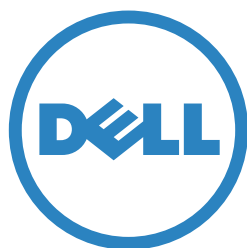


Hosted Email Security 2.0 Administrator's Guide



SonicWALL

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.

© 2013 Dell, Inc.

Trademarks: Dell™, the DELL logo, SonicWALL™, SonicWALL Hosted Email Security, SonicWALL Email Security, MySonicWALL™, Reassembly-Free Deep Packet Inspection™, Dynamic Security for the Global Network™, SonicWALL Global Response Intelligent Defense (GRID) Network™, and all other SonicWALL product and service names and slogans are trademarks of Dell, Inc.

Microsoft Windows, Internet Explorer, and Active Directory are trademarks or registered trademarks of Microsoft Corporation.

Other product and company names mentioned herein may be trademarks and/or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

2013 – 04 P/N 232-001493-00 Rev. A

Chapter 1 Pre-Configuration Tasks	7
Introduction	7
Initial Configuration	7
Activating the Hosted Email Security Service	8
Logging In	9
Chapter 2 System	11
Introduction	11
License Management	11
Available Services	11
License Table	12
License Keys	12
Administration	13
Invalid Login Policy	13
Network Architecture	14
Server Configuration	14
Spooling	17
LDAP Configuration	18
Configuring LDAP	18
LDAP Query Panel	19
Add LDAP Mappings	20
User View Setup	22
Monitoring	23
Viewing Alerts	24
Chapter 3 Anti-Spam Anti-Phishing Techniques	25
Hosted Email Security and Mail Threats	25
Managing Spam	25
Spam Identification	26
Default Spam Management	27
Address Books	29
Import Address Book	31
Anti-Spam Aggressiveness	32
Configuring GRID Network Aggressiveness	32
Configuring Adversarial Bayesian Aggressiveness Settings	32
Determining Amounts and Flavors of Spam	33
Languages	33
Miscategorized Email Messages	33
Anti-Phishing	34
What is Enterprise Phishing?	34
Preventing Phishing	34
Configuring Phishing Protection	35
Use SonicWALL Email Security's Community to Alert Others	36
Report Phishing and Other Enterprise Fraud to SonicWALL Email Security	36

Domain Keys Identified Mail (DKIM)	36
Chapter 4 Anti-Virus Techniques	39
How Virus Checking Works	39
Configuring Anti-Virus Protection.....	40
Zombie and Spyware Protection	42
CHAPTER 5 Auditing	43
Email Auditing	43
Searching Inbound & Outbound Emails.....	43
Audit Simple Search	44
Audit Advanced View.....	44
Configure Auditing.....	46
Chapter 6 Policy Management	47
Hosted Email Security and Mail Threats	47
Basic Concepts for Policy Management	47
Adding Filters.....	48
Managing Filters	50
Editing a Filter	50
Deleting a Filter	50
Changing Filter Order	50
Chapter 7 Users, Groups, & Domains	51
Working with Users	51
Finding All Users	51
Sort	52
Signing In as a User.....	52
Resetting User Message Management Setting to Default.....	52
Edit User Rights.....	52
Import.....	53
Export.....	53
Adding a Non-LDAP User	54
Editing a Non-LDAP User	54
Removing a Non-LDAP User.....	55
Enabling Authentication for Non-LDAP Users	55
Working with Groups	56
About LDAP Groups	56
Add a New Group	56
Finding a Group.....	57
Removing a Group.....	57
Listing Group Members	57
Setting an LDAP Group Role.....	57
Setting Junk Blocking Options for LDAP Groups.....	58
User View Setup	59

Anti-Spam Aggressiveness	60
Languages	61
Junk Box Summary	62
Spam Management	63
Phishing Management	64
Virus Management	65
Forcing All Members to Group Settings	65
Working with Domains	66
Roles	66
Chapter 8 Junk Box Management 67	
Junk Box—Simple View	67
Junk Box—Advanced View	68
Working with Junk Box Messages	70
View	70
Unjunk	70
Junk Box Summary	71
Managing Junk Summaries	73
Supported Search in Audit and Junkbox	73
Junk Box Settings	74
General Settings	74
Action Settings	75
Miscellaneous Settings	75
Chapter 9 Reports and Monitoring 77	
Reporting in Hosted Email Security	77
Overview Reports	77
Reports Dashboard	78
Inbound Good vs Junk	79
Outbound Good vs Junk	80
Junk Email Breakdown Report	81
Top Outbound Email Senders	82
Anti-Spam Reports	82
Spam Caught	82
Top Spam Recipients	83
Anti-Phishing Reports	84
Phishing Messages	84
Anti-Virus Reports	85
Inbound Viruses Caught	85
Directory Protection	85
Number of Directory Harvest Attacks (DHA)	85
Scheduled Reports	86
Customize a Report	86

Add Scheduled Report.....87
Download Report.....88
Appendix A Warranty and Licensing 1
Warranty and Licensing Agreement1
Limited Warranty1
End User Licensing Agreement.....2

Chapter 1

Pre-Configuration Tasks

Introduction

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

Activating the Hosted Email Security Service

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

The screenshot shows a web form titled "Activate Hosted Email Security". At the top, it states "Fields marked with * are mandatory." and "Your order has been completed successfully." The form contains the following fields and options:

- Domain Name: * Ex. SonicWALL.com
- Inbound Mail Server Host/IP Address: *
- Outbound Mail Server Host/IP Address:
- Email Address/Login:
- Password: * Your Password should be 6 to 30 characters.
- Re-enter Password: *
- Data Center Location: North America Europe

A red asterisk note below the radio buttons states: "* Please select Data Center, once selected can not be changed." At the bottom right of the form is a button labeled "Activate Services".

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

- **Domain Name**—The primary domain name that is associated with your Dell SonicWALL Hosted Email Security solution.
- **Inbound Mail Server Host / IP Address**—The IP address of the mail server hosting your user mailbox(es) for inbound messages.
- **Outbound Mail Server Host / IP Address**—The IP address provided during the provisioning stage of your Hosted Email Security solution. For example, if you registered the domain name *soniclab.us.snwlhosted.com*, then the Outbound Mail Server Host will be *soniclab.outbound.snwlhosted.com*.
- **Email Address / Login**—The email address or login name associated with your Dell SonicWALL Hosted Email Security account.
- **Password**—The password associated with your Dell SonicWALL Hosted Email Security account.
- **Re-enter Password**—The password you entered in the previous field.
- **Data Center Location**—Select the location of your Data Center. You are not able to change this option once it has been specified.

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 for inbound email messages.

Mail eXchange (MX) records specify the delivery route for email messages sent to your newly specified Dell 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.

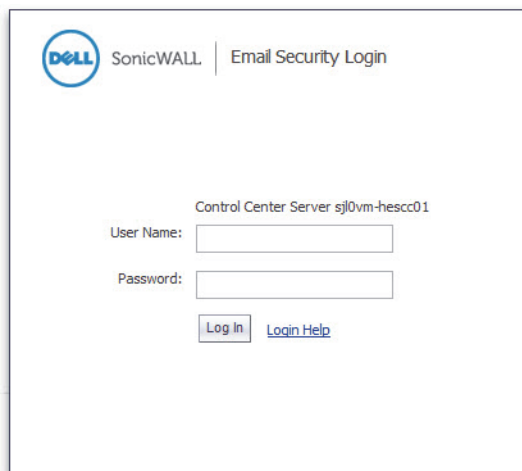
For example, a customer wishes to activate the domain name *jumbo.com*. Since the SonicWALL Data Center hosts *snwlhosted.com*, the domain then becomes *jumbo.com.snwlhosted.com*. After an MX record is created, where the customer publishes *jumbo.com MX jumbo.com.snwlhosted.com*, SonicWALL then publishes 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. SonicWALL publishes an A record for outbound messages: *jumbo.com.outbound.snwlhosted.com A 173.240.21.200*

For outbound email messages, you will need to configure the mail server hosting your user mailbox(es) for outbound messages to route all outbound emails to *jumbo.com.outbound.snwlhosted.com*.

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.fuzeugna.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**.



The screenshot shows a web browser window displaying the SonicWALL Email Security Login page. At the top left is the Dell SonicWALL logo. To its right is the text "Email Security Login". Below this, the text "Control Center Server sjl0vm-hescc01" is displayed. Underneath, there are two input fields: "User Name:" followed by a text box, and "Password:" followed by a text box. At the bottom of the form area, there are two buttons: "Log In" and "Login Help".

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 18](#)
- [“User View Setup” on page 22](#)
- [“Monitoring” on page 23](#)

License Management

The **System > 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. The following settings display on the License Management page:

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

Dell SonicWALL Hosted Email Security comes with several services that must be licensed separately. For maximum effectiveness, all services are recommended. The following services are 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 (McAfee and SonicWALL Time Zero)**—Provides updates for McAfee 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 Dell 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.
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 **System > Administration** page allows you to change the master account Username and Password. Dell SonicWALL strongly recommends that you change the master account password.



The screenshot shows the 'Administration' page with the 'Email Security Master Account' section. It contains four text input fields: 'Username' (pre-filled with 'admin@crickettes.com'), 'Old password', 'New password', and 'Confirm password'. Below the fields is an 'Apply Changes' button.

To change password, follow the procedures below:

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

Invalid Login Policy

The **System > Administration > Invalid Login Policy** feature allows administrators to configure a User Lockout feature, locking out user accounts if the number of unsuccessful attempts to login is reached. Note that Invalid Login Policy is only available if the Global Administrator configures this feature for all users. Configure the following settings:



The screenshot shows the 'Invalid Login Policy' configuration page. It has three settings: 'Number of unsuccessful attempts allowed before lockout' (input field with '5'), 'Lockout interval' (two input fields for '0' hours and '15' minutes), and 'Alert administrator when account is locked' (checkbox). An 'Apply Changes' button is at the bottom.

Number of unsuccessful attempts before lockout—Specify the number of invalid attempts allowed before the user account is locked. The default value is 5, but can range between 0-9. If the value is set to 0, this feature is disabled.

Lockout Interval—This is the amount of time the user account is locked. The user will have to wait for this time interval to lapse before being allowed to login again; any correct or incorrect attempts will not allowed. The default value is 15 minutes. The hours value can range from 0-72 hours and the minutes value can range from 1-59 minutes.

Alert administrator when account is locked—Select this checkbox to alert administrator with an emergency message about the user account lockout.

Network Architecture

Server Configuration

The **System > Network Architecture > Server Configuration** page allows you to configure both inbound and outbound capabilities for your Hosted Email Security server.

Click the **Inbound** tab to configure the inbound destination server, which is the email server that will accept good email after Dell SonicWALL 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.

System / Network Architecture /

Server Configuration

[Inbound](#) [Outbound](#)

Configure your domain

To manage Domains, use the [Users, Groups and Domains](#) page.

Settings

Any source IP address is allowed to connect to this path, but relaying is allowed only for emails sent to one of these domains:

epcoding.com
epcoding2.com

Your mail server host name or IP address. If multiple destination servers are provided then emails will be routed using load balancing:

Round-robin Fail-over

204.212.170.65:25

[Test Downstream](#)

Separate the destination servers with a <CR>. Examples:
enr.example.com:25
sales.example.com:25

Require the destination server to support StartTLS

Spooling

Under normal circumstances, the hosted email server operates as an SMTP proxy: email is not spooled. Under some circumstances, such as a service outage at your site, you may want the hosted email server to spool email temporarily. Three options are provided:

- Never spool email:** the hosted server will act as an SMTP proxy, never spooling email. Any email that is currently in the spool will be delivered.
- Automatic fallback:** if your organization's email server cannot be reached, email will be spooled on the hosted server until it is reachable again.
- Always spool email:** good email will be spooled on the hosted server. Email will **not** be delivered to your organization's email server while this option is selected.

[Apply Changes](#)

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 & 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.

Click the **Outbound** tab to configure the outbound mail server. Configure the following settings:

Configure your domain

To manage Domains, use the [Users, Groups and Domains](#) page.

Settings

Relaying is allowed only for emails sent from one of these domains:

epcoding.com
 epcoding2.com

Only these IP addresses can connect and relay through this path:

Test Upstream

Separate the source servers with a <CR>. Examples:
 engr.example.com
 sales.example.com

Require clients to connect using StartTLS

Apply Changes

<p>Relaying is allowed only for emails sent from one of these domains</p>	<p>This field only displays domain name(s) 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.</p>
<p>Only these IP addresses can connect and relay through this path</p>	<p>Enter the server name or IP address to connect and relay with.</p> <p>Test Upstream: Click this button to test connection to the specified server name or address. A message displays, notifying you if the connection was successful or if the connection failed.</p>
<p>Require clients to connect using StartTLS</p>	<p>Click this checkbox to require clients to connect using Transport Layer Security (TLS) encryption for upstream email messages.</p>

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.

Spooling

Under normal circumstances, the hosted email server operates as an SMTP proxy: email is not spooled. Under some circumstances, such as a service outage at your site, you may want the hosted email server to spool email temporarily. Three options are provided:

- Never spool email:** the hosted server will act as an SMTP proxy, never spooling email. Any email that is currently in the spool will be delivered.
- Automatic fallback:** if your organization's email server cannot be reached, email will be spooled on the hosted server until it is reachable again.
- Always spool email:** good email will be spooled on the hosted server. Email will **not** be delivered to your organization's email server while this option is selected.

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

Dell SonicWALL Hosted 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 Dell SonicWALL Hosted 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 Dell SonicWALL Hosted Email Security can automatically get user information from these directories using the LDAP. You can run Dell SonicWALL Hosted 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.

Dell SonicWALL Hosted 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 22](#) 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.
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 Dell SonicWALL Hosted 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:

The screenshot shows the 'LDAP Mappings' configuration interface. At the top left is the Dell SonicWALL logo and the title 'LDAP Mappings'. On the top right are 'Help' and 'Close' buttons. The main area is titled 'Using LDAP' and contains a dropdown menu with 'remote.crickettes.com' selected, followed by a 'Go' button. Below this is a rule configuration section with 'IF' and 'THEN' labels. The 'IF' dropdown is set to 'domain is', followed by an empty text box. The 'THEN' dropdown is set to 'replace with', followed by another empty text box. An 'Add Mapping' button is located to the right of the 'THEN' section. At the bottom of the form, there is a 'Mapping' label and the text 'Using LDAP'.

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* “enr.corp.com” then *Replaced with* “corp.com”, then mail addressed to “anybody@enr.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 “enr.corp.com” is the first domain and “sales.corps.com” is the second, then when the domain “enr.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.

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 on the **System > User View Setup** page.

System /
User View Setup

General Settings

User View Setup

Login enabled

Checked items will appear in the navigation toolbar for users:

Anti-Spam Techniques
(people, companies, lists, aggressiveness, languages)

Full user control over anti-spam aggressiveness settings

Reports

Settings

Spam Management

User download settings

Allow users to download SonicWALL Junk Button for Outlook

Allow users to download SonicWALL Anti-Spam Desktop for Outlook and Outlook Express

Quarantined junk mail preview settings

Users can preview their own quarantined junk mail

Allow the following types of users to preview quarantined junk mail for the entire organization:

Administrators

Help Desk and Group Administrators

Reports view settings

Show reports that display information about individual employees

Apply Changes Revert

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 Dell SonicWALL Hosted 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 **System > 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.

System / **Monitoring**

Monitoring

Configure System Monitoring

Email address of administrator who receives emergency alerts:

Name or IP address of backup SMTP servers:
(Separate multiple entries with a comma)

Customized signature:

Subscribe to alerts

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.

Date	Severity	Domain	Summary
05/30/12 16:29 (Local)	Critical	crickettes.com	crickettes.com : SonicWALL Email Security Gateway not responding to SMTP test
05/30/12 23:29 (GMT)			
05/17/12 17:55 (Local)	Warning	crickettes.com	crickettes.com : The SonicWALL Email Security destination server is not responding to an SMTP test
05/18/12 00:55 (GMT)			
05/17/12 16:53 (Local)	Warning	crickettes.com	crickettes.com : The SonicWALL Email Security destination server is not responding to an SMTP test
05/17/12 23:53 (GMT)			

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**.

Anti-Spam Anti-Phishing Techniques

This chapter contains the following sections:

- [“Hosted Email Security and Mail Threats” on page 25](#)
- [“Managing Spam” on page 25](#)
- [“Default Spam Management” on page 27](#)
- [“Address Books” on page 29](#)
- [“Anti-Spam Aggressiveness” on page 32](#)
- [“Languages” on page 33](#)
- [“Anti-Phishing” on page 34](#)

Hosted Email Security and Mail Threats

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

Managing Spam

Hosted 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, Hosted Email Security provides updated lists and collaborative thumbprints to aid in identifying spam and junk messages.

Spam Identification

Hosted 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 the Dell SonicWALL Hosted 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, Dell SonicWALL Hosted Email Security analyzes messages' headers and contents, and use collaborative thumbprinting to block email that contains junk.

Default Spam Management

Use the **Anti-Spam, Anti-Phishing > Default Spam Management** page 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.

Anti-Spam, Anti-Phishing / **Default Spam Management**

Anti-Spam Techniques

These settings apply to all users. You can override these settings for any individual user.

Action Settings

Action for messages marked as **Definite Spam**:

- Definite Spam blocking off (deliver messages to recipients)
- Permanently delete
- Bounce back to sender
- Store in Junk Box (recommended for most configurations)
- Send to
- Tag with added to the subject
- Add X-Header: X- :

Action for messages marked as **Likely Spam**:

- Likely Spam blocking off (deliver messages to recipients)
- Permanently delete
- Bounce back to sender
- Store in Junk Box (recommended for most configurations)
- Send to
- Tag with added to the subject
- Add X-Header: X- :

Miscellaneous

Accept automated Allowed Lists:

Skip spam analysis for internal email:

Allow users to delete junk email:

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 Dell SonicWALL Hosted 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 **Anti-Spam, Anti-Phishing > 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, Hosted 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.

Anti-Spam, Anti-Phishing /
Address Books

Allowed Blocked

Administration - Corporate

Use this page to allow or block people, companies, or mailing lists from sending you email. The final list shown is a compilation of allowed and blocked senders from your organization's lists and lists provided by default.

Search

Go Reset

People Companies Lists

Add Delete

<input type="checkbox"/>	Address	Type	Address Source
<input type="checkbox"/>	sonicwall.com	Companies	

Add Delete

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.

Notice.
Specify your additions.

Add Term

Select list type: People

Enter the email addresses separated by a carriage return.
(Example: friend@server.com, important@filtered.org)

Add Cancel

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.
- Dell SonicWALL Hosted Email Security will warn you if you attempt to add your own email address or your own organization.
- Email addresses are not case-sensitive; Hosted Email Security converts the address to lowercase.
- Hosted 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; Hosted 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.
- Dell SonicWALL Hosted 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 Dell SonicWALL Hosted 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.

Import Address Book

You can also import an address book of multiple addresses. Note that users and secondary domains should be added *prior* to importing their respective address books.

The Address Book file for import must follow specific formatting to ensure successful importing:

- <TAB> delimiter between data
- <CR> to separate entries

Each address book entry must include each of the following:

- **Identifier**—Specified as <email address / primary domain>
- **Domain / List / Email**—Specified as D / L / E
- **Allowed / Blocked**—Specified as A / B
- **Address List**—Specified as abc@domain.com, example.com

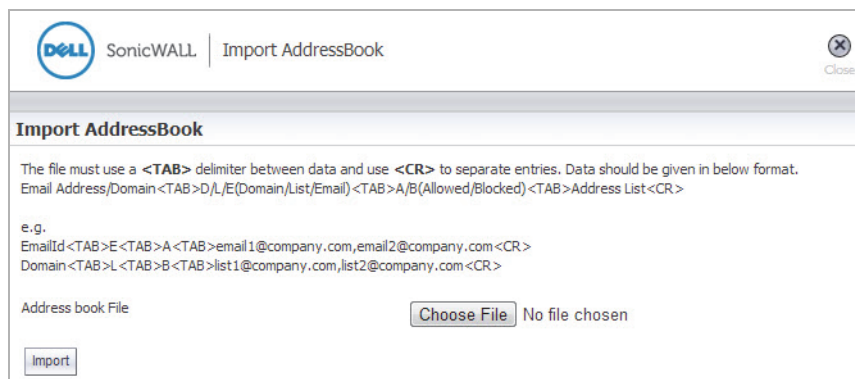
See the following examples:

EmailID<TAB>E<TAB>A<TAB>email1@company.com,email2@company.com<CR>

Domain<TAB>L<TAB>B<TAB>list1@company.com,list2@compnay.com<CR>

To import Address Books, follow the procedures listed:

1. From the **Anti-Spam, Anti-Phishing > Address Books** page, click the **Import** button on either the Allowed or Blocked tabs.
2. Click the **Choose File** button. Select the correct file from your system.
3. Click the **Import** button.



The screenshot shows a dialog box titled "Import AddressBook" from SonicWALL. It contains the following text:

The file must use a <TAB> delimiter between data and use <CR> to separate entries. Data should be given in below format.
Email Address/Domain<TAB>D/L/E(Domain/List/Email)<TAB>A/B(Allowed/Blocked)<TAB>Address List<CR>

e.g.
EmailId<TAB>E<TAB>A<TAB>email1@company.com,email2@company.com<CR>
Domain<TAB>L<TAB>B<TAB>list1@company.com,list2@company.com<CR>

Address book File No file chosen

Anti-Spam Aggressiveness

The **Anti-Spam, Anti-Phishing > Anti-Spam Aggressiveness** page allows you to tailor Dell SonicWALL Hosted Email Security to your organization's preferences. Configuring this window is optional. Dell SonicWALL 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. Dell SonicWALL Hosted 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 Hosted Email Security more likely more responsive to other users who mark a message as spam.

Use these settings to specify how stringently Dell SonicWALL Hosted 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 Hosted Email Security's spam-blocking evaluation.
- If you choose **Strong**, Hosted 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**, Hosted 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 Dell SonicWALL Hosted 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

The **Anti-Spam, Anti-Phishing > Languages** page lets you 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 Hosted 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, found on the **Anti-Spam, Anti-Phishing > Anti-Phishing** page, 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

As with spam, Hosted Email Security uses multiple methods of detecting phishing:

- Divergence Detection™ ensures that all contact points are consistent and legitimate. Contact points include email addresses, URLs, phone numbers, and physical addresses.
- Sender ID tests if the source of an email has permission to send email for that domain. Many Internet domains publish the list of IP addresses that are authorized to send email on their behalf. If the source IP address of an email is not on the domain's list of authorized addresses, Sender ID suggests that the message may be a forgery. Hosted Email Security factors Sender ID pass or fail into its junk algorithm, which can be enabled on the **Anti-Spam, Anti-Phishing > Anti-Phishing** page.

- Domain Keys Identified Mail (DKIM) uses a secure digital signature to verify that the sender of a message is who it claims to be and that the contents of the message have not been altered in transit. A valid DKIM signature is a strong indicator of a message's authenticity, while an invalid DKIM signature is a strong indicator that the sender is attempting to fake his identity. For some commonly phished domains, the absence of a DKIM signature can also be a strong indicator that the message is fraudulent.

Configuring Phishing Protection

Anti-Spam, Anti-Phishing /

Anti-Phishing

Anti-Phishing Techniques

These settings apply to all users.

Action Settings

Action for messages identified as **Definite Phishing**:

- Definite Phishing blocking off (deliver messages to recipients)
- Permanently delete
- Bounce back to sender
- Store in Junk Box (recommended for most configurations)
- Send to
- Tag with added to the subject
- Add X-Header: X- :

Action for messages identified as **Likely Phishing**:

- Likely Phishing blocking off (deliver messages to recipients)
- Permanently delete
- Bounce back to sender
- Store in Junk Box (recommended for most configurations)
- Send to
- Tag with added to the subject
- Add X-Header: X- :

Miscellaneous

Allow users to unjunk phishing messages:

Send copies of emails containing phishing attacks to the following email addresses:

(Separate multiple email addresses with a comma)

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

1. Navigate to the **Anti-Spam, Anti-Phishing > 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.

Domain Keys Identified Mail (DKIM)

Dell SonicWALL Hosted Email Security supports Domain Keys Identified Mail (DKIM) verification of inbound email messages. With the DKIM verification feature, the recipient is able to identify the domain name associated with the sender by validating the DKIM signature in the message. Mail messages are filtered based on three parameters: if the message is DKIM signed, if DKIM verification is successful, and if DKIM is strictly enforced for the domain. After Hosted Email Security completes the verification of a message, the results are written into the Junk Summary, as well as in the SMTP X header of the mail message.

Users benefit from DKIM because it verifies legitimate messages and prevents against phishing. Remember that DKIM does *not* prevent spam—proper measures should still be taken against fraudulent content. Dell SonicWALL recommends that DKIM typically not be configured with overly aggressive settings. However, with some domains, such as paypal.com, aggressive DKIM settings may be useful to stop phishing. The recommended setting is to store email messages with invalid DKIM signatures in the Junk Box. See the table below for descriptions of each setting.

To configure settings for the DKIM feature, navigate to the **Anti-Spam, Anti-Phishing > Anti-Phishing** page. Then, scroll to the **DKIM Settings** and select the action for an invalid DKIM signature:

Action	Effect
DKIM blocking off (deliver messages to recipients)	This is the default setting. All messages are delivered to the recipients.
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.

Action	Effect
Store in Junk Box (recommended for most configurations)	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.
Tag With	This email is tagged with a term in the subject line, for example, [DKIM Failed]. 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 "fraud" results in the email header as: "S-EMSJudgedThisEmail:fraud".

DKIM Settings

Action for invalid DKIM signature:

- DKIM blocking off (deliver messages to recipients)
- Permanently delete
- Bounce back to sender
- Store in Junk Box (recommended for most configurations)
- Send to:
- Tag with: added to the subject
- Add X-Header: X- :

Enforced DKIM domains (Domains required to have DKIM signature)

Domains	DKIM Action	Settings
No Data Available		

You can also add domains to the list of Enforced DKIM domains, which are domains required to have a DKIM signature. In the **DKIM Settings** section, click the **Add Domain** button. In the dialog box that appears, enter the **Domains** to enforce the DKIM feature and specify the **Action for invalid DKIM Signature**. Click **Save** when finished.

Configure Domains to Enforce DKIM Signature

Domains:

(Separate multiple domains with a comma)

Action for invalid DKIM signature:

- DKIM blocking off
- Permanently delete
- Bounce back to sender
- Store in Junk Box
- Send to:
- Tag with: added to the subject
- Add X-Header: X- :

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 39](#)
- [“Configuring Anti-Virus Protection” on page 40](#)

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® 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 engine are categorized as *Viruses*. SonicWALL Email Security also supports the SonicWALL GRID antivirus automatically. GRID virus-detection works in with the McAfee 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.

Configuring Anti-Virus Protection

To configure Anti-Virus protection, follow the procedures listed:

1. Navigate to the **Anti-Spam, Anti-Phishing > 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. Be sure to select the **Inbound** or **Outbound** tab to configure settings for the correct path.

Anti-Virus Techniques

General Settings

These settings apply to all users.

Action Settings

Action for messages identified as **Definite Viruses**:

- Definite Virus filtering off (deliver messages to recipients)
- Permanently delete
- Bounce back to sender
- Store in Junk Box (recommended for most configurations)
- Send to
- Tag with added to the subject
- Add X-Header: X- :
(The virus will be removed before the user accesses the message)

Action for messages identified as **Likely Viruses** using SonicWALL's Time Zero Virus Technology:

- Likely Virus filtering off (deliver messages to recipients)
- Permanently delete
- Bounce back to sender
- Store in Junk Box (recommended for most configurations)
- Send to
- Tag with added to the subject
- Add X-Header: X- :
(The attachment will be delivered intact)

Miscellaneous

Viruses will be removed from messages identified as definite Viruses, but will deliver attachments intact for messages identified as Likely Viruses.

Allow users to unjunk viruses: This setting applies to both Viruses and Likely Viruses.

2. Determine how to treat email messages that contain *Definite Viruses* or *Likely Viruses* and select the action to take. The following table describes the available actions:

Action	Consequences	Additional Information
Definite Virus Filtering Off	Dell SonicWALL Hosted 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.
Bounce Back to Sender	Hosted 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)	Hosted 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: Hosted Email Security recommends this option because you can retrieve the message after Hosted Email Security strips the virus.
Send To	Hosted 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]	Hosted 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].
Add X-Header	Hosted Email Security 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: "X-EMSJudgedThisEmail:DefiniteSpam".

3. Select 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.
4. Click **Apply Changes**.

Zombie and Spyware Protection

Unauthorized software may be running on a computer within your organization and sending out junk email messages such as: spam, phishing, virus, or other unauthorized content. This scenario could happen if your organization was subjected to a virus attack called Trojans or a user downloaded something from the web and unauthorized software got installed without user's knowledge. These unauthorized software programs that send out malicious content are called Zombies or Spyware.

SonicWALL Email Security's Zombie and Spyware Protection technology brings the same high standard of threat protection available on the inbound email path to email messages leaving your organization through the outbound path.

To enable Zombie and Spyware Protection, navigate to the **Anti-Virus Techniques** page. Click on the **Outbound** tab, and then select the box **Enable Zombie and Spyware Protection**.

Use the **Action Settings** section to configure the actions to take when emails are sent by Zombies. The following actions are available to select:

- Allow delivery
- Permanently delete
- Store in Junk Box

CHAPTER 5

Auditing

SonicWALL Email Security's Auditing module, found on the **Auditing** page, enables the user to monitor all emails, both inbound and outbound, that pass through Hosted 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 43](#)
- [“Searching Inbound & Outbound Emails” on page 43](#)
- [“Configure Auditing” on page 46](#)

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. Dell SonicWALL now uses a search engine to search on audit and junk messages.

Searching Inbound & Outbound Emails

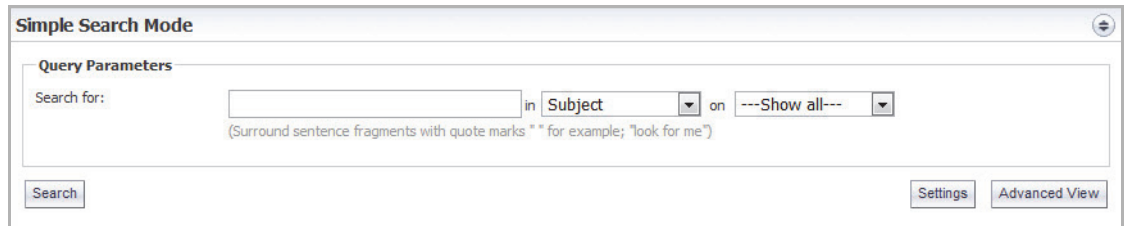
Email messages processed by Dell SonicWALL Hosted Email Security are those that originate from both inside and outside of your organization, including the total number of junk messages and good messages. Below the search section a list of emails is displayed with the following information:

- 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

Click the **Inbound** or **Outbound** tab on the **Auditing** page to do a search for inbound or outbound messages, respectively.

Audit Simple Search

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

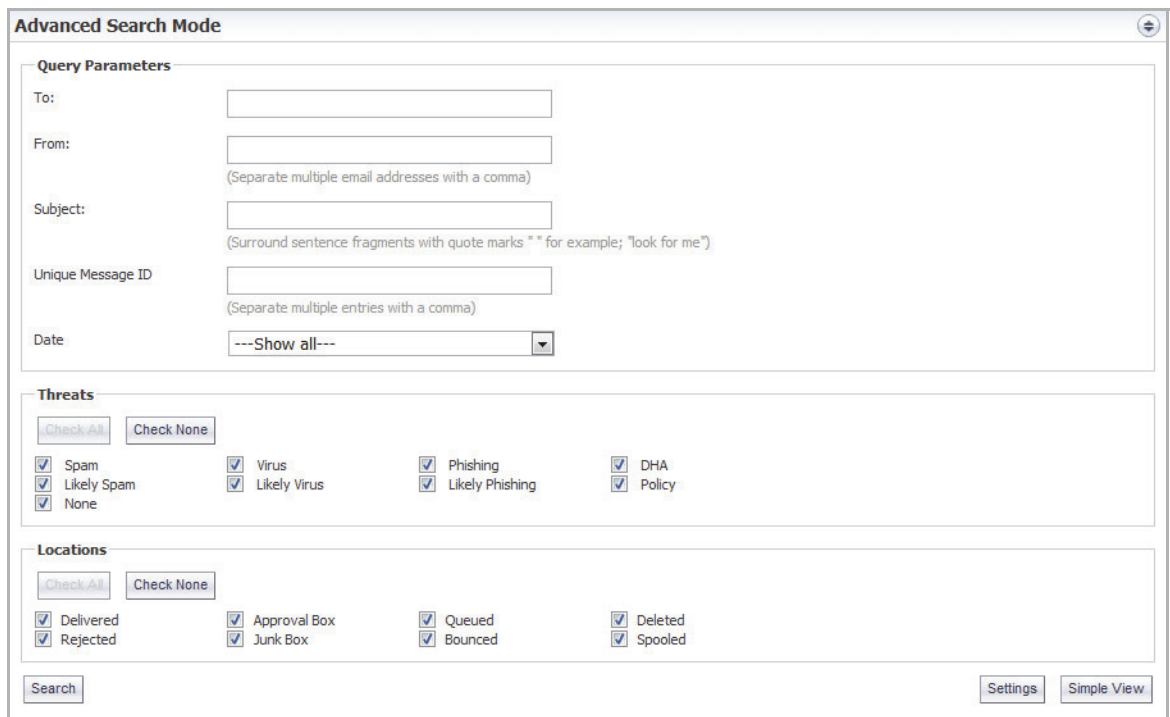


1. Search for messages by selecting specific strings from the dropdown list in the following fields: Subject, From, To, or Unique Message ID. Ensure sentence fragments are surrounded by quotation marks.
2. Select the specific date or **Show all** to search from the dropdown list.
3. Click **Search**.

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**.

The screenshot shows the 'Advanced Search Mode' interface. It is divided into three main sections: 'Query Parameters', 'Threats', and 'Locations'.
1. **Query Parameters:** This section contains several input fields: 'To:', 'From:', 'Subject:', 'Unique Message ID', and 'Date'. The 'From:' field has a note: '(Separate multiple email addresses with a comma)'. The 'Subject:' field has a note: '(Surround sentence fragments with quote marks "" for example; "look for me")'. The 'Date' field is a dropdown menu currently set to '---Show all---'.
2. **Threats:** This section has a 'Check All' button and a 'Check None' button. Below these are several checkboxes, all of which are checked: Spam, Likely Spam, None, Virus, Likely Virus, Phishing, Likely Phishing, DHA, and Policy.
3. **Locations:** This section also has a 'Check All' button and a 'Check None' button. Below these are several checkboxes, all of which are checked: Delivered, Rejected, Approval Box, Junk Box, Queued, Bounced, Deleted, and Spooled.
At the bottom of the interface, there is a 'Search' button on the left, and 'Settings' and 'Simple View' buttons on the right.

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. Hosted 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.

The screenshot shows the 'Configure Auditing' window in the SonicWALL interface. The window has a title bar with the Dell SonicWALL logo and the text 'SonicWALL | Configure Auditing'. Inside the window, there are four settings:

- 'Auditing for inbound email:' with radio buttons for 'on' (selected) and 'off'.
- 'Auditing for outbound email:' with radio buttons for 'on' and 'off' (selected).
- 'Enable Judgment Details logging:' with radio buttons for 'on' (selected) and 'off'.
- 'Keep auditing files for:' with a dropdown menu showing '30 Days'.

An 'Apply' button is located at the bottom center of the settings area.

2. Select the radio button(s) in the **On** position for the following:
 - Auditing for inbound email
 - Auditing for outbound email
 - Enable Judgment Details logging
3. Click **Apply** to save any changes to the settings.

Chapter 6

Policy Management

SonicWALL Email Security's Policy Management feature enables you to write policies to filter messages and their contents as they enter or exit your organization. Policies can be defined only by the OU Admin. Typical use of such policies include capturing messages that contain certain business terms, such as trademarked product names, company intellectual property, and dangerous file attachments.

This chapter contains the following sections:

- [“Hosted Email Security and Mail Threats” on page 47](#)
- [“Basic Concepts for Policy Management” on page 47](#)
- [“Adding Filters” on page 48](#)
- [“Managing Filters” on page 50](#)

Hosted 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, Policy Violation, 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 Dell SonicWALL Hosted Email Security determines the message is *not* any of the above threats, it is delivered to the destination server.

Basic Concepts for Policy Management

Policy Management enables you to filter email based on message contents and attachments. You can filter for specific terms that you want, such as terms in your product or terms you do not want in your organization's email.

You manage policy by creating filters in which you specify the words to search for in content, senders, or other parts of the email. After filtering for specified characteristics, you can choose from a list of actions to apply to the message and its attachments.

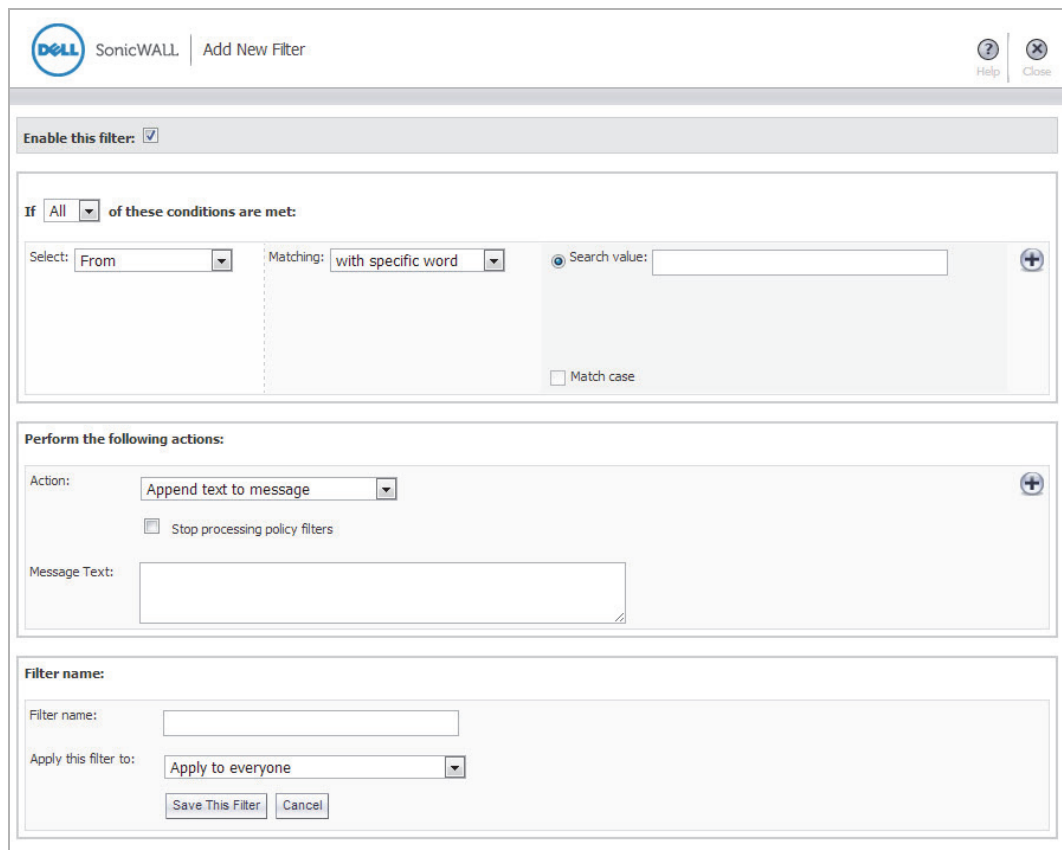
Note that any of the policies configured in the Policy section takes precedence over any configurations made in the Allowed List entries.

Adding Filters

A Policy Filter is an action or actions you want Dell SonicWALL Hosted Email Security to take on messages that meet conditions you define. Hosted Email Security's Policy Management module enables you to filter email as it enters or exits your organization. Note that Policy Management is a tool only for administrators; policies cannot be managed individually and are not user-configurable.

To create and manage policy filters, follow the procedures listed:

1. Navigate to the **Policy > Filters** page.
2. Select the **Inbound** or **Outbound** tab to create filters for inbound or outbound email messages, respectively.
3. Click the **Add New Filter** button. The **Add Filter** window displays:



Note The fields in the window change based on the action you choose.

4. The **Enable this Filter** checkbox is checked by default. Uncheck the checkbox to create rules that do not go into effect immediately.
5. Choose whether the filter matches All of the conditions or Any of the conditions
 - **All**—Causes email to be filtered when all of the filter conditions apply (logical AND)
 - **Any**—Causes email to be filtered when any of the conditions apply (logical OR)

6. Choose the parts of the message to filter.

Select	Definition
From	Filter by the sender's name
To/Cc/Bcc	Filter by the names in the To: cc: or bcc: fields
Subject	Filter by words in the subject
Body	Filter based on information in the body of the email
Subject or Body	Filter based on information in the subject and body of the email
Message header	Filter by the RFC822 information in the message header fields, which includes information including the return path, date, message ID, received from, and other information
Size of message	Filter messages based on the size of the message
All Good Messages	Filter messages that are not flagged as a mail threat

7. Choose the matching operation. The choices for matching operation vary with the message part being matched against. The following table describes the matching operations available.

Type	Explanation	Example
With Specific Word	Equivalent to "Find the whole word only"	Search for the word "Mail" from the subject line "This is Mail" will match. Search for the word "Mail" from the subject line "This is MailFrontier" will not match.
Without Specific Word	Not equivalent to "Find the whole word only"	
With Specific Phrase	Equivalent to "Find complete phrase"	Search for the words "is Mail" from the subject line "This is Mail" will match. Search for the word "is Mail" from the subject line "This is MailFrontier" will not match.
Without Specific Phrase	Not equivalent to "Find complete phrase"	
Starts With	The message part being searched for should start with the search value	Search for "This" from the subject line "This is Mail" will match.
Ends With	The message part being searched for should end with the search value	Search for "is Mail" from the subject line "This is Mail" will match.
Is	Only the search criteria should exist (exact match).	Search for the word "Mail" from the subject line "This is Mail" will not match. Search for "is Mail" from the subject line "is Mail" will match.
Is Not	Only the search criteria should not exist	Search for the phrase "is Mail" from the subject line "This is MailFrontier", will match.
Contains	Substring search	Search for "is Mail" from the subject line "This is Mail" will match.
Does not Contain	Substring search does not match	

8. Enter the words or phrase that you want to filter in the Search Value text box. Select the **Match Case** checkbox, which filters a word or words sensitive to upper and lower case.

9. From the dropdown list, select the **Policy Action** to occur.

Action	Effect
Store in Junk Box	The email message is stored in the Junk Box. It can be unjunked by users with appropriate permissions. The user has the option of unjunking the email.
Permanently Delete	The email message is permanently deleted and no further processing occurs in Hosted Email Security. This option does not allow the user to review the email and can cause good emails to be lost.
Tag Subject With	The subject of the email is tagged with the specified term.
Strip All Attachments	Removes all the attachments from the email.
Append text to message	The specified text is appended to the message body.
Issue Email Notification	Sends an email notification to the recipients of the email that triggered the rule.
Add X-Header to Message	Adds an X-header to the email.
Remove X-Header from Message	Removes an X-header from the email.

Managing Filters

The **Policy > Filters** page lists all the filters created in the system for the Inbound and Outbound path. From this view, you can **Add New Filter**, Change the order of filters, **Edit** or **Delete** filters. Filters that have been enabled are indicated with a green tick mark.

Editing a Filter

To change a filter that has been saved, follow the procedures below:

1. Click the **Edit** button adjacent to the filter to be changed.
2. Change any of the filter conditions.
3. Click **Save This Filter**.

Deleting a Filter

To delete a filter, click the **Delete** button adjacent to the filter.

Changing Filter Order

Filters are processed in the order they appear.

To change the order of the filters, use the up and down arrow icons to the left of the filters.

Chapter 7

Users, Groups, & Domains

The User and Group Management function allows you to manage the list of users who can log in to the Hosted 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 51](#)
- [“Working with Groups” on page 56](#)
- [“Setting an LDAP Group Role” on page 57](#)
- [“Setting Junk Blocking Options for LDAP Groups” on page 58](#)
- [“Working with Domains” on page 66](#)
- [“Roles” on page 66](#)

Note the following:

- To manage users and groups from within this module, you need to have configured your Hosted Email Security setup to synchronize with your organization’s LDAP server. You can configure LDAP settings and queries on the **System > LDAP Configuration** page.
- Hosted 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 Hosted Email Security, but are updated within an hour.

Working with Users

To manage users in Hosted 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

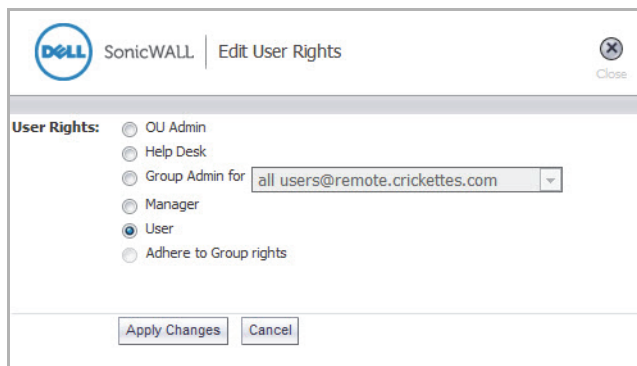
Administrators can sign in as any user, see their Junk Box, and change the settings for that user. In addition, you can sign in as a particular user to manage their delegates for them. Click the checkbox next to the User Name, then click the **Sign In as User** button.

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**.



The screenshot shows a window titled "SonicWALL | Edit User Rights" with a close button in the top right corner. Below the title bar, there is a section labeled "User Rights:" with a list of radio buttons. The options are: "OU Admin", "Help Desk", "Group Admin for" (with a dropdown menu showing "all users@remote.crickettes.com"), "Manager", "User" (which is selected), and "Adhere to Group rights". At the bottom of the dialog, there are two buttons: "Apply Changes" and "Cancel".



Note See [“Setting an LDAP Group Role”](#) on page 57 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**.

The file must use a **<TAB>** delimiter between the primary address and the alias, and use **<CR>** to separate entries. If the user does not exist in LDAP, you must include an entry listing the primary address as the initial alias address in addition to any additional alias addresses, e.g.

```
primary_email1@company.com<TAB>primary_email1@company.com<CR>
primary_email1@company.com<TAB>alias1@company.com<CR>
primary_email1@company.com<TAB>alias2@company.com<CR>
```

If the user already exists in LDAP, the entries will be:

```
primary_email2@company.com<TAB>alias1@company.com<CR>
primary_email2@company.com<TAB>alias2@company.com<CR>
```

Import Mode: append overwrite

Using Source: remote.crickettes.com

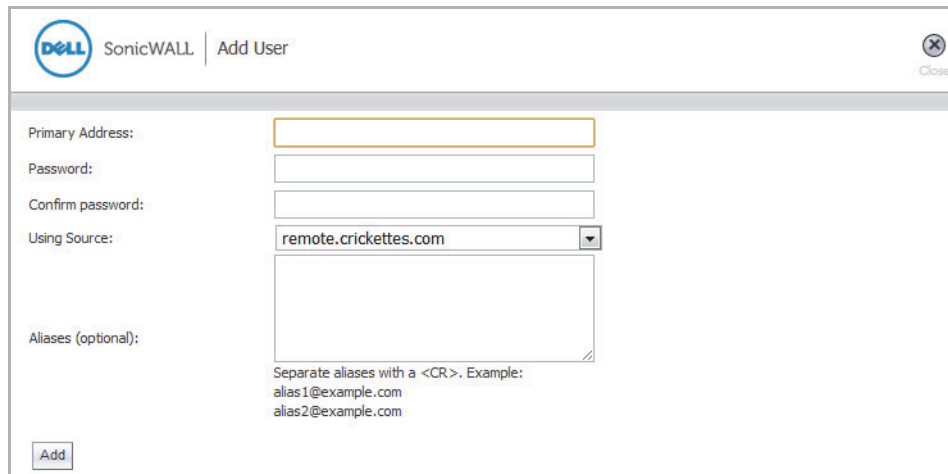
Users File: No file chosen

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 **Junk Box Management > 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 top of the screen.

User View Setup

It is recommended that the administrator add all employees to the list of users who can log in. Corporate mailing list addresses and aliases (such as info@example.com) should also be added to ensure that junk mail sent to those aliases can be filtered. There is no harm if extra addresses that do not receive email appear here as a result of too broad an LDAP query.

Enable authentication for non ldap users.

Using Source
corporateldap

Find all users in column
User Name

Show LDAP entries Show non-LDAP entries

User Name	Primary Email	Message Management	User Rights	Source
<input type="checkbox"/> 2003t	2003t@sonicwall.com	Default	User	corporateldap LDAP
<input type="checkbox"/> 3200beta	3200beta@sonicwall.com	Default	User	corporateldap LDAP
<input type="checkbox"/> 3g feedback	3gfeedback@sonicwall.com	Default	User	corporateldap LDAP
<input type="checkbox"/> 4100beta	4100beta@sonicwall.com	Default	User	corporateldap LDAP
<input type="checkbox"/> 421db0dc-e999-4842-a	421db0dc-e999-4842-a@sonicw...	Default	User	corporateldap LDAP
<input type="checkbox"/> 5.6.4 Team	5.6.4team@sonicwall.com	Default	User	corporateldap LDAP
<input type="checkbox"/> 666	666@sonicwall.com	Default	User	corporateldap LDAP
<input type="checkbox"/> 713905de-dec5-433b-8	713905de-dec5-433b-8@sonicw...	Default	User	corporateldap LDAP
<input type="checkbox"/> 926a0da4-7554-4877-a	926a0da4-7554-4877-a@sonicw...	Default	User	corporateldap LDAP
<input type="checkbox"/> A Relations	arelations@sonicwall.com	Default	User	corporateldap LDAP

1-10 of 4653 Display

Working with Groups

About LDAP Groups

This section describes how Hosted 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 Hosted Email Security in the LDAP Configuration screen.

Hosted 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, Hosted 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 Hosted 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.

The screenshot shows a web interface window titled "SonicWALL | Add Group". At the top right is a "Close" button. The main content area is divided into several sections:

- Using Source:** A dropdown menu showing "remote.crickettes.com" and a "Go" button.
- Find all groups:** A dropdown menu showing "equal to (fast)" and an empty text input field, with a "Go" button below.
- Add Group:** A button located below the "Find all groups" section.
- Table:** A table with two columns: "ID" and "Group". The table is currently empty, with the text "There are no groups." centered below the headers.
- Bottom:** Another "Add Group" button.

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.



The screenshot shows a window titled "SonicWALL | Edit Role" with a close button in the top right corner. Below the title bar, the text "For Group(s): sonicwall es help desk@remote.crickettes.com" is displayed. Underneath, the "Assigned Role:" section contains five radio button options: "OU Admin", "Help Desk" (which is selected), "Group Admin for", "Manager", and "User". The "Group Admin for" option is followed by a dropdown menu currently showing "all users@remote.crickettes.com". At the bottom of the dialog is an "Apply Changes" button.

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.

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.



Note

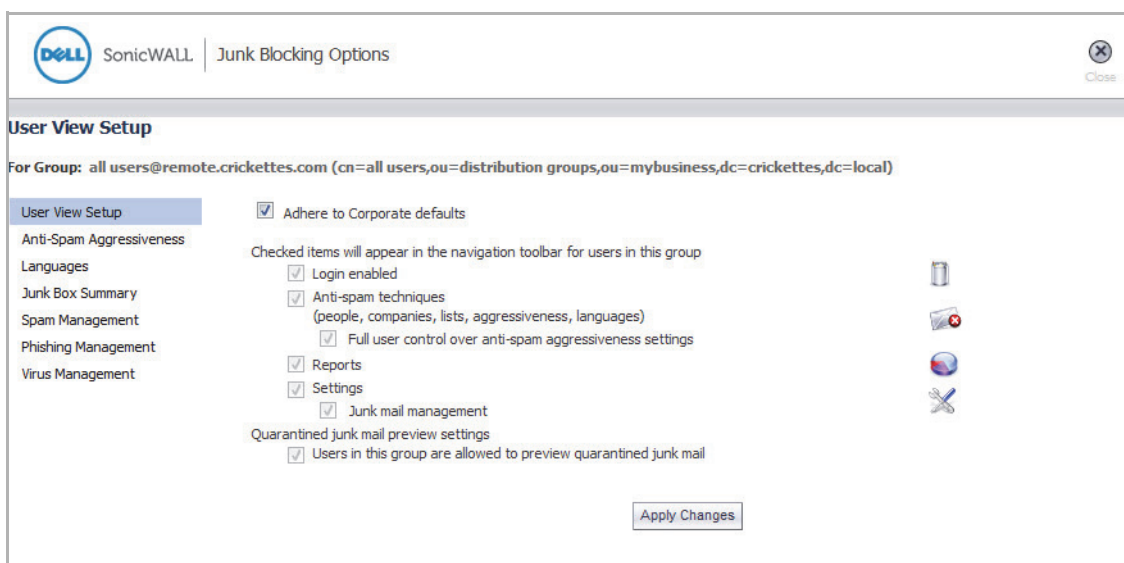
To enable the specified group to have special privileges, deselect the Adhere to Corporate/Group Defaults box.

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 Hosted 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 Hosted 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.

Anti-Spam Aggressiveness

For Group: all users@remote.crickettes.com (cn=all users,ou=distribution groups,ou=mybusiness,dc=crickettes,dc=local)

User View Setup Adhere to Corporate defaults

Anti-Spam Aggressiveness

Languages

Junk Box Summary

Spam Management

Phishing Management

Virus Management

	Mild		Medium		Strong		
	1	2	3	4	5		
Selecting a stronger setting will make Email Security more responsive to other users who mark a message as spam.							
Grid Network Aggressiveness	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>		
Selecting a stronger setting will make Email Security more likely to mark a message as spam.							
Adversarial Bayesian Aggressiveness	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>		
<input checked="" type="checkbox"/> Allow users to unjunk spam. (If unchecked, users cannot unjunk any spam messages.)							
Selecting a stronger setting will make messages with the content below more likely to be marked as spam.							
Sexual Content	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Offensive Language	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Get Rich Quick	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Gambling	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Advertisements	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>
Images	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input checked="" type="checkbox"/>


Apply Changes

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 Hosted Email Security.

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

 SonicWALL | Junk Blocking Options Close

Spam Blocking Options

For Group: all users@remote.crickettes.com (cn=all users,ou=distribution groups,ou=mybusiness,dc=crickettes,dc=local)

User View Setup Adhere to Corporate defaults

Anti-Spam Aggressiveness

Languages

Junk Box Summary

Spam Management

Phishing Management

Virus Management

This page enables administrators to allow or block emails in the languages listed below.

- Choose **Allow All** to allow all email in a language without any screening.
- Choose **Block All** to block all email in a language.
- Choose **No Opinion** to allow email in a language to be screened by all filters installed in Email Security.

Language	Allow All	Block All	No Opinion
Arabic (Persian)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Baltic	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Chinese	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Cyrillic (Russian)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Dutch	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
English	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
French	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
German	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Greek	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Hebrew	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Italian	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Japanese	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Korean	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Portuguese	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Spanish	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Swedish	<input checked="" type="radio"/>	<input type="radio"/>	<input type="radio"/>
Thai	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Turkish	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Vietnamese	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

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 the **Time Zone** that applies to when junk summary emails are sent.
5. Select if the Summaries include **All Junk Messages** or **Only Likely Junk**.
6. Select from the dropdown list the **Language of Summary Email**.
7. Choose to send **Plain Summary**. If this checkbox is not selected, Graphic Rich Summary messages are sent.
8. 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.
9. Click **Apply Changes**.

Junk Box Summary

For Group: administrators@ldapserver (cn=administrators,cn=builtin,dc=hessim,dc=eng,dc=sonicwall,dc=com)

User View Setup
Anti-Spam Aggressiveness
Languages
Junk Box Summary
Spam Management
Phishing Management
Virus Management

Adhere to Corporate defaults

Junk Box Summary

Users will be sent "Junk Box Summary" notification emails listing all of their quarantined messages.

Frequency of summaries: 1 Day

Time of day to send summary:
 Any time of day
 Within an hour of 1 AM

Day of week to send summary:
 Any day of the week
 Send summary on Monday

Time Zone: (GMT-08:00) Pacific Time (US & Canada); Tijuana

Summaries include:
 All junk messages
 Only likely junk (hide definite junk)

Language of summary email: English

Send plain summary (no graphics)
 Plain summary
([view plain example](#) | [view graphic example](#))

Send Junk Box Summary to delegates:

(When checked, the summary email will be sent to the delegate, not to the original recipient.)

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:

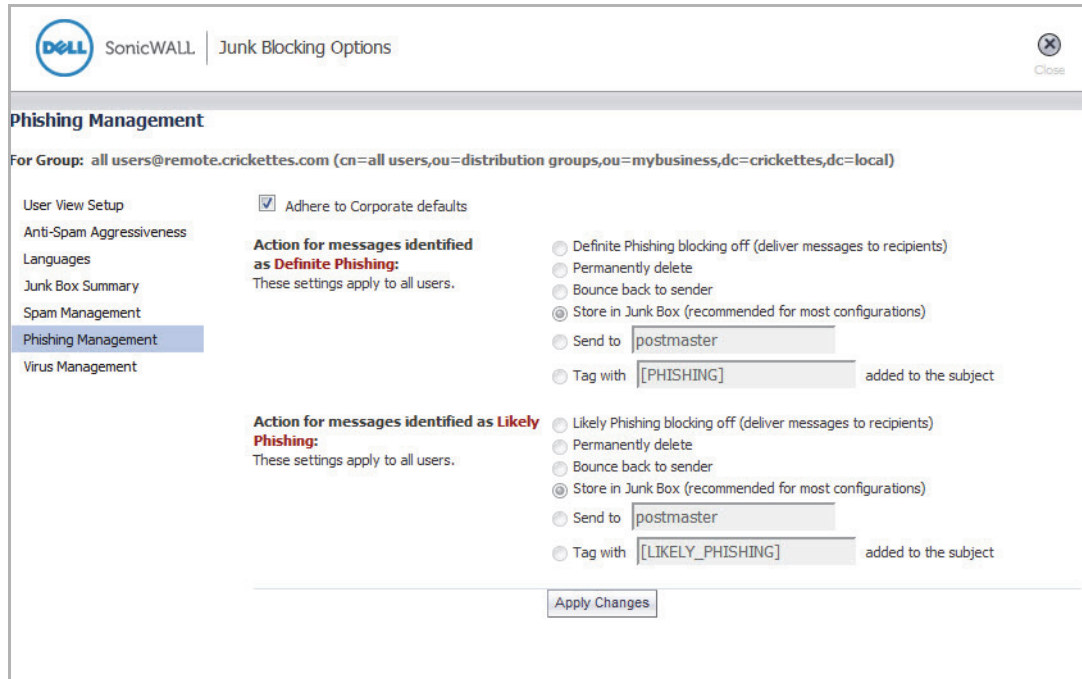
- **Spam Filtering Off**—Passes all messages to users without filtering.
- **Permanently Delete**—If determined Definite or Likely Spam, messages are permanently deleted.
- **Bounce back to sender**—Messages are sent back to the sender.
Caution: In cases of self-replicating viruses that engage the sender's 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**.

The screenshot shows the 'Junk Blocking Options' window for a group named 'all users@remote.crickettes.com'. The window is divided into several sections:

- User View Setup:** Includes a checkbox for 'Adhere to Corporate defaults' which is checked.
- Anti-Spam Aggressiveness:** A section for configuring spam actions.
- Likely Spam:** A section for configuring actions for messages marked as 'Likely Spam'. It includes radio buttons for 'Definite Spam blocking off', 'Permanently delete', 'Bounce back to sender', 'Store in Junk Box' (selected), 'Send to postmaster', and 'Tag with [LIKELY_SPAM]'. A checkbox for 'This Group accepts automated Allowed Lists' is also checked.
- Buttons:** An 'Apply Changes' button is located at the bottom.

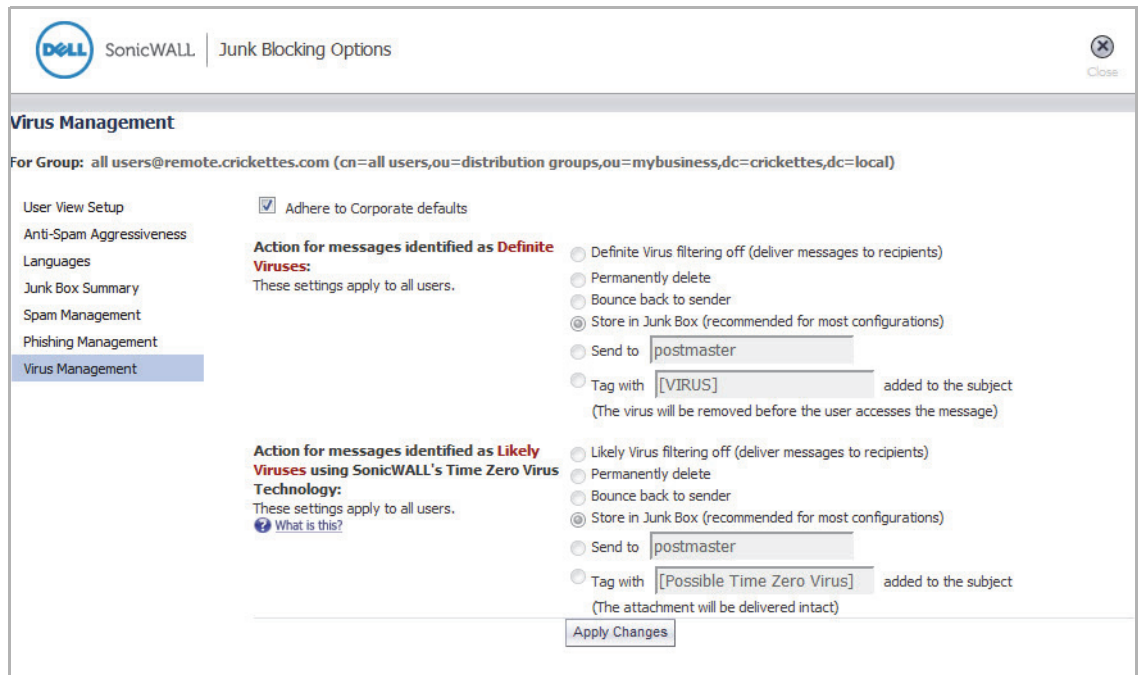
Phishing Management

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.

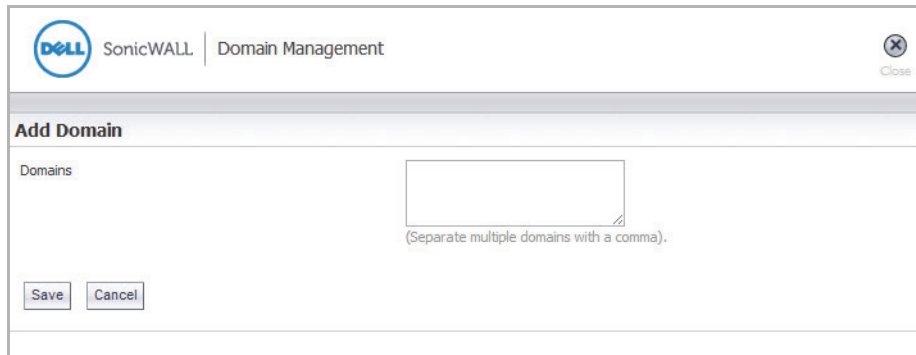


Forcing All Members to Group Settings

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 Dell 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.



The screenshot shows a web-based dialog box titled "Add Domain" within the "Domain Management" section of the Dell SonicWALL interface. The dialog has a header bar with the Dell logo, "SonicWALL", and "Domain Management". A "Close" button is in the top right corner. Below the header, the main area is labeled "Add Domain" and contains a text input field for "Domains". A small instruction "(Separate multiple domains with a comma)." is positioned below the input field. At the bottom of the dialog, there are two buttons: "Save" and "Cancel".

Roles

Roles are a set of privileges that you can grant any individual user or group of users in the Hosted 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 Hosted Email Security. Hosted 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 8

Junk Box Management

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, Dell SonicWALL Hosted 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 67](#)
- [“Junk Box—Advanced View” on page 68](#)
- [“Working with Junk Box Messages” on page 70](#)
- [“Junk Box Summary” on page 71](#)
- [“Supported Search in Audit and Junkbox” on page 73](#)
- [“Junk Box Settings” on page 74](#)
- [“Virus—Click this link to direct you to the Anti-Virus Techniques screen.” on page 75](#)

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.

The screenshot shows the 'Junk Box Management' interface. At the top, there are tabs for 'Inbound' and 'Outbound'. Below these is a 'Simple Search Mode' section with a close button. A message states: 'Items in the Junk Box will be deleted after [30 days](#).' Underneath is a 'Query Parameters' section with a search form. The form includes a text input for 'Search for:', a dropdown menu set to 'Subject', and another dropdown menu set to '---Show all---'. A note below the form says: '(Surround sentence fragments with quote marks " " for example; "look for me")'. At the bottom of the search section are buttons for 'Search', 'Settings', and 'Advanced View'.

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.

The screenshot shows the 'Junk Box Management / Junk Box' interface in 'Advanced Search Mode'. At the top, there are 'Inbound' and 'Outbound' tabs. Below them, a notification states 'Items in the Junk Box will be deleted after 30 days.' The 'Query Parameters' section includes input fields for 'To:', 'From:', 'Subject:', and 'Unique Message ID', each with a small text instruction. The 'Date' field is a dropdown menu currently set to '---Show all---'. The 'Threats' section contains two buttons, 'Check All' and 'Check None', followed by a grid of checkboxes for various threat types: Spam, Likely Spam, Virus, Likely Virus, Phishing, Likely Phishing, DHA, and Policy. All these checkboxes are checked. At the bottom, there are 'Search', 'Settings', and 'Simple View' buttons.

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**.

Advanced Search Mode

Query Parameters

To:

From:
(Separate multiple email addresses with a comma)

Subject:
(Surround sentence fragments with quote marks "" for example; "look for me")

Unique Message ID:
(Separate multiple entries with a comma)

Date:

Threats

Spam Virus Phishing DHA
 Likely Spam Likely Virus Likely Phishing Policy

Messages Found

Displaying 1 - 10 of 31896 (0.109 secs)

10 Rows << < Page 1 of 3190 > >>

<input type="checkbox"/>	To	Threat		Subject	From	Received
<input type="checkbox"/>	bd39648@easypa...	Likely Spam		You have notifications pending	member@linkedin...	02/06/2012 05:28 PM
<input type="checkbox"/>	7bniml2003@easy...	Likely Spam		Branwen Kelly sent you a message via LinkedIn	member@linkedin...	02/06/2012 05:27 PM
<input type="checkbox"/>	mable_hurley@eas...	Likely Spam		The Permanent Address for VIP Gaming	jcfmnyim@alhara...	02/06/2012 05:25 PM
<input type="checkbox"/>	bcdavid@easypay...	Likely Spam		Hayley Connor sent you a message via LinkedIn	member@linkedin...	02/06/2012 05:22 PM
<input type="checkbox"/>	howard_reeves@e...	Spam		The Permanent Address for VIP Gaming	xnaocnm@activa...	02/06/2012 05:20 PM
<input type="checkbox"/>	bell@easypaymail...	Likely Spam		Brenda ORvan sent you a message via LinkedIn	member@linkedin...	02/06/2012 05:18 PM
<input type="checkbox"/>	benad_hayden@e...	Likely Spam		Dawn Murray has sent you a message	member@linkedin...	02/06/2012 05:16 PM
<input type="checkbox"/>	ignacio_je@easyp...	Likely Spam		The Permanent Address for VIP Gaming	irfirsqwul@parasol...	02/06/2012 05:13 PM
<input type="checkbox"/>	berge30887@easy...	Likely Spam		Jacqueline Sullivan sent you a message via LinkedIn	member@linkedin...	02/06/2012 05:11 PM
<input type="checkbox"/>	camille_sanford@e...	Spam		The Permanent Address for VIP Gaming	nsilqoolsgdh@abs...	02/06/2012 05:10 PM

10 Rows << < Page 1 of 3190 > >>

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**.

Junk Box Summary

Dell SonicWALL Hosted Email Security sends an email message to users listing all the messages that have been placed in their Junk Box. The **Junk Box Management > Junk Box Summary** page allows users to 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.

Junk Box Management /

Junk Box Summary

Junk Box Summary

Users will be sent "Junk Box Summary" notification emails listing their recently quarantined messages.

Frequency Settings

Frequency of summaries:

Time of day to send summary:
 Any time of day
 Within an hour of

Day of week to send summary:
 Any day of the week
 Send summary on

Time Zone:

Message Settings

Summaries include:
 All junk messages
 Only likely junk (hide definite junk)

Language of summary email:

Send plain summary:
(no graphics)
 Plain summary
([view plain example](#) | [view graphic example](#))

Display junk statistics in summary email:

Miscellaneous Settings

Send Junk Box Summary to delegates:
(When checked, the summary email will be sent to the delegate, not to the original recipient.)

Enable "single click" viewing of messages:
 Off
 View messages only (users can preview messages without having to type their username/passwords.)
 Full access (clicking any link in a Junk Box Summary grants full access to this particular user's settings)

Enable Authentication to Unjunk:

Only send Junk Box Summary emails to users in LDAP:

To enable authentication of non ldap users: [Click here](#)

Other Settings

Email address from which summary is sent:
 Send summary from recipient's own email address
 Send summary from this email address:

Name from which summary is sent:

Email subject:

URL for user view: [?](#)

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.
4. Select the **Time Zone** from the dropdown list. Hosted Email Security will synch the selected time zone and send Junk Box Summaries accordingly.

Message Settings

5. 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.
6. Choose **Language of summary email** from the dropdown list.
7. Select the **Plain Summary** checkbox to send summaries in plain text. Leaving this checkbox unselected will send Graphic Rich Summaries. Click the links below to preview an example of a plain summary and a graphic summary.
8. Enable **Display junk statistics in summary email** by selecting the checkbox.

Miscellaneous Settings

9. 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.
10. 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.
11. Choose the **Enable Authentication to Unjunk** checkbox to make users authenticate when selecting messages to unjunk.
12. Choose to enable **Only Send Junk Box Summary emails to users in LDAP** by selecting the checkbox.
13. To **Enable Authentication for Non-LDAP Users**, click the **Click to Choose** link.

Other Settings

14. Choose the **Email address from which summary is sent**.
15. 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.
16. 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*.

17. Enter the **Email Subject** for summary messages. For example, *Summary of junk emails blocked*.
18. 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.
19. Click the **Test Connectivity** button to test that the URL connects properly. If the test fails, check that the URL is correct.
20. Click the **Apply Changes** button.

Managing Junk Summaries

Both administrators and users receive Junk Box summaries listing the incoming email that Dell SonicWALL Hosted 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

Junk Box Settings

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

Junk Box Management /
Junk Box Settings

Message Management

General Settings

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

Tag unjunked messages with this text added to the subject line: [Junk released by User action]

Tag messages considered junk, but delivered because sender/domain/list is in Allowed list with this text added to the subject line: [Junk released by Allowed List]

Tag messages considered junk, but delivered because of a Policy action with this text added to the subject line: [Junk released by Policy action]

Tag all messages processed by Email Security for initial deployment testing with this text added to the subject line: [SonicWALL Email Security]

Miscellaneous

- To set **spam** message management [click here](#)
- To set **phishing** message management [click here](#)
- To set **virus** message management [click here](#)

General Settings

Select the action the Hosted Email Security will 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.

Chapter 9

Reports and Monitoring

Hosted 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 Hosted Email Security” on page 77](#)
- [“Overview Reports” on page 77](#)
- [“Scheduled Reports” on page 86](#)

Reporting in Hosted Email Security

Dell SonicWALL Hosted Email Security provides many types of reports. All reports allow you to optionally download the data in CSV format or HTML 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 82](#)
- [“Anti-Phishing Reports” on page 84](#)
- [“Anti-Virus Reports” on page 85](#)
- [“Directory Protection” on page 85](#)
- [“Scheduled Reports” on page 86](#)

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 78](#)
- [“Inbound Good vs Junk” on page 79](#)
- [“Outbound Good vs Junk” on page 80](#)
- [“Junk Email Breakdown Report” on page 81](#)
- [“Top Outbound Email Senders” on page 82](#)

Reports Dashboard

The **Reports & Monitoring > Overview Reports > Dashboard** provides a lot of information about Hosted 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.



The following reports are displayed on the **Dashboard** page:

Inbound Good Email vs Junk Email

Displays the number of Good Inbound 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).

Junk Email Breakdown

Displays the percentage and numeric breakdown of the various categories of junk received, including Spam, Likely Spam, Viruses, Likely Viruses, Phishing, Likely Phishing, Policy Events, Directory Harvest Attacks (DHA), and Connection Management (CM).

Spam Caught

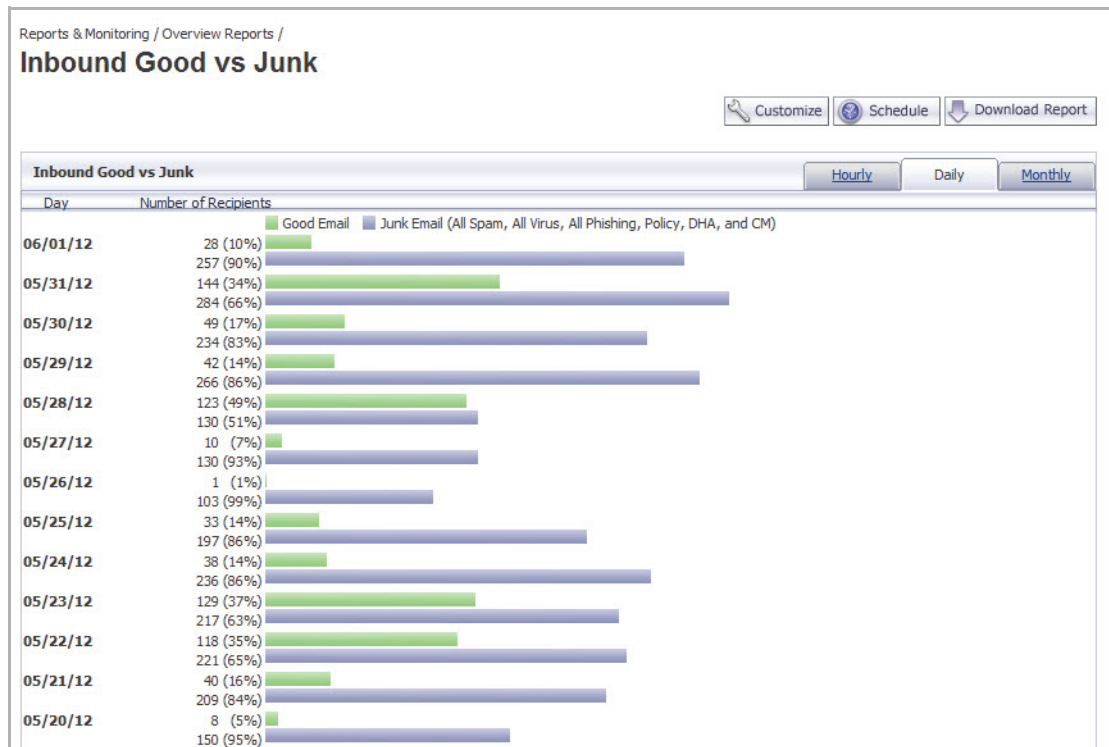
Displays the number of email messages that are Definite Spam compared to the number of messages that are Likely Spam. The information on this chart can also be found in the **Anti-Spam Reports > Spam Caught** report.

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

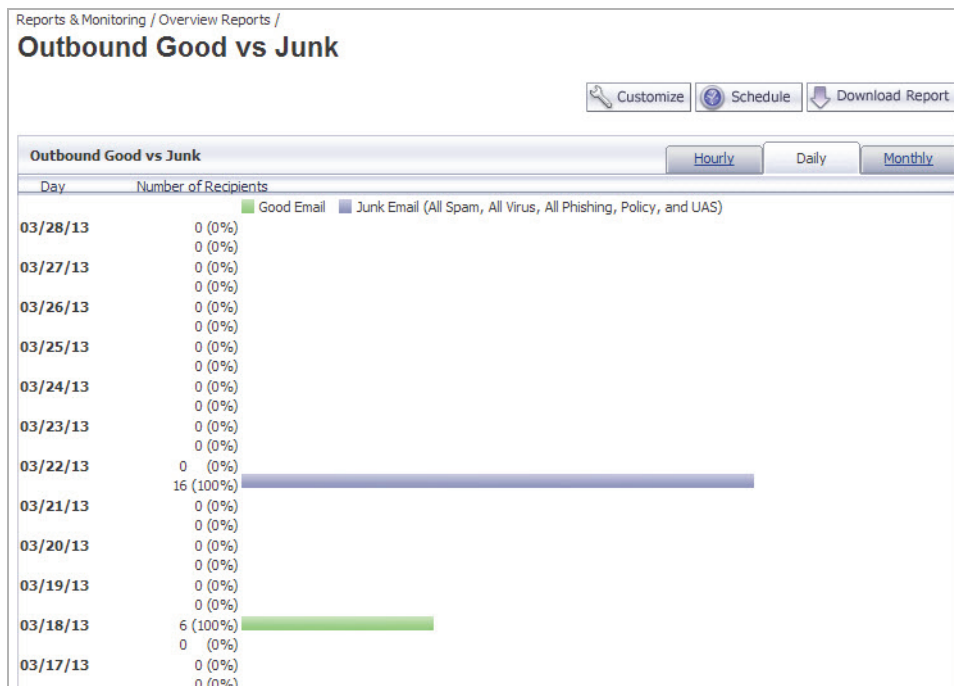
This page displays the total number of inbound messages processed by Hosted Email Security along with the total number of junk messages versus good messages.



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.

Outbound Good vs Junk

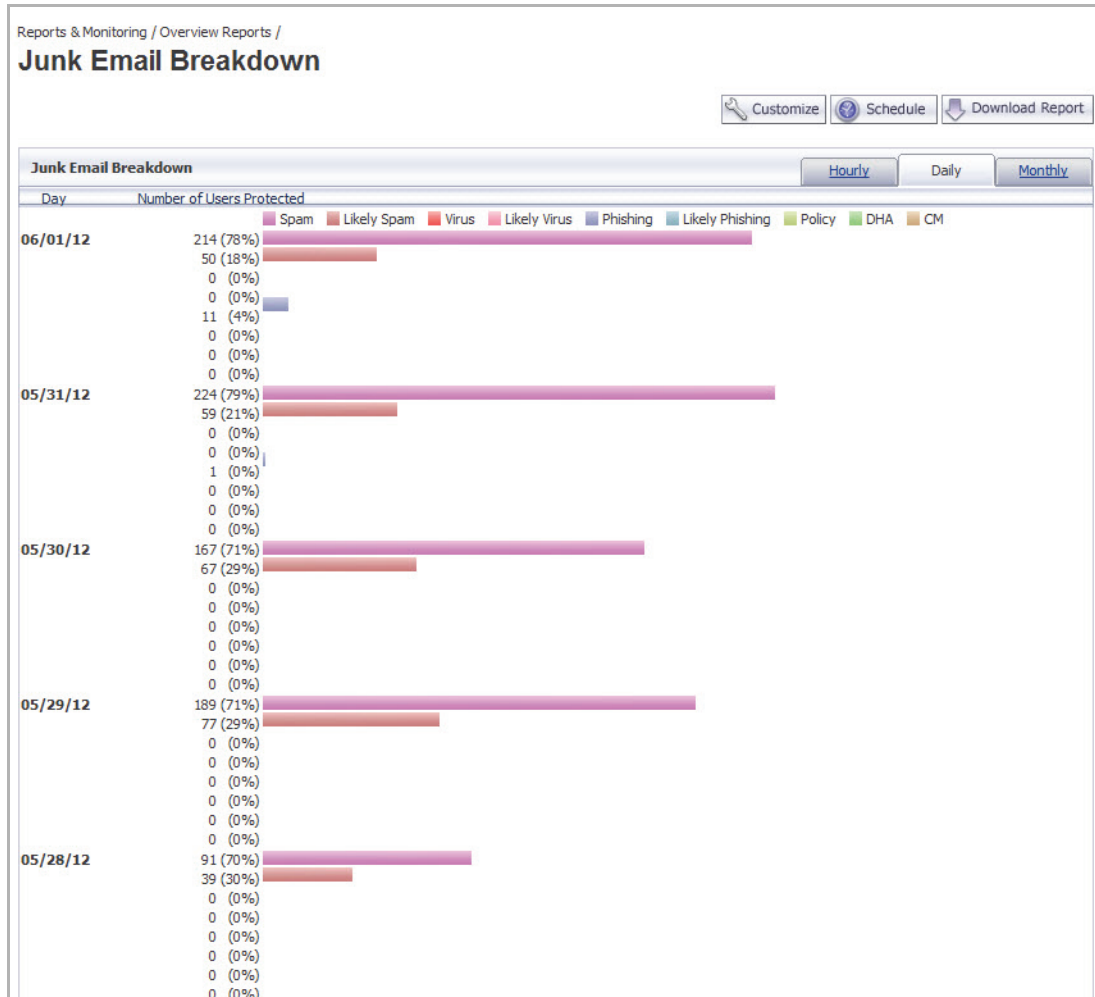
This page displays the number of Good Outbound Email messages processed by Hosted Email Security along with the total number of junk messages and good messages.



You can view the Outbound 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

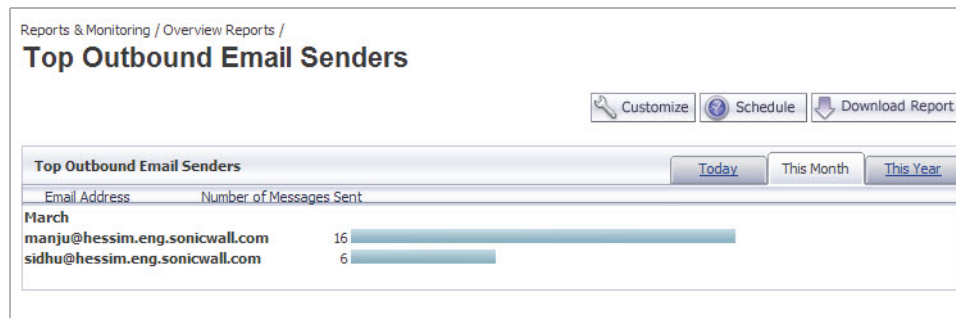
This report gives a percentage and numeric breakdown of the various categories of junk received, including Spam, Likely Spam, Viruses, Likely Viruses, Phishing, Likely Phishing, Directory Harvest Attacks (DHA), and Connection Management (CM).



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.

Top Outbound Email Senders

This report displays the email addresses of users in your organization who send the most outbound email messages in a given time period.

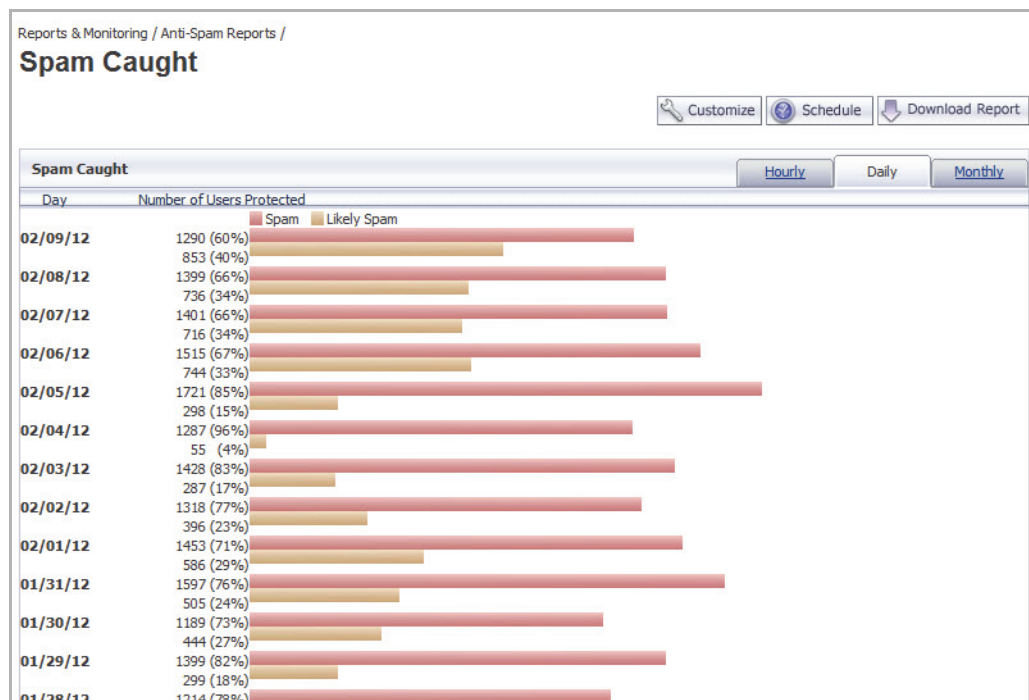


Anti-Spam Reports

The **Reports & Monitoring > Anti-Spam Reports** page provides two reports specific to the category of Anti-Spam: Spam Caught and Top Spam Recipients.

Spam Caught

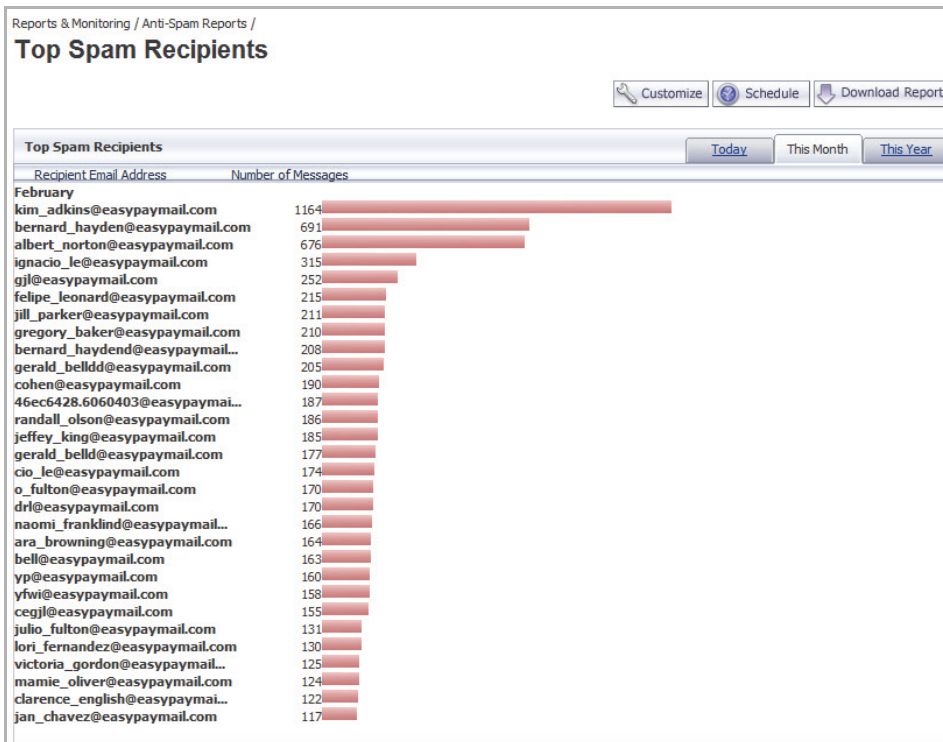
The Spam Caught report displays the number of messages filtered by Hosted Email Security that are definitely Spam compared to the amount that are Likely Spam. This report also gives a percentage breakdown.



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.



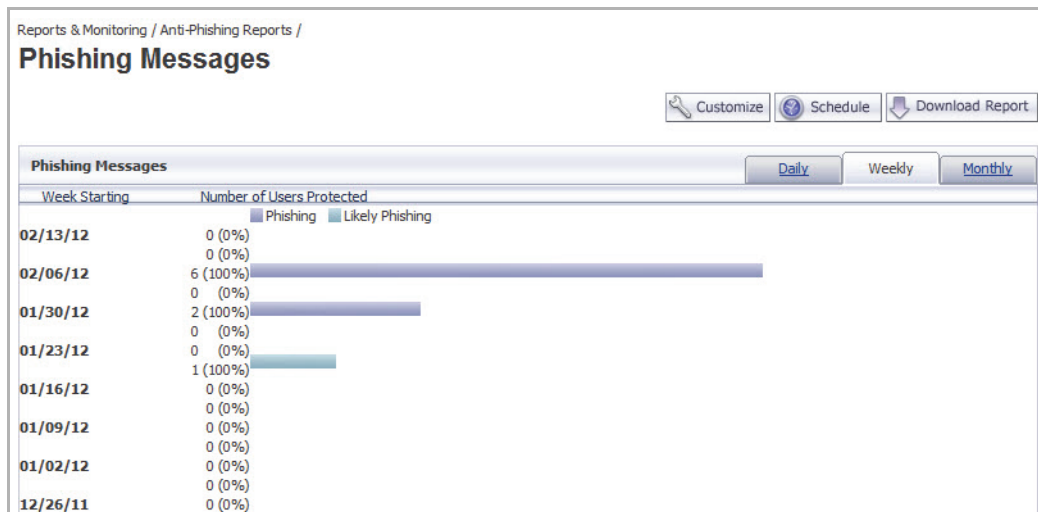
You can view the Top Spam Recipients report by specific time periods. Click the **Today**, **This Month**, or **This Year** tabs to view data for each period. By default, the **This Month** tab displays.

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. Navigate to the **Reports & Monitoring > Anti-Phishing Reports** page to see the Phishing Messages report.

Phishing Messages

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



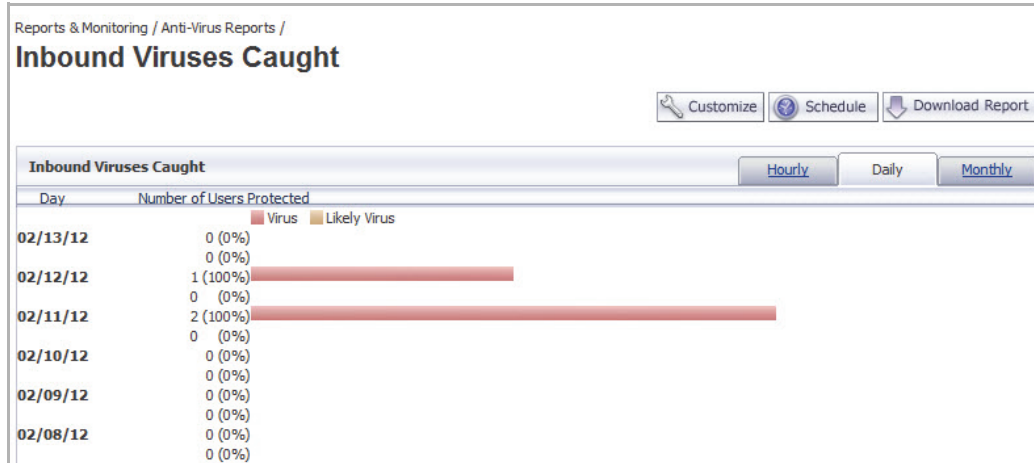
You can view the Phishing Messages by specific time periods. Click the **Daily**, **Weekly**, and **Monthly** tabs to view the data for each period. By default, the **Weekly** tab displays.

Anti-Virus Reports

The **Reports & Monitoring > Anti-Virus Reports** page allows you to view the number of viruses detected by the Hosted 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

Hosted 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. Navigate to the **Reports & Monitoring > Number of DHA Attacks**

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

Hosted Email Security allows you to schedule email delivery of reports. The **Reports & Monitoring > Scheduled Reports** page allows you to 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.

The screenshot shows the 'Custom Reports' dialog box in the Dell SonicWALL interface. The dialog box is titled 'Dell SonicWALL Custom Reports' and includes a 'Help' icon and a 'Close' button. The main content area is divided into several sections: 'Which report:' with a dropdown menu showing 'Inbound Viruses Caught'; 'Date range:' with 'Start date:' (04/01/2012) and 'End date:' (06/01/2012) dropdowns; 'List results by:' with a dropdown menu showing 'Day'; 'Delivery:' with radio buttons for 'Display' (selected) and 'Email to' (with an empty text field); 'Name from which report is sent:' with a text field containing 'admin@crickettes.com'; 'Email address from which report is sent:' with a text field containing 'admin@crickettes.com'; and 'Subject:' with an empty text field. At the bottom are 'Generate This Report' and 'Cancel' buttons.



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 Dell SonicWALL Hosted Email Security site.

Add Scheduled Report

You can add a Scheduled Report by clicking the **Add New Scheduled Report** 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.
- **Time Zone**—Select a time zone from the list provided.
- **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.

The screenshot shows a dialog box titled "SonicWALL | Add Scheduled Report". It contains the following fields and options:

- Which report:** Junk Email Breakdown (dropdown)
- Frequency of report email:** 1 Day (dropdown)
- Time of day to send report:** Any time of day, Within an hour of 12 AM (dropdown)
- Day of week to send report:** Any day of the week, Send report on Monday (dropdown)
- Time zone:** Please select a time zone... (dropdown)
- Language of report email:** English (dropdown)
- Report has data for the last:** 1 Day (dropdown)
- Report lists results by:** Hour (dropdown)
- Name from which report is sent:** (text input)
- Email address from which report is sent:** (text input)
- Recipients of report email:** (text input)
(Separate multiple email addresses with a comma)
- Report shows email sent to these domains:** (text input)
(Separate multiple domains with a comma. If left blank, the report will show email sent to all domains.)
- Report name:** (text input)

Buttons at the bottom: Save Scheduled Report, Cancel

Download Report

You can instantly download the all the reports from the **Reports & Monitoring** page 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.

