SonicWall® Global Management System 9.3 Anti-Spam Security

Administration

SONICWALL®

Contents

1

Licensing and Enabling Anti-Spam

The **Security|Anti-Spam > Settings** page allows you to activate the Anti-Spam feature, configure email threat categories, modify access lists, and set advanced options.

NOTE: Anti-Spam does not apply to the SuperMassive 9800.

Topics:

Licensing Anti-Spam Service

The Anti-Spam service needs to be licensed so that the feature can be enabled on your appliance to provide appliance-level protection from spam, phishing, and virus messages.

To license Anti-Spam for your firewall:

1. Navigate to **Register/Upgrades > Service Licenses**.
2. In **AVAILABLE SERVICES** section, select **Comprehensive Anti-Spam Service** from the **Select service** drop-down menu.
3. If the subscription status of the service is **Not Active**, enter appropriate **Activation Code** and click **Subscribe**, otherwise go to step 4.

   You can also register for free trial of Anti-Spam service.
4. Navigate to **System > Tools,** click **Synchronize Licenses,** and then click **OK** to confirm**.**

Enabling Anti-Spam Service

Prerequisite: You can enable Anti-Spam service for a firewall only when you have licensed Anti-Spam service. To license Anti-Spam service for a firewall, see Licensing Anti-Spam Service.

When you enable Anti-Spam, your appliance will have appliance-level protection from spam, phishing, and virus messages.

To enable Anti-Spam:

1. In the Management Panel, navigate to the **Security | Anti-Spam > Settings** page.

2 Click **Enable Anti-Spam Service** to activate the Anti-Spam feature.

   A message describing the effects of enabling the Anti-Spam Service and requesting agreement to proceed is displayed.

3 Click **Proceed**.

   Another message about the destination mail server to be used is displayed.

4 Click **Proceed** to perform mail server configuration.

   A dialog requesting information about the destination mail server is displayed. If the anti-spam settings are already configured for the firewall in the **Anti-spam > Base Setup** page in the firewall management interface, the details of the mail server are populated automatically.

5 Update the details of destination mail server in the boxes displayed:

   - **Mail Server Public IP**: The IP address of the server that is available for external connections (MX record).
   - **Mail Server Private IP**: The IP address of the server for internal traffic (Mail server).
   - **Junk Store IP Address**: The server IP where the junk store application runs.

6 Click **Proceed**.

   A message displays explaining what is created during the installation.

7 Click **Confirm**.

   Modify Task Description and Schedule page for destination mail server configuration is displayed.

8 To activate destination mail server settings:

   a A **Description** is displayed by default, you can edit it if required.

   b Set the schedule as to when the destination mail server should be activated:

      - Default
      - Immediate
      - At (you can specify date and time)

   c If you wish to omit any of the settings you configured for destination email server, click **Edit** and clear the selection of the items.

   d Click **Accept** to activate the destination mail server configuration at the scheduled time.

When the Anti-Spam feature is enabled, you can:

- Download and install the Junk Box; see Installing the Junk Store
- Configure the email threat categories; see Configuring Email Threat Categories.

Installing the Junk Store

Anti-Spam can create a Junk Store on your Microsoft Exchange Server. The Junk Store quarantines messages for end-user analysis and provides statistics. Log in to your Exchange system, then open a browser to log in to the management interface, and install the Junk Store.

NOTE: While SonicWall supports non-Exchange SMTP servers, such as Sendmail and Lotus Domino, it is not required to install the Junk Store on one of these servers. SonicWall recommends installing Junk Store on a stand-alone server.

To install the Junk Store:

1 Log in to the Exchange system where you want to install the junk store.

2 Open a web browser.

IMPORTANT: To download and install the SonicWall Junk Store application, you need the following on the system where you will install the Junk Store application:

- Internet Explorer 6 or above
- Microsoft Exchange Server
- Email Downloader ActiveX component for IE

3 Log in to the Management Service interface.

4 Navigate to the **Anti-spam > Base Setup** page.

5 Go to the **SonicWall Junk Store Installer** section.

6 Click the **Junk Store Installer**  icon to install the junk store on your Windows server.

NOTE: The first time the Junk Store application is installed, it takes about 5 minutes for the Junk Store to be operational.

7 If your browser warns you that the Web site is trying to load the SonicWall Email Security add-on:

a Click in the Information Bar.

b Select **Install ActiveX Control** in the pop-up menu. The Security Warning Screen displays.

8 Click **Install** to install the ActiveX Control.

9 On the **Anti-Spam > Base Setup** page, click the **Junk Store Installer**  icon again. A progress bar is displayed on the page.

10 The installer launches when it is fully downloaded.

NOTE: Migrating data to the Junk Store may take a long time to complete.

Configuring Email Threat Categories

When Anti-Spam is activated, set your preferences. After these are configured, your email is filtered and sorted according to your configuration.

To set default settings for user's messages:

1 Navigate to the **Security|Anti-Spam > Settings** page.

2 Scroll to the **Email Threat Categories** section.

3 Choose default settings for messages that contain or may contain spam, phishing, and virus issues; see Email Threat Category Settings: Options for options available in the drop-down menus:

- **Likely Spam** (default: **Store in Junk Box**)
- **Definite Spam** (default: **Permanently Delete**)
- **Likely Phishing** (default: **Tag with [LIKELY_PHISHING]**)
- **Definite Phishing** (default: **Store in Junk Box**)
- **Likely Virus** (default: **Store in Junk Box**)
- **Definite Virus** (default: **Permanently Delete**)

Email Threat Category Settings: Options

Category	Action
Filtering off	Anti-Spam does not scan and filter any email for this threat category, so all the email messages are delivered to the recipients.
Tag With [*TAG*]	The email is tagged with a term in the subject line: • [LIKELY_SPAM] • [SPAM] • [LIKELY_PHISHING] • [PHISHING] • [Possible Time Zero Virus] • [VIRUS] Selecting this option allows the user to have control of the email and can junk it if it is unwanted.
Store in Junk Box	The email message is stored in the Junk Box. It can be unjunked by users and administrators with appropriate permissions.
Reject Mail	The email message is rejected without even allowing a connection.
Permanently Delete	The email message is permanently deleted. CAUTION: **If you select this option, your organization risks losing wanted email.**

If you are using more than one domain, choose the **Multiple Domains** option in **EMAIL DOMAINS** section and contact SonicWall or your SonicWall reseller for more information.

Configuring Access Lists

The two lists in the **User-defined Access Lists** section allow you to manage static allow and reject lists by designating which clients are allowed or denied connection to deliver email.

NOTE: Entry settings in these lists take precedence over GRID IP reputation check results.

To configure the lists:

1. Navigate to the **Security | Anti-Spam > Settings** page.
2. Scroll down to the **User-defined Access Lists** section.
3. Click the **Edit** icon for the list, **Allow Client List** or **Reject Client List**, you want to configure. The **Allow/Reject Client List** dialog appears.
4. Select items from the left column you want to add to the Allow List or add to the Reject List.
5. Click the **Right Arrow** button.

   To remove items from the **Allow/Reject** List:

   a. Select the item(s) from the right box.

   b. Click the **Left Arrow** button.
6. When finished, click the **OK** button.

7 Description is displayed by default in the **Description** box, edit the description if required. Specify as to when the task should be effective. To edit the configuration before you make it effective, click **Edit** and make required changes.

8 Click **Accept**.

To add a host to the lists:

1 Navigate to the **Security|Anti-Spam > Settings** page.

2 Scroll down to the **User-defined Access Lists** section.

3 Click the **Add Host** icon. The **Add Host to Allow/Reject List** dialog appears.

4 Enter a name for the host in the **Name** field.

5 Select the type of host from the **Type** drop-down menu. The following setting(s) change, depending on the host type selected.

6 If you selected:

- **Host** (default) – enter the IP address in the **IP Address** field.
- **Range** – enter the starting and ending IP addresses in the **Starting IP Address** and **Ending IP Address** fields.
- **FQDN** – enter the FQDN hostname in the **FQDN Hostname** field.

7 Click **OK**.

Configuring Advanced Options

In the **Advanced Options** section, you can set the email options described in Anti-Spam > Settings: Advanced Options:.

Anti-Spam > Settings: Advanced Options

Setting type	Setting	Description
Anti-Spam Advanced Settings	Allow/Reject delivery of unprocessed mails when SonicWall Anti-Spam Service is unavailable	If the Anti-Spam service is not enabled or unavailable for some other reason, you can choose to let all unprocessed emails go through or to reject all unprocessed emails. Spam messages are delivered to users as well as good email. Choose from the drop-down menu: • **Allow** (default) • **Reject**
	Tag and Deliver/Delete/Reject Emails when SonicWall Junk Store is unavailable	If Junk Store cannot accept spam messages, you can choose to delete them or deliver them with cautionary subject lines such as `[Phishing] Please renew your account.` Choose from the drop-down menu: • **Tag & Deliver** (default) • **Delete** • **Reject**

Anti-Spam > Settings: Advanced Options

Setting type	Setting	Description
Monitoring Service Probes	Probe Interval (minutes)	Set the timer frequency, in minutes, for probing Email Security components in the WAN and LAN networks. The minimum time is 1 minute, the maximum is 60 minutes, and the default is **5** minutes.
	Probe Timeout (seconds)	Set the time, in seconds, for the probe to wait for response from the target before flagging as failure. The minimum time is 30 seconds, the maximum is 300 seconds, and the default is **30** seconds.
	Success Count Threshold	Set the number of consecutive successful responses before declaring the entity as operational. The minimum number is 1 response, the maximum is 10 responses, and the default is **1** response.
	Failure Count Threshold	Set the number of consecutive successful responses before declaring the entity as unreachable. The minimum number is 1 response, the maximum is 10 responses, and the default is **3** response.
Destination Mail Server Settings	Server Public IP Address	The IP address of the server that is available for external connections. MTAs use this WAN IP address for SMTP connection. This number is populated by the address you specified when activating and installing Anti-Spam and Junk Store. You can change the address.
	Server Private IP Address	The IP address of the server for internal traffic. This is the internal mail server IP address behind the appliance. This number is populated automatically by the address you specified when activating and installing Anti-Spam and Junk Store. You can change the address.
	Inbound Email Port	The TCP service port your appliance has open to receive inbound emails. The minimum is 0, the maximum is 65535, and the default is **function generated**.
Junk Store Settings	Use Destination Mail Server Private Address as Junk Store Address	If the Junk Store is on the destination mail server, select the checkbox. The address is populated automatically by the address you specified when activating and installing Anti-Spam and Junk Store. You can change the address. This checkbox is selected by default, and the Junk Store IP Address field is dimmed. ***To change the address:*** 1 Uncheck the checkbox. The Junk Store IP Address field becomes available. 2 Enter the Junk Store IP address of where the server is located.
Others	Enable Email Subsystem Detection	Enables discover of available email system resources in the network. This checkbox is selected by default.

After you configure Advanced Anti-spam settings, click **Update** to save the changes or click **Reset** to restore the default settings.

2

Configuring the RBL Filter

NOTE: The Anti-Spam service is an advanced superset of the standard Management Service RBL Filtering. When Anti-Spam is enabled, RBL Filtering is performed and handled by the comprehensive anti-spam service and therefore configuration options are not available in the **Anti-Spam > RBL Filter** page.

If Anti-Spam is not enabled, you can configure the settings on the **Real-time Black List Settings** page. All Anti-Spam and Junk Box pages are unavailable, however.

NOTE: **Anti-Spam > RBL Filter** does not apply to the SuperMassive 9800.

About RBL Lists

SMTP Real-Time Black List (RBL) is a mechanism for publishing the IP addresses of SMTP servers from which or through which spammers operate. There are a number of organizations that compile this information both for free: http://www.spamhaus.org, and for profit: https://ers.trendmicro.com/.

NOTE: SMTP RBL is an aggressive, spam-filtering technique that can be prone to false-positives because it is based on lists compiled from reported spam activity. The Management Service implementation of SMTP RBL filtering provides a number of fine-tuning mechanisms to help ensure filtering accuracy.

RBL list providers publish their lists using DNS. Blacklisted IP addresses appear in the database of the list provider's DNS domain using inverted IP notation of the SMTP server in question as a prefix to the domain name. A response code from `127.0.0.2` to `127.0.0.11` indicates some type of undesirability:

For example, if an SMTP server with IP address `1.2.3.4` has been blacklisted by RBL list provider `sbl-xbl.spamhaus.org`, then a DNS query to `4.3.2.1.sbl-xbl.spamhaus.org` provides a `127.0.0.4` response, indicating that the server is a known source of spam, and the connection is dropped.

NOTE: Most spam today is known to be sent from hijacked or zombie machines running a thin SMTP server implementation.Unlike legitimate SMTP servers, these zombie machines rarely attempt to retry failed delivery attempts. After the delivery attempt is blocked by RBL filter, no subsequent delivery attempts for that same piece of spam is made.

Management Service Response to a Blacklist Query

The DNS responses are collected and cached. If any of the queries result in a blacklisted response, the server is filtered. Responses are cached using TTL values, and non-blacklisted responses are assigned a cache TTL of 2 hours. If the cache fills up, then cache entries are discarded in a FIFO (first-in-first-out) fashion.

The IP address check uses the cache to determine if a connection should be dropped. Initially, IP addresses are not in the cache, and a DNS request must be made. In this case, the IP address is assumed innocent until proven guilty, and the check results in the allowing of the connection. A DNS request is made and results are cached in a separate task. When subsequent packets from this IP address are checked, if the IP address is blacklisted, the connection is dropped.

Enabling the RBL Filter

When Real-time Black List blocking is enabled, inbound connections from hosts on the WAN, or outbound connections to hosts on the WAN, are checked against each enabled RBL service with a DNS request to the DNS servers configured under RBL DNS Servers.

To enable the Real-time Black List filter:

1. Navigate to the **Anti-Spam > RBL Filter** page.
2. Select **Enable Real-time Black List Blocking**.
3. Select the DNS Servers from the RBL DNS Servers drop-down menu:
   - **Inherit Settings from WAN Zone** (default) — The DNS server(s) IP address(es) are displayed, but dimmed in the **DNS Server 1/2/3** fields.
   - **Specify DNS Servers Manually** — The **DNS Server 1/2/3** fields become available.
     1) Enter one or more DNS server IP addresses in the **DNS Server 1/2/3** fields.
4. Click **Update**.
5. Edit the **Description** if required, specify when the RBL filter should be activated, and click **Accept**.

Managing RBL Services

You can add additional RBL services in the **Real-time Black List Services** section.

The **Real-time Black List Services** section displays information about and actions for the available RBL services:

- **RBL Service** – The name of the RBL service. Two are provided by SonicWall, but you can add others:
  - sbl-xbl.spamhaus.org – Spamhaus Project, which provides real-time anti-spam protection for Internet networks
  - dnsbl.sorbs.net – SORBS (Spam and Open Relay Blocking System), which provides access to its DNS-based Black List (DNSBL) database
- **Response Codes** – Mouse over the **Comment** icon to display a list of response codes. For information about response codes, see About RBL Lists.
- **Enable** – Select the checkbox to enable the RBL service. The checkboxes for the two provided services are selected by default.

To disable an RBL service, clear its checkbox. This does not delete the entry from the table, so you can enable the service in the future.

- **Configure** – Displays icons for various actions:
  - **Edit** icon – Displays the **Edit RBL Domain** dialog. See Editing an RBL Service.
  - **Delete** icon – Deletes the RBL service entry. See Deleting an RBL Service.

Topics:

Adding an RBL Service

To add an RBL service:

1. Navigate to the **Security | Anti-Spam > RBL Filter** page.
2. Scroll to the **Real-Time Black List Services** section.
3. Click the **Add** button. The **RBL Domain Settings** page displays.
4. Enable the service for use by selecting the **Enable RBL Domain** checkbox.
5. Specify the domain name of the RBL service to be queried in the **RBL Domain** field.
6. Specify the expected response codes by selecting their checkboxes. Most RBL services list the responses they provide on their Web site, although selecting **Block All Responses** is generally acceptable.

   TIP: Selecting the **Block All Responses** checkbox selects the checkboxes for all the blocked responses. Deselecting the **Block All Responses** checkbox deselects the checkboxes of all the blocked responses.

7. Click **Update**.

   The RBL service is added to the **Real-Time Black List Services** table.

Editing an RBL Service

To edit an RBL Service:

1. Navigate to the **Security | Anti-Spam > RBL Filter** page.
2. Scroll down to the **Real-Time Black List Services** section.
3. Click the **Edit** icon associated with the RBL Service you want to change. The **Add RBL Domain** dialog displays.
4. Optionally, edit the domain name of the RBL service to be queried in the **RBL Domain** field.

   TIP: You can enable or disable an RBL service by selecting/deselecting its **Enable** checkbox in the **Real-time Black List Services** table.

5. Optionally, enable or disable the service for use by selecting/deselecting the **Enable RBL Domain** checkbox.

6 Optionally, select or deselect the expected response codes by selecting their checkboxes.

> **TIP:** Selecting the **Block All Responses** checkbox selects the checkboxes for all the blocked responses. Deselecting the **Block All Responses** checkbox deselects the checkboxes of all the blocked responses.

7 Click **OK**.

Deleting an RBL Service

To delete one RBL service:

1 Navigate to the **Security | Anti-Spam > RBL Filter** page.

2 Click the **Delete** icon for the service in the **Real-time Black List Services** table. A warning message displays.

3 Click **OK**. The entry is deleted from the **Real-Time Black List Services** table.

To delete one or more RBL services:

1 Navigate to the **Security | Anti-Spam > RBL Filter** page.

2 Select the checkbox of one or more services in the **Real-time Black List Services** table. The **Delete** button becomes active.

3 Click the **Delete** button. A warning message displays.

4 Click **OK**. The entry is deleted from the **Real-Time Black List Services** table.

User-Defined SMTP Server Lists

> **NOTE:** You can modify, but not delete, the **RBL User White List** or the **RBL User Black List**.

The **User Defined SMTP Server Lists** section allows for Address Objects to be used to construct a white-list (explicit allow: **RBL User White List**) or black-list (explicit deny: **RBL User Black List**) of SMTP servers. Entries in these lists bypass the RBL querying procedure.

To ensure that you always receive SMTP connections from a partner site's SMTP server:

1 Navigate to the **Security | Anti-Spam > RBL Filter** page.

2 Scroll down to the **User-Defined SMTP Server Lists** section.

3 Click the **Edit** icon in the **Configure** column of the **RBL User White List**. The **Edit Address Object Group** dialog displays.

4 Select the address objects to be added from the left column. Multiple address objects can be selected at one time.

5 Click the **Right Arrow** button.

To delete an address object from the group, select the address object and click the **Left Arrow** button.

6 Click **OK**. The table is updated, and that server is always allowed to make SMTP exchanges.

3

SonicWall Support

Technical support is available to customers who have purchased SonicWall products with a valid maintenance contract.

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 and participate in the Community forum discussions at https://community.sonicwall.com/technology-and-support.
- 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

NOTE: A NOTE icon indicates supporting information.

IMPORTANT: An IMPORTANT icon indicates supporting information that may need a little extra attention.

TIP: A TIP indicates helpful information.

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

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

Global Management System Anti-Spam Security Administration
Updated - October 2020
232-005141-00 Rev B