Postini Message Security

Using Postini with Google Apps Education Edition

Google Inc.
1600 Amphitheatre Parkway
Mountain View, CA 94043
www.google.com

July 9, 2010

Google, the Google logo, Google Apps, Google Apps Mail, Google Docs, Google Calendar, Google Sites, Google Video, Google Talk, Gmail, Google Message Filtering, Google Message Security, Google Message Discovery, Postini, the Postini logo are trademarks, registered trademarks, or service marks of Google Inc. All other trademarks are the property of their respective owners.

Use of any Google solution is governed by the license agreement included in your original contract. Any intellectual property rights relating to the Google services are and shall remain the exclusive property of Google, Inc. and/or its subsidiaries ("Google"). You may not attempt to decipher, decompile, or develop source code for any Google product or service offering, or knowingly allow others to do so.

Google documentation may not be sold, resold, licensed or sublicensed and may not be transferred without the prior written consent of Google. Your right to copy this manual is limited by copyright law. Making copies, adaptations, or compilation works, without prior written authorization of Google. is prohibited by law and constitutes a punishable violation of the law. No part of this manual may be reproduced in whole or in part without the express written consent of Google. Copyright © by Google Inc.

Google provides this publication "as is" without warranty of any either express or implied, including but not limited to the implied warranties of merchantability or fitness for a particular purpose. Postini, Inc. may revise this publication from time to time without notice. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions; therefore, this statement may not apply to you.

Using Postini Message Security with Google Apps Education Edition

Overview

Postini Message Security for Google Apps provides additional security features and controls for Google Apps Gmail.

This guide shows you how to use Postini Message Security to meet common needs for Google Apps Education Edition customers, including:

- **Email policies just for students**: Set up different user organizations, such as groups of students, faculty, or IT administrators, and apply specific email policies.
- **Blocking external mail to your students**: Allow only internal or specified users to send mail to users in your Google Apps domain, therefore blocking external senders from mailing your users.
- **Limiting messages your students can send:** Help limit students from sending mail outside of your Google Apps domain.
- **Blocking certain types of message attachments**: Filter messages that contain specific file attachments, such as MP3 or movie files.
- **Email signatures for all your students or faculty:** Set up a standard email footer for outbound mail for your users.
- **Limiting exposure to quarantined junk messages**: Turn off the Quarantine Summary, which is the daily message sent to users that lists their messages quarantined by the Postini service. The Quarantine Summary shows the titles of messages (you may not want your students to see titles of junk messages) and allows users to deliver quarantined messages.

Getting Started

Postini Message Security for Google Apps provides additional security features and controls for Google Apps Mail. See the Service Overview in the Help Center for more information on Postini features and how they work.

The Postini Message Security service is available with:

- Google Apps Education Edition: K-12 (primary or secondary education) institutions may also be eligible for Postini Message Security for Google Apps at no cost. See the Help Center for more information.
- Google Apps Premier Edition: Postini Message Security for Google Apps is included.

For an additional cost, you can upgrade your service to **Message Discovery**, which provides an archive of all messages for your domain. See Postini Services for Google Apps for more information and pricing.

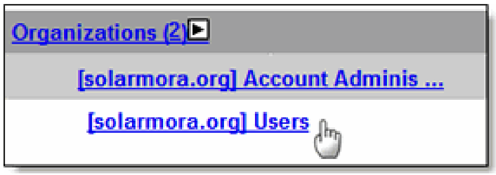
To activate the Postini service:

In your Google Apps control panel Dashboard page, under **Service Settings**, click **Add more services**, and choose **Postini services** to get started with the service and begin your activation. See the Activation Guide in the Help Center for step-by-step information.

During activation, your email is delivered as usual with no interruption, and the activation wizard guides you through the process step-by-step. Your users are automatically added and synchronized with the service. After activation, you can follow the next steps in this guide to configure settings and services for your users.

Create an organization for your staff

When you activate your service, your Postini service has two organizations that contain your users:

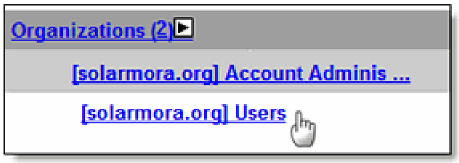


- **Account Administrators org**: The top-level organization, which contains the account administrator's account (the initial administrator specified during activation of the service) and the Default User (a user account template).
- **Users org**: The second-level organization, which contains **all the user accounts** that existed in Google Apps when you activated the service. All new accounts you add to Google Apps are automatically placed in this org.

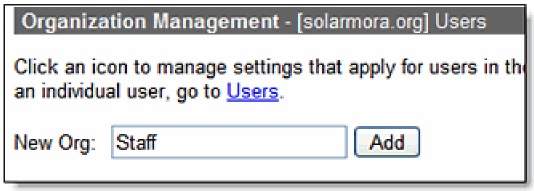
You may want your staff to have different policies than your students. For example, you may limit mail to your students from senders in your organization only, while your staff can receive mail from any domain.

To tailor service differently for another group of users, create a new org for them. This step creates an organization for your staff, and shows you how to move their user accounts to the new organization.

1. Go to **Orgs and Users** > **Orgs**, and click the **"Users"**, under which you want to add the new *sub-org*.



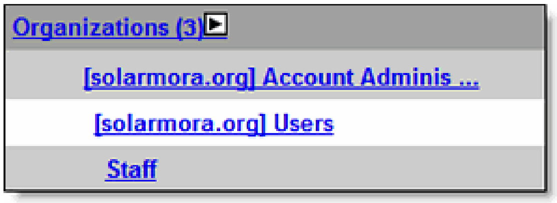
2. On the "Users" **Organization Management** page, type a name for the org in the **New Org** form (100 characters or less), such as "Staff". Then click **Add**.


Organization Management - [solarmora.org] Users

Click an icon to manage settings that apply for users in th
an individual user, go to Users.

New Org: Staff

The name in the gray bar changes, indicating that you're now looking at your new org's settings.



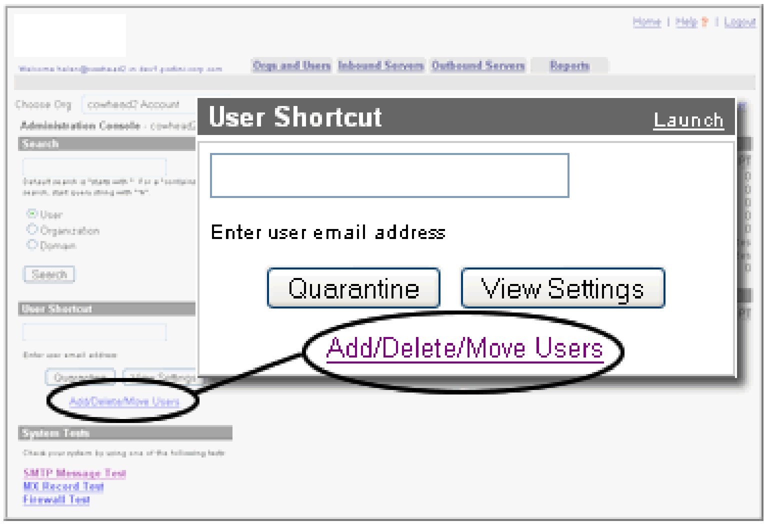
Organizations (3)

[solarmora.org] Account Adminis ...

[solarmora.org] Users

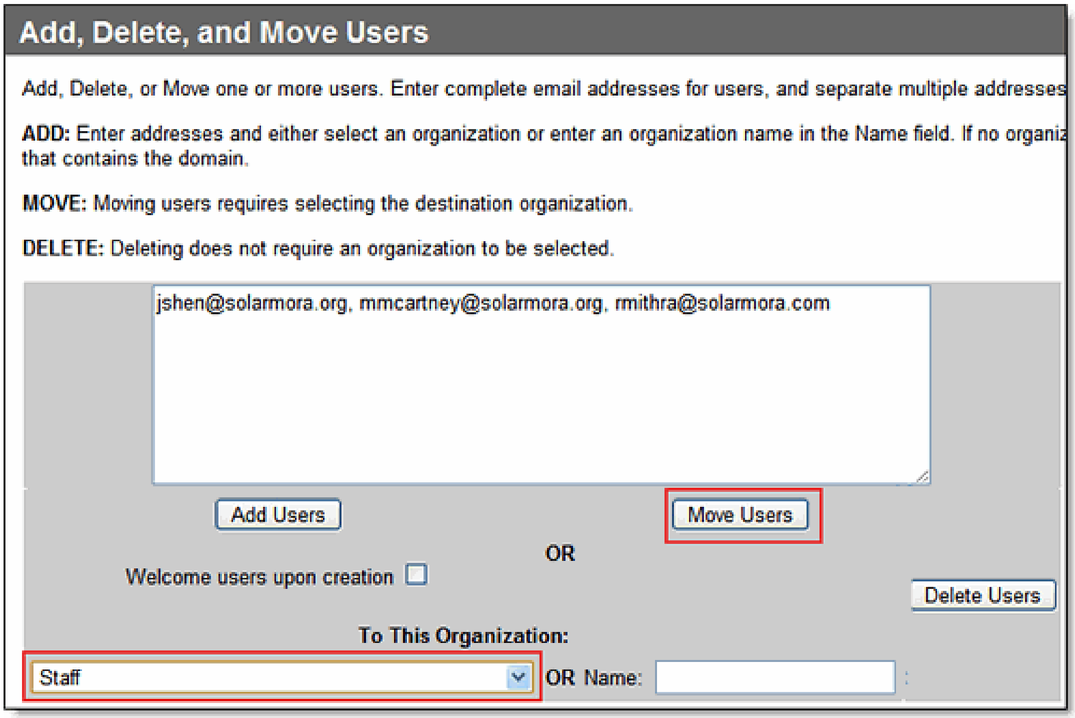
Staff

3. Next, move your staff users to the new org. In the Administration Console’s **Home** page, click the **Add/Delete/Move Users** link, just above the System Test links.



4. On the **Add, Delete, and Move Users** page, enter addresses of your staff. Separate addresses with a comma or put them on a separate line. Each user should already have an email account in your Google Apps Edu domain.

Tip: Enter several users at once by pasting their addresses from a text file or user database.



Add, Delete, and Move Users

Add, Delete, or Move one or more users. Enter complete email addresses for users, and separate multiple addresses

ADD: Enter addresses and either select an organization or enter an organization name in the Name field. If no organiz that contains the domain.

MOVE: Moving users requires selecting the destination organization.

DELETE: Deleting does not require an organization to be selected.

jshen@solarmora.org, mmcartney@solarmora.org, rmithra@solarmora.com

Welcome users upon creation □

To This Organization: Staff

OR Name:

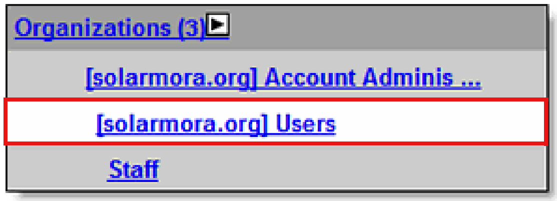
5. Leave **Welcome users upon creation** unchecked.

6. Move your users by choosing the “Staff” org you created from the list at the bottom of the panel.

7. Click the **Move Users** button.

   Each user receives service settings from the organization, and default filter levels from the org’s Default User.

The next steps in this guide refer to making changes to the settings in the **Users** organization, which contains all of your *students*.



For more information on user organizations, see the Organizations chapter in the ***Administration Guide***.

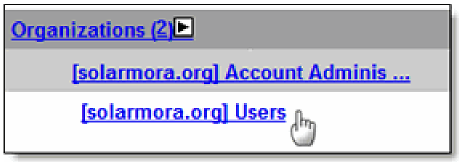
Add Your Approved Senders

Before limiting your incoming mail to your domain only, you may want to add certain senders to the **Senders Lists**, which bypass the inbound Content Manager filters. Approved senders typically include:

- Trusted partners or organizations. For example, another school or group that you want to allow to send messages to your students.
- Automated email notifications sent by Google. For example, your Google Calendar appointment reminders or Google Site update notifications.

Set up Approved Senders

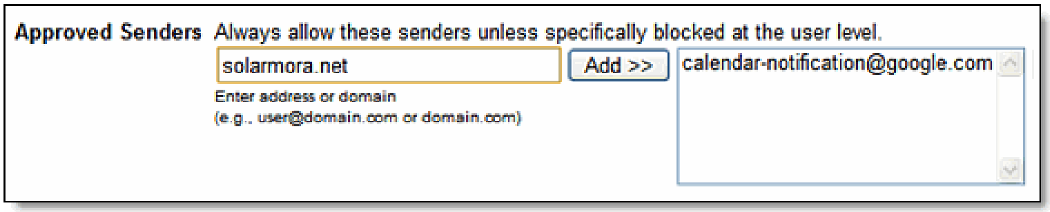
1. Access the Administration Console:
    a. Log in to Google Apps using your administrator account.
    b. On the Google Apps dashboard, click Postini services.
    c. Click System Administration.
2. Go to Orgs and Users > Orgs, and then select the organization that has your **students** (not your staff or faculty). In this procedure, this is your **Users** organization.



3. On the org's **Organization Management** page, scroll down and click **Sender Lists**.
4. On the **Sender Lists** page, enter the Google notification addresses and your trusted sender addresses or trusted domains that apply for all users in this org, in the **Approved Senders** field, and click **Add**.

Approved senders addresses for Google notifications:

Notification	Address
Google Calendar reminders	calendar-notification@google.com
Google Sites updates	noreply@google.com



Approved Senders Always allow these senders unless specifically blocked at the user level.

solarmora.net

calendar-notification@google.com

Enter address or domain
(e.g., user@domain.com or domain.com)

WARNING: We strongly recommend that you do not add your own domain/addresses or popular domains to the Approved Senders list. Spammers routinely spoof these domains to bypass the message security service filtering. Also, the service's anti-spam heuristics can recognize legitimate messages from popular domains and minimize any false positives.

For more information on Senders lists, see the Approved and Blocked Senders chapter in the ***Administration Guide***.

Set up a Content Manager Filter

Postini Message Security includes Content Manager, which you can use to create custom filters based on a message’s content, senders, and recipients.

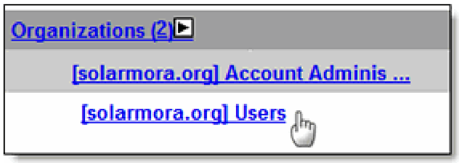
This section describes how to use Content Manager to:

- Prevent users outside of your domain from sending mail to your students.
- Reduce the potential for students to send mail outside for your domain. Note: At this time, it’s not possible for Content Manager to completely prevent users from sending messages outside of their domain.

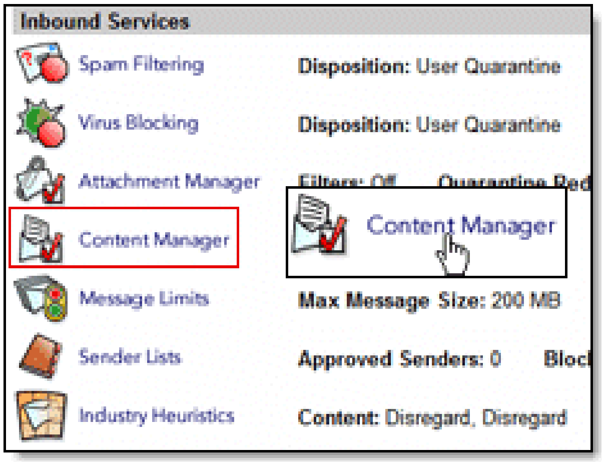
You can also configure Content Manager to block specific words or profanity. See the ***Administration Guide*** for instructions.

Set up Content Manager

1. Access the Administration Console:
   a. Log in to Google Apps using your administrator account.
   b. On the Google Apps dashboard, click Postini services.
   c. Click System Administration.
2. Go to Orgs and Users > Orgs, and then select the organization that has your **students** (not your staff). In this procedure, this is your **Users** organization.

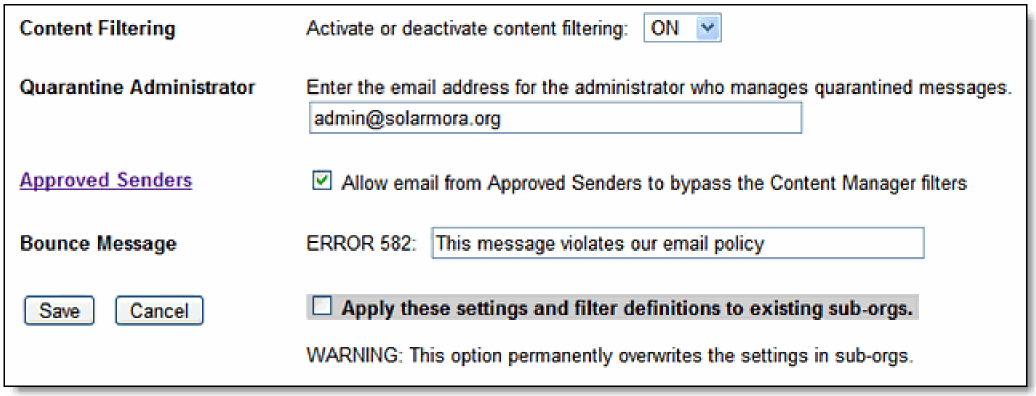


3. On the **Organization Management** page, under **Inbound Services**, click **Content Manager**:



Spam Filtering — Disposition: User Quarantine
Virus Blocking — Disposition: User Quarantine
Attachment Manager — Filters: Off Quarantine Red
Content Manager
Message Limits — Max Message Size: 200 MB
Sender Lists — Approved Senders: 0 Bloc
Industry Heuristics — Content: Disregard, Disregard

4. On the Inbound Content Manager page, click **Edit Settings**.



Content Filtering	Activate or deactivate content filtering: ON
Quarantine Administrator	Enter the email address for the administrator who manages quarantined messages. admin@solarmora.org
Approved Senders	☑ Allow email from Approved Senders to bypass the Content Manager filters
Bounce Message	ERROR 582: This message violates our email policy
Save Cancel	□ **Apply these settings and filter definitions to existing sub-orgs.** WARNING: This option permanently overwrites the settings in sub-orgs.

5. Set **Content Filtering** to **On**.

6. In the **Quarantine Administrator** field, enter the address of the administrator who should receive messages captured by content filters. (Content Manager sends these messages to the administrator's quarantine in the Message Center.)

7. Select "**Allow mail from Approved Senders to bypass Content Manager filters**" (so messages from the org's Approved Senders aren't blocked by content filters).

8. Leave the default text in the Bounce Message field, unless you want to change the message the senders receive if a filter returns their messages.

9. Leave the checkbox "**Apply settings to existing sub-orgs**" **unchecked**.

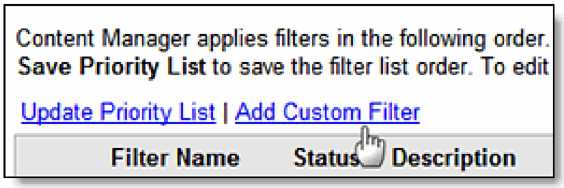
10. Click **Save**.

Create a Filter to Block Inbound Messages

Follow these steps to create a filter that limits incoming messages to only users in your domain:

1. Access the Inbound Content Manager page for your user organization, as described in "Enable Content Manager."

2. Click **Add Custom Filter**.



Content Manager applies filters in the following order.
Save Priority List to save the filter list order. To edit

3. In the **Filter Name** field, enter a descriptive name for the filter, for example, "Internal Inbound Mail" (the name can be up to 15 characters long).

4. Set **Filter Status** to **On**.

5. Under **Rules**, in the **Match** drop-down list, choose whether Content Manager executes this filter's disposition if an email message contains a match for any rule or all rules you specify.

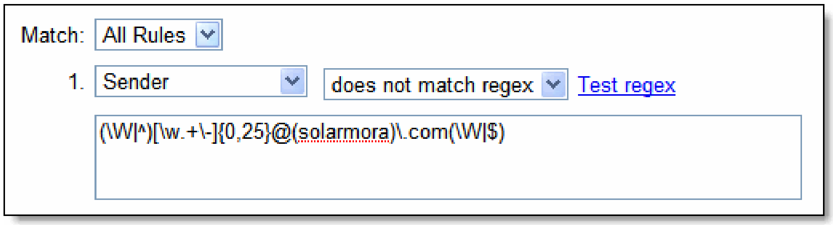
6. Specify up to three rules for this filter. For each rule, enter the following:

   - **Location**: The part of the message to scan. Note that Entire Message also scans content in file attachments. Choose "**Sender**".
   - Filter Type: Choose "**does not contain**".
   - Enter this value (a regular expression) and replace *yourdomain* with the name of your Google Apps Education Edition domain. If your domain ends in ".com" or another top-level domain, enter this instead of ".edu". This expression filters out any messages from senders who don't have an email address in your domain.

     ```
     (\W|^)[\w.+\-]{0,25}@(yourdomain)\.edu(\W|$)
     ```

     For example, if your organization's domain is **solarmora.edu**, you would enter:

     ```
     (\W|^)[\w.+\-]{0,25}@(solarmora)\.edu(\W|$)
     ```



Match: All Rules

1. Sender | does not match regex | Test regex

```
(\W|^)[\w.+\-]{0,25}@(solarmora)\.com(\W|$)
```

7. Under **Routing**, choose how you want messages that match the filter (in this case messages not sent within your domain) to be handled.

   Choose **Bounce**. This rejects the message and returns an error message to the sender. When an external users attempts to send a message to a user, the message will be bounced back with an error message of "582- This message violates our email policy".

8. Your administrator can also receive a copy of the message. This may be useful if you'd like to monitor who's attempting to send mail to your students.

   Under **Copy to Quarantine**, click **Add quarantine address** to send a copy of the message to another user:

   a. **Quarantine Administrator**: Sends a copy of the message to the Message Center quarantine of the administrator you specified when enabling Content Manager. We recommend that you **start with this option** so you can monitor which message trigger your filters.

   b. **Recipient**: Places the message in the recipient's quarantine in the Message Center (option available with only Inbound Content Manager). Do not choose this option as this will place the incoming messages that trigger the filter in the student's quarantine.

   c. **Other User**: Places the message in the quarantine of the user you specify. In the box, you can enter the email address of any user account that resides in a user organization for which you have Content Manager administrator authorization.

9. Click **Save**.

Create a Filter to Help Limit Outbound Messages

Content Manager can be configured to help limit students from sending messages to users outside of your domain. However, at this time, outbound messages sent to external users can bypass the Content Manager in two cases:

- A user sends a message to multiple recipients and includes both internal and external users on the “To” line of a message.
- A user includes an external recipient in the “Bcc” line of a message.

To help limit outbound messages, follow the basic steps for configuring Inbound Content Manager with two changes:

- To enable Outbound Content Manager: In the Organization Management page, under **Outbound Services**, click **Content Manager**, then follow the steps to configure.
- When creating a filter for Outbound Content Manager, set up the filter to check the **recipient** (instead of sender) field in step 6:
    - **Location**: The part of the message to scan. Choose “**Recipient**”.

For more information on how Content Manager works and additional uses, see the Content Manager chapter in the ***Administration Guide***.

Set up an Attachment Manager Filter

The Postini Message Security service includes Attachment Manager, which you can use to filter messages based on file attachment size and type. For example, you can block or quarantine MP3 files or movie files. You can set up attachment filters for both inbound and outbound email.

Set up Attachment Manager

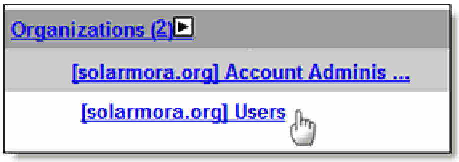
1. Access the Administration Console:

   a. Log in to Google Apps using your administrator account.

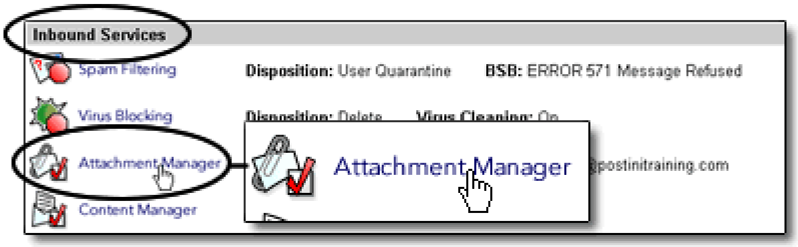
   b. On the Google Apps dashboard, click Postini services.

   c. Click System Administration.

2. Go to Orgs and Users > Orgs, and then select the organization that has your **students** (not your staff or faculty). In this procedure, this is your **Users** organization.



3. On the **Organization Management page**, click **Attachment Manager**, listed under **Inbound Services**.

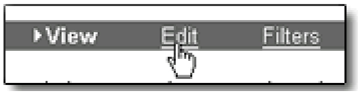


Disposition: User Quarantine BSB: ERROR 571 Message Refused

Disposition: Delete Virus Cleaning: On

@postinitraining.com

4. On the **Inbound Attachment Manager page**, click the **Edit** link, in the dark gray bar.



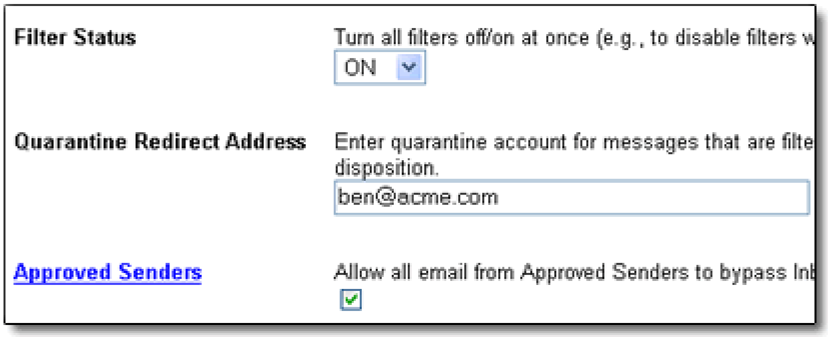
5. On Attachment Manager's **Edit page**:

   a. Set **Filter Status** to **On**.

   b. Enter the **address of an administrator** who should handle all messages quarantined by attachment filters.

   c. Check **Approved Senders** (so messages from the org's Approved Senders don't get blocked by attachment filters).

   d. Click **Save**.



Filter Status Turn all filters off/on at once (e.g., to disable filters w

ON

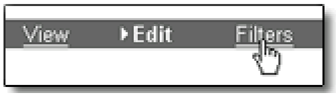
Quarantine Redirect Address Enter quarantine account for messages that are filte disposition.

ben@acme.com

Approved Senders Allow all email from Approved Senders to bypass Inb

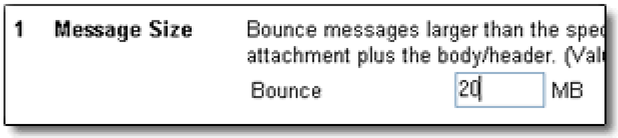
☑

6. Click the **Filters link** in the dark gray bar.



7. On the **Filters page**, enter a **Maximum Message Size** that users in this organization can receive. Messages with total attachments that exceed this limit will be bounced back to the sender.

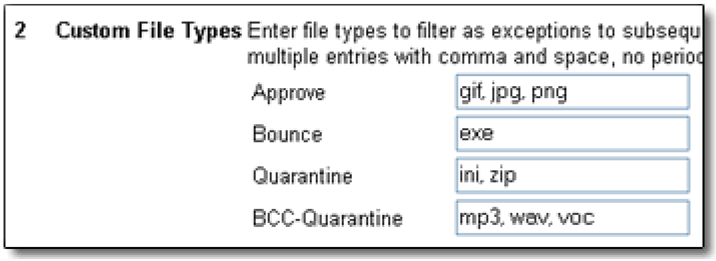
   Note: This changes the size limit for Postini filters. The size limit for Google Apps mail is not changed and still applies.



1 **Message Size** Bounce messages larger than the spec attachment plus the body/header. (Val

Bounce 20 MB

8. Under **Custom File Types**, enter file extensions in appropriate fields, depending on your desired *disposition* for messages containing those types of attachments (as described below). Separate each extension with a comma.



2 **Custom File Types** Enter file types to filter as exceptions to subsequ multiple entries with comma and space, no period

Approve	gif, jpg, png
Bounce	exe
Quarantine	ini, zip
BCC-Quarantine	mp3, wav, voc

Approve Skips all remaining Attachment Manager filters.

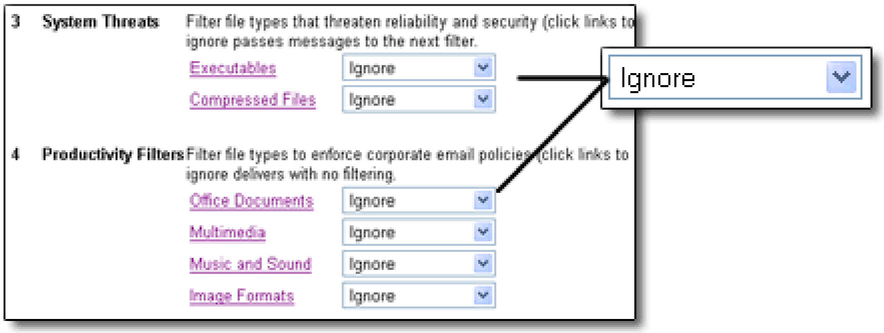
Bounce Rejects the message and returns the sender an error message.

Quarantine Diverts the message to the administrator Quarantine you specified above, without delivering it to the user.

BCC Quarantine (Blind Carbon Copy) Copies the message to the administrator Quarantine, but also delivers it to the recipient (if the messages passes through remaining filters). You therefore review the types of attachments users are receiving, without preventing people from receiving them.

NOTE: Custom filters override any subsequent attachment filters (under System Threats or Productivity).

9. Leave filters under **System Threats** and **Productivity** set to **Ignore**. Then click **Save**.



3 System Threats Filter file types that threaten reliability and security (click links to
ignore passes messages to the next filter.

Executables Ignore

Compressed Files Ignore

4 Productivity Filters Filter file types to enforce corporate email policies (click links to
ignore delivers with no filtering.

Office Documents Ignore

Multimedia Ignore

Music and Sound Ignore

Image Formats Ignore

To instead filter entire categories of file types, select a disposition for any category shown above. Just be aware that each category contains a lot of file types.

10. Leave “Apply settings and filters to existing sub-orgs” unchecked.

11. Click **Save**.

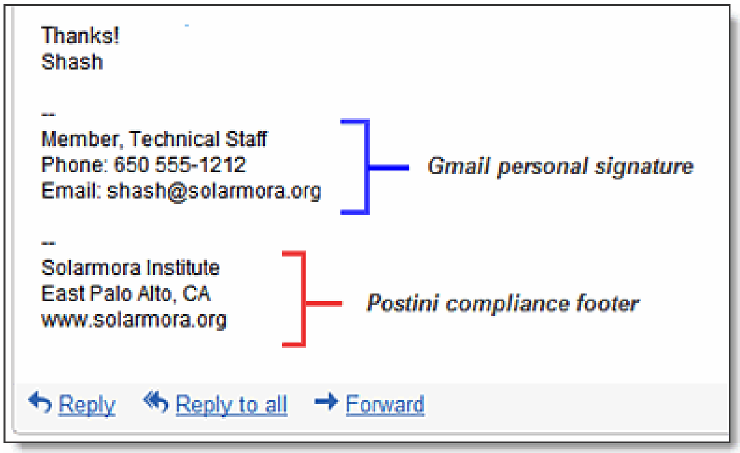
You can set up also filters for outbound attachments: On the **Organization Management page**, click **Attachment Manager**, listed under **Outbound Services**, and follow the previous steps to create an attachment filter.

For more information on how Attachment Manager works and additional uses, see the Attachment Manager chapter in the ***Administration Guide***.

Set up an outbound footer

Outbound messages can be configured with footer text that describes an email policy or standard address information. This *compliance footer* is added into the last existing text portion of a message after the user's personal signature (configured in Gmail).

Compliance footers are configured at the organization level. The compliance footer currently supports ASCII and English character sets only.



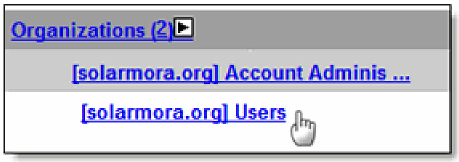
Thanks!
Shash

--
Member, Technical Staff
Phone: 650 555-1212
Email: shash@solarmora.org

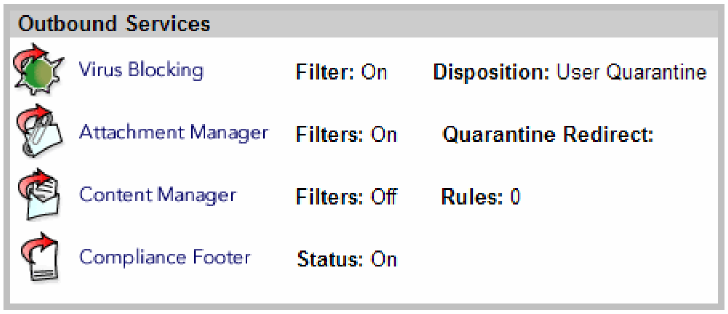
--
Solarmora Institute
East Palo Alto, CA
www.solarmora.org

Add a footer to outgoing Gmail messages

1. Access the Administration Console:
   a. Log in to Google Apps using your administrator account.
   b. On the Google Apps dashboard, click Postini services.
   c. Click System Administration.
2. Go to Orgs and Users > Orgs, and then select the organization that has your **students** (not your staff or faculty). In this procedure, this is your **Users** organization.



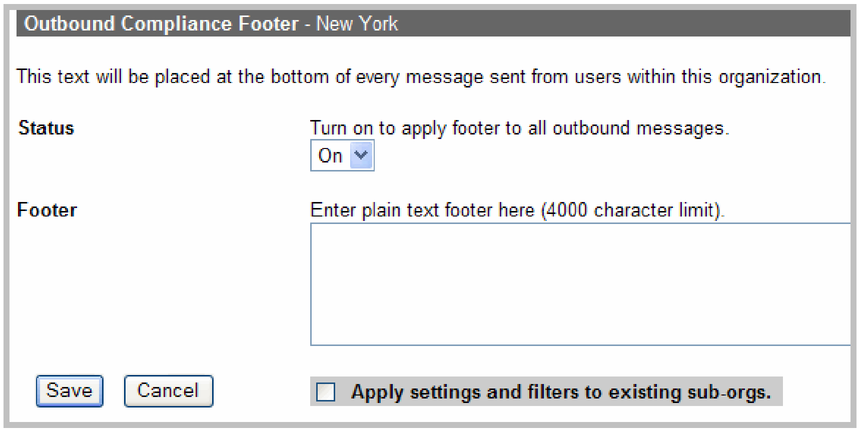
3. In the Organization Management page, scroll to the Outbound Services section, and click the Compliance Footer icon.



Outbound Services

Virus Blocking	**Filter:** On	**Disposition:** User Quarantine
Attachment Manager	**Filters:** On	**Quarantine Redirect:**
Content Manager	**Filters:** Off	**Rules:** 0
Compliance Footer	**Status:** On	

4. In the Outbound Compliance Footer page:
   - Set the footer Status to On.
   - Add the footer text. We recommend plain-text footers.
   - Choose whether to propagate the footer to sub-orgs.



Outbound Compliance Footer - New York

This text will be placed at the bottom of every message sent from users within this organization.

Status Turn on to apply footer to all outbound messages.
On

Footer Enter plain text footer here (4000 character limit).

□ **Apply settings and filters to existing sub-orgs.**

5. Click **Save**.

6. Once you have configured and enabled the compliance footer, you can test it by sending a message to another address, **not your own** (the footer does not appear when you send the message to yourself).

Formatting the Compliance Footer Text

The Outbound Compliance Footer is designed to be a text-only footer (no graphics or logos). However, it is possible to add some minimal HTML to the footer. If the Compliance Footer is added to an HTML-formatted message, any HTML in the footer is rendered as expected. If the footer is added to a plain-text or RTF message, the HTML is not rendered and the footer is displayed as plain text including the HTML code.

Also, if you do not include line breaks in the footer, it is displayed as one long string:

```
Sentence 1, Sentence 2, Sentence 3, Sentence 4....
```

To include line breaks, press `Enter` at each point where you would like a break:

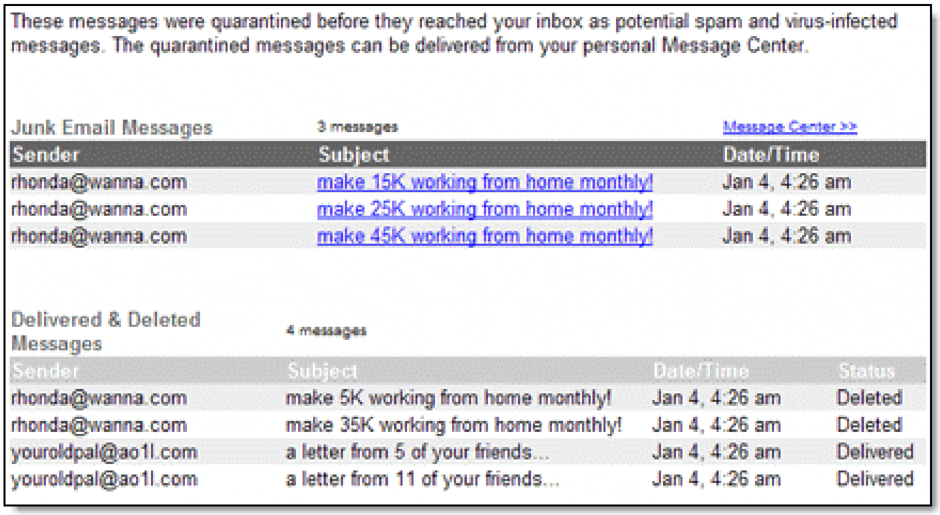
```
Sentence 1[press Enter]

Sentence 2[press Enter]
```

For more information about the outbound footer, see the Compliance Footer section in the ***Administration Guide***.

Turn off the Quarantine Summary

The Quarantine Summary is an email message that contains a list of any new messages that your message security service has quarantined for a user and a link to deliver the message to the user's Google Apps inbox. Users receive this message a maximum of once a day, depending on the frequency you select.

You may want to turn off the Quarantine Summary for students if you do not want them to see any junk message titles or to deliver quarantined messages to their Gmail inbox.



These messages were quarantined before they reached your inbox as potential spam and virus-infected messages. The quarantined messages can be delivered from your personal Message Center.

Junk Email Messages 3 messages Message Center >>

Sender	Subject	Date/Time
rhonda@wanna.com	make 15K working from home monthly!	Jan 4, 4:26 am
rhonda@wanna.com	make 25K working from home monthly!	Jan 4, 4:26 am
rhonda@wanna.com	make 45K working from home monthly!	Jan 4, 4:26 am

Delivered & Deleted Messages 4 messages

Sender	Subject	Date/Time	Status
rhonda@wanna.com	make 5K working from home monthly!	Jan 4, 4:26 am	Deleted
rhonda@wanna.com	make 35K working from home monthly!	Jan 4, 4:26 am	Deleted
youroldpal@ao1l.com	a letter from 5 of your friends...	Jan 4, 4:26 am	Delivered
youroldpal@ao1l.com	a letter from 11 of your friends...	Jan 4, 4:26 am	Delivered

Turn off the Quarantine Summary

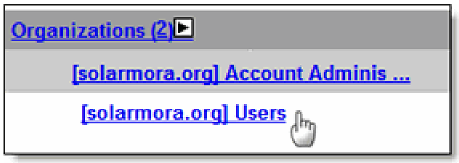
1. Access the Administration Console:

   a. Log in to Google Apps using your administrator account.

   b. On the Google Apps dashboard, click Postini services.

   c. Click System Administration.

2. Go to Orgs and Users > Orgs, and then select the organization that has your **students** (not your staff or faculty). In this procedure, this is your **Users** organization.

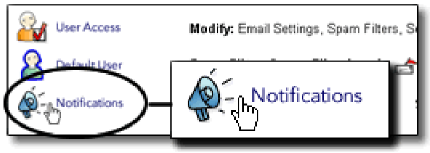


Organizations (2) ▶

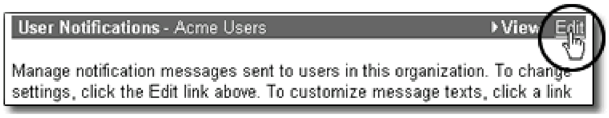
[solarmora.org] Account Adminis ...

[solarmora.org] Users

3. On the **Organization Management** page, scroll down to the bottom of the page, and click **Notifications**.



4. On the **User Notifications** page, click the **Edit** link, in the dark gray bar.



User Notifications - Acme Users ▸**View** Edit

Manage notification messages sent to users in this organization. To change settings, click the Edit link above. To customize message texts, click a link

5. On the User Notifications **Edit** page**:**
   a. Set **My First Spam** to **Off**.
   b. Set **Spam** to **Off**.
6. Click **Save**.

For more information on the Quarantine Summary and other notifications, see the Notifications chapter in the ***Administration Guide***.