Google Apps Email Security

by - Eric Curts

Table of Contents:

Watch the video training for this content here - Gmail Safety and Security for Schools - https://www.youtube.com/watch?v=DLOZq8kwVpU

Introduction

Google Apps provides a number of ways to manage and secure Gmail for your users. This is especially helpful for schools with students using Gmail. With Google Apps you are able to manage such things as:

- A bad word list to block messages that contain objectionable content.
- Ability to determine which domains (if any) students are allowed to send email to and receive email from.
- Ability to restrict students from sending email to email groups (listservs).
- Ability to restrict students from sending email to certain grade levels.
- And more...

Before you begin: Putting Users in Organizations

The email security settings for Google Apps are applied by Organization. Therefore it is important to consider the Organizations you set up for your users. For example, a common Organization structure for schools might be to create a Org named “Students” and then sub-Orgs for each grade level. Or if you have multiple buildings you may want to make an Org for “Students” then sub-Orgs for each building, then sub-Org below those for each grade level.

The key is to put your users in well defined groups since you will be applying the email rules and filters to each Organization.

Before you begin: Naming your Users

If you have already created your user accounts, this may not apply to you. However, if you are still setting up your users, now is a good time to consider the naming scheme. The reason for this is because many rules and filters rely on being able to match users based on an identifiable pattern. Even though rules are applied to Organizations, the rules are not able to match users based on the Org they are in.

For example, if all student usernames are simply the last name, followed by the first name, there will be no easy way to tell apart users from different grade levels. However, if you put their graduation year into their usernames, then you can use that to write rules and filters that match students based on their grade level.

For those that have already created users without considering this issue, all hope is not lost. Later we will see how you can use some tricks to match students even if their usernames do not distinguish them.

Accessing the Email Security Settings

To access and edit the email security settings, you have to have administrative privileges for your Google Apps domain. To access the settings for Email Security:

1. Log into your Google Apps Control Panel as normal
2. Click **Apps** in the Admin Console.
3. Then click **G Suite**
4. Then click **Gmail** in the list of services.
5. Finally click **User settings**.

Disabling Themes

By default Gmail allows users to change their theme by choosing from a wide range of images and colors. However, themes also allow the user to upload their own image or choose an image off of the Internet. If this is something you do not want your students to do, themes can be disabled as follows.

1. Select the Organization you wish to edit.
2. Scroll down through the **End User Settings** to locate the section titled **Themes**.
3. Simply uncheck the box for **Let users choose their own themes**.
4. Click **Save changes** at the bottom.

Disabling Automatic Forwarding

One simple setting to change is the ability for users to automatically forward their school email to a personal account. Often this is something you do not want students doing, to keep all school email discussions inside of your domain. There are other ways to block student email from leaving the domain (see later in the guide) but this method also removes the forwarding option in the first place.

1. Select the Organization you wish to edit.
2. Scroll down through the **End User Access** to locate the section titled **Automatic forwarding**.
3. Simply uncheck the box for **Allow users to automatically forward incoming email to another address**.
4. Click **Save changes** at the bottom.

Managing a Bad Word List

Google Apps allows you to reject or modify email messages that contain specific words you have listed as objectionable. This allows you to simply block the message from being delivered, or to send it to a different account, such as one that can be monitored by certain staff members (principals, guidance, etc.)

For a sample list of objectionable words, feel free to use this list we have created:
http://tiny.cc/bad-word-list

The list is about 100 words long. It used to be longer but over time we have tried to remove words that were giving us false-positives. That is, words that could be used in multiple ways, including proper usage.

To access the settings for a bad word list do the following:

- Select the Organization you wish to edit.
- Scroll down through the settings to locate the section titled **Compliance**.
- In the **Compliance** section, find the entry titled **Objectionable content**.
- Hover your mouse over this section and click **Configure** or **Edit** (if there are already settings).

In Section #1, you will choose which messages to affect:

- Your options include:
    - **Inbound** (email coming in from outside of the domain)
    - **Outbound** (email being sent to outside the domain)
    - **Internal - sending** (email being sent to another user within the domain)
    - **Internal - receiving** (email coming from another user within the domain)
- Select all four options to be safe.

In Section #2, you will add the list of objectionable words.

- Click **Edit** next to **Custom objectionable words**.
- Click **Add** to add new words.
- You can now type in, or copy and paste in, the word list.
- The words can be separated by spaces or commas.
- Click **Save** when done.

In Section #3, you will choose to either reject, modify, or quarantine email messages that contain objectionable words.

If you wish to reject the message:
- Simply choose **Reject message** from the drop-down menu.
- If a student attempts the send an email with objectionable words, the message will immediately be rejected.
- If you wish, you can add a custom rejection message here.

If instead you wish to modify the message:

- Choose **Modify message** from the drop-down menu.
- Now you need to choose how you wish to modify the message. Options include such things as:
- **Subject** - add some custom words to the subject line.
- **Envelope recipient** - send the email to someone else, instead of the intended recipient.
- **Also deliver to** - send the email to other accounts as well.
- **Attachments** - remove attachments from the message.
- And more

An example of this use might be to add the words [Objectionable Content] to the subject line, and redirect the message to the principal's account.

If instead you wish to quarantine the message:

- Choose **Quarantine message** from the drop-down menu
- Choose the quarantine you wish to send the message to
- Note: If you do choose to quarantine the messages, you will later need to go to https://email-quarantine.google.com/adminreview to view and manage the quarantined items

When all done, click **Add Setting** or **Save**, and then **Save changes**.

Blocking Email to Other Domains

One of the most common uses of the Gmail security settings is to manage where students can send email to and where they can receive email from. An easy way to control this is by specifying a list of approved domains for email. Any email sent to or received from these domains will be allowed.

To access these settings:

- Select the Organization you wish to edit.
- Scroll down through the settings to locate the section titled **Compliance**.
- In the **Compliance** section, find the entry titled **Restrict delivery**.
- Hover your mouse over this section and click **Configure** or **Edit** (if there are already settings).

In Section #1, you will add the approved domains.

- Click the link to create a new list, or click **Edit** to modify an existing list.
- Type in a name for your domain list, and click **Create**.
- Now click **Edit** next to your new list.
- Click **Add** to add approved domains or specific email addresses to the list.
- The entries can be separated by spaces or commas.
- Click **Save** when done.

In Section #2, you can enter a rejection message to be sent for message not to or from these approved domains.

In Section #3, you can (and should) check the option to bypass these settings for internal messages. This will allow email to be sent to and received from users within your Google Apps domain.

Advanced Rules with Content Compliance

If you need to set up rules and filters that are more specific, you may need to use the **Content Compliance** settings. These settings allow you to match messages on a wide variety of factors, and then reject or modify the messages as needed.

Examples for such use might include:

- Blocking students from sending email to certain grade levels.
- Blocking students from sending email to email distribution groups (listservs).
- Having a different set of domains approved for receiving than for sending.

Several samples will be given in detail later, but for now here are the basics of using **Content Compliance**.

To access these settings:

- Select the Organization you wish to edit.
- Scroll down through the **End User Settings** to locate the section titled **Compliance**.
- In the **Compliance** section, find the entry titled **Content compliance**.
- Hover your mouse over this section and click **Configure** or **Edit** (if there are already settings) or **Add another** (if you are adding more rules).

In Section #1, you will choose which messages to affect:

- Your options include:
    - **Inbound** (email coming in from outside of the domain)
    - **Outbound** (email being sent to outside the domain)
    - **Internal - sending** (email being sent to another user within the domain)
    - **Internal - receiving** (email coming from another user within the domain)

In Section #2, you will add **Expressions** to describe the content you want to match.

- In the first drop down menu, choose **ANY** or **ALL** to determine if all of the criteria have to be met (think of this as the **AND** operator) or if only one of the criteria must be met (think of this as the **OR** operator).
- In the **Expressions** section, click **Add**.
- If you choose **Simple content match** then you can enter the word (or words) you want to match and the rule will search for these anywhere in the message.
- If you choose **Advanced content match** then you can specify much more:
- **Location** - here you can indicate where the matching content must be found including:
    - Headers + Body
    - Full headers
    - Body
    - Subject
    - Sender header
    - Recipients header
    - Envelope sender
    - Any envelope recipients
    - Raw message
- **Match Type** - here you can determine how the content is to be matched including:

    - Starts with
    - Ends with
    - Contains text
    - Not contains text
    - Equals
    - Is empty
    - Matches regex
    - Not matches regex
    - Matches any word
    - Matches all words
- **Content** - here you type in the content to match or the regular expression (regex) you wish to use.

In Section #3, you will choose to either reject or modify email messages that match the content.

If you wish to reject the message:
- Simply choose **Reject message** from the drop-down menu.
- If a student attempts the send an email that matches the content, the message will immediately be rejected.
- If you wish, you can add a custom rejection message here.

If instead you wish to modify the message:
- Choose **Modify message** from the drop-down menu.
- Now you need to choose how you wish to modify the message. Options include such things as:
- **Subject** - add some custom words to the subject line.
- **Envelope recipient** - send the email to someone else, instead of the intended recipient.
- **Also deliver to** - send the email to other accounts as well.
- **Attachments** - remove attachments from the message.

If instead you wish to quarantine the message:
- Choose **Quarantine message** from the drop-down menu
- Choose the quarantine you wish to send the message to
- Note: If you do choose to quarantine the messages, you will later need to go to https://email-quarantine.google.com/adminreview to view and manage the quarantined items

---

Regular Expressions

To get the most power out of the Content Compliance rules, you will want to learn how to use Regular Expressions. A Regular Expression (or regex) is a very specific code that can be used to make sophisticated matches. Google Apps uses a simpler subset of Regular Expressions, so some of the more advanced features are missing.

Below are links to several excellent resources to help learn Regular Expressions, especially in the context of Google Apps and Gmail:

- Guidelines for Using Regular Expressions
  http://support.google.com/a/bin/answer.py?hl=en&answer=1346938
- Examples of Regular Expressions
  http://support.google.com/a/bin/answer.py?hl=en&answer=1371417

A great feature of Google Apps Email Security is that you can test any regex as you write it to make sure it is working the

way you planned. Once you type in your regex, click the link **Test expression** to open a window where you can type in examples and counterexamples to see if your regex functions as you have planned.

Content Compliance Example - Blocking email to certain grade levels

One example for using Content Compliance would be if you wish to restrict which grade levels students can send email to. For example say you only want students to send email to staff members and other students within their same grade level. You need a much more sophisticated method to match such messages. Below is an example of how Content Compliance and Regular Expressions could be used to solve this.

- In this example we will say that students have usernames that are their graduation year, followed by their first initial of their first name, followed by their entire last name.
- We will say that staff usernames are just their first initial of their first name, followed by their entire last name.
- So, a student email address may be 2020jsmith@mydomain.org.
- A staff email address may be mjones@mydomain.org.

So basically we need a filter that says if the recipient does not match students in the same graduation year, and does not match a staff member, then reject the message. We would select the Organization that contains all students graduating in 2020, and we would create a Content Compliance filter like this:

- Messages to affect
  - Internal - sending
- Conditions
  - If ALL of the following match the message
  - Location = Envelope recipients
  - Match type = Not matches regex
  - Regexp = (?i)(\W|^)(2020[a-z]{1,25}@mydomain\.org|[a-z]{1,25}@mydomain\.org)(\W|$)
- Consequences
  - Reject message

To explain the Regular Expression (regex) here is what each of the part do:

- **(?i)** - Ignore case so upper and lower case are matched
- **(\W|^)** - Begin the match at the start of the string or after a non-word character
- **(** - Begin a group of options
- **2020[a-z]{1,25}@mydomain\.org** - match an email address for a student in the 2020 graduating class
- **|** - or
- **[a-z]{1,25}@mydomain\.org** - match a staff email address
- **)** - End a group of options
- **(\W|$)** - End the match at the end of the string or at a non-word character

As with all regular expressions there are probably several other ways the expression could be written.

Content Compliance Example - Blocking messages to email distribution groups

Another example for using Content Compliance is to stop students from sending messages to email distribution groups

(listservs). You may have email groups for staff, students, and parents, and you want any staff member to be able to send email to these groups, without having to be a part of each group. Therefore you need to allow anyone from the domain to send email to the group, not just members of the group. However, you do not want students to be able to send email to the groups, which is where Content Compliance filters can come in.

- In this example we will say all staff email groups fit the pattern of list-[groupname]@mydomain.org
- And all student email groups fit the pattern of stu-[groupname]@mydomain.org

We could create a Content Compliance filter like this:

- Messages to affect
    - Internal - sending
- Conditions
    - If ALL of the following match the message
    - Location = Envelope recipients
    - Match type = Matches regex
    - Regexp = (?i)(list|stu)-[a-z0-9-]{1,25}@mydomain\.org
- Consequences
    - Reject message

Alternate Example - Blocking email to certain grade levels

Earlier we mentioned the importance of naming users in such a way that it would be possible to distinguish between different grade levels, such as putting the graduation year in the students' usernames. However, if you have not done this, there is still a workaround to be able to control which grade levels students can send email to.

In Google Apps Email Security you are able to add several types of filters, including one called "Append footer". This allows you to add some text onto the end of all email sent out by users of that specific Organization. So, what you can do is use the "Append footer" option to add something unique to the emails for each grade level that will identify any email sent by those students as being from that grade level. Then, you can create "Content compliance" filters for other organizations that look for that unique filter and then reject the ones they are not supposed to communicate with.

For example, let's say I have an organization called "Grade 1" that has all my first grade students. And let's say I do not want the 1st grade students to be able to send email to the high school students. Now technically I can't stop the 1st grade student from sending the email to a high school student, but I can now set a filter on the high school students that looks for and rejects any email that comes from a 1st grade student.

So for the "Grade 1" organization we add the **Append footer** filter with settings like this:

- Select the Organization you wish to edit.
- Scroll down through the **End User Settings** to locate the section titled **Compliance**.
- In the **Compliance** section, find the entry titled **Append footer**.
- Hover your mouse over this section and click **Configure** or **Edit** (if there are already settings) or **Add another** (if you are adding more rules).
- In Section #1, for all outbound email messages, append the following footer = ***Sent from Grade 1 account*** (or something that will uniquely identify the emails from this grade level.)
- In Section #2, for **Options** check the box for "Append the footer to messages being sent within your organization."

The key here is to come up with a very unique footer message that no one else would be likely to ever type into an email message, so that you can be sure it is only appearing for students of this grade level.

Now any time a student from the "Grade 1" organization sends an email message it will have ***Sent from Grade 1 account*** added to the bottom of their message.

So we can now use that unique text to key off of when creating a filter for the high school students. What we want to do is now create a **Content compliance** filter for our "High School" organization like this:

- Select the Organization you wish to edit.
- Scroll down through the **End User Settings** to locate the section titled **Compliance**.
- In the **Compliance** section, find the entry titled **Content compliance**.
- Hover your mouse over this section and click **Configure** or **Edit** (if there are already settings).

In Section #1, **Messages to affect** just choose **Internal - receiving** (since we are looking to block emails sent from 1st grade students to high school students)

In Section #2, choose:

- If ANY of the following match the message
- Location = Body
- Match type = Contains text
- Content = ***Sent from Grade 1 account***

For Section #3, choose **Reject message**.

So now if any student in the "High School" organization gets an email from a student in the "Grade 1" organization, the email will have unique text appended to the sent email that will match the "Content compliance" filter and trigger the rejection of the message. Of course you will want to tailor this to your specific organizations, but the process would be the same.

Further Resources

For more details and helpful information, see the Google Apps help page specific to email security settings:

- Configure email settings for an organizational unit - Google help link

For helpful resource to help teach students about email safety and digital citizenship, see the following resources:

- Common Sense Media - link, link
- Be Internet Awesome - link
- BrainPOP - Digital Etiquette - link
- BrainPOP Jr - Internet Safety - link
- Email Etiquette for Elementary Students - link

Other resources

- Bring me to your organization: My training and consulting services - on-site or online - link
- All of my free training materials, help guides, presentations, videos, and more - link

---