SonicWall ® Hosted Email Security 10.0

Administration Guide

SONICWALL®

Contents

Part 1. Introduction

Part 2. Monitor

Part 3. Investigate

Part 4. Manage

Part 1

Introduction

- Introduction to Hosted Email Security

1

Introduction to Hosted Email Security

Welcome to *SonicWall Hosted Email Security*. This Administration Guide provides information about configuring and using the different features for all facets of the SonicWall Hosted Email Security product.

SonicWall Hosted Email Security is a cloud-based email security solution that can help you safeguard your data and meet compliance requirements. It can help protect your organization from outside attacks with effective virus, zombie, phishing and spam blocker by leveraging multiple-threat detection techniques. It can also help you better understand email usage, archive for compliance, efficiently perform e-discovery, and audit all mailboxes and access controls to prevent violations.

More information is provided in the following sections:

Topics:

Description of Email Security

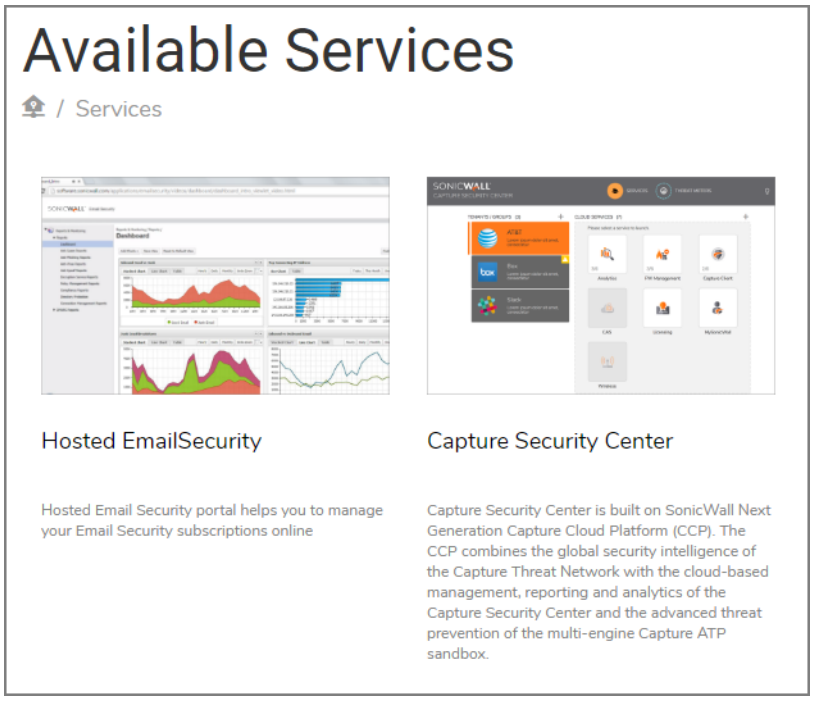
Email-based communications are fundamental to effectively conduct business. Given the volume of worldwide emails and the continued growth each year, email continues to be a popular vector for a variety of threats. It offers hackers a vehicle to deliver a variety of vulnerabilities. These threats require a new set of features for detection and protection. SonicWall Hosted Email Security deploys a multi-layer solution dedicated to combating emerging threats.

Advanced Threat Protection	Helps protect against ransomware and unknown malware that requires a sandbox to detect and protect against attacks.
Known Threat Protection	Screens malicious inbound emails using known anti-virus signatures and prevents your employees from sending viruses with outbound email. Using multiple virus-detection engines can improve coverage.
Phishing Protection	Incorporates advanced content analysis and dynamic blacklists to filter emails with malicious links.
Fraud Protection	Takes advantage of mail configurations such as SPF, DKIM and DMARC—along with pattern recognition and content analysis—to enforce validation of incoming messages.
Spam Protection	Uses multiple methods like allowed and blocked lists, pattern recognition and the ability to enable third-party blocked lists.

Data Loss Prevention	Allows encryption of sensitive emails and attachments for protection.
Time-of-Click URL Malware Protection	URL filtering mechanism checks malicious URLs in email messages when users on their endpoints click on them rather than at the time they are delivered.
HTTPS Strict Transport Security (HSTS) Implementation	Redirects web browsers to only use HTTPS to access websites. HSTS is automatically enabled. It allows web servers to enforce the use of Transport Layer Security and the browsers only access sites using HTTPS safely.
LDAP User Role Administration	Anonymous users now only access Email Security by using legitimate user and administrator roles, which determine which features they could access and tasks they can perform.
Remote Drive Mount Settings	You are now allowed to mount remote folders from a remote server that supports **NFS** protocol besides **CIFS** protocol.
New UX / UI Changes	New user experience and user interface changes. The Email Security website skin matches the SonicWall style and color theme. New icons appear on the left navigation panel aided by an orange slider ball to indicate your spot.

Capture Security Center

SonicWall Capture Security Center now integrates Hosted Email Security. You can access the service by clicking on the Hosted Email Security tile from the CSC. You need to have a MySonicWall account to access the CSC. Sign up for an account by going to https://mysonicwall.com/muir/login/step2 and click on **Sign Up**.



To enable Capture Cloud:

1 Navigate to https://mysonicwall.com/muir/login/step2 and login using your MySonicWall credentials.

2 Select the MySonicWall tile.

3 On the MySonicWall Dashboard, click on the Add Product icon.

4 Enter the serial number and click Continue.

5 Provide the Friendly name and the Authentication code.

6 Select the Product group from the drop-down menu.

7 Click Register.

> **NOTE:** Firewalls that are managed with these services require that **Comprehensive/Advanced Gateway Security Suite** (CGSS/AGSS) be enabled. It it is not enabled, navigate to MySonicWall to license it.

> **NOTE:** If you want to take advantage of Zero Touch Deployment, be sure your firewall is running SonicOS 6.5.1.1-42n or newer. The Zero Touch functionality does work with lower level firmware.

8 Once registered, select the new firewall and expand the Product Details tab.

9 Enable Zero Touch for this product.

10 Return to the Capture Security Center by clicking on the down arrow at the top of the page.

11 Select **Licensing** from the Capture Security Center.

12 Find the firewall that you are licensing and click on **Try** to activate Analytics. Wait a for seconds until you see the green confirmation at the bottom of the screen.

13 Return to the Capture Security Center by clicking on the down arrow at the top of the page. The tiles associated with your cloud services license are now active and not grayed out.

14 Select the **Management**, **Reports**, or **Analytics** tile to continue with managing the firewall or accessing data.

Provisioning Capture Client

To provision the Capture Client:

1 Select **MySonicWall** from the Capture Security Center.

2 Navigate to **Product Management > My Products**.

3 Select the **+** icon to **Add Client Licenses**.

4 Enter a name for the **Client License Group**. The name may be up to 30 characters.

5 Click **Confirm**.

6 In the newly created product, click on the **LICENSES** tab,

7 Scroll down to Capture Client. You may need to scroll down using the inside scroll bar.

8 Click on the Key icon for Capture Client Advanced Protection to activate the service.

9 Enter the activation key provided by your SonicWall representative.

10 Click Submit.

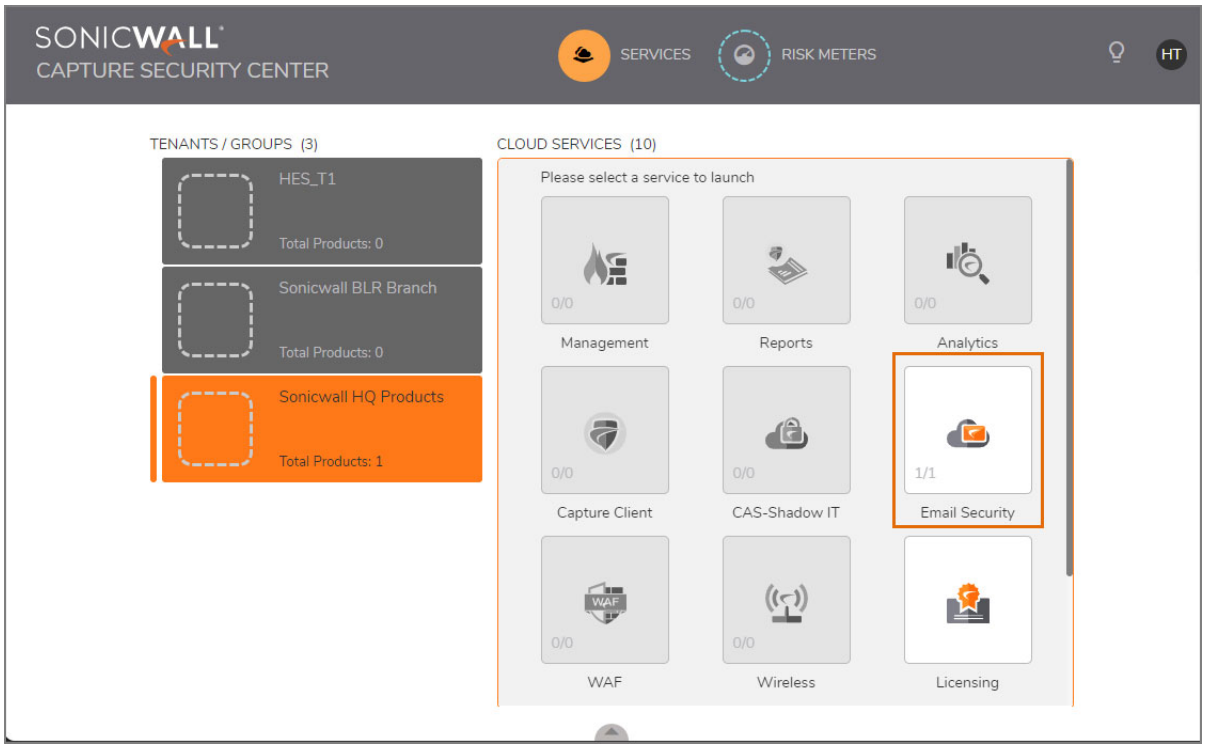
11 Click on the link for Capture Client Advanced Protection.

12 Select Click here to access the Security Center. This redirects you to the Capture Client Management Console for login.

Logging in to Capture Security Center

When you log in to the Capture Security Center client user interface, click on the Hosted Email Security tile to land on the Hosted Email Security user interface. Hosted Email Security is supported on the CSC-MA XX platform.

NOTE: Hosted Email Security requires that certain ports be left open to operate correctly. Refer to the *SonicWall Hosted Email Security 10.0 Release Notes* for the most recent list.



Available Module Licenses

Hosted Email Security (HES) is licensed through simplified bundles. The following are the options available:

Hosted Email Security Essentials	Essentials bundle includes Anti-Spam, Anti-Virus, Anti-Phishing, AntiSpoofing, DLP and Compliance, Email Continuity, Software Updates, and 24*7 Support.
Hosted Email Security Advanced	Advanced bundle includes Anti-Spam, Anti-Virus, Anti-Phishing, AntiSpoofing, DLP and Compliance, Email Continuity, Capture Advanced Threat Protection (ATP) for zero-day malware, Time-of-Click URL protection, Software Updates, and 24*7 Support.
Email Encryption (add-on)	Email Encryption are add-on licenses which can be added to the Essentials or Advanced bundle. Email Encryption enables secure exchange of sensitive and confidential information.

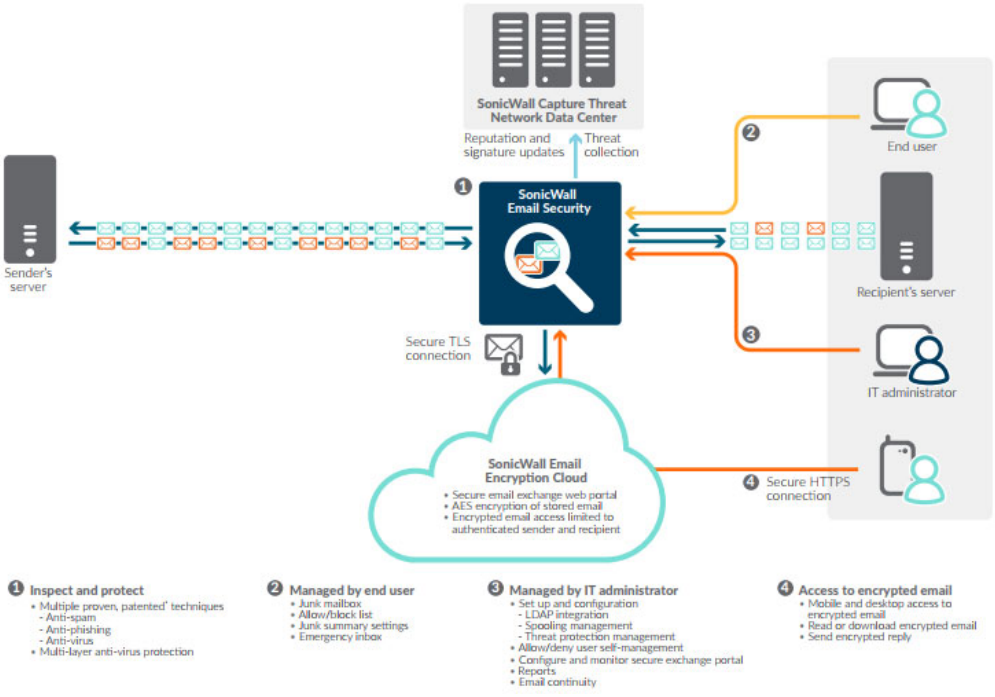
Hosted Email Security Overview

SonicWall Hosted Email Security offers superior, cloud-based protection from inbound and outbound threats, including ransomware, phishing, business email compromise (BEC), spoofing, spam and viruses, at an affordable, predictable and flexible subscription price. At the same time, it minimizes upfront deployment time and costs, as well as ongoing administration expenses.

SonicWall Hosted Email Security includes advanced compliance scanning, management and, optionally, email encryption to prevent confidential data leaks, regulatory violations and to ensure the secure exchange of sensitive data. Policies may be configured at the organizational level, to scan outbound email content and attachments for sensitive data and route email for approval or encryption. Encrypted email can be tracked to confirm the time of receipt and time opened. A notification email is delivered to the recipient's inbox with instructions to simply log into a secure portal to read or securely download the email.

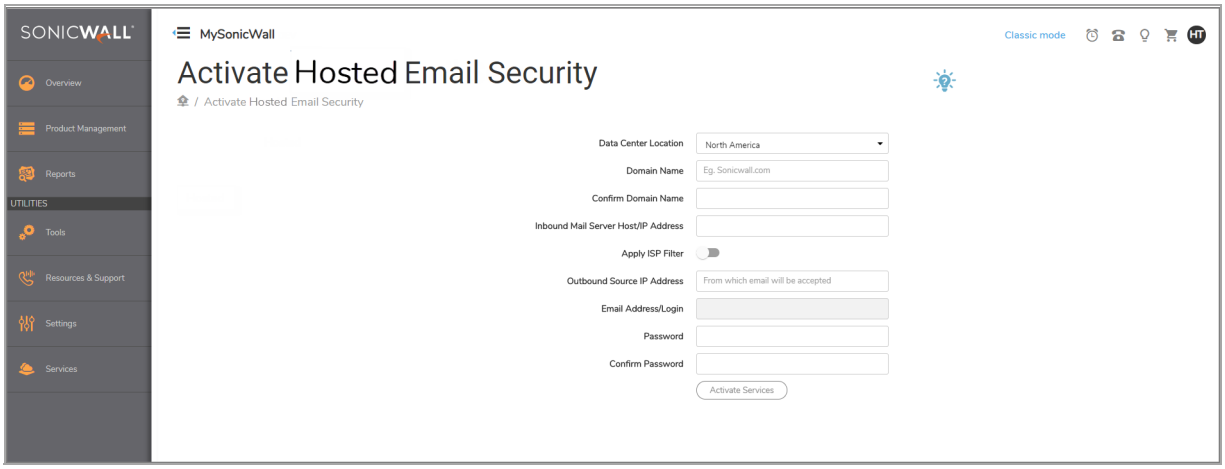
Other features include integration with Capture Advanced Threat Protection (ATP) and Email Continuity. Capture ATP gives you an effective and responsive defense against ransomware and zero-day attacks. Email Continuity provides cost-effective protection against planned or unplanned downtime events, whether your email servers are on-premises, hybrid environments or in the cloud.

Hosted Email Security is cloud-based, with no additional client software necessary. Unlike competitive solutions, the encrypted email may be accessed and read from mobile devices or laptops.



Activating the Hosted Email Security Service

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



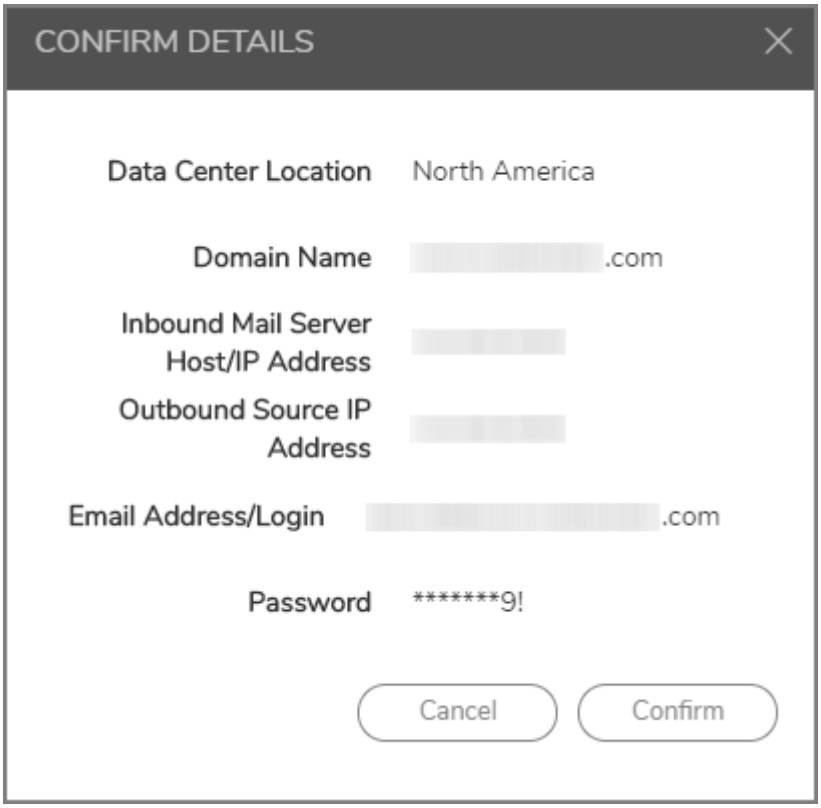
1 Specify the following fields, then click **Activate Services**:

- **Select the location of your Data Center. North America** or **Europe**.

NOTE: You cannot change this option once it has been specified.

- **Domain Name**—The primary domain name that is associated with your SonicWall Hosted Email Security solution.
- **Confirm Domain Name**—Example: SonicWall.com
- **Inbound Mail Server Host / IP Address**—The IP address of the mail server hosting your user mailbox(es) for inbound messages.
- **Apply ISP Filter**—Only the ISP selected can connect and relay through this path.
- **Outbound Mail Server Host / IP Address**—The outbound IP address of your Hosted Email Security solution. For example, if you registered the domain name soniclab.us.snwlhosted.com, then the Outbound Mail Server Host is soniclab.outbound.snwlhosted.com.
- **Email Address / Login**—The email address or login name associated with your Hosted Email Security account.
- **Password**—The password associated with your Hosted Email Security account.
- **Re-enter Password**—The password you entered in the previous field.
- **Confirm Password**—Re-enter your password.
- Click the **Activate Services** button. A message displays confirming successful activation and product registration.

2 Click the **Confirm** button on the **CONFIRM DETAILS** popup dialog box.



A message displays confirming successful activation and product registration.

Managing Your Product

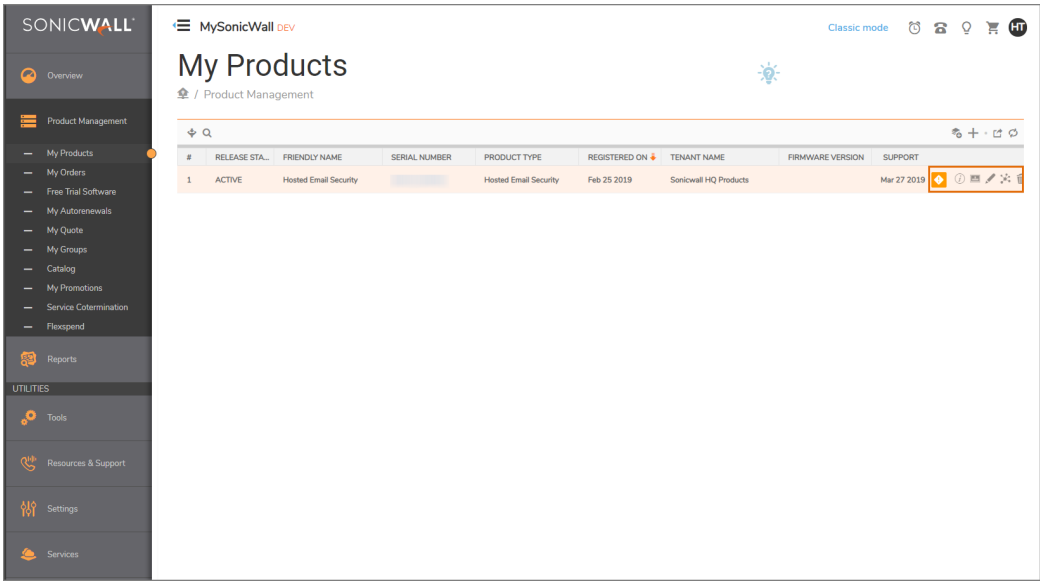
To manage your Hosted Email Security product:

1 Navigate to **Product Management > My Products** on the side menu to see your Hosted Email Security purchase. The **My Products** table gives you information about your product in columns described below:

- **RELEASE STATUS**—Shows your product is ACTIVE.
- **FRIENDLY NAME**—Shows your product name.
- **SERIAL NUMBER**—Shows the unique identifier assigned to your product.
- **PRODUCT TYPE**—Shows your product kind.
- **REGISTERED ON**—Shows the date you registered your product with SonicWall.
- **TENANT NAME**—Shows that your product is based under **SonicWall HQ Products**.
- **FIRMWARE VERSION**—Shows firmware version if applicable.
- **SUPPORT**—Shows the date of the last support service.

2 Hover over your purchase product row in the **My Products** table to **Enter the User Name and Password** you configured in the Activation process.

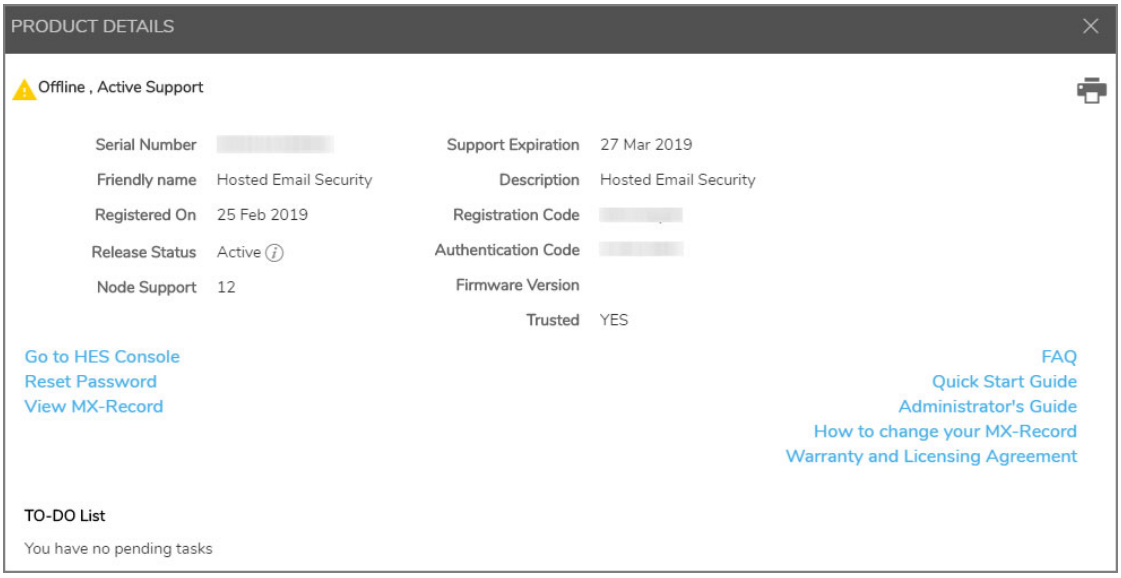
3 Click Log In.



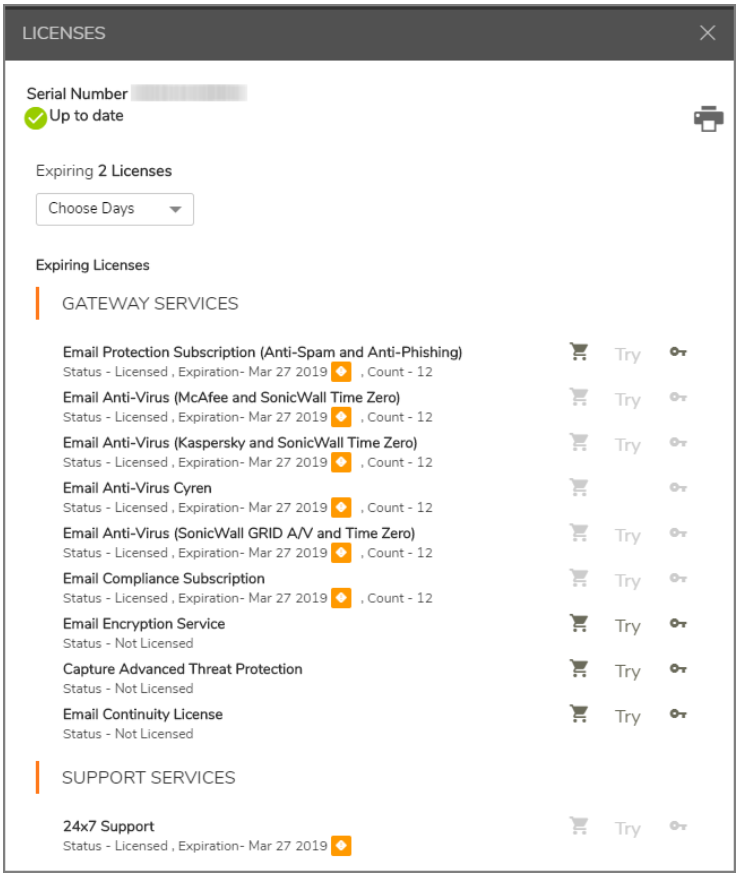
4 Use the six icons on the top right of the **My Products** table to learn more about your Hosted Email Security.

5 Click on the orange diamond icon, with the exclamation mark, to learn about your 24x7 customer support expiration date.

6 Click on the information icon to see your **PRODUCT DETAILS**.



7 Click on the **Licenses** icon to see your LICENSES.

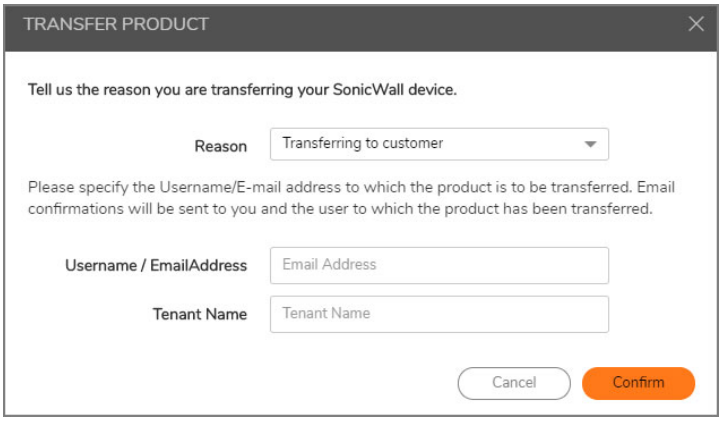


8 Rename your product, if you want, by clicking on the pencil icon.

9 Click **Confirm** after you give your Hosted Email Security product a **friendly name**.

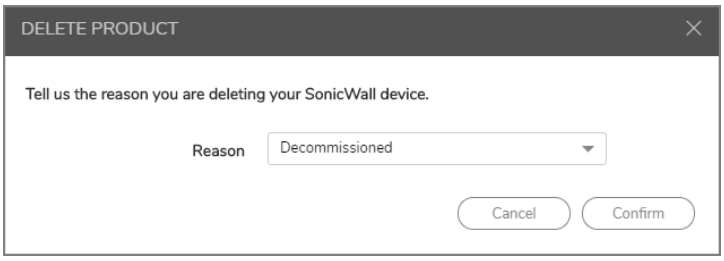
10 Click on the transfer icon to transfer your product to another username and email address.

NOTE: Email confirmations are sent to you and the user to which the product has been transferred.



11 Click **Confirm** to finish the transferring of your product.

12 Click the **Delete** icon to delete your SonicWall product.



13 Select your reason for wanting to delete your product from the drop-down list next to **Reason**. You have five choices:

- Decommissioned
- Returned
- Upgraded to newer SonicWall
- Other (please specify)

14 Click **Confirm** when done.

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 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 *example.com*. Since the SonicWall Data Center hosts *snwlhosted.com*, the domain then becomes *example-com.snwlhosted.com*. After an MX record is created, where the customer publishes example.com MX *example-com.snwlhosted.com*, SonicWall then publishes an A-record: *example-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: *example.com.outbound.snwlhosted.com A 173.240.21.200.*

For outbound email messages, you need to configure the mail server hosting your user mailboxes for outbound messages to route all outbound emails to *example.com.outbound.snwlhosted.com*.

For more information regarding MX records, contact your ISP or refer to the Knowledge Base article titled, How to set up your MX record after you activated Email Security Hosted Solution.

Logging into the Hosted Console

After completing the activation process, click the **Go to Hosted 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 **Email address** and **Password** you configured during the Activation process, then click **LOGIN**.

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

Part 2

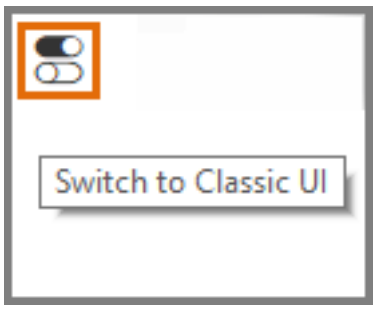
Monitor

- Dashboard

2

Dashboard

On the default **MONITOR** view, the **Dashboard** summarizes Hosted Email Security at a glance. Hosted Email Security supports a toggle at the top right corner of the page that allows you to see the new interface by default and opt for the classic interface if you want.



The Dashboard also includes interactive charts that are updated hourly. They display the statistics for the last 24 hours and the views for each report can be customized. The reports are grouped into collections based on the organization shown in the left navigation pane, or you can put any report into any collection.

- Using the Reports
- Dashboard
- Event Summaries
- Policy and Compliance Reports
- Appliance Health and LDAP Users

Using the Reports

The reports shown on the **MONITOR** view can be managed and customized in a similar way across all the options.

Topics:

- Navigation
- Customizing Chart Views
- Filtering Chart Data

Navigation

Navigate to **MONITOR | Event Summaries** to see the buttons you can use to manage and customize the reports shown for each of the options.

Button	Function
Add Charts	Allows you to add charts to be displayed. Click on the down arrow to select the report category, and then click on the report name you want to add. **Note:** You can only add Dashboard reports to the Dashboard view, Anti-Spam reports to the Anti-Spam view, and so forth.
Save View	Saves the view after you configured or made adjustments to your settings.
Reset to Default View	Resets the report view to the default settings.
Customize	Opens **Custom Reports** page so you can define the parameters for any report displayed. 1 Select the report to customize. 2 Specify the date range for the report. 3 Select the units for how you want to list results: by the hour, day, week or month. 4 Enter the domains in the text field for **Report shows email sent to these domains**. Separate multiple domains with a comma, if left blank the report shows email sent to all domains. 5 Select delivery method. Choose **Display** to show data on the dashboard. Choose **Email to** send the report to someone and provide the email address for the report recipient. 6 If you selected **Email to**, provide the following information in the text fields: • Name from which report is sent • Email address from which report is sent • Subject 7 Select **Generate This Report**.
Refresh Reports	Refreshes the data in the charts.

NOTE: The **Overview | Dashboard** option is not customizable so these buttons do not appear in those tables.

Customizing Chart Views

Each of the charts can be moved up and down or left and right in the display. Simply drag-and-drop the chart wherever you want it. You can also customize the data displayed in the charts by using the options provided. Select the tabs across the top of a chart to set the format and contents as described below:

To set the data style:	Select the data format you want: Some data can be presented in **Stacked Chart**, **Line Chart**, or **Table** form. • Some data can only be presented in **Bar Chart** or **Table** form. • Select the tab for the style of data you want.
To set the time style:	Select one of the following: • **Hourly** • **Daily** • **Monthly**
To zoom:	Use the mouse to draw a box around the segment you want to zoom in on and the display adjusts to show only that portion of the data.
To undo zoom:	Click the **Undo Zoom** button to reset the view in that chart to the default setting. You might have to click the right-arrow to scroll over and make the **Undo Zoom** button visible.
To download data:	Click the download arrow to allow you to download the chart in **PDF**, **JPEG**, or **CSV** formats.
To minimize or open the chart:	Use the double arrow head to minimize the chart when arrows are pointing up and opens the chart when the arrows are pointing down.
To close a chart and remove it from the view:	Click the close (X) button.

Filtering Chart Data

Since some charts display several types of data in a single view, you can customize what data shows in the charts. Click on an item listed in the legend. That item becomes grayed out and the data is removed from the display. To restore that item to the chart or table, click on the grayed out item and the data is returned.

Managing Table Formats

If you choose to show a table instead of a chart, use the following options to customize how the data is displayed, sorted or filtered.

Topics:

- Configuring Data Table Formats
- Sorting
- Search Filters

Configuring Data Table Formats

Most of the tables in the **MONITOR** view can be configured by selecting which columns of data to show and which columns to omit.

To define the columns of data to display:

1. Go to any heading in a table and click on the down arrow to see the drop box.
2. Navigate to **Columns** to see what columns of data are available for that table.
3. Check the box by those columns you want to appear and uncheck the boxes you want to hide. The table reconfigures itself in response to each action.

Sorting

The columns in the data table can be sorted in sorted in ascending or descending order.

To sort a column:

1. Click in a the column you want to sort. A small arrowhead appears in the column. The arrowhead points up to indicate ascending order and down to indicate descending order.
2. Click in the column again to change the direction of the arrowhead. The data refreshes immediately to reflect the choice you made.

In the drop-down menus for the column headings, you can also chose **Sort Ascending** or **Sort Descending**.

Search Filters

Search filters have been integrated into the reporting tool so you can show just part of the data. Filters can be applied to multiple columns, but not all columns have the option to be filtered. The filtering is performed directly on the data that's displayed.

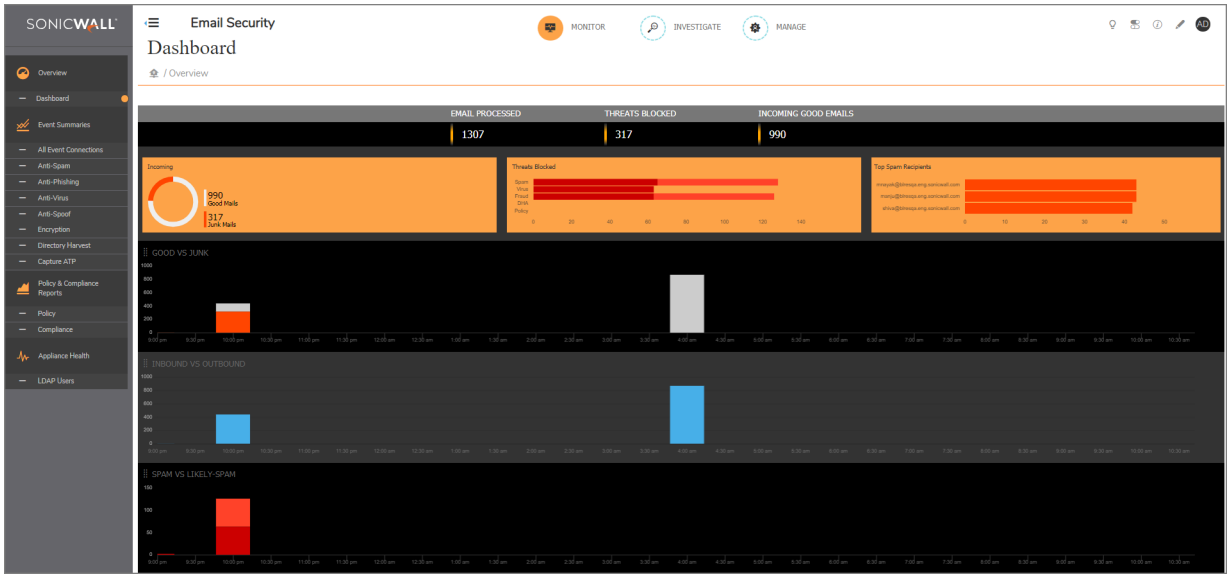
To filter data in a column:

1. Select the down arrow next to the column title.
2. Highlight the **Filter** option.
3. Depending on the options provided, do one of the following:
   - Type in a string of text to filter on.
   - Choose one or more filters from a list of pre-populated options.

   The results of any filtering are immediately shown in the data table.

Dashboard

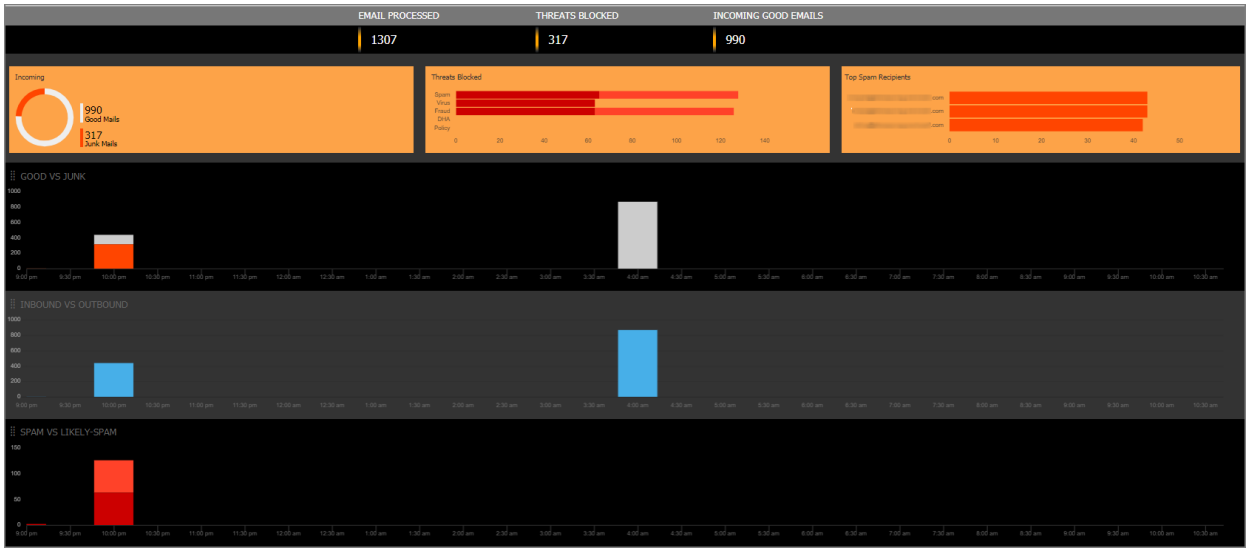
The **Dashboard** displays a series of reports that show at a glance what Hosted Email Security is doing. You can customize the **Dashboard** view by adding or deleting charts or by customizing how the data is displayed. The predefined reports are divided into three categories: **EMAIL PROCESSED**, **THREATS BLOCKED**, and **INCOMING GOOD EMAILS**. For a description of the Dashboard reports refer to the image and table below.



NOTE: You can add reports from any of the other categories to the **Dashboard** view.

Dashboard Reports

Report Name	Description
Email Processed	Displays the email that Hosted Email Security processed for all of your domains.
Incoming Good Emails	Displays the number of good messages versus junk messages received in an hour in **inbound** email traffic. Junk is comprised of spam, likely spam, phishing, likely phishing, viruses, likely viruses, policy events, Directory Harvest Attacks (DHA), and rejected connections. Rejected connections are those that Hosted Email Security deliberately drops because of IP reputation and other issues.
Threats Blocked	Displays the total number threats processed by Hosted Email Security. Threats are broken down into the following categories: • Spam (Confirmed Spam and Likely Spam) • Virus (Virus and Likely Virus) • Fraud (Confirmed Fraud and Likely Fraud) • Directory Harvest Attacks (DHA) • Policy **NOTE:** The Threats Blocked breakdown chart displays only those categories of email that your organization filters.
Top Connecting IPs	Displays the IP addresses accessed by most of the users in your organization.
Top Spam Recipients	Displays the top spam per recipients.
Good vs. Junk	Displays the number of good vs junk email messages.
Inbound vs. Outbound	Displays the number of inbound email messages compared to the number of outbound email messages. This chart is displayed only if the Outbound Module is licensed.
Spam vs. Likely Spam	Displays the number of spam email messages compared to the number of likely spam email messages.



Event Summaries

Event Summaries provides several predefined groupings. Each of these groupings can be customized to suit your needs as described in Using the Reports.

Topics:

- All Event Connections
- Anti-Spam
- Anti-Phishing
- Anti-Virus
- Anti-Spoof
- Encryption
- Directory Harvest
- Capture ATP

All Event Connections

Hosted Email Security provides connection management to reduce the traffic your system must analyze and automatically rejects connections from bad IP addresses. The **All Event Connections** report displays the countries where the most spam comes from and the volume of connections for each in the **Top Spam Countries** report.

Anti-Spam

Hosted Email Security provides the following reports specific to the **Anti-Spam** function:

Anti-Spam Reports

Report Name	Description
Spam Caught	Displays the number of email messages that are Definitely Spam compared to the number that are Likely Spam.
Top Spam Recipients	Displays a list of the email addresses in your organization that receive the most spam.

Anti-Phishing

The **Phishing Messages** report displays the number of messages identified as **Phishing Attacks** and **Likely Phishing Attacks**.

Anti-Virus

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

Anti-Spoof

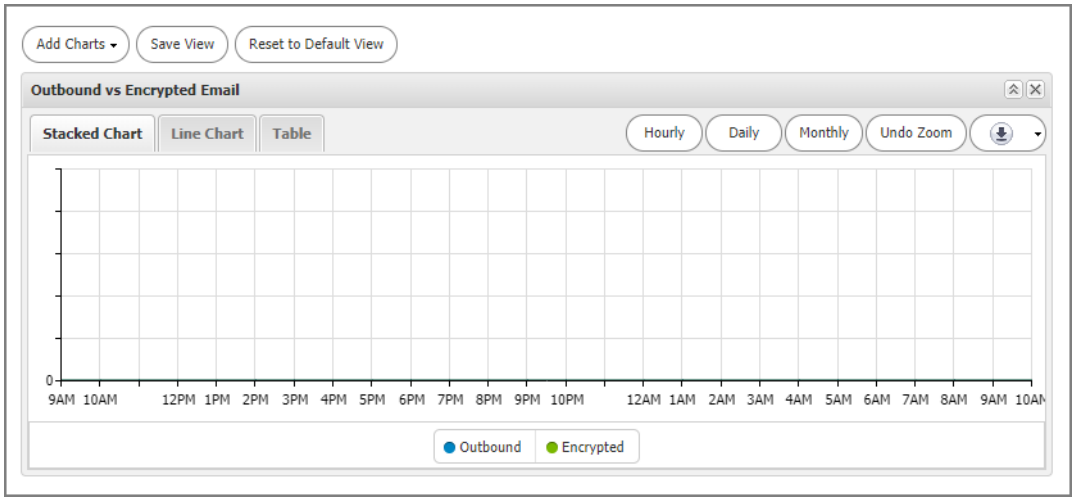
The Anti-Spoof reports provide summary and detailed reports on the types of anti-spoof messages detected.

Anti-Spoof Reports

Report Name	Description
Likely Spoof Messages	Displays the total number of Likely Spoof messages caught in inbound email traffic.
Likely Spoof Message Breakdown	Shows the breakdown of the Likely Spoof messages according to the categories used to detected them in the inbound email traffic.
SPF Breakdown	Shows the breakdown of Likely Spoof messages that were detected using SPF parameters.
DKIM Breakdown	Shows the breakdown of Likely Spoof messages that were detected using DKIM parameters.
DMARC Breakdown	Shows the breakdown of Likely Spoof messages that were detected using SPF and DMARC parameters.

Encryption

The **Outbound vs Encrypted Email** report displays the total number of outbound messages and messages sent as [SECURE] through the Encryption Service.



Directory Harvest

SonicWall Hosted Email Security provides protection against directory attacks. The directory protection reports give more information on the directory attacks targeted towards your organization.

Directory Harvest Reports

Report Name	Description
Number of Directory Harvest Attacks (DHA)	Shows the number of DHAs and the number of invalid recipients.
Top DHA Sending Domains	Shows the top DHA sending domains.

Capture ATP

The Capture ATP reports provide data about the quantity and types of files scanned.

Capture ATP Reports

Report Name	Descriptions
Total Files Scanned	Shows the total number of files sent to and scanned by Capture ATP. The data is displayed as a function over time.
File Types Scanned	Shows the types of files that Capture ATP scanned. These might include archives, binary files, scripts, images or media files. Data is presented as a percentage of total file count.
Malicious File Types	Shows the kinds of malicious files Capture ATP identified. Each type is presented as a percentage of the total number of malicious files identified.
Top Malicious URLs	Shows the top malicious URLs found by deep ULR inspection. Capture ATP. The data is displayed as a function over time.
Top URLs Analyzed	Shows the total number of URLs analyzed by deep URL inspection over time.
Malicious URLs Caught	Shows the kinds of malicious URLs that deep ULR inspection identified.
Total URLs Clicked	Shows the total number of URLs clicked over time.
Malicious URLs Clicked	Shows the kinds of malicious URLs Capture ATP identified.
URLs Rewritten	Shows the total number of URLs that are rewritten over time.

Policy and Compliance Reports

The pre-configured reports grouped in **Policy and Compliance Reports** show data comparison processed through policies and compliance.

Topics:

- Policy
- Compliance

Policy

The **Policy** group includes the reports that are relevant to policy filters in Hosted Email Security.

Policy Management Reports

Report Name	Description
Inbound Policies Filtered	Displays the total number of inbound email messages that Hosted Email Security has filtered based on your configured policies.
Top Inbound Policies	Displays the policy filter names that are triggered most often in inbound email traffic.

Policy Management Reports

Report Name	Description
Outbound Policies Filtered	Displays the total number of outbound messages that Hosted Email Security has filtered based on your configured policies.
Top Outbound Policies	Displays the policy filter names that are triggered most often in outbound email traffic.

Compliance

The **Compliance** option groups reports that are relevant to compliance in Hosted Email Security.

Compliance Reports

Report Name	Description
Top Inbound Approval Boxes	Lists the approval boxes in which inbound email messages sent through Hosted Email Security are stored most often. This report also displays the amount of messages that are stored in each approval box.
Top Outbound Approval Boxes	Lists the approval boxes in which outbound email messages sent through Hosted Email Security are stored most often. This report also displays the amount of messages that are stored in each approval box.

Appliance Health and LDAP Users

The **Appliance Health | LDAP Users** report is presented as a function of the number of users per domain or organization. It helps you determine if the number of users are license compliant. The views available for selection are:

- Domain Person vs. Group Email Addresses
- Domain Primary vs. Alias Email Addresses

Part 3

Investigate

- INVESTIGATE | Junk Box
- Email Continuity
- Logs
- Tools

3

INVESTIGATE | Junk Box

The **INVESTIGATE** view is made up of the **Inbound** and **Outbound** Junk Box tabs. You can review and process email messages that have been quarantined in the Junk Box. Through analysis, these emails have been flagged as spam, virus-infected, policy violations, or phishing attempts. After review you can unjunk a falsely identified message. When you or the recipient unjunks an inbound or outbound message, Hosted Email Security adds the sender of the message to the recipient's Allowed list and delivers the email to the recipient.

To configure the Junk Box, go to the **MANAGE** view and select **SYSTEM SETUP | Junk Box > Message Management**. To set up email notifications about email quarantined in the Junk Box, go to the **MANAGE** view and select **SYSTEM SETUP | Junk Box > Summary Notifications**. Refer to Junk Box for more information.

Topics:

- Using the Junk Box
- Managing Junk Box Messages

Using the Junk Box

The information in the Junk Box page can be managed and customized much like other information in Hosted Email Security.

Topics:

- Simple Searching for Data
- Filtering Table Data
- Customizing the Display

Simple Searching for Data

At the top of the **Inbound** or **Outbound** tabs, a simple search tool is offered to search for specific strings or sentence fragments. The search parameters are applied directly on the data in the table. Surround sentence fragments with quotes (for example: "look for me"). Boolean operators AND, OR, and NOT are also supported.

To perform a simple search:

1 Enter the text you want to search for in the **Simple search** field.

2 Select the field to search on from the drop-down menu. Choose from **Subject**, **To**, **From**, **Unique Message ID**.

3 Click on **Search**. The results are displayed in the data table.

4 Click **Clear Filters** to see all the data.

Filtering Table Data

Advanced search filters are performed directly on the data that's displayed. Select the down arrow next to the column title to filter the data. Some columns are searchable by typing in a string of text to search on. Other columns allow you to choose one or more filters from a list of pre-populated options. You can also filter more than one column at a time. The results of any filtering are immediately shown in the data table.

Click the **Clear Filters** button to see all the data in the table.

Customizing the Display

Several buttons are provided so you can customize what data is shown in the Junk Box table. The options are the same for both **Inbound** and **Outbound** tables.

Button name	Definition
Add Columns	Select Add Columns to get the drop-down menu. Check the box for the data you want to appear in the table. Uncheck them to remove them from the table.
Clear Filers	Clears any filters you set during an advanced filtering search.
Save View	Saves the view you created after adding or removing columns.
Reset to Default View	Resets the data table back to the default view.
Settings	Takes you to **SYSTEM SETUP | Junk Box > Message Management** on the **MANAGE** view to customize the setting that defines what appears in the Junk Box.

Managing Junk Box Messages

The default view displays inbound messages. Click on the **Outbound** tab to see the outbound messages. Click the **Inbound** tab to return to the inbound view. The messages you see in the Junk Box are based on the options selected in **SYSTEM SETUP | Junk Box | Message Management** in the **MANAGE** view.

Inbound message management detects messages sent to users in your organization from people outside of your organization. Outbound message management detects messages sent by users in your organization that contain viruses, likely viruses, and message that trigger policy alerts. Outbound message management also quarantines outbound spam and phishing.

NOTE: Messages stored in the Outbound Junk Box cannot be reviewed by users. They cannot see their messages in their Junk Box Summary notifications. Only administrators can review and process messages quarantined in the Outbound Junk Box.

You can take several actions after reviewing the messages in the Junk Box. See the table below for a description of the buttons at the top left of the data table.

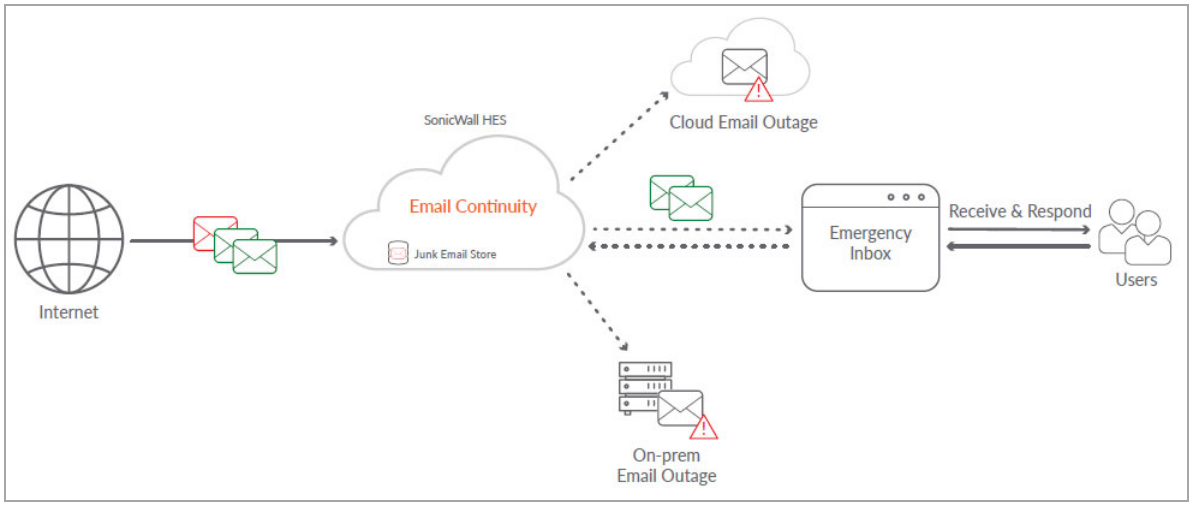
Button name	Definition
Delete	Deletes the selected messages. Select one message by clicking on it. Select a series of messages by clicking on the first message and then shift-clicking on the last one. Select disconnected messages by control-clicking on each one you want. Then click on **Delete**.
Unjunk	Allows you to remove a valid email message from the Junk Box. Select one message by clicking on it. Select a series of messages by clicking on the first message and then shift-clicking on the last one. Select disconnected messages by control-clicking on each one you want and click on the **Unjunk** button.
Send Copy To	Sends selected messages to a specific recipient. Select one message by clicking on it. Select a series of messages by clicking on the first message and then shift-clicking on the last one. Select disconnected messages by control-clicking on each one you want.
Refresh	Updates the data in the table.

The size of the junk box can grow rapidly. By default, the messages are stored in the junk box for 30 days and deleted after that. You may need to customize this setting, depending on your organization's policies and the storage capacity on the shared data directory where messages are stored.

4

Email Continuity

SonicWall Hosted Email Security delivers Email Continuity against planned or unplanned downtime events. It is an add-on subscription that delivers email to end users.



Email Continuity is automatically activated with the subscription. When an email outage occurs, the administrator is notified and users can access emails through the emergency inbox. During an outage SonicWall Hosted Email Security acts as the email server. All suspicious emails are quarantined and only safe email is delivered.

Once the primary email server is back online, the Email Continuity servers automatically reconnect and synchronize all email sent or received during the outage.

Topics:

Managing the Email Tables

The Email Continuity tables are much like any other data table in Hosted Email Security. You can search, filter, or change the table appearance.

Simple Search for Data

At the top of each data table, a simple search tool is offered to search for specific strings or sentence fragments. The search parameters are applied directly on the data in the table. Surround sentence fragments with quotes (for example: “look for me”). Boolean operators AND, OR, and NOT are also supported.

For **Advanced** search filters, click on the drop-down icon in the respective column.

To perform a simple search:

1. Enter the text you want to search for in the **Simple search** field.
2. Select the field to search on from the drop-down menu. Choose from **Subject**, **To**, **From**, or **Unique Message ID**.
3. Click on **Search**. The results are displayed in the data table.
4. Click **Clear Filters** to see all the available data again.

Filtering Table Data

Advanced search filters are performed directly on the data that's displayed. Select the down arrow next to the column title to filter the data. Some columns are searchable by typing in a string of text to search on. Other columns allow you to choose one or more filters from a list of pre-populated options. You can also filter more than one column at a time. The results of any filtering are immediately shown in the data table.

Click the **Clear Filters** button to display all the available data again.

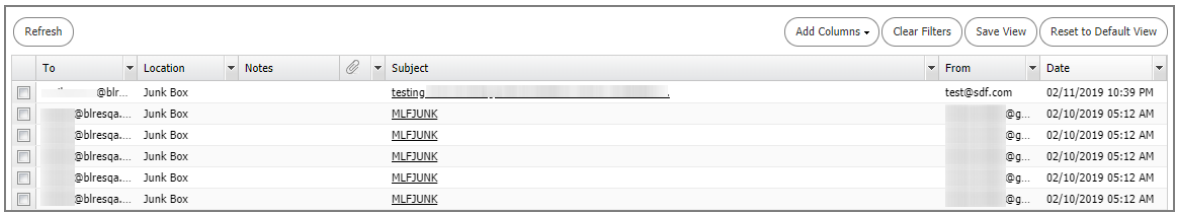
Customizing the Display

Several button are provided so you can customize what data is shown in the Email Continuity tables. The options are the same for **Inbox**, **Outbox**, and **Sent**.

Button name	Definition
Add Columns	Select **Add Columns** to see the drop-down list. Check the box for the data you want to appear in the table. Uncheck them to remove them from the table.
Clear Filters	Clears any filters you set during an advanced filtering search.
Save View	Saves the view you created after adding or removing columns or setting filters.
Reset to Default View	Resets the data table back to the default view.
Refresh	Updates the table data.

Inbox

Email Continuity | Inbox displays all the messages received on the inbound path during the period when the primary email server is inaccessible. You can confirm this once and make the required changes. These represent all good email messages for the past 7 days.



Use the buttons at the top of the table to manage the inbox:

Button	Definition
Refresh	Click Refresh to update the data in the inbox.
Add Columns	Select **Add Columns** to get the drop-down menu. Check the box for the data you want to appear in the table. Uncheck them to remove them from the table.
Clear Filters	Clears any filters you set during an advanced filtering search.
Save View	Saves the view you created after adding or removing columns.
Reset to Default View	Resets the data table back to the default view.

Refer to Managing the Email Tables for information on how to customize the table views.

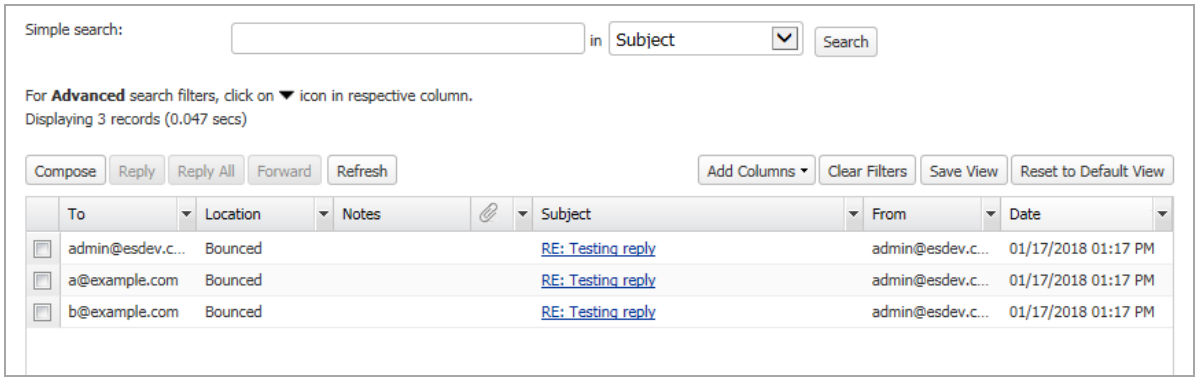
Outbox

Email Continuity | Outbox displays all the messages that are currently in the queue, waiting to be delivered. Use the buttons at the top of the table to manage the email in the outbox. They are the same as the buttons in the Inbox.

Refer to Managing the Email Tables for information on how to customize the table views.

Sent

Email Continuity | Sent displays all the messages sent on the outbound path. These represent messages that have been delivered in the past 7 days.



Use the buttons at the top of the table to manage the email in the sent path. They are the same as the buttons in the Inbox and Outbox tables.

Refer to Managing the Email Tables for information on how to customize the table views.

5

Logs

Topics:

Message Logs

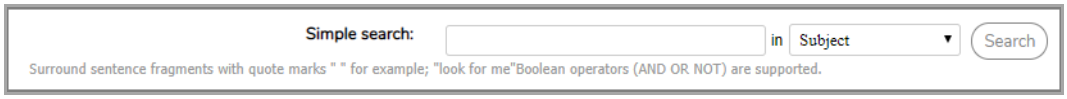
Message Logs displays messages captured in the auditing database. The messages selected are based on the auditing parameters you set. Select **Inbound** to see to see the inbound messages and select **Outbound** to see the outbound messages. Click the link in the Subject field to see the details about the message.

NOTE: You can be in either the **Inbound** or the **Outbound** tabs when setting the auditing parameters. The **Settings** option is the same in either view.

Topics:

Simple Searching for Data

At the top of the page, a simple search tool is offered to search for specific strings or sentence fragments. The search parameters are applied directly on the data in the table. Surround sentence fragments with quotes (for example: “look for me”). Boolean operators AND, OR, and NOT are also supported.



To perform a simple search:

1. Enter the text you want to search for in the **Simple search** field.
2. Select the field to search on from the drop-down menu. Choose from **Subject**, **To**, **From**, or **Unique Message ID**.
3. Click on **Search**. The results are displayed in the data table.
4. Click **Clear Filters** to see all the available data again.

Filtering Table Data

Advanced search filters are performed directly on the data that's displayed. Select the down arrow next to the column title to filter the data. Some columns are searchable by typing in a string of text to search on. Other columns allow you to choose one or more filters from a list of pre-populated options. You can also filter more than one column at a time. The results of any filtering are immediately shown in the data table.

Click the **Clear Filters** button to display all the available data again.

Customizing the Display

Several button are provided so you can customize what data is shown in the Message Log table. The options are the same for both **Inbound** and **Outbound** tables.

Button name	Definition
Add Columns	Select **Add Columns** to get the drop-down menu. Check the box for the data you want to appear in the table. Uncheck them to remove them from the table.
Clear Filters	Clears any filters you set during an advanced filtering search.
Save View	Saves the view you created after adding or removing columns.
Reset to Default View	Resets the data table back to the default view.
Settings	Opens a window you can customize the settings for Auditing. 1 Select on or off to enable the following: • Auditing for inbound email • Auditing for outbound email • Enable Judgment Details logging • Keep Email auditing files for **NOTE:** You can keep email auditing files for up to 2 weeks. 2 Click **Apply**.

Sharing Data

Data from the Message Logs table can be shared in many ways.

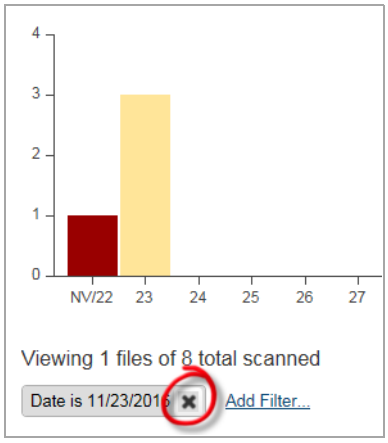
Button Name	Definition
Send Copy to	Sends selected messages to a specific recipient. Select one message by clicking on it. Select a series of messages by clicking on the first message and then shift-clicking on the last one. Select disconnected messages by control-clicking on each one you want.
Download	Sends the selected messages to the downloads file in zip format.
Release from Capture Box	Releases the email in the Capture Box without waiting for it to finish processing.
Refresh	Refreshes the data in the table.

Capture ATP Logs

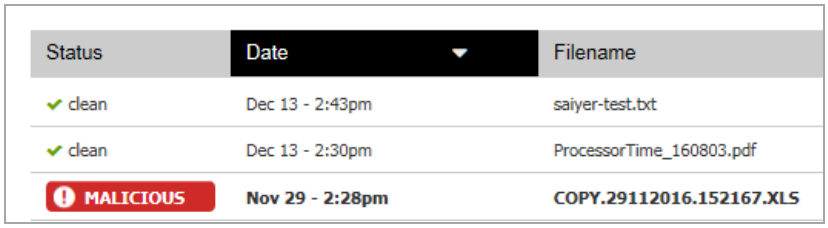
The Capture ATP logs provide a summary of Capture ATP activity in the last 30 days. It displays a bar graph showing how many files were scanned each day and a table listing the scanned files.

Additional data is available by dragging the cursor over the bars in the graph; a window pops up showing how many files were scanned that day and what percentage of them were malicious. The colors of the bars also indicate what percentage of the files were malicious. A white bar indicates that none were malicious. A red bar indicates 100% of them were malicious, and various shades of blue and purple represent different percentages in between, as shown in the legend on the graph.

If you click on a bar in the graph, the data in the table below the graph is filtered to show only the files scanned on that day. The bar changes to yellow to show that it was selected for filtering. A date appears below the graph; click on the X next to the date to remove the filtering.



Data in the table can also be sorted. Click in one of the headings to change the order of the data. The small arrow next to the heading indicates whether the data is listed in ascending or descending order as shown in the figure below:



To upload a specific file for scanning:

1 Select **Upload a File** to select a file for scanning.

2 Browse your disk to find and select the file.

3 Select **Upload** to start the scan.

NOTE: The following file types are supported for scanning:

- EXE
- MSI
- ZIP
- APK applications
- PE

IMPORTANT: The maximum file size allowed is 10 MB.

6

Tools

Run DMARC Reports

When the Hosted Email Security Mail Server plays the role as email sender and RUA receiver, it extracts and aggregates daily RUA files from the email receiver and from RUA providers, such as Google, Yahoo, etc. The DMARC Reporting Scheduler then imports the RUA files hourly into its database.

Based on date range and data filter, you can obtain five different types of reports. One report is a graphic chart; the others are tables. The reports include:

- DMARC Statistic Report (Graphic Chart)
- DMARC Master Detail Report
- Source IP Aggregation Report
- Source IP and Known Network Aggregation Report
- Provider Aggregation Report
- Source IP and Provider Aggregation Report

Users with an Admin Role or an OU Admin Role are allowed to access the DMARC reports. Admin role users can access all policy domains data, while OU Admin role users can only access the data in the domains assigned in **SYSTEM SETUP | Users, Groups & Organizations** on the **MANAGE** view.

NOTE: To receive reports, configure RUA address on the **MANAGE** view, under **SECURITY SERVICES | Security Services > Anti-Spoofing**. Refer to Anti-Spoofing for more information.

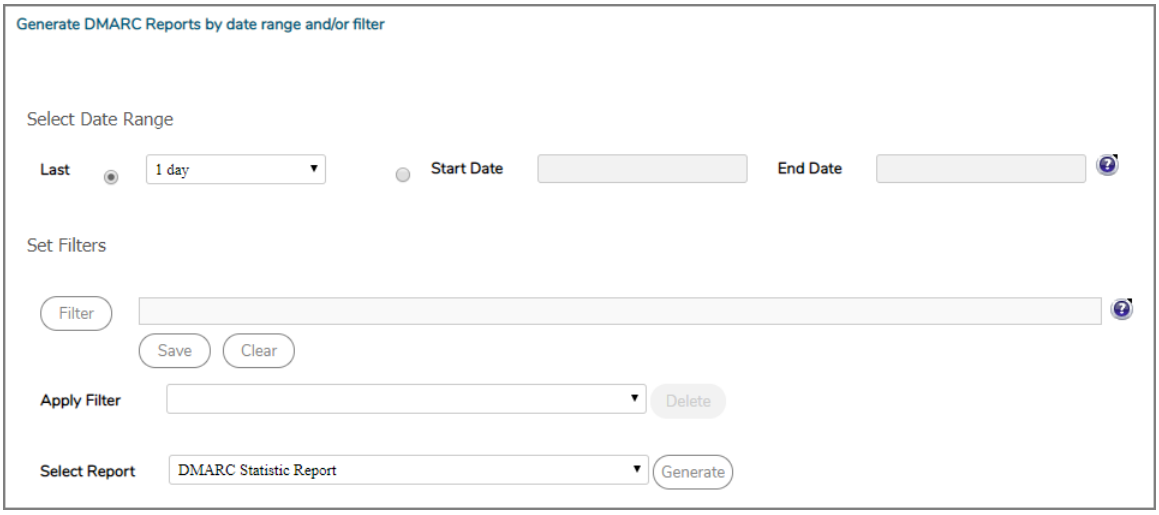
Topics:

- Generating the Report
- Defining New Filters

Generating the Report

To generate a DMARC report:

1 Navigate to **INVESTIGATE | Tools > Run DMARC Reports.**



2 Choose a Date Range using one of the following methods:

- Select **Last** and choose a pre-defined option from the drop-down menu. Choices range from 1 to 21 days.
- Select **Start Date** and enter a **Start date** and **End date** from the pop up calendars.

3 Choose the filters for the report. You can select available filters from the **Apply Filters** drop-down menu or you can build a new filter by selecting the **Filter** button. Refer to Defining New Filters for more information about building a new filter.

4 Select the report type from the **Select Report** drop-down list. The options include:

- DMARC Statistic Report
- DMARC Master Detail Report
- Source IP Aggregation Report
- Provider Aggregation Report
- Source IP and Provider Aggregation Report

5 Click on the **Generate** button to generate the report. Reports are shown in a window below the 'Set Filters' section.

6 Click **Download PDF** to download a PDF report once the HTML report is generated. The PDF report name includes the Report Name and a time stamp.

All reports can be rendered in HTML format and downloadable PDF file. (HTML reports allow you to mouse over 'Alignment' value to see alignment reason description.)

The statistics report displays either horizontally or vertically, depending on the date range. If days of selected date range are less than 15 days, three (3) bar charts are horizontally displayed. If the date range is greater than 15 days, the bar charts display vertically. For tabulated reports, scrolling the mouse over the 'Alignment' value displays the Alignment Reason. For example, if the 'Alignment' is 'No', moving the mouse over this 'No' makes the Title Box show: “No DKIM and SPF is passed, On SPF Relaxed, SPF Organization Domain(sina.com) Not Matched From Header Domain(sonicwall.com)” This informational message can be useful for DMARC troubleshooting.

Defining New Filters

You can define a new filter to use for the DMARC reports. This filter then becomes an option for filtering the DMARC Report database.

To build a new filter:

1. Navigate to the **INVESTIGATE** view and select **Tools > Run DMARC Reports**.
2. Click on the **Filter** button to create a new filter. (If a filter already exists, clicking this button allows you to edit the filter.) The **Set Filter** page opens.
3. Define the parameters of the filters using the conditions provided.
    a. Select one of the **Condition Names** from the left.
    b. Select the operators for how the data is acted upon. For example, you might choose between **include** and **exclude** or mathematical operators like == (equals) and!= (not equals).
    c. In the right column, **Select or Input Values**. Values are automatically provided for some Condition Names, but you need to type in the values you want if none are provided.
    d. Click **OK** to exit the Set Filter pages.
4. Click **Save** to save the newly configured settings.

Other buttons are available to help you manage the filters. They include:

Save	Saves a selected filter.
Clear	Clears all settings of the current filter.
Delete	Deletes a selected filter.
Generate	Generates a selected report.

Part 4

Manage

- Basic Administration
- Policy & Compliance
- System Setup | Server
- System Setup | Customization
- Users, Groups & Domains
- System Setup | Network and Junkbox Commands
- Anti-Spam
- Anti-Spoofing
- Anti-Phishing and Anti-Virus
- Capture, Time of Click
- Encryption and Connections
- Reporting

7

Basic Administration

The basic administration tasks for an Hosted Email Security instance are grouped at the top of the menu. They include things you do more often, like:

- License Management
- Downloads

License Management

The **License Management** option allows you to view and manage current Security Service and Support Service for your Hosted Email Security solution.

Key information for your Hosted Email Security solution is provided in the upper right corner:

- **Serial Number**—The serial number of your SonicWall Hosted Email Security appliance/software.
- **Authentication Code**—The code you entered upon purchasing/activating the SonicWall Hosted Email Security solution.
- **Model Number**—The model number of the SonicWall Hosted Email Security appliance. If you are using the SonicWall Hosted Email Security software, the model number is listed as Software.

The following buttons, located at the bottom of the page, allow you to perform certain licensing functions:

- **Manage Licenses**—Click this button to log in to your MySonicWall account to register appliances and manage all security services, upgrades, and changes.
- **Refresh Licenses**—Click this button to refresh the license status for Security and Support services.
- **Test Connectivity**—Click this button to validate connectivity to the SonicWall License Manager.

NOTE: The hourly license update synchronizes with the online license manager and overwrite licenses applied by the offline method.

This Administration comes with several service modules that must be licensed separately. For maximum effectiveness, all services are recommended.

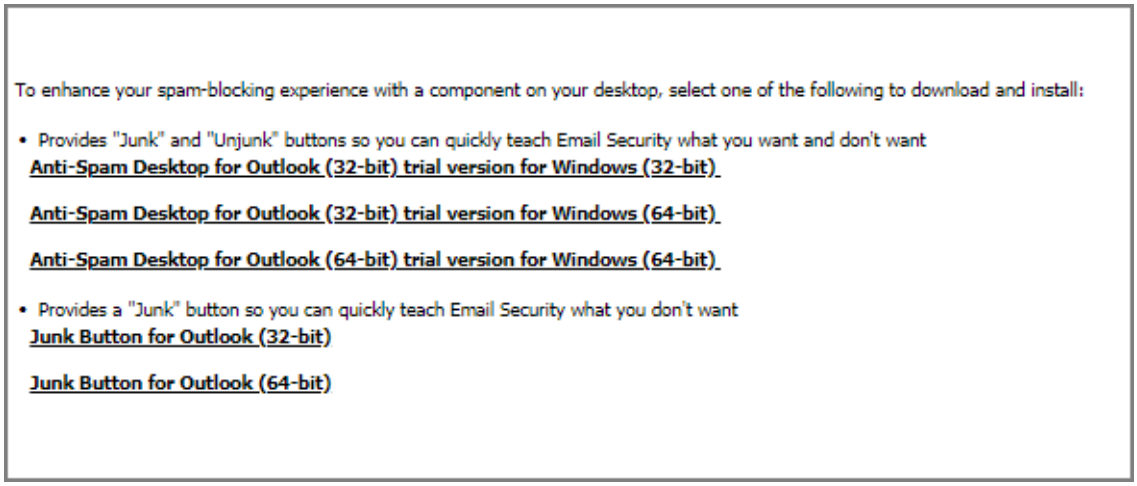
The Security Service table on the **License Management** page provides information on the status of the various offerings in your configuration.

Status	The status for the Security or Support Service may be one of the following:	
	Licensed	Services have a regular valid license.
	Free Trial	Services are using a 14-day free trial license.
	Not licensed	Service has not been licensed.
	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.
	Expired	Services that have expired.
Count	The number of users to which the license applies.	
Expiration	The expiration date of the service. Either a specific expiration date is listed or **Never** is listed, indicating no expiration.	

The Support Service table shows the kinds of service support agreements that have been licensed for your solution. It includes license status and expiration date.

Downloads

SonicWall provides some tools you can download that enhance the spam-blocking experience on the desktop. Navigate to the **Downloads** page to download and install the following tools.



The Anti-Spam Desktop for Outlook are trial versions of the SonicWall Anti-Spam Desktop feature. It is offered in 32-bit and 64-bit combinations. This download provides “Junk” and “Unjunk” buttons for you to customize your own Hosted Email Security solution.

The Junk Button for Outlook link provides a “Junk” button for you to install on your own Windows program. Both 32-bit and 64-bit options are offered. These downloads help customize your Hosted Email Security solution.

8

Policy & Compliance

SonicWall Hosted 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 an administrator. Typical use of 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:

Policy Management and Mail Threats

As SonicWall Hosted Email Security evaluates email, it uses the following 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 is categorized as a virus since virus is higher in precedence than spam. If SonicWall Hosted Email Security determines that the message is not any of the above threats, it is delivered to the destination server.

Policy Management plays a key role in evaluating the email threats by filtering email based on message contents and attachments. You can create policy filters in which you specify an action or actions you want Hosted Email Security to take on messages that meet the conditions you define. For example, you can specify words to search for—a product term, for example—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: Any of the policies configured in the Policy section take precedence over any entries made in the Allowed List.

Filters

The **Policy & Compliance > Filters** page is where you manage preconfigured files and define new filters for both inbound and outbound paths.

NOTE: Policies created on the inbound path can not be shared with the outbound path and vice versa. See Managing Filters for examples of adding inbound and outbound policies.

Topics:

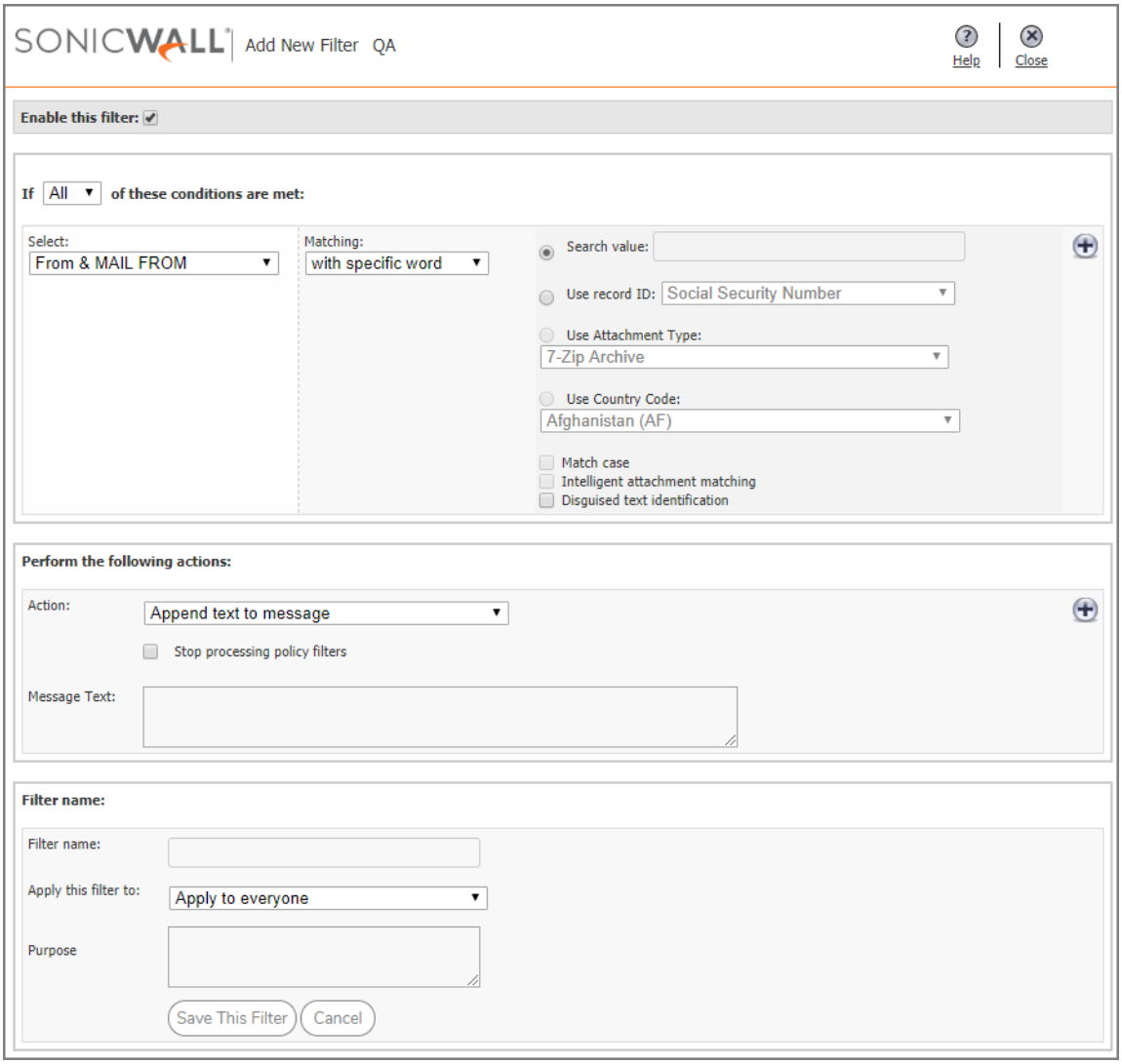
- Adding Filters
- Language Support
- Managing Filters
- Advanced Filtering

Adding Filters

You can add filters for email as it enters or exits your organization.

To create a policy filter:

1. Navigate to the **Policy & Compliance > Filters** page on the **MANAGE** view.
2. Select the **Inbound** or **Outbound** tab to create filters for inbound or outbound email messages.
3. Click the **Add New Filter** button.



NOTE: The fields in the window are context sensitive; they change based on the actions you choose.

4 Note that the **Enable this Filter** checkbox is checked by default. Uncheck the box 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 only when *all* of the filter conditions apply (logical AND)
- **Any**—Causes email to be filtered when *any* single condition applies (logical OR)

6 In the **Select** field, choose the parts or types of message to filter See the following table for more information:

Select	Definition
Spam/Phishing Judgment	Filters messages based on the judgment that it is spam or phishing attempts.
Likely Spoof Judgment	Filters on messages based on the judgment that it is a Likely Spoof attempt.

Select	Definition
Address Book	For any email coming is the policy first checks to see if the email address is a valid address in the address book, then takes further action based on how the policy is defined.
From & MAIL FROM	Examines both envelope and header **From** fields for a match.
To/Cc/Bcc & RCPT TO	Examines both envelope **To** field and header **To/Cc/Bcc** fields for a match.
From	Filters by sender's name or portion of a sender's name.
To	Examines the To header field for a match.
CC	Examines the **CC** header field for a match.
Reply-To	Examines the **Reply-To** header field for a match.
Envelope MAIL FROM	Examines the **MAIL FROM** envelope field for a match.
Envelope RCPT TO	Examines the **RCPT TO** envelope field for a match.
Subject	Filters 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
Subject, Body or Attachments	Filter based on information in the subject, body, and attachments of the email
Message Headers	Filter by the RFC822 information in the message header fields, which includes information like the return path, date, message ID, received from, and other information
Attachment Name	Filter attachments by name
Attachment Contents	Filter based on information in the email attachments
Attachment Type	Filter based on type of attachment
Country Code	Filter based on sender's country code
Size of Message	Filter messages based on the size of the message
Number of Recipients	Filter messages based on the number of recipients
Source IP	Filter messages based on the sender's IP address
Single Message Header	Filter messages containing a single message header
Originating IP	Filter messages based on the IP address from where the message was sent
All Good Messages	Filter all good messages.

7 Choose the matching operation in the **Matching** field. The matching options vary based on the filtering option you selected.

8 Enter the value you want to filter in the **Search Value** text box, or select one of the other options listed, if enabled:

- **User dictionary** and **Use record ID** are part of the Compliance Subscription License.

NOTE: If the Compliance Subscription License is active, the administrator has additional filtering conditions that can be set. The **Use dictionary** option of using terms from a dictionary can be selected, as well as the **Use Record ID** option which looks for numbers such as telephone numbers or social security numbers.

- **Use Attachment Type** allows you to select a specific type of file attachment. About 137 files types are listed.
- **Use Country Code** allows you to select the country code you want to filter on.

9 Select the appropriate check boxes to further refine your search:

- **Match Case**—Filters a word or words sensitive to upper and lower case.
- **Intelligent attachment matching**—the content taxonomy is used to match the attachment type.
- **Disguised text identification**—Filters disguised words through the sequence of its letters, for example Vi@gr@.

NOTE: Disguised text identification cannot be used with **Match Case** and can be selected only for Body and Subject message parts.

10 Click the **+** icon if you want to add another layer of filtering.

You can add up to 20 layers. Filter layers are similar to rock sifters: Each additional layer adds further filtering that tests email for additional conditions.

11 Under **Perform the following actions**, select the response from the **Action** drop-down list. The following table describes the available response actions:

Action	Effect
Store in Junk Box	The email message is stored in the Junk Box. It can be unjunked by users and administrators with appropriate permissions. The user has the option of unjunking the email.
Deliver and skip Spam and Phishing Analysis	The message is delivered without spam or phishing analysis.
Permanently delete	The email message is permanently deleted and no further processing occurs in any SonicWall Hosted Email Security module occurs. This option does not allow the user to review the email and can cause good email to be lost.
Store in Approval Box	The email message is stored in the Approval Box. It is not delivered until an administrator approves it for delivery.
Reject with SMTP error code 550	The message is returned to sender with an error message indicating that it was not deliverable.
Deliver and reject with SMTP error code 550	The message is delivered to the recipient and is bounced back to the sender with an error message.
Route to IP	The message is routed to the specified email address. The message can be routed to only one email address.
Deliver and route to IP	Deliver to the recipients and also route to the specified email address. The message can be routed to only one email address
Deliver and Route to IP	Deliver to the recipients and also route to the specified IP address. The message can be routed to only one IP address.
Tag subject with	The subject of the email is tagged with a the specified term.
Strip all attachments	Remove all the attachments from the email.
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 an email.
Skip Capture ATP	Message is not sent for Capture analysis.
Skip Time-of-Click URL rewrite	Email message URL is not rewritten at the time of click.
Append text to message	The specified text is appended to the message body.

12 Select the **Stop processing policy filters** checkbox when no additional filtering is required on a message. This check box is automatically selected and grayed out when you have selected a terminal action.

13 If additional actions need to be performed on the same message, select the **+** icon to the right. You cannot add the same action more than once to a specific filter rule. As a result, once an action has been selected, it is not available in the drop-down list for further selection within the current filter rule.

14 Type a descriptive name in the **Filter Name** text box.

15 Select a policy group you want to apply this filter to. By default, **Apply to everyone** is selected and this filter applies to all email messages.

16 Add a brief description to the **Purpose** text box.

17 Click the **Save This Filter** button.

Language Support

Policy management supports filtering messages based on non-English terms in the **Search Value**. For example, you can search for a Japanese word or phrase in the body of a message. However, Hosted Email Security does not support adding text strings to email messages in languages other than English and does not support foreign language filter names.

Managing Filters

The Filters page lists all the filters created in the system for the **Inbound** and **Outbound** path. They are processed in the order they are listed.

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 check mark.

To change a filter that has been saved:

1 On the **MANAGE | Policy & Compliance > Filters** page, select the **Inbound** or **Outbound** view (wherever the filter is located).

2 Select the **Edit** button adjacent to the filter to be changed.

3 Change any of the filter conditions.

4 Select **Save This Filter**.

To delete a filter:

1 Select the **Delete** button adjacent to the filter.

2 Confirm your choice when asked.

To change the order of the filters:

1 Drag and drop the filter in the order you prefer.

Advanced Filtering

This section contains various advanced configuration examples related to Filters:

- Creating a Multi-Layered Filter
- Creating an Outbound Filter to Add a Company Disclaimer
- Configuring a Policy Filter for Inbound Email
- Exclusive Actions
- Parameterized Notifications

Creating a Multi-Layered Filter

You can create filters with multiple conditions chained together and multiple actions performed on the message if the specified conditions are met.

For an example, if the email message is:

- Sent from NASA *and*...
- The body contains the word Mars.
- Then tag the subject with the term [Mars Update from NASA] *and* route the message to engineering.

To create a multi-layered filter like the example above:

1. Click the **Add New Filter** button from the **Policy & Compliance > Filters > Inbound** page.
2. Select **All** conditions to be met.
3. **With Specific Words** operation, search for nasa.org in the message part **From**.
4. Select the **+** button to the right to add another condition.
5. **With Specific Words** operation, search for Mars in the message part **Body**. **Enable Match Case** to get an exact case match.
6. Select the action **Tag Subject With**. Set the Tag field to [Mars Update from NASA].
7. Verify that the **Stop processing policy filters** check box is not enabled.
8. Select the **+** icon to the right to add another action.
9. Select the action **Route To** and set the **To** field to `engineering@company.com`.
10. Select the S**top Processing Policy Filters** check box to stop further policy filtering on this message.
11. Select the **Save This Filter** button.

Creating an Outbound Filter to Add a Company Disclaimer

This section provides steps to add a company disclaimer to the end of each outgoing message from your organization. In this example, if email is sent from anyone at sonicwall.com, the following message is appended to the end of the message: `This is my company disclaimer`

To create the outbound policy filter:

1. In the SonicWall management interface, navigate to the **Policy & Compliance > Filters** screen, and click the **Outbound** tab.
2. Click the **Add New Filter** button.
3. Select **All** conditions to be met.
4. Select **From** in the **Select** drop-down list.
5. Select **Contains** in the Matching drop-down list.
6. Type **`sonicwall.com`** In the **Search Value field**.
7. To protect against internal spammers or zombies, click the **+** icon to add another condition.
8. Select **Spam/Phishing Judgement** from the **Select** drop-down list.
9. Select **is good** in the **Matching** drop-down list.
10. Select the action **Append text to message**.
11. In the **Message text** type: **`This is my company disclaimer.`**
12. Type the **Filter Name**: **`Outbound Disclaimer`**.
13. Select **Apply to Everyone** from the drop-down menu for the **Apply this filter to** field.
14. Add a brief description to the **Purpose** Text field: for example, **`Adds a company disclaimer to outgoing mail`**.
15. Click the **Save This Filter** button.

Configuring a Policy Filter for Inbound Email

To filter email messages sent to your organization that are not judged as spam but contain the words “job application” in the subject or body of the email message, follow the procedures listed:

If an email is:

- Not judged as spam and
- The subject or body of the email contains the words job application.

Then route the email to hr@sonicwall.com

To create the inbound policy filter like the example above:

1. Click the **Add New Filter** button under the **Inbound** tab.
2. Select **All** conditions to be met.
3. Select **Spam/Phishing Judgement** operation.
4. Set **Matching** to **is not spam**.
5. Select the **+** icon to add another condition.
6. Select the **Subject or Body** option from the drop-down list.
7. Set **Matching** to **with specific phrase**.

8 Type the words **job application** in the **Search value** field.

9 Select the action **Route to**.

10 Enter the email address **hr@sonicwall.com** in the **To** field.

11 Name the filter `Resume Routing`.

12 Select **Apply to Everyone** from the drop-down menu in the **Apply this filter to** section.

13 Add a brief description to the **Purpose** Text field.

14 Select the **Save This Filter** button.

Exclusive Actions

Exclusive actions are terminal in nature and no further policy filtering is possible after this action has been performed. The **Stop Processing Policy Filters** check box is automatically enabled and grayed out if an exclusive action is selected.

Parameterized Notifications

Hosted Email Security supports parameterized notifications where you can use pre-defined parameters in the text fields for the Issue Email Notification action. These parameters get substituted with corresponding values when the message is processed. You can use these parameters in either the Subject or Message Text fields of the Issue Email Notification action. The parameters can be used multiple times and are substituted each time they are used. Each parameter entered should start and end with % symbol. Parameters for Notifications provides more details.

Parameters for Notifications

Parameter	Value
%SUBJECT%	the Subject content from the triggering email
%FROM%	the From content from the triggering email
%ATTACHMENT_NAMES%	a comma-separated list of attachment names from the triggering email
%FILTER_NAME%	the name of the policy filter which took the action on the triggering email
%MATCHED_RECORDID%	the Record ID file name which has a matching pattern in the triggering email
%MATCHED_TERM%	the Dictionary term which matched in the triggering email

Policy Groups

In some cases, you may want to associate a policy filter to a group of users rather than the entire organization. For example, you may want a policy filter to be applied to all incoming email messages sent to your sales team and no one else in your organization. If you want policy filters you create to be applied to particular group of users, you first have to create policy groups from LDAP. Policy groups, once created, can be associated with either inbound or outbound policies.

NOTE: For administrative purposes, a user is a member of only one group. If a user is a member of more than one group, that user is treated as if they were only a member of the first group in the list.

Topics:

Adding a New Policy Group

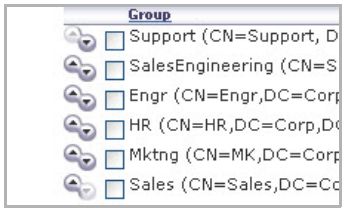
To add a new policy group:

1. Navigate to **Policy & Compliance > Policy Groups** on the **MANAGE** view.
2. Select the **Add Group** button.
3. If managing policy groups from multiple LDAP servers, select the source for the groups lists from the **Using Source** drop-down list in the **Add Group** popup window and click **Go**.
4. From the **Find all groups** drop-down list, select one of three methods to locate a desired group:
   - **equal to (fast)**—search using the actual name, which is a faster search
   - **starting with (medium)**—search using the first few characters, which may take more time
   - **containing (slow)**—search using a substring of characters, which is the slowest search
5. Type a search string in the text box and click **Go**.
6. Once the list of group names is displayed, check the box of the group or groups you wish to add.
7. Click on the **Add Group** button. The group appears in table on the main page.

Removing a Policy Group

To remove a group, check the group(s) to be removed and select the **Remove Group** button. You can view the members of a group by selecting that group and clicking on the **List Group Members** button.

If a user is present in more than one group, that user is treated to be a member of the group that is listed highest in the list. You can change group ordering, by clicking on the arrows to the left of listed groups. To change the order in which groups are listed, use the up and down arrow icons to the left of the groups.



For example in the above illustration, if jdoe@company.com is listed under both SalesEngineering and Sales, the policy filter that is associated with SalesEngineering is applied to email messages for jdoe@company.com.

Listing Members

You can view a list of the members of a specific policy group.

1. Navigate to **Policy & Compliance > Policy Groups** on the **MANAGE** view.
2. Check the box by the group name you want to see.
3. Select **List Members**.
4. Close the window when done.

Dictionaries

A dictionary is a convenient collection of words or phrases that you can group together for use in policy filters. A dictionary can be specified as a search value in a policy filter. Dictionaries can be created or modified manually or by importing from a file on the file system.

A predefined dictionary is a group of words or phrases all belonging to a specific theme such as medical or financial terms, which can be used as a database of words that filters can look for. By default, SonicWall provides these pre-installed dictionaries, which can be modified by clicking on the **Edit** button.

- Financial Terms
- Medical Drug Names
- Encryption Service IPs

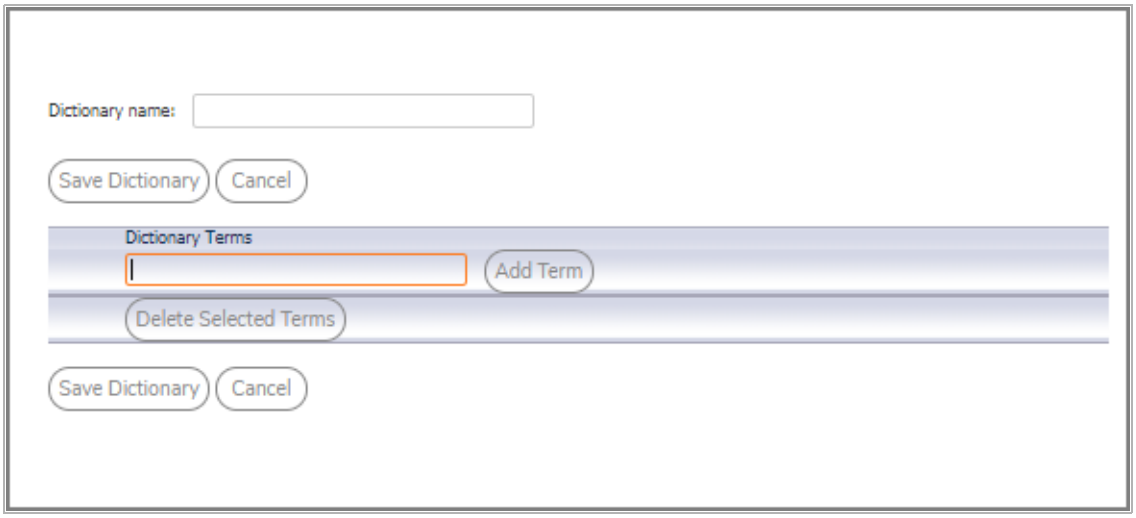
Topics:

- Add New Dictionary
- Import Dictionary
- Delete Dictionaries or Terms

Add New Dictionary

To manually add a dictionary:

1 Click on the **Add New Dictionary** button.



2 Type the new dictionary name in the **Dictionary name** field.

3 Enter a word or phrase in the **Dictionary Terms** text field.

4 Select **Add Term**.

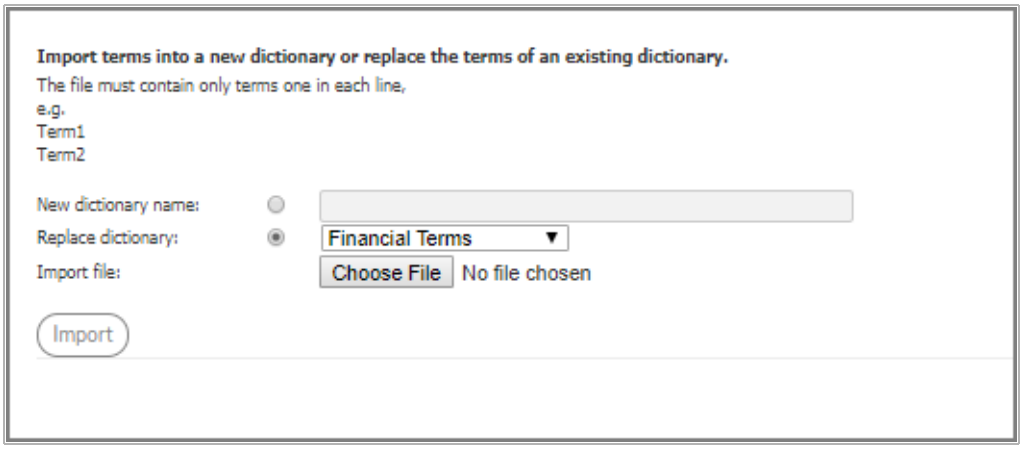
5 Repeat for all the terms you want to add to the dictionary.

6 Click **Save Dictionary**.

Import Dictionary

To import a dictionary from a file on the file system:

1 Click on the **Import Dictionary** button.



2 Choose **New dictionary name** or **Replace dictionary** by selecting the appropriate button next to your selection.

3 Find the import file by selecting **Choose File** and navigating to the correct location.

The imported file should contain one word or phrase per line and each line should be separate by a carriage return.

4 Click the **Import** button.

Delete Dictionaries or Terms

To delete a dictionary:

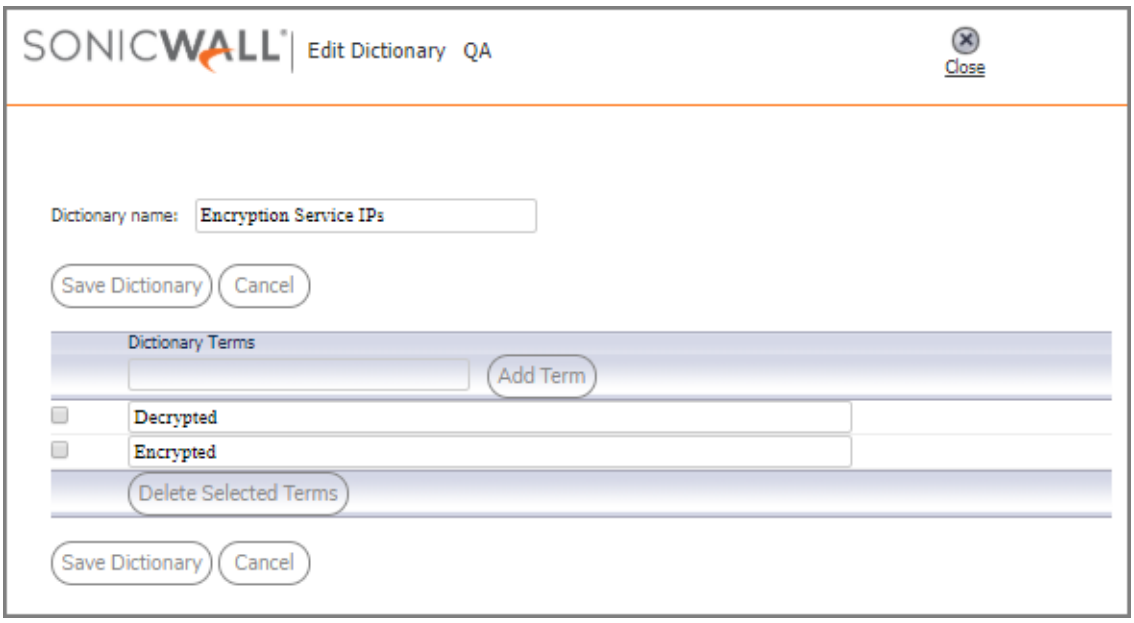
1 Navigate to **Policy & Compliance > Dictionaries** on the **MANAGE** view.

2 Select the **Delete** button for the dictionary you want removed.

To edit terms from a dictionary:

1 Navigate to **Policy & Compliance > Dictionaries** on the **MANAGE** view.

2 Select the **Edit** button for the dictionary whose terms you want to remove.



3 Check the box by the terms you want to delete.

4 Select **Delete Selected Terms** (you may need to scroll to the bottom of the list to see this button).

5 Select **Save Dictionary** save the changes.

Approval Boxes

An Approval Box is a list of stored email messages that are waiting for an administrator to take action on. They are not delivered until an administrator approves them for delivery. The View Approval Box drop-down list allows you to have two different views of Approval Boxes: The Manager view and the individual approval box view.

To see a list of the Approval Boxes that have been created, select **Approval Box Manager** from the drop-down list in the **View** field. The **Approval Box Manager** view allows you to edit or delete existing Approval Boxes, and to create new Approval Boxes.

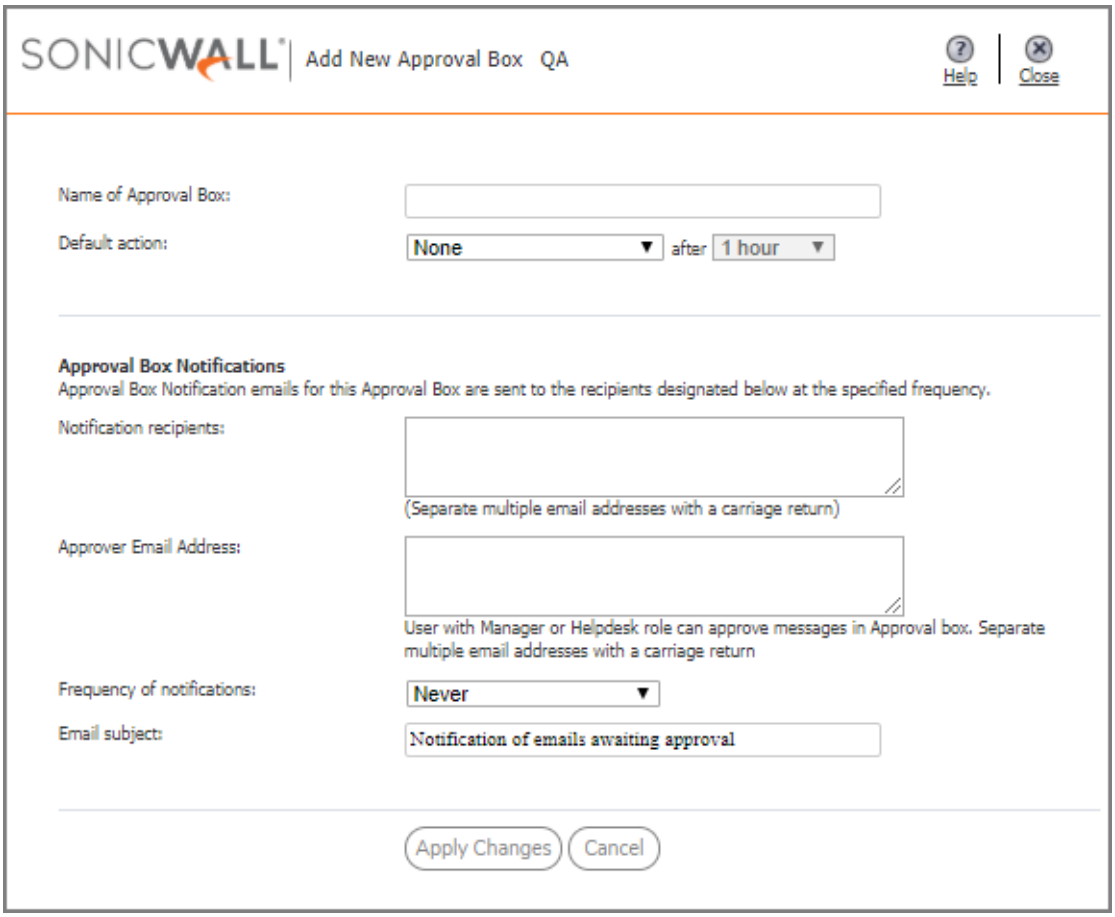
To see the contents of a particular Approval Box, choose the desired Approval Box name from the table. This page allows you to search the messages stored in that Approval Box and to take action on any of those messages.

NOTE: Only users who have administrative rights can see the contents of an approval box. See Users, Groups & Domains for managing user rights and privileges.

To set up an Approval Box:

1 Navigate to **Policy & Compliance > Approval Boxes** on the **MANAGE** view.

2 Create the Approval Box by selecting **Add New Approval Box**.



3 Enter the **Name of Approval Box**. This name appears in the approval box table and in the drop-downdrop-down list that allows you to select the detailed view of individual approval boxes.

4 From the **Default action** drop-down list, select an action to be taken. This action is automatically taken on the message waiting for approval if the administrator does not respond to the notification within the time specified.

None	No action is taken. The email remains in the Approval Box.
Approve and Deliver	The email is passed to the recipient.
Delete	The email is deleted.
Bounce Back to Sender	The email is automatically bounced back to the sender and removed from the Approval Box after the specified length of time elapses.

5 Select the amount of time the messages are held in the Approval Box before action is automatically taken. The time values range from 1 hour to 30 days.

6 Enter a list of **Notification recipients** in the text box. Separate multiple email addresses with a carriage return.

> **NOTE:** Make sure that the email recipients you list are users that have administrative rights to the SonicWall server. If they do not have administrative access, they cannot view the approval boxes when they receive email notification.

7 Enter the **Approver Email Address** in the text box. Separate multiple email addresses with a carriage return.

> **NOTE:** A user with a Manager or Helpdesk role can approve messages in Approval Box.

8 Select a **Frequency of notifications** value from the drop-down list for this approval box. Email notification is sent according to the schedule you choose here.

9 Write the **Email subject** line for this notification, like `Notification of emails awaiting approval`.

10 Click the **Apply Changes** button to save your changes.

11 Navigate to the **Policy & Compliance | Filters** page.

12 Create a policy filter that sets the **Action** to **Store in Approval Box**.

13 Choose the desired Approval Box for email messages caught by that filter.

Enhanced Approval Box

Partners and customers leveraging the Approval Box feature require the ability to have designated approvers that can view and approve notifications in the Approval Box. In prior versions, this required full administrative permissions like root administration rights or OU administrative rights. This level of access is undesirable given some approvers just need one specific role function.

With the enhanced Approval Box, you can designate people in other roles, such as Managers and Helpdesk, to see the Approval Box and act as an approver.

To set up an approver:

1 Navigate to **MANAGE | SYSTEM SETUP | Customization > User View Setup**.

2 In the **Policy View Settings** section, check the box for **Helpdesk** or **Manager**, depending on which role you set up your approvers with.

3 Navigate to **MANAGE | Policy & Compliance > Approval Boxes.**

4 Select **Add New Approval Box**.

5 Define the Approval Box as needed, being sure to include the approver's email address in the **Approver Email Address** field.

6 Click **Apply Changes**.

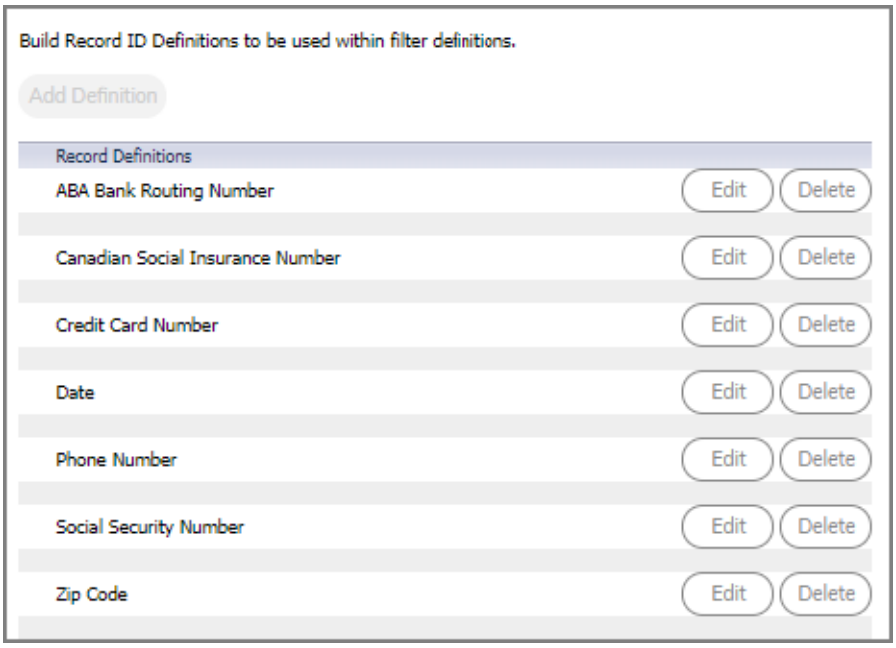
7 Verify that the new Approval Box appears in the Approval Box table.

Record ID Definitions

Record ID Definitions can be used to detect specific IDs described by a series of generic patterns. The P**olicy & Compliance | Record ID Definitions** section allows the administrator to define a cluster or clusters of letters and numbers into logical sets of groups such as social security numbers, patient medical record numbers, or credit card numbers. When these patterns are discovered, compliance actions can be taken to ensure that the organization's privacy and security regulations are met. The filter stops processing a message after it finds the first matching Record ID Definition.

By default, Hosted Email Security provides the following Record ID Definitions pre-installed:

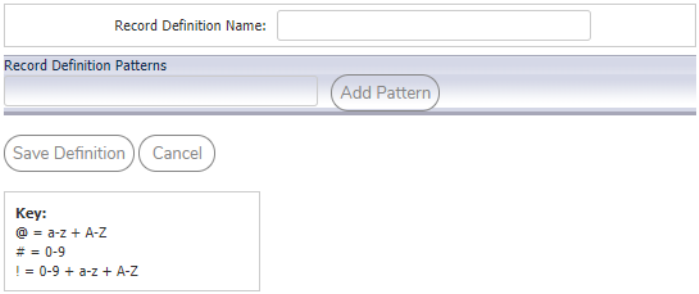
- ABA Bank Routing Number
- Canadian Social Security Number
- Credit Card Number
- Date
- Phone Number
- Social Security Number
- Zip Code
- main



To add a new Record ID Definition:

1 Navigate to the **Policy & Compliance > Record ID Definitions** page.

2 Click the **Add Definition** button.



3 Enter a name in the **Record Definition Name** field.

4 Enter a **Records Definition Pattern**, including correct spacing, dashes or other symbols. Use the key to set values to the sets of characters.

5 Click **Add Pattern** to add the term to the Record ID. Repeat this step for each Record ID as necessary.

6 Select **Save Definition** when finished.

9

System Setup | Server

This section provides configuration procedures for server administration and settings.

Topics:

Administration

You can manage the following key settings on the **Server > Administration** page:

Email Security Master Account

Change the master account username and password in the **Email Security Master Account** section.

NOTE: SonicWall strongly recommends that you change the master account password.

To change the password:

1. Navigate to **Email Security Master Account** section of the **Server > Administration** page on the **MANAGE** view. Note that the **Username** you originally registered with appears as the default Username.
2. Type in the **Old password**.
3. Type in the **New password**.
4. Type the same new password in the **Confirm password** field.
5. Click **Apply Changes**.

User Interface Preference

The user interface was enhanced in the Hosted Email Security 10.0 release. The new menu structure aligns commands under the key functions of **MONITOR**, **INVESTIGATE**, and **MANAGE**. Related commands are grouped on the left-hand menu under divider labels for easier navigation.

In the **User Interface Preference** section, you can choose which interface you want to use. The **Enhanced** interface is the default, but you can select **Classic** if you prefer the old interface. Be sure to **Apply Changes** if you change the setting.

A table that maps the old interface to the new interface is provided in Interface Map.

Miscellaneous

In the **Miscellaneous** section, you can **Enable Support user to handle organization changes**.

1. Check the box next to Enable Support user to handle organization changes.
2. Click on the **Apply Changes** button.
3. A **Success** popup window notifies you that you have saved support role authorization changes.

Allow Admin Access from Specific IPs

This feature allows the administrator to add restricted IP addresses or address ranges. This restricts administrators so that they have admin access only from those specific IP addresses. The IP addresses can be entered in these formats: IPv4, IPv6, or IPv4 CIDR. Multiple IPs can be entered but must be separated by commas.

IMPORTANT: Users with admin roles can be locked out of web access if the incorrect IPs are specified.

LDAP Configuration

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 on your mail server, this information is automatically reflected in 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 Hosted Email Security can automatically get user information from these directories using LDAP. You can run SonicWall Hosted Email Security without access to an LDAP server as well.

NOTE: If your organization does not use a directory server, users cannot access their Junk Boxes, and all inbound email is managed by the message-management settings defined by the administrator.

SonicWall Hosted Email Security uses the following data from your mail environment:

- **Login Name and Password**

  When users attempt to log into the Hosted 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 Hosted Email Security in real time.

- **Multiple Email Aliases**

  If your organization allows users to have multiple email aliases, Hosted 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**

  Email groups or distribution lists in your organization are imported into SonicWall Hosted 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. 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 is filtered, but they cannot view their personal Junk Box or change default message management settings.

The default view for the LDAP Configuration page shows the **Available LDAP Servers** section expanded and the other sections (Global Configurations, Server Configuration, LDAP Query Panel, and Add LDAP Mappings) minimized. The **Available LDAP Servers** lists the LDAP servers that have been configured and provides the option to add, edit, or delete a server.

Read-Only for OU LDAP Configurations

Multi-tenant root administrators need the ability to set the LDAP configuration options to read-only on a tenant by tenant basis. The goal is to not allow OU administrators to edit or change such items as User/Group Directory Search parameters. This is especially important where a single AD/LDAP directory structure is being utilized by root tenant for all serviced OUs and their administrators. It also keeps OU administrators from seeing the rest of the LDAP directory by altering search directory parameters.

Configuring LDAP

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.

To add an LDAP server or configure an existing server:

1 Navigate to the **Server > LDAP Configuration**.

2 Click the **Add Server** button to add a new LDAP Server or select the **Edit** icon to edit a server's configuration. The Server Configuration section of the page opens.

> **NOTE:** When the **Server Configuration** section is expanded to allow editing, the **LDAP Query Panel** and **Add LDAP Mappings** sections are also enabled for editing.

Server Configuration

To configure or edit a server:

1 Check one of the following boxes that appear under the **Settings** section:

- **Show Enhanced LDAP Mappings fields**—Select this option for Enhanced LDAP or LDAP Redundancy. You have to specify the Secondary Server IP address and Port number.
- **Auto-fill LDAP Query fields when saving configuration**—Select this option to automatically fill the LDAP Query fields upon saving.

2 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 drop-down list.
- **LDAP page size**—Specify the maximum page size to be queried. The default size is 100.
- **Managed Domains**—Uses your organization's email address domain to add users to your account automatically.
- **Requires SSL**—Select this check box if your server requires a secured connection.
- **Allow LDAP referrals**—Leaving this option unchecked disables LDAP referrals and speed up logins. You may select this option if your organization has multiple LDAP servers in which the LDAP server can delegate parts of a request for information to other LDAP servers that may have more information.

3 In the **Authentication Method** section, specify if the LDAP login method for your server is by **Anonymous Bind** or **Login**.

4 Specify the **Login name** and **Password**. This is the credential used to allow a user access to the LDAP resource. It may be a regular user on the network, and 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.

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 Hosted Email Security.

6 Click **Save Changes**.

LDAP Query Panel

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

Query Information for LDAP Users

Email Security uses your existing Active Directory or LDAP server to authenticate groups as they log into their Junk Boxes. This LDAP configuration section must be filled out correctly to return the complete list of groups who are allowed to log into their Junk Box. If a group does not appear in this list, their email is still filtered, but they can not log in to the group junk box. Refer to the detailed field help for information on each of the text fields.

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 check box 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 Hosted Email Security automatically complete the remainder of this section.

Query Information for LDAP Groups

Email Security uses your existing Active Directory or LDAP server to authenticate groups as they log into their Junk Boxes. This LDAP configuration section must be filled out correctly to return the complete list of groups who are allowed to log into their Junk Box. If a group does not appear in this list, their email is still filtered, but they can not log in to the group junk box. Refer to the detailed field help for information on each of the text fields.

If you have a large number of user mailboxes, applying these changes could take several minutes.

1 Navigate to **MANAGE | SYSTEM SETUP | LDAP Configuration**.

2 Enter values for the following fields:

- **Directory node to begin search**—The node of the LDAP directory to start a search for users.
- **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.

3 Click the **Test User Query** button to verify that the configuration is correct.

4 Click **Save Changes** to save and apply all changes made.

NOTE: Click the Auto-fill Group Fields button to have SonicWall Hosted Email Security automatically complete the remainder of this section.

Add LDAP Mappings

SonicWall Hosted Email Security uses your existing Active Directory or LDAP server to authenticate end users as they log in to their personal Junk Boxes. The **Add LDAP Mappings** segment of the page must be correctly filled out to return the complete list of users who are allowed to log in to their Junk Box. If a user does not appear in this list, their email is filtered, but they can not log in to their personal junk box.

For the Microsoft Window Environment

In a Microsoft Windows environment, you need to specify the NetBIOS domain name, sometimes called the pre-Windows 2000 domain name.

To locate the NT/NetBios domain name:

1 Login to your domain controller.

2 Navigate to **Start > All Programs > Administrative Tools > Active Directory Domains and Trusts**.

3 In the left pane of the Active Directory Domains and Trusts dialog box, highlight your domain.

4 Click **Action**.

5 Click **Properties**. In the domain's Properties dialog box on the General tab you should find the domain name or pre-Windows 2000 name.To add the Windows NT/NetBIOS domain names:

1 Add the Windows NT/NetBIOS Domain Names into the field provided. Domain names can be made of up to 200 alphanumeric characters with hyphens and periods allowed.

2 Separate multiple domain names with a comma.

3 Click **Save Changes** to save the new domain names.

For the LDAP Environment

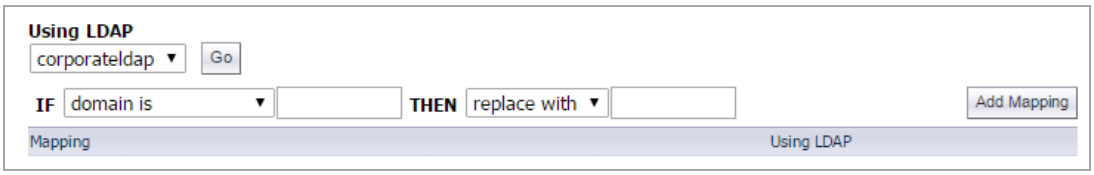
On some LDAP servers, such as Lotus Domino, some valid addresses do not appear in LDAP, for example, LDAP servers that only store the “local” or “user” portion of the email addresses. This section provides a way to add additional mappings from one domain to another. For example, a mapping could be added that would ensure emails addressed to anybody@engr.corp.com are sent to anybody@corp.com.

It also provides a way of substituting single characters in email addresses. For example, a substitution could be created that would replace all the spaces to the left of the “@” sign in an email address with a “-”. In this example, email addressed to Casey Colin@corp.com would be sent to Casey-Colin@corp.com

NOTE: This feature does not make changes to your LDAP system or rewrite any email addresses; it makes changes to the way SonicWall Hosted Email Security interprets certain email addresses.

To add LDAP Mappings:

1 Scroll to the Conversion Rules section, and click **View Rules**.



2 From the first and second drop-down list, choose one of the following combinations:

First drop-down menu	Second drop-down menu	Resulting action
domain is	**replace with**	The domain name typed in the first field is replaced with the domain name typed in the second field.
domain is	**also add**	When domain listed in the first field is found, the second domain is added to the list of valid domains.

First drop-down menu	Second drop-down menu	Resulting action
left hand side character is:	**replace with**	The character typed in the first field is replaced with all characters to the left of the “@” sign in the email address.
left hand side character is:	**also add**	A second email address is added to the list of valid email addresses.

3 Enter text into the text fields as dictated by your choices.

4 Click the **Add Mapping** button.

Updates

SonicWall Hosted Email Security uses collaborative techniques as one of many tools to block junk messages. The collaborative database incorporates thumbprints of junked email from SonicWall Anti-Spam Desktop and SonicWall Junk Button products as well as thumbprints generated by the Email security products team. Your appliance uses the HTTP and HTTPS protocols to communicate with a data center hosted by SonicWall to download data used to block spam, phishing, viruses, and other evolving threats.

To configure settings for updates to the Hosted Email Security service:

1 Navigate to the **SYSTEM SETUP | Server > Updates** page.

2 Check the box next to **Submit URLs** to enable your collaborative settings.

3 Click the **Apply Changes** button.

Monitoring

The **SYSTEM SETUP | Server > Monitoring** page allows you to configure settings and alerts for system monitoring. Some of these fields may be pre-defined based on the information provided upon initial setup of Hosted Email Security.

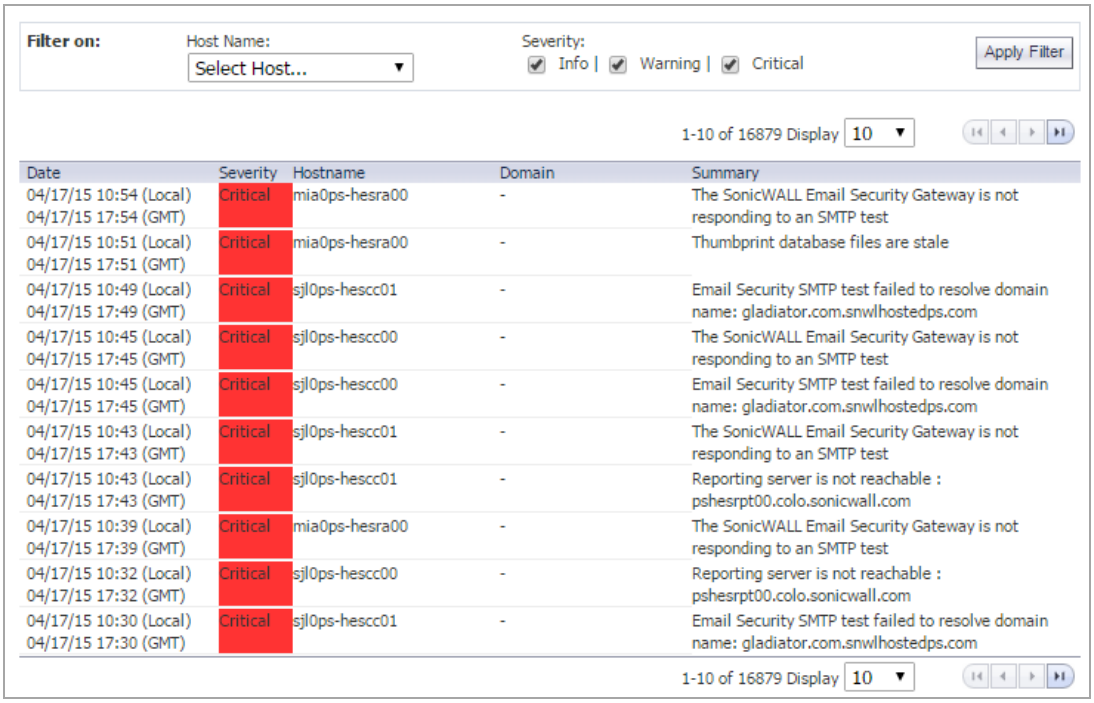
NOTE: If you are running SonicWall Hosted Email Security in split mode, and you route outbound email through Hosted Email Security, you must enter the IP addresses or fully-qualified domain names of any Remote Analyzers through which outbound email is routed in this text box on the Control Center.

Configure System Monitoring

You can set up Hosted Email Security to monitor certain parameters and notify key personnel.

To configure the Monitoring section:

1. Provide the **Email address of the administrator who receives emergency alerts** in the text box. Enter the complete email address: for example, user@example.com. Separate multiple email addresses with a comma.
2. **Select the preferred language to send alerts** from the drop-down menu.
3. If you want to **Use MX Record to deliver mail**, check the box.
4. Enter the **Name or IP address of backup SMTP servers**. You may have one or more SMTP servers that are used as fallback servers to send alerts to if the configured downstream email server(s) cannot be connected. Separate multiple entries with a comma.
5. Enter a **Customized signature** to append at the end of your email messages.
6. Check the box next to **Subscribe to alerts**.
7. Click on **Apply Changes**. If you want to go back to prior settings click on **Revert**.
8. Click on **Test Fallbacks** to make sure you are connected to the monitoring SMTP server.
9. Click on **View Alerts** to view all configured alerts. You can filter by server or by host name. Time stamp and summary of the issue is also provided.



10

System Setup | Customization

This section provides information on the **SYSTEM SETUP | Customization** option.

Topics:

User View Setup

You can customize the user view by setting the options on this page. Select **Apply Changes** to save any updates you make. Click **Revert** to revert back to the previously saved settings.

To configure User View Setup:

Check the **Login enabled** box to allow users to log into Hosted Email Security and have access to their personal settings and Junk Box. By default, if a user can log in and has items in his or her Junk Box, the Junk Box icon is visible to the user. If you disable this, mail is still analyzed and quarantined, but users do not have access to their Junk Box.

For the remaining items in this section, you can select the features that are made available to the users in your organization. For example, an administrator can specify that users may not administer their own allowed and blocked lists. Checked items appear in the navigation toolbar for users.

1. **Login enabled** allows users to access their personal settings and Junk Box by logging into their individual accounts. By default, if a user can log in and has items in his or her Junk Box, the Junk Box icon is visible to the user. For the remaining items in this section, you can select the features that are made available to the users in your organization. For example, an administrator can specify that users may not administer their own allowed and blocked lists. Checked items appear in the navigation toolbar for users.
2. **Anti-spam** includes the user-configurable options available for blocking spam emails. People, companies, lists, aggressiveness and languages are the categories of Allowed and Blocked lists the user can customize.
3. If the Anti-Spam option is selected you can also allow users to have **Full user control over anti-spam aggressiveness settings**. Check the box to enable full control by the user.
4. Continuity enables **email continuity** for the hosted user. Users can view and reply to email messages even when the users' downstream server is unavailable
5. **Reports** provides junk email blocking information about your organization as a whole. Even if this option is checked, users may view only a small subset of the reports available to administrators.
6. **Policy** enables user to define policy settings.
7. **Settings** provide options for management of the user's Junk Box, including setting up individual junk summary reports and specifying delegates.
8. If the Settings options is selected, you can also enable **Spam Management** for the user.

9 **Allow audit view to Helpdesk users** lets the support staff on the Helpdesk view audit information so they can more effectively help with diagnostics, when needed.

NOTE: Checked items appear in the navigation tool bar for users.

To define the User download settings section:

1 Select the **Allow users to download SonicWall Junk Button for Outlook** check box so users can download the Hosted Email Security Junk Button for Outlook. The Junk Button is a lightweight plugin for Microsoft Outlook that allows users to mark emails they receive as junk, but it does not filter email.

2 Select the **Allow users to download SonicWall Anti-Spam Desktop for Outlook and Outlook Express** check box so users can 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.

3 Select the **Allow users to Download SonicWall Secure Mail Outlook plugin** check box, so users can download the Secure Mail plugin for Microsoft Outlook. The Secure Mail button allows users to send mail securely through the Encryption Service.

To define the Quarantined junk mail preview settings:

1 Check the box so generic users can preview their own quarantined junk mail.

2 Choose which other types of users can preview quarantined junk mail for the entire organization:

- Administrators
- Help Desk and Group Administrators

To define the Report view settings:

1 Select the option to **Show reports that display information about individual employee**.

2 Choose which other types of users can view the reports:

- Administrators
- Help Desk and Group Administrators

To define the Policy View Settings:

Check the box to enable those with the Helpdesk or Manager roles to view the users' approval boxes.

Branding

Branding provides the ability to customize aspects of the user interface. Administrators can upload replacement assets for the key branding elements, including company name, logo, and other branding assets. Navigate to **SYSTEM SETUP | Customization > Branding** on the **MANAGE** view to configure Branding feature settings. Select either the **Quick Settings** tab or the **Packages** tab. The **Quick Settings** tab allows administrators to specify global settings for the most commonly modified asset files on the GUI. The **Packages** tab allows administrators to manage, upload, and apply branding packages to their GUI.

Topics:

Quick Settings

Use the Quick Settings tab on the **SYSTEM SETUP| Customization > Branding** page to specify global settings for particular user interface elements.

NOTE: Any settings specified in this section overrides those specified by deployed packages.

Text Preferences

The **Contact Us URL** is the email address or URL that appears as the “Contact Us” link at the footer of each page. This field supports “http://”, “https://”, and “mailto:” formats. To change the **Contact Us URL**, type the email address or URL in the field provided.

Click the **Test Connectivity** button to verify the email address or URL you specified is valid.

Image Preferences

The **Image Preferences** files can all be modified by clicking the **Choose File** button or clicking the **Download** icon. The Choose File option allows you to select a file from your local system. The **Download** icon downloads the default SonicWall image file. Note that an error message displays if you upload an incorrect file type.

The following Image Preferences can be modified:

- Web Icon file—This field replaces the 4-bit SonicWall logo that appears in the address bar of every web page across all browser platforms.
- Logon logotype file—This field replaces the logon, logout, and mini-logon generic bitmap that displays the SonicWall challenge screen layout and design.
- Logon backdrop art file—This field replaces the logotype bitmap that appears upon every challenge screen.
- Page logotype file—This field replaces the short version of the SonicWall logotype that appears at the top of each web page’s banner art.
- Page header art file—This field replaces the SonicWall banner art bitmap at the top of each web page.
- Pop-up logotype file—This field replaces the smaller version of the SonicWall logotype that appears at the top of each pop-up dialog’s page banner art.
- Pop-up header art file—This field replaces the smaller version of the SonicWall banner art that appears at the top of each pop-up dialog page.

Junk Summary Preferences

The **Junk Summary Preferences** can all be modified by clicking the **Choose File** button or clicking the **Download** icon. The **Choose File** option allows you to select a file from your local system. The **Download** icon downloads the default SonicWall image file. Note that an error message displays if you have uploaded an incorrect file type.

The following Junk Summary Preferences can be modified:

- **Junk Summary logotype file**—This field replaces the black-on-white logotype that always appears at the top of each Junk Summary email.
- **Junk Summary header art file**—This field replaces the Junk Summary banner art bitmap at the top of each page.

Click the **Save** button when you have finished modifying settings on the **Quick Settings** tab.

Packages

The Packages tab allows administrators to manage, upload, and apply branding packages to their user interface. The Manage Packages table displays the available packages the administrator can apply, including the SonicWall brand package.

NOTE: The SonicWall branding package can never be deleted, but administrators can edit or delete all other brand packages that have been uploaded.

To upload a new package:

1. Navigate to **SYSTEM SETUP| Customization > Branding** on the **MANAGE** view.
2. Click the **Packages** button.
3. Click the **Upload** button under the **Manage Packages** section.

   NOTE: Uploads are restricted to `.zip` files and must contain the exact structure of the directories being modified or replaced.

4. Click on **Choose File** and navigate to and select the **File to upload**.
5. Enter the **Brand Label** name.
6. Enter the **Full name** of the packaging label.
7. Provide the email address or web sites as a contact point listed in the **Contact Us** field.
8. Add any additional notes about the package in the **Notes** field.
9. Click on **Save** to upload the package.

To manage the packages once they are loaded in the table, you can click on the management icons (**Edit**, Download, or **Delete**) listed in the **Configure** column of the table.

11

Users, Groups & Domains

The **Users, Groups & Domains** section gives you the ability to set parameters on individuals or on subsets of the whole company.

Topics:

- Users
- Groups
- Domains

NOTE: To manage users and groups, you have to configure your SonicWall Hosted Email Security setup to synchronize with your organization's LDAP server. Refer to LDAP Configuration for more information on configuring LDAP settings and queries.

Users

SYSTEM SETUP | Users, Groups & Domains > Users displays the list of users who can log in. The list is determined by the query entered on the **SYSTEM SETUP | Server > LDAP Configuration** page. While Hosted Email Security filters the email messages received by users not on the list, such users cannot log in to configure their individual settings.

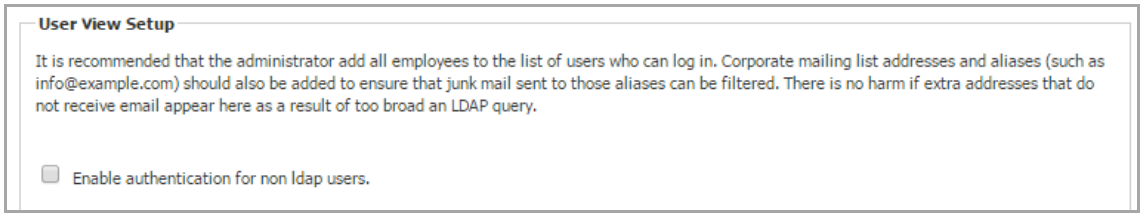
NOTE: The user data may come from multiple sources, so before performing a task on any user, select an option from the **Using Source** drop-down list, then click **Go**.

Select the **Refresh Users & Group** button to refresh the entries in the data table.

User View Setup

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

To **Enable authentication for non-LDAP users**, select the corresponding check box in the **User View Setup** section under **Users**.



Searching for Users

If too many users show in a window, you can conduct a search using the **Find all users in column** search tool.

To use this search feature:

1. Navigate to the **SYSTEM SETUP | Users, Groups & Domains > Users** page.
2. In the drop-down list, choose the search type: **User Name** or **Primary Email**.
3. In the next drop-down list, select from the search parameters: **equal to (fast)**, **starting with (medium)**, or **containing (slow)**.
4. In the text field, type the word or phrase you are searching for.
5. Check the box if you want the search to **Show LDAP entries** or **Show non-LDAP entries** next to each option.
6. Click **Go**.

Sorting the User List

To sort the list of users, click the **User Name** or **Primary Email** heading. The arrowhead in the column indicates whether the data is sorted in ascending or descending order. Click the arrowhead to reverse the order.

Signing In as a User

You can sign in as any user in the list, see their Junk Box, and change the settings for that user. You can also manage an user's delegates for them. Select the check box next to the **User Name**, then click the **Sign In as User** button.

The user's Junk Box is displayed and you can make changes as needed. Refer to the *SonicWall Email Security Administration Guide* for more information, if needed.

Editing User Rights

Administrators can assign different privileges to different users by assigning them pre-defined roles. The pre-defined roles are described below.

Pre-defined Roles for Users and Groups

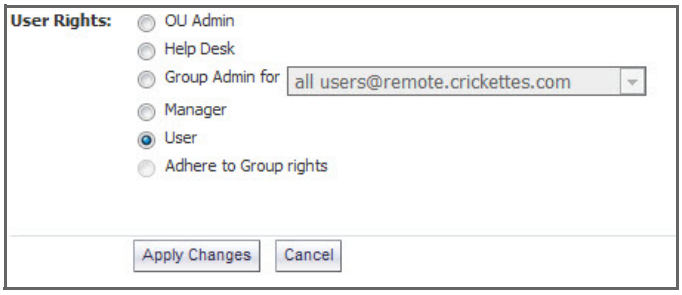
Role	Description
OU Admin	The Admin role has full administrative rights to a specific list of domains the Global Administrator specifies. Typically, the Global Administrator of an enterprise-sized organization may wish to delegate the management of a smaller group of domains, or Organizational Units, between several users requiring administrative rights for successful management of these OUs. The OU Admin can log in as any other user within the group of domains assigned to change a user's individual settings, view and manage Junk Boxes, and configure other areas of the SonicWall system.
Help Desk	A user assigned as Help Desk has access to the corporate Junk Box and can unjunk items. This role also allows the user to log in as any user to change that user's individual settings and view Junk Boxes. The Help Desk role does not allow the user to change global settings or other server configurations.

Pre-defined Roles for Users and Groups

Role	Description
Group Admin for	A group administrator role is similar to the Help Desk role except that this role's privileges are limited to users for the group that they are specified to administer. The Group Admin role is always associated with one or more groups added to the Spam Blocking Options for Groups section.
Manager	A user assigned as Manager has access to corporate Reports and Monitoring screens. The user cannot change any configuration settings, nor are they able to sign in as any other user.
User	A user role is only allowed to log in to the SonicWall Hosted Email Security system, has access to his own individual user settings, and can only customize his own settings.
Adhere to Group rights	The user rights are made to adhere to the right of the group.

To assign a role to a user:

1 Select the user and click on **Edit User Rights** button.



2 Choose which role to assign to a user. (Refer to Pre-defined Roles for Users and Groups.)

3 Click on **Apply Changes**.

Resetting User Message Management 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.

Adding a User

The administrator can add individual non-LDAP users.

1 Fill out the **Primary Address** field.

2 If users have aliases associated with them, added them the **Aliases** field. Separate each alias with a carriage return.

3 Click **Add**. This is not dependent on LDAP status.

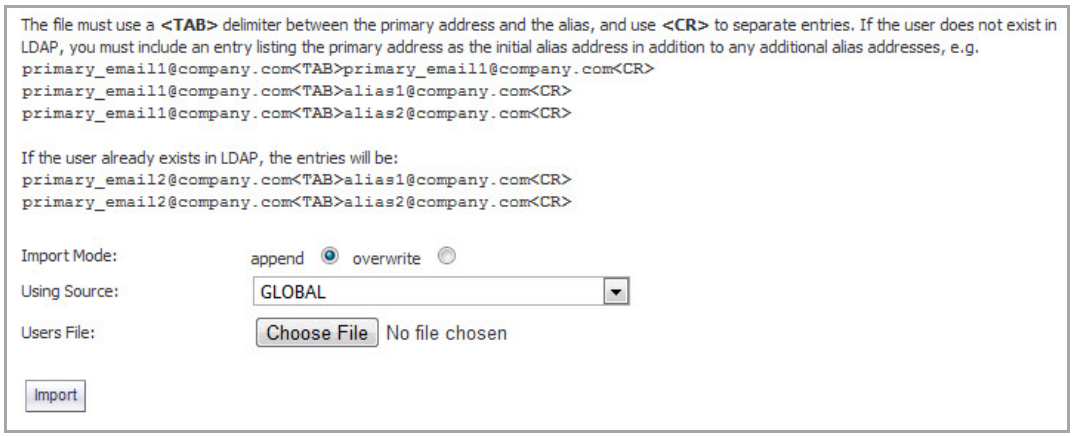
NOTE: Users added in this way remain non-LDAP users. Their User Rights can be changed. Their source is listed as Admin. Users can edit their Junk Box setting only if the administrator sets the Junk Box setting: **Enable "Single Click" viewing of messages** to **Full access** on the **SYSTEM SETUP | Junk Box > Summary Notifications** page.

Removing Users

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

Importing Users

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:

1. Click the **Import** button.
2. Set the **Import Mode** to **append** or **overwrite**.
3. **Choose File** to locate the file and click **Import**.

Exporting Users

The administrator can download a tab-delimited list by clicking **Export**. The file generated lists multiple non-LDAP users and can edited and imported later.

Locked Users

On the Users page, in the **Locked Users** section, SonicWall Hosted Email Security displays a list of users that are currently locked out. The administrator can reset the lockout for any user.

To unlock the user:

1 Check the box by the locked out user or select multiple users.

2 Select the **Unlock User** button.

Groups

Navigate to the **SYSTEM SETUP | Users, Groups & Domains > Groups** page to manage Group settings. Settings on this page are optional. The members of each group listed on this page are determined from LDAP. Groups are refreshed automatically from LDAP once per hour

This section describes how SonicWall 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. Different groups may have—or need—different settings specified. Configure LDAP groups on your corporate LDAP server before configuring the rights of users and groups on SonicWall Hosted Email Security in the LDAP Configuration screen.

SonicWall 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, SonicWall 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.

NOTE: Any policy filter created by a group admin is applicable to all users belonging to the group.

Updates to groups settings in this section do not get reflected immediately. The changes are 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.

Topics:

- Assigning Roles to Groups Found in LDAP
- Set Junk Blocking Options for Groups Found in LDAP

Assigning Roles to Groups Found in LDAP

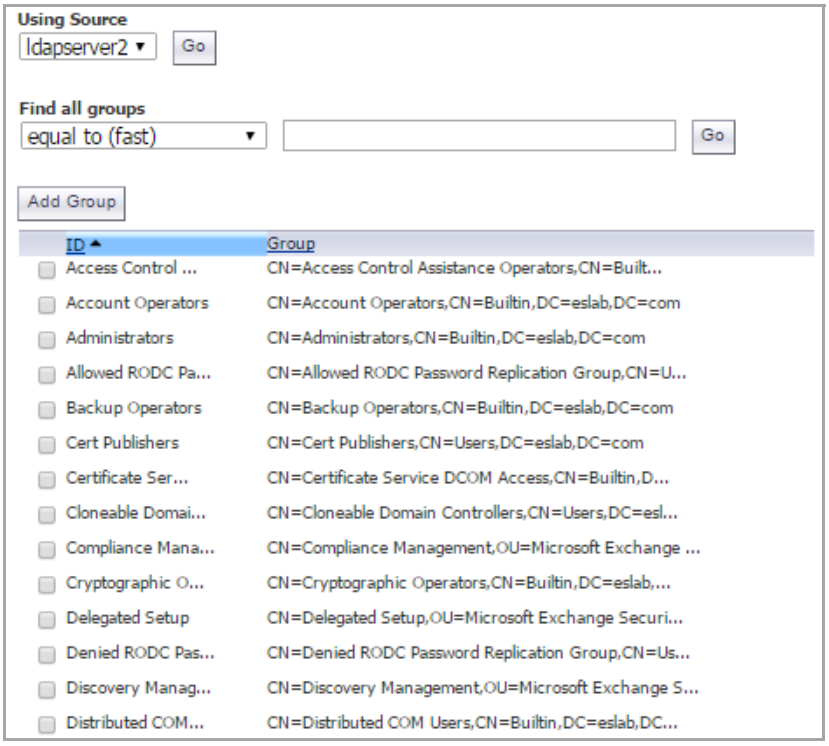
Topics:

- Finding and Adding a Group
- Removing a Group
- Listing Group Members
- Setting an LDAP Group Role

Finding and Adding a Group

To find a group to add:

1 Click the **Add Group** button under the heading **Assign Roles to Groups Found in LDAP**.



2 Choose the search mechanism in the **Find all groups** field. Select from **equal to (fast)**, **starting with (medium)**, or **containing (slow)**.

> **NOTE:** The type of search you choose could affect the length of the search. The relative speed is indicated in the parentheses.

3 Type the search string in the text box.

4 Click **Go** to begin the search.

> **NOTE:** Optionally, you can scroll through the list of groups to locate the group you want to add.

5 Check the box next to the group you want to include.

6 Click **Add Group**. A message displays stating that the group was added successfully.

Removing a Group

To remove a group:

1 Click the check box adjacent to the group(s) to remove.

2 Click the **Remove Group** button. A success message displays.

Listing Group Members

To list group members:

1 Click the check box adjacent to the group to list.

2 Click the **List Group Members** button. Users belonging to that group are listed in a pop-up window.

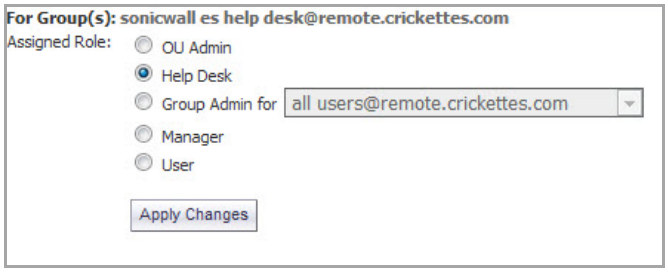
Setting an LDAP Group Role

All members of a group are also given the role assigned to the group.

To set the role of a group:

1 Click the check box adjacent to the group to edit.

2 Click **Edit Role**.



3 Select the appropriate role that you want to assign to the group. Definitions for these roles can be found in Pre-defined Roles for Users and Groups.

4 Click **Apply Changes**. A message appears stating that the group was changed successfully.

NOTE: 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 SonicWall, but are updated within an hour.

Set Junk Blocking Options for Groups Found in LDAP

In this section of the Groups page, you can set up and manage the groups that need to be set up for junk blocking. Each group can have different settings.

Topics:

- Find and Add a Group
- Remove a Group
- List Members
- Edit Junk Blocking Options

Find and Add a Group

To find a group to add:

1 Click the **Add Group** button under the heading **Set Junk Blocking Options for Groups Found in LDAP**.

2 Choose the search mechanism in the **Find all groups** field. Select from **equal to (fast)**, **starting with (medium)**, or **containing (slow)**.

> **NOTE:** The type of search you choose could affect the length of the search. The relative speed is indicated in the parentheses.

3 Type the search string in the text box.

4 Click **Go** to begin the search.

5 Check the box next to the group you want to include.

6 Select **Add Group**. A message displays stating that the group was added successfully.

Remove a Group

To remove a group:

1 Select the check box adjacent to the group or groups to remove.

2 Click the **Remove Group** button. A success message displays.

List Members

To list group members:

1 Select the check box adjacent to the group to list.

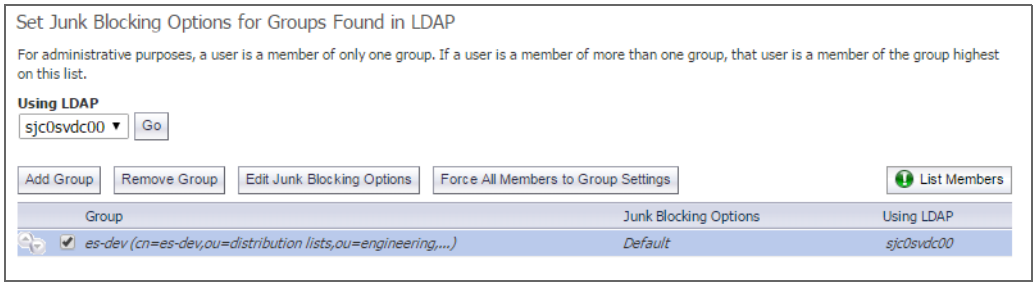
2 Click the **List Group Members** button. Users belonging to that group are listed in a pop-up window.

Edit Junk Blocking Options

Once a group has been added you can set up the junk blocking options for the group. You can choose to adhere to junk blocking parameters that have been defined for the corporate level, or you can customize the options for each group. The following parameters can be set:

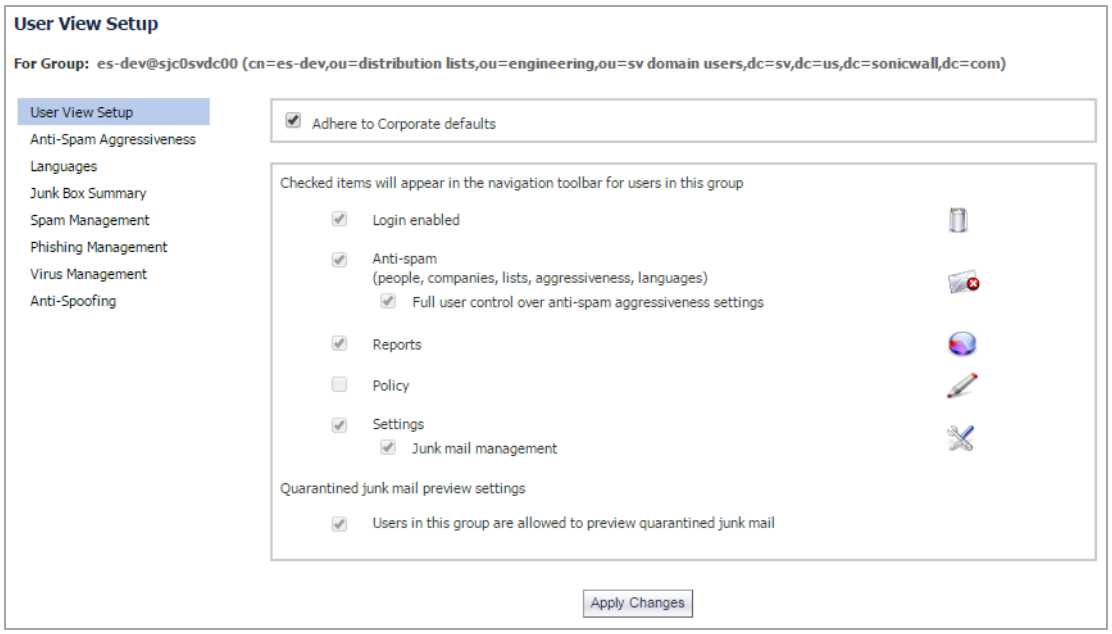
- User View Setup
- Anti-Spam Aggressiveness
- Languages
- Spam Management
- Phishing Management
- Virus Management
- Anti-Spoofing

To edit junk blocking options:



1 Check the box by the name of the group for which you want update junk blocking options.

2 Select **Edit Junk Blocking Options**. The following page displays with User View Setup as the default view. Each of the Junk Blocking Options are described in more detail the following sections.



User View Setup

The User View Setup option for Junk Blocking controls what options are available to the users in this group when they log in to the server using their user name and password. Enable any of the options by checking the box associated with the option. The options are defined in User View Setup Options. Be sure to select **Apply Changes** when done.

User View Setup Options

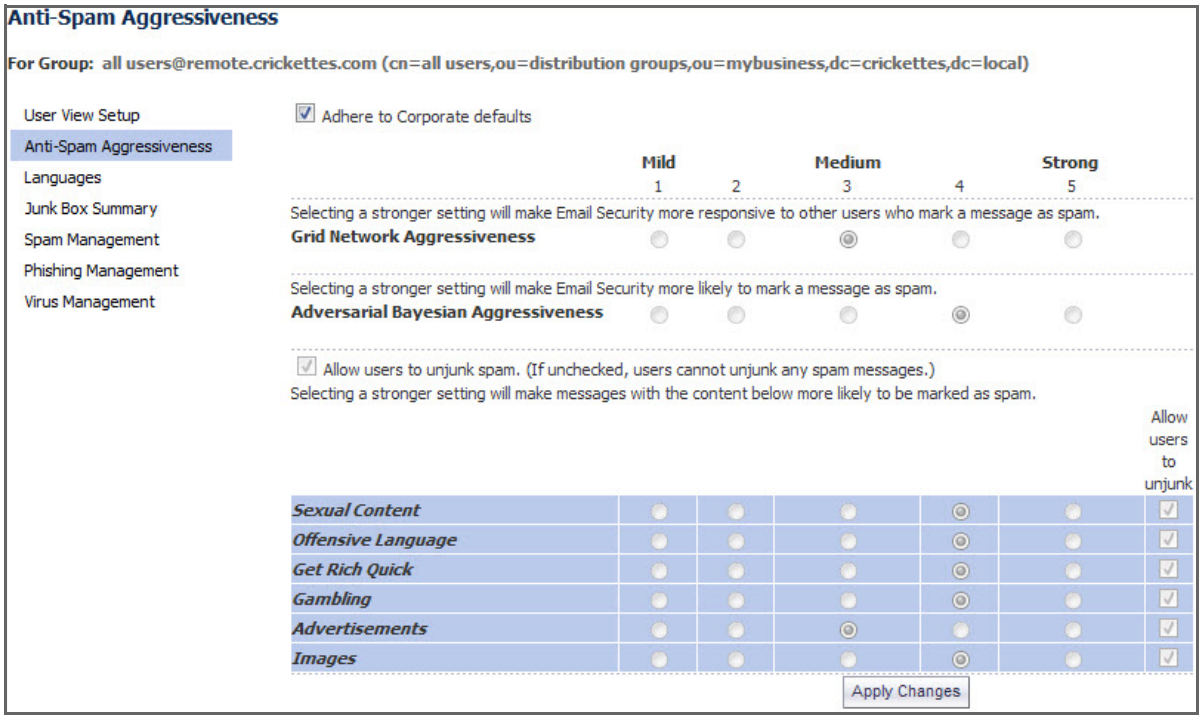
Option	Definition
Adhere to Corporate defaults	Sets the group options the same as the options defined at the corporate level. If this option is selected, the other options are grayed out and not available.
Login enabled	Enables users in this group to log into their Junk Box.
Anti-spam	Allows or blocks specified people companies, lists, aggressiveness and languages. You can enable more user control by checking the box for **Full user control over anti-spam aggressiveness settings**.
Reports	Allows users in this group to view their spam reports.

User View Setup Options

Option	Definition
Settings	Enables users in this group to view their settings. You can allow user access to their junk management settings by also checking the box for **Junk mail management**.
Quarantined junk mail preview settings	Allows users to preview quarantined junk mail if the box is checked for **Users in the group are allowed to preview quarantined junk mail**.

Anti-Spam Aggressiveness

On the Junk Blocking Options page, select **Anti-Spam Aggressiveness** on the left of the page. Here you can opt to **Adhere to Corporate defaults** by checking the box at the top of the page. If you wish to customize settings for the group, set the anti-spam aggressiveness as described below.

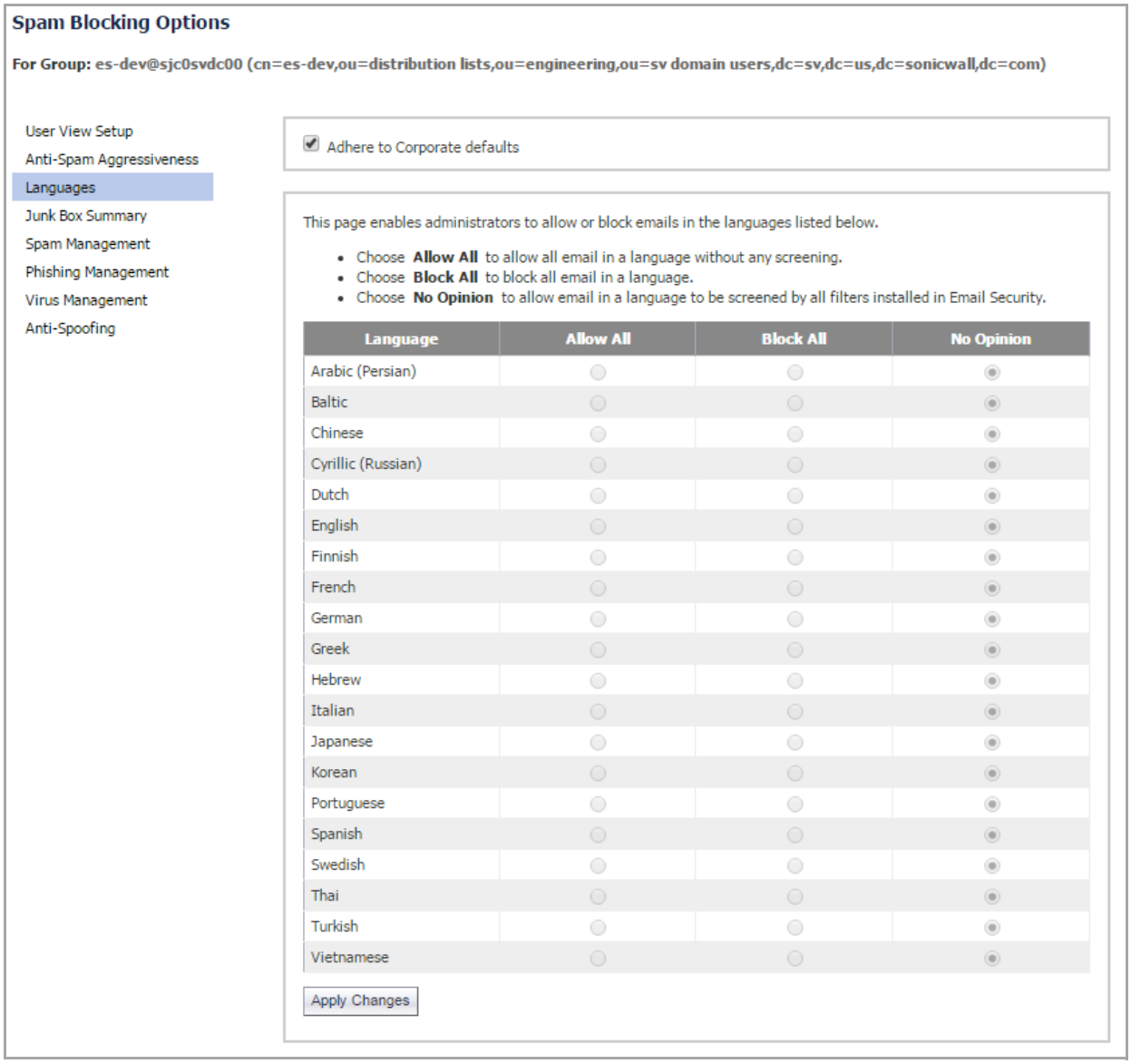


To configure Anti-Spam Aggressiveness settings for a group:

1. Choose the appropriate **GRID Network Aggressiveness** level for this group. Note that selecting a stronger setting makes Hosted Email Security more responsive to other users who mark a message as spam.
2. Choose the appropriate **Adversarial Bayesian Aggressiveness** level for this group. Note that selecting a stronger setting makes Hosted Email Security more likely to mark a message as spam.
3. Select the check box to **Allow users to unjunk spam**. If the check box is unchecked, users are not able to unjunk spam messages.
4. For each category of spam, determine level and whether members of the group are allowed to unjunk their Junk Boxes.
5. Click **Apply Changes**.

Languages

On the Junk Blocking Options page, select **Languages** on the left of the page. Here you can opt to **Adhere to Corporate defaults** by checking the box at the top of the page. If you wish to customize settings for the group, set the blocking options as described below.



To determine the foreign language emails that groups can receive:

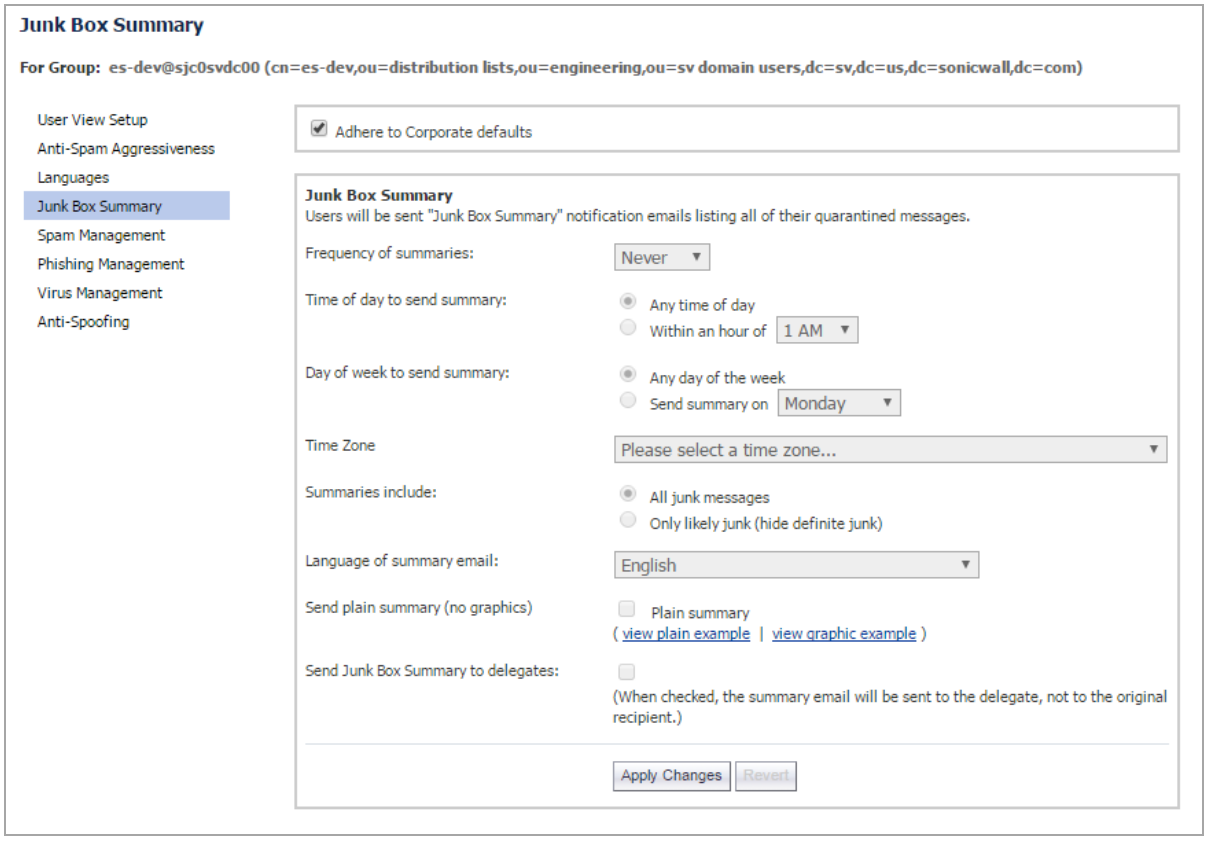
1 Select one of the following options for each language:

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

2 Click **Apply Changes** to save setting made.

Junk Box Summary

On the Junk Blocking Options page, select **Junk Box Summary** on the left side of the page. Here you can opt to **Adhere to Corporate defaults** by checking the box at the top of the page. If you wish to customize settings for the group, set the options for the Junk Box Summary as described below.



To configure settings for the Junk Box for groups:

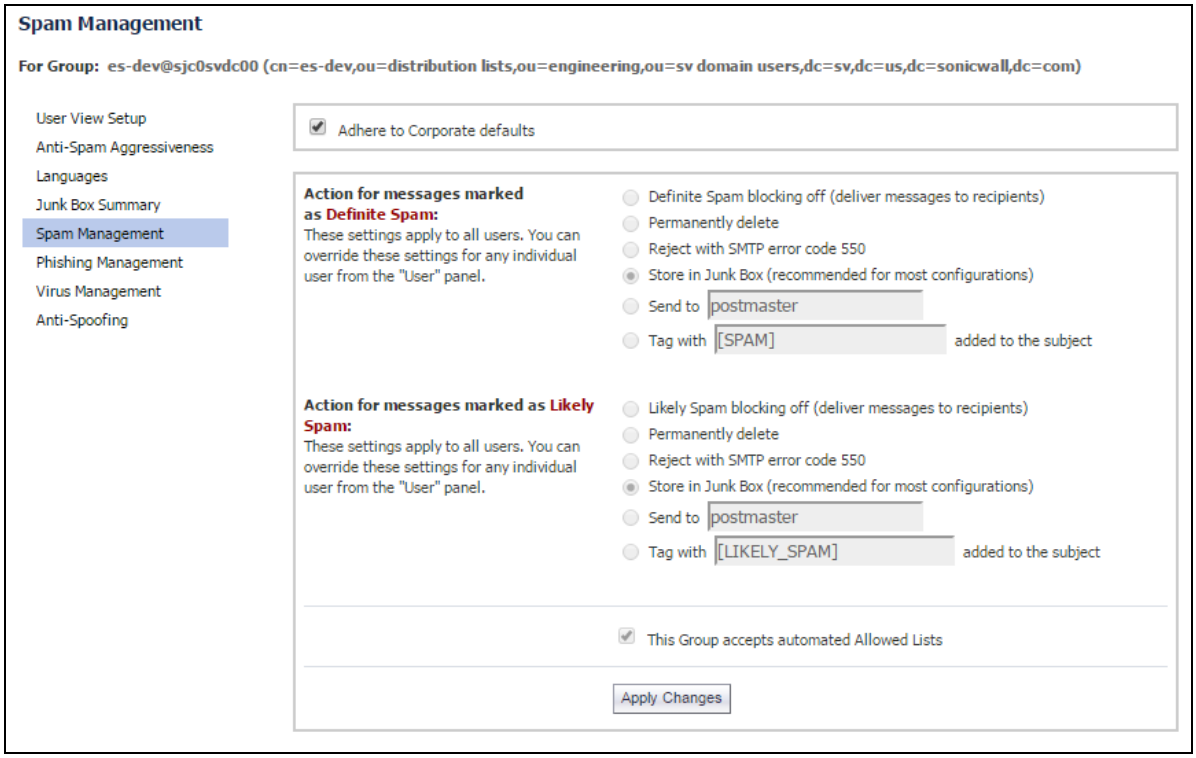
1. Select the **Frequency of Summaries** sent to users. Options include: **Never**, **1 Hour**, **4 Hours**, **1 Day**, **3 Days**, **7 Days** or **14 Days**.
2. Select the **Time of Day** users receive junk summary emails. Choose **Any time of day** or **Within an hour of** <*select hour*>.
3. Select the **Day of the Week** users receive junk summary emails. Choose **Any day of the week** or **Send summary on** <*select day*>.
4. Choose one option for summaries to include: **All junk messages** or **Only likely junk (hide definite junk)**.
5. Select the **Language of Summary Email** from the drop-down list.
6. Check the box if you want to receive a **Plain Summary.** The default is to receive a Graphic Summary.
7. Select the check box to if you want to **Send Junk Box Summary to Delegates**.

   NOTE: When this check box is selected, the summary email is sent to the delegate, not to the original recipient.

8. Click **Apply Changes**.

Spam Management

On the Junk Blocking Options page, select **Spam Management** on the left side of the page. Here you can opt to **Adhere to Corporate defaults** by checking the box at the top of the page. If you wish to customize settings for the group, set the options for mail tagged as Definite Spam and LIkely Spam as described below.



To manage Definite Spam or Likely Spam for this group:

1 Chose an action for messages marked as Definite Spam. The options are defined below.

- **Spam blocking off (deliver messages to recipients)**—Passes all messages to users without filtering.
- **Permanently Delete**—If determined Definite or Likely Spam, messages are permanently deleted.
- **Reject with SMTP error code 550**—Messages are sent back to the sender. 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.
- **Store in Junk Box (recommended for most configurations)**—Messages are quarantined in the Junk Box for review and deletion later.
- **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].

2 Choose an action message marked as Likely Spam. The options are the same as defined for Step 1.

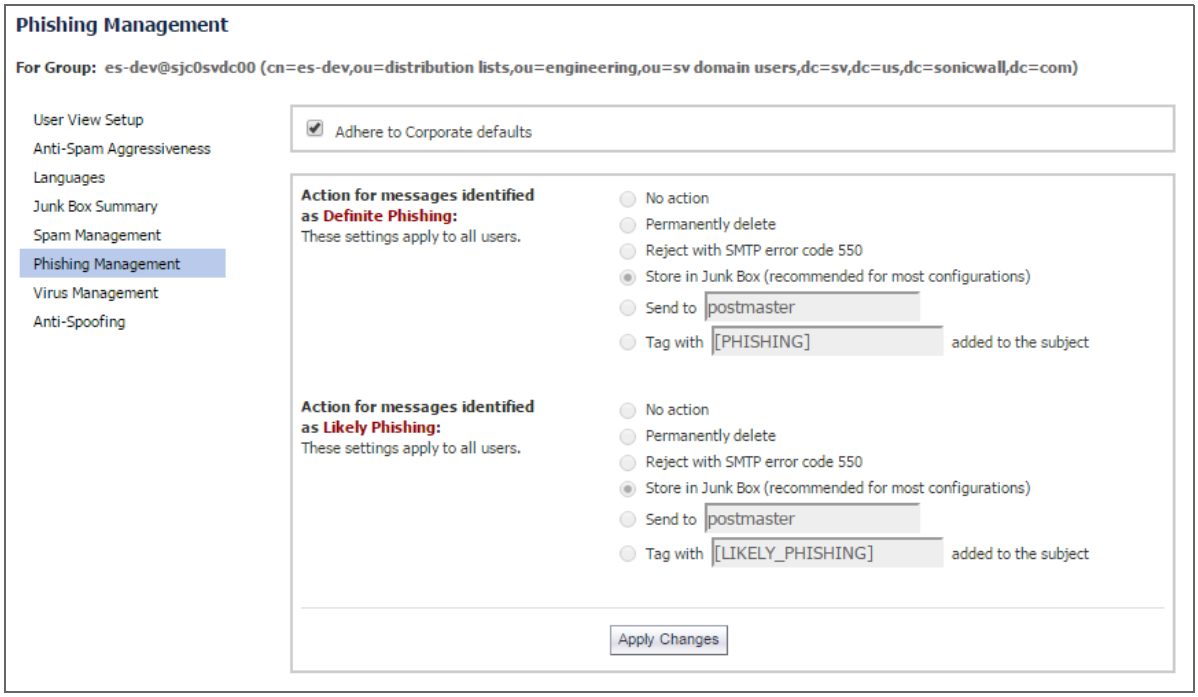
3 Select the check box **This Group accepts automated Allowed Lists** if you want automated Allowed Lists to apply to this group.

4 Click **Apply Changes**.

Phishing Management

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

On the Junk Blocking Options page, select **Phishing Management** on the left side of the page. Here you can opt to **Adhere to Corporate defaults** by checking the box at the top of the page. If you wish to customize settings for the group, set the options for mail tagged as Definite Phishing and LIkely Phishing as described below.



To manage Definite Phishing or Likely Phishing for this group:

1 Chose an action for messages marked as Definite Phishing. The options are defined below.

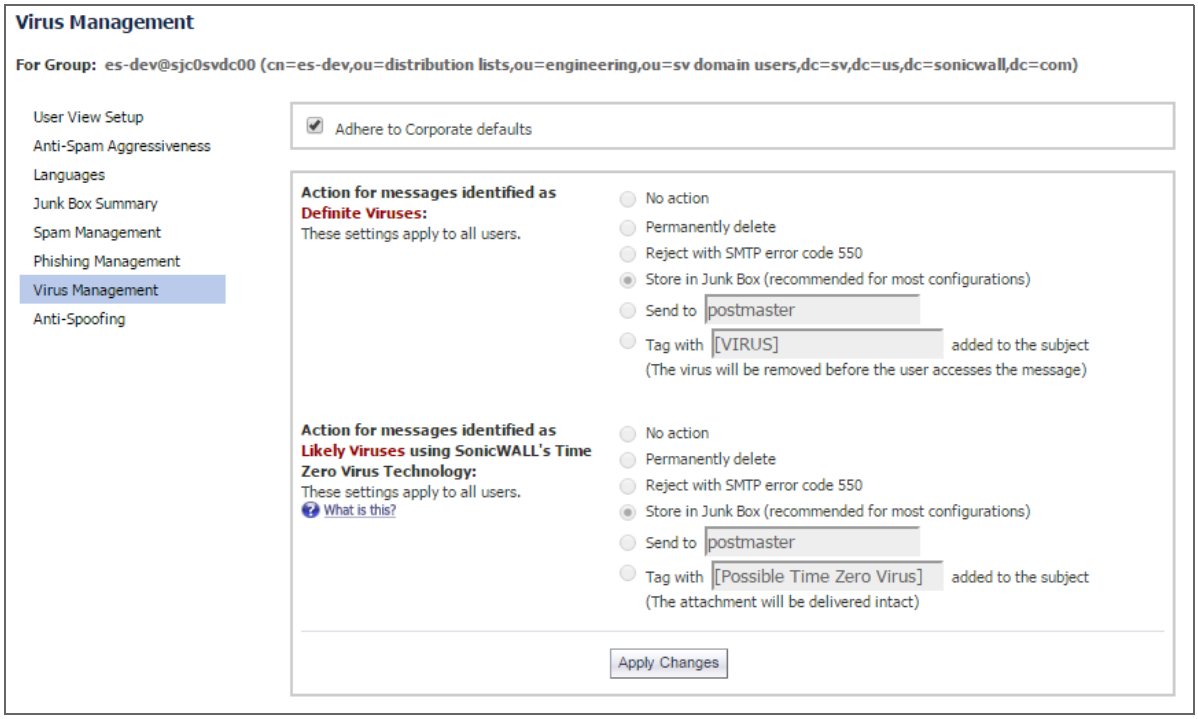
- **No action**—Passes all messages to users without filtering.
- **Permanently Delete**—If determined Definite or Likely Phishing, messages are permanently deleted.
- **Reject with SMTP error code 550**—Messages are sent back to the sender. In cases of self-replicating viruses that engage the sender's address book, this can inadvertently cause a denial-of-service to a non-malicious user.
- **Store in Junk Box (recommended for most configurations)**—Messages are quarantined in the Junk Box for review and deletion later.
- **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].

2 Choose an action message marked as Likely Phishing. The options are the same as defined for Step 1.

3 Click **Apply Changes**.

Virus Management

On the Junk Blocking Options page, select **Virus Management** on the left side of the page. Here you can opt to **Adhere to Corporate defaults** by checking the box at the top of the page. If you wish to customize settings for the group, set the options for mail tagged as Definite Viruses and LIkely Viruses as described below.



To manage Definite Viruses or Likely Viruses for this group:

1 Chose an action for messages marked as Definite Viruses. The options are defined below.

- **No action**—Passes all messages to users without filtering.
- **Permanently Delete**—If determined Definite or Likely Phishing, messages are permanently deleted.
- **Reject with SMTP error code 550**—Messages are sent back to the sender. 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.
- **Store in Junk Box (recommended for most configurations)**—Messages are quarantined in the Junk Box for review and deletion later.
- **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].

2 Choose an action message marked as Likely Viruses. The options are the same as defined for Step 1.

3 Click **Apply Changes**.

Anti-Spoofing

On the **Junk Blocking Options** page, select **Anti-Spoofing** on the left side of the page. Here you can opt to **Adhere to Corporate defaults** by checking the box at the top of the page. If you wish to customize settings for the group, set the options as described below.

To configure the anti-spoofing settings:

1 If you want to **Ignore allow lists** for SPF hard failures, check the box provided.

2 Choose an action message marked as **SPF hard fail**. The options are:

No Action	No action is taken against messages marked as SPF hard fail.
Permanently delete	Messages marked as SPF hard fail are permanently deleted.
Reject with SMTP error code 550	Messages marked as SPF hard fail are rejected with an SMTP error code 550.
Store in Junk Box (recommended for most configurations)	Messages marked as SPF hard fail are stored in the Junk Box. This is the recommended setting for most configurations.
Send to [field]	Messages marked as SPF hard fail are sent to the user specified in the available field. For example, you can send to `postmaster`.
Tag with [field] added to the subject	Messages marked as SPF hard fail are tagged with a term in the subject line. For example, you may tag the messages `[SPF Hard Failed]`.
Add X-Header: X-[field]:[field]	Messages marked as SPF hard failed add 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 `spfhard` results in the email header as: `X-EMSJudgedThisEmail:spfhard`.

3 For SPF soft failures, decide if you want to **Ignore allow lists**. A check ignores the allowed lists and unchecked uses the lists.

4 For DKIM settings, decide if you want to **Ignore allow lists**. A check ignores the allowed lists and unchecked uses the lists.

5 Choose the action to take for messages marked as **DKIM signature failed**. The options are the same as those listed for Step 2. In the text field, you can use text to indicate DKIM failures, rather than SPF failures.

6 Select **Apply Changes** when done.

Forcing All Members to Group Settings

Select the check box 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.

Domains

The **SYSTEM SETUP | Users, Groups & Domains > Domains** page lists the available organizational units associated with the SonicWall solution.

NOTE: The Global Admin sees Users, Groups & Organizations. The Organizations Unit (OU) Admin sees Users, Groups & Domains.

Topics:

Domains Overview

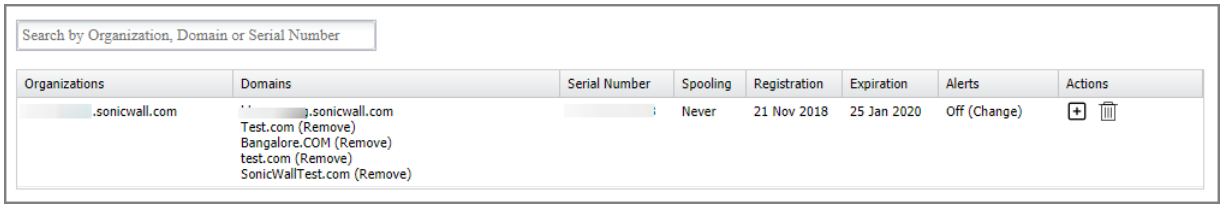
Domains are set by the Global Administrator as an efficient way of managing an entire enterprise-sized SonicWall system setup. These subset groups, also known as an OU, are managed by a sub-administrator, called the OU Administrator. The OU Administrator role has full administrative rights to the OU he has been assigned to by the Global Administrator.

The OU Admin can log in as any other user within the group of domains assigned to edit a user's individual settings, edit group settings for groups within their OU, and manage Junk Boxes, and view Reports. The OU Admin is not able to add or remove domains from an Organization, regardless if he is the OU Admin of that Organization; only the Global Administrator has the ability to perform these tasks.

Adding a Domain

To add a domain:

1. Navigate to the **SYSTEM SETUP | Users, Groups & Domains > Domains** page.
2. Click the plus icon **+** on the far right under the **Actions** column.
3. Enter the **Domain Name** in the small popup dialog box. Acceptable domains follow the form of `domain.com` or `sub.domain.com`. The **Organization Admin Login ID** is automatically populated based on what is entered as the Domain Name.
4. Click **OK**.
5. The domain name appears under the **Domains** column.



Consider the following when creating a new domain:

- User settings are migrated to the newly created domain.
- LDAP configured at the Global Administrator level is not automatically migrated when creating a new organization. The OU Admin needs to reconfigure the LDAP for his organization. Neglecting to configure the LDAP can potentially break user authentication for domains of that organization.
- Group Settings configured at the Global Administrator level are not automatically migrated when creating a new organization. The OU Admin needs to reconfigure the Group Settings for his organization.
- User Rights configured at the Global Administrator level is not automatically migrated when creating a new organization. The OU Admin needs to reconfigure the User Rights for the users in his organization.

- Group Roles configured at the Global Administrator level are not automatically migrated when creating a new organization. The OU Admin needs to reconfigure the Group role for the groups in his organization.

NOTE: Any domains added in the Create Organization screen that are not already listed in the **Network Architecture > Server Configuration** page are not automatically added to the server. The Global Administrator needs to add these domains to the Network Architecture path separately.

Signing In as an OU Admin

As a Global Administrator, you can sign in to any **Organization** as an OU Admin. Click the **Sign in as OU Admin** icon. You are automatically directed as the OU Admin to the respective OU in a new window. Click the **Log Out** icon to log out as the OU Admin.

Configuring OU Settings

As a Global Administrator, you can subscribe to alerts for a specific Organization so that you are notified about updates and changes made to this Organization. Click the **Settings** icon of the Organization you want alerts for. Then, click the **Change** link in the **Alerts** column, and confirm your choice.

Removing a Domain

To delete a Domain, click the **Remove** button of the Domain you wish to delete.

Users and Groups in Multiple LDAP

The administrators of each organization can create a master LDAP group that encompasses all their users and groups. That master group can then be used to administer SonicWall settings across the organization, even if there are multiple domains. With a group that contains all the members of the LDAP, the administrator effectively administers the LDAP.

See the following sections for more information:

- Users
- Groups

Users

When an administrator logs in and views the **SYSTEM SETUP | Users, Groups & Domains > Users** page, one sees all the email addresses that exist on that instance of SonicWall. The administrator can then narrow the view to only the entries from that LDAP.

NOTE: The **Using Source** selection allows administrators to access users who were added directly to SonicWall, and did not come in through an LDAP entry. These entries are not deleted with an LDAP deletion.

Topics:

Filtering through User View Setup

To filter the user view setup by source:

1. Log in as the SonicWall administrator.
2. Click **Users, Groups & Domains**, and then **Users**.
3. Scroll down to **User View Setup**.
4. From the **Using Source** drop-down menu, choose the LDAP source associated with the users you want to view. Click **Go**.

You only see the users associated with that LDAP source. The list of users can be sorted by user name, primary email address, user rights, or source. If you have already filtered by source, sorting by source does not retrieve anything outside the filter.

To sort a list of users, click on the column heading that describes the sort type. Click again to sort in reverse order.

Each LDAP user record has a check box next to it. To edit a user or users, select the box. If you select one user, you can log in as that user or edit that user's rights, for example, to elevate them to group admin or help desk-level rights. If you select more than one user, you can only change their message management style to the default style.

Finding a Specific User

Because an LDAP source usually has many records, SonicWall has provided several ways of looking for a specific user.

To find a specific user:

1. Log in as the SonicWall administrator.
2. Click **Users, Groups & Domains**, and then click **Users**.
3. Scroll down to **User View Setup**.
4. From the F**ind all users in column** drop-down menu, choose either the username or the primary email address to search on.
5. Choose which type of search you want. Exact matches are the fastest, but matches contain your search term may help you more if you cannot remember the exact username or address you are looking for.
6. Enter your search term.
7. Click **Go**. You see the users who match your search criteria.

Adding a New User

If you want to add a user who does not appear in the automatically generated list from your LDAP, you can choose to manually add an account. If an LDAP is not provided, the user is added to the default LDAP source. You cannot add users to your LDAP from the Hosted Email Security interface.

To add a user:

1. Log in as the SonicWall administrator.
2. Click **Users, Groups & Domains**, and then click **Users**.
3. Scroll down to **User View Setup**.
4. Click **Add**.
5. Enter the user's fully-qualified email address, choose a source (if any), and any aliases you wish to associate with the user.

Deleting a User

To delete a user:

1. Log in as the SonicWall administrator.
2. Click **Users, Groups & Domains**, and then **Users**.
3. Scroll down to **User View Setup**.
4. Select the user you wish to delete. Deleting a user does not remove the user's LDAP entry, only the entry in the Hosted Email Security system.
5. Click **Remove**.

Groups

Use the **Users, Groups & Domains > Groups** page to incorporate or extend existing LDAP groups. You can also change a group's security role in the Hosted Email Security system and view the membership of a group.

This section contains the following subsections:

- Filtering Through Group View
- Changing a Group's Role
- Viewing Members of a Group
- Setting Junk Blocking by Group

Filtering Through Group View

To filter the group view by source:

1. Log in as the Hosted Email Security administrator.
2. Click **Users, Groups & Domains**, and then **Groups**.
3. Scroll down to **Assign Roles to Groups Found in LDAP**.
4. From the **Using Source** drop-down menu, choose the LDAP source associated with the groups you want to view. Click **Go**.

5 If you do not see the group you want, click the **Add Group** button. You can choose an existing group from one of your sources. You cannot create a group that does not exist.

Changing a Group's Role

You can change each group's role in Hosted Email Security. These roles determine a user's permissions to change Hosted Email Security settings, including user settings.

To change a group's role:

1 Log in as the Hosted Email Security administrator.

2 Click **Users, Groups & Domains**, and then **Groups**.

3 Scroll down to **Assign Roles to Groups Found in LDAP**.

4 Select the box next to the group you want to change.

5 Click **Edit Role**.

6 In the pop-up window, choose the role you want that group to have. You can choose only one role per group. If a user is in multiple groups, permissions are granted in the order in which the groups are listed in the user's profile.

7 Click **Apply Changes**. You see a status update at the top of the page.

Viewing Members of a Group

To view the members of a particular group:

1 Log in as the Hosted Email Security administrator.

2 Click **Users, Groups & Domains,** and then **Groups**.

3 Scroll down to **Assign Roles to Groups Found in LDAP**.

4 Select the box next to the group to see its membership.

5 Click **List Members**. A pop-up window displays that lists the group's membership by primary email address.

Setting Junk Blocking by Group

You can use the existing LDAP groups to configure the filtering sensitivity for different user groups. For example, your sales group might need to receive email written in foreign languages.

To set junk blocking by group:

1 Log in as the Hosted Email Security administrator.

2 Click **Users, Groups & Domains**, and then **Groups**.

3 Scroll down to **Set Junk Blocking Options for Groups Found in LDAP**.

4 Under **Using LDAP**, select your LDAP.

5 Select a group to edit.

6 Click **Edit Junk Blocking Options**. The Group Junk Blocking Options window displays. Follow the recommendations described in Anti-Spam.

12

System Setup | Network and Junkbox Commands

This section provides configuration procedures for the network and Junk Box settings.

Topics:

Network

On the **MANAGE | SYSTEM SETUP | Network** page, you can configure your Server Configuration.

Server Configuration

You can configure your domain for the inbound path through which all incoming mail for your domain is filtered. The Hosted Email Security solution filters out spam and viruses, then passes the mail to the server. Use the Configure Inbound Mail Flow below to configure.

You can also configure your domain for the outbound path through which all mail is sent from your domain via Hosted Email Security to the recipient. As the outbound gateway, Hosted Email Security processes the mail by filtering out spam and viruses before final delivery. By configuring the outbound mail flow you instruct the server to pass all outgoing mail from your domain to the Hosted Email Security Service (the gateway server).

Inbound Mail Flow Configuration

1 Navigate to **MANAGE | SYSTEM SETUP > Network > Server Configuration > Inbound** tab.

2 The domain names are listed in the text box under **Settings**.

> **IMPORTANT:** Any source IP address is allowed to connect to this path, but relaying is allowed only for emails sent to the domains listed in the box.

3 For the mail server host name or IP address, specify a fully qualified domain name in the text box. An example would be engr.example.com:25.

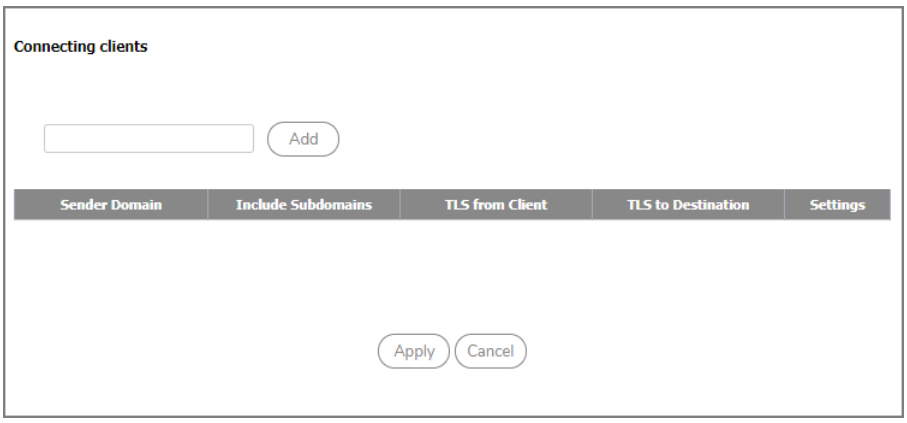
> **IMPORTANT:** If multiple destination servers are provided then emails are routed using load balancing.

- Leave the Routing option to **Round-robin**.

- If **Round robin** is specified, email traffic is balanced by sending a portion of the flow through each of the servers specified in the text box in round-robin order. All of the servers process email all the time.
- If **Failover** is specified, the first server listed handles all email processing under normal operation. If the first server cannot be reached, email is routed through the second server. If the second server cannot be reached, email is routed through the third server, and so on.

4 Click the **Test Downstream** button to verify that you are connected to the downstream server.

5 Click the check box next to **Configure STARTTLS** to require the destination server to support STARTTLS and configure encrypted email communication. SonicWall Hosted Email Security uses Transport Layer Security (TLS) to provide the secure internet connection.



6 Enter the sender domain name in the text box under **Connecting clients**.

7 Click **Add** and then click **Apply**.

8 Set your **Directory Harvest Attack (DHA) Protection Settings**.

9 Configure any of the following settings:

- **Action for messages sent to email addresses that are not in your LDAP server**—Select one of the following from the drop-down menu:
  - **Process all messages the same—**Messages from addresses not in your LDAP are processed the same as messages from addresses in your LDAP server.
  - **Permanently delete—**Messages from addresses not in your LDAP are permanently deleted.
  - **Reject invalid addresses—**Messages from addresses not in your LDAP are rejected.
  - **Always store in Junk Box—**Messages from addresses not in your LDAP are stored in your Junk Box.
- **Apply DHA protection to these recipient domains**—Select one of the following options for applying DHA protection:
  - **Apply to all recipient domains**—Select to apply DHA protection to all recipient domains.
  - **Apply only to the recipient domains listed below**—In the text box, specify the recipient domains to which DHA protection applies.
  - **Apply to all recipient domains except those listed below**—In the text box specify the recipient domains to which DHA protection does NOT apply.

10 Choose when you want your Hosted Email Security server to spool your email. Three options are provided:

- **Never spool email**

- **Automatic fallback**
- **Always spool email**

11 Click **Apply Changes**.

Outbound Mail Flow Configuration

1 Navigate to **MANAGE | SYSTEM SETUP > Network > Server Configuration > Outbound** tab.

2 The domain names are listed in the text box under **Settings**.

> **IMPORTANT:** Relaying is allowed only for emails sent from the domains listed in the box.

3 Click the **Test Upstream** button to verify that you are connected to the upstream server.

4 For the mail server host name or IP address, specify a fully qualified domain name in the text box. An example would be engr.example.com:25.

5 Only IP addresses can connect and relay through the Outbound path. Separate the source IP addresses with a carriage return.

6 Click on the radio button next to **Only Office 365 can connect and relay through the outbound path** if you want that specific setting.

7 Click the check box next to **Configure STARTTLS** to **require clients to connect using STARTTLS**.

8 Click on **Configure Authentication** to configure SMTP AUTH on this outbound path.

9 Scroll to the bottom of the page and select **Apply Changes**.

Junk Box

You can use the **SYSTEM SETUP | Junk Box** options to define the parameters for junk message management and for Junk Box Summary notification.

Message Management

On the **SYSTEM SETUP| Junk Box > Message Management** page, you define General Settings, Action Settings, and Miscellaneous Settings for managing junk messages.

General Settings

In the **General Settings** section, you choose options for saving messages in the junk box and for unjunking messages.

To define General Settings:

1 Select one of the following options for **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

2 Scroll to the bottom of the page and select **Apply Changes** if done or select **Reset to Defaults** if you want to return to prior settings.

Action Settings

In the **Action Settings** section, you define how unjunked messages are tagged and delivered to users' inboxes. Review each of the four options, check the box to enable that option and type in the text you want added to the subject line. The table below provides more information on the options.

Unjunked Tagging Option	Notes
Tag unjunked messages with this text added to the subject line	Example of words to be 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	Example of words to be 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:	Example of words to be added to the subject line: `[Junk released by Policy Action].`
Tag all messaged processed by Hosted Email Security for initial deployment testing with this text added to the subject line:	Example of words to be added to the subject line: `[SonicWall` Hosted Email Security`].`

Miscellaneous Settings

The **Miscellaneous** section provides links that take you to message management features for the Anti-Spam, Anti-Phishing, Anti-Virus, and Policies modules.

Miscellaneous Message Management Options	Where link goes
To set spam message management	**SECURITY SERVICES > Security Services > Spam Management**
To set phishing message management	**SECURITY SERVICES > Security Services > Anti-Phishing**
To set virus message management	**SECURITY SERVICES > Security Services > Anti-Virus**
To set policies for your organization	**Policy & Compliance > Filters**

Summary Notifications

On the **SYSTEM SETUP| Junk Box > Summary Notifications** page, you define Frequency Settings, Message Settings, Miscellaneous Settings, and Other Settings for the Junk Box Summary that is sent to users and administrators. The Junk Box summaries list the incoming email that Hosted Email Security has quarantined. From these summaries, users can choose to view or unjunk an email if the administrator has configured these permissions. From the **Summary Notifications** page, users can determine the language, frequency, content, and format of Junk Box summaries.

Frequency Settings

To define the frequency settings of the Junk Box Summary:

1. Select the **Frequency of summaries** from the drop-down list. Options range from **Never** to **14 Days**.
2. Select the **Time of day to send summary**. You can select **Any time of day** or specify an hour to send by selecting **Within an hour of** and choosing the hour from the drop-down menu.
3. Select the **Day of week to send summary**. You can select **Any day of the week** or select **Send summary on** and specify a day.
4. Specify the **Time Zone** for the Hosted Email Security system.
5. Scroll to the bottom of the page and select **Apply Changes** if done.

Message Settings

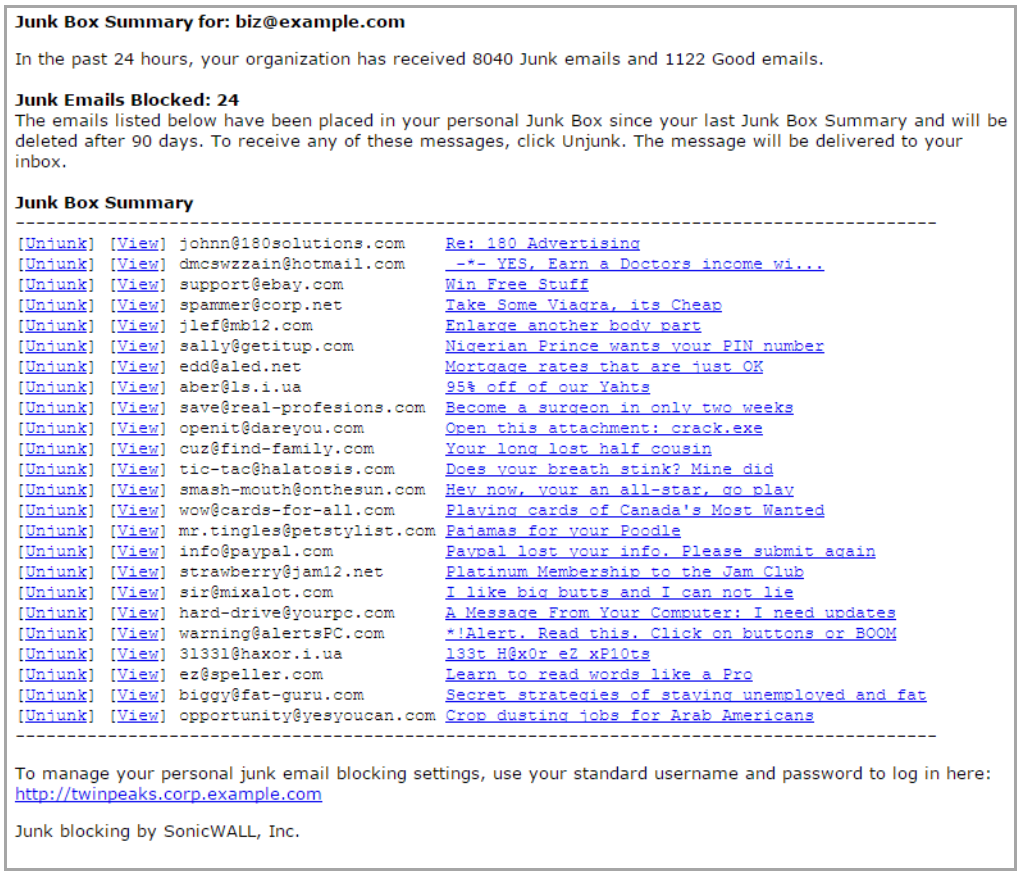
To define the Message Settings for the Junk Box Summary:

1. In the **Summaries include** section, choose **All Junk Messages** or **Only likely junk (hide definite junk)** in Junk Box Summaries.

   NOTE: If **All Junk Messages** is selected, both definite and likely junk messages are included. If **Only likely junk** is selected, only likely junk messages are included in the summary.

2. Select the **Language of summary email** from the drop-down list.
3. Check the box to enable **Plain summary** if you want to send junk box summaries without graphics.

The following image shows a Plain Summary:



Junk Box Summary for: biz@example.com

In the past 24 hours, your organization has received 8040 Junk emails and 1122 Good emails.

Junk Emails Blocked: 24
The emails listed below have been placed in your personal Junk Box since your last Junk Box Summary and will be deleted after 90 days. To receive any of these messages, click Unjunk. The message will be delivered to your inbox.

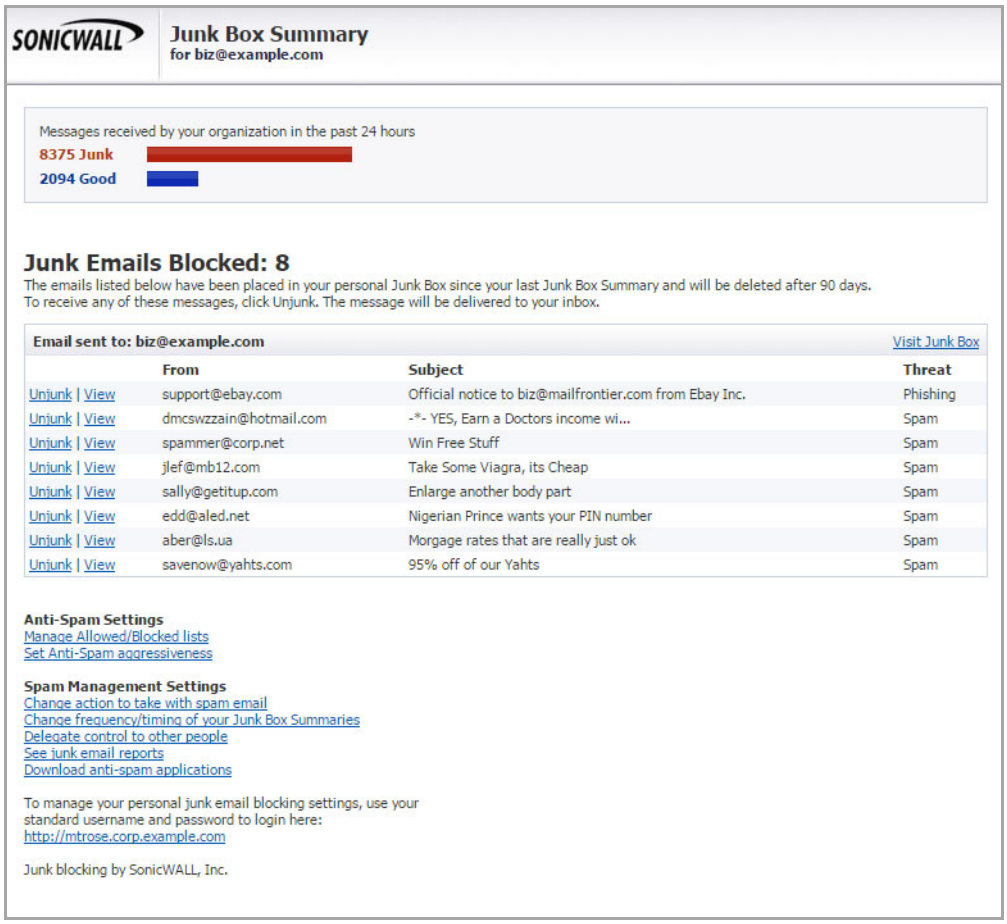
Junk Box Summary

[Unjunk]	[View]	johnn@180solutions.com	Re: 180 Advertising
[Unjunk]	[View]	dmcswzzain@hotmail.com	-*- YES, Earn a Doctors income wi...
[Unjunk]	[View]	support@ebay.com	Win Free Stuff
[Unjunk]	[View]	spammer@corp.net	Take Some Viagra, its Cheap
[Unjunk]	[View]	jlef@mb12.com	Enlarge another body part
[Unjunk]	[View]	sally@getitup.com	Nigerian Prince wants your PIN number
[Unjunk]	[View]	edd@aled.net	Mortgage rates that are just OK
[Unjunk]	[View]	aber@ls.i.ua	95% off of our Yahts
[Unjunk]	[View]	save@real-profesions.com	Become a surgeon in only two weeks
[Unjunk]	[View]	openit@dareyou.com	Open this attachment: crack.exe
[Unjunk]	[View]	cuz@find-family.com	Your long lost half cousin
[Unjunk]	[View]	tic-tac@halatosis.com	Does your breath stink? Mine did
[Unjunk]	[View]	smash-mouth@onthesun.com	Hey now, your an all-star, go play
[Unjunk]	[View]	wow@cards-for-all.com	Playing cards of Canada's Most Wanted
[Unjunk]	[View]	mr.tingles@petstylist.com	Pajamas for your Poodle
[Unjunk]	[View]	info@paypal.com	Paypal lost your info. Please submit again
[Unjunk]	[View]	strawberry@jam12.net	Platinum Membership to the Jam Club
[Unjunk]	[View]	sir@mixalot.com	I like big butts and I can not lie
[Unjunk]	[View]	hard-drive@yourpc.com	A Message From Your Computer: I need updates
[Unjunk]	[View]	warning@alertsPC.com	*!Alert. Read this. Click on buttons or BOOM
[Unjunk]	[View]	31331@haxor.i.ua	133t H@x0r eZ xP10ts
[Unjunk]	[View]	ez@speller.com	Learn to read words like a Pro
[Unjunk]	[View]	biggy@fat-guru.com	Secret strategies of staying unemployed and fat
[Unjunk]	[View]	opportunity@yesyoucan.com	Crop dusting jobs for Arab Americans

To manage your personal junk email blocking settings, use your standard username and password to log in here:
http://twinpeaks.corp.example.com

Junk blocking by SonicWALL, Inc.

The following image shows a Graphic Summary:



4 Check the box to **Display junk statistics in summary email.** This includes junk statistics in the Junk Box Summary.

5 Scroll to the bottom of the page and select **Apply Changes** if done.

Miscellaneous Settings

To define the Miscellaneous Settings for the Junk Box Summary:

1 Check the box to enable **Send Junk Box Summary to delegates**. This send summary emails sent directly to a user's delegates. Users with delegates no longer receive summary emails.

2 Select one of the options for **Enable "single click" viewing of messages**. You can select from the following:

- Off—The "single click" viewing of messages setting is not enabled.
- View messages only—Users can preview messages without having to type their name or password.
- Full Access—Users can click any link in a Junk Box Summary and are granted full access to the particular user's settings.

3 Check the box to **Enable Authentication to Unjunk** if you want to require authentication for unjunking messages in the Junk Box Summary.

4 Check the box **Only send Junk Box Summary emails to users in LDAP** to only include LDAP users as recipients of the Junk Box Summary emails. With this setting selected, users not associated with the LDAP do not receive Junk Box Summary emails.

5 To enable authentication for non-LDAP users, click the link. You are automatically directed to the **SYSTEM SETUP | Users, Groups & Organizations > Users** page. For more information regarding LDAP and non-LDAP users, refer to Users.

6 Scroll to the bottom of the page and select **Apply Changes** if done.

Other Settings

To define the Other Settings for the Junk Box Summary:

1 Choose **Email address from which summary is sent**. Select one of the following:

- **Send summary from recipient's own email address**
- **Send summary from this email address** and specify the email address in the space provided.

2 Specify the **Name from which summary is sent** in the field provided.

3 Specify the **Email subject** in the space provided.

4 Select **Apply Changes** if done. Select **Revert** if you want to fall back to the previously save definitions.

13

Anti-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. This chapter reviews the configuration information for Anti-Spam:

- Spam Management
- Address Books
- Anti-Spam Aggressiveness
- Languages

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

Spam Management

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 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 have 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, Hosted Email Security analyzes the messages' headers and contents and uses collaborative thumb-printing to block email that contains junk.

Use **SECURITY SERVICES | Anti-Spam > Anti-Spam Aggressiveness** to select options to control spam-blocking aggressiveness.

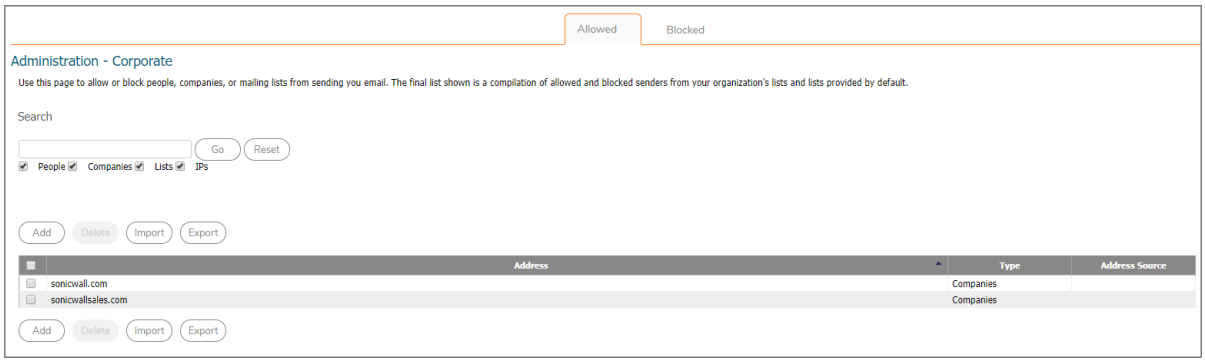
Address Books

From **SECURITY SERVICES | Anti-Spam > Address Books** you can create an address book of people, companies, and a mailing list or a list of IP addresses who those who are allowed to or are blocked from sending email to you.

Select the **Allowed** or **Blocked** tabs to view the respective type of address.

If you attempt to add your own email address or your organization's domain, SonicWall Hosted Email Security displays 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.



People

Use the **Allowed** tab to add or identify people, companies or mailing lists or IP addresses that are allowed to send you email. Use the **Blocked** tab to add or identify people, companies or IP addresses that are blocked from sending you email. Both lists can be sorted in ascending or descending order by clicking in the **Address** column heading.

NOTE: An email address cannot be on both the Allowed and Blocked lists. If you move an allowed address to the Blocked list, it is removed from the Allowed list.

The features described below apply to both Allowed and Blocked address lists.

Searching the Address Lists

To search for an item in the Allowed or Blocked address list:

1. Selected **Allowed** or **Blocked** to see the right list.
2. Enter a keyword or character string in the search field**.**
3. Below the search field, select the type of information you want to search. Any or all of the types can be selected.
4. Click **Go.**
5. Click **Reset** to restore all the data to the table and reset the search parameters.

Adding Entries to the Address Lists

To add an item to the Allowed or Blocked address list:

1. From the **SECURITY SERVICES | Anti-Spam > Address Books** page, click the **Allowed** or **Blocked** tab. Select **Allowed** or **Blocked** to see the right list.
2. Click the **Add** button.
3. Select the list type (People, Companies, Lists, IPs) from the drop-down menu.

4 Enter one or more addresses, separated by carriage returns. Based on the type selected, enter the data required:

5 Select **Add** to complete.

When adding addresses, consider 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.
- Hosted Email Security warns 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.
- 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.
- 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 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 mis-classified messages.
- **People**--Enter the email address in the field provided. Separate each email with a carriage return.
- **Companies**--Enter the domains in the field provided. Separate each email with a carriage return.
- **Lists**--Enter the mailing lists in the field provided. Separate each list with a carriage return. (This option is offered for the Allowed list only.)
- **IPs**--Enter the IP addresses in the field provided. Separate each IP address with a carriage return.

Removing Entries from the Address Lists

To remove an entry from the Allowed or Blocked list:

1 Select **Allowed** or **Blocked** to see the right list.

2 Check the box by the item you want to remove

3 Click **Delete**.

NOTE: Your organization's entries always override user and SonicWall entries. In the user view, your organization's entries are indicated with a dimmed check box, and users cannot delete these items from the lists.

Importing and Exporting the Address Book

You can import an address book of multiple addresses to create our Allowed or Blocked lists. 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

For example:

```
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>
```

To import an Address Book:

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

To export an Address Book:

1. Select the **Export** button.
2. Save the .txt Notepad file to your local system.

Anti-Spam Aggressiveness

The **SECURITY SERVICES | Anti-Spam > Anti-Spam Aggressiveness** page allows you to tailor the SonicWall Hosted Email Security product to your organization's preferences. Configuring this window is optional.

SonicWall Hosted Email Security recommends using the default setting of Medium unless you require different settings for specific types of spam blocking. Be sure to select **Apply Changes** to save the settings or select **Reset to Defaults** to go back to the prior settings.

Topics:

Configuring Grid Network Aggressiveness

The GRID Network Aggressiveness determines the degree to which you want to use the collaborative database produced by the SonicWall Grid Network. 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. By selecting a stronger setting a message is more likely to be marked mark as spam when other people have already marked that message as spam.

Use the following settings to specify how stringently Hosted Email Security evaluates messages:

- If you choose **Mildest**, you 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 through 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

The Adversarial Bayesian technique refers to 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 the following settings to specify how stringently SonicWall Hosted Email Security evaluates messages:

- If you choose **Mildest**, you 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 through 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.

Unjunking spam

Select the **Allow users to unjunk spam** check box if you want to enable users to unjunk spam messages. If left unchecked, users cannot unjunk spam messages.

Category settings

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

For each type of spam:

- 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 Hosted 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, if you don’t want to receive any email with sexual content, select **Strong**. If you are less concerned about receiving other categories, select Mild.

You can also select the **Allow Unjunk** check box to allow users to unjunk specific types of spam.

Languages

Allow or block all messages in a particular language. For example, you can block all messages in Russian, allow all messages in Turkish, and choose No Opinion for all other languages.

Choosing the default option of No Opinion for a language causes messages in that language to be screened by all the junk modules installed on your configuration.

From the **SECURITY SERVICES | Anti-Spam > Languages** page, you can **Allow All**, **Block All**, or enter **No Opinion** on email messages in various languages. If you select **No opinion**, Hosted Email Security judges the content of the email message based on the modules that are installed. After configuring Language settings, click the **Apply Changes** button.

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.

Spam Submissions

The **SECURITY SERVICES| Security Services > Spam Management** page allows you to manage email that is miscategorized and to create probe accounts to collect spam and catch malicious hackers. Managing miscategorized email and creating probe accounts increases the efficiency of Hosted Email Security’s spam management. This page enables administrators and users to forward the following miscategorized email messages to their IT groups, create probe accounts, and accept automated allowed lists to prevent spam.

Managing Spam Submissions

To manage spam submissions:

1. Navigate to **SECURITY SERVICES | Security Services > Spam Management** on the **MANAGE** view.
2. Under **Action Settings**, click on the action for messages marked as **Definite Spam**:
   - No action
   - Permanently delete
   - Reject with SMTP error code 550
   - Store in Junk Box (recommended for most configurations)
   - Send to
   - Tag with [SPAM] added to the subject
   - Add X-Header: X- : spam
3. Under **Action Settings**, click on the action for messages marked as **Likely Spam**:
   - No action
   - Permanently delete

- Reject with SMTP error code 550
- Store in Junk Box (recommended for most configurations)
- Send to
- Tag with [LIKELY SPAM] added to the subject
- Add X-Header: X- : likely spam

4 Click **Apply Changes** when done.

5 Under Miscellaneous choose from the following choices:

- Accept automated Allowed Lists:
- Skip spam analysis for internal email:
- Allow users to delete junk email:

6 Click **Apply Changes** when done.

7 Under **Miscellaneous** settings, check the box for:

- Accept automated Allowed Lists
- Skim spam analysis for internal email
- Allow users to delete junk email

8 Click **Apply Changes** when done.

14

Anti-Spoofing

The SonicWall Hosted Email Security solution allows you to enable and configure settings to prevent illegitimate messages from entering your organization. Spoofing consists of an attacker forging the source IP address of a message, making it seem like the message came from a trusted host. By configuring SPF, DKIM, and DMARC settings, your Hosted Email Security solution runs the proper validation and enforcement methods on all incoming messages to your organization. This chapter provides configuration information specific to Anti-Spoofing, including:

- Inbound SPF Settings
- Inbound DKIM Settings
- Inbound DMARC Settings
- Inbound DMARC Report Settings
- Outbound DKIM Settings

The Anti-Spoofing feature works in an order of precedence, where features rules set at the top of the page are of a lower priority than features rules set towards the bottom of the page: Generally, a message is subjected to SPF, DKIM, and DMARC if all are enabled. The results from DKIM validation take precedence over the results from SPF validation, and DMARC validation results take precedence over DKIM validation results. DKIM actions take precedence over SPF, and DMARC actions take precedence over DKIM. This precedence order determines what settings action is applied to the message if the message is determined to be a likely spoof. Messages are subjected to SPF, DKIM, and DMARC validation in that order, if all are enabled.

Inbound SPF Settings

The **SECURITY SERVICES | Security Services > Anti-Spoofing > Inbound** tab features **SPF (Sender Policy Framework)** validation for inbound email messages. SPF is an email validation system designed to prevent email spam by verifying that sender IP addresses are valid. SPF records, which are published in the DNS records, contain descriptions of the attributes of valid IP addresses. SPF is then able to validate against these records if a mail message is sent from an authorized source. If a message does not originate from an authorized source, the message fails. You can configure the actions against messages that hard fail.

SPF hard fail—The SPF has determined that the host is not allowed to send messages and does not allow those messages through to the recipient.If an email message from a domain originates from an IP address outside of the IP range defined in the SPF record for the domain, the message is rejected.

To enable SPF:

1 To **Enable SPF validation for incoming messages**, check the box. Then define the settings for hard fail and soft fail. Be sure to **Apply Changes** when done.

2 Configure the action to take:

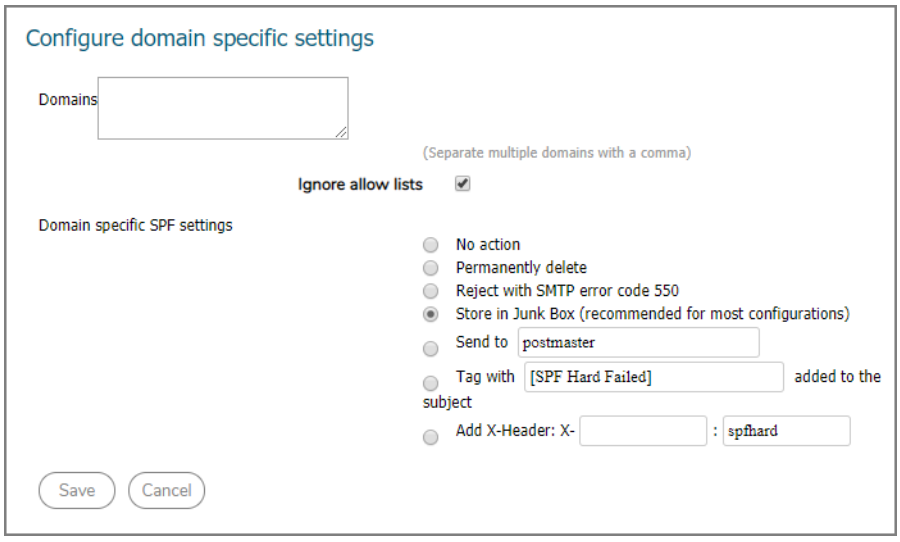
a Decide if you want to **Ignore allow lists**. A check ignores the allowed lists and unchecked uses the lists.

b Select an action to take for messages marked as **SPF hard fail**. Actions to Take for Hard Failures describes the options.

Actions to Take for Hard Failures

No Action	No action is taken against messages marked as SPF hard fail.
Permanently delete	Messages marked as SPF hard fail are permanently deleted.
Reject with SMTP error code 550	Messages marked as SPF hard fail are rejected with an SMTP error code 550.
Store in Junk Box (recommended for most configurations)	Messages marked as SPF hard fail are stored in the Junk Box. This is the recommended setting for most configurations.
Send to [field]	Messages marked as SPF hard fail are sent to the user specified in the available field. For example, you can send to `postmaster`.
Tag with [field] added to the subject	Messages marked as SPF hard fail are tagged with a term in the subject line. For example, you may tag the messages `[SPF Hard Failed]`.
Add X-Header: X-[field]:[field]	Messages marked as SPF hard failed add 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 `spfhard` results in the email header as: `X-EMSJudgedThisEmail:spfhard`.

c Click **Add Domain** if you want to define specifications for an identified domain.



d List the domains in the **Domains** field. Separate domains with a comma.

e Select one of the actions for a hard failure. Refer to the Step above for their definitions.

3 Click on **Apply Changes**.

Inbound DKIM Settings

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. 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.

To configure DKIM signature settings:

1 Navigate to **SECURITY SERVICES | Security Services > Anti-Spoofing > Inbound** on the **MANAGE** view, and scroll down to the section labeled **DKIM Settings**.

2 Click **Add Domain** if you want to define specific actions for an identified domain.

   a List the domains in the **Domains** field. Separate domains with a comma.

   b Select one of the actions for a hard failure. Refer to Actions to Take for Hard Failures above for their definitions.

   c Decide if **Domain** is **required to have DKIM signature**. A check requires the signature and unchecked doesn't require it.

3 Click on **Apply Changes** to save the DKIM definitions.

Inbound DMARC Settings

Domain-based Message Authentication, Reporting & Conformance (DMARC) is a policy that works in tandem with SPF and DKIM to fully authenticate incoming and outgoing email messages. A DMARC policy allows a sender to indicate that his emails are protected by SPF and/or DKIM, and also tells a receiver what to do if neither of those authentication methods passes, such as junk or reject the message. By default, the DMARC feature is enabled. You can specify the exact domain names to exclude from DMARC Policy Enforcement. The DMARC feature also allows you to specify domains for Incoming and Outgoing message reports.

To configure DMARC settings:

1 Navigate to **SECURITY SERVICES | Security Services > Anti-Spoofing > Inbound** on the **MANAGE** view, and scroll down to the section labeled **DMARC Settings**.

2 Select the **Enable DMARC judgment for incoming messages** check box.

ⓘ **NOTE:** To use DMARC, you must also enable DKIM and SPF.

3 Select the **Enable DMARC Policy Enforcement for incoming messages** check box.

4 In the field provided, **Exclude these sender domains**, enter any sender domains (for example, sonicwall.com or gmail.com) you want excluded from DMARC policy enforcement. Multiple domains can be entered and should be separated by a comma.

5 Choose whether to **Enable DMARC outgoing reports** settings:

6 Select the Enable DMARC outgoing reports check box.

You can configure an **Outbound Path for RUA delivery** of the reports by clicking the provided link (**SYSTEM SETUP > Network > Server Configuration**).

7 If you want to override reporting attributes for a specific domain, select **Add Domain**:

   a Enter the domain name to send DMARC reports to. You have the option of using '*' as a value for the domain field. Consider the following:

      - A configuration created with the domain name * is considered the default domain.
      - If the domain is not provided, DMARC uses configuration settings from the * domain.
      - If no * domain is added, then a hard-coded default value, such as postmaster@domain, is used as the Sender ID.

   b Enter the email address from which the report originates in the field called **Report From: address**.

   c Optionally add any **Notes** regarding this domain.

   NOTE: The RUA is the aggregated report for domains with published domain records. Reports are sent daily.

   d Select **Save**.

8 Click on **Apply Changes** to save the DMARC definitions.

Inbound DMARC Report Settings

You can configure DMARC incoming report settings by clicking the **Add Domain** button in the **DMARC Reports Settings** section. DMARC Incoming Reports are collected and processed only for the domains added.

To set up the DMARC reports:

1 Navigate to **SECURITY SERVICES| Security Services > Anti-Spoofing > Inbound** on the **MANAGE** view, and scroll down to the section labeled **DMARC Report Settings**.

2 Select **Add Domain**.

3 Enter the **Domain** name for DMARC incoming reports.

4 Check the box to override reports being sent to the RUA email address specified in the DNS record. An example from the DNS record is `rua=mailto:aggrep@yourcompany.com`.

5 If you selected the **Override DNS RUA Email Address**, specify the **RUA Email Address** to which the reports should be sent. Multiple addresses can be entered and should be separated by a comma.

   NOTE: The RUA is the aggregated report for domains with published domain records. Reports are sent daily.

6 Click **Save** to save the report definition.

7 Select **Apply Changes** to update the report settings.

NOTE: You can select the **Refresh** button to refresh the data in report domains table.

Outbound DKIM Settings

Set up the DKIM Signature Configurations options for the outbound mail.

To set up DKIM settings on the outbound path:

1 Navigate to **SECURITY SERVICES | Security Services > Anti-Spoofing > Outbound** on the **MANAGE** view.

2 Click the **Add Configuration** button. The DKIM Outbound Configuration page displays.

3 Select the Enable signature on outbound email check box.

NOTE: DKIM TXT record should be added to the domain's DNS before enabling DIM configuration.

4 To define the **Settings for DKIM Signature**, complete the fields as described below:

Domain	Enter the **Domain** name.
Identity of Signer	Enter an **Identity of Signer**. Select the **Same as domain** check box to use the specified Domain name as the Identity of Signer.
Selector	Enter a value for the **Selector**. The selector is used to differentiate between multiple DKIM DNS records within the same organization (for example, `feb2014.domainkey.yourorganization.com`.
List of Header fields for Signing	Check the **Sign all standard headers** box to include all headers, or specify the headers in the designated field, except for Authentication-Results, Return-Path, any existing DKIM-Signature fields, and any X- field. Separate multiple headers with a colon (for example, `from:to:subject`).

5 To set up the Public Private key pair for SKIM Signing, complete the fields as described below:

Generate Key Pair	If you want to generate key pair for the DKIM signing, select **Generate key pair**. Specify the Key Size from the values in the drop-down list, then click the Generate Key Pair button.
Key Size	Specify the **Key Size** from the values in the drop-down list, then select the **Generate Key Pair** button.
Import existing public-private key pair	Choose Import existing public-private key pair, if you want to use an existing pair. Click on **Choose File** to **Upload Public key** and click on **Choose File** to **Upload Private key**. Type in the **Passphrase for private key.** Use only alphanumeric characters.

6 Click the **Save** button to finish. The signature is added to the DKIM Signature Configurations list.

Generating DNS Record

Once a domain has been successfully added to the DKIM Signature Configurations table, you can generate a DNS Record.

To generate a DNS record:

1 Under the DNS Record column for the domain you want to generate a record for, click the **Generate** button.

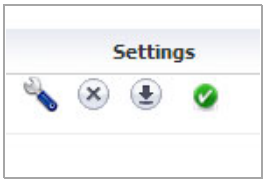
2 Set the following options on the Generate DNS Record page:

- **Domain**—This field auto-populates with the Domain you entered when adding a new configuration. This field cannot be edited.
- **Selector**—This field auto-populates with the Selector you entered when adding a new configuration. This field cannot be edited.
- **Public Key**—This field populates with the Public Key for your DNS record. You can copy and paste from this field.
- **Domain is testing DKIM**—Select the check box to enable testing DKIM for this domain.
- **Subdomains required to have their own DKIM keys**—Select the check box to enable the requirement for all subdomains to have their own DKIM keys.

3 Click the **Generate DNS Record** button to save the settings and generate your DNS record.

Managing Outbound DKIM Settings

The Settings column of each domain listed in the DKIM Signature Configurations table has the following icons:



- **Edit**—Click this icon to edit the DKIM Signature settings. Note that not all fields are editable.
- **Delete**—Click this icon to delete the DKIM Signature.
- **Download**—Click this icon to download the Public Key for this DKIM Signature.
- **Status**—The status icon notifies you if the DKIM Signature is enabled (green icon) or disabled (gray icon).

15

Anti-Phishing and Anti-Virus

The Anti-Phishing and Anti-Virus features protect your organization from email messages with fraudulent content. They also safeguard inbound email from viruses and prevent your employees from sending viruses with outbound email. Phishing attacks are a form of fraud. Phishing attacks use email with fraudulent content to steal your personal identity data and financial account credentials. Use these pages to take action on messages that could pose a phishing or virus attack.

Topics:

Anti-Phishing

Topics:

Phishing Overview

Two audiences are targeted for fraudulent phishing schemes:

- *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 Website 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.

Configuring Action Settings

To configure Hosted Email Security for phishing:

1 Navigate to **SECURITY SERVICES | Security Services > Anti-Phishing** on the **MANAGE** view of your Hosted Email Security solution.

2 Select which action to take for messages identified as **Definite Phishing**. For more information about available actions, see the following table:

Response	Effect
No Action	No action is taken for messages.
Permanently Delete	The email message is permanently deleted. **CAUTION: If you select this option, your organization risks losing wanted email. Deleted email cannot be retrieved.**
Reject with SMTP error code 550	The message is rejected and responds with a 550 error code, which indicates the user's mailbox was unavailable (for example, not found or rejected for policy reasons).
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 recommended for most configurations.
Send to	Forward the email message for review to the specified email address. For example, you could "Send to user%40example.com."
Tag with	The email is tagged with a term in the subject line, for example [Phishing fraud] or [LIKELYPHISHING]. 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: "X-EMSJudgedThisEmail:Fraud"

3 Select which action to take for messages identified as **Likely Phishing**. These are the same as for **Definite Phishing**.

Configuring Miscellaneous

1 Select the A**llow users to unjunk phishing messages** check box if you want to allow users to unjunk fraudulent messages.

2 To send copies of fraudulent email messages to a person or people designated to deal with them, enter the recipients' email addresses in the test box for **Send copies of emails containing phishing attacks to the following email addresses**. Separate multiple emails addresses with a comma.

3 Click **Apply Changes**.

Anti-Virus

Topics:

Inbound Anti-Virus Protection

Anti-Virus protection can be configured on the **Inbound** and **Outbound** paths. You are able to define separate actions for **Definite Viruses** and **Likely Viruses**.

To configure Anti-Virus protection on the inbound path:

1 Navigate to **SECURITY SERVICES | Security Services > Anti-Virus** on the **MANAGE** view and select the **Inbound** tab.

NOTE: If you have licensed more than one virus-detection engines. They work in tandem.

2 Choose one of the actions in **Action for messages identified as Definite Viruses**.

Action for Messages Identified as Definite Viruses

Response	Effect
No Action	No action is taken for messages.
Permanently Delete	The email message is permanently deleted. **CAUTION: If you select this option, your organization risks losing wanted email. Deleted email cannot be retrieved.**
Reject with SMTP error code 550	The message is rejected and responds with a 550 error code, which indicates the user's mailbox was unavailable (for example, not found or rejected for policy reasons). **NOTE:** When Capture analysis confirms a definite virus or likely virus, the message is quarantined—even if the reject action is selected—and any attachments are stripped. The quarantine preserves a record of the action and the message is recoverable if needed, rather than being lost.
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 recommended setting for most configurations.

Action for Messages Identified as Definite Viruses

Response	Effect
Send to	Send to email_address, where email_address is the email address of the person designated to deal with viruses. For example, you could Send to `postmaster@ww.com`.
Tag with	The email is tagged with a term in the subject line, for example [VIRUS]. 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 "virus" results in the email header as: "X-EMSJudgedThisEmail:virus"

3 Choose one of the actions in **Action for messages identified as Likely Viruses using SonicWall's Time Zero Virus Technology**. SonicWall's Time Zero Virus Technology uses a combination of Predictive and Responsive techniques to identify messages with a possible virus. This technology is most useful when a virus first appears and before a virus signature is available to identify, stop and clean the virus.

Response	Effect
No Action	No action is taken for messages.
Permanently Delete	The email message is permanently deleted. **CAUTION: If you select this option, your organization risks losing wanted email. Deleted email cannot be retrieved.**
Reject with SMTP error code 550	The message is rejected and responds with a 550 error code, which indicates the user's mailbox was unavailable (for example, not found or rejected for policy reasons). **NOTE:** When Capture analysis confirms a definite virus or likely virus, the message is quarantined—even if the reject action is selected—and any attachments are stripped. The quarantine preserves a record of the action and the message is recoverable if needed, rather than being lost.
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 for most configurations.
Send To	Send to email_address, where email_address is the email address of the person designated to deal with viruses. For example, you could Send to `postmaster`.
Tag with	The email is tagged with a term in the subject line, for example [Possible Time Zero Virus]. 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 "likely_virus" results in the email header as: "X-EMSJudgedThisEmail:likely_virus"

NOTE: Messages that are likely to contain viruses should be stored in the Junk Box so that users can retrieve these messages if no virus is found.

4 Click **Apply Changes**.

Configuring Miscellaneous

Viruses removed from messages are identified as definite viruses, but deliver attachments intact for messages identified as likely viruses.

1 Select the A**llow users to unjunk viruses** check box. This setting applies to viruses and likely viruses.

2 Click **Apply Changes**.

Outbound Anti-Virus Protection

Use this page to guard your organization from accidentally sending malicious viruses. SonicWall Email Security Zombie and Spyware Protection blocks spam, phishing attacks, and virus zombies. It also alerts administrators immediately when a zombie has infected your organization. Unauthorized software using an infected computer to send out junk email messages is called a Zombie or Spyware. Spyware may also be used to steal a user's private information, such as credit card numbers or passwords. 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 on the outbound path.

- General Settings
- Zombie Protection Settings
- Monitoring for Zombie and Spyware Activity
- Flood Protection

General Settings

To configure Anti-Virus protection on the outbound path:

1 Navigate to **SECURITY SERVICES | Security Services > Anti-Virus** on the **MANAGE** view and select the **Outbound** tab.

2 Choose one of the actions in:

- Action for messages identified as **Definite Viruses** leaving your organization.
- Action for messages identified by SonicWall's Time Zero Virus Technology as **Likely Viruses** leaving your organization.

Action for Messages identified as Definite Viruses

Response	Effect
No Action	No action is taken for messages.
Permanently Delete	The email message is permanently deleted. **CAUTION: If you select this option, your organization risks losing wanted email. Deleted email cannot be retrieved.**

Action for Messages identified as Definite Viruses

Response	Effect
Reject with SMTP error code 550	The message is rejected and responds with a 550 error code, which indicates the user's mailbox was unavailable (for example, not found or rejected for policy reasons). **NOTE:** When Capture analysis confirms a definite virus or likely virus, the message is quarantined—even if the reject action is selected—and any attachments are stripped. The quarantine preserves a record of the action and the message is recoverable if needed, rather than being lost.
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 recommended setting for most configurations.
Send to	Send to email_address, where email_address is the email address of the person designated to deal with viruses. For example, you could Send to `postmaster@ww.com`.

Zombie Protection Settings

The general settings apply to all users. Enable Zombie and Spyware Protection to block spam, phishing attacks, and virus zombies and to alert administrators immediately when a zombie has infected your organization:

To define the General Settings:

1 Navigate to **SECURITY SERVICES | Security Services > Anti-Virus** on the **MANAGE** view and select the **Outbound** tab.

2 Check the box in **Enable Zombie and Spyware Protection**.

Monitoring for Zombie and Spyware Activity

None of the settings below take any action other than alerting the administrator of a potential zombie infection.

Choose one of the actions in the table below in **Send an Alert to the administrators if**:

Response	Effect
Email is sent from an address not in Lightweight Directory Access Protocol (LDAP)	No action is taken for messages.
More than (specify number) messages are identified as possible threats (within the last hour)	Administrator becomes aware of potential zombie infection.
More than (specify number) messages are sent by one user	Administrator becomes aware of potential zombie infection

Action Settings

The table below contains the actions to take when emails are sent by Zombies. These settings can affect email flow leaving your organization.

Zombie Protection Options

Action	Description
Action for messages leaving your organization that are identified as spam, phishing attacks, or other threat:	Select one of the following settings: **Allow Delivery**—Allows the delivery of the message without interference. **Permanently Delete**—The message is permanently deleted. Use this option with caution since deleted email cannot be retrieved. **Store in Junk Box**—Stores messages with potential threats in the outbound Junk Box.
Action for messages leaving your organization in which the "From" address is not in LDAP:	Select one of the following settings: **Allow any "From" address**— Allows messages from all email addresses. Note that this is the only option you are able to use if you have not configured LDAP. **Permanently delete**—The message is permanently deleted. Use this option with caution since deleted email cannot be retrieved. **Store in Junk Box**—Stores messages from unknown senders in the Junk Box.
Activate/Deactivate Outbound Safe Mode preventing any dangerous attachments from leaving your organization:	Outbound **Safe Mode is on** blocks all emails with potentially dangerous attachments from leaving your organization. When there is a new virus outbreak and one or more of your organization's computers is affected, the virus can often propagate itself using your outbound email traffic. Outbound Safe Mode also minimizes the possibility of new virus outbreaks spreading through your outbound email traffic. Administrators are alerted every 60 minutes that Safe Mode is on.

Zombie Protection Options

Action	Description
When Outbound Safe Mode is on, take this action for any message with dangerous attachments:	If you have enabled Outbound Safe Mode, select one of the following actions when a message with dangerous attachments is received: **Permanently delete**—The message is permanently deleted. Use this option with caution since deleted email cannot be retrieved. **Store in Junk Box**—Stores messages from unknown senders in the Junk Box.
Automatically turn Outbound Safe Mode on and alert administrators every 60 minutes that Safe Mode is on if:	These settings do not take any action other than alerting the administrator of a potential zombie infection. Select any of the check boxes to send and alert to the administrator if: • **Email is sent from an address not in the LDAP (within the last hour)** • **More than (specify number) messages are identified as possible threats within the last hour** • **More than (specify number) messages are sent by one user within an hour**

Miscellaneous

Allow a list of email addresses to be exempt from Zombie Protection: (This list might include any email addresses that are not in LDAP and email addresses that are expected to send a lot of messages.)

Specify senders that will not trigger alerts or actions	Enter email addresses in this box that you want exempt from Zombie Protection. Separate multiple email addresses with a comma. (This list might include any email addresses that are not in LDAP and email addresses that are expected to send a lot of messages.)

Flood Protection

The Flood Protection feature supports Zombie Protection by automatically blocking specified users from sending outbound mail when it exceeds the specified Message Threshold.

To enable Flood Protection:

1. Navigate to **SECURITY SERVICES | Security Services > Anti-Virus** on the **MANAGE** view and click the **Outbound** tab.
2. Scroll down to the **Flood Protection** section.
3. Click the **Enable Flood Protection** check box.
4. Configure the following settings:
    - **Message Threshold**—Specify the amount of outbound messages (between 1-10,000) that are sent by a single sender. Then, specify the interval (in hours) by selecting a value from the drop-down list. The Flood Protection service activates when a sender has exceeded the amount of messages sent within the specified interval of hours.

- **Alert sender when threshold is crossed**—Enable this option to alert the sender that he/she has exceeded the organizational threshold. Note that as a result, outbound emails are now affected.
- **Action on outbound message from Flood Senders**—Select one of the following options to determine what action is taken on outbound messages from flood sender(s):
    - **Permanently delete**—The message is permanently deleted. Use this option with caution since deleted email cannot be retrieved.
    - **Store in Junk Box**—The message moves to the Junk Box and flagged as 'likely virus' with the category name 'flood_protection.' The administrator is able to unjunk the message, which is then delivered from the outbound path.
    - **None**—No action is taken; messages go through as usual.
- **Flood Protection Senders Exception List**—Found under the Miscellaneous section, specify the list of outbound senders that are exempt from the Flood Protection rule.
- **Flood Senders List**—Users that exceeded the specified Message Threshold values are added to this table by Email Address and the time which the Flood Sender was found exceeding the threshold. To remove a user from the Flood Senders List, select the check box next to the email address(es) you wish to remove, then click the **Delete** button.

5 When finished configuring the **Flood Protection** settings, click the **Apply Changes** button.

16

Capture, Time of Click

Topics:

Capture ATP

Capture ATP performs the following functions:

- Scans suspected messages.
- Renders a verdict about the message.
- Takes action based on what the administrator configures for that verdict.

Unlike the anti-virus engines that check against malware signatures stored locally, messages for Capture ATP are uploaded to the back end cloud servers for analysis. These messages are typically advanced threats that evade identification by traditional static filters. They need to be identified by their behavior, and thus need to be run in a highly instrumented environment. Capture ATP accepts a broad range of file types to analyze.

To engage Capture ATP:

1. Inbound email is first scanned by the other anti-virus plug-ins.
    - If a threat is detected, then the appropriate action is taken (discard, junk, tag, etc.).
    - If the service is enabled, all the anti-virus plug-ins return a no threat result, and the message contains an eligible attachment, the email is sent to Capture ATP for analysis.
2. The attachment is uploaded to the Capture server and quarantined in the Capture Box.
3. Capture ATP performs the analysis and returns a verdict.
4. Further analysis is performed and Hosted Email Security applies the policy based on the final disposition of the message.

Capture ATP status and settings can be managed at **SECURITY SERVICES > Security Services > Capture ATP** on the **MANAGE** view.

Basic Setup Checklist

The Basic Setup Checklist shows the status of the various licenses required for Capture ATP. For each item listed, a red X indicates no subscription or an expired one. A green check indicates the license is active or a service is functional.

The items tracked in the checklist include:

- Status of your ATP subscription and the date until when the service is good for. A **disable it** link allows you to stop the service.
- Status of the required base license. A **manage licenses** link takes you to **Overview > License Management**.
- Status of the anti-spam license. A **manage licenses** link takes you to **Overview > License Management**.

Blocking Behavior

Files that are not blocked or excluded by traditional Hosted Email Security services are sent to Capture ATP for analysis. If the Capture analysis returns a malicious judgment, Hosted Email Security applies the actions defined by the Anti-Virus options. A link is provided so you can jump immediately to the Anti-Virus page and view the settings for inbound and outbound traffic.

IMPORTANT: When Capture analysis confirms a definite virus or likely virus, the message is quarantined and any attachments are stripped. This action occurs even if the anti-virus settings specify a reject action. The quarantine preserves a record of the action and the message is recoverable if needed.

Exception Management

Exception Management provides the flexibility for you to define those unique situations in your environment where you do not want certain types of files transferred to Capture ATP for analysis.

In the upper part of the Exception Management section, specify the maximum file size of attachments that can be transferred to Capture ATP for analysis. The default and recommended option is a maximum file size of 10 MB. You can opt for larger file sizes, but the trade-off is the possibility of processing delays for likely good email.

Click on **Submit** once you define the maximum file size.

In the lower part of the Exception Management section, specify the file types, people, companies, mailing lists or IP addresses whose attachments are not be sent to Capture ATP for analysis.

To define the exceptions:

1. Select **Add exception**.
2. Choose the exception type at the top of the popup window:
   - Sender email address
   - Recipient email address
   - Sender email domain
   - Source IP address
   - Attachment file type
3. Enter the details in the text box. Enter only one element, email address or domain per line. If you chose Attachment file type, select the file type from the drop-down list provided.

4 Click on **Add**.

Click on **Clear Filters** to remove all the filters defined in the table.

Within the table, you can sort and filter the exceptions. Click in the heading for the column you want to sort in ascending or descending order. The order is indicated by the small arrowhead in the heading field.

To filter data in the table:

1 Click on the drop-down option in the column heading you want to filter.

2 Check the box by **Filters**.

3 Type the search string in the text box, and the table adjusts to show the results of the filtering.

4 Uncheck the box to remove the filter and the table returns to its prior view.

Time of Click URL Malware Protection

Time-of-Click URL Malware Protection provides a URL filtering mechanism that checks malicious URLs in email messages when users, on their endpoints, click on them rather than at the time they are delivered to Email Security. The feature is enabled by default and rewrites the URLs for further analysis blocking harmful ones.

Enabling Time-of-Click URL Malware Protection

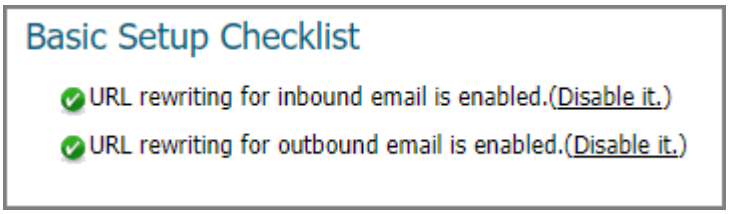
Email Security provides Time-of-Click URL Malware Protection against malicious URLs found in incoming and outgoing email messages. It detects link-based malware and phishing attacks by analyzing the reputation of a URL at the time of click.

To enable Time-of-Click:

1 Navigate to **MANAGE | SECURITY SERVICES > Security Services > Time of Click**.

2 Under **Basic Setup Checklist** you have two choices:

- To enable the feature for inbound email messages, click **Enable it** next to **URL rewriting for inbound email is disabled**.
- To enable the feature for outbound email messages, click **Enable it** next to **URL rewriting for outbound email is disabled**.



NOTE: Time-of-Click URL Malware Protection is disabled by default. The circles next to the commands for inbound and outbound email are red until you enable them and they turn green.

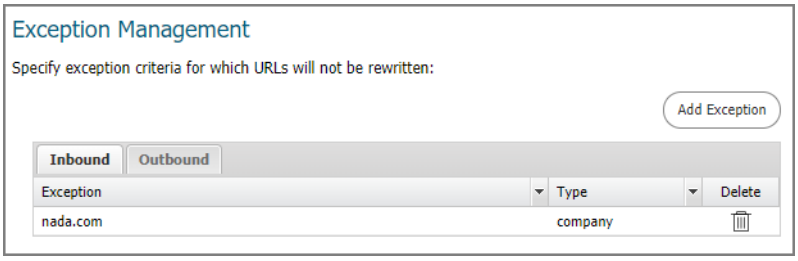
3 Once the URL has been rewritten and the capture service has determined that it is a threat and should not go any further, a default block page pops up and prevents the user from continuing.

4 To customize the **You cannot move forward** generic message, under **Configure Block Page**, click the check box next to **The block page should not allow the email recipient to proceed to the original URL** and type in the text box a message to be displayed at the bottom of the blocked page.

5 Click **Submit**.

6 Under **Exception Management**, specify the email addresses of people (senders) and companies (sender domains) whose email messages do not have their URLs rewritten.

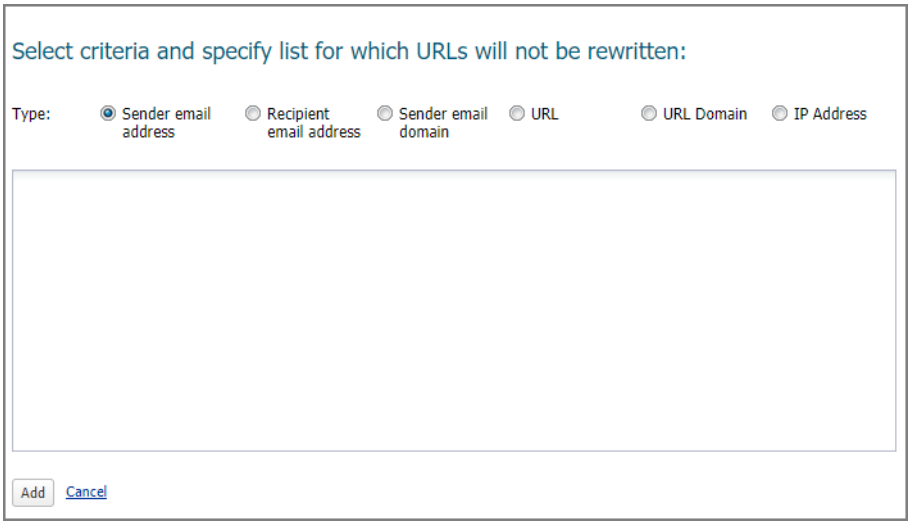
7 Click **Add Exception**.



8 Click on the **Inbound** or **Outbound** buttons and then click on **Add Exception** to type in the popup text box the URLs and URL domains that do not need to be rewritten.

9 **Specify URLs and URL domains that will not be rewritten** by the following types:

- **Sender email address**
- **Recipient email address**
- **Sender email domain**
- **URL**
- **URL Domain**
- **IP Address**



10 Click **Add** when done or click **Cancel** to cancel your selection.

17

Encryption and Connections

Encryption Service

The Encryption Service feature works in tandem with Hosted Email Security as a Software-as-a-Service (SaaS), which provides secure mail delivery solutions. Additionally, the administrator can create a policy with some condition and an action of **Route to Encryption Service**. Emails which satisfy the set conditions are encrypted. Enable **outbound policy** to send secure mail. The mail messages that have `[SECURE]` as part of the Subject are encrypted and securely delivered to the recipient via the Encryption SaaS.To receive secure mails from Encryption Service without them getting flagged as SPF failures, enable the corresponding inbound policies.

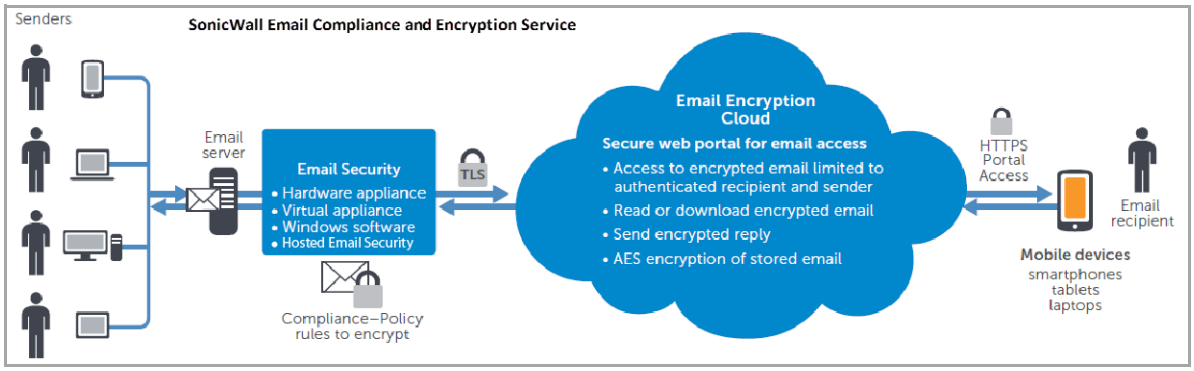
A few things to consider when using the SonicWall Encryption Service:

- The customer is responsible for protecting user passwords and using care in spelling email addresses when sending emails, especially emails containing sensitive information.
- Encrypted emails automatically expire after 30 days and are not recoverable.
- The subject lines of email messages are not encrypted and should not include electronic protected health information (ePHI) or confidential information.

Topics:

- Encryption Service Overview
- Licensing Email Encryption Service
- Configuring Encryption Service

Encryption Service Overview



The Encryption Service works with outbound and inbound email messages. The Encryption Service must first be licensed through the **License Management** page on the **MANAGE** view. The administrator can then enable the default policy filter that allows sending secure email via the Encryption Service. After adding the necessary sender domains and public IP addresses, the administrator can then add users that are licensed to use Encryption Service.

Outbound messages flow in the following order:

1 A user in an organization sends a secure email message. It is sent through the exchange email server of the organization.

2 The message is then processed by Hosted Email Security. Hosted Email Security recognizes the message as Secure Mail based on the auto sender domains or any other policy set to **Route to Encryption Service**.

3 The message is sent from the Hosted Email Security appliance via TLS to the SonicWall Email Encryption Cloud. The Email Encryption Cloud determines if this is a secure message based on the auto sender domains or any other policy set to 'Route to Encryption Service.'

4 The Email Encryption Cloud then sends a notification email to the recipient. This email includes a URL to the secure message.

5 The Secure Mail recipient clicks the URL and is required to log into the Email Encryption Cloud to retrieve the message. Once the recipient views the message, the sender gets a notification mail from Email Encryption Cloud indicating that the secure message has been viewed.

Licensing Email Encryption Service

Because Encryption Service is a subscription service, you must purchase a license by logging in to your MySonicWall account or by contacting your SonicWall reseller.

NOTE: The Encryption Service subscription license must match the Email Protection Subscription (Anti-Spam and Anti-Phishing) user account. If not, you receive an error message.

To license the Email Encryption Service:

1 Navigate to the **MANAGE | Overview > License Management** page.

2 Select **Manage Licenses**.

3 Log in to your **MySonicWall** account with your **username** and **password** and select **LOGIN**.

4 Click on the **Try** or **Activate** links to try or activate Email Encryption Service.

5 Enter the **Email Encryption Service Activation Key** in the text field provided if you choose **Activate**.

6 Click **CONTINUE** if you choose to try the subscription service for free for 30 days.

7 Click on **Return to License Summary**, from the activation or try page, to go back to **License Management**.

8 Navigate to **SECURITY SERVICES | Security Services > Encryption Service** to verify that the settings you just entered are shown in the **Settings** section.

Configuring Encryption Service

Once you have successfully licensed the Email Encryption Service and enabled the Secure Mail outbound policy, you can configure the settings for the service.

Topics:

- DNS Configuration
- Account Management Settings
- Settings
- User View Setup

DNS Configuration

The SonicWall Encryption Service sends secure email on your behalf. To eliminate potential email rejection due to SPF failure, you should include "_spf.sonicsecuremail.com" if you registered the service in the North America Data Center and "_spf.sonicsecuremail.eu" if you registered the service in the European Data Center. If you are unsure of which one your service is registered with, you may include both in your SPF record.

Account Management Settings

To configure Account Management settings:

1. Navigate to **SECURITY SERVICES | Security Services > Encryption Service** on the **MANAGE** view.
2. Under **Account Management Settings**, click the **Refresh** button to synchronize the account management settings from Encryption Service.
3. Select the **Reset Credentials** button to reset and create new credentials. The credentials are used to authenticate the Secure Mail Server Email gateway.
4. Select **Apply Changes** when finished.

Settings

To configure the Encryption Service Settings:

1. Under **Settings**, edit the **Company Name**, if needed.
2. Enter the **Auto Sender Domains** in the space provided. A user account is automatically created for the mail sent from these domains.

   NOTE: Be sure you own and control the domains listed here.

3. Check the box if you want to **Allow the SonicWall Encryption Service to route email replies directly to your organization's Email Server over a secure channel**.

   NOTE: The TLS has to be enabled on your inbound paths on the **SYSTEM SETUP| Server** page.

4. Select **Apply Changes** when finished.

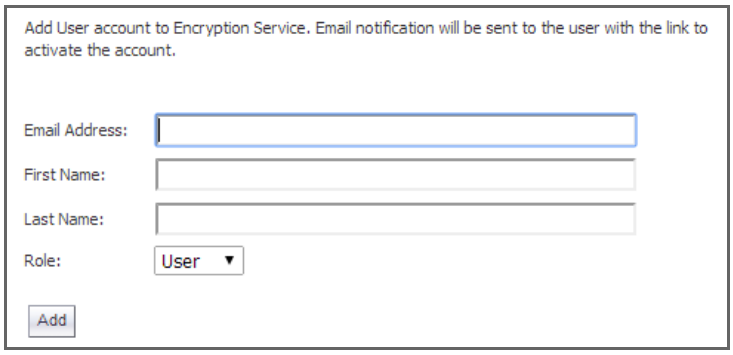
User View Setup

SonicWall recommends that the administrator should add users to the Encryption Service. If any email messages are sent to Encryption Service and the sender's account (whose domain is listed in the Auto-Sender Domains) does not exist, it is automatically created. Click on **Refresh** to sync the user accounts from the Encryption Service.

Adding a New User

To add a new user to the Encryption Service:

1 Scroll down to the **User View Setup** section, and click the **Add** button.



2 Enter the following fields:

- **Email Address**—Enter the email address for the user.
- **First Name**—Enter the first name of the user.
- **Last Name**—Enter the last name of the user.
- **Role**—Select the role of the user from the drop-down list. The available options are User or Admin.

3 Click **Add** to finish. The new user displays in the User View Setup list.

NOTE: You may need to click the **Refresh** button to synchronize user accounts and settings from the Secure Email Encryption server if it does not automatically display.

Updating an Existing User

To update the information of an existing user:

1 Select the check box corresponding to the user you want to update.

2 Click the **Update** button.

3 Edit the **First Name**, **Last Name**, and **Role** in the popup window that displays.

NOTE: You cannot update the **User Email Address**.

4 Click **Update** to save your changes and update the user information.

Deleting an Existing User

To delete an existing from the list:

1 Navigate to **SECURITY SERVICES > Security Services > Encryption Service** and scroll down to **User View Setup**.

2 Select the check box corresponding to the user you want to delete.

3 Click the **Delete** button.

4 Click **OK** on the popup window that displays asking if you want to delete the selected user.

5 After a few seconds, the user is automatically deleted.

Adding an Existing User

If you have LDAP configured, you can add existing users to the Secure Email Encryption Service.

To add existing users:

1 Click the **Add** button.

2 Enter the user's **Email Address**, **First Name**, **Last Name**, and **Role** in the popup window that displays.

3 The new user displays in the User View Setup list.

NOTE: The new user receives an email notification with a link to activate the account.

Importing Users

If you would like to add multiple users, you can import a .txt list of users to be added to the Secure Email Encryption Service.

The .txt file must use a <TAB> delimiter between the primary email address, first name, last name, and role of each user. You must use <CR> to separate entries. See the following example:

```
primary_email@company.com<TAB>firstname<TAB>lastname<TAB>admin<CR>
primary_email@company.com<TAB>firstname<TAB>lastname<TAB>user<CR>
```

The primary email address is mandatory, while the other fields are optional.

To import users:

1 Navigate to S**ECURITY SERVICES > Security Services > Encryption Service** and scroll down to **User View Setup**.

2 Click the **Import Users** button.

3 Click the **Choose File** button to select the file containing the list of users.

4 Click **Import**.

Exporting Users

To export the list of Encryption Service users:

1 Navigate to **SECURITY SERVICES > Security Services > Encryption Service** and scroll down to **User View Setup**.

2 Click on the **Export Users** button. The list exports a .txt file and saves it to your local system.

Cobranding and Reporting

The Encryption Service allows you to customize features on the SonicWall Email Encryption Service Portal management console.

The following are Cobrand and Reporting settings you can configure through the **SonicWall Email Encryption** service portal:

Topics:

SonicWall Email Encryption Service Portal

The SonicWall Email Encryption Service Portal displays as a popup window. The columns at the top of the portal include:

- **Compose**—Click on this column to create an email message. Use the buttons at the top of the compose text box to **Send Secure** messages, **Save Draft** messages, access your **Address Book**, or **Cancel** your message.
  - In the **To** text field, enter the **email address** of the person you want to send your message to.
  - Enter the **Subject** of your email message in the text field provided.
  - **Choose File** for your message **Attachments**. Click **Add** or **Remove** for your Attachment function.
  - Write your **Message** in the text field provided.
  - Click **Show Options** to select your message **Priority**, **Receipt** confirmation, **Expiration** date, **File in Folder**, **Password Protection**, and other **Restrictions**.
  - Click **Hide Options** to conceal your message options.
  - Click the **Send Secure** button when finished.
- **Member Center**—Click on this column to see your launch pad to all your account features. It allows you to access your messages, your **SecureMail 500 administrator** credentials, and your **Message & Files**, **My Account**, **Download Console**, **Admin Console**, and **Account Details**.
- **Administration** —See Administering Your Corporate Accounts for information about the content of this column.
- **Inbox**—Click on this column to see your messages in the Inbox folder. You can enter a query in the **Search** text field or search by selecting a **Subject** from the drop-down list choices which are **ID**, **From**, and **Date**. Click **Go** when you are finished.
- **Track Sent**—Click on this column to see the secure email messages that you send, which are placed in your Track Sent folders. You can enter a query in the **Search** text field or search by selecting a **Subject** from the drop-down list choices which are **ID**, **From**, and **Date**. Click **Go** when finished.

- Choose your **View Folders** from the drop-down list: **All Folders**, **Track Sent**, **Drafts**, **Trash**, **Deleted Trash**, and **Archive**.
- Choose your **Page Size** from the drop-down list: **All**, **10**, **15**, **20**, **25**, **50**, **100**, and **250**.

- **Help**—Click on this column after you click on any of the portal interface elements to learn more about the features.

At the bottom of the portal you find:

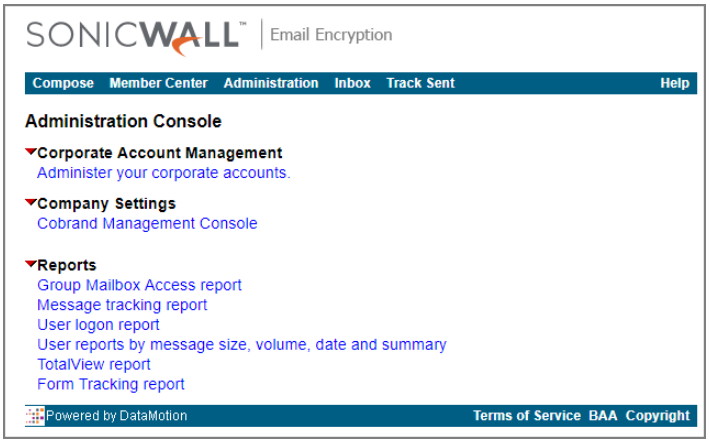
- **Terms of Service**—Click on this column to learn about the Terms of Service you agree to when you sign up for the **Encryption Service** license.
- **BAA**—Click on this column to learn about the **Business Associate Agreement** you sign to use the Encryption Service.
- **Copyright**—Click on this column to learn about the copyright information related to the Encryption Service Portal.

Administering Your Corporate Accounts

You can edit your organization's information on the **Company Configuration > Company** page from the Secure Email Encryption service portal.

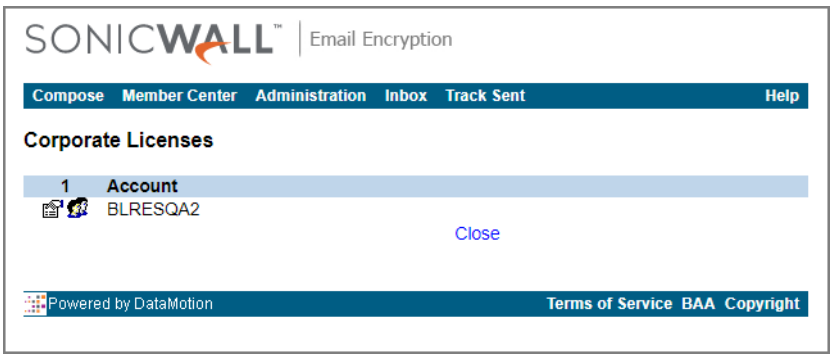
1 Navigate to **SECURITY SERVICES > Security Services > Encryption Service** and scroll down to **User View Setup**.

2 Click on the **Co-Branding and Reporting** button. The Secure Email Encryption service portal popup window displays showing the **Administration Console**: **Corporate Account Management**, **Company Settings**, and **Reports**.



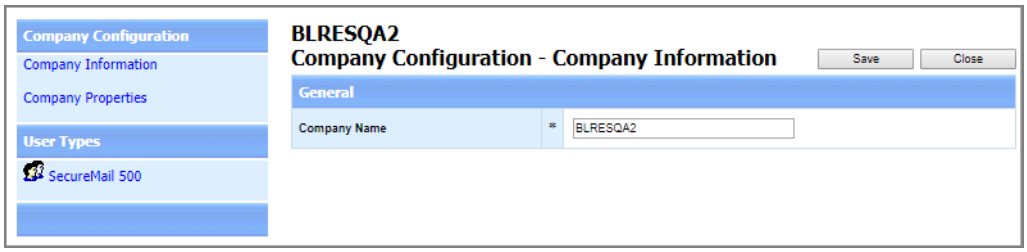
3 Under **Corporate Account Management**, click on the **Administer your corporate accounts** link.

4 Under **Corporate Licenses**, click on the icon under the number **1**.



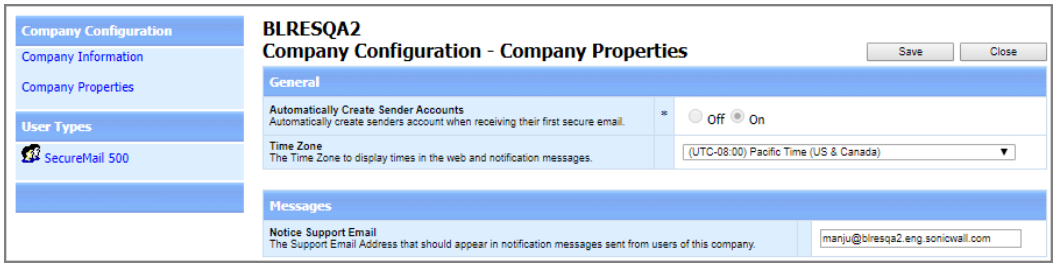
5 Under **Company Configuration**, click on **Company Information** and **Company Properties** to do the following:

- Under **Company Information**, edit your **Company Name** specified on the **License Management** page once licensing the Encryption Service is completed.
- Click **Save** or **Close** when done.



- Under **Company Properties > General**, edit the **Automatically Create Sender Accounts** setting. Select **Off** or **On**. The accounts are created after the senders receive their first secure email.
- Edit the **Time Zone** setting from the drop-down menu. This time displays on the web and in the notification messages.
- Under **Company Properties > Messages**, edit the **Email Address** of the administrator specified on the **License Management** page once licensing the Encryption Service is completed.

> **NOTE:** This is the support email address that should appear in the notification messages that company users send.

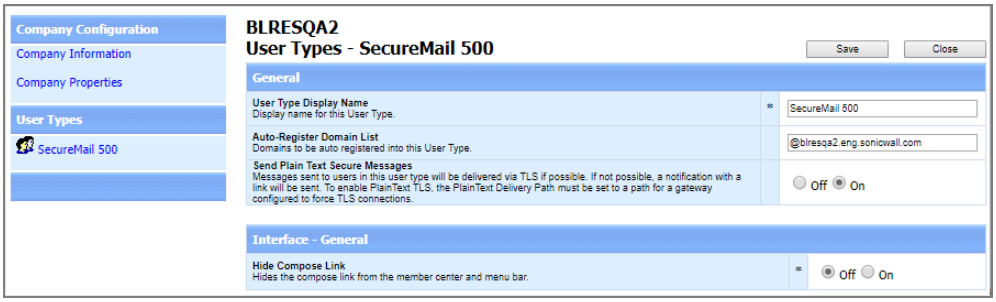


6 Under **User Types**, click **SecureMail 500** to do the following:

- Under **User Types > General**, you can edit these:
  - The **User Type Display Name** in the text field provided.
  - The **Auto-Register Domain List** in the text field provided.
  - The **Send Plain Text Secure Messages**. Select **Off** or **On**.

7 Under **User Types > Interface - General**, choose **Off** or **On** to **Hide Compose Link** from the member center and menu bar.

8 Click **Save** or **Close** when done.

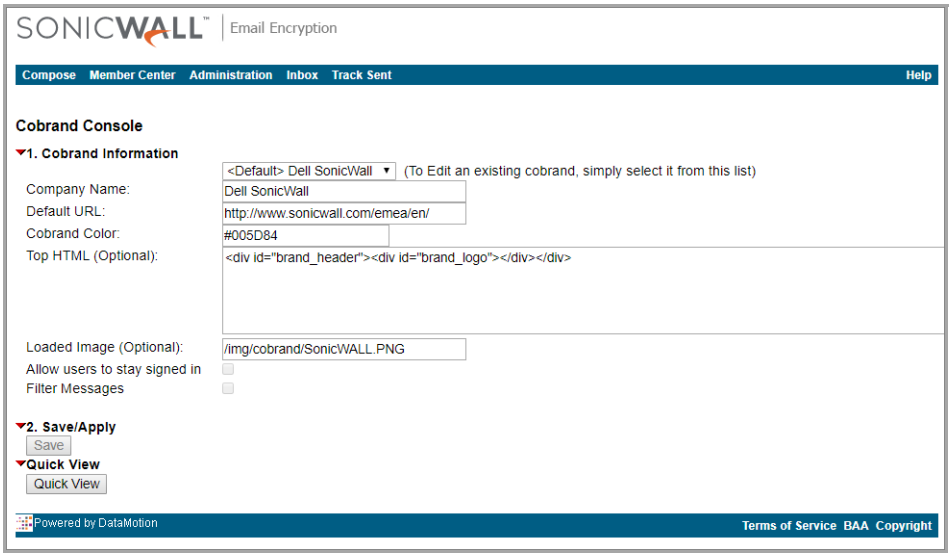


Cobrand Management Console

The **Cobrand Management Console** page allows you to edit your organization's existing cobrand settings or create a new cobrand.

To edit an existing cobrand or create a new cobrand:

1. In the **Co-Branding and Reporting Email Encryption** popup window, go to **Administration Console > Company Settings > Cobrand Management Console**.
2. To create or edit an existing cobrand, select it from the drop-down list.
3. Specify the following cobrand settings:
    - Company Name—A descriptive name that is associated with the cobrand and is displayed in the drop-down list for editing.
    - Default URL—The URL where users are directed when they click the cobrand image. Note that you must include the protocol/scheme ("http://") in the URL.
    - Cobrand Color—The web color used for the login panel, top and bottom ribbon bars (menu and status bars) for Web pages on the server portal. The web color is identified with 6-character hexadecimal number, commonly used with HTML, CSS, and other applications. You can also identify the cobrand color using the Color Selector box that displays upon editing the hexadecimal number.
    - Top HTML (Optional)—Allows you to specify a block of HTML coding to be used in place of the cobrand image in the page header. The HTML can contain text, links, graphics, and columns, or follow an HTML style sheet.
    - Note that if the Top HTML field contains boilerplate code, do not delete it unless you intend to replace it with customized HTML.
    - Loaded Image (Optional)—Displays the database server path and internal filename for the uploaded cobrand image.
    - Allow users to stay signed in—Select the check box to enable, and then specify the amount of time for users to stay signed in.
    - Filter Messages—Select the check box to enable. Allows you to limit the messages that users see in their mailbox to messages related to the cobranded company. If enabled, the Secure Mail recipient's mailbox only displays messages from or to the cobranded company, as long as the recipient accesses the server using the notification email link.
4. Click the **Save/Apply** button to save your changes and apply the cobrand to your organization.
5. Click **Quick View** if you want to see a quick preview of your selections.

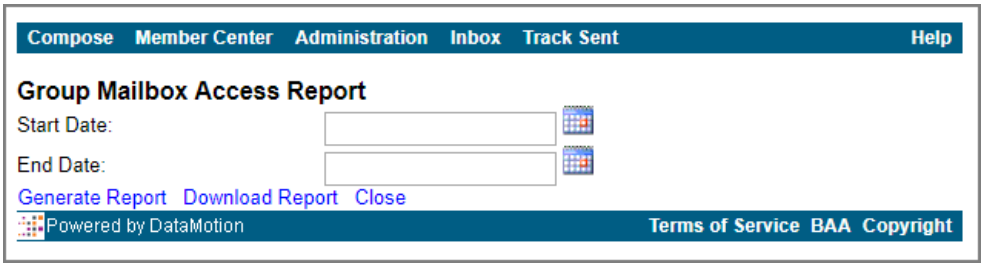


Group Mailbox Access Report

Use the **Group Mailbox Access Report** to generate reports about groups of users.

To generate a Group Mailbox Access Report:

1 Click the Group Mailbox Access Report link from the Secure Email Encryption service portal.



2 Select your report **Start Date** and **End Date** by clicking on the calendar icon to the right of the text fields provided.

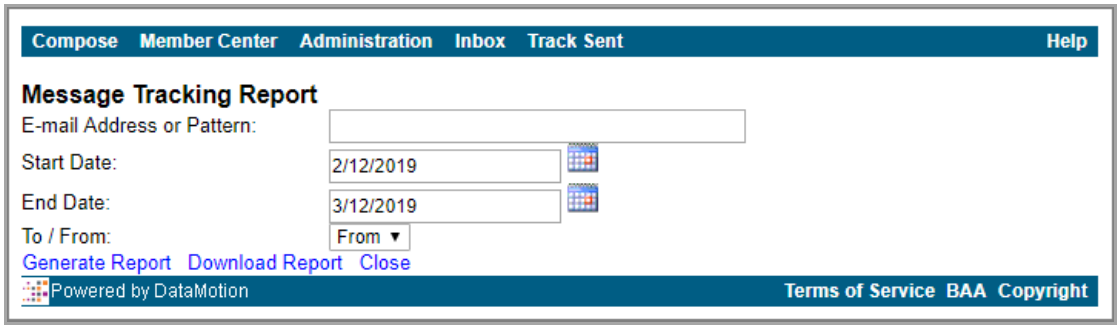
3 Click the **Generate Report**, **Download Report**, or **Close** links provided. The report displays all the messages matching the specific criteria.

Message Tracking Report

Use the **Message Tracking Report** to search through email addresses and subject lines of encrypted messages (message bodies are not included in the search).

To generate a Message Tracking Report:

1 Click the **Message Tracking Report** link from the Secure Mail Encryption Service portal.



2 Enter the search parameters into the **Email Address** or **Pattern**, **Start Date**, and **End Date** fields. The **To/From** drop-down list specifies whether to search for the parameters in the To or From field of email messages.

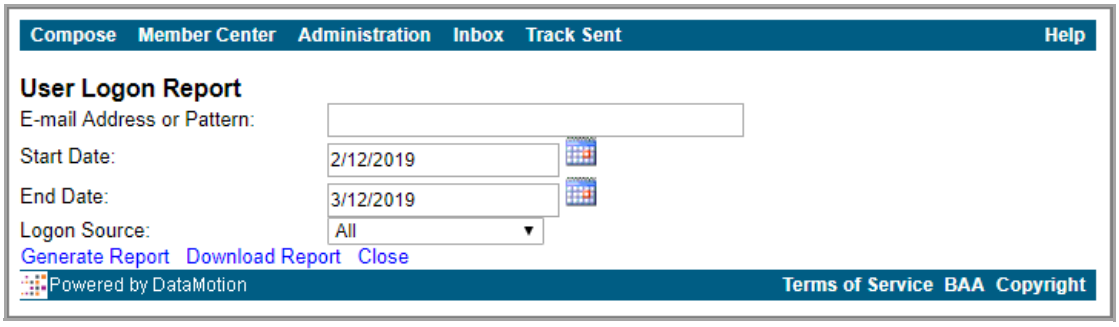
3 Click **Generate Report**, **Download Report**, or **Close** links. The report displays all messages matching the specified criteria.

User Logon Report

The User Logon Report generates reports about user log on activity. You can search activity based on specific users, defined time frames, and also how the user logged into the service.

To generate a User Logon Report:

1 Click the **User Logon Report** link from the Secure Email Encryption service portal.



2 Enter the search parameters into the **Email Address** or **Pattern**, **Start Date**, and **End Date** fields. The **Logon Source** drop-down list specifies which service the user accessed. The default is **All**, which includes every service the user may have used.

3 Click the **Generate Report**, **Download Report**, **or Close** links. The report generates all log on events for the user, based on the specified criteria.

User Reports by Message Size, Volume, Date, and Summary

There are several types of user reports, each of which can be filtered for sent or received messages (or both) for each user and the complete statistics by user. These reports are summaries of user statistics, differing from the more detailed reports such as the Message Tracking Report. You can **View** and **Download** the reports.

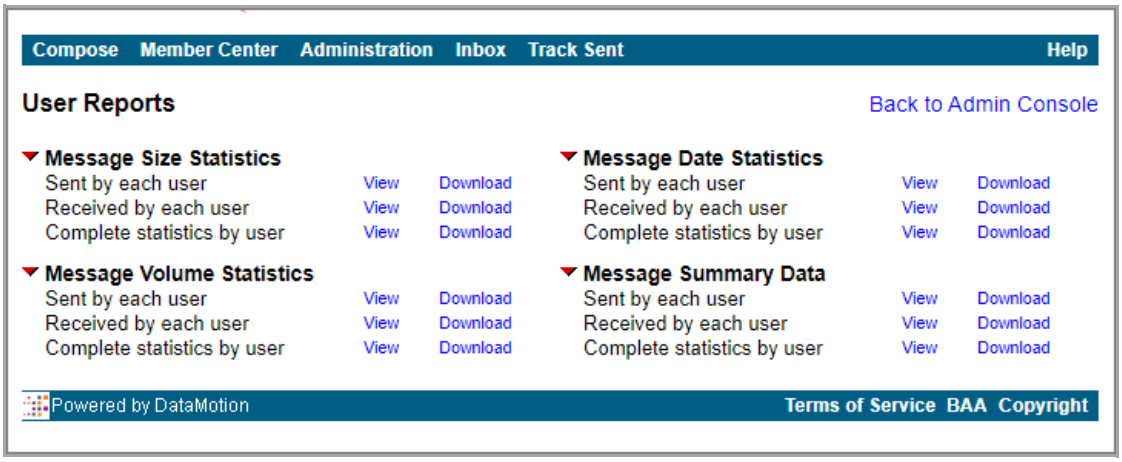
Types of User Reports describes the types of reports that can be generated:

Types of User Reports

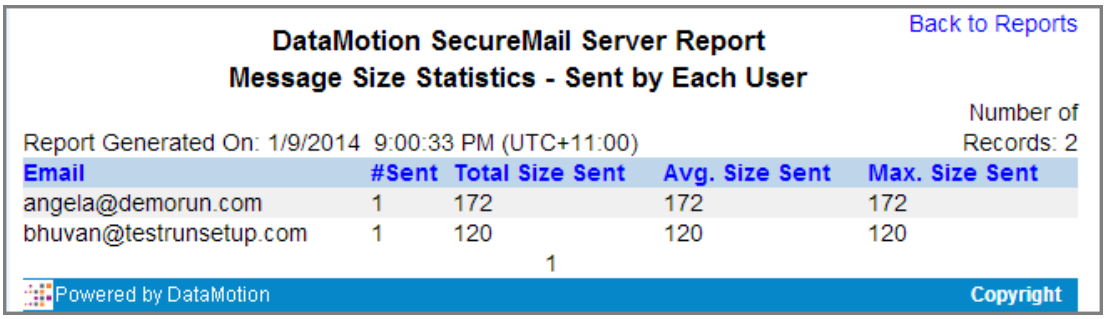
Report Type	Description
Message Size Statistics	Shows the size of messages sent and received by each user and the complete statistics by user.
Message Date Statistics	Shows when messages have been sent by the user (first and last messages for each user) and the complete statistics by user.
Message Volume Statistics	Shows the number of messages sent/received by the user and the complete statistics by user.
Message Summary Data	Shows the fields of other statistics reports on one screen and the complete statistics by user.

To access any User Report:

1 Click the **User Reports by Message Size, Volume, Date, and Summary** link from the Secure Email Encryption service portal.



2 Click on the Report to view the information.



Total View Report

The **Total View Report** provides complete tracking of all messages sent through the Encrypted Service. The report contains a record of every messages sent along with the tracking data for the message (and attachments) in a single report.

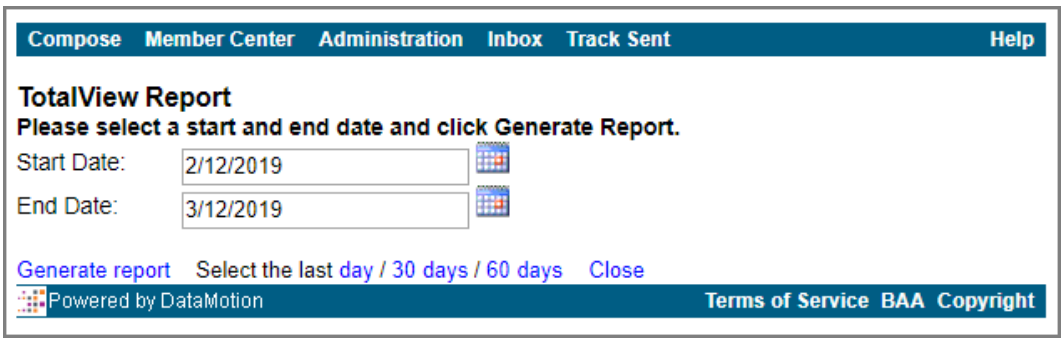
To generate a Total View Report:

1 Click the **Total View Report** link from the Secure Email Encryption service portal.

2 Select your report **Start Date** and **End Date** by clicking on the calendar icon to the right of the text fields provided.

3 Click the **Generate Report**, **Select the last day / 30 days / 60 days**, and **Close** links provided. The report displays all the messages matching the specific criteria.

4 Click the **Download Report** link to save the CSV file to your local system. Click **Select Different Dates** to return to the previous screen and conduct a new search with different dates.



This report is provided as an Excel file that includes the following fields:

- Message ID
- Custom ID
- Date
- From Email
- To Email
- Subject
- Notification Timestamp
- Message Status (Opened / Not Opened)
- Message Open Time
- Attachment Name
- Attachment Size
- Attachment Status (Accessed / Not Accessed)
- Attachment Open Time

NOTE: Each message and every attachment within a message is reported separately. For example, a message to two recipients with two attachments generates four rows of data: Two for each recipient, with one attachment listed on each line per recipient.

Form Tracking Report

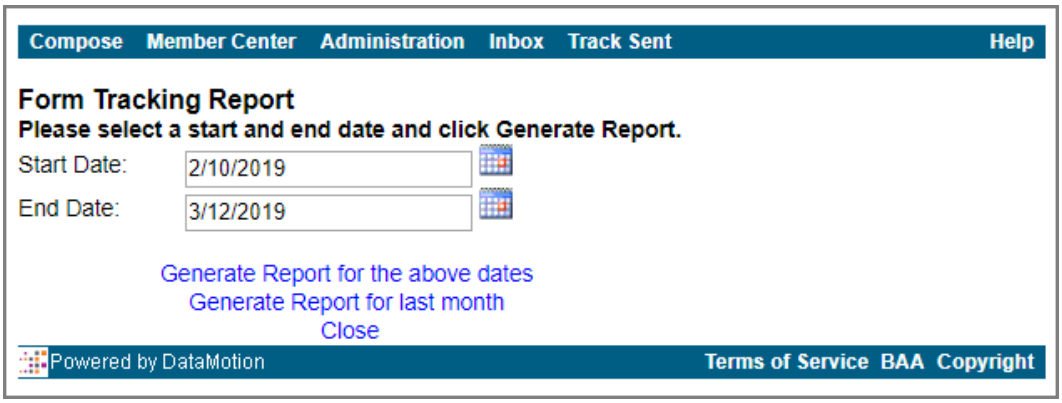
The **Form Tracking Report** provides complete tracking of all forms sent through the Encrypted Service. The report contains a record of every form sent along with the tracking data for the message (and attachments) in a single report.

To generate a Form Tracking Report:

1 Click the **Form Tracking Report** link from the Secure Email Encryption service portal.

2 Select your report **Start Date** and **End Date** by clicking on the calendar icon to the right of the text fields provided.

3 Click the **Generate Report for the above dates**, **Generate Report for last month**, or **Close** links provided. The report displays all the reports matching the specific criteria.



4 Click on the **Download Report** or **Select Different Dates** links to get your report or choose another time frame.

18

Reporting

The **REPORTING** section of the **MANAGE** view allows you do Scheduled Reports to customize and schedule delivery of your reports through email.

Scheduled Reports

You can have Hosted Email Security reports emailed to you regularly. You can choose the type of report, a time span the data covers, the list of recipients, and so forth.

Data in the scheduled reports is displayed in the time zone of the server where the data is stored (either an All in One or a Control Center), just like the reports on the **MONITOR** view. Scheduled report emails are sent according to the time zone on that system as well.

To add a a scheduled report:

1. Navigate to **REPORTING | Scheduled Reports** on the **MANAGE** view.
1. Select the **Add New Scheduled Report** button.
2. Select **Which report** from the drop-down list in the page that displays.
3. Select **Frequency of report email** from the drop-down list. Options range from **1 Day** to **30 Days**.
4. For **Time of day to send report**, select one of the following options:
    - **Any time of day**
    - **Within an hour of** <*choose time from drop-down menu*>.
5. For **Day of week to send report**, select one of the following:
    - **Any day of the week**
    - **Send report on** <*choose day from drop-down menu*>.
6. For **Time zone**, select from the drop-down list.
7. Select **Language of report email** from the drop-down list.
8. Select **Report has data for the last** <*choose time period from drop-down menu*>. Options range from **1 Day** to **180 Days**.
9. For **Report lists results by**, choose for the results to be listed by the **Hour** or by the **Day**.
10. Choose the **Report Format**: **JPEG**, **CSV**, or **PDF**.
11. Type the **Name from which report is sent** in the text field provided.
12. Type the **Email Address From Which Report is Sent** in the text field provided.
13. Type the email addresses for the **Recipients of Report Email** in the text field provided. Separate multiple email addresses with a comma.
14. Specify the **Report Name** in the text field provided.

15 Click **Save Scheduled Report** when finished. The report appears in the Reports table.

Part 5

Appendixes

- Interface Map
- SonicWall Support

A

Interface Map

Beginning with Hosted Email Security 10.0, the interface has been enhanced so commands align under the key functions of **MONITOR**, **INVESTIGATE**, and **MANAGE**. Related commands on the left-hand menu are grouped under a divider labels for easier navigation. Refer to the following table to see how the classic interface maps to the enhanced interface.

Classic Menu Structure			Enhanced Menu Structure			
Group 1	**Group 2**	**Group 3**	**Top Nav**	**Divider Label**	**Group**	**Node**
Report & Monitoring	Reports	Dashboard	MONITOR			Dashboard
Report & Monitoring	Reports	Connection Management Reports	MONITOR	Event Summaries		All Event Connections
Report & Monitoring	Reports	Anti-Spam Reports	MONITOR	Event Summaries		Anti-Spam
Report & Monitoring	Reports	Anti-Spoof Reports	MONITOR	Event Summaries		Anti-Spoof
Report & Monitoring	Reports	Anti-Phishing Reports	MONITOR	Event Summaries		Anti-Phishing
Report & Monitoring	Reports	Anti-Virus Reports	MONITOR	Event Summaries		Anti-Virus
Report & Monitoring	Reports	Directory Protection	MONITOR	Event Summaries		Directory Harvest
Report & Monitoring	Reports	Capture ATP Reports	MONITOR	Event Summaries		Capture ATP
Report & Monitoring	Reports	Policy Management Reports	MONITOR	Policy & Compliance		Policy
Report & Monitoring	Reports	Compliance Reports	MONITOR	Policy & Compliance		Compliance
Report & Monitoring	Reports	Encryption Service Reports	MONITOR	Policy & Compliance		Encryption
Report & Monitoring	Monitoring	Real-Time System Monitor	MONITOR	Appliance Health		Live Monitor
Report & Monitoring	Reports	Performance Metrics	MONITOR	Appliance Health		Performance Metrics
Report & Monitoring	Reports	User Statistics	MONITOR	Appliance Health		LDAP Users
Report & Monitoring	Monitoring	System Status	MONITOR	Current Status		System Status

Classic Menu Structure			Enhanced Menu Structure			
Group 1	**Group 2**	**Group 3**	**Top Nav**	**Divider Label**	**Group**	**Node**
Report & Monitoring	Monitoring	MTA Status	MONITOR	Current Status		MTA Status
Junk Box Management		Junk Box	INVESTIGATE			Junk Box
	(new feature)		INVESTIGATE	Email Continuity		Inbox
	(new feature)		INVESTIGATE	Email Continuity		Outbox
	(new feature)		INVESTIGATE	Email Continuity		Sent Items
Auditing		Messages	INVESTIGATE	Logs		Message Logs
Auditing		Connections	INVESTIGATE	Logs		Connections Logs
Capture ATP		Status	INVESTIGATE	Logs		Capture ATP Logs
Reports & Monitoring	DMARC Reports	DMARC Reports	INVESTIGATE	Tools		Run DMARC Reports
System		Audit Trail	INVESTIGATE	Tools		Audit Trail
System		Diagnostics	INVESTIGATE	Tools		Diagnostics
System		License Management	MANAGE			License Management
System		Advanced	MANAGE			Firmware Update
System		Manage Backups	MANAGE		Backup & Restore	Manage Backups
System		Schedule Backup	MANAGE		Backup & Restore	Schedule Backup
System		FTP Profiles	MANAGE		Backup & Restore	FTP Profiles
		Downloads	MANAGE			Downloads
Policy & Compliance		Filters	MANAGE	Policy & Compliance		Filters
Policy & Compliance		Policy Groups	MANAGE	Policy & Compliance		Policy Groups
Policy & Compliance	Compliance	Dictionaries	MANAGE	Policy & Compliance	Compliance	Dictionaries
Policy & Compliance	Compliance	Approval Boxes	MANAGE	Policy & Compliance	Compliance	Approval Boxes
Policy & Compliance	Compliance	Encryption	MANAGE	Policy & Compliance	Compliance	Encryption
Policy & Compliance	Compliance	Record ID Definitions	MANAGE	Policy & Compliance	Compliance	Record ID Definitions
Policy & Compliance	Compliance	Archiving	MANAGE	Policy & Compliance	Compliance	Archiving
System		Administration	MANAGE	System Setup	Server	Administration

Classic Menu Structure			Enhanced Menu Structure			
Group 1	**Group 2**	**Group 3**	**Top Nav**	**Divider Label**	**Group**	**Node**
System		LDAP Configuration	MANAGE	System Setup	Server	LDAP Configuration
System		Updates	MANAGE	System Setup	Server	Updates
System		Monitoring	MANAGE	System Setup	Server	Monitoring
System		Host Configuration	MANAGE	System Setup	Server	Host Configuration
System		Advanced	MANAGE	System Setup	Server	Advanced
System		User View Setup	MANAGE	System Setup	Customization	User View Setup
System		Branding	MANAGE	System Setup	Customization	Branding
System	Certificates	Generate/ Import	MANAGE	System Setup	Certificates	Generate/ Import
System	Certificates	Generate CSR	MANAGE	System Setup	Certificates	Generate CSR
System	Certificates	Configure	MANAGE	System Setup	Certificates	Configure
Users, Groups & Organizations		Users	MANAGE	System Setup	Users, Groups & Organizations	Users
Users, Groups & Organizations		Groups	MANAGE	System Setup	Users, Groups & Organizations	Groups
Users, Groups & Organizations		Organizations	MANAGE	System Setup	Users, Groups & Organizations	Organizations
System	Network Architecture	Server Configuration	MANAGE	System Setup	Network	Server Configuration
System	Network Architecture	MTA Configuration	MANAGE	System Setup	Network	MTA Configuration
System	Network Architecture	Email Address Rewriting	MANAGE	System Setup	Network	Email Address Rewriting
System	Network Architecture	Trusted Networks	MANAGE	System Setup	Network	Trusted Networks
Junk Box Management		Junk Box Settings	MANAGE	System Setup	Junk Box	Message Management
Junk Box Management		Junk Box Summary	MANAGE	System Setup	Junk Box	Summary Notifications
Anti-Spam		Spam Management	MANAGE	Security Services	Anti-Spam	Spam Management
Anti-Spam		Address Books	MANAGE	Security Services	Anti-Spam	Address Books
Anti-Spam		Anti-Spam Aggressiveness	MANAGE	Security Services	Anti-Spam	Anti-Spam Aggressiveness
Anti-Spam		Language	MANAGE	Security Services	Anti-Spam	Language
Anti-Spam		Black List Services	MANAGE	Security Services	Anti-Spam	Black List Services

Classic Menu Structure			Enhanced Menu Structure			
Group 1	**Group 2**	**Group 3**	**Top Nav**	**Divider Label**	**Group**	**Node**
Anti-Spam		Spam Submissions	MANAGE	Security Services	Anti-Spam	Spam Submissions
		Anti-Spoofing	MANAGE	Security Services		Anti-Spoofing
		Anti-Phishing	MANAGE	Security Services		Anti-Phishing
		Anti-Virus	MANAGE	Security Services		Anti-Virus
Capture ATP		Settings	MANAGE	Security Services		Capture ATP
		Encryption Service	MANAGE	Security Services		Encryption Service
System		Connection Management	MANAGE	Security Services		Connection Management
Reports & Monitoring	DMARC Reports	Configure Known Networks	MANAGE	Reporting		Configure Known Networks
Reports & Monitoring		Scheduled Reports	MANAGE	Reporting		Scheduled Reports

B

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract and to customers who have trial versions.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. To access the Support Portal, go to https://www.sonicwall.com/support.

The Support Portal enables you to:

- View knowledge base articles and technical documentation
- View video tutorials
- Access MySonicWall
- Learn about SonicWall professional services
- Review SonicWall Support services and warranty information
- Register for training and certification
- Request technical support or customer service

To contact SonicWall Support, visit https://www.sonicwall.com/support/contact-support.

About This Document

Legend

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

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

IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.

Hosted Email Security Administration Guide
Updated - February 2023
Software Version - 10.0
232-004796-00 Rev C