



Email Filter-Only Service

July 1, 2010

Table of Contents

| | |
|--|---|
| Introduction..... | 3 |
| How OpenSRS email filtering works..... | 3 |
| Implementation steps | 4 |
| Step 1: Logging in to the MAC..... | 4 |
| Step 2: Creating a new domain inside the MAC..... | 5 |
| Step 3: Creating anti-spam filter-only accounts | 6 |
| Creating a single filter-only mailbox | 6 |
| Creating filter-only accounts in bulk | 6 |
| Step 4: Setting up your anti-spam portal..... | 7 |
| Step 5: Informing your users about the new anti-spam system..... | 7 |
| Step 6: Updating the MX record in the domain name’s DNS servers..... | 8 |
| Step 7: Ensuring that mail is accepted by your mail server..... | 8 |
| Additional documentation resources | 8 |

Introduction

OpenSRS offers an effective, low-cost email filtering service specifically designed for the needs of service providers. The Email Filter-Only service stands between your email servers and the Internet, acting as a gateway that protects your users and infrastructure from email threats like spam and viruses.

How the OpenSRS Email Filter-Only Service works

OpenSRS Email Filter-Only Service evaluates each and every email message using the latest in scanning technology to make a determination as to whether the content of the message is legitimate and wanted, or contains spam, phishing attacks, or a virus payload.

If the message is deemed legitimate, it's delivered to the recipient's email inbox. If the message is deemed spam, the subject line can be tagged, and a custom configurable header can be added to the message for delivery by your existing mail server to your users' inboxes, or designated spam folder. You may also chose to have spam delivered to a web-based Spam Quarantine where the recipient can periodically login to view and review messages flagged as spam. If a message contains a virus, it is simply discarded, protecting your users from infection.

Implementation steps

The steps to implement the Email Filter-Only system are as follows:

- 1 Log in to the *Mail Administration Center*, often referred to as the MAC.
- 2 Create a new domain profile within the MAC for the domain name being filtered.
- 3 Create email addresses using the **New Filter-Only** or **Bulk Create** options in the MAC.
- 4 Set up access to the web-based Spam Portal using the domain name's DNS servers, implementing a CNAME record to point to the OpenSRS Email Service system.
- 5 Educate your users about the new anti-spam system.
- 6 Change the MX record in the domain name's DNS servers to the OpenSRS Email Filter-Only Service. This will force incoming email to pass through the OpenSRS Email Filter-Only Service anti-spam system.
- 7 Test email accounts on your system to see if email is flowing through the OpenSRS Email Filter-Only Service and then to your mail server.

Step 1: Logging in to the MAC

You need to log into the Mail Administration Center to create and configure the Email Filter-Only system for your mail server.

To log in to the MAC

1. Use your browser to navigate to the MAC:

`https://admin.<cluster>.hostedemail.com`

OpenSRS employs two email clusters: A and B. If you do not know which cluster you are on, contact your account manager. Currently the majority of users are on cluster A, which is located here:

`https://admin.a.hostedemail.com`

2. Enter your administrator email address and password.
3. Click **Log In**.

To learn more about the Mail Administration Center see the *Mail Administration Center (MAC) User's Guide* located at <http://www.opensrs.com/resources/email/documentation>

Step 2: Creating a new domain inside the MAC

You need to create a new domain profile in the MAC so that the OpenSRS Email Filter-Only System understands that it should handle its mail flow. This is also where you specify the options that apply to the entire domain, such as the location of your mail server and the email addresses or systems that should not be examined by the OpenSRS Email Filter-Only System.

To create a new domain

1. In the navigation pane, click **New Domain**.
The **New Domain** page appears.
2. Complete the following fields:

| Field | Definition |
|--------------------------|--|
| Domain Name | The name of the new domain. This field is mandatory. |
| Domain Aliases | Enter any domain aliases, separating multiple domains with commas. Note: You must set a domain aliases' DNS record. Consult the <i>DNS Configuration Guide</i> located at http://www.opensrs.com/resources/email/documentation for information on setting DNS records. |
| Filteronly Spam Delivery | Choose the way in which you want spam messages to be handled by the OpenSRS email filters: <ul style="list-style-type: none"> • Use Default—Use the Filter-Only Spam Delivery option set at the Company level. • Quarantine—Do not deliver spam messages to the Reseller's mail server. • Pass Through—Allow spam messages to be delivered to the Reseller's designated mail server. |
| Filteronly MX Host | The MX Host address is the target mail server to which filtered, spam and virus free email will be delivered. This can be either a hostname or IP address and must also include the inbound port that accepts connections (usually port 25), for example, mail.mymail server.com:25 |
| Spam Header | The tag that will be assigned to the header of spam messages. The format for the header must be X-[<i>Capital letter</i>]anything[:][<i>Description</i>], for example, X-Spam: Spam detected . This tag must be in a valid email header format. |
| Spam Tag | If defined, the tag is prepended to the subject of all spam. |
| Spam Folder | Default is <i>Spam</i> . Important: Do not change this setting; it is only applicable to the full email service. |

| Field | Definition |
|---------------------|---|
| Spam Blocking Level | Choose the aggressiveness level for the spam filtering. Choosing a level other than Normal causes the filtering engine to be more aggressive in labeling mail as spam; however, it may also result in more false positives. Using Default uses the Company profile setting. |

3. Click **OK** to create the domain profile.

Step 3: Creating anti-spam filter-only accounts

All email addresses that exist in your mail server must have accounts created in the OpenSRS Email Filter-Only System. This enables the anti-spam filter, and allows valid email to pass through to your mail server. You can create accounts in two ways: create individual account using **New Filter-Only** command, or create multiple accounts at once using the **Bulk Create** tool.

Creating a single filter-only mailbox

A filter-only account functions as a spam quarantine, trapping all spam and allowing good mail to flow through to a target account on your mail server.

To create a new filter-only mailbox

1. In the navigation pane, click **New Filter-Only**.
2. Complete the following fields:
 - **New Filteronly for**—Choose the domain for this account from the drop-down menu.
 - **Mailbox name**—Specify the email address that will be subject to spam filtering.
 - **Password**—Specify the password to log in to the user’s Quarantine Portal.
 - **Password (again)**

The rest of the fields are optional; see “Creating a new mailbox account” in the *Mail Administration Center User’s Guide* for an explanation of these fields.

3. Click **OK**.

Creating filter-only accounts in bulk

Bulk Create can be used to create any mailbox type including Filter-Only accounts.

To bulk create new accounts

1. In the navigation pane, click **Bulk Create**.
2. Click the **data** tab.
3. Enter the account information in the text area. Each Filter-Only account requires a single line as follows:

[user@domain.com],filter,[user_password],,,[Firstname],[Lastname],

Note: Firstname and Lastname are optional

Example:

john@mydomain.com,filter,abc123!,,,John,Moore,

You can click the **help** tab for an explanation and examples of the correct data format.

4. Optionally, click the checkbox **Create domains as needed**. When this box is checked, if you try to create an account for a domain that does not already exist, the domain profile is created.
5. Click **Process**.

Note: Creating domain profiles using the Bulk Create tool does not set the **Filter MX Host** variable; each domain profile needs to be updated with the required value.

Step 4: Setting up your anti-spam portal

If you chose to have the Email Filter-Only system quarantine spam, you need to supply your users with an interface where they can log in to view the captured spam. This tool allows them to release emails that were captured as spam in error.

If you set the **Filteronly Spam Delivery** to **Pass Through** then you do not need to give your users access to a spam portal. Domains that use the **Pass Through** setting deliver all spam to your server, and add additional information to emails identified as spam.

To create a portal, create a CNAME record in your DNS server that points to a special hostname based on the domain name you are having filtered. For the domain name **example.com**, the anti-spam portal located at **portal.example.com** points to **mail.example.com.cust.[cluster].hostedemail.com**. The DNS record looks similar to:

```
portal.example.com in cname mail.example.com.cust.[cluster].hostedemail.com
```

You can use either **portal** or **spam** as part of the hostname that points to the web based spam portal. Using either of these terms ensures that the portal login button displays **Log in to Spam Quarantine**. Using any other term causes the login button to display **Log in to Webmail**.

Step 5: Informing your users about the new anti-spam system

You need to inform the users of your email system that changes will be made to the flow of email to their account. If you are taking advantage of the **Quarantine** system, they need to know where you have set up the Anti-Spam Portal and their username and password. They should also be given instructions on how to manage Safe and Deny Sender Lists and how to release quarantined.

If you have set the system to **Pass Through** spam to your users, they should be informed how this spam can be identified, either by a modified Subject line or extra information in the Header of the email.

Step 6: Updating the MX record in the domain name's DNS servers

Once the accounts have been created in the MAC and the **Filteronly MX Host** has been set to the destination mail server, you need to update the MX record in the DNS server for the domain name. This causes all incoming mail for the domain name to be delivered to the OpenSRS Email Service anti-spam system before being delivered to the destination mail server. If you are using the OpenSRS DNS service, you can find instructions on how to change the MX record in the *DNS Configuration Guide* located at <http://www.opensrs.com/resources/email/documentation>. If you are using another DNS service, ask the Support staff of that service how to update the MX record.

Example MX record:

```
example.com. IN MX 0 mx.example.com.cust.[cluster].hostedemail.com.
```

Step 7: Ensuring that mail is accepted by your mail server

Once you've changed your domain's MX record to point to the OpenSRS Email Filter-Only Service, send some mail through to test its delivery to your mail server. If the email is not received, check the web based Spam Quarantine Portal to see if it was flagged as spam. You can also consult the connection and delivery logs of your mail server to determine the cause of the problem.

Certain mail servers may need to be configured to accept mail from our Filter-Only service. Connections will be received from **hostedemail.com**. Depending on the mail server being used, you may need to allow mail relaying from **hostedemail.com**, or you may need to configure the mail server to regard mail for the domain as being handled locally.

Additional documentation resources

The OpenSRS.com web site contains documentation for all OpenSRS products and services including the Email and Email Filter-Only systems. The documentation is found at the following location:

<http://www.opensrs.com/resources/email/documentation>