# SonicOS 7.0

# Anti-Spam

## Administration Guide

SONICWALL®

# Contents

**Anti-Spam** ..... **4**
About Anti-Spam ..... 4
What is Anti-Spam? ..... 4
Benefits ..... 5
How Does the Anti-Spam Service Work? ..... 5
GRID Network ..... 6
Address and Service Objects ..... 7
Purchasing an Anti-Spam License ..... 8

**Status** ..... **10**

**Settings** ..... **11**
Activating Anti-Spam ..... 12
Installing the Junk Store ..... 12
Configuring Email Threat Categories ..... 14
Configuring Access Lists ..... 15
Configuring User-defined Access Lists ..... 16
Adding a Host to the Access Lists ..... 16
Configuring Advanced Settings ..... 18

**Relay Domains** ..... **21**
About Open Relay ..... 21
Listing Allowed Relay Domains ..... 22

**Junk Box Messages** ..... **23**
Information Displayed in the Junk Box Messages Table ..... 24
Managing Junk Box Messages ..... 25

**Junk Box Settings** ..... **27**

**Junk Box Summary** ..... **28**
Managing the Junk Box Summary ..... 29

**User View Setup** ..... **31**
Configuring User View Setup ..... 31

**Address Books** ..... **33**
About the Tabs ..... 33

Allowed Lists ..... 33
Blocked Lists ..... 34
Adding Items to the Allowed or Blocked List ..... 34
Deleting Items from the Allowed or Blocked List ..... 34
Importing Address Book Entries ..... 35
Exporting Address Book Entries ..... 35
Searching the Allowed and Blocked Lists ..... 36

**Manage Users ..... 37**
Updating the User Table ..... 37
Enabling Non-LDAP User Authentication ..... 38
Viewing Users ..... 38
Selecting the Type and Sever of User to View ..... 38
Selecting a Server's Users to View ..... 39
Finding a User ..... 39
Adding Users ..... 39
Adding Users Manually to the User Table ..... 39
Importing Users to the User Table ..... 40
Signing In as a User ..... 40

**LDAP Configuration ..... 42**
Adding an LDAP Server ..... 42
Configuring LDAP Queries ..... 45
Adding LDAP Mappings ..... 47
Editing an LDAP Server Configuration ..... 49
Deleting an LDAP Server ..... 49

**Advanced ..... 50**
Downloading System/Log Files ..... 51
Selecting Log Settings ..... 52

**Downloads ..... 54**

**SonicWall Support ..... 55**
About This Document ..... 56

1

# Anti-Spam

**NOTE:** Anti-Spam is a separate, licensed feature that provides a quick, efficient, and effective way to add anti-spam, anti-phishing, and anti-virus capabilities to your existing firewall. This feature is not available in NSv series.

**Topics:**


- About Anti-Spam
- How Does the Anti-Spam Service Work?
- Purchasing an Anti-Spam License


## About Anti-Spam

**Topics:**


- What is Anti-Spam?
- Benefits


### What is Anti-Spam?

The Anti-Spam feature provides a quick, efficient, and effective way to add anti-spam, anti-phishing, and anti-virus capabilities to your existing firewall.

In a typical Anti-Spam configuration, you choose to add Anti-Spam capabilities by selecting it in the SonicOS interface and licensing it. The firewall then uses the same advanced spam-filtering technology as the SonicWall Email Security products to reduce the amount of junk email delivered to users.

There are two primary ways inbound messages are analyzed by the Anti-Spam feature:

- Advanced IP Reputation Management
- Cloud-based Advanced Content Management

IP Address Reputation uses the GRID Network to identify the IP addresses of known spammers, and reject any mail from those senders without even allowing a connection. GRID Network Sender IP Reputation Management

checks the IP address of incoming connecting requests against a series of lists and statistics to ensure that the connection has a probability of delivering valuable email. The lists are compiled using the collaborative intelligence of the SonicWall GRID Network. Known spammers are prevented from connecting to the firewall, and their junk email payloads never consume system resources on the targeted systems.

Email that does not come from known spammers is analyzed based on “GRIDprints” generated by SonicWall’s research laboratories and are based on data from millions of business endpoints, hundreds of millions of messages, and billions of reputation votes from the users of the GRID Network. Our Grid Network uses data from multiple SonicWall solutions to create a collaborative intelligence network that defends against the worldwide threat landscape. GRIDprints uniquely identify messages without exposing data contained in the email message.

The Anti-Spam service determines that an email fits only one of the following threats: Spam, Likely Spam, Phishing, Likely Phishing, Virus, or Likely Virus. It uses the following precedence order when evaluating threats in email messages:

| | | |
|---|---|---|
| • Phishing | • Virus | • Spam |
| • Likely Phishing | • Likely Virus | • Likely Spam |

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

If the Anti-Spam service determines that the message is not any of the above threats, it is judged as good email and is delivered to the destination server.

## Benefits

Adding anti-spam protection to your firewall increases the efficiency of your system as a whole by filtering and rejecting junk messages before users see them in their inboxes.

- Reduced amount of bandwidth and resources consumed by junk email in your network
- Reduced number of incoming messages sent to the mail server
- Reduced threat to the organization, because users cannot accidentally infect their computers by clicking on virus spam
- Better protection for users from phishing attacks

# How Does the Anti-Spam Service Work?

This describes the Anti-Spam feature, including the SonicWall GRID Network, and how it interacts with SonicOS as a whole. The two points of significant connection with SonicOS are Address and Service Objects. You use the address and service objects to configure the Anti-Spam feature to function smoothly with SonicOS. For example, use the Anti-Spam Service Object to configure NAT policies to archive inbound email as well as sending it through a filter.

The Comprehensive Anti-Spam Service analyzes messages’ headers and contents and uses collaborative GRID printing to block spam email.

**Topics:**

- GRID Network
- Address and Service Objects

# GRID Network

The GRID Connection Management with Sender IP Reputation feature is used by SonicWall Email Security and by the Anti-Spam service in SonicOS. GRID Network Sender IP Reputation is the reputation a particular IP address has with members of the SonicWall GRID Network. When this feature is enabled, email is not accepted from IP addresses with a bad reputation. When SonicOS does not accept a connection from a known bad IP address, mail from that IP address never reaches the email server.

GRID Network Sender IP Reputation checks the IP address of incoming connection requests against a series of lists and statistics to ensure that the connection has a probability of delivering valuable email. The lists are compiled using the collaborative intelligence of the SonicWall GRID Network. Known spammers are prevented from connecting to the firewall, and their junk email payloads never consume system resources on the targeted systems.

**Topics:**

- Benefits
- GRID Connection Management with Sender IP Reputation and Connection Management Precedence Order

## Benefits

- As much as 80 percent of junk email is blocked at the connection level, before the email is ever accepted into your network. Fewer resources are required to maintain your level of spam protection.
- Your bandwidth is not wasted on receiving junk email on your servers, only to analyze and delete it.
- A global network watches for spammers and helps legitimate users restore their IP reputations if needed.

## GRID Connection Management with Sender IP Reputation and Connection Management Precedence Order

When a request is sent to your first-touch firewall, the Anti-Spam service evaluates the ‘reputation’ of the requester. The reputation is compiled from white lists of known-good senders, block lists of known spammers, and denial-of-service thresholds.

If IP Reputation is enabled, the source IP address is checked in the order shown in Evaluation order:

### EVALUATION ORDER

| Evaluation | Description |
|---|---|
| **Allow-list** | If an IP address is on this list, it is allowed to pass messages through Connection Management. The messages are analyzed by your firewall as usual. |
| **Block-list** | This IP address is banned from connecting to the firewall. |
| **Reputation-list** | If the IP address is not in the previous lists, the firewall checks with the GRID Network to see if this IP address has a bad reputation. |
| **Defer-list** | Connections from this IP address are deferred. A set interval must pass before the connection is allowed. |
| **DoS** | If the IP address is not on the previous lists, the firewall checks to see if the IP address has crossed the Denial of Service threshold. If it has, the appliance uses the existing DoS settings to take action. |

Only if the IP address passes all of these tests does the firewall allow that server to make a connection and transfer mail. If the IP address does not pass the tests, there is a message from SonicOS to the requesting server indicating that there is no SMTP server. The connection request is not accepted.

# Address and Service Objects

The Anti-Spam feature of SonicOS supports Address and Service Objects to manage a customer's email server (s). These objects are used by the Anti-Spam Service for its NAT and Access Rule policies. Automatically-created rules are not editable and will be deleted if the Anti-Spam Service is disabled.

When enabled, the Anti-Spam service creates NAT policies and Access Rules to control and redirect email traffic. The policies and rules are visible in the **POLICY | Rules and Policies > NAT Rules** page, but are not editable. These automatically-created policies are only available when the Anti-Spam service is enabled. For further information about these rules and policies, see the *SonicWall SonicOS Rules and Policies Administration Guide*.

When the Anti-Spam service is licensed and activated, the **POLICY | Anti-Spam > Settings** page shows a single option to enable Anti-Spam. Selecting the option invokes the **Destination Mail Server Policy Wizard** if there is no existing custom access rule and NAT policy for an already-deployed scenario. When you set up generated policies, the Anti-Spam service must know where the emails are routed behind the firewall. Specifically it needs the destination mail server IP address and its zone assignment. The **Destination Mail Server Policy Wizard** is launched if this data cannot be found.

You need the following information for the wizard:

- **Destination Mail Server Public IP Address** – The IP address to which external MTAs (message transfer agents) connect by SMTP.
- **Destination Mail Server Private IP Address** – The internal IP address of the Exchange or SMTP server (behind the firewall).
- **Zone Assignment** – The zone to which the Exchange server is assigned.
- **Inbound Email Port** – The TCP service port number to which emails will be sent, also known as the inbound SMTP port.

If this information is needed, a message displays.

Clicking PROCEED walks you through the wizard's requests

Policies and Address Objects created by the wizard are editable and persist even if the Anti-Spam service is disabled.

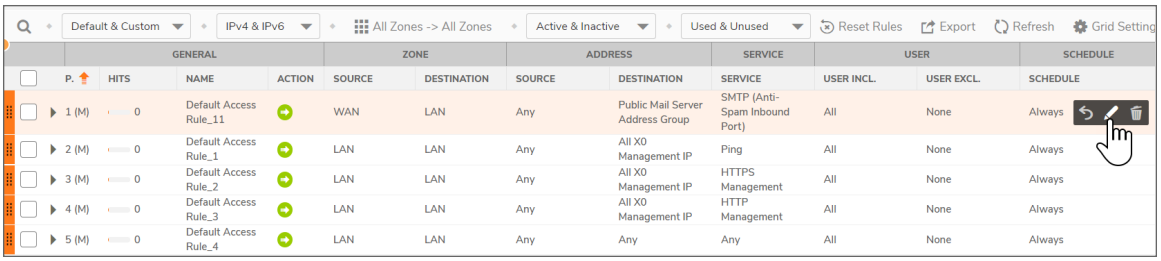
**Topics:**

- Objects Created When the Anti-Spam Service Is Enabled

## Objects Created When the Anti-Spam Service is Enabled

This section provides an example of the type of rules and objects generated automatically as Firewall Access Rules, NAT Policies and Service Objects. These objects are not editable and will be removed if the Anti-Spam service is disabled.

The **POLICY | Rules and Policies > Access Rules** page shows the generated rules used for Anti-Spam.




The top row shows the access rules generated when Anti-Spam is activated. It is the default rule that Anti-Spam creates when there are no existing mail server policies.

You could also create the following access rules:

- WAN to WAN rule for incoming email (SMTP) from any source to all the WAN IP addresses
- WAN to LAN rule for processed email from Email Security Service to all the WAN IP address using the Anti-Spam service port (default:10025)

The Anti-Spam Service Object is created in the **OBJECT | Match Objects > Services | Service Objects** page.

This Service Object is referenced by the generated NAT policies.

# Purchasing an Anti-Spam License

The following deployment prerequisites are required to use the Anti-Spam feature:

- A licensed SonicWall network security appliance
- Anti-Spam License for the appliance

- One of the following Microsoft Windows Servers:
  - Windows Server 2012 R2 (64-bit)
  - Windows Server 2012 (64-bit)
  - Windows SBS 2008 R2 Server (64-bit)
  - SBS 2008 (64-bit)

Purchasing an Anti-Spam license for the firewall can be done directly through MySonicWall.com or through your reseller.

ⓘ | **NOTE:** Your SonicWall network security appliance must be registered with MySonicWall.com before use.

***To purchase an Anti-Spam license:***

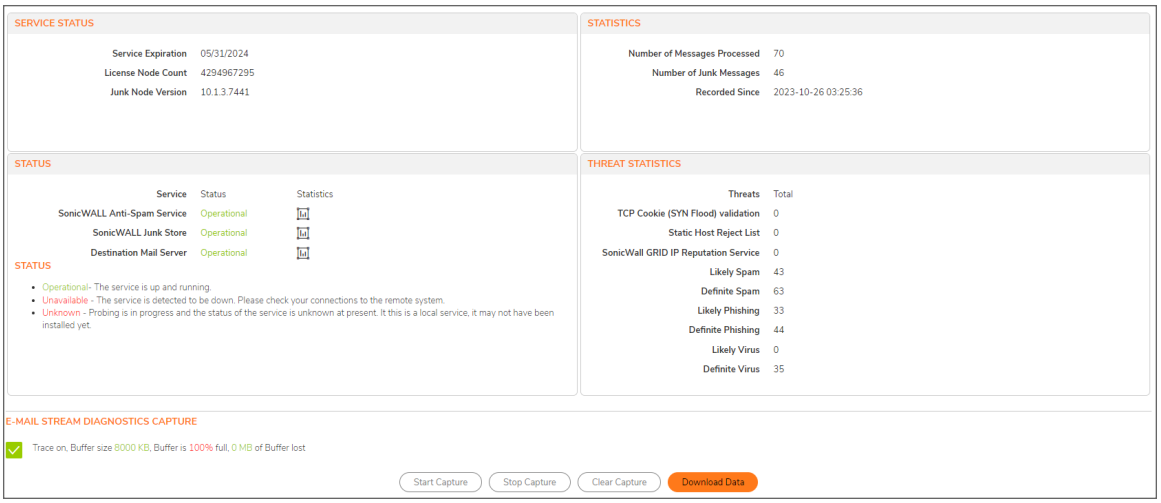
1. Open a Web browser on the computer you use to manage your SonicWallappliance.
2. Enter `http://www.MySonicWall.com` in the **location** or **address** field.
3. Enter your MySonicWall.com account user name and password in the appropriate fields.
4. Click **Submit**.
5. Navigate to **My Products** in the left-hand navigation bar.
6. Select the appliance to which you wish to add Anti-Spam capability.
7. Register for an Anti-Spam license.
8. Login to your appliance's web management interface.
9. Navigate to the **MANAGE | Updates > Licenses** page from the navigation bar at MySonicWall.com.
10. In the **Manage Security Services Online** section, click the link to activate or renew your license. Alternately, enter your key or keyset in the **Manual Upgrade** section.
11. Enter your MySonicWall.com login information.

2

# Status

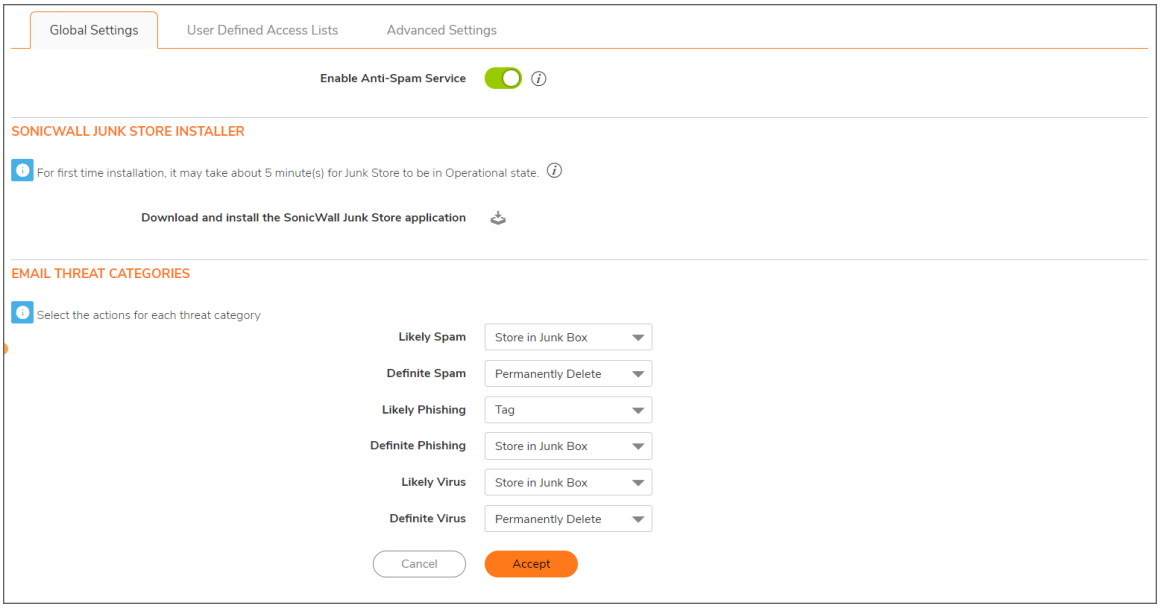
You can look at the **Status** page like an Anti-Spam service dashboard for quick access to your **Service Status** such as expiration and version, various **Threat Statistics**, services you have available, and an **E-mail Stream Diagnostics Capture** area to start and stop captures and the ability to download that data for later review.

The **Status** page is available at **POLICY | Anti-Spam > Status**.



3

# Settings




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

ⓘ | **NOTE:** For information about the Anti-Spam feature and how to license it, see About Anti-Spam.

## Topics:

- Activating Anti-Spam
- Installing the Junk Store
- Configuring Email Threat Categories
- Configuring Access Lists
- Configuring Advanced Options

# Activating Anti-Spam

After you have registered Anti-Spam, activate it to start your appliance-level protection from spam, phishing, and virus messages.

***To activate Anti-Spam:***

1. Navigate to **POLICY | Anti-Spam > Settings**.
2. In the **Global Settings** tab, click **Enable Anti-Spam Service** to activate the Anti-Spam feature. A message displays describing the effects of enabling the Anti-Spam Service and requesting agreement to proceed.

   Enabling the SonicWall Anti-Spam Service will:

   - Disable RBL Filter and override its settings. The SonicWall GRID System provides enhanced IP reputation checks.
   - Enable GAV (if separately licensed and not yet enabled)
   - Create and activate system-generated NAT policies and firewall access rules.
   - Deactivate custom user NAT and rule policies for an existing mail server.

   By Clicking the **Proceed** in the confirmation alert, you agree to be bound by the terms and conditions of the agreement located at this link: EULA. By clicking **Proceed** in the confirmation alert, you agree to be bound by the terms and conditions of the agreement located at this link: EULA.
3. To proceed, click **Proceed**. Another message about the mail server to be used displays.
4. Click **Next**. A dialog requesting information about the server displays. The dialog's settings are populated with information taken from the system.
5. Optionally, change the information.
6. Click **Next**. A message displays explaining what is created during the installation.
7. Click **Confirm**.

When the Anti-Spam application is installed, 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.

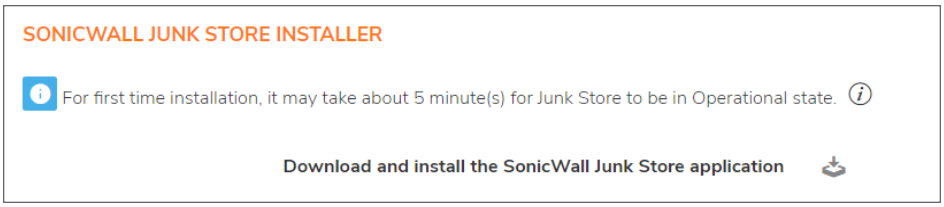
**NOTE:** While SonicWall supports non-Exchange SMTP servers, such as Sendmail and Lotus Domino, it is not required to install the Junk Store on one of these servers. Similar to the SonicWall Email Security product, the CASS 2.0 feature allows you to install the Junk Store on a stand-alone server.
To fully utilize the newest functionality available with CASS 2.0, SonicWall recommends installing Junk Store on a stand-alone server.

***To install the Junk Store:***

1. Log in to your Exchange system.
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 SonicOS interface.
4. Navigate to the **POLICY | Anti-Spam > Settings** 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.

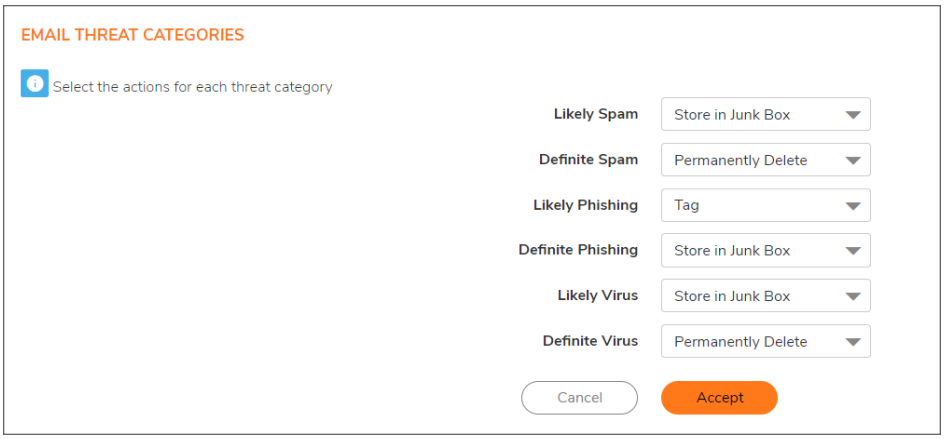
   **NOTE:** The first time the Junk Store application is installed, it takes about 5 - 15 minutes for the Junk Store to be operational.
7. If your browser warns you that the Web site is trying to load the SonicWall Email Security add-on:
   a. Click in the Information Bar.
   b. Select **Install ActiveX Control** in the pop-up menu. The **Security Warning Screen** displays.
8. Click **Install** to install the ActiveX Control.
9. On the **POLICY | Anti-Spam > Settings** 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.
11. Migrating data to the Junk Store may take a long time to complete.
12. Navigate to the **POLICY | Anti-Spam > Status** page and verify that the SonicWall Junk Store is Operational.

# Configuring Email Threat Categories

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

***To set default settings for users' messages:***

1. On the **POLICY | Anti-Spam > Settings** page, scroll to the **Email Threat Categories** section.




2. 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. |

| Category | Action |
| --- | --- |
| **Tag With [TAG]** | The email is tagged with a term in the subject line:<br>• [LIKELY_SPAM]<br>• [SPAM]<br>• [LIKELY_PHISHING]<br>• [PHISHING]<br>• [LIKELY_VIRUS]<br>• [VIRUS]<br>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. |
| **Permanently Delete** | The email message is permanently deleted.<br>**CAUTION: If you select this option, your organization risks losing wanted email.** |

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

3. Click **Accept**.

# 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.

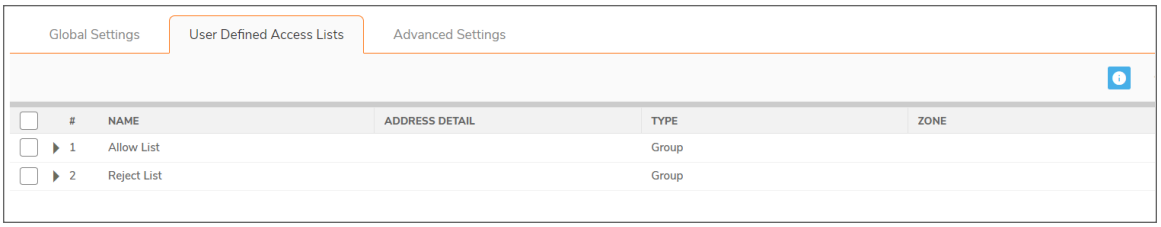
### Topics:

- Configuring User-defined Access Lists
- Adding a Host to the Access Lists

# Configuring User-defined Access Lists

***To configure the user-defined access lists:***

1. On the **POLICY | Anti-Spam > Settings** page, click the **User-defined Access Lists** tab.




2. Click the **Edit** icon for the list, **Allow Client List** or **Reject Client List**, you want to configure. The **Allow/Reject Client List** dialog displays.
3. Select items from the **Not In Group** column you want to add to the **In Group** column.
4. Click the **Right Arrow**.

   To remove items from the **In Group** column:

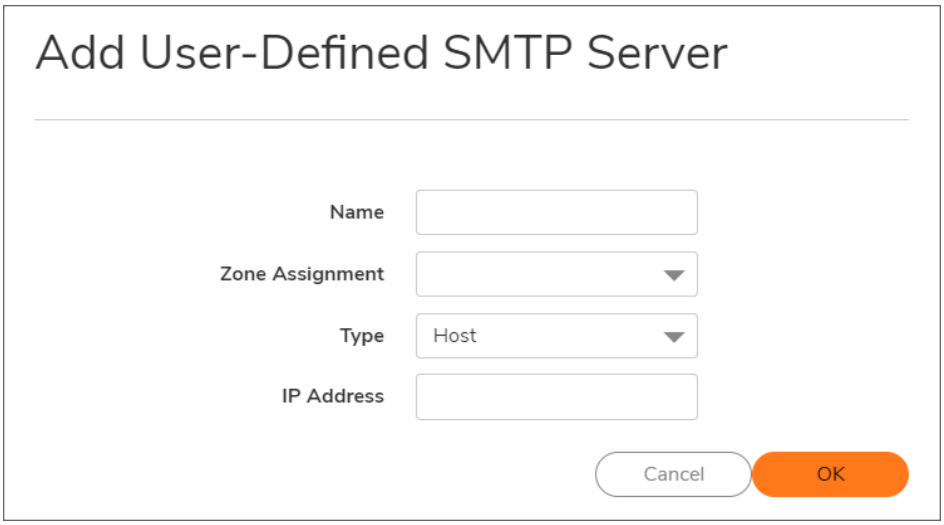
   a. Select the item(s) from the **In Group** column.

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

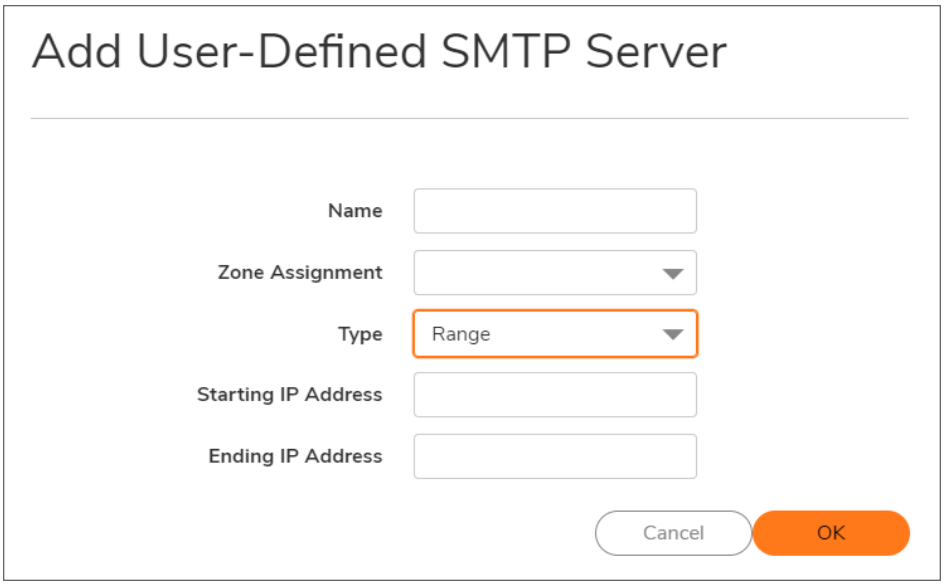
# Adding a Host to the Access Lists

***To add a host to the lists:***

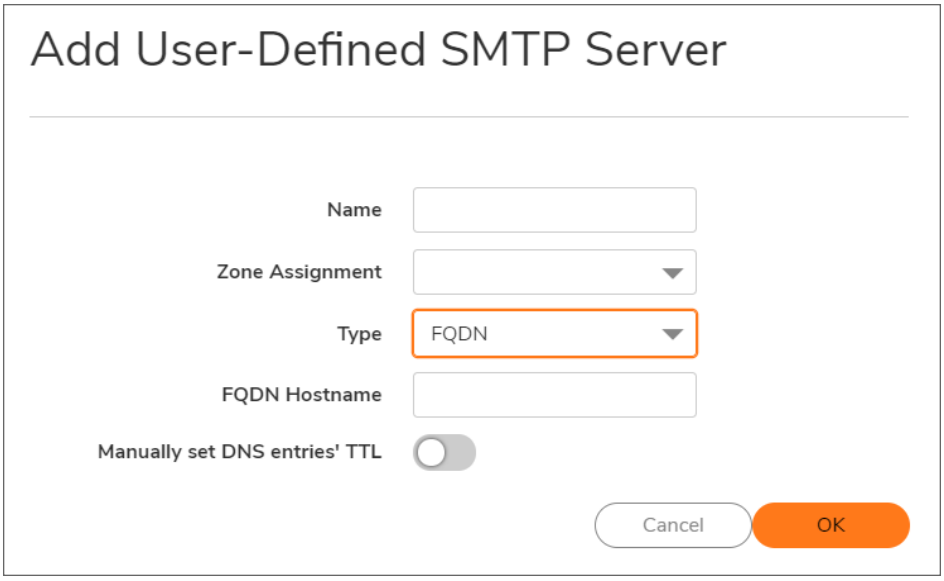
1. Scroll to the **User-defined Access Lists** section.
2. Click the **+** icon. The **Add User-defined SMTP Server** dialog displays.




3. Enter a name for the host in the **Name** field.
4. Select the type of host from the **Type** drop-down menu. The following setting(s) change, depending on the host type selected.
5. 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.

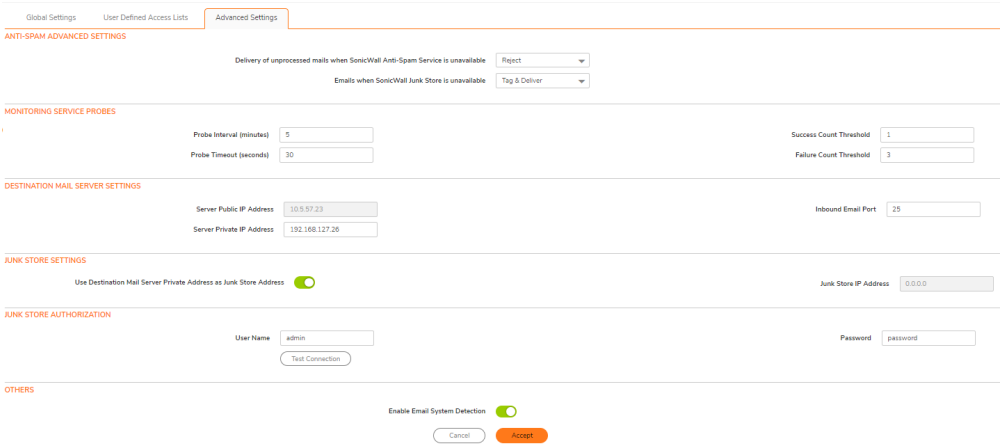


- **FQDN** – enter the FQDN hostname in the **FQDN Hostname** field.




6. Click **OK**.

# Configuring Advanced Settings




On the **Advanced Settings** tab, you can set the email options described in **POLICY | Anti-Spam > Settings**.

## ANTI-SPAM > SETTINGS | ADVANCED SETTINGS

| 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.<br><br>Choose from the drop-down menu:<br><br>• **Allow** (default)<br>• **Reject** |
| | **Tag and Deliver/Delete 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]`<br><br>`Please renew your account.`<br><br>Choose from the drop-down menu:<br><br>• **Tag & Deliver** (default)<br>• **Delete** |
| **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. |

| Setting Type | Setting | Description |
|---|---|---|
| **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.<br><br>***To change the address:***<br>1. Uncheck the checkbox. The **Junk Store IP Address** field becomes available.<br>2. Enter the Junk Store IP address of where the server is located. |
| **Junk Store Authorization** | **User Name and Password** | Enter the user name and password to access Junk Store on port 10443. |
| **Others** | **Enable Email Subsystem Detection** | Enables discover of available email system resources in the network. This checkbox is selected by default. |

4

# Relay Domains

The **POLICY | Anti-Spam > Relay Domains** page allows you to list domains authorized for relaying email by CASS. Restricting domains that can relay emails avoids open-relay issues.

**Topics:**

- About Open Relay
- Listing Allowed Relay Domains

## About Open Relay

An open relay is a SMTP server configured in such a way that it allows a third party to relay (send/receive email messages) that are neither from nor for local users. Such servers, therefore, are usually targets for spammers.

When CASS is configured as an open relay, the mail is relayed even if the mail is not destined to the recipient domain. When CASS is not configured as an open relay, it relays the emails that have one of the listed recipient domains; for domains not listed, the mails are rejected. Listing allowed relay domains avoid unnecessary relaying of emails even when mails are not destined to the user.

# Listing Allowed Relay Domains

You can list all domains used for relay.

***To list an authorized relay domain:***

1. Navigate to **POLICY | Anti-Spam > Relay Domains**.
2. Scroll to the **Settings** section.

3. Select whether to restrict relay domains:
   - **Any source IP address is allowed to connect to this path**: Allows any domain to relay messages. Go to Step 5.

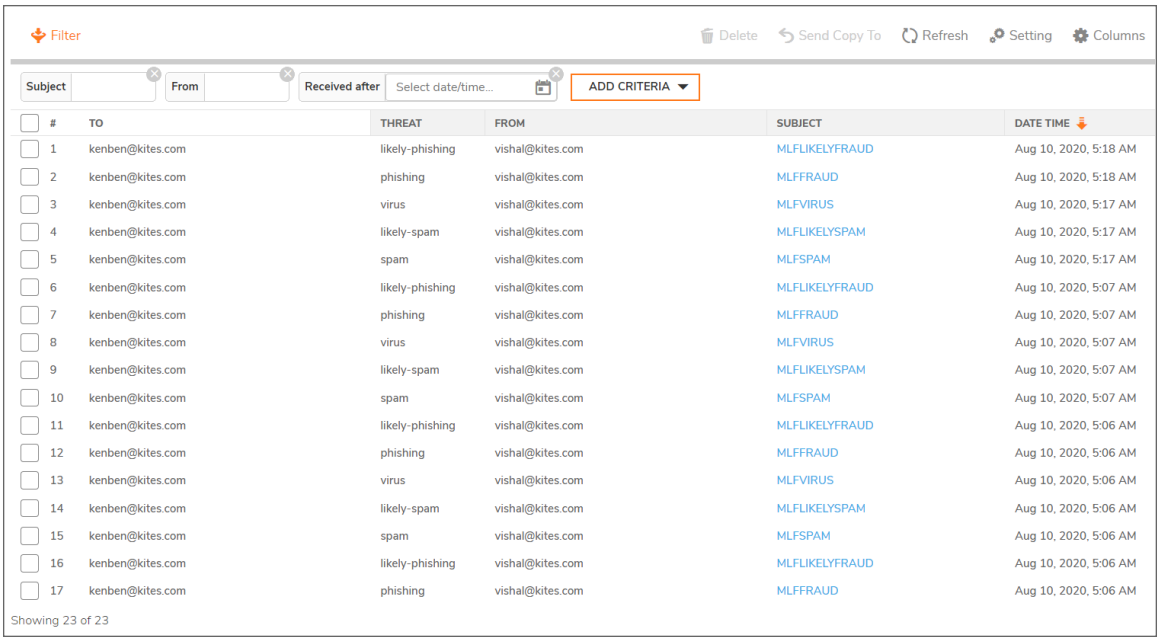
     **CAUTION: Selecting this option may make a CASS open relay. Even if the mail is not destined to the recipient's domain, the mail is relayed, which could result in spamming.**
   - **Any source IP address is allowed to connect to this path, but relaying is allowed only for emails sent to one of these domains**: Allows only listed domains to relay messages.
4. Enter the domain(s) allowed to relay messages in the field. Separate domains with a carriage return (<CR>).
5. Click **Accept**.

5

# Junk Box Messages

On the **POLICY | Anti-Spam > Junkbox Messages** page, you can view, search, and manage all email messages that are currently in the Junk Store on the Exchange or SMTP server.

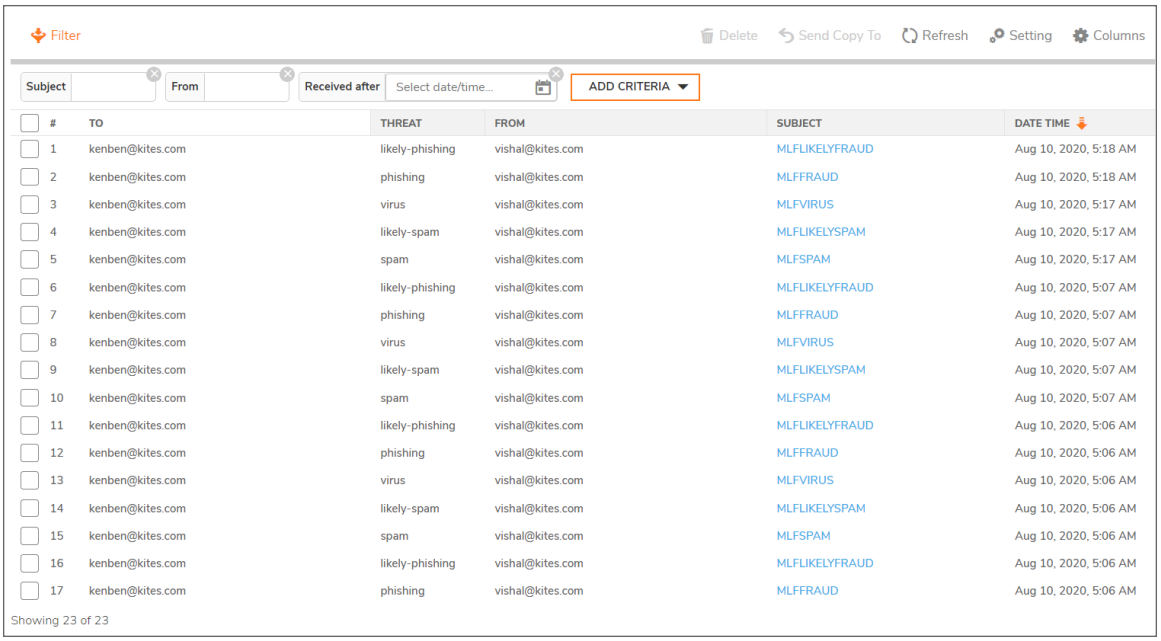
ⓘ | **NOTE:** This page is only available if the Junk Store is installed.




| # | TO | THREAT | FROM | SUBJECT | DATE TIME |
|---|---|---|---|---|---|
| 1 | kenben@kites.com | likely-phishing | vishal@kites.com | MLFLIKELYFRAUD | Aug 10, 2020, 5:18 AM |
| 2 | kenben@kites.com | phishing | vishal@kites.com | MLFFRAUD | Aug 10, 2020, 5:18 AM |
| 3 | kenben@kites.com | virus | vishal@kites.com | MLFVIRUS | Aug 10, 2020, 5:17 AM |
| 4 | kenben@kites.com | likely-spam | vishal@kites.com | MLFLIKELYSPAM | Aug 10, 2020, 5:17 AM |
| 5 | kenben@kites.com | spam | vishal@kites.com | MLFSPAM | Aug 10, 2020, 5:17 AM |
| 6 | kenben@kites.com | likely-phishing | vishal@kites.com | MLFLIKELYFRAUD | Aug 10, 2020, 5:07 AM |
| 7 | kenben@kites.com | phishing | vishal@kites.com | MLFFRAUD | Aug 10, 2020, 5:07 AM |
| 8 | kenben@kites.com | virus | vishal@kites.com | MLFVIRUS | Aug 10, 2020, 5:07 AM |
| 9 | kenben@kites.com | likely-spam | vishal@kites.com | MLFLIKELYSPAM | Aug 10, 2020, 5:07 AM |
| 10 | kenben@kites.com | spam | vishal@kites.com | MLFSPAM | Aug 10, 2020, 5:07 AM |
| 11 | kenben@kites.com | likely-phishing | vishal@kites.com | MLFLIKELYFRAUD | Aug 10, 2020, 5:06 AM |
| 12 | kenben@kites.com | phishing | vishal@kites.com | MLFFRAUD | Aug 10, 2020, 5:06 AM |
| 13 | kenben@kites.com | virus | vishal@kites.com | MLFVIRUS | Aug 10, 2020, 5:06 AM |
| 14 | kenben@kites.com | likely-spam | vishal@kites.com | MLFLIKELYSPAM | Aug 10, 2020, 5:06 AM |
| 15 | kenben@kites.com | spam | vishal@kites.com | MLFSPAM | Aug 10, 2020, 5:06 AM |
| 16 | kenben@kites.com | likely-phishing | vishal@kites.com | MLFLIKELYFRAUD | Aug 10, 2020, 5:06 AM |
| 17 | kenben@kites.com | phishing | vishal@kites.com | MLFFRAUD | Aug 10, 2020, 5:06 AM |

# Information Displayed in the Junk Box Messages Table

The Junk Box Messages table displays information and filtering possibilities for quarantined messages.




| # | TO | THREAT | FROM | SUBJECT | DATE TIME |
|---|---|---|---|---|---|
| 1 | kenben@kites.com | likely-phishing | vishal@kites.com | MLFLIKELYFRAUD | Aug 10, 2020, 5:18 AM |
| 2 | kenben@kites.com | phishing | vishal@kites.com | MLFFRAUD | Aug 10, 2020, 5:18 AM |
| 3 | kenben@kites.com | virus | vishal@kites.com | MLFVIRUS | Aug 10, 2020, 5:17 AM |
| 4 | kenben@kites.com | likely-spam | vishal@kites.com | MLFLIKELYSPAM | Aug 10, 2020, 5:17 AM |
| 5 | kenben@kites.com | spam | vishal@kites.com | MLFSPAM | Aug 10, 2020, 5:17 AM |
| 6 | kenben@kites.com | likely-phishing | vishal@kites.com | MLFLIKELYFRAUD | Aug 10, 2020, 5:07 AM |
| 7 | kenben@kites.com | phishing | vishal@kites.com | MLFFRAUD | Aug 10, 2020, 5:07 AM |
| 8 | kenben@kites.com | virus | vishal@kites.com | MLFVIRUS | Aug 10, 2020, 5:07 AM |
| 9 | kenben@kites.com | likely-spam | vishal@kites.com | MLFLIKELYSPAM | Aug 10, 2020, 5:07 AM |
| 10 | kenben@kites.com | spam | vishal@kites.com | MLFSPAM | Aug 10, 2020, 5:07 AM |
| 11 | kenben@kites.com | likely-phishing | vishal@kites.com | MLFLIKELYFRAUD | Aug 10, 2020, 5:06 AM |
| 12 | kenben@kites.com | phishing | vishal@kites.com | MLFFRAUD | Aug 10, 2020, 5:06 AM |
| 13 | kenben@kites.com | virus | vishal@kites.com | MLFVIRUS | Aug 10, 2020, 5:06 AM |
| 14 | kenben@kites.com | likely-spam | vishal@kites.com | MLFLIKELYSPAM | Aug 10, 2020, 5:06 AM |
| 15 | kenben@kites.com | spam | vishal@kites.com | MLFSPAM | Aug 10, 2020, 5:06 AM |
| 16 | kenben@kites.com | likely-phishing | vishal@kites.com | MLFLIKELYFRAUD | Aug 10, 2020, 5:06 AM |
| 17 | kenben@kites.com | phishing | vishal@kites.com | MLFFRAUD | Aug 10, 2020, 5:06 AM |

## INFORMATION ABOUT QUARANTINED MESSAGES

| This column | Contains or indicates |
|---|---|
| Checkbox icon | Checkbox for each item in the table. Clicking the Checkbox icon in the heading selects all items in the table. |
| **To** | Recipient's email address. |
| **Threat** | Type of threat the email poses; for more information about threat categories, see Email Threat Category Settings: Options in Configuring Email Threat Categories. |
| **From** | Sender's email address. |
| **Subject** | Subject line of the email. |
| **Date Time** | Date and time the email was sent. |

Use the buttons at the top of the **Junk Box Messages** table to perform the following Junk Store management tasks (see Junk Box Messages Table Buttons) on the **POLICY | Anti-Spam > Junk Box Messages** page:

### JUNK BOX MESSAGES TABLE BUTTONS

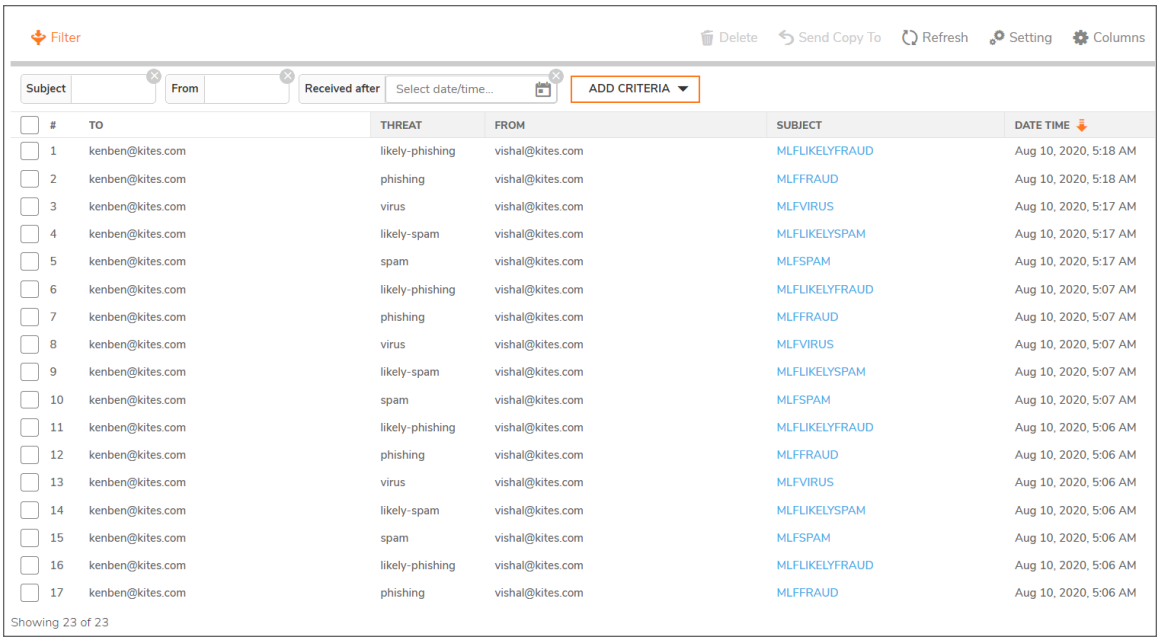
| Button | Function |
|---|---|
| **Filter** | Opens sorting and filtering features that can help narrow down Junk Box results using Column criteria |
| **Delete** | Permanently delete the selected message(s) from the Junk Store; to delete all messages click the checkbox in the table heading |
| **Send Copy To** | Keep the selected message(s) in the Junk Store and send a copy of it (them) to a user. |
| **Refresh** | Refreshes all data. |
| **Settings** | Opens the **General** and **Action Settings** located at Junk Box Settings. |
| **Columns** | Click headings to add or subtract Column data. |

# Managing Junk Box Messages

You can Filter, Delete, or send a copy of Junk Store messages.

***To manage the Junk Store:***

1. On the **POLICY | Anti-Spam > Junk Box Messages** page, scroll to the Junk Box Messages table.




| # | TO | THREAT | FROM | SUBJECT | DATE TIME |
|---|---|---|---|---|---|
| 1 | kenben@kites.com | likely-phishing | vishal@kites.com | MLFLIKELYFRAUD | Aug 10, 2020, 5:18 AM |
| 2 | kenben@kites.com | phishing | vishal@kites.com | MLFFRAUD | Aug 10, 2020, 5:18 AM |
| 3 | kenben@kites.com | virus | vishal@kites.com | MLFVIRUS | Aug 10, 2020, 5:17 AM |
| 4 | kenben@kites.com | likely-spam | vishal@kites.com | MLFLIKELYSPAM | Aug 10, 2020, 5:17 AM |
| 5 | kenben@kites.com | spam | vishal@kites.com | MLFSPAM | Aug 10, 2020, 5:17 AM |
| 6 | kenben@kites.com | likely-phishing | vishal@kites.com | MLFLIKELYFRAUD | Aug 10, 2020, 5:07 AM |
| 7 | kenben@kites.com | phishing | vishal@kites.com | MLFFRAUD | Aug 10, 2020, 5:07 AM |
| 8 | kenben@kites.com | virus | vishal@kites.com | MLFVIRUS | Aug 10, 2020, 5:07 AM |
| 9 | kenben@kites.com | likely-spam | vishal@kites.com | MLFLIKELYSPAM | Aug 10, 2020, 5:07 AM |
| 10 | kenben@kites.com | spam | vishal@kites.com | MLFSPAM | Aug 10, 2020, 5:07 AM |
| 11 | kenben@kites.com | likely-phishing | vishal@kites.com | MLFLIKELYFRAUD | Aug 10, 2020, 5:06 AM |
| 12 | kenben@kites.com | phishing | vishal@kites.com | MLFFRAUD | Aug 10, 2020, 5:06 AM |
| 13 | kenben@kites.com | virus | vishal@kites.com | MLFVIRUS | Aug 10, 2020, 5:06 AM |
| 14 | kenben@kites.com | likely-spam | vishal@kites.com | MLFLIKELYSPAM | Aug 10, 2020, 5:06 AM |
| 15 | kenben@kites.com | spam | vishal@kites.com | MLFSPAM | Aug 10, 2020, 5:06 AM |
| 16 | kenben@kites.com | likely-phishing | vishal@kites.com | MLFLIKELYFRAUD | Aug 10, 2020, 5:06 AM |
| 17 | kenben@kites.com | phishing | vishal@kites.com | MLFFRAUD | Aug 10, 2020, 5:06 AM |

2. Select the checkbox for the message(s) that you want to manage.

   ⓘ | **TIP:** To select all messages, select the checkbox in the table header. All checkboxes are selected.

3. Perform the management task(s):
    - To permanently delete the selected messages from the Junk Store, click **Delete**.

      ⓘ | **NOTE:** Messages are deleted automatically after 30 days.

      The selected messages are deleted immediately — there is no confirmation dialog before the deletion. If the deletion is successful, a green notification is displayed at the top of the page. If the deletion fails, the notification is red.

      The selected messages are unjunked and sent immediately — there is no confirmation dialog before the action. If the action is successful, a green notification is displayed at the top of the page. If the action fails, the notification is red.
    - To send a copy of the selected messages to a user, click the **Send Copy To** button. The **Send Copy To** dialog displays.

    a. Do one of the following:
        - Select **Send a copy to original recipient**.
        - Type the email address into the **Recipient email address** field.

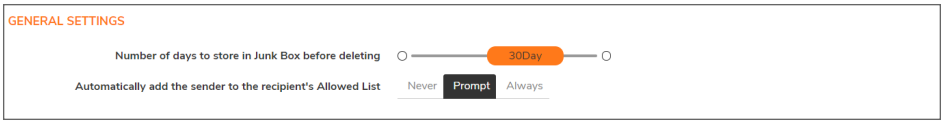
    b. Click **Send**.
4. The selected message is sent immediately — there is no confirmation dialog before the action. If the action is successful, a green notification is displayed at the top of the page. If the action fails, the notification is red.

6

# Junk Box Settings

The **POLICY | Anti-Spam > Junkbox Settings** page allows you to set the:

- Length of time that messages are stored in the Junk Box before being deleted.
- Number of Junk Box messages to be displayed per page.
- Action performed when a user unjunks a message.




***To perform message management:***

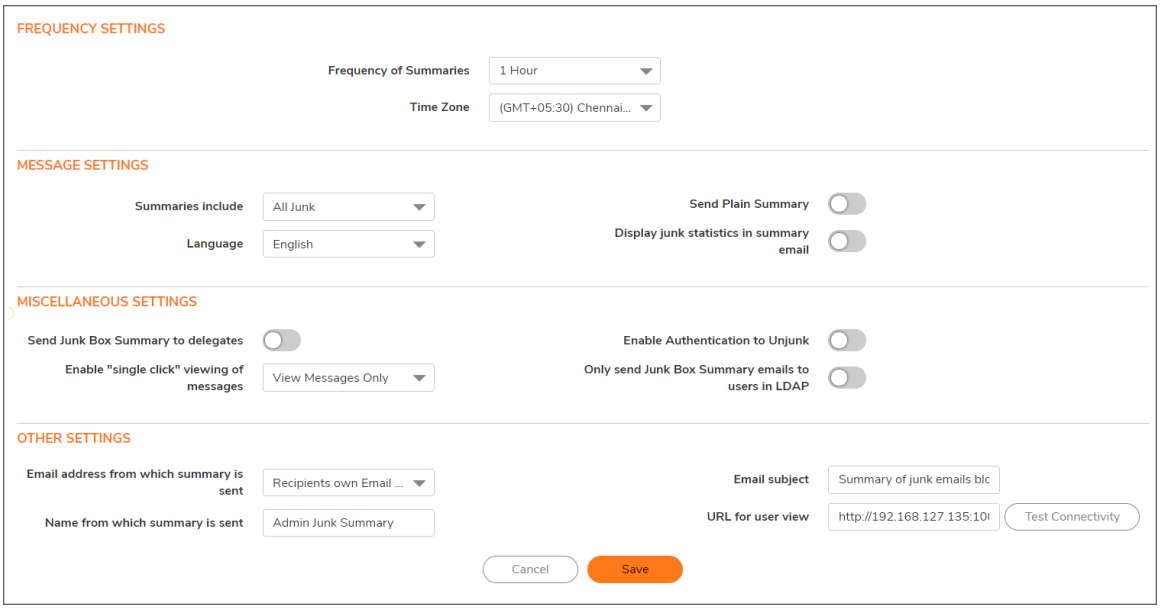
1. In the **General Settings** section, use the slider to select the number of days to retain junk mails before deleting them from the **Number of days to store in Junk Box before deleting** drop-down menu. The minimum is 1 Day, the maximum is 180 Days, and the default is 15 Days.
2. Select the frequency to **Automatically add the sender to the recipient's Allowed List.** The **Prompt** option is selected by default:
   - Never
   - Prompt
   - Always
3. Click **Save**.

7

# Junk Box Summary

The Junk Store sends an email message to users listing all the messages placed in their Junk Summary. The **POLICY | Anti-Spam > Junk Box Summary** page allows you to set up the Junk Summary for users.

To configure the types of messages that are logged, navigate to the **POLICY | Anti-Spam > Advanced** page.




The **POLICY | Anti-Spam > Junk Box Summary** page allows you to set these options:

- **Frequency Settings** – Set the frequency and time Junk Box summaries are sent to you.
- **Message Settings** – Configure what is included in the summary, the language, and whether the summary contains graphics.
- **Miscellaneous Settings** – Set options such as single-click viewing of messages and authentication.
- **Other Settings** – Set options such as sender of summary, email subject, and URL for users.

## Topics:

- Managing the Junk Box Summary

# Managing the Junk Box Summary

***To manage the Junk Box Summary:***

1. In the **Frequency Settings** section of the **Junk Box Summary** Setings page, select how often summaries are sent to you from the **Frequency of Summaries** drop-down menu.

   Minimum frequency is **14 Days**, maximum is **1 Hour**, the default is **1 Day**. To prevent summaries from being sent to you, select **Never**.
2. Select from the **Time Zone** you would like your users to receive email notifications. From the **Time Zone** drop-down menu, select the Greenwich Mean Time (GMT) to be used in determining the frequency.
3. If you selected **Weekly** or **Bi-Weekly** from the **Frequency of Summaries** drop-down menu, the **Time of day to send summary** and **Day of week to send summary** options become available. To customize the date your users receive email notifications select either:
   - **Any Time**
   - **Specific Hour**
4. **Day of Week to send summary on** – select aday of the week from the drop-down menu.
   - **Any Day**
   - **Specific Day** (choose the day).
5. In the **Message Settings** section, select what to include in the message summary from the **Summaries include** options:
   - **All Junk** (default)
   - **Likely Junk** (hide definite junk)
6. Select a language for the emails from the **Language** of summary emails drop-down menu.
7. For **Send Plain Summary**, enable whether the summary can contain graphics.
8. For **Display junk statistics in summary email**. enable to include junk statistics.
9. In the **Miscellaneous Settings** section, enable **Send Junk Box Summary to delegates** to send summary emails to assigned proxies.
10. Choose how email junk box summary notifications are viewed from the **Enable "single click" view of messages** options:
    - **OFF**
    - **View Messages Only** (user can preview messages without having to type their username/passwords.) (default)
    - **Full Access** (clicking any link in a Junk Box Summary grants full access to the particular user's settings)
11. To allow your users to authenticate to unjunk email messages, select the **Enable Authentication to Unjunk** checkbox. This option is not selected by default.

12. To limit junk box summaries notifications to users in LDAP, select the **Only send Junk Box Summary emails to users in LDAP** checkbox.
13. In the **Other Settings** section, choose how the summary is to be sent by selecting an option from **Email address from which summary is sent**:
    - **Send summary from recipient's own email address** (default)
    - **Send summary from this email address**: Enter an email address in the field
14. In the **Name from which summary is sent** field, enter the name to be displayed in the user's email for the summary emails. The default name is **Admin Junk Summary**.
15. In the **Email subject** field, enter the subject line for the Junk Box Summary email. The default is **Summary of junk emails blocked**.
16. The **URL for user view** field is filled in automatically based on your server configuration. It is the basis for all the links in the Junk Box Summary email. If this setting is configured, each user Junk Box Summary emails listing that user's received email threats are sent.

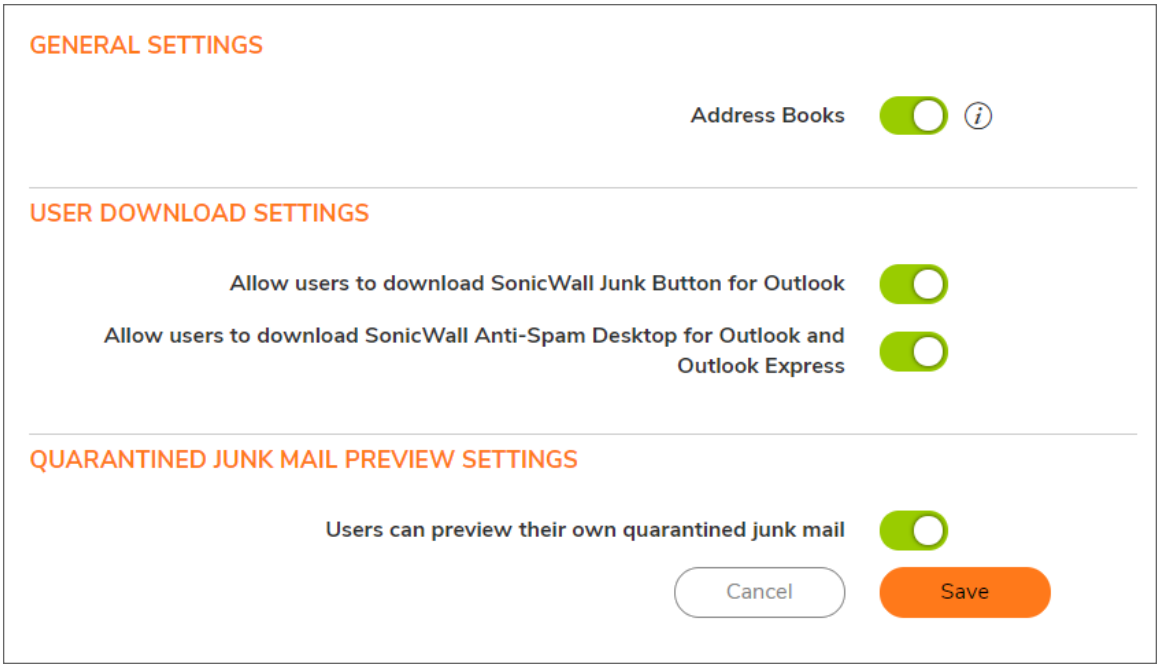
    Junk Box Summary emails contain URLs to:
    - View quarantined emails.
    - Unjunk quarantined emails; users unjunk items in the Junk Box summary email by clicking links in the email.
    - Log in to the Junk Box.

    ⓘ **IMPORTANT:** If you change this URL, to ensure connectivity, test the link if you make any changes by clicking **Test Connectivity** . If the test fails, ensure the URL is correct.
17. Click **Save**.

8

# User View Setup

The **POLICY | Anti-Spam > User View Setup** page allows you to select and configure which settings are visible for users.




**Topics:**

- Configuring User View Setup

## Configuring User View Setup

ⓘ | **NOTE:** Selected options appear in a user's navigation toolbar.

***To configure what the user sees:***

1. In the **General Settings** section, to allow users to see their own Address Book (people, companies, and lists) in the navigation toolbar, enable **Address Books**. This option is enabled by default.
2. In the **User Download Settings** section, to allow Outlook users to download the Junk Button, select **Allow Users to download SonicWall Junk Button for Outlook**. This option is selected by default.
3. To allow Outlook and Outlook Express users to download the Anti-Spam Desktop, select the **Allow users to download SonicWall Anti-Spam Desktop for Outlook and Outlook Express** checkbox. This option is selected by default.
4. In the **Quarantined Junk Mail Preview Settings** section, to allow users to preview their quarantined junk mail, select the **Users can preview their own quarantined junk mail** checkbox. This option is selected by default.
5. After you have made all of the necessary changes, click **Save**.

9

# Address Books

The **POLICY | Anti-Spam > Address Books** page allows you to configure the **Allowed** and **Blocked** lists for your organization. The lists are a combination of allowed and blocked senders from the organization's lists and lists provided by the firewall.

The **Blocked** view only filters addresses by people, IPs, and companies, while the **Allowed** view filters addresses by people, companies, IPs, and lists.

If your lists are long, you can use a **Search** function to display only desired table entries.

**Topics:**


- About the Tabs
- Adding Items to the Allowed or Blocked List
- Deleting Items from the Allowed or Blocked List
- Importing Address Book Entries
- Exporting Address Book Entries
- Searching the Allowed and Blocked Lists


## About the Tabs

The two tabs, **Allowed** and **Blocked**, are identical except the search categories for both pages are People, Companies, and IPs while the **Allowed** page also has **Lists**.

**Topics:**


- Allowed Lists
- Blocked Lists


## Allowed Lists

The **Allowed** view enables you to permit people, companies, IP addresses, or lists to send mail to your organization. You can import address books to the **Allowed** list and export the Corporate Address Book to an

Excel spreadsheet or text file.

## Blocked Lists

ⓘ **NOTE:** Senders added to the Corporate Blocked List by an Administrator are blocked automatically for all users and can only be deleted by an Administrator.

The **Blocked** view allows you to restrict people, companies, and IP addresses from sending mail to your organization. You can import address books to the Blocked list and export the Corporate Address Book to an Excel spreadsheet or text file.

# Adding Items to the Allowed or Blocked List

***To add an item to the Corporate Allowed/Blocked List:***

1. Navigate to the appropriate view on **POLICY | Anti-Spam > Address Books**.
2. Click **Add**. The **Add Items Allowed List** dialog displays.
3. Select the type of list user from the **Select list type** drop-down menu:
   - **People**
   - **Companies**
   - **Lists** (available only for the **Allowed** view)
   - **IPs**
4. Enter the address(es)/domain(s) in the field. Depending on the list type selected, the field name changes:
   - **People** – Enter IP Addresses separated by a carriage return
   - **Companies** – Enter the domains separated by a carriage return
   - **Lists** – Enter the mailing lists separated by a carriage return
   - **IPs** – Enter IP Addresses separated by a carriage return

Click **Add** to finish. The address(es)/domain(s) are added to the **List** on the **Allowed/Blocked** view.

# Deleting Items from the Allowed or Blocked List

***To delete a sender from the Corporate Allowed/Blocked List:***

1. Click the appropriate view.
2. Select the checkbox next to the email address(es) you wish to delete. **Delete** becomes active.

3. Click **Delete**. A success message appears confirming the deletion.
   ⓘ | **TIP:** To delete all entries, click the checkbox in the table header.

# Importing Address Book Entries

You can import entries from one or more address books.

***To import address book entries:***

1. Navigate to **POLICY | Anti-Spam > Address Books**.
2. Click the appropriate view.
3. Click **Import**. The **Import Address Book** dialog displays.
4. Click **Browse**. The **Windows File Upload** dialog displays.
5. Select the file to upload. It must be in this format:
   `<TAB>D/L/E/I<TAB>A/B<TAB>Address List<CR>`
   where:
   - `D/L/E/I` – Domain/List/Email/IP Address
   - `A/B` – Allowed/Blocked
   - Address List – Address book entries separated by commas and email addresses, domains, IP addresses, and lists are separated with a carriage return.

   For example:

   ```
   <TAB>E<TAB>A<TAB>email1@company.com,email2@company.com<CR>
   <TAB>L<TAB>B<TAB>list1@company.com,list2@company.com<CR>
   ```

6. Click **Open**.
7. Click **Import**.

# Exporting Address Book Entries

You can export entries to an Excel spreadsheet or text file.

***To export address book entries:***

1. On the appropriate view, click **Export**. The **Windows Opening filename** dialog displays.
2. Select either:
   - **Open with Microsoft Excel** (default)
   - **Save file**
3. Click **OK**.

# Searching the Allowed and Blocked Lists

A search field is available to quickly find Allowed and Blocked entries in the **Allowed** and **Blocked** tables. You can access this field from either the **Allowed** view or the **Blocked** view.

***To search the Allowed or Blocked lists:***

1. Click the appropriate view.
2. Go to the **Search** section.
3. Enter an address or domain in the **Search** field. Enter multiple entries separated by a comma.
4. Optionally, you can filter the search between the **Type** of addresses (**People**, **Companies**, **IPs**, or **Lists** [Allowed list only]) by selecting the checkboxes below the search bar; by default, all are selected.
5. Click the **Go** button to begin the search. The results are shown in the **List** table.

***To clear the search field:***

1. Click **Reset**.

10

# Manage Users

The **POLICY | Anti-Spam > Manage Users** page allows you to add, remove, and manage all users, on both the Global and LDAP servers. For more information regarding LDAP configuration, refer to Managing Users.

The **User** table displays this information:

| Column | Description |
|---|---|
| **Name** | User's user name, which may not be part of the primary email address. |
| **Primary Email** | Email address of the user. |
| **Message Management** | Displays whether the user adheres to the settings on the **POLICY \| Anti-Spam > Junk Box Summary** page or has modified them:<br>• **Default** – All administrator's settings are used<br>• **Custom** – User has changed one or more settings |
| **Role** | Is always **User** as user right cannot be modified in CASS. |
| **Source** | Displays the user's server name. |

**Topics:**


- Updating the User Table
- Enabling Non-LDAP User Authentication
- Viewing Users
- Adding Users
- Signing In as a User


# Updating the User Table

***To update the list of users in the User Table:***

1. Navigate to the **Users** section of **POLICY | Anti-Spam > Manage Users**.
2. Click **Refresh Users**.

# Enabling Non-LDAP User Authentication

Authentication for non-LDAP users must be enabled.

***To enable authentication for non-LDAP users:***

1. Scroll to the **User View Setup** section of **POLICY | Anti-Spam > Manage Users**.
2. Select **Enable authentication for non ldap users**. A cautionary message displays.
3. Click **OK**.

# Viewing Users

The **User Table** displays all the users who can log in. You can filter the users to only those you want to see at the moment by:

- Selecting user type: Selecting the Type of User to View
- Specifying a particular user; see Finding a User

# Selecting the Type and Sever of User to View

You can see all users, only LDAP users, or only non-LDAP users.

***To select the type of user to display:***

1. Scroll to the Find All users in column section of **POLICY | Anti-Spam > Manage Users**.
2. Select which type of user:
    - From the **Using Source** drop-down menu, select which server, or source, to view:
        - **Cloud**(default): A cloud LDAP server is added.
        - **GLOBAL** : A Global server is always available.
        - **LDAP server name**: If one or more LDAP servers have been added, all server names are listed.
    - **Only LDAP**: Select **Show LDAP entries**; this is the default if your system has only LDAP users.
    - **Only non-LDAP**: Select **Show non-LDAP entries**; this is the default if your system has only non-LDAP users.
    - **Both LDAP and non-LDAP**: Select both checkboxes; this is the default if your system has both types of users.

# Selecting a Server's Users to View

You can limit the User table to display only those users from a particular server.

***To select a source (server):***

1. Go to the filter section of **User View Setup**.
2. Click **Go**.

# Finding a User

You can restrict the view to just one user.

***To find a user:***

1. Go to the filter section of the **User View Setup** section of **POLICY | Anti-Spam > Manage Users**.
2. From the **User name or Email address**, enter the user name or email address and click **Search**

***To restore the User table display:***

1. Remove the search criterion from the **User name or Email address** field.
2. Click **Search**.

# Adding Users

You can add users to the list of users who can log in:

- Manually; see Adding Users Manually to the User Table
- By importing them; see Importing Users to the User Table

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

# Adding Users Manually to the User Table

***To add a user to the Global or LDAP Server::***

1. Click **Add** above the **User Table**. The **Add User** dialog displays.
2. Enter the primary address of the user in the **Primary Address** field.

3. If the user is an LDAP user, enter the user's password in the **Password** and **Confirm Password** fields.
4. Select which server the user belongs to from the **Using Source** drop-down menu.
5. Optionally, enter any Alias(es) of the user in the **Aliases** field. Separate each entry with a carriage return (<CR>).
6. Click **Add** to finish adding a user.

# Importing Users to the User Table

***To import a list of users from a file:***

1. Click **Import** above the **User Table**. The **Import Users** dialog displays.
2. Select how the imported file is to be treated by selecting an **Import Mode**:
   - **Append** – Adds the users to the end of the file containing the list of approved users.
   - **Overwrite** – Replaces the existing users with the imported users.
3. Specify the server to be used as a source:
   - **Cloud**
   - **GLOBAL**
   - **LDAP server name**
4. Click **Select**. The **Windows File Upload** dialog displays.
5. Select the file to upload. It must be in this format, with a tab <TAB> delimiter between the primary address and the alias and a carriage return <CR> delimiter to separate entries:

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

   For example:

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

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

   ```
   primary_email2@company.com<TAB>alias1@company.com<CR>
   primary_email2@company.com<TAB>alias2@company.com<CR>
   ```
6. Click **Open**.
7. Click **Import**.

# Signing In as a User

You can sign in to a user's account to see their Email Security **POLICY | Anti-Spam Junkbox**.

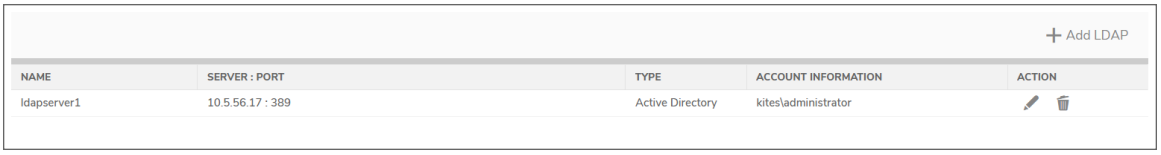
***To sign in as a user:***

1. Navigate to the User table of **POLICY | Anti-Spam > Manage User**.
2. Select the checkbox of the user you want to sign in as. The Sign in as User button becomes active.
3. Click **Sign in as User**. A separate window displays the **Email Security Anti-Spam > Junk Box Settings** page for that user.
4. To return to the **POLICY | Anti-Spam > Manage Users** page, click the **Logout** icon on the Email Security page.

11

# LDAP Configuration

The **POLICY | Anti-Spam > LDAP Configuration** page allows you to add and configure various settings specific to LDAP servers.




This section displays information about any LDAP Servers configured on the firewall:

- **Name** – Displays the friendly name of the server. Clicking the link displays the **Server Configuration**, **LDAP Query Panel**, and **Add LDAP Mappings** sections.
- **Server:Port** – Displays the IP address and port of the server.
- **Type** – Displays the type of server, such as Active Directory or OpenLDAP.
- **Account Information** – Displays active user name.
- **Action** – Contains **Edit** and **Delete** icons.

**Topics:**


- Adding an LDAP Server
- Configuring LDAP Queries
- Adding LDAP Mappings
- Editing an LDAP Server Configuration
- Deleting an LDAP Server

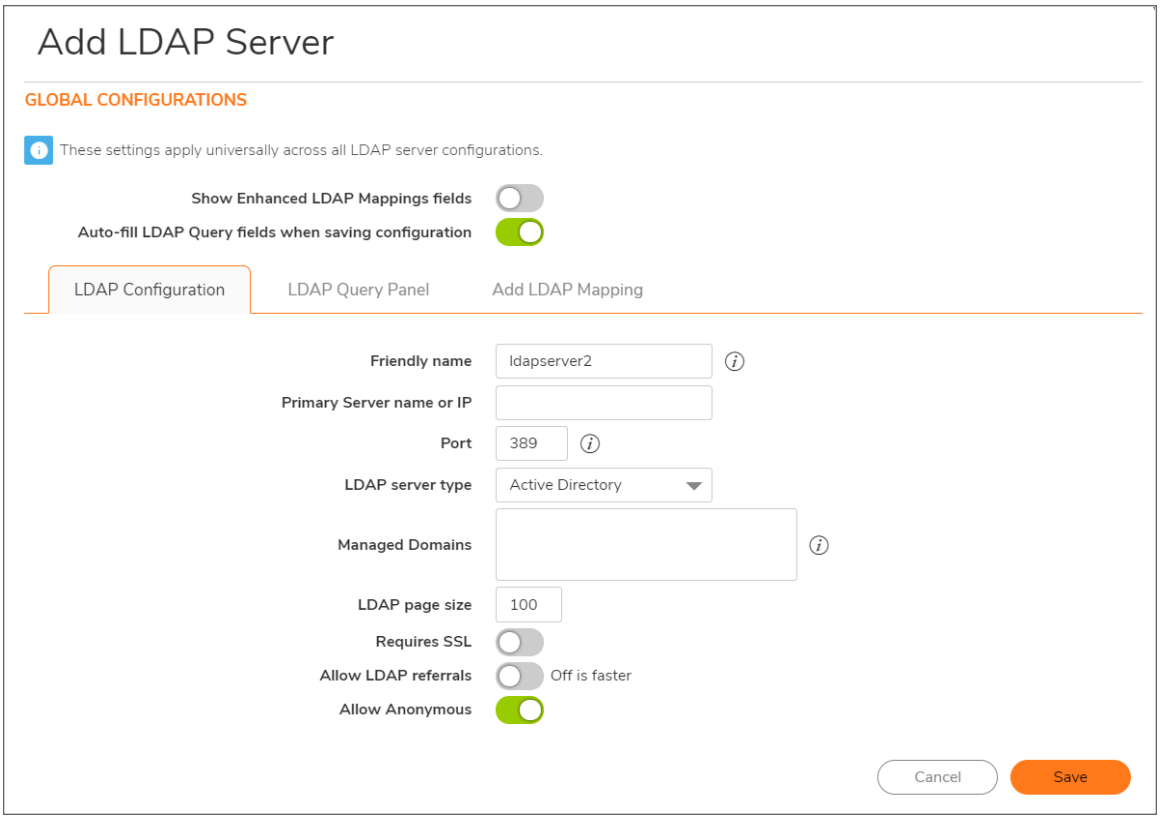

# Adding an LDAP Server

Configure a new LDAP server to enable per-user access and management.

**IMPORTANT:** Anti-Spam uses your existing Active Directory or LDAP server to authenticate end users as they log in to their personal Junk Boxes. The **POLICY | Anti-Spam > LDAP Configuration** 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 cannot log in to their personal junk boxes. Correctly filling out the LDAP configuration requires completing the **LDAP Configuration** tab, **LDAP Query Panel** tab, and the **Add LDAP Mapping** tab.

***To add an LDAP server:***

1. Navigate to **POLICY | Anti-Spam > LDAP Configuration**.
2. Click **+Add LDAP**. The **Add LDAP Server** dialog appears.




3. Optionally, on the **LDAP Configuration** tab, enable the **Show Enhanced LDAP Mappings fields** option. When this option is enabled, fields for a secondary server display.
4. To have the fields in the **LDAP Query Panel** completed automatically, ensure the **Auto-fill LDAP Query fields when saving configuration** option is enabled. This option is selected by default.
5. On the **LDAP Configuration** tab, configure the new LDAP server's settings:

   **TIP:** The primary and secondary names and IP addresses can be up to 200 alphanumeric characters including a hyphen (-) and period (.), but no spaces. Examples:
   192.168.4.100
   host-name123.com

- **Friendly Name**—Enter a friendly name for the LDAP server. The default name is ldapservern, where n is a sequential number.
- **Primary Server name or IP**—The server name or IP address of the LDAP Server.
- **Port**—The port number of the LDAP Server. The default port number is 389.
- **Secondary Server or IP**—The server name or IP address of the secondary LDAP Server.

  ⓘ **NOTE:** The Secondary Server name or IP address and Port number options, in red, display only if you selected Show Enhanced LDAP Mapping fields in the Settings section.
- **Secondary server port**—The port number of the secondary LDAP Server. The default port number is 389.
- **LDAP server type**—Select from the drop-down menu:
  - **Active Directory**
  - **Exchange**
  - **Open LDAP**
  - **Lotus-Domino**
  - **iPlanet**
  - **Other**
- **Managed Domains**—Comma delimited alphanumeric: allows hyphen, dot, but no spaces; max 200 characters. Separate multiple domains with a comma. Example: company.com, payroll.company.com, net-engr.com
- **LDAP page size**—Enter the maximum page size to be queried on the LDAP Server. The default is 100.

  △ **CAUTION: Many LDAP servers, including Active Directory, have a setting that specifies the maximum page size to be queried. If the LDAP Page Size setting exceeds that maximum page size, performance problems may occur on both the LDAP server and on . In the rare circumstances that this needs to be adjusted, consult SonicWall Technical Support.**
- **Requires SSL**—To have the LDAP Server require SSL, select this checkbox. This option is not selected by default.
- **Allow LDAP Referrals**—Select this option if you have multiple LDAP servers, each of which may have different information. When LDAP referral is enabled, one LDAP server can delegate parts of a login request for information to other LDAP servers that have more information. This delegation is called a referral and occurs when an administrator or user logs in. A referred login request can be very slow, taking 20 seconds or more. This setting is not selected by default.

ⓘ **NOTE:** To speed log ins for administrators and users, disable this option if you have:
- Only one LDAP server.
- Two or more LDAP servers that all share the same information.

ⓘ **TIP:** It is safe to disable referrals and then test whether any users are blocked from logging in. No data or settings are lost.

6. Configure the LDAP login method for users:
   - **Allow Anonymous** (default) – Many LDAP servers are configured to provide the list of users to anyone who asks. This is called Anonymous Bind.

ⓘ | **TIP:** Select this option first, then test it; see Step 9.

- **Login** – If the **Anonymous bind** option failed, select this option. You then need to provide a username and password to get LDAP to return the list of users.

7. If you selected **Login**, Specify the **Username** and **Password**.

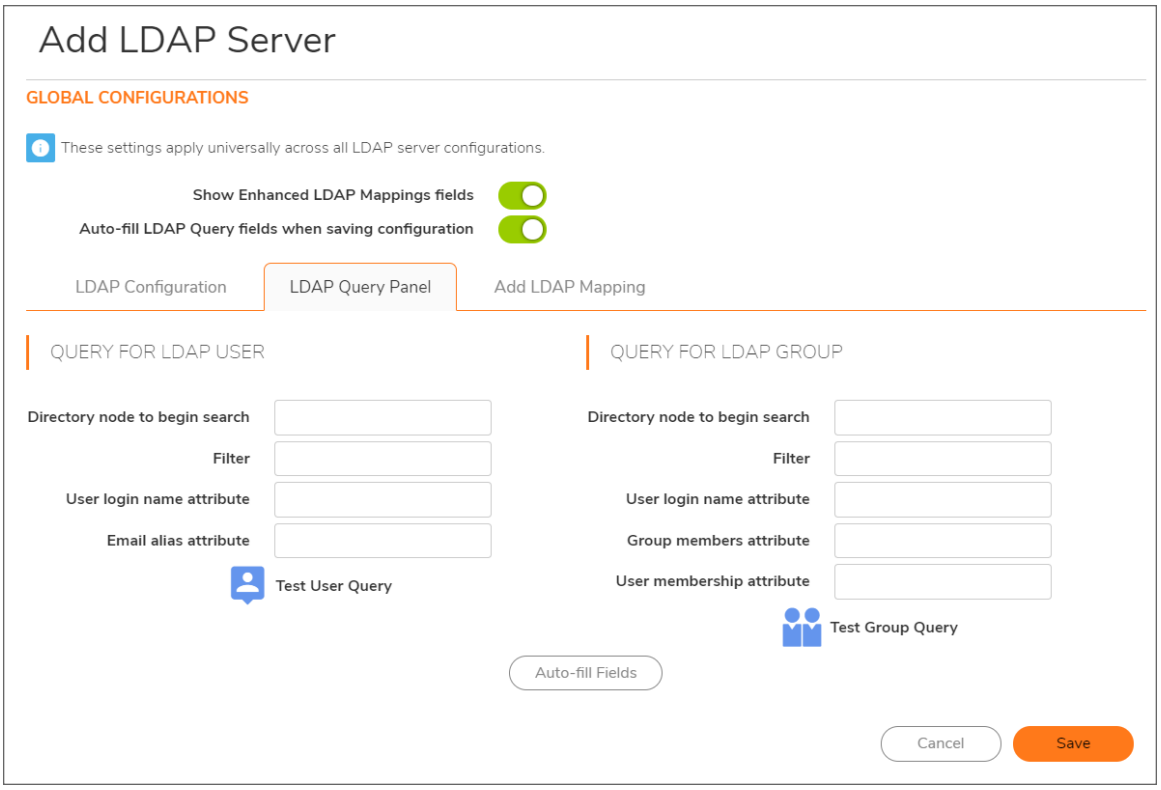
   **Username** is the credential used to allow a user access to the LDAP resource. Each type of LDAP server has a format for a log in name. Use the format appropriate for your server.

   ⓘ | **TIP:** To see examples of the different formats, click the **Question Mark** icon by the **Login name** field.

8. To test the settings you just configured, click **Test LDAP Login**. The **Test Results** message displays.
9. Click **Save Changes** to finish adding an LDAP Server.

# Configuring LDAP Queries

ⓘ | **TIP:** If you selected the **Auto-fill LDAP Query when saving configuration** option on the **LDAP Configuration** tab, the **LDAP Query Panel** fills with default values automatically.




***To successfully allow users to login to their Junk Box:***

ⓘ | **TIP:** To examine your LDAP tree in its entirety to get a comprehensive look at your LDAP structure and its various attributes and object classes, run the free program, Softerra LDAP Browser 2.5, available at: http://www.ldapbrowser.com/download/index.php

On a Windows PC, download the program. When it is running, to determine the best query for your network, browse to a user on the network and examine their attributes.

1. In the **LDAP Query Panel** tab, go to the **Query for LDAP User** section.
2. To use the optional **Query for LDAP Group** functionality, in the **Directory node to begin search** field, specify a full LDAP directory path that points towards a node (directory inside LDAP) containing the information for all groups in the directory. This path narrows the search for LDAP groups to a reasonable size.

   The information contained in LDAP is organized into a directory tree much like an ordinary file system. Each directory is specified as a `name=value` pair, where:

   - **name** is commonly:

     | | |
     |---|---|
     | `DC`(domain component) | `OU`(organizational unit) |
     | `DN`(distinguished name) | `O` (organization) |

   - **value** is commonly one segment of a fully specified hostname (for example, the word `companyxyz` in `sales.companyxyz.com`).

   To specify a particular node in LDAP you use a comma-separated list. To specify multiple nodes to search in, use the ampersand (&) character between full paths.

   For example, if the hostname of a particular machine inside `companyxyz` was `computer27.sales.companyxyz.com`, the LDAP path might be:

   ```
   DC=computer27,DC=sales,DC=companyxyz,DC=com
   ```

   To see examples for the various directory types, click the Question Mark icon next to the **Directory Node to Begin Search** field
3. Enter an LDAP filter in the standard LDAP filter syntax in the **Filter** field.

   Anti-Spam must be instructed on how to find and identify users and mailing lists. By specifically stating the Object Class and mail attribute in the **Filter** field, non-primary email accounts (such as printers and computers) are not included during an LDAP query. Focusing on primary user accounts speeds up the query.

   The Filter field contains an example syntax:

   ```
   (&(|(objectClass=group)(objectClass=person)(objectClass=publicFolder))(mail=*))
   ```

   All LDAP filters are grouped in parenthesis, and the filter itself has a pair of parentheses surrounding the whole string. The very next character from the left is an ampersand (&). The LDAP filter syntax is prefix notation, which means this filter only returns the logical AND of three sub-filters, each grouped in parentheses. Other operators include a pipe (|) for OR and an exclamation point (!) for NOT.
4. Specify the text attribute a user uses fora login name in the **User login name attribute** field. The generally accepted attribute for this field is **sAMAccountName**, which is the default. This attribute should work for Microsoft Windows, as well as all other environments.

   ⓘ **IMPORTANT:** This field works in conjunction and needs to agree with the **Filter** field. If you change **sAMAccountName**, you must change it in both the **Filter** field and the **User login name attribute** field.
5. Specify the email address, employee ID, phone number, or other alias attributes that link a single user to his or her junk box in the **Email alias attribute** field.

At many companies, an end user has multiple email accounts that all map to one true email account. For example, `JohnS@example.com` and `John.Smith@example.com` might both be valid email addresses for John Smith's InBox. Anti-Spam supports this by allowing an end user to have one junk email box that groups all email from their various email addresses.

The generally accepted single attribute for this field is **proxyAddresses**. All other attributes must be separated by a comma. For example:

- `proxyAddresses,legacyExchangeDN`
- `proxyAddresses,EmployeeID,PhoneNumber`

ⓘ | **TIP:** In Microsoft Windows environments, the single attribute, **proxyAddresses**, is often sufficient.

6. Optionally, test to see if your settings work, click the blue icon **Test User Query** under the **Query for LDAP User** section.
7. Save the changes by clicking **Save**.
8. Go to the Query Information for LDAP Groups section.

   ⓘ | **TIP:** If you did not specify **Auto-fill LDAP Query** fields when saving configuration in the **Settings** section, you can click **Auto-fill Group Fields** to do so.
9. To use the optional Groups functionality, in the **Directory node to begin search** field, specify a full LDAP directory path that points towards a node (directory inside LDAP) containing the information for all groups in the directory. This narrows the search for LDAP groups to a reasonable size. For further information about this setting, see Step 2.
10. To instruct Anti-Spam on how to find and identify users and mailing lists, enter an LDAP filter in the standard LDAP filter syntax in the **Filter** field. The field contains an example syntax. For further information about this setting, see Step 3.
11. Specify the attribute of the group that corresponds to Group names in the **User login name attribute** field.
12. A common way to specify a group is a mailing list. In the mailing list entry in LDAP, there is one particular field that specifies the members of the list. Enter that information in the **Group members attribute** field.
13. In some LDAP configurations, there is an attribute, inside each user's entry in LDAP, that lists the groups or mailing lists of which this user is a member. Specify that attribute in the **User membership attribute** field.
14. Optionally, test to see if your settings are functioning correctly, click the blue icon, **Test User Query** or **Test User Query** .
15. Save the changes by clicking **Save**.

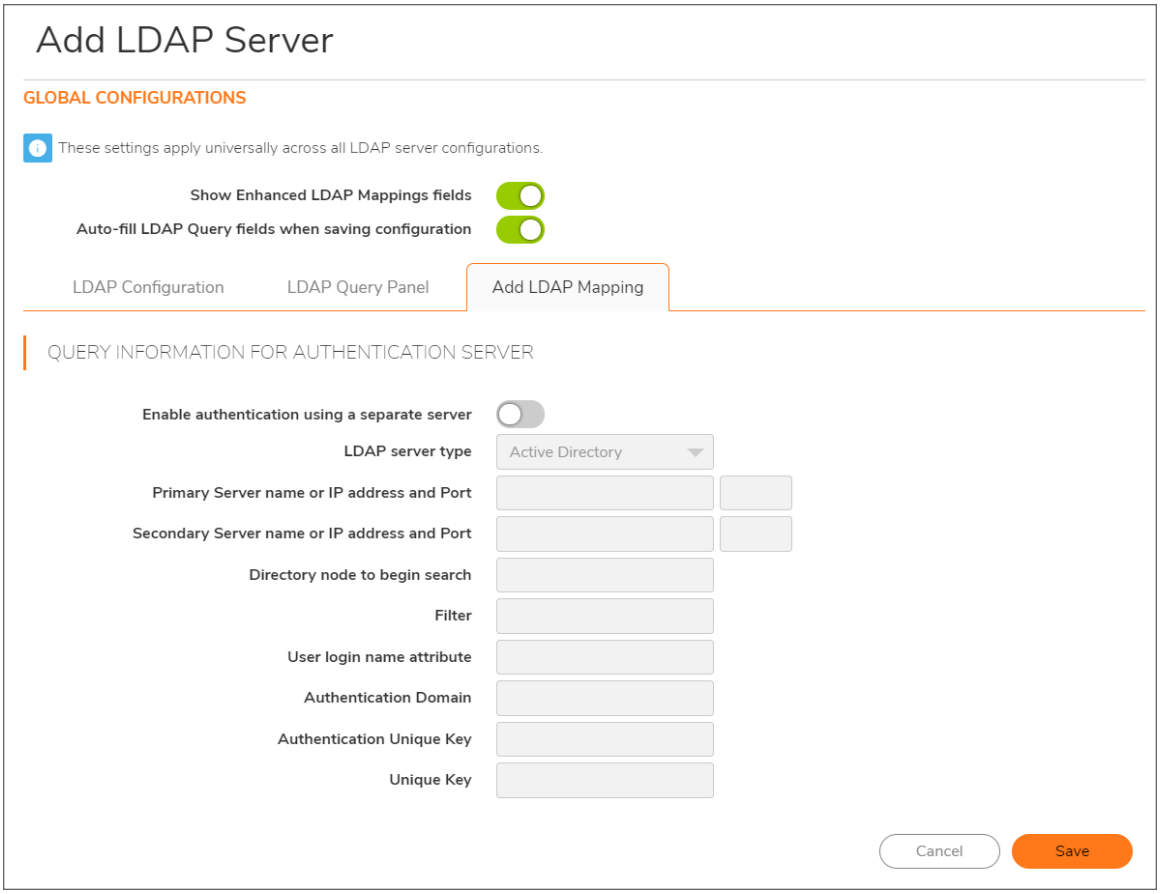
# Adding LDAP Mappings

If you are using a Microsoft Windows environment, you need to specify the NetBIOS domain name in the **Add LDAP Mappings**tab.

ⓘ | **NOTE:** The NetBIOS domain name is sometimes called the pre-Windows 2000 domain name.

***To add LDAP mapping:***

1. Determine your domain name(s).
    a. Login to your domain controller.
    b. Navigate to **Start > All Programs > Administrative Tools > Active Directory Domains and Trusts**.
    c. Highlight your domain from the **Active Directory Domains and Trusts** dialog.
    d. Click **Action**.
    e. Click **Properties**. The domain name(s) appear on the domain's Properties dialog on the **General** view.
    f. Record the domain name(s).
2. Navigate to the **Add LDAP Mapping** tab of **POLICY | Anti-Spam > LDAP Configuration**.




3. Enable the **Enable authentication using a separate server** option to activate the options that follow.
4. Select the **LDAP server type** you are using from the drop-down menu.

5. Create a mapping between the primary and secondary server by entering both the IP addresses and Ports for **Primary Server name or IP address and Port** and **Secondary Server name or IP address and Port**.
6. Complete the remaining fields and click **Save** to complete the mapping.

# Editing an LDAP Server Configuration

Editing an LDAP server configuration requires the same settings as adding a server.

***To configure an LDAP server:***

1. From the list of available LDAP servers, click the **Edit** icon. These sections expand for editing:
    - Server Configuration – see Adding an LDAP Server
    - LDAP Query Panel – see Configuring LDAP Queries
    - Add LDAP Mappings – see Adding LDAP Mappings

# Deleting an LDAP Server

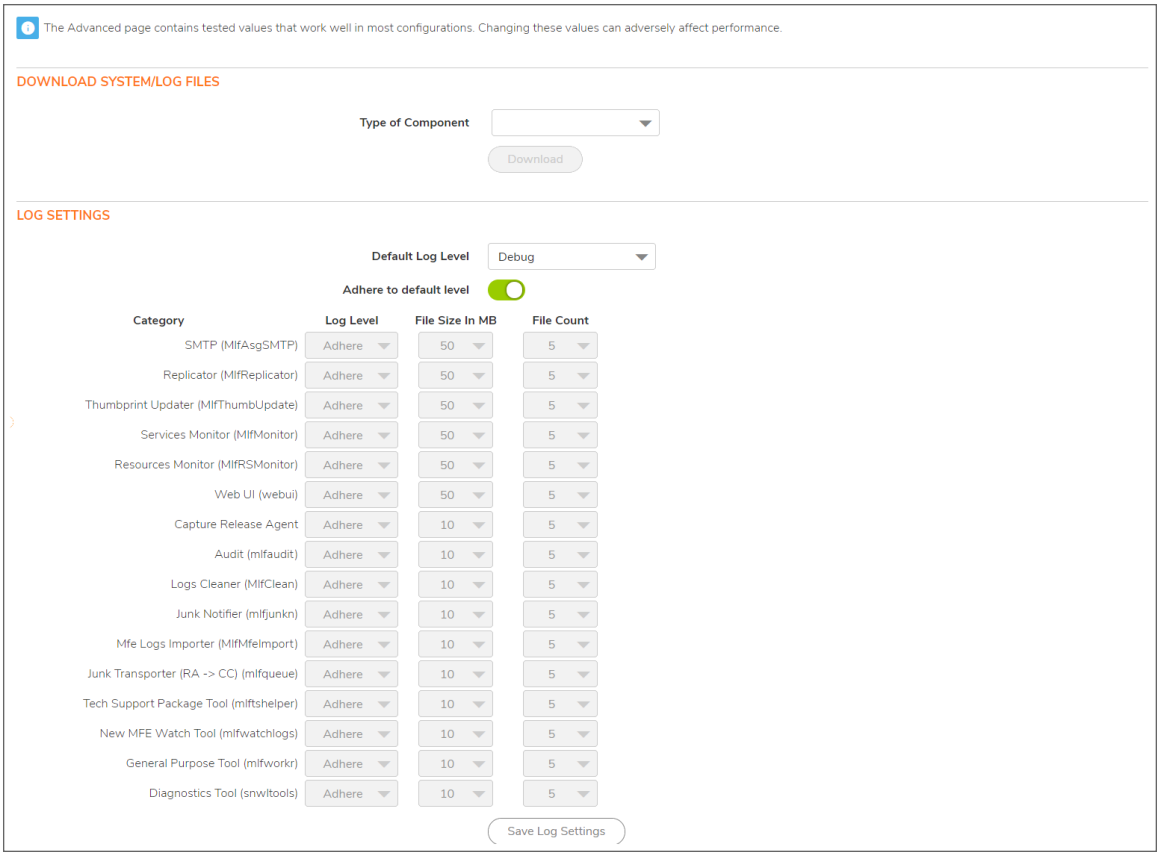
***To delete an LDAP server:***

1. Click the **Delete** icon for the server to be deleted. A warning message appears.
2. Click **OK**. A success message appears at the top of the **POLICY | Anti-Spam > LDAP Configuration** page.

12

# Advanced

The **POLICY | Anti-Spam > Advanced** page allows you to download log and system configuration files from your server as well as configure the log level.




## Topics:

- Downloading System/Log Files
- Selecting Log Settings

# Downloading System/Log Files

ⓘ **NOTE:** Some log file names, such as those found in the `commonlogs` directory, contain a two-digit number such as `12.log`. The "`12`" indicates that the log is for the 12th day of the most recent month. Some log file names end with a digit, such as `MlfThumbUpdate_2.log`. The "`2`" indicates that this is an older log. The current log is `MlfThumbUpdate.log`. The next most recent log is `MlfThumbUpdate_0.log`, followed by `MlfThumbUpdate_1.log`, and so forth.
Most log data is in Greenwich Mean Time (GMT), not in the local time of the server the logs come from. This applies to the names of the log files as well.

***To download log or system configuration files from your SonicWall Email Security server:***

1. Navigate to the **Download System/Log Files** section of **POLICY | Anti-Spam > Advanced**.

2. Select the type of file to download from the **Type of Component** drop-down menu. The **Choose specific files** list becomes populated with those types of files.
3. From the **Choose specific files** list, select one or more specific items. The file names turn orange when selected. The **Download** button becomes active.

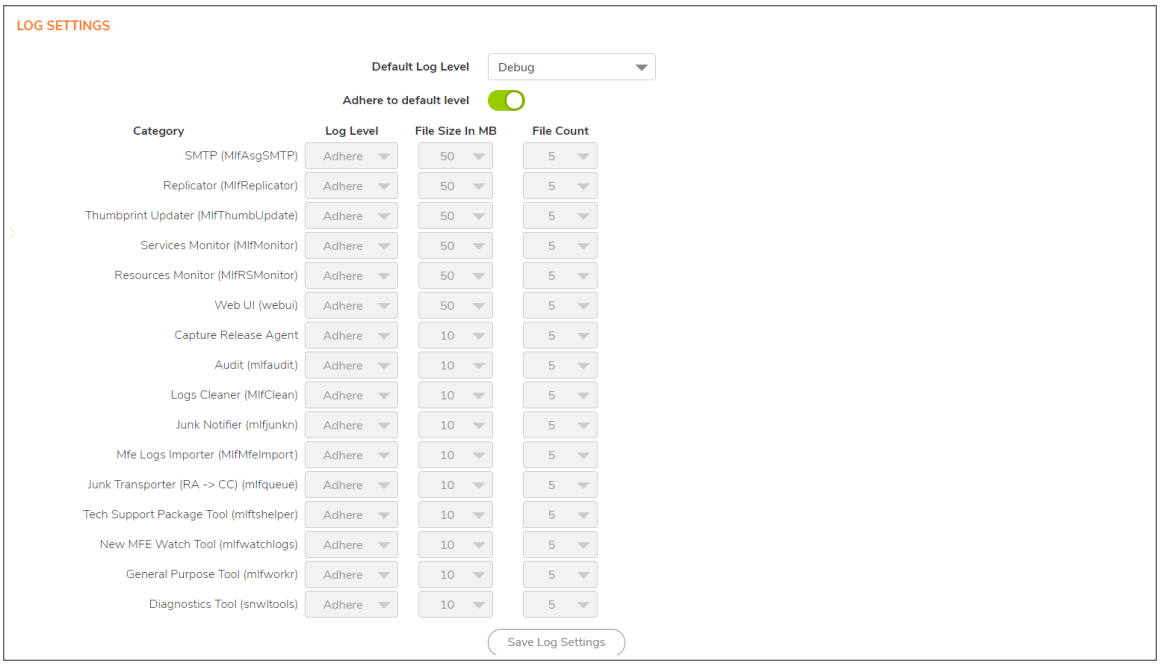
   ⓘ | **NOTE:** The selected files are combined into a zip file.
4. Click **Download** to download the file(s) to your local hard drive.

# Selecting Log Settings

You can select the level and amount of system report information to be stored in your logs in the **Log Settings** section.

***To configure the level and amount of log information:***

1. Navigate to the **Log Settings** section of **POLICY | Anti-Spam > Advanced**.




2. Select the default log level from the **Default Log Level** drop-down menu; levels are listed from lowest to highest:

   ⓘ **NOTE:** The higher the default log level, the more events recorded. For example, the **info** level also records **trace** and **debug** levels.

   - **trace** – lowest level
   - **debug** – default
   - **info**
   - **warn**
   - **error**
   - **fatal** – highest level

   All logs adhere to the default level with the **Adhere to default level** option enabled.

3. To make changes to the logs in the **Log Settings** section, disable **Adhere to default level**. All drop-down menus for all service categories become active.

4. To change the log level for specific services and subservices from the **Log Level** drop-down menu for the service/subservice to be changed, select the desired log level. The levels are the same as for those in Step 3, plus the **Adhere** option.
5. The default log level for all service and subservice categories is **Adhere**, that is, the log level set by the **Default Log Level** drop-down menu is used.
6. Optionally, select the number of log files to retain in **File Count**. By default, Junk Box keeps three log files for these services:

   - SMTP
   - Replicator
   - Thumbprint Updater
   - Services Monitor
   - Resources Monitor
   - Web UI

   When a fourth log file is generated, the oldest log file is discarded, the second oldest becomes the oldest, and the third oldest becomes the second oldest.

   a. You can increase the number of logs kept for a service by selecting a number from the **File Count** drop-down menu for that service:

      - 3
      - 5
      - 6
      - 7
      - 8
      - 9
      - 10

      A lower number of logs saves disk space, but older data might not be available. A larger number of logs retains more data, but takes more disk space.
7. Optionally, select a size for the service logs (see Step 6) from the **File Size in MB** drop-down menus. The default size of each log is 10 Mb.

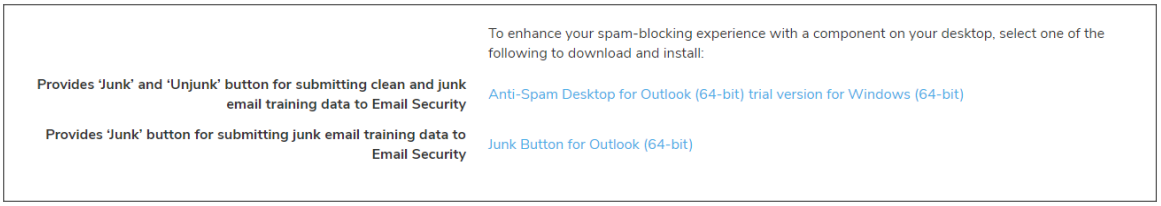
   You can increase the size of the logs, in 10 MB increments, from 10 Mb (default) to 100 Mb. A smaller log size saves disk space, but larger logs contain more data.

   ⓘ | **IMPORTANT:** Changing the size of a log requires restarting the Tomcat server.
8. Click **Save Log Settings** to save any changes made.

13

# Downloads

The **POLICY | Anti-Spam > Downloads** page allows you to download and install one of latest spam-blocking buttons from SonicWall onto your desktop for easier access.




By clicking on a link, you can download these buttons to your desktop:

- Junk button to teach Email Security what you want easily and quickly; select one:
  - **Junk Button for Outlook (64-bit)**

14

# 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.

The Support Portal enables you to:

- View Knowledge Base articles and Technical Documentation
- View and participate in the Community Forum discussions
- View Video Tutorials
- Access MySonicWall
- Learn about SonicWall Professional Services
- Review SonicWall Support services and warranty information
- Register at SonicWall University for training and certification

# About This Document

SonicOS Anti-SpamAdministration Guide
Updated - April 2024
Software Version - 7.0
232-005327-00 Rev C

Copyright © 2024 SonicWall Inc. All rights reserved.

The information in this document is provided in connection with SonicWall and/or its affiliates' products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, SONICWALL AND/OR ITS AFFILIATES ASSUME NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL SONICWALL AND/OR ITS AFFILIATES BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF SONICWALL AND/OR ITS AFFILIATES HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. SonicWall and/or its affiliates make no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. and/or its affiliates do not make any commitment to update the information contained in this document.

For more information, visit https://www.sonicwall.com/legal.

## End User Product Agreement

To view the SonicWall End User Product Agreement, go to: https://www.sonicwall.com/legal/end-user-product-agreements/.

## Open Source Code

SonicWall Inc. is able to provide a machine-readable copy of open source code with restrictive licenses such as GPL, LGPL, AGPL when applicable per license requirements. To obtain a complete machine-readable copy, send your written requests, along with certified check or money order in the amount of USD 25.00 payable to "SonicWall Inc.", to:

General Public License Source Code Request
Attn: Jennifer Anderson
1033 McCarthy Blvd
Milpitas, CA 95035