



Spam Manager

Quarantine Admin Guide

Contents

Introduction	1
About Spam Quarantine Tasks.....	1
Quarantine Deployment Tasks.....	1
Before Activation of Spam Manager.....	3
After Activation of Spam Manager	3
Accessing Spam Manager and Logging In	4
Accessing Spam Manager	4
Logging into Spam Manager	4
Managing Accounts.....	5
About Managing Accounts.....	5
Viewing Details of Spam Manager Accounts	5
Creating New Spam Manager Accounts	6
Deleting Spam Manager Accounts.....	7
Managing Aliases and Account Groups	8
About Managing Aliases and Account Groups.....	8
Managing Aliases	8
Managing Account Groups	10
Accessing Other Spam Manager Accounts	11

Introduction

This guide is for Quarantine Administrators. Quarantine Administrators are users of Spam Manager with extended privileges that allow them to perform some administrative functions. It describes the role of a Quarantine Administrator and guides you through the administrative tasks.

About Spam Quarantine Tasks

Quarantine Administrators are users of Spam Manager who have extended privileges. These privileges allow them to perform some administrative functions.

You can perform these tasks within the domains for which you have the necessary permissions.

The following table describes the spam quarantine administration tasks.

Task	Description
Displaying details of Spam Manager accounts	See the identity, last access date, and status of accounts.
Creating accounts	Generate new user accounts and specify whether to enable the sending of welcome messages and notifications.
Creating account groups	Consolidate the spam that is sent to a number of designated addresses into a single Spam Manager account. The settings for the individual accounts still apply and users can still access their individual accounts, if necessary.
Creating aliases	Consolidate multiple email addresses under a single email address - the owner address. The 'owner' account manages the spam that is sent to any of the aliased addresses. The 'owner' account defines the settings for the aliased addresses. Creating an alias account to manage multiple email addresses is useful where an individual has several email addresses within your organization, for example.
Accessing different accounts	Access the account of another user, and being able to work as if logged in as that user.
Deleting accounts	Delete selected accounts.

Quarantine Deployment Tasks

Quarantine Administrators' tasks fall into two categories:

Before activation of Spam Manager Tasks that must be performed during deployment.

After activation of Spam Manager Tasks that may need to be performed on an ongoing basis.

The role of the Quarantine Administrator within your organization depends on how Spam Manager is deployed.

The deployment of Spam Manager is discussed in more detail in the *Anti-Spam Administrator Guide*.

The main deployment policies are as follows:

Deployment option	Description
Direct management	<p>All users can register with and log in to Spam Manager. Users receive email notifications when they receive spam messages. Users can manage their spam themselves. The notifications do one of the following:</p> <ul style="list-style-type: none"> List the spam messages that have been detected since the last notification, and request that the user logs into Spam Manager to view or release the emails List the spam messages that have been detected since the last notification, and provide a Release link for users to release them without needing to continually log into Spam Manager. <p>These are called active summary notifications.</p>
Silent deployment	<p>Users are not asked to register with and log in to Spam Manager, and they do not receive notifications. A Quarantine Administrator can access and manage users' Spam Manager accounts on their behalf. Depending on the way Anti-Spam is set up, users may still be able to receive active summary notifications to release emails. In this case, no links to Spam Manager appear in the notifications.</p>
Targeted deployment	<p>Some targeted users (for example, key personnel) are given access to their Spam Manager accounts, while silent deployment is used for others.</p>

The following table shows the tasks that the Quarantine Administrator performs under different deployment policies.

Deployment Policy	Before activation of Spam Manager	After activation of Spam Manager
Direct management	<p>May set up account groups and aliases to direct the spam of multiple users or an individual with multiple email addresses to a single account.</p>	<p>May access users' accounts (e.g., if the user is away from the office). View users' personal approved and blocked senders lists (if these are defined).</p>
Silent deployment for all users		<p>Access users' accounts to search for specific messages (if the user suspects that a non-spam message may have been redirected to Spam Manager). Search for specific messages (if a user suspects that a non-spam message may have been redirected to Spam Manager).</p>
Targeted deployment	<p>Create Spam Manager accounts that override the default notification setting (usually to give access to targeted users when the default is silent deployment).</p>	<p>For 'silent' users: Access a user's account to search for specific messages (if a user suspects that a non-spam message may have been redirected to Spam Manager). For 'targeted' users: May access a user's account (e.g., if the user is away from the office). May view a user's personal approved and blocked senders lists (if these are defined)</p>

Before Activation of Spam Manager

The following are tasks that a Quarantine Administrator may need to perform before the activation of Spam Manager:

- Ensure that you have Address Registration is in use for your Email Security services. Address registration is used to reject any email that is sent to an address in your domains that does not appear on a database of known valid email addresses. You can set this up manually or automatically by using the Synchronization Tool. If required, create Spam Manager accounts that override the default notification setting (usually to give access to targeted users when the default is silent deployment).
- Set up account groups and aliases.
 - To direct the spam of any email address to a nominated owner.
 - To consolidate the spam of a user with multiple email addresses into a single owner account (alias).

See *About Managing Aliases and Account Groups* for more information.

These tasks should be completed before the activation of Spam Manager, especially where new accounts need to be created that override the default notification setting for users within a domain. You cannot override the default notification setting for accounts that are created automatically by the arrival of spam—that is, for accounts that are deployed silently. The default notification can only be overridden if Users control notifications is selected during the configuration of Spam Manager in the service portal.

After Activation of Spam Manager

The quarantine administration tasks that may need to be carried out after the activation of Spam Manager are described in the following table.

Task	Description
Maintaining the list of accounts	Create new accounts and deleting unwanted accounts. You may want to delete an account so that you can then recreate it without the default notification settings.
Updating account groups and aliases	Add new email addresses to an account group.
Accessing the account of another user	Access the account of another user to: <ul style="list-style-type: none"> • Manage their spam— for example, if the owner is away from the office, or where Spam Manager is deployed silently • Change the notification setting—for example, to turn on notifications for a targeted user in a silent deployment setting
Managing approved and blocked senders lists	If users are enabled to maintain personal approved and blocked senders lists, Quarantine Administrators may be required to add or remove entries from the lists.

Accessing Spam Manager and Logging In

Accessing Spam Manager

Quarantine Administrators can access Spam Manager before it has been activated for all regular users. Once your IT Administrator has created your Quarantine Administrator's account, you are given the Spam Manager URL (see below) so that you can register.

Once you have been given the Spam Manager URL, you can enter your email address into Spam Manager and request a password.

NOTE: You only receive the login URL once you receive your first item of quarantined spam.

To access with Spam Manager:

1. Access <https://spammanager-6.messagelabs.com/login.xsp>.
The Spam Manager **Login** page displays.
2. Enter your email address.
The **New Account** page displays.
3. Click **Send me a password**.
A confirmation message containing your password and a link to the login page are sent to your usual email inbox.

To access with Spam Manager before you receive your first item of quarantined spam:

1. Ask your IT Administrator for the Spam Manager URL.
The Spam Manager **Login** page displays.
2. Enter your email address.
3. Click **Forgot password**.

Logging into Spam Manager

Once you have received a confirmation message containing your password, you can log in.

Once you have logged in, you should change your password to something unique and memorable. Spam Manager may enforce certain requirements in your new password, such as the use of numeric and non-alphabetic characters. The password policy may also prevent the use of dictionary words or certain other character sequences. See your organization's password policy or security policy for details.

For information on how to change your password, see the *Spam Manager User Guide*.

To log in:

1. Click the URL in your confirmation message.
The Spam Manager **Login** page displays.
2. Enter your password and click **[Login]**.
Quarantine Administrators' tasks are performed from the **Administration** tab.

Managing Accounts

About Managing Accounts

This section describes the tasks that a Quarantine Administrator may perform in order to maintain Spam Manager accounts.

It is important to understand how accounts are created in Spam Manager, because under certain circumstances accounts are created automatically and you may not be able to override the default settings for welcome messages and notifications.

New Spam Manager accounts may be created manually or automatically. Where accounts are created automatically, they use the default Spam Manager settings. You may not be able to override the default settings for welcome messages and notifications. If you want new accounts to override the default Spam Manager settings, you should create the accounts manually.

- **Manually** when a Quarantine Administrator creates a new account. The Quarantine Administrator may override the default settings for welcome messages and notifications.
- **Automatically** in the following circumstances:
 - When a user responds to a welcome message from Spam Manager by requesting a password.
If the generation of welcome messages is enabled as a default, then, following activation of Spam Manager, a welcome message will be issued when spam is sent to an email address for which an account does not yet exist.
 - When a Quarantine Administrator sets up an account group and the email address of the owner does not yet exist.
 - When a user receives an active summary notification allowing them to release an email directly from the notification.
When Spam Manager is deployed using active summary notifications, users will not receive a separate welcome message.

Viewing Details of Spam Manager Accounts

You can view details of the Spam Manager accounts within the domains that you administer.

The account details that are available in Spam Manager include:

- The email address that identifies the account
- The account creation method (i.e., whether it was created manually or automatically)
- The account type (i.e., whether it is a Quarantine Administrator account or not)
- The date of last login
- Whether the account has spam

The most likely reason for viewing account details is to check whether an account exists for a specific email address.

Reasons for checking whether a Spam Manager account exists include:

- Before setting up an account group or alias
- Before accessing another user's account
- If a user asks whether they have an account

To view details of accounts:

1. In the **Administration** tab, click **Show Accounts**.
2. To locate the accounts to view, enter appropriate search text in the **show accounts containing** box. (Leave this box blank to display all accounts within a domain.)
3. Select a domain from the **within domain** drop-down list.
4. To display accounts created both manually and automatically, check the in **any way** option button.
5. Click **Search**.

The search results display. If a large number of accounts display, you can view a page at a time. Use the markers at the bottom of the screen to move between pages.

Creating New Spam Manager Accounts

You can create new Spam Manager accounts for any domains that you administer. Creating an account manually enables you to override the default settings for welcome messages and notifications.

You will need to decide whether to enable notifications and welcome messages for the accounts that you create. Notifications are email messages, generated automatically and at preset intervals, listing new spam held in the user's Spam Manager account. Welcome messages are email messages, sent automatically by Spam Manager to the email addresses of users for whom either a new Spam Manager account has been created explicitly, or spam has been received for the first time (i.e., an account is being created implicitly). The message invites the user to visit their Spam Manager account and review their spam.

Accounts can be created in batches with the same settings for welcome messages and notifications.

To create a new Spam Manager account or a batch of accounts:

1. In the **Administration** tab, click **Create Accounts**.
2. Enter or copy and paste the email addresses in the blank text box.
3. To enable the sending of welcome messages and notifications, check the associated checkboxes.
4. Click **Create Accounts**.

A message displays, informing you whether the accounts have been created successfully.

Deleting Spam Manager Accounts

You can delete accounts within the domains that you administer. You may need to delete a Spam Manager account in the following circumstances:

- To change the notification settings (i.e., delete the existing account and create a new account with different notification setting).

NOTE: If Spam Manager has been configured with users control notifications selected, a Quarantine Administrator can also change the notification setting by accessing the account directly, without having to delete and then recreate the account.

- To remove the account of someone who has left the organization.

NOTE: When a Spam Manager account is deleted and recreated with a different notification setting, any spam that was held for the original account is forwarded to the new account.

To delete an account:

1. In the **Administration** tab, click **Show Accounts**.
2. Locate the account to delete, and select the checkbox to the left of the account address.
3. Click the **[Delete]** button.

Managing Aliases and Account Groups

About Managing Aliases and Account Groups

Depending on your organization's configuration, you may not see all of the functionality described here.

Two kinds of Spam Manager accounts can be used for grouping multiple email addresses into a single Spam Manager account.

Quarantine Administrator may need to establish aliases and account groups before Spam Manager is activated. Further aliases and account groups may need to be created after the activation of Spam Manager.

Group account type	Description	Benefits
Alias	An email address that is managed by the account of another email address—the owner address. The owner account defines the settings of the aliased address and manages the spam that it receives.	Set up an alias if the aliased email addresses do not need their own individual Spam Manager account and settings. For example, use aliases where an individual has several email addresses within your organization.
Account group	A single account to manage the spam that is sent to a number of designated addresses. The settings for the individual accounts still apply and group members can still access their individual accounts, if necessary.	Set up an account group if the group members should still be able to access their individual accounts and retain their particular settings. For example, use an account group to manage spam that is sent to distribution lists and for an Administrator to manage spam for several other users.

NOTE: Only email addresses within your organization's domains can be used as aliases and assigned to account groups.

Managing Aliases

An alias is an email address that is managed by the account of another email address—the owner address. The owner account defines the settings of the aliased address and manages the spam that it receives.

Viewing Aliases

You can review current aliases. You may need to review aliases to see which email addresses are aliased to a specified Spam Manager account, for example. Or you can check whether a specified email address is aliased to another account.

To view aliases:

1. In the **Administration** tab, click **Manage Aliases**.
2. In the **Owner** and **Alias** search boxes, enter at least the first few characters of the email address to search for, as required.
3. Click **Search**.

The search results display. If there is more than a single page, use the markers at the bottom of the screen to move between pages.

Creating Aliases

To create an alias:

1. In the **Administration** tab, click **Manage Aliases**.
2. In the **Owner** box, enter the email address of the Spam Manager account to which all spam is directed.
3. In the **Aliases** box, enter the email addresses of the account that the owner is to manage.
4. If you want the owner of the email address to be notified that the alias has been set up, select the **Notify** checkbox.

NOTE: If this checkbox is not shown, Spam Manager has been configured with a default to notify owners of aliases.

5. Either:
 - To add the aliases to those already established for the owner, click **Add**.
 - To replace all of the owner's existing aliases, click **Replace**, and then **Confirm Replace**.

To display the new or the edited aliases, search for the owner or alias using the search boxes. The updated list displays.

Deleting Aliases

You can remove an alias to enable the owner of the previously aliased email address to manage their own spam. After an alias is deleted, any spam that is received for that email address is no longer directed to the alias' owner. Instead, the spam is directed to a new Spam Manager account for that email address. If Spam Manager is configured to send welcome messages when spam is received, a message inviting the user to register with Spam Manager is sent to the previously aliased email address. The user can then request a password and manage their own Spam Manager account.

To delete an aliased email address:

1. In the **Administration** tab, click **Manage Aliases**.
2. In the lower section of the page, use the **Alias** search box to locate the email address of the alias to remove.
3. Select the checkbox to the right of the selected email address.
4. Click **Delete**.

Managing Account Groups

Setting up an account group enables spam for several email addresses to be viewable through one Spam Manager account. The settings for the individual accounts still apply to those individual's email and the users in the group can still access their accounts, if necessary.

Viewing Account Groups

You can review current account groups. You may need to review an account group to see which email addresses are under the management of an account group owner, for example. Or you can check whether a specified email address belongs to a certain account group.

To view account groups:

1. In the **Administration** tab, click **Manage Account groups**.
2. In the **Owner** and **Account** search boxes, enter at least the first few characters of the email address to search for, as required.
3. Click the **[Search]** button next to the completed search box.
The search results are displayed. If there is more than a single page, use the markers at the bottom of the screen to move between pages.

Creating Account Groups

To create an account group:

1. In the **Administration** tab, click **Manage Account groups**.
2. In the **Owner** box, enter the email address of the Spam Manager account that the spam for the member accounts is to be directed.
3. In the **Accounts in group** box, enter the email address of the account to add to the group.
An email address that you add to an account group can be the address of a single distribution list, or a number of email addresses.
4. To add the member account to those already established for the owner, click **Add**.
To display the new or the edited member accounts, search for the owner or the member accounts using the search boxes. The updated list is displayed.

Deleting Account Groups

You can remove an account from an account group. After the account has been removed, any spam that is received for that email address is no longer directed to the owner of the account group. Removing an account from an account group does not affect the user to whom the email address belongs. Typically, with account groups, the group members manage their own spam.

To delete an account from an account group:

1. In the **Administration** tab, click **Manage Account groups**.
2. In the lower section of the page, use the **Account** search box to locate the email address of the account to remove.
3. Select the checkbox to the right of the selected email address.
4. Click **Delete**.

Accessing Other Spam Manager Accounts

As a Quarantine Administrator, you can log in to the accounts of other users within the domains you administer. You can then view and manage the spam of those users. You can release or delete messages and change certain user settings, but you cannot change the user's password.

You can view and edit a user's Approved Senders and Blocked Senders lists, if these have been configured for your users.

You may need to access other accounts in the domains you administer in the following circumstances:

- If the owner of the account is away from the office
- If Spam Manager is deployed silently and users are not expected to manage their own accounts directly
- To change the notification setting for an account
Spam Manager must have been configured to allow users to control notifications.
- To view a user's Approved Senders and Blocked Senders lists.

NOTE: For full details of the user tasks in Spam Manager, see the *Spam Manager User Guide*.

To access another account:

1. In the **Administration** tab, click on **Access Different Account**.
2. Enter the email address of the account to access.
3. Click **Select**.

Spam Manager displays the selected account with the email address of the selected account that is displayed against a colored background.

You can now perform the tasks that are available to the user within this account (except changing the password).

To return to your own account:

- Click **Logout** and then **Confirm**.
You are returned to your own account.