. Note that when this checkbox is selected, the summary email is sent to the delegate, not to the original recipient.
8. Click **Apply Changes**.

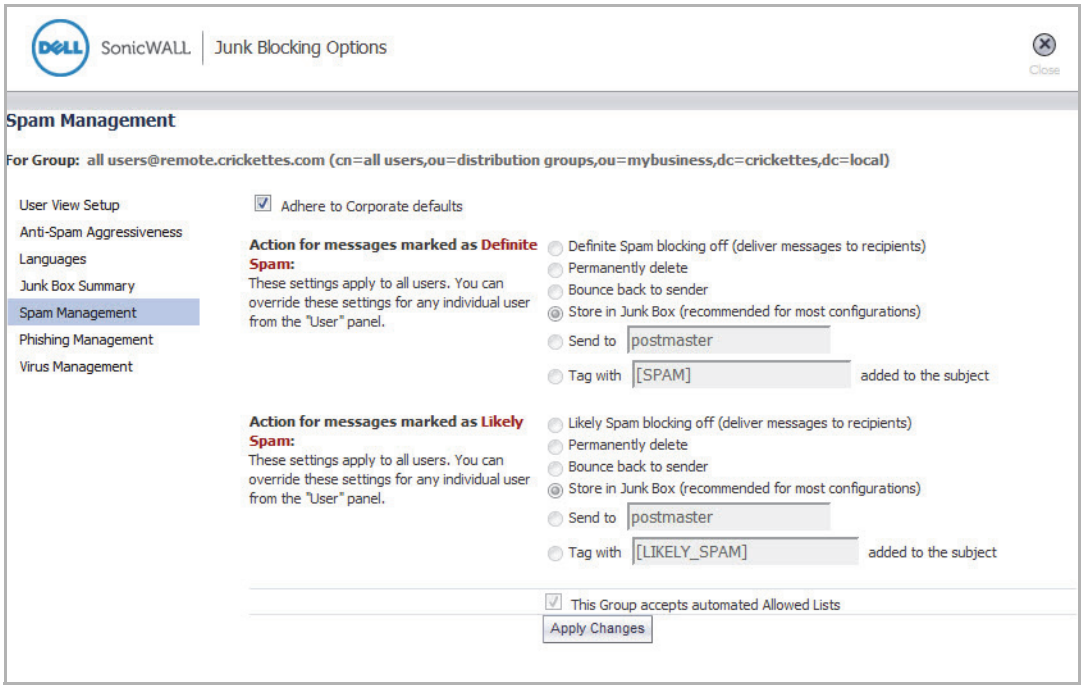


Spam Management

You can manage how groups deal with spam through the Spam Management window.

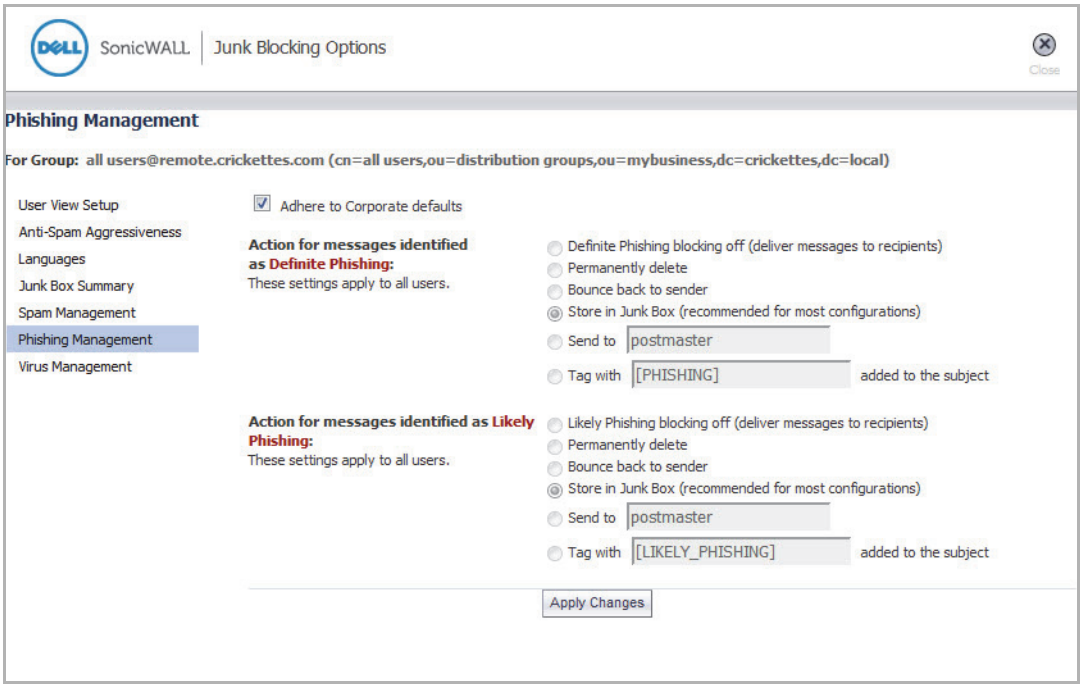
To manage messages marked as Definite Spam or Likely Spam for this group, choose what you want done with messages:

- **Spam Filtering Off**—Passes all messages to users without filtering.
- **Permanently Delete**—If determined Definite or Likely Spam, messages are permanently deleted.
- **Bounce back to sender**—Messages are sent back to the sender.
  Caution: In cases of self-replicating viruses that engage the sender's address book, this can inadvertently cause a denial-of-service to a non-malicious user.
- **Send to**—Specify an email address for the recipient.
- **Tag with**—Label the email to warn the user. The default is [SPAM] or [LIKELY_SPAM].
- Select the checkbox **This Group accepts automated Allowed Lists** if you want automated Allowed Lists to apply to this group.
- Click **Apply Changes**.



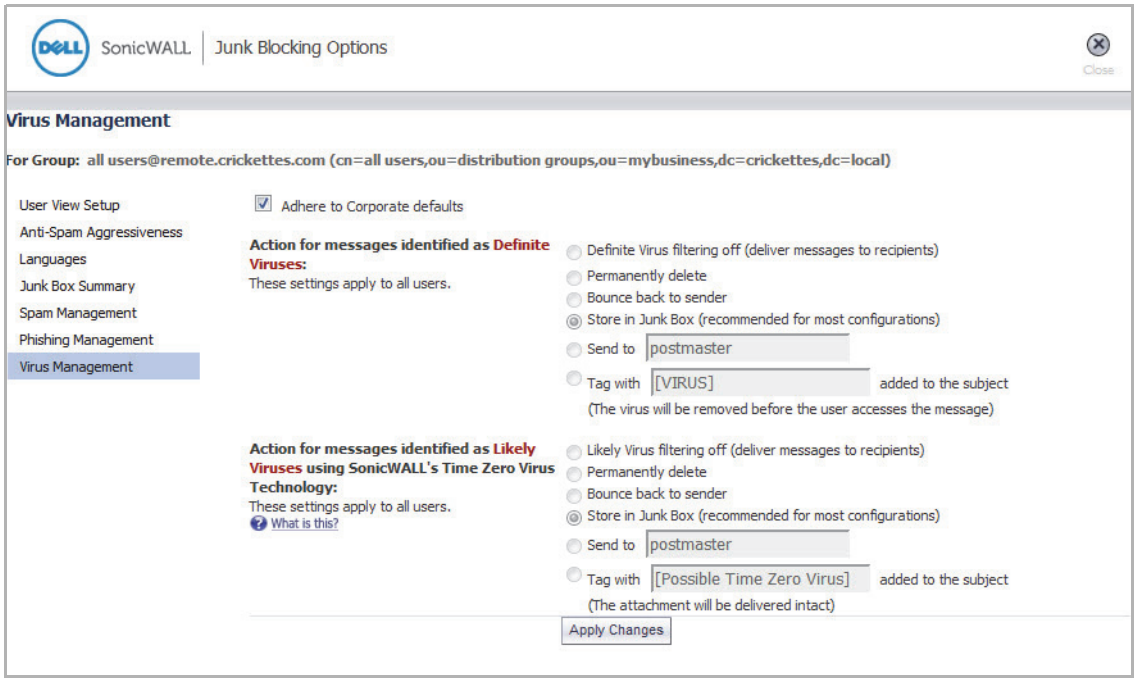
Phishing Management

The phishing management window gives you the option of managing phishing and likely phishing settings at a group level. Just like Spam Management options, it allows to you deal with phishing differently for different groups. However, unlike Spam Management options, these settings cannot be altered for individual users.



Virus Management

The virus management window gives you the option to manage Definite Virus and Likely Virus settings at a group level. Just like Spam Management options, it allows to you deal with viruses and likely viruses differently for different groups. However, unlike Spam Management options, these settings can not be altered for individual users.



Forcing All Members to Group Settings

Select the checkbox next to the Group(s) you want to adhere to Group Settings. Then, click the **Force All Members to Group Settings** button. All individual settings are overwritten by the Group Settings.

Working with Domains

The Domains page lists the available Organizational Units paired with the SonicWALL Hosted Email Security solution. To add a domain, click the **Add Domain** button and type the domains in the provided space, separating multiple domains with a comma. Then, click the **Save** button.

SonicWALL Email Security Roles

Roles are a set of privileges that you can grant any individual user or group of users in the SonicWALL Email Security. There are five defined roles that can be assigned to any user or group.

- **OU Admin**—An administrator role has full rights over the system. Administrators are taken to the system status page after logging in. They can log in as any user to change individual settings and view Junk Boxes, manage the corporate Junk Box, and configure everything.
- **Help Desk**—A Help Desk role can sign in as any user in the system, change their settings and address books, or operate on the Junk Box. This role is not allowed to change any corporate-wide settings and other server configurations.
- **Group Admin**—A group administrator role is similar to the Help Desk role except that this role's privileges are limited to users for the group they are specified to administer. Group Admin role is always associated with one or more groups added to the Spam Blocking Options for Groups section.
- **Manager**—A manager role has access to only system reports.
- **User**—Using the user role, you can allow users in your organization to log in to SonicWALL Email Security. SonicWALL Email Security displays their Junk Box as the opening window. In addition, you can also allow them access to other areas such as reports, message management, and lists.

CHAPTER 7

Junk Box

The Junk Box allows you to review and process email messages that have been flagged as spam, virus-infected, or phishing. You can unjunk or release a falsely identified message. When you or the recipient unjunks an incoming message, SonicWALL Email Security adds the sender of the message to the recipient's Allowed list and delivers the email to the recipient.

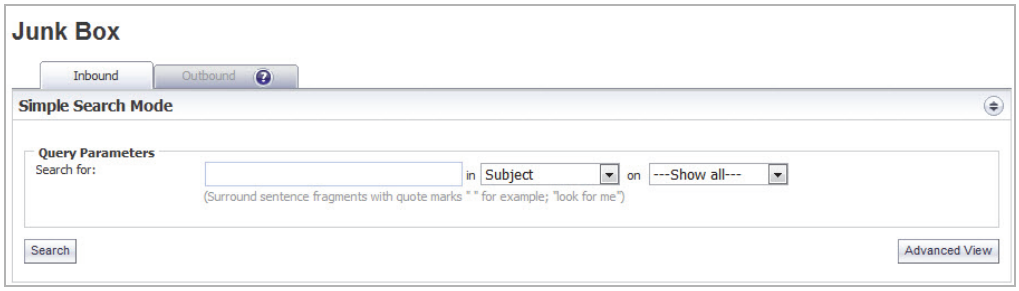
The chapter contains the following sections:

- "Junk Box—Simple View" on page 65
- "Junk Box—Advanced View" on page 66
- "Working with Junk Box Messages" on page 68
- "Managing Junk Summaries" on page 68
- "Supported Search in Audit and Junkbox" on page 69

Junk Box—Simple View

The window displays all the messages that have been categorized as the selected threats. You can also:

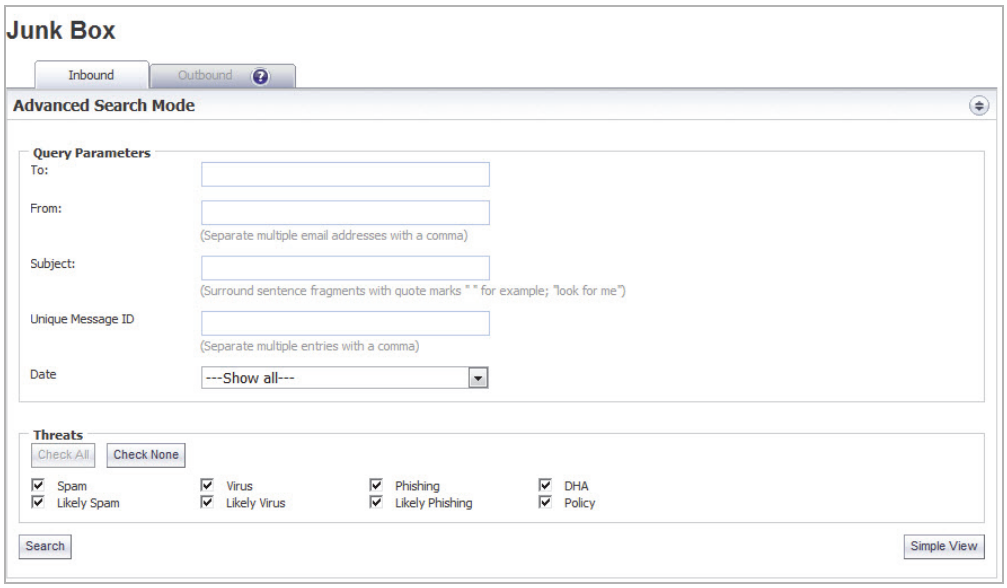
- Search for messages containing specific strings in the following fields: **Subject**, **From**, **To**, or **Unique Message ID**. Search is not case sensitive.
- Select a specific date to search on any particular date.



Junk Box—Advanced View

Additional search capabilities give administrators the ability to support users more effectively, audit more selectively, and dispose of unwanted messages with more granularity.To use Advanced Search, follow the procedures listed below:

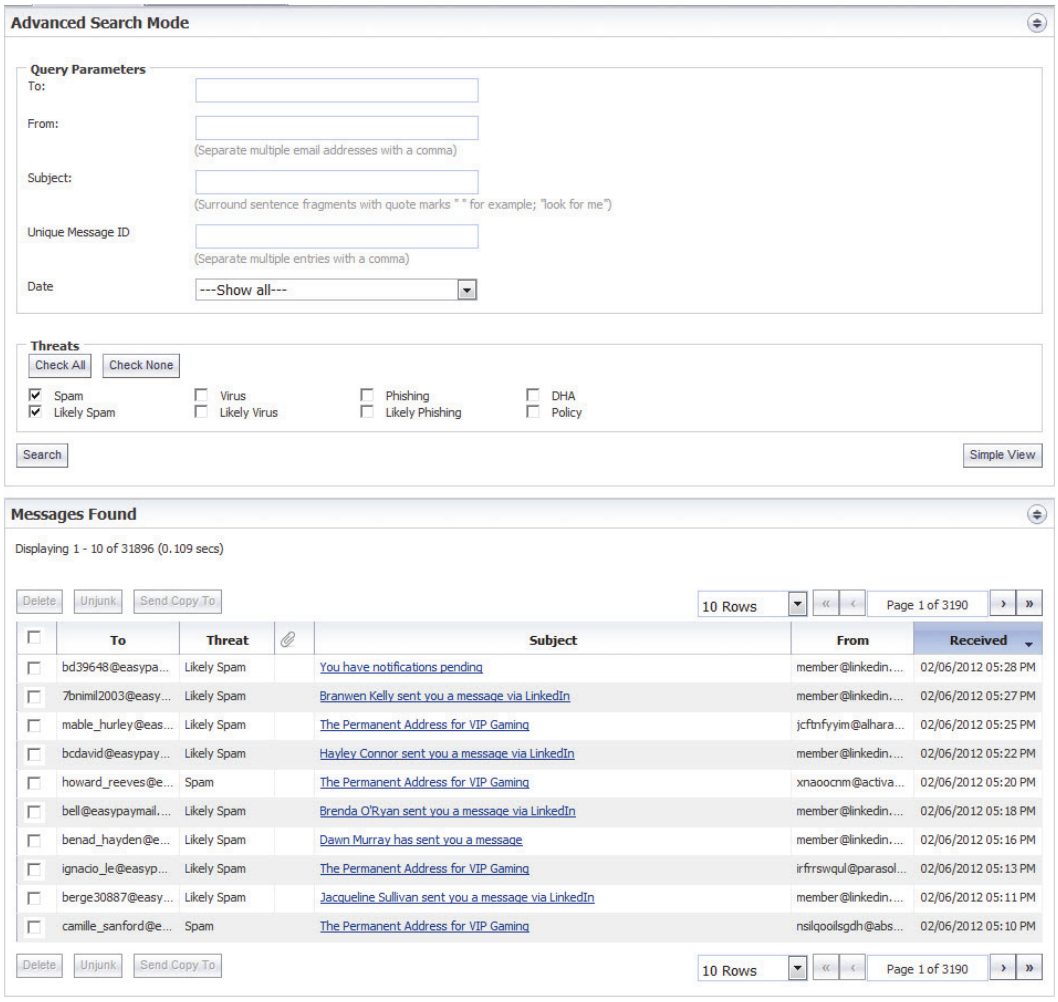
1. On the **Junkbox** page, click the **Advanced View** button.



2. To search for specific email threat types, select the checkboxes in the Threats section.
3. Click **Search**.

   Messages matching your search criteria are displayed. To move quickly through results pages, click in the field that says “Page 1 of 14” and type the result page you want to view. You can also change the number of messages displayed on each page. As an example,

suppose you wanted to see only messages that were Spam or Likely Spam. Clear all the checkboxes except the **Show *Spam** and **Show Likely Spam** check boxes. Leave all the locations selected and click **Search**.



Working with Junk Box Messages

View

To view any message, click the email link under the **Subject** field. The message appears in a new window, which displays the contents of the message.

Unjunk

This button is available only on the inbound junk box. Select **Unjunk** to forward the selected messages to the recipient and add the sender of each message to the recipient's Allowed list. Unjunking a message removes it from the Junk Box.

Send Copy To

Select **Send Copy To** to forward a copy of the messages (including attachments, if any) to the specified email address. The message will still remain in the Junk Box. This button will only be available to members of administrative group and only if they are allowed to view the messages in the Junk Box.

Delete

Deletes the selected messages. Use this option with care, as deleted emails cannot be retrieved.

Message Details

You can scroll through the messages and click the Subject field to view more information about the message in plain text. Depending on your user access set up, you might see the content of the messages. To control who is allowed to preview the content of messages, go to **System > User View Setup**.

Managing Junk Summaries

Both administrators and users receive Junk Box summaries listing the incoming email that SonicWALL Email Security has classified as junk. From these email messages, users can choose to view or unjunk an email if the administrator has configured these permissions.

From the Junk Box Summary window, users can determine the language, frequency, content, and format of Junk Box summaries. To configure Junk Box Summaries:

1. Select the timing and frequency for email summaries.
2. Select the language for Junk Box summaries from the **Language of summary email**: list.

Supported Search in Audit and Junkbox

The following types of search can be performed in the To, From, or Subject field.

Boolean Search

- **OR Operator**: This is the default search. Add **OR** in between search words. The results will contain any of these search words.
- **AND Operator**: Add '+' before the search word (or) **AND** in between search words. Each result must contain these words.
- **NOT Operator**: Add '-' before the search words (or) **NOT** in between search words. The results must not contain these search words.

Wildcard Search

- *** operator**: Add * to the middle or end of the word. This substitutes more than one character to the search word, and attempts to perform a search on all possible words.
- **? operator**: Add ? to the middle or end of the word. This substitutes one character and will find the match for the word.

Note Wildcard operators should be added to the middle or end of the text, rather than at that beginning.

Phrase Search

A phrase is a group of words surrounded by **"quotes."** The exact phrase will be searched.

Fuzzy Search

Add '**~**' to the end of the word to search for the closest possible match. This search is useful when search words have an error, or the exact spelling for the text is unknown.

Proximity Search

This searches for words closer to each other.
The syntax is **"word 1 word2"~distance**

CHAPTER 8

Reports and Monitoring

SonicWALL Email Security allows you to view system status and data through the Reports and Monitoring module. View statistics for different time periods on the local system or the mail transfer agent (MTA). Monitor the flow of email traffic passing through Email Security in real time. Use SNMP to send information to a monitoring agent.

This chapter contains the following sections:

- "Reporting in SonicWALL Email Security" on page 71
- "Overview Reports" on page 71
- "Scheduled Reports" on page 79

Reporting in SonicWALL Email Security

SonicWALL Email Security provide many types of reports. All reports allow you to optionally download the data in CSV format. You can also create custom reports by specifying a time period for the data, and download the report for analysis or email the report.

For descriptions of the different report types, see the following sections:

- "Anti-Spam Reports" on page 75
- "Anti-Phishing Reports" on page 77
- "Anti-Virus Reports" on page 78
- "Directory Protection" on page 78
- "Scheduled Reports" on page 79

Overview Reports

The following report types are available in the Overview Reports section of the Email Security management interface. See the following sections:

- "Reports Dashboard" on page 72
- "Inbound Good vs Junk" on page 73
- "Junk Email Breakdown Report" on page 74

Reports Dashboard

The **Dashboard** provides a lot of information about SonicWALL Email Security at a glance. These charts are updated hourly and display the statistics for the last 24 hours. Click the **Refresh Reports** button to update the data in the reports with the most current data.

Inbound Good Email vs Junk Email

Displays the number of Good Email messages in comparison to the Junk messages received. The Junk Email messages include spam, likely spam, phishing, likely phishing, viruses, likely viruses, Directory Harvest Attacks (DHA), and Connection Management (CM).

Spam Caught

Displays the number of email messages that are Definite Spam compared to the number of messages that are Likely Spam. The information on this chart can also be found in the **Anti-Spam Reports** > **Spam Caught** report.

Junk Email Breakdown

Displays the number of Junk messages, classified into the following categories:

- Spam (Definite Spam and Likely Spam)
- Phishing (Definite Phishing and Likely Phishing)
- Virus (Definite Virus and Likely Virus)
- Directory Harvest Attack (DHA)
- Connection Management (CM)

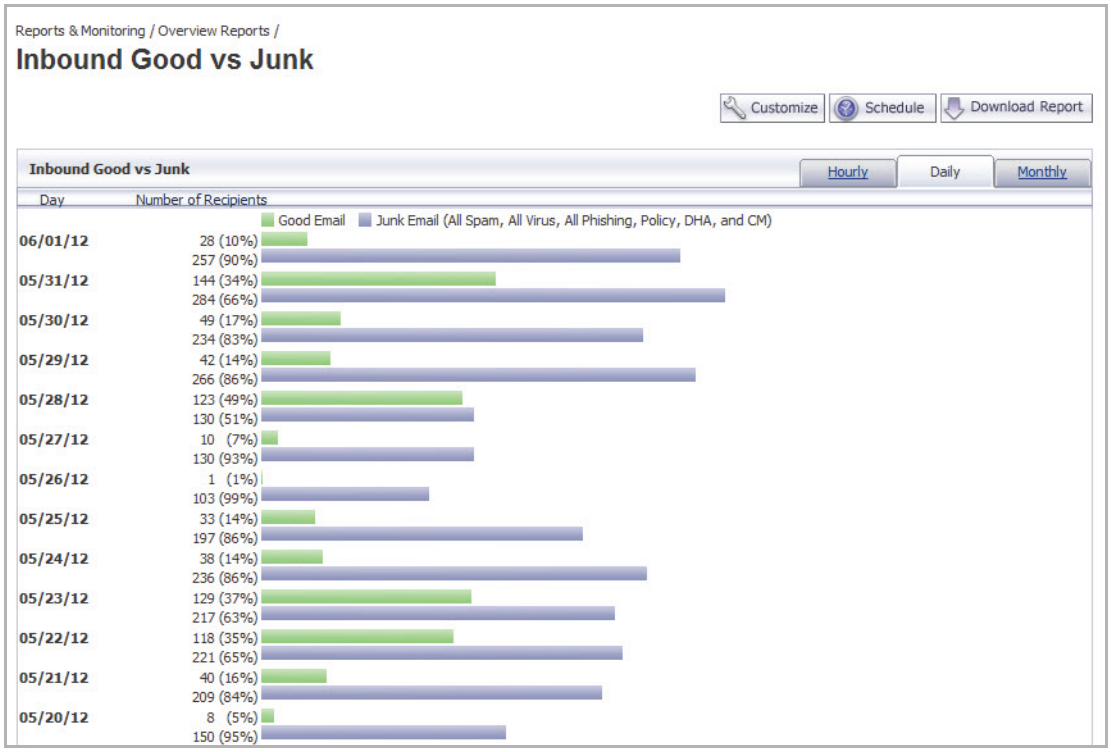
Note You can also find this information in "Junk Email Breakdown Report" on page 74.

Top Spam Recipients

Displays the volume of spam received by the top 12 recipients in your organization within the last
24 hours. This information is also available in the **Top Spam Recipients** report.

Inbound Good vs Junk

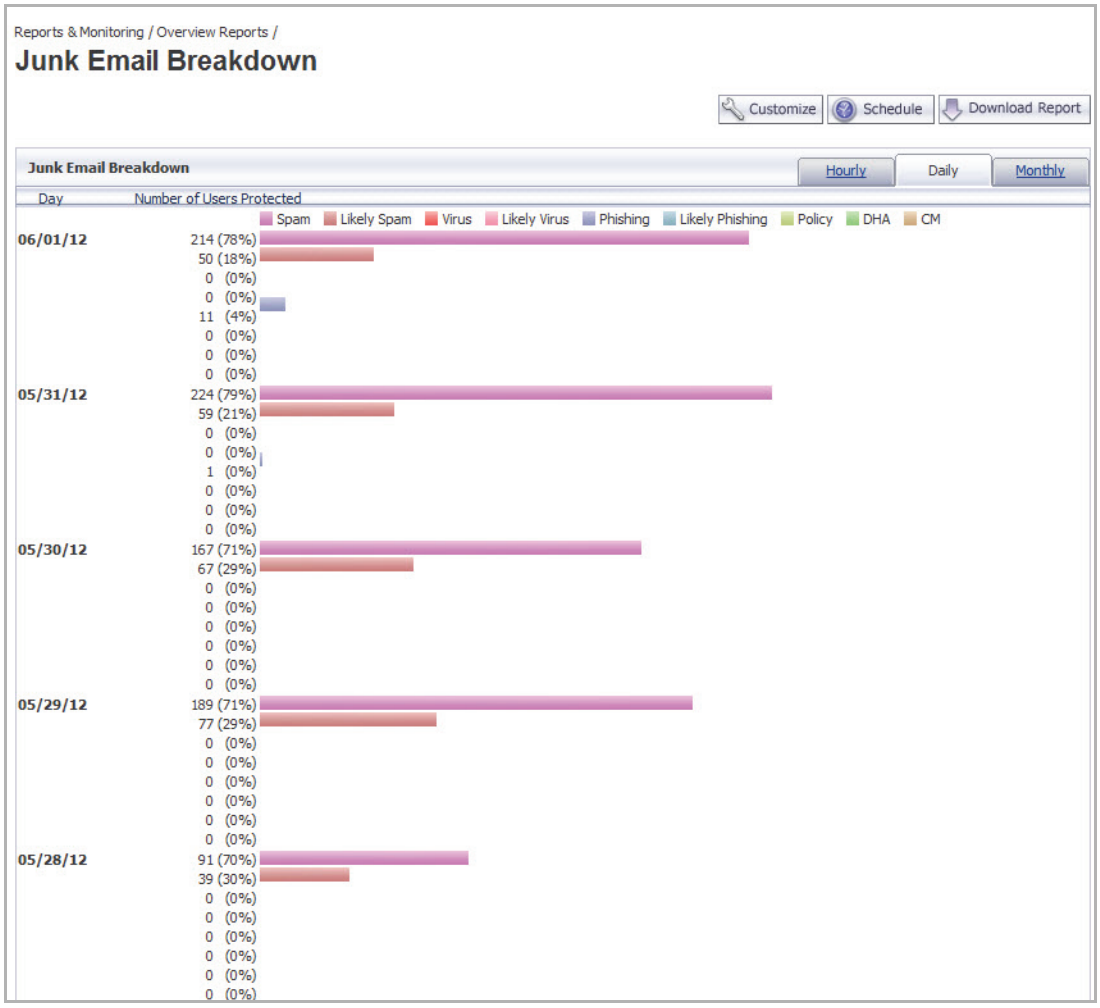
This page displays the total number of inbound messages processed by SonicWALL Email Security along with the total number of junk messages versus good messages.



You can view the Inbound Good messages versus Junk messages by specific time periods. Click the **Hourly**, **Daily**, or **Monthly** tabs to view data for each period. By default, the Daily tab displays.

Junk Email Breakdown Report

This report gives a percentage and numeric breakdown of the various categories of junk received, including Spam, Likely Spam, Viruses, Likely Viruses, Phishing, Likely Phishing, Directory Harvest Attacks (DHA), and Connection Management (CM).



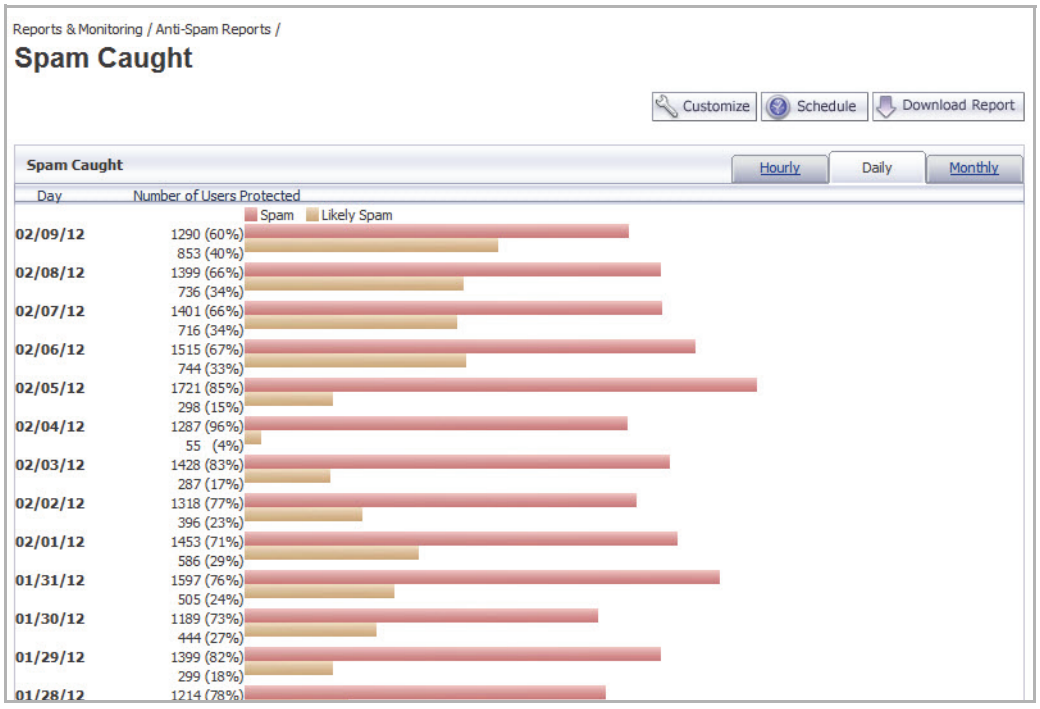
You can view the Junk Email Breakdown by specific time periods. Click the **Hourly**, **Daily**, or **Monthly** tabs to view data for each period. By default, the Daily tab displays.

Anti-Spam Reports

SonicWALL Email Security provides two reports specific to the category of Anti-Spam: Spam Caught and Top Spam Recipients.

Spam Caught

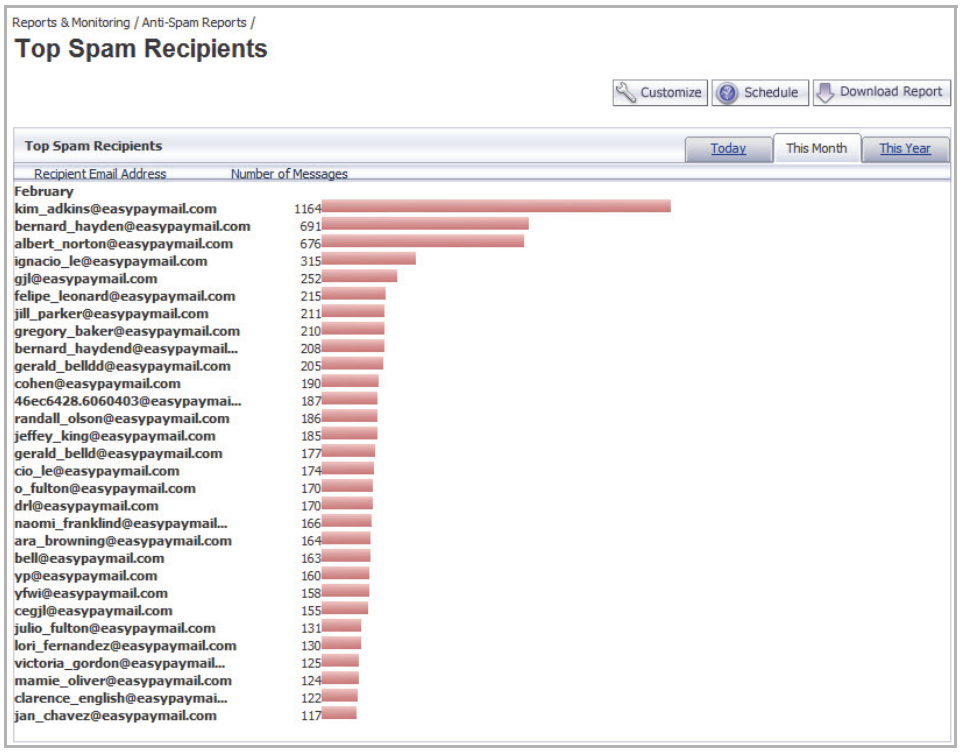
The Spam Caught report displays the number of messages filtered by SonicWALL Email Security that are definitely Spam compared to the amount that are Likely Spam. This report also gives a percentage breakdown.



You can view the Spam Caught report by specific time periods. Click the **Hourly**, **Daily**, or **Monthly** tabs to view data for each period. By default, the Daily tab displays.

Top Spam Recipients

The Top Spam Recipients report lists the email addresses in your organization that receive the most spam.



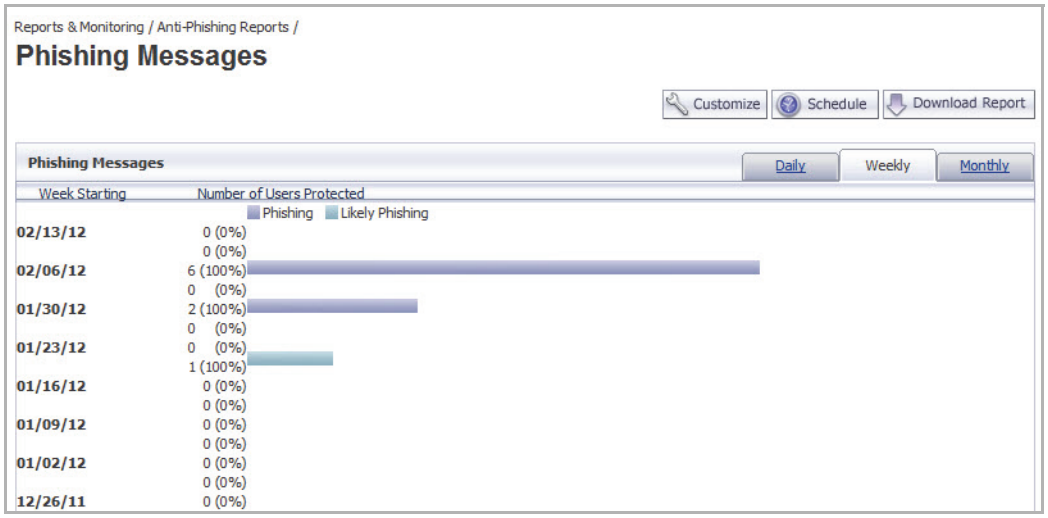
You can view the Top Spam Recipients report by specific time periods. Click the **Today**, **This Month**, or **This Year** tabs to view data for each period. By default, the **This Month** tab displays.

Anti-Phishing Reports

Phishing Messages are an especially pernicious form of fraud that use email with fraudulent content to steal consumers' personal identity data and financial account credentials.

Phishing Messages

This report displays the number of messages that were identified as Phishing Attacks and Likely Phishing Attacks.



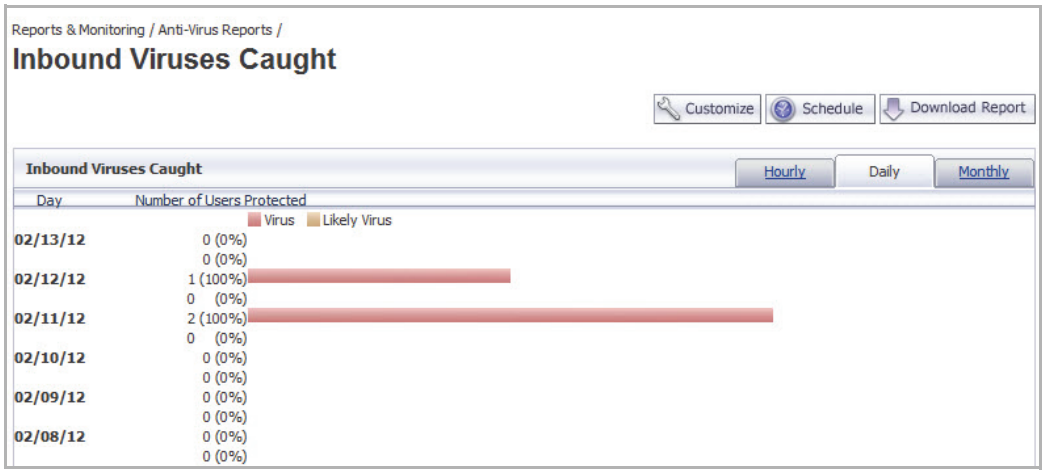
You can view the Phishing Messages by specific time periods. Click the **Daily**, **Weekly**, and **Monthly** tabs to view the data for each period. By default, the **Weekly** tab displays.

Anti-Virus Reports

The Anti-Virus Report allows you to view the number of viruses detected by the SonicWALL Email Security.

Inbound Viruses Caught

The Inbound Viruses Caught report displays the number of viruses caught in inbound email traffic.



You can view the Inbound Viruses Caught by specific time periods. Click the **Hourly**, **Daily**, or **Monthly** tabs to view the data for each period. By default, the **Daily** tab displays.

Directory Protection

SonicWALL Email Security provides protection against directory attacks. Following directory protection reports are available to give more information on the directory attacks targeted towards your organization.

Number of Directory Harvest Attacks (DHA)

This report displays the number of messages with invalid email addresses that were sent to your organization. If this number is large, your organization may be experiencing one or more Directory Harvest Attacks (DHA), in which spammers try to harvest a list of all your email addresses.

You can view the Number of DHA Attacks by specific time periods. Click the **Hourly**, **Daily**, or **Monthly** tabs to view the data for each period. By default, the **Daily** tab displays.

Scheduled Reports

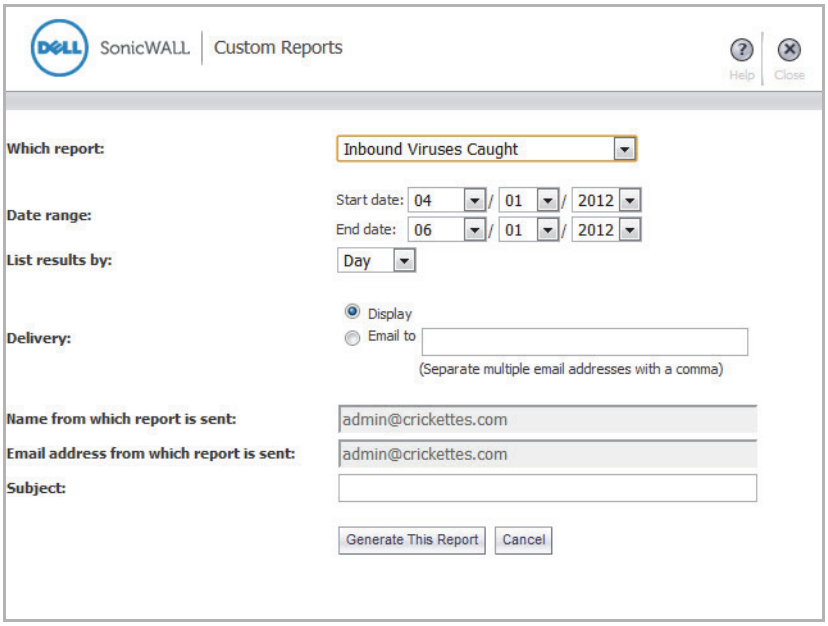
SonicWALL Email Security allows you to schedule email delivery of reports. You can choose the type of report, a time span the data covers, the list of recipients, etc.

Customize a Report

Clicking the **Customize** button on any Report screen brings up the Custom Reports dialog box. You can generate a report based on the following settings:

- **Which Report**—Select from the dropdown list the report you want to generate.
- **Date Range—**Specify the period of dates you want to report to include.
- **List Results By—**Select for the results to be listed by **Hour**, **Day**, **Week**, or **Month**.
- **Delivery**—Select if you want the report to **Display** (in a separate window) or if you want the report **Emailed To** the specified email address.
- **Subject**—Add a subject name for the report.

Enter all the specifications for a report, then click the **Generate This Report** button.



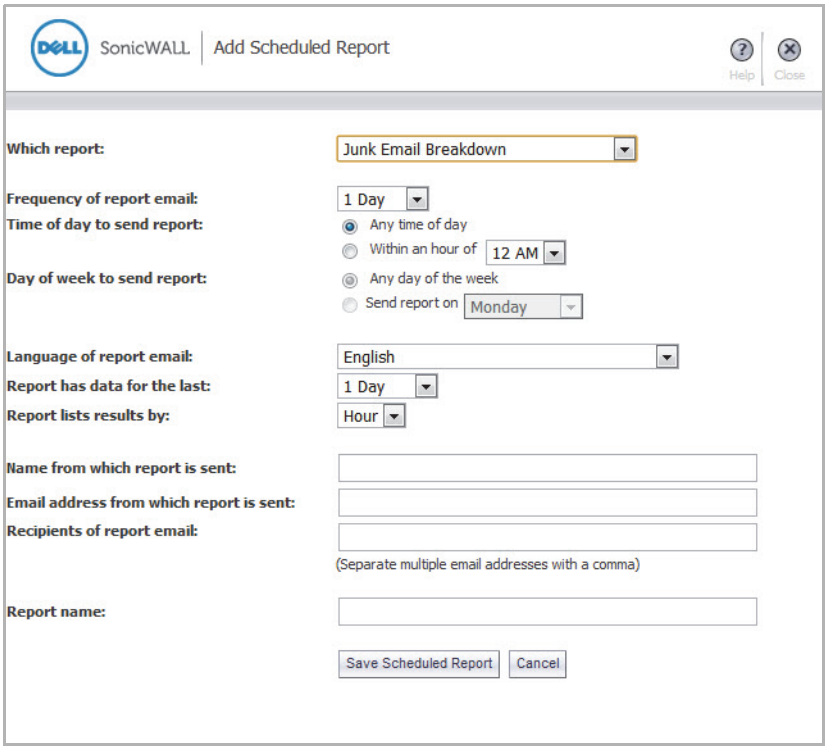
Note The Custom Reports page displays the generated report in a new window. If you have configured a popup blocker for your web browser, it may interfere with displaying the window with the data. Configure your browser to allow popup windows from your organization's SonicWALL Email Security site.

Add Scheduled Report

You can add a Scheduled Report by clicking the **Schedule** button. A dialog window displays where you can specify the following settings:

- **Which Report**—Select from the dropdown list of reports.
- **Frequency of Report Email**—Select from the dropdown list how frequent the chosen report is sent.
- **Time of Day to Send Report—**Select either to send the report at **Any time of day** or **Within an hour of** the time you specify.
- **Day of Week to Send Report—**Select either to send the report **Any day of the week** or **Send report on** the day you specify.
- **Language of Report Email—**Select the language for the report.
- **Report has Data for the Last—**Select the period of how many days to include in the report.
- **Report Lists Results By—**Select for the results to be listed by **Day**, **Week**, or **Month**.
- **Name From Which Report is Sent—**Type in the name from which the report is sent (i.e. Admin).
- **Email Address From Which Report is Sent**—Type in the email address from which the report is sent (i.e. admin@easypaymail.com).
- **Recipients of Report Email—**Type in the email address(es) of who receives the report email.
- **Report Name—**Specify the name of the report.

Click **Save Scheduled Report** when finished.



Download Report

You can instantly download the Junk Email Breakdown report to your local system. Click the **Download Report** button, then click **Open** or **Save** to view the report.

Appendix A: Warranty and Licensing

Warranty and Licensing Agreement

This appendix provides information about SonicWALL's Limited Warranty and End User Licensing Agreement.

This document contains the following sections:

- "Limited Warranty" on page 1
- "End User Licensing Agreement" on page 2

Limited Warranty

SonicWALL, Inc. warrants that commencing from the delivery date to Customer (but in any case commencing not more than ninety (90) days after the original shipment by SonicWALL), and continuing for a period of twelve (12) months, that the product will be free from defects in materials and workmanship under normal use. This Limited Warranty is not transferable and applies only to the original end user of the product. SonicWALL and its suppliers' entire liability and Customer's sole and exclusive remedy under this limited warranty will be shipment of a replacement product. At SonicWALL's discretion the replacement product may be of equal or greater functionality and may be of either new or like-new quality. SonicWALL's obligations under this warranty are contingent upon the return of the defective product according to the terms of SonicWALL's then-current Support Services policies.

This warranty does not apply if the product has been subjected to abnormal electrical stress, damaged by accident, abuse, misuse or misapplication, or has been modified without the written permission of SonicWALL.

DISCLAIMER OF WARRANTY. EXCEPT AS SPECIFIED IN THIS WARRANTY, ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS, AND WARRANTIES INCLUDING, WITHOUT LIMITATION, ANY IMPLIED WARRANTY OR CONDITION OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT, SATISFACTORY QUALITY OR ARISING FROM A COURSE OF DEALING, LAW, USAGE, OR TRADE PRACTICE, ARE HEREBY EXCLUDED TO THE MAXIMUM EXTENT ALLOWED BY APPLICABLE LAW. TO THE EXTENT AN IMPLIED WARRANTY CANNOT BE EXCLUDED, SUCH WARRANTY IS LIMITED IN DURATION TO THE WARRANTY PERIOD. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATIONS ON HOW LONG AN IMPLIED WARRANTY LASTS, THE ABOVE LIMITATION MAY NOT APPLY TO YOU. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS, AND YOU MAY ALSO HAVE OTHER RIGHTS WHICH VARY FROM JURISDICTION TO JURISDICTION. This disclaimer and exclusion shall apply even if the express warranty set forth above fails of its essential purpose.

DISCLAIMER OF LIABILITY. SONICWALL'S SOLE LIABILITY IS THE SHIPMENT OF A REPLACEMENT PRODUCT AS DESCRIBED IN THE ABOVE LIMITED WARRANTY. IN NO EVENT SHALL SONICWALL OR ITS SUPPLIERS BE LIABLE FOR ANY DAMAGES WHATSOEVER, INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION, LOSS OF INFORMATION, OR OTHER PECUNIARY LOSS ARISING OUT OF THE USE OR INABILITY TO USE THE PRODUCT, OR FOR SPECIAL, INDIRECT, CONSEQUENTIAL, INCIDENTAL, OR PUNITIVE DAMAGES HOWEVER CAUSED AND REGARDLESS OF THE THEORY OF LIABILITY ARISING OUT OF THE USE OF OR INABILITY TO USE HARDWARE OR SOFTWARE EVEN IF SONICWALL OR ITS SUPPLIERS

HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. In no event shall SonicWALL or its suppliers' liability to Customer, whether in contract, tort (including negligence), or otherwise, exceed the price paid by Customer. The foregoing limitations shall apply even if the above-stated warranty fails of its essential purpose. BECAUSE SOME STATES OR JURISDICTIONS DO NOT ALLOW LIMITATION OR EXCLUSION OF CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

End User Licensing Agreement

FOR SONICWALL HOSTED EMAIL SECURITY SERVICE

PLEASE READ THIS AGREEMENT CAREFULLY BEFORE USING THE SONICWALL HOSTED EMAIL SECURITY SERVICE (“HOSTED SERVICE”). BY USING THE HOSTED SERVICE, YOU (AS THE CUSTOMER, OR IF NOT THE CUSTOMER, AS A REPRESENTATIVE/AGENT AUTHORIZED TO BIND THE CUSTOMER) INDICATE ACCEPTANCE OF AND AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT FOR AND ON BEHALF OF THE CUSTOMER. IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT, THEN DO NOT USE THE HOSTED SERVICE. IF YOU DO PROCEED TO USE THE HOSTED SERVICE, YOU WILL HAVE INDICATED ACCEPTANCE AND AGREEMENT WITH THE TERMS AND CONDITIONS HEREIN. NOTWITHSTANDING THE FOREGOING, THIS AGREEMENT SHALL NOT SUPERSEDE ANY OTHER SIGNED AGREEMENT BETWEEN YOU AND SONICWALL THAT EXPRESSLY GOVERNS THE HOSTED SERVICE.

“Hosted Service” means the SonicWALL Hosted Email Security Service, provided by SonicWALL utilizing equipment and proprietary software managed and maintained by SonicWALL in facilities owned and/or controlled by SonicWALL. “Documentation” means the end user documentation SonicWALL makes available to end users of the Hosted Service. “Reseller” shall mean those entities to which SonicWALL or SonicWALL’s authorized distributors offer the Hosted Service for resale to end users. Except as otherwise agreed upon by the parties, this Agreement will also cover any updates and upgrades to the Hosted Service provided to Customer by SonicWALL directly or through a Reseller (except as may be otherwise indicated, such updates and upgrades shall be deemed Hosted Service). Software or hardware provided to Customer for use with the Hosted Service, if any, shall be governed by SonicWALL’s standard End User Product Agreement (http://sonicwall.com/us/end_user_product_agreement.html) and not this Agreement.

1.ACCESS AND USE OF HOSTED SERVICE

(a)License. Subject to the terms and conditions of this Agreement, SonicWALL grants to Customer, and Customer accepts from SonicWALL, a nonexclusive, non-transferable (except as otherwise set forth herein) and non-sublicensable license (“License”) to access and use the Hosted Service in accordance with its Documentation.

(b)Limitations. The License to the Hosted Service is limited to use by no more than the number of Individual Users, and only during the subscription period(s) (“Term(s)”), as sold to Customer and as indicated in the ordering and sales documentation from SonicWALL or Reseller. “Individual User” means an individual in the employ of Customer or engaged in Customer’s internal business, and who receives and sends emails through Customer’s email system(s).

(c)For Customer's Internal Business. The Hosted Service shall be used by Customer solely to manage its own internal business operations as well as the business operations of its Affiliates. Notwithstanding the foregoing, if Customer is in the regular business of providing email security management for a fee to entities that are not its Affiliates ("MSP Customers"), Customer may use the Hosted Service for its MSP Customers provided that this Agreement must be provided to MSP Customers and they must agree that their use of the Hosted Service is subject to the terms and conditions of this Agreement. Customer agrees to indemnify and hold SonicWALL harmless from and against any claims by MSP Customers against SonicWALL relating to the Hosted Service. "Affiliate" means any legal entity controlling, controlled by, or under common control with a party to this Agreement, but only for so long as such control relationship exists.

(d)Evaluation Use. If the Hosted Service is provided by SonicWALL or a Reseller at no charge for evaluation purposes, then Section 1(a) above shall not apply and instead Customer is granted a non-production License to use Hosted Service and the associated Documentation solely for Customer's own internal evaluation purposes for an evaluation period of up to thirty (30) days from the date of access to the Hosted Service, plus any extensions granted by SonicWALL in writing (the "Evaluation Period"). There is no fee for Customer's use of the Hosted Service for nonproduction evaluation purposes during the Evaluation Period. Notwithstanding anything otherwise set forth in this Agreement, Customer understands and agrees that the Hosted Service if provided for evaluation is provided "AS IS" and that SonicWALL does not provide a warranty or maintenance services for evaluation Licenses.

(e) Prohibited Uses and Restrictions. Customer shall not use the Hosted Service: (i) to infringe, misappropriate, or otherwise violate the intellectual property rights or proprietary rights, or rights of publicity or privacy, of any third party; (ii) to violate any applicable law, statute, ordinance, or regulation; (iii) to disseminate content that is harmful, threatening, abusive, harassing, tortuous, defamatory, vulgar, obscene, libelous, or otherwise objectionable; (iv) to disseminate any software viruses or any other computer code, files, or programs that may interrupt, destroy or limit the functionality of any computer software or hardware or telecommunications equipment; (v) to perform comparisons or other "benchmarking" activities, either alone or in connection with any other software or service, without SonicWALL's written permission; or publish any such performance information or comparisons; or (vi) in violation of SonicWALL's standard policies then in effect. SonicWALL may take appropriate action to prohibit any use of the Hosted Service that it believes may be (or that is alleged to be) in violation of the foregoing. Customer may not (vii) modify, translate, localize, adapt, rent, lease, loan, create or prepare derivative works of, or create a patent based on the Hosted Service or any part thereof, (viii) modify or resell the Hosted Service, or (ix) except as expressly authorized in Section 1(c) above, use the Hosted Service in any time-sharing, outsourcing, service bureau or application service provider type environment.

(f)Content. Customer shall be solely responsible for all content that Customer uploads, posts, emails, transmits, or otherwise disseminates using, or in connection with, the Hosted Service. Customer acknowledges that Customer's accessing of content using the Hosted Service is solely at Customer's own risk and that SonicWALL will not be liable for any damage to any person or entity resulting therefrom.

(g)Withholding, Storing and Accessing Withheld Mail. The Hosted Service provides for configuration settings that enable the Customer administrator, based on certain criteria, to withhold and store, deliver or delete emails that the Hosted Service judges as either spam, a phishing email, an email containing a virus or an email that is or contains some other form of malware as set forth in the Documentation. Any stored emails ("Withheld Emails") will be stored for a limited period of time as described in the then current Documentation ("Holding Period"), and thereafter will be inaccessible by the Customer. Customer acknowledges and agrees, if it desires to review, delete or mark for delivery any Withheld Email, it must do so within the Holding Period.

(h)Equipment and Security. Customer shall be solely responsible for obtaining and maintaining all applicable configuration settings as set forth in the Hosted Service documentation or SonicWALL's published policies then in effect. Customer shall be solely responsible for maintaining the security of its equipment and software, including, but not limited to, Customer's account concerning the Hosted Service passwords (including, but not limited to, administrative and other passwords).

2.OWNERSHIP

SonicWALL and its licensors are the sole and exclusive owners of the Hosted Service, and all underlying intellectual property rights therein. All rights not expressly granted to Customer are reserved by SonicWALL and its licensors.

3.TERMINATION OF HOSTED SERVICE

The License to use and access the Hosted Service hereunder shall terminate upon the end of the Term(s), and shall also terminate if Customer fails to comply with any of the provisions of this Agreement and does not remedy such breach within thirty (30) days after receiving written notice from SonicWALL. Customer agrees upon termination to immediately cease using and accessing the Hosted Service. Notwithstanding the foregoing, unless the Hosted Service is terminated due to breach by Customer, Customer may access remaining Withheld Emails during the applicable Holding Period for such Withheld Emails after the termination of the Hosted Service (as described in Section 1(g)).

4.SUPPORT SERVICES

SonicWALL's current Support Service offerings ("Support Services") and the terms and conditions applicable to such Support Services are set forth in SonicWALL's Support Services Terms located http://www.sonicwall.com/us/support/Services.html and are incorporated herein by reference. Support Services may require an additional fee. Unless otherwise agreed to in writing, SonicWALL's Support Services are subject to SonicWALL's Support Services Terms that are in effect at the time the Support Services are purchased by Customer, and these terms and conditions will be incorporated herein by reference at that time. SonicWALL reserves the right to change the Support Services Terms from time to time by posting such changes on its website, which shall apply to any Support Services purchased on or after the date of such posting.

5.SONICWALL LIMITED WARRANTY

(a)Limited Warranty. SonicWALL shall use commercially reasonable efforts to provide the Hosted Service in a manner that reasonably conforms to the Documentation. The preceding warranty will not apply if: (i) the Hosted Service is not used in accordance with this Agreement or the Documentation; (ii) the Hosted Service or any part thereof has been modified by any entity other than SonicWALL; or (iii) a malfunction in the Hosted Service has been caused by any equipment or software not supplied by SonicWALL.

(b)Disclaimer TO THE EXTENT PERMITTED BY LAW SONICWALL'S (INCLUDING ITS SUPPLIERS') SOLE AND EXCLUSIVE LIABILITY FOR ANY BREACH OF THE ABOVE WARRANTY SHALL BE LIMITED TO RE-PERFORMANCE OF THE HOSTED SERVICE, PROVIDED YOU NOTIFY SONICWALL WITHIN FIVE (5) DAYS OF ITS FAILURE TO PROVIDE THE HOSTED SERVICE, UNLESS, IN SONICWALL'S OPINION, SUCH RE-PERFORMANCE WOULD BE INADEQUATE OR IMPRACTICAL, THEN YOU WILL HAVE THE RIGHT TO TERMINATE YOUR ACCESS TO THE HOSTED SERVICE AND REQUEST A REFUND OF THE UNUSED PORTION OF THE FEES PAID BY YOU FOR THE HOSTED SERVICE.

SONICWALL DOES NOT WARRANT THAT THE PROVISION OF HOSTED SERVICE WILL BE UNINTERRUPTED OR ERROR-FREE. SONICWALL IS NOT RESPONSIBLE FOR ANY DELAYS, DELIVERY FAILURES, INTERCEPTIONS OR DATA LOSSES CAUSED BY THE HOSTED SERVICE OR TRANSFER OF DATA OVER THE INTERNET OR OTHER COMMUNICATIONS NETWORKS. THE HOSTED SERVICE MAY BE TEMPORARILY UNAVAILABLE FOR SCHEDULED MAINTENANCE OR FOR UNSCHEDULED EMERGENCY MAINTENANCE, EITHER BY SONICWALL OR BY THIRD-PARTY PROVIDERS, OR BECAUSE OF OTHER CAUSES BEYOND SONICWALL'S REASONABLE CONTROL. FURTHER, IN CONJUNCTION WITH THE HOSTED SERVICE, SONICWALL RESERVES THE RIGHT TO (I) ALLOCATE BANDWIDTH WHEN CIRCUMSTANCES WARRANT AND (II) CHANGE THE CUSTOMER'S HOSTED SERVICE TO COMPORT WITH THE RECOMMENDED USAGE.

EXCEPT FOR THE EXPRESS LIMITED WARRANTY SET FORTH ABOVE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW SONICWALL HEREBY DISCLAIMS ON BEHALF OF ITSELF, ITS SUPPLIERS, DISTRIBUTORS AND RESELLERS ALL WARRANTIES, EXPRESS, STATUTORY AND IMPLIED, APPLICABLE TO THE HOSTED SERVICE AND/OR THE SUBJECT MATTER OF THIS AGREEMENT, INCLUDING, BUT NOT LIMITED TO, ANY WARRANTY OF MERCHANTABILITY, NON-INFRINGEMENT OR FITNESS FOR A PARTICULAR PURPOSE.

6.LIMITATION OF LIABILITY

The Hosted Service is not designed, manufactured, authorized or warranted to be suitable for use in any system where a failure of such system could result in a situation that threatens the safety of human life, including without limitation any such medical, life support, aviation or nuclear applications. Any such use and subsequent liabilities that may arise from such use are totally the responsibility of Customer, and all liability of SonicWALL, whether in contract, tort (including without limitation negligence) or otherwise in relation to the same is excluded. Customer shall be responsible for mirroring its data, for backing it up frequently and regularly, and for taking all reasonable precautions to prevent data loss or corruption. SonicWALL shall not be responsible for any system downtime, loss or corruption of data or loss of production. NOTWITHSTANDING ANYTHING ELSE IN THIS AGREEMENT OR OTHERWISE, TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL SONICWALL, ITS SUPPLIERS, DISTRIBUTORS OR RESELLERS BE LIABLE FOR ANY INDIRECT, INCIDENTAL, PUNITIVE OR CONSEQUENTIAL DAMAGES, LOST OR CORRUPTED DATA, LOST PROFITS OR SAVINGS, LOSS OF BUSINESS OR OTHER ECONOMIC LOSS OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, ARISING OUT OF OR RELATED TO THIS AGREEMENT OR THE THE HOSTED SERVICE, WHETHER OR NOT BASED ON TORT, CONTRACT, STRICT LIABILITY OR ANY OTHER LEGAL THEORY AND WHETHER OR NOT SONICWALL HAS BEEN ADVISED OR KNEW OF THE POSSIBILITY OF SUCH DAMAGES. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, SONICWALL'S MAXIMUM LIABILITY TO CUSTOMER ARISING FROM OR RELATING TO THIS AGREEMENT AND THE HOSTED SERVICE SHALL BE LIMITED TO THE AMOUNTS RECEIVED BY SONICWALL FOR THE HOSTED SERVICE PROVIDED TO CUSTOMER DURING THE TWELVE (12) MONTHS PRECEDING THE CLAIM).

CUSTOMER EXPRESSLY AGREES TO THE ALLOCATION OF LIABILITY SET FORTH IN THIS SECTION, AND ACKNOWLEDGES THAT WITHOUT ITS AGREEMENT TO THESE LIMITATIONS, THE PRICES CHARGED FOR THE HOSTED SERVICE WOULD BE HIGHER.

7.GOVERNMENT RESTRICTIONS

By accepting this Agreement and receiving access to the Hosted Service, Customer confirms that it and its employees and agents who may access the Hosted Service are not listed on any governmental export exclusion lists and will not export or re-export the Hosted Service to any country embargoed by the U.S. or to any specially denied national (SDN) or denied entity identified by the U.S. Applicable export restrictions and exclusions are available at the official web site of the U.S. Department of Commerce Bureau of Industry and Security (www.bis.doc.gov). For purchase by U.S. governmental entities, the technical data and computer software in the Hosted Service are commercial technical data and commercial computer software as subject to FAR Sections 12.211, 12.212, 27.405-3 and DFARS Section 227.7202. The rights to use the Hosted Service and the underlying commercial technical data and computer software is limited to those rights customarily provided to the public purchasers as set forth in this Agreement. The Hosted Service and accompanying Documentation are deemed to be "commercial computer software" and "commercial computer software documentation," respectively, pursuant to DFAR Section 227.7202 and FAR Section 12.212, as applicable. Any use, modification, reproduction, release, performance, display or disclosure of the Hosted Service and accompanying Documentation by the United States Government shall be governed solely by the terms of this Agreement and shall be prohibited except to the extent expressly permitted by the terms of this Agreement.

8.GENERAL

(a) Governing Law and Venue. This Agreement shall be governed by and construed in accordance with the laws of the State of California, without giving effect to any conflict of laws principles that would require the application of laws of a different state. The parties agree that neither the United Nations Convention on Contracts for the International Sale of Goods, nor the Uniform Computer Information Transaction Act (UCITA) shall apply to this Agreement, regardless of the states in which the parties do business or are incorporated. Any action seeking enforcement of this Agreement or any provision hereof shall be brought exclusively in the state or federal courts located in the County of Santa Clara, State of California, United States of America. Each party hereby agrees to submit to the jurisdiction of such courts. Notwithstanding the foregoing, SonicWALL is entitled to seek immediate injunctive relief in any jurisdiction in the event of any alleged breach of Section 1 and/or to otherwise protect its intellectual property.

(b) Assignment. Except as otherwise set forth herein, Customer shall not, in whole or part, assign or transfer any part of this Agreement or any rights hereunder without the prior written consent of SonicWALL. Any attempted transfer or assignment by Customer that is not permitted by this Agreement shall be null and void. Any transfer/assignment of a License that is permitted hereunder shall require the assignment/transfer of all copies of the applicable Software along with a copy of this Agreement, the assignee must agree to all terms and conditions of this Agreement as a condition of the assignment/transfer, and the License(s) held by the transferor Customer shall terminate upon any such transfer/assignment.

(c) Severability. If any provision of this Agreement shall be held by a court of competent jurisdiction to be contrary to law, such provision will be enforced to the maximum extent permissible and the remaining provisions of this Agreement will remain in full force and effect.

(d) Privacy Policy. Customer hereby acknowledges and agrees that SonicWALL's performance of this Agreement may require SonicWALL to process or store personal data of Customer, its employees and Affiliates, and to transmit such data within SonicWALL or to SonicWALL Affiliates, partners and/or agents. Such processing, storage, and transmission may be used for the purpose of enabling SonicWALL to perform its obligations under this Agreement, and as described in SonicWALL's Privacy Policy (www.SonicWALL.com/us/Privacy_Policy.html, "Privacy Policy") and may take place in any of the countries in which SonicWALL and its Affiliates conduct business. SonicWALL reserves the right to change the Privacy Policy from time to time as described in the Privacy Policy.

(e)Confidential Information. SonicWALL recognizes that it may store and/or process data that constitutes confidential information of Customer. SonicWALL agrees to store and process such information with reasonable security standards similar to what it uses to protect its own confidential information, and to use such confidential information only to the extent necessary to perform its obligations under this Agreement.

(f) Notices. All notices provided hereunder shall be in writing, delivered personally, or sent by internationally recognized express courier service (e.g., Federal Express), addressed to the legal department of the respective party or to such other address as may be specified in writing by either of the parties to the other in accordance with this Section.

(g) Disclosure of Customer Status. SonicWALL may include Customer in its listing of customers and, upon written consent by Customer, announce Customer's selection of SonicWALL in its marketing communications.

(h) Waiver. Performance of any obligation required by a party hereunder may be waived only by a written waiver signed by an authorized representative of the other party, which waiver shall be effective only with respect to the specific obligation described therein. Any waiver or failure to enforce any provision of this Agreement on one occasion will not be deemed a waiver of any other provision or of such provision on any other occasion.

(i) Force Majeure. Each party will be excused from performance for any period during which, and to the extent that, it is prevented from performing any obligation or service as a result of causes beyond its reasonable control, and without its fault or negligence, including without limitation, acts of God, strikes, lockouts, riots, acts of war, epidemics, communication line failures, and power failures.

(j) Audit. Customer shall maintain accurate records to verify compliance with this Agreement. Upon request by SonicWALL, Customer shall furnish (a copy of) such records to SonicWALL and certify its compliance with this Agreement.

(k) Headings. Headings in this Agreement are for convenience only and do not affect the meaning or interpretation of this Agreement. This Agreement will not be construed either in favor of or against one party or the other, but rather in accordance with its fair meaning. When the term "including" is used in this Agreement it will be construed in each case to mean "including, but not limited to."

(l) Entire Agreement. This Agreement is intended by the parties as a final expression of their agreement with respect to the subject matter hereof and may not be contradicted by evidence of any prior or contemporaneous agreement unless such agreement is signed by both parties. In the absence of such an agreement, this Agreement shall constitute the complete and exclusive statement of the terms and conditions and no extrinsic evidence whatsoever may be introduced in any judicial proceeding that may involve the Agreement. This Agreement represents the complete agreement and understanding of the parties with respect to the subject matter herein. This Agreement may be modified only through a written instrument signed by both parties.