Message Manager Administrator Guide

Symantec.cloud

Documentation version: 2.0

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Clients are advised to seek specialist advice to ensure that they use the Symantec services in accordance with relevant legislation and regulations. Depending on jurisdiction, this may include (but is not limited to) data protection law, privacy law, telecommunications regulations, and employment law. In many jurisdictions, it is a requirement that users of the service are informed of or required to give consent to their email being monitored or intercepted for the purpose of receiving the security services that are offered by Symantec. Due to local legislation, some features that are described in this documentation are not available in some countries.

Configuration of the Services remains your responsibility and entirely in your control. In certain countries it may be necessary to obtain the consent of individual personnel. Symantec advises you to always check local legislation prior to deploying a Symantec service. You should understand your company's requirements around electronic messaging policy and any regulatory obligations applicable to your industry and jurisdiction. Symantec can accept no liability for any civil or criminal liability that may be incurred by you as a result of the operation of the Service or the implementation of any advice that is provided hereto.

The documentation is provided "as is" and all express or implied conditions, representations, and warranties, including any implied warranty of merchantability, fitness for a particular purpose or non-infringement, are disclaimed, except to the extent that such disclaimers are held to be legally invalid. Symantec Corporation shall not be liable for incidental or consequential damages in connection with the furnishing, performance, or use of this documentation. The information that is contained in this documentation is subject to change without notice.

Symantec may at its sole option vary these conditions of use by posting such revised terms to the Web site.

Technical Support

The Global Client Support Center (GCSC) seeks to provide a consistently high level of service. The team consists of technically-trained client-focused individuals. They respond to your issue with the aim of resolving it within the first contact.

To reduce the time it takes to resolve an issue, before you contact the team refer to the Help on rasing support tickets. The Help explains the information that is required for the various types of support issue.

We welcome comments and questions about our services.

Contact GCSC using the following contact details:

Email us at:	support.cloud@symantec.com
Call us on:	EMEA: +44 (0) 870 850 3014 or +44 (0)1452 627766 US: +1 (866) 807 6047 Asia Pacific: +852 6902 1130 Australia: 1 800 088 099 New Zealand: 0800 449 233 Hong Kong: 800 901 220 Singapore: 800 120 4415 Malaysia: 1 800 807 872 South Korea: 00798 14 800 6906
Open a support ticket	Log into ClientNet and navigate to **Support > Ticketing**
Visit the Web site	www.symanteccloud.com
Visit the Online Help	Online Help

We recommend that you check ClientNet frequently for maintenance information and to learn what's new. You can also add your mobile number in the **Administration > SMS Alerts** section of ClientNet to receive critical service-related issues by text message.

Contact and escalation details are available in the following PDF: Contact and Escalations document.

Contents

Technical Support 3

Chapter 1 Introduction 7

About Message Manager 7
Privacy Users 9
The management portal and Message Manager 10
Logging on to Message Manager 10
Logging On and Off ClientNet 11
Address Registration and Message Manager 11
Reporting on Message Manager 11

Chapter 2 Configuring Message Manager in ClientNet 13

Defining custom settings 13
Defining default notification settings 14
Enabling users to access Message Manager 15
Viewing default settings for Privacy Users 16
Enabling users to override the default notification settings 17
Enabling users to request a sender to be approved 18
Notifying users when an alias is changed 18
Making your Acceptable Use Policy (AUP) available 19
Defining Message Manager Administrators 19
Adding Privacy Users 20

Chapter 3 What's new in Message Manager? 23

What's new in Message Manager 23

Chapter 1

Introduction

This chapter includes the following topics:

- About Message Manager
- Privacy Users
- The management portal and Message Manager
- Logging on to Message Manager
- Logging On and Off ClientNet
- Address Registration and Message Manager
- Reporting on Message Manager

About Message Manager

The Message Manager service can be made available for administrators only, or for administrators and users. Message Manager enables administrators and users to manage the email that is quarantined by the Email AntiSpam, Email Image Control, and Email Content Control services. Message Manager can be made available to users for any or all of these email services, as required.

Note: Privacy Users have access to all their email for all services that are active for their account.

See "Privacy Users" on page 9.

Administrators are Message Manager users who have extended privileges. These privileges allow them to perform some administrative functions, as described in the following table. Administrators can perform these tasks within the domains and services that they have permission for.

Table 1-1 Message Manager administrator privileges

Privilege	Description
Reviewing accounts	You can see the identity, last access date, and status of accounts. It may sometimes be necessary to delete an account and recreate it with the settings that override the current defaults for notifications. Detailed configuration reports are also available to administrators. See "Reporting on Message Manager" on page 11.
Creating accounts	You can generate new user accounts and specify whether to enable welcome messages and notifications to be sent to users.
Creating account groups	An account group consolidates the quarantined messages that are sent to a number of designated addresses into a single Message Manager account. The settings for the individual accounts still apply and users can still access their individual accounts, if necessary. For example, account groups are useful when a PA or secretary looks after a manager's account. The PA can view quarantined email for themselves and the manager through the PA's own Message Manager account. The manager's settings still apply to their quarantined email.
Creating aliases	An alias consolidates multiple email addresses under a single email address – the owner address. So, the quarantined messages that are sent to each of the aliased addresses use the settings of the 'owner' account and the owner manages them. Aliases are useful where an individual has several email addresses within the organization.
Accessing different accounts	You can access the account of another user and work as if you are logged in as that user. When accessing a different account, you can: ■ Manage their quarantined messages. For example, if the owner is away from the office, or where Message Manager is deployed silently. ■ Change the notification setting. For example, turn on notifications for a targeted user in a silent deployment setting. ■ Manage outbound messages. For example, you can manage the emails that are quarantined for a user in line with their outbound Email Image Control and Email Content Control policy. Users cannot access outbound quarantined email themselves. ■ Manage approved and blocked senders lists. Your users may be enabled to maintain personal approved and blocked senders lists. If so, you can add or remove entries from the lists. This facility is available within the management portal as well as in Message Manager.

Privacy Users

Depending on your organization's deployment of the Email Security services, some or all of your users may be *Privacy Users*. Privacy Users have access to all their inbound email using Message Manager for all services that are active – Email AntiSpam, Email Image Control, and Email Content Control. The actions that an Administrator can perform for a Privacy User's account are more limited than for other users.

These limitations are:

- A Privacy User account cannot be created manually.
  Accounts for Privacy Users are only created automatically when they receive their first quarantined email.
- A Privacy User's account can only be accessed by two Administrators at the same time. This is known as "Paired Administration".
  Paired Administrators can only access a Privacy User's account if the domain is provisioned with Paired Administration.
- Paired Administrators can only see the **Summary** tab for a Privacy User. Within the **Summary** tab, Paired Administrators can:

  View the user's list of messages

  View the detail of a message

  Release messages to the originally intended recipient

- The following restrictions apply to Paired Administrators:

  The delete functionality is not available

  Paired Administrators cannot access or adjust the user's settings

  The Email AntiSpam **Approved Senders**, **Blocked Senders**, and **Options** tabs of Privacy User accounts are not visible to paired Administrators

- A single Administrator can view a list of Privacy User accounts, but cannot delete or access these accounts.
- An Administrator cannot change any alias settings for Privacy User's account.
- An Administrator cannot define account group settings for a Privacy User's account.
- Notifications cannot be disabled for Privacy Users.

- A Privacy User cannot be added to an exclusion list within the Email Image Control or Email AntiSpam services in the management portal.
- Administrators cannot see actions including **Block and Delete**, **Redirect**, or **Copy**, in any domain that has Privacy enabled.
- Administrators cannot access through the management portal the blocked and approved senders lists that a Privacy User has defined at user level.
- User-level blocked and approved senders lists are always set up to replace the domain-level lists on a privacy-enabled domain.
- Any two administrators that are configured in the usual way can act as Paired Administrators by logging in synchronously.
- Privacy Users can opt in to or opt out of the Message Manager service. An administrator cannot configure whether a Privacy User is enabled with Message Manager on their behalf.

See "Adding Privacy Users" on page 20.

See "Viewing default settings for Privacy Users" on page 16.

The management portal and Message Manager

The management portal is the online interface for configuring the settings for Message Manager, as well as other related services such as Email AntiSpam, Email Image Control and Email Content Control.

Locating the Message Manager pages in the management portal

Note: Depending on your organization's configuration, you may not see all of the pages in the management portal that are described in this guide.

To locate the Message Manager pages in the management portal

1. In the top navigation bar, click **Configuration > Email Services**.
2. In the left navigation bar, click **Message Manager**.

Settings that are made under the tabs in the management portal are not applied until they have been saved. Make all the changes that you want to, then select **Save and Exit**.

Logging on to Message Manager

Message Manager is available to users by clicking on the link in a notification email that they have received.

Logging On and Off ClientNet

To log on to ClientNet, you need a user name and password.

To log on to ClientNet

1. Enter your user name.
2. Enter your password.
3. Click **Log in**.

To log out of ClientNet

- From any screen in ClientNet, click the **Log Out** link in the top right of the screen.

Address Registration and Message Manager

All email addresses used with the Message Manager service must be registered in our infrastructure.

To locate the Address Registration pages in the management portal

- Click **Configuration > Email Services > Platform > Address Registration**.

For full details about registering your email addresses manually, by CSV upload, and automatically using the Synchronization Tool, see Help on Address Registration.

Reporting on Message Manager

Detailed reports are available for Message Manager.

To locate the Reporting pages in the management portal

- Click **Reports > Report Requests**.

For full details about reporting on the Message Manager service, see Help on Reports.

The following table describes the Message Manager reports that are available.

Table 1-2 Message Manager reports

Email data type	Report name	Description
Email Detailed Report (CSV)	Quarantine (Message Manager Release and Delete detailed)	

Table 1-2 Message Manager reports *(continued)*

Email data type	Report name	Description
Email Detailed Report (CSV)	Quarantine (Message Manager Release and Delete summary)	
Email Configuration Report (CSV)	User Block and Approved List Entries	This report is only available where user-level settings have been provisioned for the client.
Email Configuration Report (CSV)	User Opt-In and Opt-Out Requests	This report is only available where Privacy Users have been provisioned for the client.
Email Configuration Report (CSV)	Message Manager User Logins	
Email Configuration Report (CSV)	Message Manager All Accounts	
Email Configuration Report (CSV)	Message Manager Linked Accounts	

Chapter 2

Configuring Message Manager in ClientNet

This chapter includes the following topics:

- Defining custom settings
- Defining default notification settings
- Enabling users to access Message Manager
- Viewing default settings for Privacy Users
- Enabling users to override the default notification settings
- Enabling users to request a sender to be approved
- Notifying users when an alias is changed
- Making your Acceptable Use Policy (AUP) available
- Defining Message Manager Administrators
- Adding Privacy Users

Defining custom settings

For the full functionality of Message Manager and its related services to be available, domain-specific custom settings must be selected, rather than global settings.

Once your organization is provisioned for Message Manager, certain actions are not possible within the management portal in the Email Security configuration pages. These are:

- You cannot revert a domain back to global settings, even if the option to do so is visible
- Using actions such as **Copy**, **Redirect**, and **Block and Delete** is not possible, even if they appear in the drop-down list of actions.

If you select try to define these settings, an error message is displayed. Select the **Back** button in your Web browser to clear the error message, and set the custom settings, as required.

To define a custom setting

1. Select **Configuration** > **Message Manager**.
2. Select the required domain from the drop-down list at the top of the page.
3. Select the **Use custom settings** option.

If **Use Global Settings** is selected, options pertaining to individual domains are inactive. They can be seen but not amended for that domain, until you select the **Custom Settings** option.

Defining default notification settings

You can define the following settings for notifications for your users:

- Whether they receive welcome messages and notifications
- The frequency of notifications
- The default language of notifications and the Message Manager screens

Select a domain or use global settings, depending on your requirements.

Note: You cannot turn off notifications for Privacy Users.

To define default notification settings

1. Click **Configuration** > **Email Services** > **Message Manager**.
2. In the **New Account Defaults** section of the **Settings** tab, the following settings are available:

Setting	Description
Users receive welcome messages and summary notifications	Message Manager quarantines messages and protects users without any intervention being required from them. Check the **Notifications** box for your users to receive: ■ A welcome email that notifies them that Message Manager is available to them ■ Emails that notify them when there are messages to review or release Message Manager
Summary notifications frequency	When there are messages in Message Manager that users can review or release, they can be sent notification emails. Select an appropriate frequency for these notification emails from the drop-down list. Set the frequency at an appropriate level, so that the notifications are not a nuisance, but the user is alerted adequately to quarantined emails. This setting only affects the default configuration for new accounts. If this setting is changed after the activation of Message Manager, it does not affect existing accounts.
Default language for notifications	A range of languages is available for the Message Manager user interface and notification emails. The default language can be set for new users using the drop-down list. A user can change the language to any of the available languages when they log on to Message Manager. The languages that are currently available are: ■ English ■ French ■ German ■ Italian ■ Japanese ■ Spanish

See "Enabling users to override the default notification settings" on page 17.

Enabling users to access Message Manager

Message Manager enables your users to see the emails that the following services have quarantined:

- Email AntiSpam
- Email Image Control

- Email Content Control

Users can only view messages for the services that have been provisioned for access in Message Manager, and those that are selected in the management portal.

To select the Email Security services for Message Manager to operate with

1. Click **Configuration > Email Services > Message Manager**, and navigate to the **Account Controls** section of the **Settings** tab.
2. Under the **User Message Manager access** heading, select the required service(s).

Note: The **User Message Manager access** setting does not apply to Privacy Users. Privacy Users have access to all of their inbound quarantined email in Message Manager. The setting cannot be turned off for them.

Viewing default settings for Privacy Users

For organizations with the Privacy Users facility enabled, a **Privacy Users** tab is available in the management portal.

Some settings cannot be configured in the management portal. These settings are set up to the client's requirements for each domain when the Message Manager service is provisioned.

To view default settings for Privacy Users

1. In the management portal, select **Configuration** > **Email Services** > **Message Manager**.
2. Select the domain you are interested in.
3. In the **Privacy Users** tab under the **Privacy User Configuration** section, you can see the default settings.

   The default Privacy User settings are described in the following table.

Table 2-1 Non-configurable settings fro Privacy Users

Setting	Description
Default privacy user filtering configuration	The **Default privacy user filtering configuration** setting is set to *Opted In* or *Opted Out*: ■ *Opted In* – your users' email is scanned according to the services that you subscribe to and that you have selected to operate with the Message Manager service. Users can opt out of having their email scanning in Message Manager. ■ *Opted Out* – your users' email is NOT scanned even if you subscribe to Email Security services and have selected them to work with the Message Manager service. Users can opt in to having their email scanned in Message Manager.
Paired administration	The **Paired administration** setting is set to *Active* or *Inactive*. To enable Administrators to perform a restricted set of activities, **Paired Administration** needs to be set to *Active*.
Quarantine period	The quarantine period is set to the agreed period when your service is provisioned. By default, this period is 45 days for Privacy Users (and 14 days for standard users). Any quarantined email that has been held on the Message Manager system for this period is deleted automatically when the quarantine period has elapsed

See "Privacy Users" on page 9.

Enabling users to override the default notification settings

You can enable users to change their notification settings within Message Manager.

Note: This setting only affects the default configuration for new accounts and does not affect existing accounts.

To enable users to change the default notification settings

1. Click **Configuration > Email Services > Message Manager** and select the **Settings** tab.
2. In the **Account Controls** section, under the **User notification control** heading, check the **User can override notification defaults** box.

See "Defining default notification settings " on page 14.

Enabling users to request a sender to be approved

The **Approved Senders Request Facility** setting determines whether users can request that the sender of a quarantined email is added to the organization's global approved senders list. If this facility is enabled, when a user releases a message from Message Manager, the user can request that the sender is added to the list.

This option is only relevant for domains without User Settings enabled. On domains with user settings, users can approve senders themselves without an administrator's approval.

To enable users to request approved senders

1. Select **Configuration > Email Services > Message Manager** and select the **Settings** tab.
2. In the **Approved sender request facility** section, check the **Message Manager users can send an email request to approve a sender** checkbox.
3. Enter the address to which approved senders list requests are sent.

   This address should be the address of the person who is responsible for managing the approved senders lists in the management portal.
4. Click **Save & Exit**.

   The address is validated to check that it is a valid email address format and that its domain belongs to your organization.

Notifying users when an alias is changed

When administrators change settings relating to the aliases of a user, the user can be notified.

Aliases are used to:

- Direct all quarantined email that is sent to a user with multiple email addresses to a single Message Manager account.

- Manage the quarantined email that is sent to a distribution list email address, using a single Message Manager account.

By their nature, aliases operate in the background and users check any quarantined email using Message Manager as required. If an Administrator makes a change to an alias, it may be useful for the users who are affected to be notified.

To notify users when a change is made to an alias

1. Select **Configuration > Email Services > Message Manager**.
2. Select **Settings**.
3. In the **Aliases** section, check the box **Users are always informed of operations by administrators on aliases**.
4. Click **Save and Exit**.

Making your Acceptable Use Policy (AUP) available

Your organization's Internet and Email Acceptable Use Policy (AUP) is an important document. You can give your users easy access to its URL P. You can also select where and to whom the link is visible.

Note: At present, the AUP URL is not displayed anywhere in the Message Manager screens. The option is included here as it may be possible in the future.

To make your Acceptable Use Policy available

1. Select **Configuration > Email Services > Message Manager**.
2. With **Global Settings** selected, open the **Settings** tab.
3. In the **Acceptable Use Policy** section, check **Users can view your company Acceptable Use Policy (AUP)**.
4. In the **Specify URL link to your AUP** box, enter the URL for the location of the AUP document.
5. Specify where and to whom the link is visible.
6. Click **Save and Exit**.

Defining Message Manager Administrators

Administrators can be set up for use within Message Manager.

Message Manager administrators can review and release messages for users, depending on their global and their domain settings.

You can enter up to 65 Message Manager Administrator email addresses.

Note: Any two Message Manager Administrators can perform Paired administration on Privacy Users' accounts

---

To define a Message Manager Administrator

1. Select **Configuration > Email Services > Message Manager**.
2. In the **Administrators** tab, enter the email address of the Message Manager Administrator.

   Multiple addresses must be separated with a semi-colon.
3. Click **Add**.

   The email address is added to the list of Administrators.

To delete a Message Manager Administrator

1. Select **Configuration > Email Services > Message Manager**.
2. In the **Administrators** tab, check the box to the left of the email address in the list of administrators, and click **Delete Selected**.

See "Defining custom settings" on page 13.

Adding Privacy Users

Organizations with the Privacy Users facility enabled must set up their Privacy Users for each domain.

You can add Privacy Users manually in ClientNet or upload multiple Privacy Users by a TXT or a CSV file.

To add a Privacy User manually

1. Select **Configuration > Email Services > Platform**.
2. Select the required domain from the drop-down list at the top of the page.
3. Select the **Privacy Users** tab.

   Click **Search** to see the registered email addresses for the domain in the left box. Your existing Privacy users are listed in the right-hand box. Only the first 500 users are displayed in each box. If you have many users, use the search box to locate the required user.

4 Select the email address of your privacy user from the **Registered Email Address** list, and click **Add**.

The user is listed in the **Privacy Users** box.

5 Click **Save and Exit**.

Uploading multiple Privacy Users

1 Create a text or CSV file with one email address per line. Use the following format:

```
exampleuser1@exampledomain.com
exampleuser2@exampledomain.com
```

2 Save the file locally. For example, *c:\privacy_users.txt* or *c:\privacy_users.csv*

3 Select **Configuration > Email Services > Platform**.

4 Select the required domain from the drop-down list at the top of the page.

5 Select the **Privacy Users** tab.

6 Click **Upload Privacy Users** and browse to the file that you created in step 2.

7 Select the required option either to:

- Delete the existing email addresses that are held by Email Security and replace them with the email addresses that you upload.
- Merge the uploaded addresses with those already in the list.

8 Click **Upload**.

The upload starts. If the list of Privacy Users is very long, the upload may take a considerable time.

9 Click **Save and Exit**.

Chapter 3

What's new in Message Manager?

This chapter includes the following topics:

- What's new in Message Manager

What's new in Message Manager

- You can see from the Message Manager **Summary** page whether a quarantined email contains an attachment.
  A column contains an attachment icon if that an email has an attachment. The file name of the attached file is displayed to the right of the attachment icon (up to 30 characters). You can see at a glance the file name that is contained within an email to determine whether or not to release it. For instance, you may be less likely to release an EXE file than a DOC file. If there is more than one attachment, the **Filename** column says *more....*
  You can sort the **Summary** list by attachment file name.
- If Email Content Control triggered an email to be quarantined, the name of the rule that detected the email is shown in the **Summary** list. Knowing the rule that triggered the email to be quarantined helps you to determine if you can release the email.
  You can sort the **Summary** list by Email Content Control rule name, which may help you to look for a specific quarantined email.
- The search capabilities of Message Manager have been extended.
  You can search for the quarantined messages that a specific Email Content Control rule blocked. You can also search for an attachment by its file name.

- You can select an email address to release a quarantined email to an Administrator rather than to the intended recipient. The Administrator email address is defined in the Message Manager section of ClientNet.
  As an Administrator, you may want to inspect an email that is quarantined. You can release the email to a specific email address. You can then release the email to the intended recipient if required.
  As a user, you may want to release a copy of a quarantined email to an Administrator to inquire why the email was blocked.