

Postini Transition Guide

Getting started with Google Apps advanced Gmail settings

February 23, 2015



Contents

Introduction

- [Using this guide](#)
- [Defining the word 'transition'](#)
- [Defining the different Postini customer types](#)

Prepare for your transition: Postini Classic

- [Configure your firewall](#)
- [Configure your SPF record](#)
- [Change your directory sync settings](#)
- [Verify ownership of your domains](#)
- [Review the various domain mapping scenarios](#)
- [Confirm that your Postini admins have the correct administrative privileges](#)
- [Check your prepare screen in the Postini Transition Console](#)
- [About transitioning user accounts containing over 30 aliases](#)

Prepare for your transition: Postini Hybrid

- [If you route some of your mail to an on-premise server, change your firewall](#)
- [Configure your SPF record](#)
- [Change your directory sync settings](#)
- [Verify ownership of your domains](#)
- [Review the various domain mapping scenarios](#)
- [Confirm that your Postini admins have the correct administrative privileges](#)
- [Check your prepare screen in the Postini Transition Console](#)
- [About transitioning user accounts containing over 30 aliases](#)
- [Set up your organizational hierarchy for Hybrid transitions](#)
 - [Before you transition: Set up a pilot org in Postini with a subset of users](#)
 - [Analyze your org hierarchy](#)
 - [Copy settings from one org to another](#)
 - [Consolidate your org hierarchy](#)
 - [Restructure your org hierarchy](#)
 - [Confirm routing for non-Gmail mailbox users](#)
 - [Configure Google Apps Directory Sync \(GADS\)](#)
 - [Complete your transition](#)

Begin your service transition

Transition steps for Postini Classic customers

- [1. Prepare for your transition](#)
- [2. Review your transition invitation email](#)
- [3. Begin your service transition in the Postini Transition Console](#)
- [4. Review your confirmation email and confirmation message](#)
- [5. Update your Google Apps Directory Sync \(GADS\) settings](#)
- [6. Get started with Google Apps email settings](#)
- [7. Outbound customers only: Route your outbound mail through Google Apps](#)

[8. Complete your final transition steps](#)

[Transition steps for Postini Hybrid customers](#)

- [1. Prepare for your transition](#)
 - [2. Review your transition invitation email](#)
 - [3. Begin your service transition in the Postini Transition Console](#)
 - [4. Review your confirmation email and confirmation message](#)
 - [5. Update your Google Apps Directory Sync \(GADS\) settings](#)
 - [6. Review and verify your Google Apps settings, and modify if needed](#)
 - [7. Log in to the Postini Administration Console to continue your transition](#)
 - [Change mail processing to Google Apps](#)
 - [Finish your service transition](#)
 - [Sign in to Google Apps to get started](#)
 - [8. Complete your final transition steps](#)
- [Managing spam and users during the GMS Hybrid service transition](#)

[Using GADS and DSS during the transition](#)

- [Before the transition](#)
- [During the transition](#)
- [After the transition](#)

[Steps to complete your transition](#)

- [Change your MX records to Google Apps](#)
 - [Why you need to change your MX records](#)
 - [How to change your MX records](#)
- [Route your outbound mail through Google Apps](#)
- [Remove your Postini inbound gateway](#)

[After your transition: Google Apps mail flow diagrams](#)

- [Inbound mail flow](#)
- [Outbound mail flow](#)

[Improvements and changes in moving from Postini to Apps](#)

- [Google Apps feature enhancements compared to Postini GMS](#)
- [Postini features that work differently in Google Apps](#)

[Get started with the Google Admin Console](#)

- [Sign in to the Google Admin console](#)
- [Advanced settings for Gmail](#)
- [Review and manage your users in Google Apps](#)
- [Review and manage your orgs and org structure](#)
- [Review and manage your domains](#)
- [Set up and manage admin roles in Google Apps](#)
- [Other common tasks in the Admin console](#)

[Message Center and Quarantine Summary](#)

- [How the transition works for the Message Center and Quarantine Summary](#)
- [Configure Message Center and Quarantine Summary](#)

[Instructions for your users](#)
[Compare Google Apps spam and virus filtering to Postini](#)
[Message Center feature differences and improvements](#)

[How Gmail spam and virus filtering differs from Postini](#)

[Spam filtering differences](#)
[How should admins and users deal with bulk email messages?](#)
[How can you file a Support case for systemic spam issues?](#)
[How can an administrator prevent users from viewing spam?](#)
[How your non-Gmail users manage spam with Message Center](#)
[How your non-Gmail users manage spam with Quarantine Summary](#)
[How your Gmail users manage spam](#)
[Virus filtering differences between Postini and Gmail](#)

[Message processing in Google Apps](#)

[Processing order](#)
[Inheritance](#)

[Get started with advanced settings for Gmail](#)

[Configuring advanced settings for Gmail](#)

[Email setting descriptions](#)
[Setup](#)
[End user settings](#)
[End user access](#)
[Spam](#)
[Compliance](#)
[Routing](#)
[How to use the controls on the Gmail advanced settings page](#)
[Hover controls](#)
[Inherited versus locally applied Gmail settings](#)
[Settings that are only configurable at the top level](#)
[Hosts tab](#)
[Default routing tab](#)

[Guidelines for configuring advanced settings for Gmail](#)

[Organizational units, settings, conditions, and actions](#)
[General guidelines for predicting the behavior of settings](#)

[Content compliance setting](#)

[How the transition works for Content Manager and Content compliance](#)
[Using and configuring Content compliance setting options](#)
[Feature differences and improvements](#)

[Attachment compliance](#)

[How the transition works for Attachment compliance](#)
[Using the Attachment compliance setting](#)
[Feature differences and improvements](#)

Google Apps routing settings

[How the transition works for routing settings](#)

[Descriptions of the Google Apps routing settings](#)

[Hosts tab](#)

[Default routing](#)

[Receiving routing](#)

[Sending routing](#)

[Routing based on message content, attachment, or TLS controls](#)

[Non-Gmail mailbox routing](#)

[SMTP relay service](#)

[Vault settings for Exchange journals](#)

[Recipient address map](#)

[Alternate secure route](#)

[Legacy routing settings](#)

Google Apps Message Encryption

[Your GAME order](#)

[How the transition works for GAME](#)

[How GAME works](#)

[Add new users or domains](#)

Google Apps features that protect against spoofing

[How the transition works for spoofing protection features](#)

[Using spoofing protection features in Google Apps](#)

[Feature differences and improvements](#)

[Message senders: Protect your domain from being spoofed](#)

[Message recipients: Identify incoming messages from spoofed domains](#)

'Spooling' in Google Apps: Retrying messages

[Delivery status notifications](#)

[Use Log Search to monitor the status of retried messages](#)

[Update your Host setting to redirect mail to another mail server](#)

Troubleshooting

[I don't have a Postini root admin account](#)

[How will I gain access to my new Google Apps admin account after my transition?](#)

[If I don't have a Postini admin account that will receive email updates about my transition, how will I know when my transition has been initiated?](#)

[Users can't sign in to Google services](#)

[What is a conflicting account?](#)

FAQs: Postini Transition to Google Apps

Transition Support

Introduction

The Postini Transition to Google Apps enables you to copy your orgs, users, and email settings from Postini to the Google Admin console. With this transition, you'll receive email security features that are comparable to your Google Message Security (GMS) features, but through the more robust Google Apps platform.

Google is also taking most of the Google Message Discovery (GMD/Postini archiving) features and rebuilding comparable features into Google Apps Vault. For details, see the help center to access the companion guide: [Getting started with Google Apps Vault](#).

NOTE: This guide is subject to change during the Postini Transition project. The contents will not be maintained or updated after the Postini Transition project is completed. For the latest instructions on using Google Apps, see [Configure advanced settings for Gmail](#) in the Google Apps help center. For the latest instructions on using Vault, see the [Google Apps Vault help center](#).

Using this guide

The Postini Transition Guide will help you do the following before, during, and after your transition:

- Prepare for your service transition.
- Initiate and complete your service transition.
- Get started with Google Apps after your service transition is completed.

Defining the word 'transition'

The word *transition* is used in different ways throughout this guide:

- **Service transition**—Refers to the transfer of orgs, settings, and users from Postini to Google Apps. For GMD customers, this also includes the transfer of archive data from GMD to Google Apps Vault. The service transition—which is sometimes referred to as the *settings migration*—is initiated from the Postini Transition Console.
- **Transition**—In many cases, the word *transition* is referring to the *overall* transition process from start to finish. This includes all preparation steps, the process of initiating your *service transition*, and the cleanup steps that are needed after your service transition is completed.
- **Postini transition**—Refers to the overall transition *project*, which involves the transition of several Postini customers to Google Apps and Google Apps Vault.

Defining the different Postini customer types

The steps in the transition process will vary depending on the type of Postini customer you are. The three basic types of customer are *Classic*, *Hybrid*, and *Integrated*.



Postini Classic customers—If you use only Postini and do not use Google Apps or Gmail, you are a Postini Classic customer. This means you purchased Postini message security or message discovery (archiving) for on-premise or non-Gmail mail servers. For instructions on how to complete your transition, see [Transition steps for Postini Classic customers](#).

Postini Hybrid customers—Most customers who use both Postini and Google Apps are defined as Postini Hybrid customers. You're a Postini Hybrid customer if the following applies to you:

- You're a Google Apps customer who can route mail to on-premise mail servers.
- In addition to Google Apps, you also use Postini message security or message discovery (archiving).
- You log in to both the Google Admin console and the Postini Admin Console with separate login credentials.

For instructions on how to complete your transition, see [Transition steps for Postini Hybrid customers](#).

Postini Integrated customers—A small percentage of Postini customers are defined as Postini Integrated customers. You're a Postini Integrated customer if the following applies to you:

- You're using both Postini and Google Apps but you're not using on-premise mail servers.
- You can access both Postini and the Google Admin console with one login, and your users are automatically synchronized between the two systems.

For details, see [Transition steps for Postini Integrated customers](#) in the Google Apps help center.

Prepare for your transition: Postini Classic

Your preparation steps vary depending on the type of Postini customer you are -- either Classic or Hybrid. If you're a Postini Classic customer, follow the steps in this section.

Configure your firewall

Prior to initiating your service transition, your email server and firewall must be configured to allow mail traffic from Google IP ranges. We recommend that you make this change immediately even if you haven't received your transition invitation. For instructions, see [Allow email from Google IPs to your email server](#).

Configure your SPF record

If you already have an SPF record, you'll need to update your existing SPF record to include `_spf.google.com` to work with Google Apps and avoid failed delivery of outgoing mail. If you need to update your existing SPF record, we recommend that you make this change immediately even if you haven't received your transition invitation. For instructions, see [Configure SPF records to work with Google Apps](#).

If you do not already have an SPF record, do not create a new SPF record until after your transition is complete. Partial or incomplete SPF records may cause delivery and spam classification issues.

Change your directory sync settings

If you already use Google Apps Directory Sync (GADS) and Postini Directory Sync Service (DSS), you'll need to modify your GADS settings, and disable GADS and DSS before your service transition begins so that GADS does not delete Google Apps user accounts that are created during the service transition, such as former employee, Postini-only, and sharded user accounts.

Do not enable or re-enable GADS until you are notified that your orgs, users, and settings have transitioned from Postini to Google Apps.

For instructions, see [Using GADS and DSS during the transition](#).

Verify ownership of your domains

If you haven't yet verified ownership of your domains, you must complete this step before you can begin your transition. If this applies to you, you'll receive an email from Google with details about which domains must be verified. If you fail to verify a domain, that domain will not be transitioned -- including that domain's users and settings, as well as any archive data (if you're a Postini GMD customer).

Create the following TXT record for each of the domains you wish to have automatically transitioned:
P2A_XXXXXXX_X



For instructions, see [Add TXT records to verify Postini domain ownership](#).

Review the various domain mapping scenarios

Before you transition your Postini accounts to Google Apps, you should consider how you want to map those accounts and domains to your new or any existing Google Apps accounts and domains.

This article presents some sample scenarios for how you might want to transition accounts from Postini to Google Apps. For details, see [Domain mapping scenarios](#).

IMPORTANT: In general, your Postini domains are automatically mapped to Google Apps during your service transition. However, for a small percentage of Postini Hybrid customers, one or more Postini domains cannot be automatically transitioned because of conflicts with existing Google Apps domains.

If your transition is affected by this scenario, you'll need to take action to resolve these conflicts. For instructions, see [Transitioning Postini domains with mapping conflicts](#).

Confirm that your Postini admins have the correct administrative privileges

Before beginning your transition, make sure that only admins who need access to Postini have access. Assign root admin privileges to admins who are responsible for completing your transition steps, and remove privileges for admins who shouldn't be allowed to progress the transition. Communicate the transition plan to any admins that typically should have these rights.

For instructions on changing Postini permissions, see [Viewing and Editing Authorization Records](#) in the Message Security Administration Guide.

Check your prepare screen in the Postini Transition Console

Before you begin your Postini transition to Google Apps, view the prepare screen for important transition information.

The prepare screen alerts you of any items blocking your transition and, in some cases, requires you to resolve those items; for example, preparation steps that you haven't completed yet (such as verifying your Postini domains).

Many of the items on the prepare screen are not blocking your transition, but you should be aware of them before you begin; for example, Postini features that aren't supported in Google Apps, or a Google Apps setting that behaves differently than a comparable setting in Postini.

To access the prepare screen, [log in to the Postini Administration Console](#) and click **Before your transition**.

For more details, see [Prepare screen in the Postini Transition Console](#).

About transitioning user accounts containing over 30 aliases

Google Apps supports up to 30 aliases per user account. If your Postini user accounts contain no more than 30 aliases, the transition tool simply migrates those aliases into the corresponding user account in



Google Apps.

If any of your Postini user accounts contains over 30 aliases, the transition tool manages the alias email addresses to ensure that mail routing behavior remains the same after your transition is complete. The process differs depending on whether the user account already exists in Google Apps.

While no action is required on your part, we recommend that you review the details in [Transitioning user accounts containing over 30 aliases](#) before beginning your transition.



Prepare for your transition: Postini Hybrid

Your preparation steps vary depending on the type of Postini customer you are -- either Classic or Hybrid. If you're a Postini Hybrid customer, follow the steps in this section.

If you route some of your mail to an on-premise server, change your firewall

You'll need to adjust your firewall configuration if you have non-Gmail mailboxes or delivery endpoints such as Exchange mailboxes, ticketing systems, or other on-premise systems. If this is true for you, your on-premise email server and firewall must be configured to allow mail traffic from Google IP ranges. We recommend that you make this change immediately even if you haven't received your transition invitation. If you do not take these steps now, your mail flow may be interrupted during your transition. For instructions, see [Allow email from Google IPs to your email server](#).

Configure your SPF record

If you already have an SPF record, you'll need to update your existing SPF record to include `_spf.google.com` to work with Google Apps and avoid failed delivery of outgoing mail. If you need to update your existing SPF record, we recommend that you make this change immediately even if you haven't received your transition invitation. For instructions, see [Configure SPF records to work with Google Apps](#).

If you do not already have an SPF record, do not create a new SPF record until after your transition is complete. Partial or incomplete SPF records may cause delivery and spam classification issues.

Change your directory sync settings

If you already use Google Apps Directory Sync (GADS) and Postini Directory Sync Service (DSS), you'll need to modify your GADS settings, and disable GADS and DSS before your service transition begins so that GADS does not delete Google Apps user accounts that are created during the service transition, such as former employee, Postini-only, and sharded user accounts.

Do not enable or re-enable GADS until you are notified that your orgs, users, and settings have transitioned from Postini to Google Apps.

For instructions, see [Using GADS and DSS during the transition](#).

Optional: We recommend that you create a pilot org in Postini with a subset of test users

During your transition steps, you can use the Postini Transition Console to route your mail through Google for specific organizational units. This will enable you to test mailflow to Google Apps for a subset of your users before completing your transition. To prepare for this step, we recommend that you set up a pilot org in Postini prior to your service transition.



Verify ownership of your domains

If you haven't yet verified ownership of your domains, you must complete this step before you can begin your transition. If this applies to you, you'll receive an email from Google with details about which domains must be verified. If you fail to verify a domain, that domain will not be transitioned -- including that domain's users and settings, as well as any archive data (if you're a Postini GMD customer).

If you're a [Postini Hybrid customer](#) -- Verify ownership of your domains by adding them to your Google Apps account. For instructions, see [Add a domain or domain alias](#).

If you're a Postini Classic customer -- Create the following TXT record for each of the domains you wish to have automatically transitioned:

P2A_XXXXXXX_X

For instructions, see [Add TXT records to verify Postini domain ownership](#).

Turn off non-account bouncing in Postini

Before you begin your transition to Google Apps, be sure to turn off non-account bouncing in Postini if this feature is already turned on. If you fail to turn off non-account bouncing, mail may be bounced for any new users you add to Google Apps during your service transition. To turn off non-account bouncing:

1. Sign in to Postini.
2. Click **Orgs and Users**.
3. Click the top-level org.
4. Click **General Settings**.
5. Under Non-Account Bouncing, select **Off**.
6. Click **Save**.

Review the various domain mapping scenarios

Before you transition your Postini accounts to Google Apps, you should consider how you want to map those accounts and domains to your new or any existing Google Apps accounts and domains.

This article presents some sample scenarios for how you might want to transition accounts from Postini to Google Apps. For details, see [Domain mapping scenarios](#).

IMPORTANT: In general, your Postini domains are automatically mapped to Google Apps during your service transition. However, for a small percentage of Postini Hybrid customers, one or more Postini domains cannot be automatically transitioned because of conflicts with existing Google Apps domains.

If your transition is affected by this scenario, you'll need to take action to resolve these conflicts. For instructions, see [Transitioning Postini domains with mapping conflicts](#).

Confirm that your Postini admins have the correct administrative privileges

Before beginning your transition, make sure that only admins who need access to Postini have access. Assign root admin privileges to admins who are responsible for completing your transition steps, and remove privileges for admins who shouldn't be allowed to progress the transition. Communicate the



transition plan to any admins that typically should have these rights.

For instructions on changing Postini permissions, see [Viewing and Editing Authorization Records](#) in the Message Security Administration Guide.

Check your prepare screen in the Postini Transition Console

Before you begin your Postini transition to Google Apps, view the prepare screen for important transition information.

The prepare screen alerts you of any items blocking your transition and, in some cases, requires you to resolve those items; for example, preparation steps that you haven't completed yet (such as verifying your Postini domains).

Many of the items on the prepare screen are not blocking your transition, but you should be aware of them before you begin; for example, Postini features that aren't supported in Google Apps, or a Google Apps setting that behaves differently than a comparable setting in Postini.

To access the prepare screen, [log in to the Postini Administration Console](#) and click **Before your transition**.

For more details, see [Prepare screen in the Postini Transition Console](#).

About transitioning user accounts containing over 30 aliases

Google Apps supports up to 30 aliases per user account. If your Postini user accounts contain no more than 30 aliases, the transition tool simply migrates those aliases into the corresponding user account in Google Apps.

If any of your Postini user accounts contains over 30 aliases, the transition tool manages the alias email addresses to ensure that mail routing behavior remains the same after your transition is complete. The process differs depending on whether the user account already exists in Google Apps.

While no action is required on your part, we recommend that you review the details in [Transitioning user accounts containing over 30 aliases](#) before beginning your transition.

Set up your organizational hierarchy for Hybrid transitions

The [Postini Hybrid transition process](#) automatically copies your orgs, users and email settings from Postini to Google Apps. During this process, your Postini data is copied to a new organization, so your existing Google Apps configuration is not overwritten. Your Postini org structure is replicated in a new org below your top-level org in Google Apps, and your Postini users and settings are transitioned to this new hierarchy.

After your orgs, users, and settings are copied over, your mail continues to be filtered by Postini. Before you complete your transition, you can check your Google Apps configuration to verify that your settings were copied to your satisfaction. Next, you can return to the Hybrid transition console to place select organizations in passthrough mode. This enables you to test the functioning of your settings before you

complete your transition. During this time, you may also need to make a few changes to your organizational hierarchy in Google Apps, as described in this section.

We recommend that you do the following during your Hybrid transition:

1. Set up a pilot org in Postini before you initiate your service transition.
2. After your service transition is completed, sign in to the Google Admin console to verify the transition of your orgs, users, and settings.
3. Analyze your org hierarchy to determine your next steps.
4. If needed, copy settings from one organization to another as you restructure or consolidate your org hierarchy.
5. If you use Google Apps Directory Sync (GADS) and Postini Directory Sync Service (DSS), [configure GADS](#) during your transition.
6. Return to the Hybrid Transition Console to complete your transition.

For details about each of these steps, see the sections below.

NOTE: Postini Hybrid customers use both Postini and Google Apps. For more details, see [Defining the different Postini customer types](#).

Before you transition: Set up a pilot org in Postini with a subset of users

During your transition steps, you can use the Postini Hybrid transition console to route your mail through Google for specific organizational units. This enables you to test mailflow to Google Apps for a subset of your users in select organizations before completing your transition.

If you have a simple hierarchical structure in Postini (one account org, one email config org, and one user org), we recommend that you create a pilot org in Postini before starting your transition. You can move a few users into this pilot org (preferably admins or power users), and you can later test your Google Apps email security settings during your Hybrid transition steps.

If you have multiple organizations in Postini, you can select an existing organization to test your settings after your transition, rather than create a pilot org.

By using a pilot org or test org, you can enable passthrough for a few users prior to enabling passthrough for everyone else. You can then test and fine-tune your Google Apps email security settings for the test or pilot org before rolling out to everyone.

For instructions on creating a new org in Postini, see [Create an Organization](#) in the Message Security Administration Guide. For more details about Hybrid transitions, see *Transition steps for Postini Hybrid customers* in this guide.

NOTE: *Passthrough* means your mail is "passed through" from Postini to Google Apps, and your MX records continue pointing to Postini temporarily. By placing Postini in passthrough, you have the option to "roll back" your transition until you are satisfied with your mail flow and the functioning of your Google Apps settings.

After you click Begin Transition Now in the Hybrid transition console to begin your service transition, the Postini Administration Console becomes read-only (you can view the settings but you can't edit them).



Once you're satisfied with your settings in Google Apps, then you can complete your transition.

Analyze your org hierarchy

If your Google Apps org hierarchy differs from your Postini org hierarchy, you must decide how you want to move forward on the Apps platform. Your Postini hierarchy will be transitioned to a temporary org structure under your current Apps hierarchy. To set up your org hierarchy in Apps following your transition, you can take the following actions:

- Copy settings from some of your child orgs to the root org.
- Delete any duplicate settings in the child orgs.
- Move users from one org to another org.
- Delete any organizations not in use.
- [Configure Google Apps Directory Sync](#).

The above steps will help you either consolidate or restructure your org hierarchy. Consolidating your org hierarchy is recommended if all of your users are just one type of user—whether it's all Gmail users or all non-Gmail users. Restructuring your org hierarchy is recommended if you have both Gmail and non-Gmail users.

Note how your current hierarchy is set up—whether it's by job description, group, location, application/feature access, or a combination of these. Configure your base settings (all settings that users have in common) at the root level organization. Since settings are inherited, child organizations will automatically be configured with these base settings.

See the sections below for more details and instructions.

NOTE: If your Postini configuration includes just one account org, one email config, and one user org, you will see just one transitioned org in the Google Admin console when you first sign in. In Google Apps, the account org and email config org are not necessary, so the org structure will be simplified for you. If needed, you can add sub-organizations after your service transition.

Copy settings from one org to another

After verifying that your Postini orgs, settings, and users are successfully transitioned to Google Apps, you can make sure your Google Apps orgs are production ready by copying settings to the root org level. You can do this using the Copy to organization feature for various Google Apps email settings.

We recommend that you copy your transitioned settings to an existing Google Apps org. This enables Gmail users to have continued access to their native apps—such as Calendar, Contacts, and Drive—while also experiencing the granularity and flexibility of Google Apps email filtering.

At the same time, non-Gmail users will also get their email filtered by the Google Apps platform prior to it being delivered to the on-premise server and then on to their inbox. For example, any “needed” messages caught in quarantine can be delivered by users directly to their non-Gmail inbox via the [Quarantine Summary](#) and [Message Center](#) (these features are for non-Gmail users only). Gmail users will manage their spam via their Spam label—however, both Gmail and non-Gmail users will have the ability to train the system with regard to reporting spam. For more details, see [How Gmail spam and virus](#)

[filtering differs from Postini.](#)

To copy a setting from one organization to another:

1. [Sign in to your Google Admin console.](#)
2. Click Google Apps > Gmail > Advanced settings.
3. Select the relevant organization from the list at the top of the page.
4. Highlight any of the email security settings—for example, the Append footer setting.
5. Click Copy to organization.
6. Choose the organization that you want to copy the setting to.



Consolidate your org hierarchy

Consolidating your org hierarchy is recommended if all of your users are just one type of user; whether it's all Gmail users or all non-Gmail users.

When you copy settings up to the Google Apps root organization, you may see duplicate settings at the child org levels. You can remove any duplicate setting by deleting the setting that's "local" to that org. Once you configure your base settings at the root level and remove any duplicate settings at the child org level(s), you can then take a more granular approach by configuring the child orgs to meet the needs of the users configured in each organization.

Once you configure your organizations as desired, you can delete any organizations not in use.

For more details about using Google Apps email settings, see [Configure advanced settings for Gmail](#) and [Guidelines for configuring advanced settings for Gmail](#). See also [modifying the organizational structure](#) in the Google Apps help center.

Restructure your org hierarchy

Restructuring your Google Apps org hierarchy is recommended if you have both Gmail and non-Gmail users. There are several factors to consider when restructuring your hierarchy—including your current setup, configuration, complexity and ratio of unique users vs. existing Apps users.

To modify or fine-tune your org structure in the Google Admin console, see [Create an organizational structure](#), [Add an organizational unit](#), and [Modify the organizational structure](#) in the Google Apps help center.

For hybrid environments that have both Gmail and non-Gmail users, only the unique users (non-Gmail or Apps users configured in Postini but not Apps) will be transitioned to Apps in a temporary organizational hierarchy. Per the process stated above, it would be most efficient to copy all of the base settings to the root org, delete any duplicates, and configure child org(s) as needed. Also remember to clean-up or delete organizations no longer in use.

For unique Gmail users that were copied over from Postini to the temporary hierarchy, you can [move those users](#) to an appropriate existing Google Apps org that's configured especially for them. If no such org exists, you can [add a suborg](#) and configure that org to the specific requirements of the users in question.

Confirm routing for non-Gmail mailbox users

During your Hybrid service transition, your Google Apps settings for your non-Gmail users are automatically configured to route mail to your non-Gmail mailboxes. However, you can review your non-Gmail mailbox settings before you complete your transition. This will help you confirm that your mail is being routed to your on-premise server.

Do the following:

1. [Sign in to the Google Admin console](#).
2. Click Google Apps > Gmail > Advanced settings.
3. In the Organizations section, highlight your domain or the organizational unit for which you want to configure this setting (for more details, see [Configure advanced settings for Gmail](#)).
4. Scroll to the Non-Gmail mailbox section, or enter this term in the Search settings field.
5. Click Edit to edit or view an existing configuration. The Edit setting dialog box appears.

In the **Mail server** section, your on-premise mail host should be selected.

6. For more details and step-by-step instructions, see [Set options for non-Gmail mailbox users](#).

Configure Google Apps Directory Sync (GADS)

If you use GADS and Postini Directory Sync Service (DSS), you must configure GADS during your transition. For details, see [Using GADS and DSS during the transition](#).

Complete your transition

After you have completed the above steps, you'll need to return to the Hybrid Transition Console to test your pilot org(s) to make sure your Google Apps configuration is working to your satisfaction. You can place select organizations in passthrough mode to test your mail flow and the functioning of the settings. Once you are sure that your settings and mail flow are working to your satisfaction, you can complete your transition in the Hybrid transition console. For details and step-by-step instructions, see *Transition steps for Postini Hybrid customers*.



Begin your service transition

When you click **Begin Transition Now** in the Transition Console, Google will automatically transfer the orgs, users, and email settings for your domain from Postini to the Google Admin console:

- **Orgs and users** - Both primary addresses and aliases are copied over, as well as your Postini organizations and sub-organizations. In general, the parent-child relationships will be preserved; however, the account org and email config org are not necessary in Google Apps, so the org structure will be simplified for you in the case of a single Postini user org. If needed, you can add sub-organizations.
- **Domain names** - Each of your domain names are transferred to the Domain settings page in the Google Admin console. This might include just a single primary domain, or it may also include additional domains or domain aliases that were part of your Postini configuration. Domain verification will be set automatically for primary domains, as well as for additional domains and domain aliases. If your account does include multiple domains, you'll be given the option to select the primary domain for your account before you initiate your service transition in the Postini Transition Console.
- **Email settings** - Email settings are also transferred to Google Apps, including content filters, attachments filters, mail routing, and more.

NOTE: Postini Hybrid customers: See Managing spam, users, or archiving during [GMS](#) or [GMD](#) service transition for information about completing common user and administrative tasks. For instructions about getting started with Google Apps and Google Apps Vault after your service transition, see [Getting started with Google Apps email settings](#) and [Getting started with Google Apps Vault](#).

How long will it take for the service transition?

For many accounts, the process of automatically moving your orgs, users, and settings from Postini to Google Apps will be completed within a few minutes, but it may take longer for many other accounts. You'll receive a confirmation email when the process is completed, and the Transition Console -- which you can access using your Postini Admin Console username and password -- will also display updates so you can monitor the status of your transition.

If you are a Postini message discovery (archiving) customer, the process of moving your archive data will require extra time. You'll receive another confirmation email when this process is completed.

Note that your transition is not completed until you [change your MX records](#) from Postini to Google Apps.

NOTE: For details about the GMD transition to Google Apps Vault, see [Getting started with Google Apps Vault](#).



Transition steps for Postini Classic customers

The steps for your service transition will vary depending on your Postini customer type. If you're a Postini *Classic* customer:

- You use only Postini; you're not using Google Apps.
- You use an on-premise (non-Gmail) mail server.

The transition for Postini GMS Classic customers includes the following steps:

1. Prepare for your transition.
2. Review your transition invitation email.
3. Begin your service transition in the Postini Transition Console.
4. Review your confirmation email and confirmation message.
5. Update your Google Apps Directory Sync (GADS) settings.
6. Get started with Google Apps email settings.
7. Outbound customers only: Route your outbound mail through Google Apps.
8. Complete your final transition steps.

See the sections below for detailed instructions.

1. Prepare for your transition

To prepare for your transition, you'll need to configure your firewall, configure your SPF record (if you already have one), change your Google Apps Directory Sync (GADS) and Directory Sync Service (DSS) setting (if you already use GADS and DSS), verify ownership of your domains, and confirm admin privileges. For details, see [Prepare for your transition: Postini Classic](#).

2. Review your transition invitation email

Once your account is eligible for transition, Google will send a Transition Invitation email to administrators for your domain as well as your organization's business contact. Your Transition Invitation email will provide a link to the Classic Transition Console, where you can log in using your Postini Admin Console username and password.

Your Transition Invitation will specify the deadline for you to complete your transition -- which is within 60 days of receiving this email. (Note that online customers will have 30 days to complete their transition. For details, see [What's different if I purchased Postini online?](#) in the Postini Transition Resource Center.)



Google Postini Transition

Dear Postini customer,

Your action is now required. Your Postini account is ready for transition to Google Apps, and you must complete your transition for the following domains by **12/31/2014**:

solarmora.com

Note that mail flow and filtering for your domain will not be interrupted when you start your transition.

To get started, click the following link to log in to your Transition Console:

[Start your transition](#)

Use your Postini Admin Console username and password to log in, and then follow the instructions to begin your transition.

For more information and detailed instructions, see [Transition steps for Postini Classic customers](#) and [Getting started with Google Apps email settings](#).

If you have questions during your transition, contact [Support](#).

Thank you,
The Postini / Google Apps Transition Team

3. Begin your service transition in the Postini Transition Console

Once you open the transition console, you can click **Begin Transition Now** to automatically move your orgs, users and email settings from Postini to Google Apps. During this process, your mail flow is changed to route mail through Google Apps, and your filtering is now occurring in Google Apps. Postini is placed in passthrough mode -- which means your mail is "passed through" from Postini to Google Apps. Your MX records will continue pointing to Postini temporarily, and your Postini Admin Console will be in read-only mode.

NOTE: If you're a Postini archiving (GMD) customer, initiating your service transition also begins the automatic transfer of your GMD archive data.

If your account includes multiple domains, you'll be given the option to select the primary domain for your account before you initiate your service transition in the Postini Transition Console.

Your Postini service is ready to transition to Google Apps.



Before you begin, our records indicate that you own multiple domain names. Google Apps supports only a single primary domain name for signing in to the Google Admin panel. We will transfer all of your domains, but you need to choose one of the following as your primary domain name to transition to Google Apps:

DOMAIN	NUMBER OF USERS	EMAIL USAGE (IN LAST 7 DAYS)
<input checked="" type="radio"/> john1.in.test.postini-corp.com (recommended)	3	0
<input type="radio"/> john2.in.test.postini-corp.com	0	0
<input type="radio"/> john3.in.test.postini-corp.com	0	0
<input type="radio"/> john1alias.in.test.postini-corp.com	0	0

We will provision a Google Apps account for your domain; copy over all of your orgs, users, and settings; and switch your mail flow to Google. Your Postini settings will be set to read-only during the transition process. (For more information, see [this Help Center article](#).)

Click the button below, and your transition process will begin automatically. We will send an email to custadmin30@john1.in.test.postini-corp.com with more instructions once the process is completed.

If you have just one domain, you can initiate your service transition and message transition by clicking [Begin Transition Now](#). This automatically copies your orgs, users, email settings, and messages from Postini to Google Apps.

During this process, your mail flow and filtering will continue without interruption, your MX records will continue pointing to Postini temporarily, and your Postini Admin Console will be in read-only mode. If you're a Google Message Discovery (GMD) customer, initiating your service transition also begins the automatic transfer of your GMD archive data.

Your Postini service is ready to transition to Google Apps.



We will provision a Google Apps account for your domain (solarmoracomp.com); copy over all of your orgs, users, and settings; and switch your mail flow to Google. Your Postini settings will be set to read-only during the transition process. (For more information, see this [Help Center article](#).)

Click the button below, and your transition process will begin automatically. We will send an email to administrator@solarmoracomp.com with more instructions once the process is completed.

Non-blocking items

This section contains a list of items that are not blocking your transition, but you should be aware of these details before you begin your transition. For example, the behavior of a Google Apps setting may be slightly different than the behavior of a comparable setting in Postini.

Binary attachment scanning is not available (UNS_ATTACHMENT_MANAGER_SCAN_BINARIES)

The Postini Attachment Manager "scan inside binaries" feature is not yet available in Google Apps. During your service transition, this setting will not be copied to the Google Apps *Attachment compliance* setting.

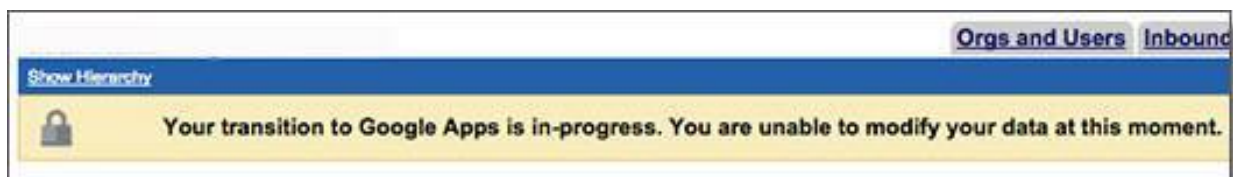
Affected organization: solarmoracomp.com

Catchall spam rejection is unsupported (UNS_UI_CATCHALL_SPAM)

You are using a Postini catchall on one or more domains, and have configured spam rejection for the domain(s). This is not supported in Google Apps. Catchall mail will be delivered to your host with a header indicating the spam status. You are encouraged to set up enumerated addresses for your domain(s) so that you do not need to accept catchall mail.

[Begin Transition Now](#)

When you click [Begin Transition Now](#), the Postini Administration Console will display an in-progress message at the top of the page. The lock icon on the left signifies that Postini is in read-only mode.



4. Review your confirmation email and confirmation message

For many domains, the process of moving your orgs, users, and settings from Postini to Google Apps will be completed within a few minutes, but it may take longer for many other domains. You'll receive a confirmation email when the process is completed, and the Transition Console will display updates so you can monitor the status of your transition.

The length of time required for your transition to be completed depends on the number of users in your account. In general the process will take a few minutes, but it could take longer for some domains that include a large number of users.

If you're a GMD customer, the transition of your archive data, users, and messages to Google Apps Vault will require more time. For very large organizations, the process may take several weeks. You'll receive a separate confirmation message when the process of copying your GMD data to Google Apps Vault is completed. Additionally, you can monitor the process of your GMD transition in the Postini Transition Console by viewing a progress bar at the top of the page.



5. Update your Google Apps Directory Sync (GADS) settings

If you plan to or already use GADS:

After you are notified that your orgs, users, and settings have transitioned to Google Apps, you'll need to [create exclusion rules](#) that prevent GADS from deleting the Google Apps user accounts created during your service transition for former employees, Postini-only users, and sharded user accounts. Then, enable GADS to synchronize user accounts.

For instructions, see [Using GADS and DSS during the transition](#).

6. Get started with Google Apps email settings

Once you receive confirmation that your GMS transition is completed (your orgs, users, and settings are moved to Google Apps), sign in to the Google Admin console to review your email security settings. See [Getting started with advanced settings for Gmail](#) for a detailed mapping of Postini GMS features to Google Apps, and for links to important articles.

7. Outbound customers only: Route your outbound mail through Google Apps

If you're using Postini Outbound filtering, you'll need to follow these steps to complete your Postini transition to Google Apps:

1. Route your outbound mail through Google Apps using the SMTP relay service setting in the Google Admin Console.
2. Configure your on-premise outbound mail server to point to smtp-relay.gmail.com, port 25 or port 465.

For detailed instructions on completing these steps, see [SMTP relay service setting](#).

8. Complete your final transition steps

To complete your transition to Google Apps, you'll need to finish a few cleanup steps, including changing your MX records. You can complete these steps any time after you have clicked **Finish** (for Postini Hybrid customers) or after you have clicked **Begin** (for Postini Classic customers), although we recommend that you wait at least 1 week to change your MX records to verify mail flow. For detailed instructions, see [Steps to complete your transition](#).



Transition steps for Postini Hybrid customers

The steps for your service transition will vary depending on your Postini customer type. If you're a Postini Hybrid customer:

- You're a Google Apps customer who can route mail to on-premise mail servers.
- In addition to Google Apps, you also use Postini message security or message discovery (archiving).
- You log in to the Google Admin console and the Postini Admin Console with separate login credentials.

When you're eligible to transition, you'll receive a transition invitation email, which includes a link to the Postini Transition Console. The Hybrid Transition Console enables you to initiate your transition, test your settings and mail flow in Google Apps, and finish your transition.

Non-Google Apps Postini customers who use on-premise mail servers will use the Classic version of the Transition Console (see *Transition steps for Postini Classic customers*). Most Postini customers who use both Postini and Google Apps will use the Hybrid version of the Transition Console, which is described in this section.

The transition for Postini GMS Hybrid customers includes the following steps:

1. Prepare for your transition.
2. Review your transition invitation email.
3. Begin your service transition in the Postini Transition Console.
4. Review your confirmation email and confirmation message.
5. Update your Google Apps Directory Sync (GADS) settings.
6. Review and verify your Google Apps configuration, and modify if needed.
7. Log in to the Postini Administration Console to continue your transition.
8. Complete your final transition steps.

NOTE: The *service transition* is the process of automatically copying your orgs, users, and settings from Postini to Google Apps. You set this process in motion when you click **Begin Transition Now** in the Transition Console. For most domains, this process is completed within a few minutes, but it may take longer for some domains. You'll receive a confirmation email when it's completed. The *message transition* is the process of automatically moving your messages from Postini to Google Apps. For Postini Hybrid customers, this process is set in motion by clicking **Finish transition** in the Transition Console. For larger organizations, and for organizations transitioning from GMD to Vault, this process will require much more time.

1. Prepare for your transition

To prepare for your transition, you may need to configure your firewall, configure your SPF record (if you already have one), change your Google Apps Directory Sync (GADS) and Directory Sync Service (DSS) setting (if you already use GADS and DSS), verify ownership of your domains, confirm admin privileges,

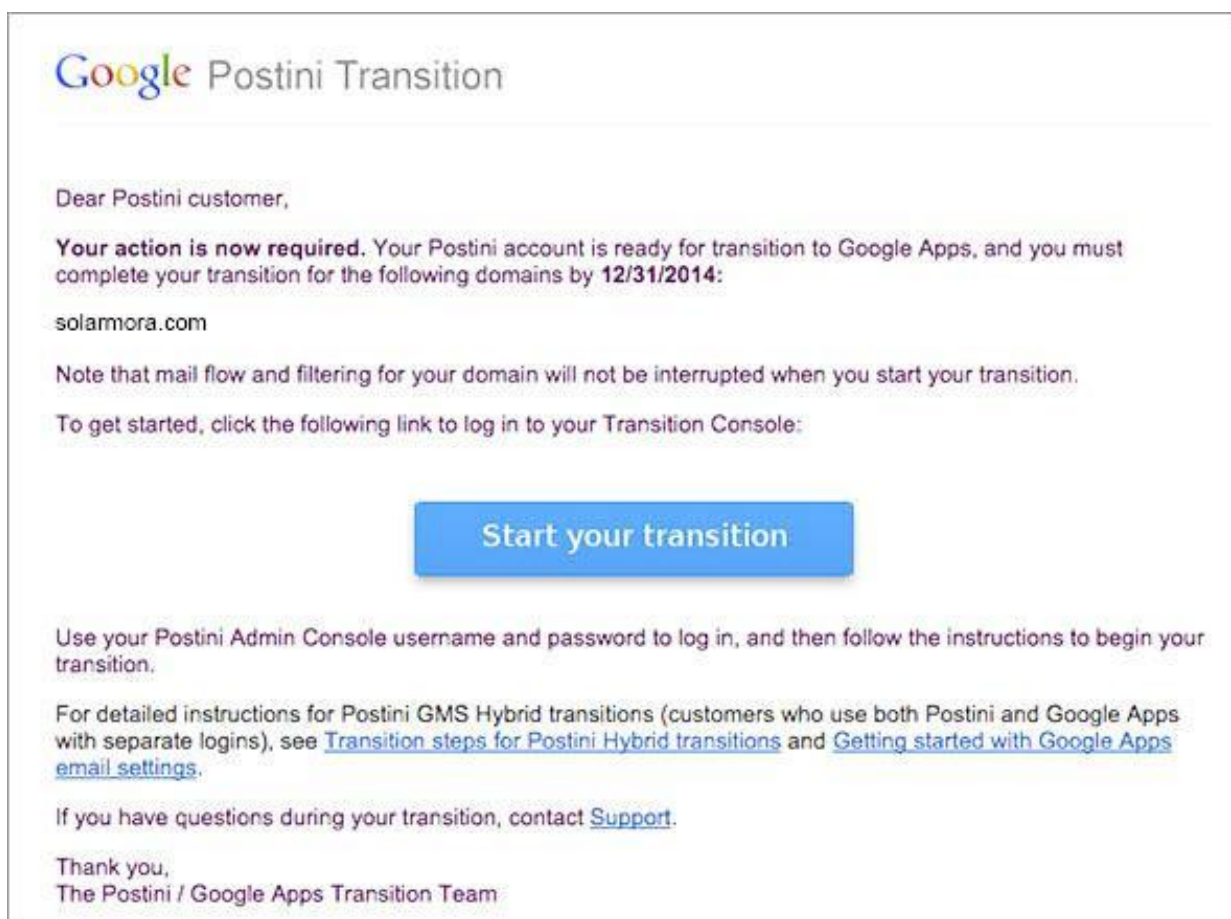


and more. For details, see [Prepare for your transition: Postini Hybrid](#).

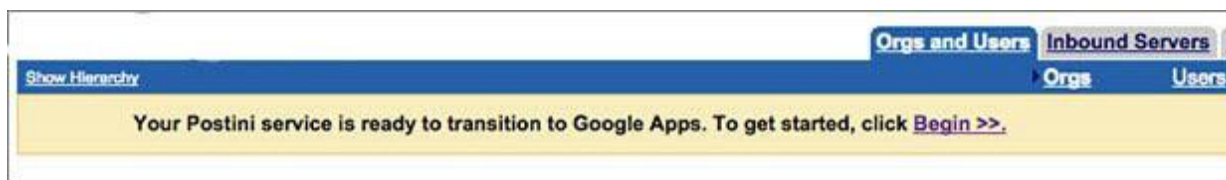
2. Review your transition invitation email

When your account is eligible for transition, Google will send a transition invitation email to administrators for your domain as well as your organization's business contact. Click **Start your transition** to access the Transition Console. You can log in using your Postini Administration Console username and password.

Your transition invitation email will specify the deadline for you to complete your transition—which is within 60 days of receiving the email. (Online Postini customers will have 30 days to complete their transition. For details, see [What's different if I purchased Postini online?](#) in the Postini Transition Resource Center.)



When your account is ready to transition, your Postini Administration Console also displays a link to the Transition Console. Similar to the transition invitation email, a message notifies you that your account is ready for transition.



3. Begin your service transition in the Postini Transition Console

If you have a single Postini account but multiple Google Apps accounts, for each domain in Postini, you must select the Google Apps account to which you want to transition that domain.

NOTE: In general, your Postini domains are automatically mapped to Google Apps during your service transition. However, for a small percentage of Postini Hybrid customers, one or more Postini domains cannot be automatically transitioned because of conflicts with existing Google Apps domains. For details, see [Transitioning Postini domains with mapping conflicts](#).

[Admin Console](#)
[Message Center](#)
[Help Center](#)
[Firewall Check](#)
[Domain Verification](#)

Your Postini service is ready to transition to Google Apps and Google Apps Vault.

Your Postini service is ready to transition to Google Apps and Google Apps Vault for the following domains:

omgmdb.in.test.postini-corp.com, omgmdb3.in.test.postini-corp.com, omgmdb2.in.test.postini-corp.com, omgmdb4.in.test.postini-corp.com

The above domains are part of a single Postini account that you must map to multiple Google Apps accounts. Before initiating your service transition, use the section below to choose how you will map your Postini domains. Every Postini domain must be assigned to one Google Apps account.

Postini domain	Use this Apps domain
omgmdb.in.test.postini-corp.com	omgmdb.in.test.postini-corp.com
omgmdb3.in.test.postini-corp.com	omgmdb.in.test.postini-corp.com
omgmdb2.in.test.postini-corp.com	omgmdb2.in.test.postini-corp.com
omgmdb4.in.test.postini-corp.com	omgmdb2.in.test.postini-corp.com

Once you have finished mapping your Postini domains to your Google Apps accounts, click **Begin Transition Now** to transfer your orgs, users, and settings to your Google Apps accounts. We'll automatically copy your Postini data to a new organizational unit within each account, so your existing Google Apps configuration will not be overwritten.

Non-blocking items

This section contains a list of items that are not blocking your transition, but you should be aware of these details before you begin your transition. For example, the behavior of a Google Apps setting may be slightly different than the behavior of a comparable setting in Postini.

You have one or more Postini user aliases that can't be created in Google Apps (USER_ALIAS_FROM_NOT_ELIGIBLE_OR_SKIPPED_DOMAIN)

You have one or more Postini user aliases that can't be created in Google Apps, or that belong to a different Google Apps account from the users' primary email address. You'll need to transition these user aliases manually.

Affected organization: omgmdb.in.test.postini-corp.com Users

Affected organization: omgmdb.in.test.postini-corp.com Users


NOTE: For a Google Apps account to appear as a destination, it must contain at least one of your Postini account domains.

If you have just one Google Apps account, you can initiate your service transition and message transition by clicking the **Begin Transition Now** button to transfer your orgs, users, and settings to your Google Apps account. Google automatically copies your Postini data to a new organizational unit in Google Apps, so your existing Google Apps configuration will not be overwritten:

- Your Postini org structure will be replicated in a new org below your top-level org in Google Apps.
- Any users that exist only in Postini will be created within this new hierarchy.
- Your transitioned Postini settings will be created in this new hierarchy.

During this process, your mail flow and filtering will continue without interruption, your MX records will continue pointing to Postini temporarily, and your Postini Admin Console will be in read-only mode. See [Managing spam, users, or archiving during GMS or GMD service transition](#) for information about completing common user and administrative tasks.

Your Postini service is ready to transition to Google Apps.



Your Postini service is ready to transition to Google Apps for the following domain:

Click **Begin Transition Now** to transfer your orgs, users, and settings to your Google Apps account. We'll automatically copy your Postini data to a new organizational unit, so your existing Google Apps configuration will not be overwritten.

Next, you'll need to review and verify your settings in Google Apps, move users, and modify your organizational structure if needed. Then, follow the steps in this transition console to route your email through Google.

For more information and instructions, see this [Help Center article](#).

solamora.com

Non-blocking items

This section contains a list of items that are not blocking your transition, but you should be aware of these details before you begin your transition. For example, the behavior of a Google Apps setting may be slightly different than the behavior of a comparable setting in Postini.

Binary attachment scanning is not available (UNS_ATTACHMENT_MANAGER_SCAN_BINARIES)

The Postini Attachment Manager "scan inside binaries" feature is not yet available in Google Apps. During your service transition, this setting will not be copied to the Google Apps *Attachment compliance* setting.

Affected organization: solamora.com users

Catchall spam rejection is unsupported (UNS_UI_CATCHALL_SPAM)

You are using a Postini catchall on one or more domains, and have configured spam rejection for the domain(s). This is not supported in Google Apps. Catchall mail will be delivered to your host with a header indicating the spam status. You are encouraged to set up enumerated addresses for your domain(s) so that you do not need to accept catchall mail.

Begin Transition Now

Non-blocking items

If there are relevant items to display for your account, the Transition Console also reminds you of any non-blocking items you should be aware of before beginning your transition. For example, the behavior of a Google Apps setting may be slightly different than a comparable setting in Postini.

Message transition

From the Transition Console, you can initiate the transition of your email messages later in the process, when you click Finish transition. If you're a Google Message Discovery (GMD) customer, you'll also initiate the transition of your archive data and messages later in the process. For more details, see "Change mail processing to Google Apps."

IMPORTANT:

When you've been invited to transition, you have no blocking items preventing you from transitioning, and you have passed the dry-run tests. Initiating your service transition will not disturb your existing configuration in Google Apps.

Additionally, because you can set up your organizations in passthrough mode during the Hybrid transition process, this enables you to "roll back" your transition temporarily as you test your settings and mail flow. Passthrough mode means your mail is "passed through" from Postini to Google Apps, and your MX records continue pointing to Postini temporarily. Passthrough enables you to test the functioning of your settings before you complete your transition.

The transition process is only irreversible when you click **Finish transition** on the last page of the Transition Console.

4. Review your confirmation email and confirmation message

After your orgs, users, and settings are copied to your Google Apps account, you'll receive a confirmation email that will prompt you to continue your transition by returning to the Transition Console.

5. Update your Google Apps Directory Sync (GADS) settings

For details, see [Using GADS and DSS during the transition](#).

6. Review and verify your Google Apps settings, and modify if needed

After your Postini orgs, users, and settings are copied to a new organizational unit in Google Apps, you'll need to sign in to the Google Admin console to [review](#) and verify your settings in Google Apps (see [Getting started with advanced settings for Gmail](#)), move users, [modify your organization structure](#) if needed, and adjust your routing settings. While making these adjustments, mail will still flow from Postini. You will be asked to change mail processing to Google Apps in later steps in the Transition Console.

During your service transition, your Postini GMS OU structure is replicated in a new OU below your top-level OU in Google Apps. After this is done, you may wish to adjust your orgs by moving users and/or copying settings. To review your Google Apps settings and org structure, sign in to the [Google Admin console](#). Note that while making adjustments to your Google settings, mail will still flow from Postini.

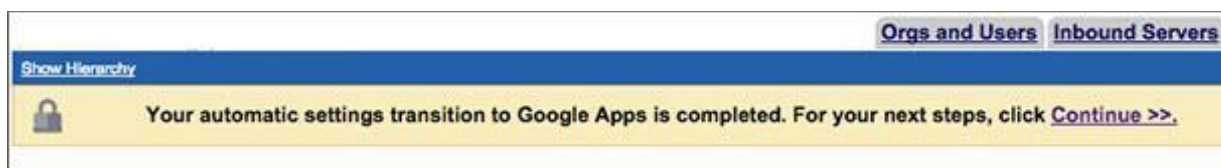


From the Google Admin console, do the following:

- Review and verify your transitioned settings (see Admin checklist: [Getting started with advanced settings for Gmail](#)).
- If needed, copy your transitioned Postini settings to the appropriate organizational units. For example, you might want to copy settings from one of your transitioned Postini OUs to an OU that's already existing in your Apps org structure. For instructions on how to copy a setting to another OU, see [How to use the controls on the Advanced settings page](#).
- Review your organizations, and if needed modify your organizational structure (see [Modify the organizational structure](#)).
- Review your users, and if needed, move your users to the appropriate organizational units (see [Move a user to an organizational unit](#)).
- If needed, enable domain default routing (see [Default routing setting](#) for instructions).
- Verify routing to your on-premise mail hosts. If needed, adjust the Non-Gmail mailbox routing setting (see [Non-Gmail mailbox routing](#)).

7. Log in to the Postini Administration Console to continue your transition

Once you have reviewed your Google Apps configuration, return to the Postini Transition Console to complete your transition. The Admin Console displays a message at the top of the page. Click Continue to access the Transition Console. (The lock icon on the left signifies that Postini is in read-only mode.)



How to access the Postini Transition Console

Your Transition Invitation email provides a link to the Transition Console, where you can log in using your Postini Admin Console username and password, or you can [sign in directly](#) to Postini and click the links to the Transition Console. You'll need to follow the steps in the Transition Console to route your email through Google, and then observe mail flow in your domain before completing your transition.

After you verify your Google Apps settings, check all of the boxes on this page, and click Next.

Modify and verify your Google Apps configuration



Your Postini orgs, users, and settings have been copied to a new organizational unit in Google Apps. Sign in to the [Google Admin console](#) to verify your settings in Google Apps, move users, modify your organizational structure if needed, and adjust your routing settings. While making these adjustments, mail will still flow from Postini. You will be asked to change mail processing to Google Apps in the next step. See this [Help Center article](#) for instructions.

Once you have verified your Google Apps settings, highlight the following check boxes and click **Next** to confirm:

- ☒ I have reviewed and verified my transitioned settings
- ☒ I have reviewed my organizational structure, and have modified, if needed
- ☒ I have reviewed my users, and have moved them to the appropriate organizational units, if needed
- ☒ I have enabled default routing, if needed
- ☒ I have applied and verified routing to my on-premise mail hosts, if needed

Next

Change mail processing to Google Apps

During your service transition, your Postini orgs, users, and settings were copied to a new organizational unit (OU) in your Google Apps account, and the Postini Admin Console was placed in read-only mode. However, your mail continues to be routed through Postini temporarily, and Postini filtering remains in effect.

Once you have verified your Google Apps configuration, it's time to re-route your Postini mail to Google Apps. Before you do this, test your mail flow by selecting ON for a subset of organizational units, or select ON for all OUs. You can then test mail flow to and from users in your domain, and click OFF if needed.


NOTE: As a preparation step for your transition, we recommend that you create a pilot org in Postini before you initiate your service transition—especially if you have a simple hierarchical structure in Postini (one account org, one email config org, and one user org). This enables you to test mail flow to Google Apps for a subset of your users in select organizations before completing your transition. If you have multiple organizations in Postini, you can select any existing organization to test your settings after your transition, rather than create a pilot org.

Once your Google Apps configuration is working to your satisfaction, select ON for every organizational unit, and click Finish transition.

If you're a Postini archiving (GMD) customer, clicking Finish transition also begins the transfer of your

GMD archive data.

Change mail processing to Google Apps



During your service transition, your Postini orgs, users, and settings were moved to a new organizational unit (OU) in your Google Apps account, and the Postini Admin Console was placed in read-only mode. However, your mail continues to flow through Postini temporarily, and Postini filtering remains in effect.

Now that you have verified your Google Apps configuration, it's time to change your mail processing from Postini to Google Apps. First, check that you're satisfied with your Google Apps settings by selecting **ON** for a subset of organizational units, or select **ON** for all OUs. By doing this, Postini filtering is disabled, but mail flows through, thereby relying solely on filters and policies configured in Apps. You can then test mail flow to and from users in these OUs, and click **OFF** if you need to reinstate Postini filters while you make adjustments in Apps.

Once your Google Apps configuration is working to your satisfaction, select **ON** for every organizational unit, and click **Finish Transition**.

Organization	Re-route mail
solarmora.com Account	<input type="button" value="OFF"/>
solarmora.com Email Config 1	<input type="button" value="OFF"/>
solarmora.com Users	<input type="button" value="OFF"/>

When you click **ON**, you'll be asked to confirm your selection:

Are you sure you want to re-route mail for this organizational unit to Google Apps?

☒ Include all sub-orgs

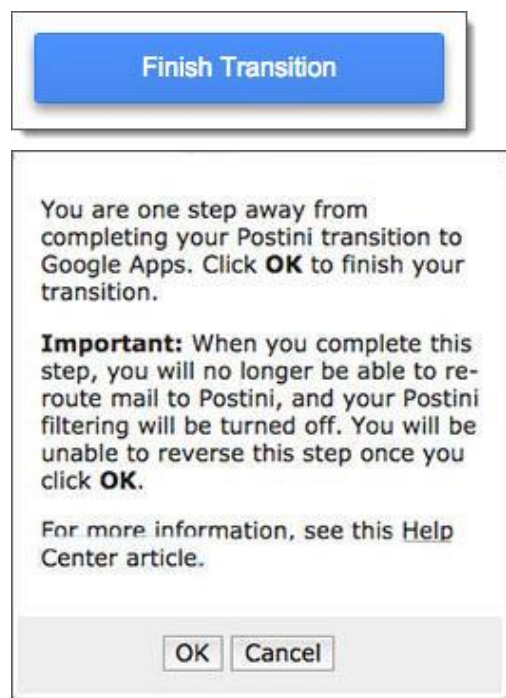
NOTE: At this point in the process, you can still change your routing back to Postini if needed.

Finish your service transition

Once you're satisfied with the functioning of your settings in Google Apps, and once you have confirmed proper mail flow, select ON for all of your organizations, click Finish Transition, and click OK to confirm.

WARNING: When you complete this step, you'll no longer be able to re-route mail to Postini, and your

Postini filtering will be turned off. You will be unable to reverse this step once you click OK. By clicking Finish Transition, and then confirming by clicking **OK**, you are initiating the transition of your email messages to Google Apps. If you're a GMD customer, this also initiates the transition of your archive data and messages.



When this process is completed, you'll receive an email confirmation message. The length of time required for your transition to be completed depends on the number of users in your account. In general the process will take a few minutes, but it could take longer for some domains that include a large number of users. You'll receive a confirmation email when this process is completed.

If you're a GMD customer, the transition of your archive data, users, and messages to Google Apps Vault will require more time. For very large organizations, the process may take several weeks. You'll receive a separate confirmation message when the process of copying your GMD data to Google Apps Vault is completed. Additionally, you can monitor the process of your GMD transition in the Postini Transition Console by viewing a progress bar at the top of the page.

Sign in to Google Apps to get started

Once you receive confirmation that your orgs, users, and settings are transitioned and then finish your transition in the Postini Transition Console, we recommend that you sign in to the Google Admin console to review your Postini settings and to familiarize yourself with how the transferred settings appear, and to make any adjustments if necessary.

For instructions on how to perform many common tasks in the Google Admin console that are comparable to Postini, and to learn how to modify specific Google Apps settings after your service transition, see the chapters below.

8. Complete your final transition steps

To complete your transition to Google Apps, you'll need to finish a few cleanup steps, including changing your MX records. You can complete these steps any time after you have clicked **Finish** (for Postini Hybrid customers) or after you have clicked **Begin** (for Postini Classic customers), although we recommend that you wait at least 1 week to change your MX records to verify mail flow. For detailed instructions, see [Steps to complete your transition](#).

Managing spam and users during the GMS Hybrid service transition

This table identifies when filtering services transition from Postini to Google Apps and in which system users and administrators perform common tasks during GMS Hybrid service transition.

		Invited	Transition started	Passthrough enabled	Transition completed
Services	MX records	Postini	Postini	Postini/Apps	Apps
	Mail filtering	Postini	Postini	Apps	Apps
Users	View spam	Postini	Postini	Apps	Apps
	Change blacklist/whitelist	Postini	X	Apps	Apps
Administrators	Add users	Postini	Apps*	Apps	Apps
	Remove users	Postini	Apps*	Apps	Apps
	Suspend users	Postini/Apps	Apps*	Apps	Apps
	Change display name	Postini/Apps	Apps	Apps	Apps
	Change primary email address	Postini	Apps	Apps	Apps
	Add a user alias	Postini	Apps	Apps	Apps
	Auto-assign licenses	Apps	Auto OFF	Manual ON	Apps
	Move OU	Postini	Apps	Apps	Apps
	Change user password	Postini	Apps	Apps	Apps
	Change spam filters	Postini	X	Apps	Apps

	Access reports	Postini	X	Apps	Apps
* Takes effect when Postini is in passthrough state. See the FAQs at the end of this guide for more information about passthrough.					

Using GADS and DSS during the transition

If you use Google Apps Directory Sync (GADS) and Postini Directory Sync Service (DSS), there are a few steps to you'll need to complete as part of your transition. These changes are important to the transition process, and will help prepare your environment for life after Postini, including new user types such as Vault Former Employee and Postini only user accounts.

NOTE: Though not mandatory for transition, we recommend that you upgrade to [GADS 4.0.1](#) for its new features and bug fixes and to avoid using deprecated APIs. For more information about deprecated APIs and timelines, see this [Google Apps Update](#).

Before the transition

1. Set up GADS to [suspend Google Apps users](#) not found in Lightweight Directory Access Protocol (LDAP).
2. Disable DSS. DSS is not used after the transition.
3. Disable the GADS scheduled sync or cron job so that GADS does not make changes during the transition.

During the transition

After you are notified that your orgs, users, and settings have been transitioned from Postini to Google Apps, continue synchronizing user accounts:

Before you enable GADS again, ensure that GADS does not want to delete users, groups or organizational units created in the transition.

1. Set up these [Google Apps Exclusion Rules](#) in GADS:

Type	Match type	Exclusion rule
Organization Complete Path	Substring match	Copied from Postini
Organization Complete Path	Substring match	Former Employees
Group Email Address	Substring match	_extra_aliases@



2. Simulate a GADS sync to verify changes.
3. Enable the GADS scheduled sync or cron job.

After the transition

After your service transition completes, you may want to:

- Combine the **Former Employees** organizational unit with any existing organizational unit for deprovisioned users.
- Merge your previous organizational unit structure with organizational units created for the transition and use GADS to manage all user accounts. You may need to restructure your organizational units and their settings and ensure that all users that are created during the transition are in your LDAP system.

Steps to complete your transition

To complete your transition, you'll need to finish the following clean-up steps. You can complete these steps any time after you receive a confirmation email that your mail is now routed through Google Apps and your orgs, users, and settings have been transitioned to Google, although we recommend that you wait at least 1 week to change your MX records to verify mail flow.

NOTE: We recommend that you wait to change your Postini inbound gateway until after you change your MX records.

1. Change your MX records to Google Apps

Changing your mail exchange (MX) records is one of the final steps in your transition from Postini to Google Apps. Once your orgs, users, and settings have been moved to Google Apps, you will need to update your domain settings (your MX records) to route email messages through the Google Apps mail servers.

This can be done any time after you have clicked **Finish** (for Postini Hybrid customers) or after you have clicked **Begin** (for Postini Classic customers), although we recommend that you wait at least 1 week after this step to verify mail flow.

To learn more about your inbound and outbound mail flow after you change your MX records, see [After your transition: Google Apps mail flow diagrams](#).

Why you need to change your MX records

Until you change your MX records, your mail is unnecessarily routing through the Postini data center. You will experience the best results -- for both your users and administrators -- after you change your MX records to Google Apps.

How to change your MX records

To complete this step, use the administration console for your domain provider. From there, you can create MX records that point to Google Apps.

For step-by-step instructions and other important details, see [Set up MX records](#) and [MX record values](#). See also the guidelines below.

Insert the following DNS MX records for each of your domains:

Priority	Mail server
1	ASPMX.L.GOOGLE.COM.
5	ALT1.ASPMX.L.GOOGLE.COM.
5	ALT2.ASPMX.L.GOOGLE.COM.



10	ALT3.ASPMX.L.GOOGLE.COM.
10	ALT4.ASPMX.L.GOOGLE.COM.

Each record points to a Google mail server. You enter these values at your domain host, not in your Google Admin console. Note that some hosts use different labels for the name and value fields, and many domain hosts also require a trailing period at the end of the server name.

Important guidelines for changing your MX records:

- ASPMX.L.GOOGLE.COM must be the top priority record.**
 The Priority column shows the relative priorities of the Google mail servers. Mail is delivered to the server with the highest priority first. If for some reason that server isn't available, mail is delivered to the server with the next highest priority, and so on through all your the servers. Priority values don't need to be exactly like those shown in the table. And in fact, different domain hosts have different systems for setting MX record priority. Regardless of your domain host's system for indicating priority, ASPMX.L.GOOGLE.COM must be the top priority record.
- After changing your MX records to Google Apps, be sure to remove all MX records that contain .PSMTP.COM (the Postini MX records).
- If your domain provider enables you to set the Time to Live (TTL) value for the record, set it to 3600 seconds if there is no suggested value from your domain provider. The TTL is the number of seconds before subsequent changes to the MX record go into effect. See [Time To Live \(TTL\)](#) for more details.
- Changes to MX records can take up to 48 hours to propagate throughout the Internet.

If you have difficulty changing MX records, contact your domain provider for assistance. For more instructions, see [MX record values](#) and [Understand MX records](#).

2. Route your outbound mail through Google Apps

If you're using Postini Outbound filtering, you'll need to follow these steps to complete your Postini transition to Google Apps:

- Route your outbound mail through Google Apps using the SMTP relay service setting in the Google Admin Console.
- Configure your on-premise outbound mail server to point to smtp-relay.gmail.com, port 25 or port 465.

For detailed instructions on completing these steps, see [SMTP relay service setting](#).

3. Remove Postini from your inbound gateway

To complete your transition to Google Apps, you'll need to remove Postini IP addresses from your inbound gateway setting. For instructions, see [Inbound mail gateway](#).



Complete this step only after you have changed your MX records to Google Apps. Once you change your MX records, mail coming from Postini should no longer get special treatment, as Postini is no longer an expected mail source.

4. Update your Google Apps Directory Sync (GADS) settings

If you plan to or already use GADS--After you are notified that your orgs, users, and settings have transitioned to Google Apps, you'll need to [create exclusion rules](#) to prevent GADS from deleting the Google Apps user accounts that are created during your service transition for former employees, Postini-only users, and sharded user accounts. Then enable GADS to synchronize user accounts.

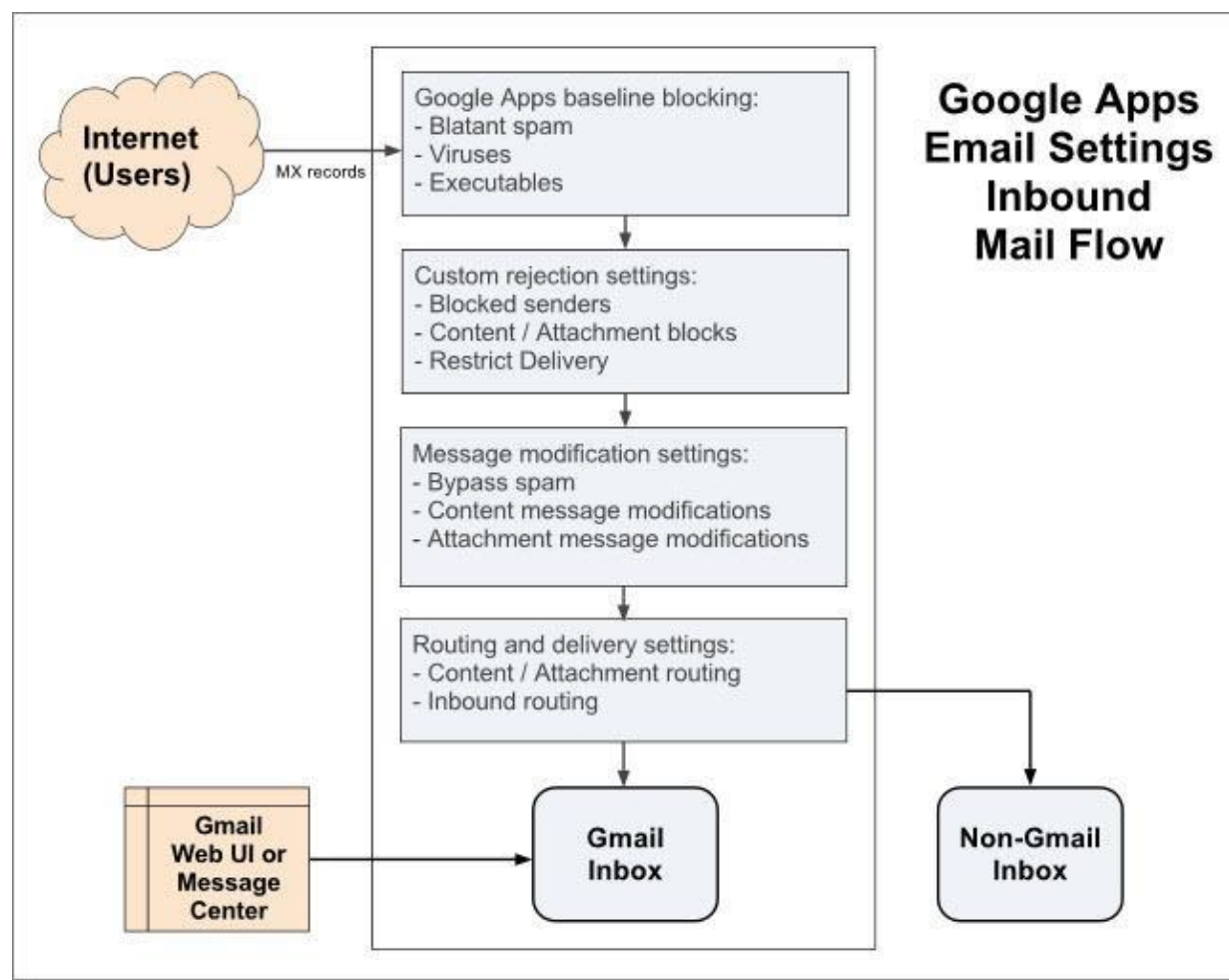
After your transition: Google Apps mail flow diagrams

Inbound mail flow

Once you complete your transition from Postini to Google Apps, your MX records point to Google, and your inbound mail is filtered for spam, viruses, and executables. Your Google Apps email settings determine if a message is rejected, modified, or rerouted. For example, you can configure your settings to modify messages based on message content or attachments.

During your transition, your Google Apps settings are automatically configured to route inbound mail to your corporate non-Gmail service.

For instructions on how to use the Google Apps email settings, see [Configure advanced settings for Gmail](#). See also [Guidelines for configuring advanced settings for Gmail](#).

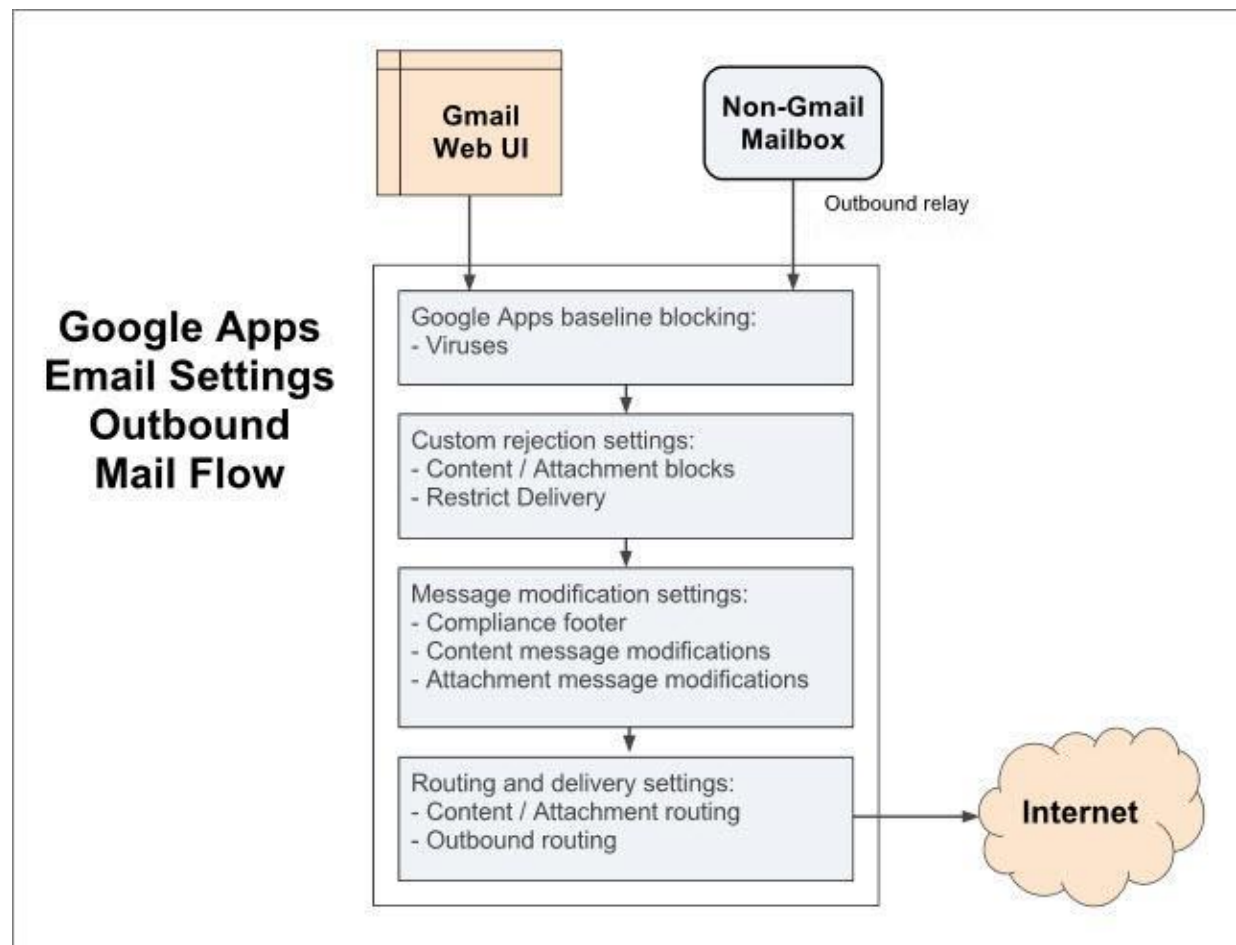




Outbound mail flow

The SMTP relay service setting will enable you to set up outbound filters for your non-Gmail corporate mailbox. The diagram below shows how various Google Apps email settings will work with outbound mail flow -- including virus filtering, custom rejection settings, message modification settings, and routing and delivery settings.

For instructions on how to use the Google Apps email settings, see [Configure advanced settings for Gmail](#). See also [Guidelines for configuring advanced settings for Gmail](#).



Improvements and changes in moving from Postini to Apps

In most cases, the tasks you can perform in the Google Apps Admin console are similar to those you did in the Postini Admin console. You can learn about those equivalent features [here](#) and within this guide.

Beyond providing similar functionality, Google Apps offers a number of feature enhancements and improvements compared to what's available in Postini. In a small number of cases, a feature that was available in Postini works differently, or is not supported, in Google Apps. This article explains those feature differences and provides comparisons between Google Apps and Google Message Security in Postini.

For a detailed comparison of Google Message Discovery (Postini archiving) to Google Apps Vault, see [Postini Transition Guide: Getting started with Google Apps Vault](#).

Google Apps feature enhancements compared to Postini GMS

Spam, virus, and content filtering

Postini Feature/Capability	Improvement/Enhancement in Google Apps
Regular expressions	Full regular expression syntax—not just a subset—is available in the Content compliance setting.
Email protection, filtering, policies, sender lists	Google Apps doesn't have a limit of 4,000 characters as Postini did. You can add large numbers of approved and blocked senders at the user organization level.
Improved spoofing protection	Google Apps lets you configure DKIM signing and DMARC for your organization's mail.
Attachment filtering	You can remove attachments that violate policies but allow delivery of the message text.
Longer spam hold times	Google Apps retains spam for 30 days, as opposed to 14 days with Postini.

Email delivery and routing

Postini Feature/Capability	Improvement/Enhancement in Google Apps
Domain restrictions	You can restrict the sending and receiving of users' emails to specific domains (often useful in educational environments).
Custom routing	Google Apps lets you route mail to preferred routes or smarthosts based on message attributes.
Advanced filter options	When a message triggers a filter, you can reroute messages or send to additional recipient mailboxes other than the Spam (quarantine) folder.

Management features

Postini Feature/Capability	Improvement/Enhancement in Google Apps
Policy inheritance	If you set or delete a policy in a user organization, the policy change automatically applies to all sub-organizations (unless you customize the policy setting within the sub-organization)
Outbound footers	You can create rich footers in HTML and set multiple footers based on message filters
Language support	The Google Apps Admin console is available in 28 languages , while Google Apps supports double and multibyte characters (supporting the same languages as Gmail).
Google Apps integration	Administrators and users no longer have to manage multiple logins, because you use a single Admin console to manage both Google Apps and the message security and compliance features.

Postini features that work differently in Google Apps

NOTE: Many of the feature differences between Postini and Google Apps are related to spam and virus filtering. To learn more about these spam and virus filtering differences, see *How Gmail spam and virus filtering differs from Postini*.

Task	Postini feature name	How Google Apps is different
Manage messages in Message Center	Message Center	Message Center is available for non-Gmail Inbox users. Users can view and manage messages marked as spam (as well as delivered messages, if the administrator enables this feature). Some features work differently, or are unavailable, in Google Apps. For details, see <i>Message Center and Quarantine Summary</i> .

Turn blatant spam blocking on/off	Blatant Spam Blocking	Google Apps automatically rejects blatant spam at a rate similar to Postini, so the on/off capability is not needed.
Delete (blackhole) messages identified as spam	Blackhole	The blackhole disposition is unnecessary, often harmful, and a violation of the Simple Mail Transfer Protocol (SMTP) specification. With poorly written filters that generate false positives, blackholed mail provides no recourse to the sender; there's little evidence to suggest spammers glean any intelligence from seeing rejections. Thus, Google Apps does not support the delete (blackhole) disposition. If you have a blackhole disposition set in Postini, the transition tool changes this to a Reject disposition.
Quarantine spam messages/attachments by user	User Quarantine	<p>Google Apps offers a single Spam folder, as opposed to the multiple quarantine folders (Junk, Virus, and so on) available in Postini. Postini let administrators further manually configure spam rules by sending messages to a quarantine folder based on attachments. This typically occurred to block the attachment and reduce the load on the receiving server.</p> <p>Google Apps has a trainable spam system that learns from user reports of "spam" or "not spam" (for details, see <i>How Gmail spam and virus filtering differs from Postini</i>). For this reason, manually curated spam rules, such as specifying a quarantine folder or sending a message to quarantine based on attachments, are unnecessary. Google Apps always scans all attachments and blocks any with a virus. Additionally, when a Gmail user downloads an attachment, the attachment is again virus-scanned.</p>
Turn virus blocking on/off	Virus blocking	Google Apps always checks for and rejects viruses, so a virus blocking on/off control is unnecessary. Additionally, when a Gmail user downloads an attachment, the attachment is again virus-scanned.
Scan binary attachments	Binary scanning	<p>Google Apps doesn't yet include the Postini Attachment Manager "scan inside binaries" feature. Postini required this feature as the only way to verify the attachment type inside a binary. From a security perspective, this feature is not needed, because Google Apps doesn't allow you to send or receive executable files (such as files ending in .exe), which can contain harmful code that might cause malicious software to download to your computer. If you have set Postini to scan inside binaries, the transition tool doesn't copy this setting to the Google Apps Attachment compliance setting.</p> <p>NOTE: The upcoming "scan inside binaries" feature will improve the existing Attachment compliance setting to leverage binary file type information.</p>
Approve or ignore executable file attachments	Executables > Approve/Ignore	As a security measure to prevent potential viruses, Google Apps doesn't allow you to send or receive executable files (such as files ending in .exe), which can contain harmful code that might cause malicious software to download to your computer. What's more, Google Apps scans binary files for executable and virus

		<p>detection, rather than relying on the filename only. If you have set Postini to approve or ignore executable files, the transition tool doesn't copy this setting to Google Apps.</p>
Approve or ignore compressed file attachments	Compressed Files > Approve/Ignore	<p>Google Apps automatically scans every attachment, including compressed files, for viruses when an attachment is delivered to you. What's more, Google Apps scans all files within a compressed file that match your Attachment compliance criteria. If you have set Postini to approve or ignore compressed files, the transition tool doesn't copy this setting to Google Apps.</p>
Detect multiple attachment file extensions	Attachment Manager > Custom Filter	<p>Postini customers didn't widely use multiple file extension detection. In addition, Google Apps doesn't need this feature from a security perspective, because Google Apps offers the same level of protection against threats as Postini. If you have Postini set to detect multiple attachment file extensions, the transition tool doesn't copy this setting to Google Apps.</p>
Redirect quarantined messages/attachments to a specified address	Quarantine redirect	<p>Google Apps offers you the ability to redirect messages to another address. However, while Postini gives you the option to deliver those messages to either the second address's Inbox or Spam (quarantine) folder, Google Apps delivers them to the second address's Inbox.</p> <p>Google Apps has a trainable spam system that learns from user reports of "spam" or "not spam" (see <i>How Gmail spam and virus filtering differs from Postini</i>). For this reason, manually curated spam rules, such as quarantine redirect, are unnecessary.</p> <p>NOTE: The upcoming Admin Quarantine feature will let you redirect messages to a special quarantine folder (separate from the Spam folder) for the administrator user.</p>
Send a copy of a message to another address's quarantine folder	Bcc Quarantine, Copy to Admin Quarantine, Copy to Other Quarantine, Copy to Recipient Quarantine	<p>In addition to redirecting a message to another user's Spam folder, Postini lets you both deliver a message to the recipient's Inbox and copy the message to a user's Spam (quarantine) folder in a number of ways: as a Bcc to a specified address, as a copy to the administrator's address, as a copy to another user's address, or as a copy to the recipient's address. Google Apps simplifies this by letting you send a copy of a message as a Bcc to the Inbox of any other user address you specify (administrator or not).</p> <p>Google Apps has a trainable spam system that learns from user reports of "spam" or "not spam" (see <i>How Gmail spam and virus filtering differs from Postini</i>). For this reason, manually curated spam rules, such as sending messages to other addresses, are unnecessary.</p>
Approve a specified type of attachment	Attachment Manager > Approve	<p>Google Apps always recognizes any combination of settings—such as reject or reroute—that you set for a given content or attachment type (to learn more, see <i>Guidelines for configuring advanced settings for Gmail</i>). The Approve disposition offered in</p>

		Postini acts to bypass or override some other settings in a complex fashion, depending on which setting overrides which. By not allowing any one setting to negate another, Google Apps is based on more straightforward, easier-to-understand logic.
Deliver a specified type of content	Content Manager > Deliver	Google Apps always recognizes any combination of settings—such as reject or reroute—that you set for a given content or attachment type (to learn more, see <i>Guidelines for configuring advanced settings for Gmail</i>). The Deliver disposition offered in Postini acts to bypass or override some other settings in a complex fashion, depending on which setting overrides which. By not allowing any one setting to negate another, Google Apps is based on more straightforward, easier-to-understand logic.
Set heuristics for legal and financial services senders	Industry Heuristics	Google Apps doesn't include industry heuristics, because they were developed in an earlier era of the spam threat environment and are no longer needed. Postini uses these rules to provide preferential treatment for legal and financial services senders, but over time they have resulted in increased false positives and are of limited utility.
Allow users to forward messages to a mobile number	Wireless Settings	Google Apps doesn't support this feature. Wireless settings allow users to forward messages to an SMS number. Developed before smartphones were widely available, this feature was available only to Message Center Classic users and now serves little purpose.
Set spam sensitivity levels for a specified message type	Filter Sensitivity	Administrator and end user spam sensitivity and category controls have limited effectiveness in the modern spam environment and can raise false positive rates. Google spam filtering is integrated into Google Apps. There are no administrative settings for changing your spam filtering (spam filtering is simply "on" by default), other than an upcoming option to enable more aggressive bulk spam filtering.
Brand Message Center/quarantine summary	Branding	Postini customers didn't widely adopt Message Center or quarantine summary branding. Google Apps doesn't include this feature.
Set spam sensitivity levels and approved/blocked sender lists per user	Users > Spam Filtering, Virus Blocking, Sender Lists	<p>Google Apps has a trainable spam system that learns from user reports of "spam" or "not spam" (see <i>How Gmail spam and virus filtering differs from Postini</i>). For this reason, manually curated approved or blocked sender lists, as well as sensitivity levels, are unnecessary.</p> <p>However, users can create an approved senders list by specifying contacts. Messages from these senders receive more lenient spam filtering.</p>
Access user quarantines	User Quarantine	Unlike Postini, Google Apps administrators can't sign in to a user's Message Center as that user. However, the Admin Quarantine feature will let an administrator quarantine inbound Spam for review prior to delivery to the end user.
Set password	Password	Google Apps allows an administrator to view a user's password

configuration policies	Policies	strength after the user sets it. An administrator can then advise the user to create a stronger password if needed. If additional security is required, Google Apps supports both two-factor authentication and Active Directory sync. Also, customers with stringent policies can implement single sign-on and whatever on-premise policy enforcement they choose.
Manage multiple primary domains		In Google Apps, there's only one primary domain. If you have multiple primary domains in Postini, each of these domain names is transferred to the Domain settings page in the Google Admin console, but the domains are displayed differently. To learn more about multiple domains in Google Apps, see Add domain or domain aliases , Managing multiple domains , and Limitations for multiple domains .
Create a catchall user for spam filtering for a domain	Catchall user	Postini includes the option to create a catchall user on one or more domains and to configure spam rejection for the domains. Google Apps delivers catchall mail to your host with a header indicating the spam status. We recommend that you set up enumerated addresses for your domains so that you don't need to accept catchall mail.
Spool mail for later delivery	Spool Mgr	When your on-premise mail server is unavailable, Postini can spool mail for later delivery. Because Google Apps Gmail is a store-and-forward system, it stores and retries messages automatically. Google Apps retries a message for a period of seven days until either it successfully delivers the message or the 7-day retry period expires. For more details, see 'Spooling' in Google Apps: Retrying messages.
Customize SPF, DKIM, and IP Lock settings	SPF, DKIM, IP Lock	SPF, DKIM, and IP Lock tools require complex management by the customer and are most useful to get around either Postini's limitation on approved sender lists or a particular sender's failure to adopt industry-standard SPF or DKIM authentication methods. By default, Google Apps approved sender lists automatically consider mail authentication. In addition, Google Apps automatically uses SPF, DKIM, and DMARC in its spam evaluation. If you have customized SPF and DKIM settings in Postini, the transition tool doesn't move these to Google Apps. If you have IP Lock settings, the transition tool copies these to equivalent Content compliance settings.
Set IP Lock to delete (blackhole) messages	IP Lock > Blackhole	The blackhole disposition is unnecessary, often harmful, and a violation of the SMTP specification. With poorly written filters that generate false positives, blackholed mail provides no recourse to the sender; there's little evidence to suggest spammers glean any intelligence from seeing rejections. Thus, Google Apps does not support the delete (blackhole) disposition. If you have a blackhole disposition set in Postini, the transition tool changes this to a Reject disposition.
Set IP Lock to skip all checks	SPF > Pass - Skip IP Lock text	Google Apps has a precedence system that allows you to skip spam checks only, and ignores other skipped checks you set in Postini. Google Apps always recognizes any combination of settings—such as reject or reroute—that you set for a given content or attachment type (for details, see Guidelines for

		configuring advanced settings for Gmail). Skipping checks acts to bypass or override these other settings in a complex fashion depending on which setting overrides which. By not allowing any one setting to negate another, Google Apps is based on more straightforward, easier-to-understand logic.
Use SSN or credit card numbers as content spam filters	Content Manager > Social Security Numbers, Credit Card Numbers	Postini includes the option to specify credit card or Social Security number filters. Google Apps doesn't have an explicit CC/SSN filter. The transition tool creates a setting that uses a regular expression to detect these patterns. Users can create additional regex filters as needed.
Allow users to set a domain as an approved sender	Approved Senders	<p>Postini allows users to specify a domain as an approved sender. Google Apps contacts lists (used in a similar capacity) support individual email addresses, but not entire domains. The transition tool doesn't include domains when it transitions your users' approved sender lists. As a workaround, you can create an administrative Spam setting to specify domains that are approved senders.</p> <p>Google Apps has a trainable spam system that learns from user reports of "spam" or "not spam" (to learn more, see <i>How Gmail spam and virus filtering differs from Postini</i>). For this reason, manually curated spam rules, such as setting a domain as an approved sender, are unnecessary.</p>
Use SMTP proxy		Postini is an SMTP proxy, where all transmissions between sender and receiver are relayed through the proxy. As a store-and-forward system, Google Apps processes messages in the Google network before sending valid mail onward. This offers the advantage of lower connection overhead, because Gmail sends only valid messages to the customer's server.
Set mail server connection limits	Delivery Manager > Email Servers	With its email proxy architecture, Postini requires mail server connection limits. Because Postini connects to the customer mail server with every spam message, these limits helped protect receiving servers from becoming overwhelmed. Google Apps delivers only clean mail to the on-premise system, so it doesn't need these connection limits.
View the Content Manager outbound activity log	Reports > Content Manager	Because the Postini Content Manager activity log is limited to 5,000 entries, this provides minimal visibility into corporate compliance with content policies. Therefore, Google Apps doesn't offer a content compliance activity log..
Send attachments up to 300 MB	Attachment Manager > Message Size	Unlike Postini's limit of 300 MB, Google Apps Gmail imposes a limit of 25 MB on any sent or received attachments. Because almost all attachments are smaller than this size, this limit has almost no impact on sending and receiving files. On the other hand, imposing this limit does prevent attempts at transmitting enormous files that could impact network speed and bandwidth.
Send the quarantine summary to a	Notifications > Notification Address	Postini allows you to send a quarantine summary to an address different from the message recipient address. This feature serves little practical purpose and Postini customers didn't

different address		widely use it, therefore, Google Apps doesn't offer this option.
Change the quarantine summary sender address	General Settings > Support Contact	Postini allows you to show a "From" address different from your administrator email address in the quarantine summary that appears to users. This feature serves little practical purpose and Postini customers didn't widely use it, therefore, Google Apps doesn't offer this option.
Send unlimited messages using SMTP relay		Unlike Postini, Google Apps Gmail sets limits on the number of messages you can send using SMTP relay. Because these limits scale depending on the number of users, this limit has almost no impact on sending messages. Setting these limits helps us maintain the health of our servers. If a customer mail server gets hijacked or becomes an open relay, the message limits stop the server from sending out too many messages. Because Postini lets a hijacked server send out unlimited messages, Postini's servers get blacklisted, negatively affecting deliverability for all customers.

Get started with the Google Admin Console

Similar to Postini, Google Apps offers a secure, web-based Admin console that lets you manage users, domains, orgs, and settings.

The primary difference is that the Postini Admin console is limited to management of message security, organizations, users, and email server configurations only, while the Google Apps Admin console offers all these capabilities plus management of many other Google Apps included with your account. Thus, Google Apps offers a single point of control for both Google Apps and the message security and compliance features.

Sign in to the Google Admin console

After your transition has completed, sign in to the Google Apps Admin console to access your transitioned settings:

1. In any web browser, go to admin.google.com.
2. On the sign-in page, enter your Google administrator address and password.
3. Click Sign in. If another screen appears asking for your email address and password, just enter this information again.

For general instructions on signing in, see [Sign in to your Admin console](#).

Advanced settings for Gmail

After you sign in to the Google Apps Admin console, you can access your message security and compliance features by clicking **Google Apps > Gmail > Advanced Settings**.

NOTE: You might need to scroll to the bottom of the page to see the Advanced Settings option.

While the message security and compliance-related tasks you can perform in the Google Apps Admin console are similar to—or improve upon—those you did in the Postini Admin console, the Google Apps Admin console may group and name certain features and functions differently.

For general instructions on how to navigate to your Google Apps email settings, and for an overview of the email settings that are available in Google Apps, see [Configure advanced settings for Gmail](#). See the sections below for details regarding specific settings and features, such as Content compliance or Attachment compliance. See also [Guidelines for configuring advanced settings for Gmail](#).

Review and manage your users in Google Apps

During your service transition, your Postini users are moved to Google Apps. Both primary addresses and aliases are copied over. To review your users:



1. [Sign in to the Google Admin console](#).
2. Click the **Users** icon to open the Users page.
3. To review your users within individual organizations -- or organizational units (OUs) -- click any of the organization links in the right column.
4. For instructions on adding users to an organization, or moving users from one organizational unit to another, see [Options for adding users](#) and [Move a user to an organizational unit](#). For instructions and details about user aliases, see [Add email aliases](#) and [Email aliases](#).

After your service transition, you will have read-only access to your Postini Administration Console, so you can sign in and keep the Postini Admin Console open in a separate browser window as you check your Google settings.

Review and manage your orgs and org structure

After your service transition is completed, you may want to review your orgs and org structure to make sure that your new setup is satisfactory to you. You may also want to review the various settings, such as Content compliance, Attachment compliance, and Receiving routing for each OU. (For instructions and details about the different settings and features within the Google Admin console, see the sections below.)

If you want to modify or fine-tune your org structure in the Google Admin console, see [Create an organizational structure](#), [Add an organizational unit](#), and [Modify the organizational structure](#).

NOTE: If your Postini configuration includes just one account org, one email config, and one user org, you will see just one OU in the Google Admin console when you first log in. In Google Apps, the account org and email config org are not necessary, so the org structure will be simplified for you. If needed, you can add sub-organizations. See [Create an organizational structure](#).

Review and manage your domains

Each of your domain names is transferred to the Domain settings page in the Google Admin console. This might include just a single primary domain, or it may also include additional domains or domain aliases that were part of your Postini configuration.

After your service transition is completed, we recommend that you confirm that domain aliases and non-primary domains are copied over. Note that domains are displayed differently in the Google Admin console. For example, in Google Apps there is only one primary domain.

For instructions and details on your domain setup in Google, see [Add domain or domain aliases](#), [Managing multiple domains](#), and [Limitations for multiple domains](#).

Set up and manage admin roles in Google Apps

The Google Admin console offers several pre-defined administrator roles that are not editable (see [Pre-defined administrator roles](#)). Using these pre-defined roles, you can grant administrator privileges appropriate to specific business roles. To create a custom administrator role with different privileges, see [Create custom administrator roles](#).



Other common tasks in the Admin console

Beyond message security and compliance, common tasks you can perform in the Google Apps Admin console include the following:

- [Access settings for non-Gmail inbox users](#)
- [Run reports](#) and [perform email log searches](#)
- Manage [licenses](#) and [billing](#)
- [Provide Admin console access to other admins](#)

Message Center and Quarantine Summary

Similar to Postini, Google Apps offers Message Center for non-Gmail mailbox users, where users can view and manage messages marked as spam (as well as delivered messages, if you enable this setting). You can enable this feature via the Non-Gmail mailbox setting in the Google Admin console.

Your non-Gmail users can also use the Quarantine Summary report, which is a periodic summary of messages sent to your users' inboxes. By default, the Quarantine Summary contains a list of emails that were recently marked as potential spam.

How the transition works for the Message Center and Quarantine Summary

Messages in your Postini Message Center are not transitioned to Google Apps during your service transition. If you want to make Message Center available in your organization, you'll need to enable this setting in Google Apps after you complete your transition.

During your service transition, your Postini Quarantine Summary settings are moved to the Non-Gmail mailbox setting. After your transition, we recommend that you check your Non-Gmail mailbox settings to make sure Quarantine Summary reports are enabled.

Configure Message Center and Quarantine Summary

For administrator instructions to help you configure Message Center and Quarantine Summary in Google Apps, see [Set options for non-Gmail mailbox users](#).

Instructions for your users

For user instructions on the Message Center, see [Manage messages in Message Center](#). For user instructions on the Quarantine Summary, see [Quarantine summary report](#). If you plan to enable both of these features, we recommend that you send an email notification to your users with links to the above two articles. See also [Manage spam messages in Gmail](#).

Compare Google Apps spam and virus filtering to Postini

After your orgs, users, and settings are transitioned from Postini to Google Apps, you'll automatically begin using the Gmail spam and virus protection instead of Postini's. You should expect the Gmail and Postini filters to behave differently, acting more strict or lenient on different types of mail.

For a detailed comparison of Postini filtering to Google Apps, and for more details about Message Center and Quarantine Summary, see *How Gmail spam and virus filtering differs from Postini*.

Message Center feature differences and improvements

Some Postini Message Center features work differently in Google Apps, including the following:



- Google Apps Message Center does not maintain a Virus Quarantine folder (because all virus-infected messages are rejected) or an Archive folder (although one may be available in the future). The available folders are Delivered, Spam (equivalent to the Postini Junk folder), and Trash.

NOTE: The Delivered folder appears only if the administrator turns on the option to display delivered messages in Message Center.

- The Google Apps Message Center settings include adding approved contacts (senders) only. They do not include the following Postini settings:
 - **Junk Settings: Block Senders; Manage Junk Filters**—Google Apps has a trainable spam system which learns from user reports of “spam” or “not spam” (learn more [here](#)). This trains the mail system to more accurately filter messages, making user-managed blacklists unnecessary.
 - **Virus Settings: Manage Virus Blocking**—Because the system rejects all viruses, this setting is unnecessary in Google Apps.
 - **Personal Settings: Change Password**—Because users access Google Apps Message Center with their Google Apps username and password, [changing this password in Google Apps](#) also changes it for Message Center.
 - **Personal Settings: Add Alternate Email Addresses**—Alternate email addresses are called “aliases” in Google Apps. The administrator can [configure aliases for users](#), but users can’t configure their own aliases.
 - **Personal Settings: Set Time Zone, Language**—The system auto-detects the time zone and language, making these settings unnecessary.
 - **Personal Settings: Set Character Encoding**—Character encoding in Google Apps applies to outgoing messages only, and is, therefore, not relevant for Message Center.

How Gmail spam and virus filtering differs from Postini

Once your orgs, users, and settings are transitioned from Postini to Google Apps, you'll automatically begin using the Gmail spam and virus protection instead of Postini's. You should expect the Gmail and Postini filters to behave differently, acting more strict or lenient on different types of mail.

Spam filtering differences

One of the basic principles of the Gmail spam filtering system is that it responds to input from users. Gmail users can “train the system” by clicking Report spam or Not spam. The more frequently a user reports spam (or indicates that a message is not spam), the more effective this filtering mechanism becomes.

NOTE: Gmail does not require explicit interaction by the user to manually adjust thresholds or add approved or blocked senders. However, as users mark messages as spam or not spam, Gmail customizes filtering behavior for those types of messages.

Following their transition to the Google Apps platform, non-Gmail users (for example, users on Microsoft Exchange) can manage spam using [Message Center and the quarantine summary](#). These enable non-Gmail users to mark messages as spam or not spam.

NOTE: Spam messages are stored in the Google Apps platform for 30 days, while Postini typically stores messages for 14 days.

How should admins and users deal with bulk email messages?

Gmail handles promotional emails differently than Postini. Postini tends to filter certain types of marketing-related or special-offer bulk mail, while Gmail is more likely to allow this type of mail through. A simple way to think of it is that mail landing in the Gmail Promotions tab likely would have been blocked as spam by Postini.

By allowing users to train the system by identifying messages as spam or not spam, Gmail provides fine-grained control over which bulk mail your users will receive without the direct use of approved and blocked senders lists. Filtering in Gmail is more dynamic because it's able to learn more quickly and in a more personalized way.

Following your transition to Google Apps, you can manage undesirable bulk mail in the following ways:

- Gmail users and users with non-Gmail mailboxes can click the unsubscribe link at the bottom of the email message.
- Admins can [turn on aggressive spam filtering](#) to enforce more stringent filtering of bulk mail.
- Admins can add the sender to a [Blocked sender](#) list.
- Admins can block the messages using the [Content compliance setting](#).



- Gmail users can enable the Smart Labels lab (not available for non-Gmail mailboxes).
- Gmail users can click the Report spam button (not available for non-Gmail mailboxes).

How can you file a Support case for systemic spam issues?

If you experience spam issues that are affecting your organization systemically, please submit a support case. See the [Transition Support](#) page for details.

How can an administrator prevent users from viewing spam?

There is currently no option to prevent users from viewing spam. The upcoming Admin Quarantine feature will enable administrators to capture a message prior to delivery and place it into a queue/quarantine that is accessible only to administrators or to another appropriate designee. The admin can then release the message for onward delivery or choose to not do so. (See the [Feature roadmap](#) in the Postini Transition Resource Center for more details.)

How your non-Gmail users manage spam with Message Center

Non-Gmail users are unable to train the Gmail system by clicking the **Report spam** and **Not spam** buttons. However, Message Center and Quarantine Summary enable this functionality.

Message Center is a web-based console that enables non-Gmail users to manage their spam messages. Message Center is available for organizations that use a non-Gmail mail service such as Microsoft Exchange (or other non-Google SMTP service). In Message Center, users can identify a message as not spam and deliver it to their non-Gmail inbox.

Message Center enables users to add approved senders at a user level. Message Center doesn't include an editable per-user blacklist, but when users mark messages as spam with Message Center, this is equivalent to adding the sender to a blacklist.

One of the advantages of Message Center is that it enables non-Gmail users to find and report “false negative” emails—emails that are falsely categorized as spam and not delivered to the user. For more information about Message Center, see [Set options for non-Gmail mailbox users](#).

NOTE: To help your users prepare for the transition, we recommend that you distribute the following help article: [Manage messages in Message Center](#).

How your non-Gmail users manage spam with Quarantine Summary

Non-Gmail users are unable to train the Gmail system by clicking the **Report spam** and **Not spam** buttons. However, Message Center and Quarantine Summary enable this functionality.

If your organization uses a non-Gmail email service such as Microsoft Exchange, you can use the Non-Gmail mailbox setting in the Google Admin console to reroute messages to your users' non-Gmail mailboxes, and to set up a quarantine summary for your non-Gmail users.

The quarantine summary is comparable to what users experience with Postini. It's a digest that lists all messages that were marked as spam. It's delivered to users in their inbox and enables them to identify a



message as not spam and deliver it to their on-premise inbox. (Non-Gmail users who transition to Google Apps can't do this without the quarantine summary.)


During your service migration, your Postini quarantine summary settings are moved to the Non-Gmail mailbox setting. For more information about quarantine summary reports, see [Set options for non-Gmail mailbox users](#).

NOTE: To help your users prepare for the transition, we recommend that you distribute the following help article: [Quarantine summary report](#).

How your Gmail users manage spam

If your users are using Gmail after your transition to Google Apps, they will notice a few differences in managing spam. For example, a user might initially notice a little more spam in their Inbox. However, Gmail users can “train the system” by clicking **Report spam** or **Not spam**. The more frequently a user reports spam (or indicates that a message is not spam), the more effective this filtering mechanism becomes.

See the table below for a summary of the differences between Postini and Gmail spam filtering. We recommend that you send this information to your Gmail users to help them prepare for the transition.

In Postini, you...	In Gmail, you...
Log in to Postini Message Center to view quarantined messages, or manage spam using the Quarantine Summary.	<p>Check your Spam label for quarantined messages.</p> <p>By default, Gmail hides the Spam label; check here first for any incoming message that could be quarantined.</p> <ol style="list-style-type: none">1. Show your Spam label.<ul style="list-style-type: none">• In Gmail, click the gear  in the top right and click Settings.• Click the Labels tab.• Under System Labels > Spam, click show.2. In your left side bar (under your Inbox), click Spam.
Approve senders so that their messages are not quarantined	<p>Add senders to your Contacts list.</p> <p>If you receive legitimate messages that often get quarantined as spam, add those senders as contacts:</p> <ol style="list-style-type: none">1. Find a message from the sender.2. Click the More drop-down list next to Reply.3. Select Add sender name to Contacts list.

Virus filtering differences between Postini and Gmail

Gmail has comprehensive virus protection that includes the following benefits:

- **Rejection of messages with executables**—Gmail automatically rejects messages that have executable file attachments, even if those files are compressed into another file, such as a zip or rar file. We do this for many types of executable files (see [Some file types are blocked](#)). Gmail also automatically rejects messages that contain a password protected zip file within another zip file.
- **Automatic scanning of attachments**—Gmail automatically scans every attachment when it's received, and automatically rejects messages that contain viruses.
- **Increased protection against phishing**—Gmail provides increased protection against phishing-based attacks and messages containing URLs that point to malicious sites.

Message processing in Google Apps

Both Google Apps and Postini have sets of rules and functions that determine what happens to a message—whether it gets delivered to the intended recipient, quarantined as spam, bounced back to the sender, and so on.

These rules and functions fall into two categories: processing order and inheritance. This article describes the processing order and inheritance features in Google Apps and compares them to Postini.

NOTE: Although many of your Postini settings are transitioned to Google Apps, the processing order and inheritance rules are independent of the transition. Google Apps always implements the message processing features described in this article, regardless of the way in which Postini processed messages.

Processing order

Postini has a set order of filters and checks for incoming messages. At any point, a given policy check can decide to reject, quarantine, or perform another action on a message, even if another setting approved the message—and vice versa. This makes for a complicated system in which one setting can override or negate another, depending on which action takes precedence.

Google Apps, by contrast, applies all relevant settings to an incoming message. If any setting indicates to reject the message (bounce back to sender), that setting always takes precedence. Otherwise, Google Apps applies all settings, with a few simple rules for [resolving settings that result in a conflict](#). By not allowing any one setting to negate another, Google Apps is based on more straightforward, easier-to-understand logic.

Learn more about the [Google Apps mail flow](#) and the [guidelines for predicting the behavior of Gmail settings](#).



Inheritance

In Google Apps, when you create, modify, or delete a setting at an organization level, that change automatically propagates to all sub-organizations and users within that organization. At the same time, settings at a lower level take precedence over those at a higher level—so if a setting configuration for an individual user or sub-organization conflicts with that same setting’s configuration at a higher organization level, the lower-level configuration applies for that user or sub-organization.

By contrast, Postini doesn’t use inheritance. If you create, change, or delete a setting at the organization level, the change applies at that level only. To apply a higher-level setting to lower levels, you must manually use the “copy downward” option for a given setting or group of settings. Google Apps make this process automatic and seamless.

Learn more about the [organizational structure in Google Apps](#).



Get started with advanced settings for Gmail

Once you receive confirmation that your orgs, users, and settings are transitioned, we recommend that you sign in to the Google Admin console to review your Postini settings and to familiarize yourself with how the transferred settings appear, and to make any adjustments if necessary.

For instructions on how to perform many common tasks in the Google Admin console that are comparable to Postini, and to learn how to modify specific Google Apps settings after your service transition, see the sections below.

NOTE: In most cases, the tasks you can perform in the Google Apps Admin console are similar to tasks in the Postini Admin console. Beyond providing similar functionality, Google Apps offers a number of feature enhancements and improvements compared to what's available in Postini. In a small number of cases, a feature that was available in Postini works differently, or is not supported, in Google Apps. For details, see [Improvements and changes in moving from Postini to Google Apps](#).

IMPORTANT: Google Apps for Business Terms of Service

The Google Apps for Business Terms of Service (ToS) will be presented to all administrators who log in to the Google Apps Admin console after orgs, users, and email settings transition from Postini, including administrators uninvolved with the transition.

Occasionally, the Vault-Hangout amendment about product compatibility will also be presented to the first super administrator who logs in to the Google Admin console. If your organization will be using Hangouts, that administrator can choose either Continue using Hangouts to enable Hangouts or Disable Hangouts to opt in later. See [Getting started with Google Hangouts](#) for more information.

After accepting the ToS and the Vault-Hangout amendment, if presented, administrators will have immediate access to the Admin console. The ToS and Vault-Hangout amendment will not be presented to users in your organization.

NOTE: To ensure that API operations continue to function, ensure that all service accounts used for Google APIs accept the ToS and acknowledge the Vault-Hangout amendment.

Postini Admin Console	Google Admin Console
Login page	Sign in and get started with the Google Admin console:



	<p>After your service transition from Postini to Google Apps, you can sign in to the Google Admin console to review your settings, and to perform other admin tasks. Sign in to the Google Admin console from the following page:</p> <p style="text-align: center;">admin.google.com</p> <p>For instructions, see Sign in to your Admin console. See also “Get started with the Google Admin console” below.</p>
Orgs and users tab	<p>Review your users.</p> <p>During your service transition, your Postini users are moved to Google Apps. Both primary addresses and aliases are copied over. To review your users:</p> <ol style="list-style-type: none"> 1. Sign in to the Google Admin console. 2. Click the Users icon to open the Users page. 3. To review your users within individual organizations -- or organizational units (OUs) -- click any of the organization links in the right column. 4. For instructions on adding users to an organization, or moving users from one organizational unit to another, see Options for adding users and Move a user to an organizational unit. For instructions and details about user aliases, see Add email aliases and Email aliases. <p>After your service transition, you will have read-only access to your Postini Administration Console, so you can sign in and keep the Postini Admin Console open in a separate browser window as you check your Google settings.</p>
Orgs and users tab	<p>Review your orgs and org structure.</p> <p>After your service transition is completed, you may want to review your orgs and org structure to make sure that your new setup is satisfactory to you. You may also want to review the various settings, such as Content compliance, Attachment compliance, and Receiving routing for each OU. (For instructions and details about the different settings within the Google Admin console, see the sections below.)</p> <p>If you want to modify or fine-tune your org structure in the Google Admin console, see Create an organizational structure, Add an organizational unit, and Modify the organizational structure.</p> <p>NOTE: If your Postini configuration includes just one account org, one email config, and one user org, you will see just one OU in the Google Admin console when you first log in. In Google Apps, the account org and email config org are not necessary, so the org structure will be simplified for you. If needed, you can add sub-organizations. See Create an organizational structure.</p>
Domains	<p>Review your domains.</p>

	<p>Each of your domain names is transferred to the Domain settings page in the Google Admin console. This might include just a single primary domain, or it may also include additional domains or domain aliases that were part of your Postini configuration.</p> <p>After your service transition is completed, we recommend that you confirm that domain aliases and non-primary domains are copied over. Note that domains are displayed differently in the Google Admin console. For example, in Google Apps there is only one primary domain.</p> <p>For instructions and details on your domain setup in Google, see Add domain or domain aliases, Managing multiple domains, and Limitations for multiple domains.</p>
Administrator privileges	<p>Set up administrator roles in Google Apps.</p> <p>The Google Admin console offers several pre-defined administrator roles that are not editable (see Pre-defined administrator roles). Using these pre-defined roles, you can grant administrator privileges appropriate to specific business roles. To create a custom administrator role with different privileges, see Create custom administrator roles.</p>
Postini email filters	<p>Review and manage your Google Apps email settings</p> <p>For general instructions on how to navigate to your Google Apps email settings, and for an overview of the email settings that are available in Google Apps, see Configure advanced settings for Gmail.</p> <p>Note that you'll need to click Gmail (rather than "Email") in the Google Admin console to access your email settings.</p> <p>See the sections below for details regarding specific settings, such as Content compliance or Attachment compliance.</p> <p>See also Guidelines for configuring advanced settings for Gmail.</p>
Content Manager	<p>Review and manage the <i>Content compliance</i> setting.</p> <p>Content Manager filters in Postini are moved to the Content compliance setting in Google Apps.</p> <p>With the Content compliance setting, you can specify what action to perform for messages based on predefined sets of words, phrases, text patterns, or numerical patterns. Using Content compliance, you can set up regular expressions to match text with patterns.</p> <p>For instructions on reviewing your Google Apps content settings after your transition, or to make any changes, see Content compliance setting. See also Objectionable content setting.</p>
Attachment Manager	<p>Review and manage the <i>Attachment compliance</i> setting.</p>

	<p>Attachment Manager filters in Postini are moved to the Attachment compliance setting in Google Apps.</p> <p>The Attachment compliance setting enables you to specify what action to perform for messages with attachments. With this setting, you can specify conditions based on file type, file name, and message size. Each setting can have its own actions -- or method of processing filtered messages.</p> <p>For instructions on reviewing your Google Apps attachment filters after your transition, or to make any changes, see Attachment compliance setting.</p>
Delivery Manager	<p>Mail routing and delivery settings</p> <p>During your Postini transition to Google Apps, your Delivery Manager settings are moved to multiple locations on the Gmail settings page -- including the Advanced Settings page, the Hosts tab, and the Default routing tab. (Note that the name Delivery Manager is not used in Google Apps email settings.)</p> <p>You can use your Google Apps routing and delivery options for split delivery, dual delivery, receiving routing, sending routing, content routing, attachment routing, and more. You can use the Default routing tab to set up default routing options for your domain.</p> <p>To review your mail routing and delivery settings after your transition, and for detailed instructions on several administrative tasks, see Mail routing and delivery: Guidelines and best practices and Google Apps routing settings.</p>
Spam and virus filtering	<p>Google spam filtering is integrated into Google Apps, and spam is purged on a rolling 30-day schedule. Spam filtering is simply "on" by default, but you can use the Spam setting to enforce more stringent filtering of bulk mail or to set up approved senders to bypass Google's spam filters. Your non-Gmail mailbox users can also manage spam with the Message Center and Quarantine Summary. For instructions on setting up the Message Center and Quarantine Summary for your users, see Set options for non-Gmail mailbox users.</p> <p>Google also has built-in virus checking. Most computer viruses are contained in executable files, so standard virus detectors scan messages for executable files that appear to be viruses. Google helps block viruses in the most direct possible way: by not allowing users to receive executable files (such as files ending in .exe) that could contain damaging executable code; even if they are sent in a compressed (.zip, .tar, .tgz, .taz, .z, .gz) format.</p> <p>For more details, see <i>How Gmail spam and virus filtering differs from Postini</i>.</p>
Message Center	<p>The Message Center is available for organizations that use a non-Gmail mail service such as Microsoft Exchange (or other non-Google SMTP</p>

	<p>service). Similar to the Postini Message Center, the Google Apps Message Center is a web-based console that, by default, lets users view and manage messages quarantined as spam.</p> <p>For detailed instructions on how to set up the Message Center, see Set options for non-Gmail mailbox users. For user instructions, see Manage messages in the Message Center.</p>
Quarantine Summary	<p>Non-Gmail mailbox routing</p> <p>During your service migration, your Quarantine Summary settings will be moved to the Non-Gmail mailbox setting, so you may want to navigate to this setting to review your Quarantine Summary configuration. For example, if you set up Postini Quarantine Summary reports for weekly delivery on Monday, you'll find the same configuration in the Non-Gmail mailbox setting after your service transition.</p> <p>For detailed instructions on how to set up Quarantine Summary reports, see Set options for non-Gmail mailbox users. For user instructions, see Quarantine Summary report.</p> <p>About the Non-Gmail mailbox setting</p> <p>If your organization uses a non-Gmail mail service such as Microsoft Exchange (or other non-Google SMTP service), you'll be able to use the Non-Gmail mailbox setting to reroute messages to your users' non-Gmail mailboxes. You'll also be able to use this setting to set up the Message Center and Quarantine Summary for your non-Gmail users.</p>
Compliance footers	<p>Append footer setting</p> <p>The <i>Append footer</i> setting in Google Apps is comparable to the Compliance Footer in Postini. Using this setting, you can configure outbound messages with footer text for legal compliance, or for informational and promotional requirements. The footer is added below the last existing text portion of a message. For instructions, see Append footer setting.</p>
Blocked senders	<p>Blocked senders setting</p> <p>The <i>Blocked senders</i> setting enables an administrator to block specific senders based on the email address or domain. For instructions, see Blocked senders setting.</p>
Approved senders	<p>Spam setting: Add approved senders to bypass the spam folder</p> <p>Incoming email messages are subjected to Google's spam filters, so messages detected as spam are automatically placed in a user's Gmail spam folder. However, the Spam setting enables you to create an approved sender list to bypass the spam folder. You can approve specific senders based on the email address or domain. For instructions, see Spam setting: Add approved senders to bypass the spam folder.</p>

	<p>Approved sender lists can also be reused across different settings. For example, you can specify the same approved sender list in both the Spam setting and the Secure Transport (TLS) compliance setting, and it would modify the behavior of both settings.</p> <p>Note: If a message from an approved sender contains a virus or is part of an email attack, Google's virus filters will still prevent it from reaching your users.</p>
Log Search	<p>Email log search</p> <p>As a super administrator, you can use the log search for your domain. For instructions, see Email log search and Finding messages with email log search.</p>

For a roadmap of Google Apps features, and for a comparison of Postini features to Google Apps, see [Feature comparison and roadmap](#) in the Postini Transition Resource Center. The roadmap also includes a list of new features, as well as features that we didn't transfer over from Postini.

Configure advanced settings for Gmail

The Gmail advanced settings page enables you to configure email settings for your Google Apps domains. You can also configure settings for specific organizational units (OUs), or groups of users.

This article provides an overview of the Gmail advanced settings page, the features that are available, and instructions for how to use the various controls on this page.

Before you begin:

- Before you can customize your email settings for specific organizational units, you first need to [add organizational units](#) and [create an organizational structure](#).
- After you configure an email setting, it may take up to one hour for that configuration to propagate to individual user accounts.
- In rare cases, some users may experience message delays if you configure a very large number of Gmail advanced settings. These delays would only affect messages with a very large number of recipients. The first recipient is always accepted no matter how many settings are configured.

To configure advanced settings for Gmail:

1. [Sign in to the Google Admin console](#).
2. From the dashboard, go to **Apps > Google Apps > Gmail > Advanced settings**.
3. In the Organizations section, highlight the top-level org or the organizational unit (sub-org) for which you want to configure settings.
4. Scroll down the page to the relevant sections to configure your settings. You can also use the Search settings text box to enter a search term to quickly find the Gmail setting that you need.
5. After you make changes to your settings, click Save Changes to finalize the new/updated configuration.

See the sections below for instructions related to specific settings.

Email setting descriptions

The Gmail advanced settings General Settings page is divided into the following sections: Setup, End user settings, End user access, Spam, Compliance, and Routing. The settings contained within these sections are listed here.

Setup

- Web address: (top-level org only) Change the URL for your users' Gmail login page.
- MX records: (top-level org only) View your MX records.
- User email uploads: (top-level org only) Allow users to upload mail using the Email Migration API.
- Uninstall service: (top-level org only) For guidelines, see [Disable your email service](#).



End user settings

- Themes: Specify whether users can choose their own themes.
- Email Read Receipts: Specify whether users can request or return read receipts (see [Enable read receipts](#)).
- Mail delegation: Let users delegate access to their mailbox to others in the domain.
- Emailing profiles: Specify whether users can send or receive emails via their Google+ profiles. Default is OFF.

NOTE: This setting only appears if you have Google+ enabled for the domain.

- Name format: Configure the name format for users, or allow your users to customize this setting.
- Apps search: Include relevant Drive documents and Sites in Mail search results. The app search results appear below the mail search results.

End user access

- POP and IMAP access: Disable POP and IMAP access for users (see [IMAP and POP access](#)).
- Outlook & BlackBerry Support: Enable Google Apps Sync and Google Apps Connector for users.
- Automatic forwarding: Specify whether users can automatically forward incoming email to another address (see [Disable automatic forwarding](#)).
- Offline Gmail: Enable offline Gmail for users.
- Allow per-user outbound gateways: Allow users to send mail through an external SMTP.
- Image URL proxy whitelist: (top-level org only) Create and maintain a whitelist of internal URLs that bypasses proxy protection (see [Image URL proxy whitelist setting](#)).

Spam

- Email whitelist: (top-level org only). Create an email whitelist—a list of IP addresses from which users expect to receive legitimate mail (see [Email whitelist](#)).
- Inbound gateway: (top-level org only) Enter inbound mail gateways if you have them (see [Inbound gateway](#)).
- Spam: Create an approved sender list to bypass the spam folder (see [Spam setting](#)).
- Blocked senders: Block specific senders based on the email address or domain (see [Blocked senders setting](#)).

Compliance

- Email retention: (top-level org only) Control the amount of mail that is stored for each user (see [Email retention](#)).
- Append footer: Configure outbound messages with footer text for legal compliance, or for informational and promotional requirements (see [Append footer setting](#)).
- Comprehensive mail storage: Ensure that a copy of all sent or received mail—including mail sent or received by non-Gmail mailboxes—is stored in the associated users' Gmail mailboxes (see [Comprehensive mail storage settings](#)).
- Restrict delivery: Restrict the email addresses users can exchange mail with (see [Restrict delivery](#)).
- Content compliance: Specify what action to perform for messages based on predefined sets of words, phrases, text patterns, or numerical patterns (see [Content compliance setting](#)).

- **Objectionable content:** Specify what action to perform for messages based on word lists that you create (see [Objectionable content setting](#)).
- **Attachment compliance:** Specify what action to perform for messages with attachments (see [Attachment compliance setting](#)).
- **Secure transport (TLS) compliance:** Require mail to be transmitted via a secure connection when users correspond with specific domains and email addresses (see [TLS setting](#)).

Routing

- **Email routing:** (top-level org only) A set of legacy routing controls for your domain. See [Managing mail routing and delivery](#) for guidelines and best practices before configuring your routing controls.
- **Outbound gateway:** (top-level org only) Set an outbound mail gateway—a server through which all mail sent from your domain passes (see [Outbound mail gateway](#)).
- **Recipient address map:** (top-level org only) Apply one-to-one mapping (aliases) to recipient addresses on messages received by your domain (see [Recipient address map](#)).
- **Receiving routing:** Set up inbound and internal-receiving delivery options, such as dual delivery and split delivery (see [Receiving routing setting](#)).
- **Sending routing:** Set up outbound and internal-sending delivery options (see [Sending routing settings](#)).
- **Vault settings for Exchange Journals:** (top-level org only) Specify an email address in your domain that receives your Exchange journal messages. See [Vault settings for Exchange journals](#).
- **Non-Gmail mailbox:** Reroute messages to users' non-Gmail mailboxes, if your organization uses a non-Gmail mail service such as Microsoft Exchange or other non-Google SMTP service. You can also use this setting to configure quarantine summary reports for your non-Gmail users (see [Non-Gmail mailbox routing and Quarantine Summary](#)).
- **SMTP relay service:** (top-level org only) Set options for routing outbound mail through Google (see [SMTP relay service setting](#)).
- **Alternate secure route:** (top-level org only) Set an alternate secure route when secure transport (TLS) is required (see [Alternate secure route](#)).

How to use the controls on the Gmail advanced settings page

The controls on the Gmail advanced settings page vary depending on the type of setting you need to configure:

- For the Setup, End User Settings, and End User Access sections, you can make changes directly within the Gmail advanced settings page using checkboxes, options, and text boxes.
- For many of the Spam, Compliance, and Routing settings, you must hover your mouse anywhere in the setting's area on the page to access the controls. These hover controls—which appear on the right—let you add, edit, disable, delete, and perform other actions on a setting's configuration.



Spam Locally applied	Spam setting 1 Bypass internal senders: Yes Bypass approved senders: Yes	Edit Disable Delete Add another Copy to organization
--------------------------------	--	--

The settings that use hover controls are as follows:

Spam

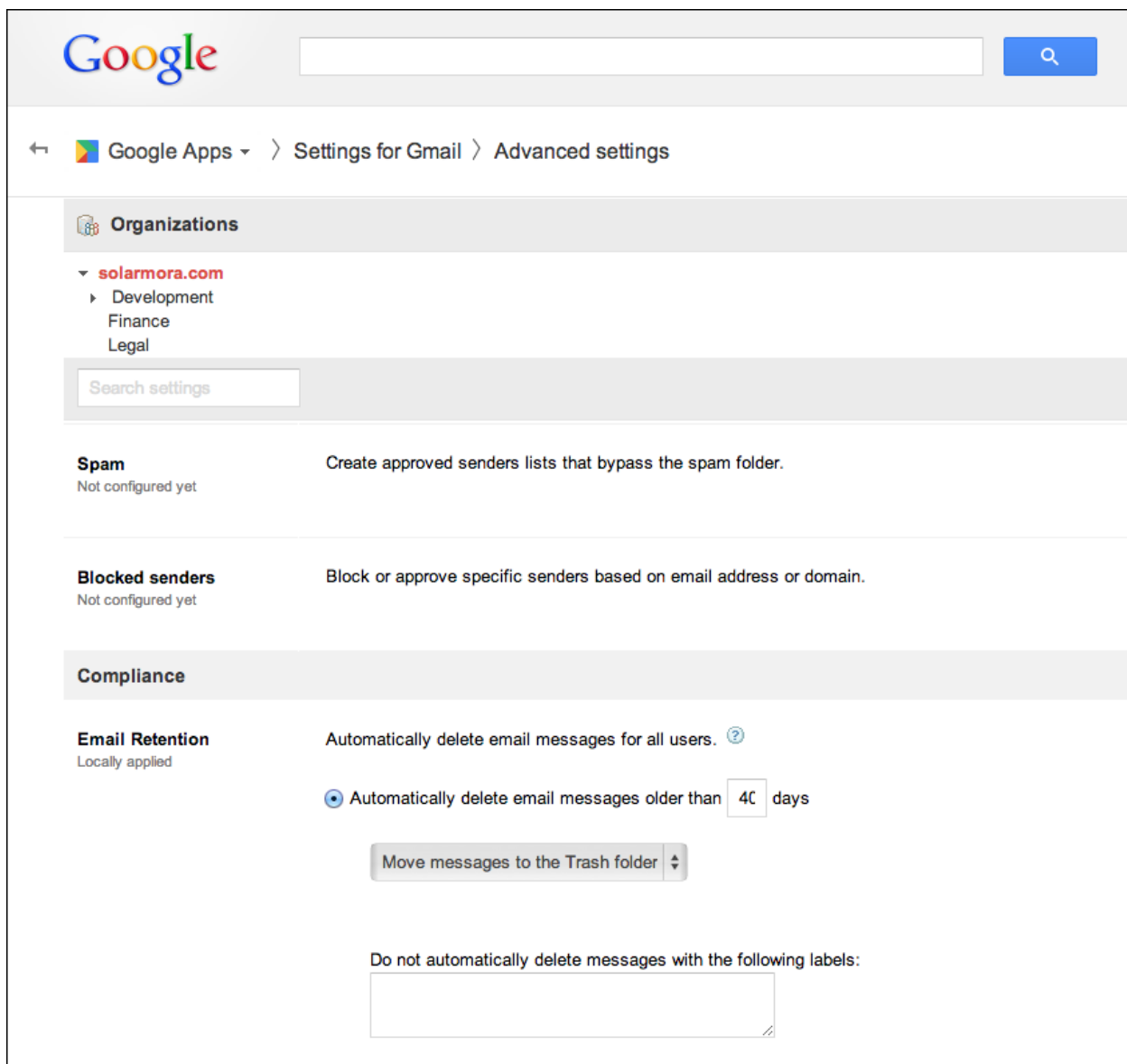
- Spam
- Blocked senders

Compliance

- Append footer
- Restrict delivery
- Content compliance
- Objectionable content
- Attachment compliance
- Secure transport (TLS) compliance

Routing

- Recipient address map
- Receiving routing
- Sending routing
- Vault Settings for Exchange Journals
- Non-Gmail mailbox
- SMTP relay service
- Alternate secure route



For settings in the Spam, Compliance, or Routing section that do not appear in this list, you configure the setting directly on the Gmail advanced settings page.

To configure settings directly on the Gmail advanced settings page (all settings in the Setup, End User, and End User Access sections, plus a few in the other sections):

1. In the Organizations section, highlight the top-level org (or the sub-org) for which you want to configure settings.
2. Scroll down the page to the relevant sections, or use the Search settings box to enter a search term or setting.
3. Adjust these settings directly within the Gmail advanced settings page.
4. Click **Save changes**.

TIP: When searching for a specific setting, you can type in a search term and then click a different

organizational unit. This enables you to review how a particular setting is configured across organizational units.

To configure settings using the hover controls (most settings in the Spam, Compliance, and Routing sections):

1. In the Organizations section, highlight the top-level org (or the sub-org) for which you want to configure settings.
2. Scroll down the page to the relevant sections, or use the Search settings box to enter a search term or setting.
3. Hover your mouse anywhere in the setting's area on the page to access the controls.
4. Click the appropriate control:
 - When you click **Configure**, **View**, **Edit**, or **Add another**, a dialog box displays with the options for that setting.
 - When you click **Copy to organization**, a dialog box displaying, enabling you to select the target organization.
 - When you click **Disable**, **Enable**, or **Delete**, no dialog box displays.
5. Click **Save changes**.

Tip: When searching for a specific setting, you can type in a search term and then click a different organizational unit. This enables you to review how a particular setting is configured across organizational units.

Hover controls

The following sections describe the various hover controls on the Gmail advanced settings page, and the situations in which you might use them:

Configure

This control displays only if you have not configured the setting yet. Click **Configure** to set options for the setting, and then click **Add Setting**.

For example, if you want to set up a new Content compliance setting, click **Configure** to set the options for this setting.

View

This control is available for inherited settings only. Use this control when you want to check the configuration of an inherited setting.

Click **View** to see the options selected for that setting. (You can't make any changes to the options.) If you need to change an inherited setting's configuration, use the **Add another** control, described below, to create a new configuration. Click **Close** when you are done.

Edit

This control is available for locally applied settings only. For a setting you configured, click **Edit** to make changes to the setting's configuration. Click **Save** when you're done. For example, if your company name or web address changes, you may need to edit the Add footer setting to update the information in your



email footer.

Disable/Enable

Disabling a setting does not impact the options you chose for the setting; it merely turns the setting off. To turn the setting back on, click **Enable**. These controls are available for both inherited and locally applied settings.

For example, if a setting's configuration is not giving you the expected results, you can disable the setting temporarily to make adjustments, and then re-enable it later.

You can also make a copy of a setting, disable it, make adjustments, and then toggle the enabled states of the original and new settings for comparison.

Delete

This control is available for locally applied settings only. For a setting you configured, click Delete to both disable the setting and delete that setting's configuration. To confirm the deletion, click Save Changes. To enable this setting again, you must click Configure and select new options for the setting.

For example, at a certain point you might want to clear your blocked senders list. Use this control to delete this setting's configuration. You can then create a new configuration.

Add another

Use this control to replace an existing setting's configuration with a new one add a new configuration for a given setting. Click Add setting when you're done. This control is available for both inherited and locally applied settings.

For example, your inherited Objectionable content setting might contain a list of objectionable words for your entire organization. For a specific organizational unit, you might want to include some additional words that apply to that unit only. You would use the Add another control to create that list of words for that organizational unit.

Copy to organization

Use this control to quickly copy a configured setting to a different organization. After you select the target organization, check the box to enable the setting for that organization. Click Apply when you're done.

For example, your domain might include 10 organizations, but a given Content compliance setting configuration might apply to only five of them. Configuring the setting in one organization and then copying it to the other four provides a fast way to configure the setting in multiple locations.

Inherited versus locally applied Gmail settings

On the Gmail advanced settings page, the controls available for a given setting might change depending on whether the setting is *Inherited* or *Locally applied*. A setting is labeled as Inherited if it was inherited from a higher-level organizational unit, or from a domain-level setting. A setting is labeled as Locally applied if it was configured at the same level from which you're viewing it. Settings that are not yet locally applied or inherited are labeled as Not configured yet.

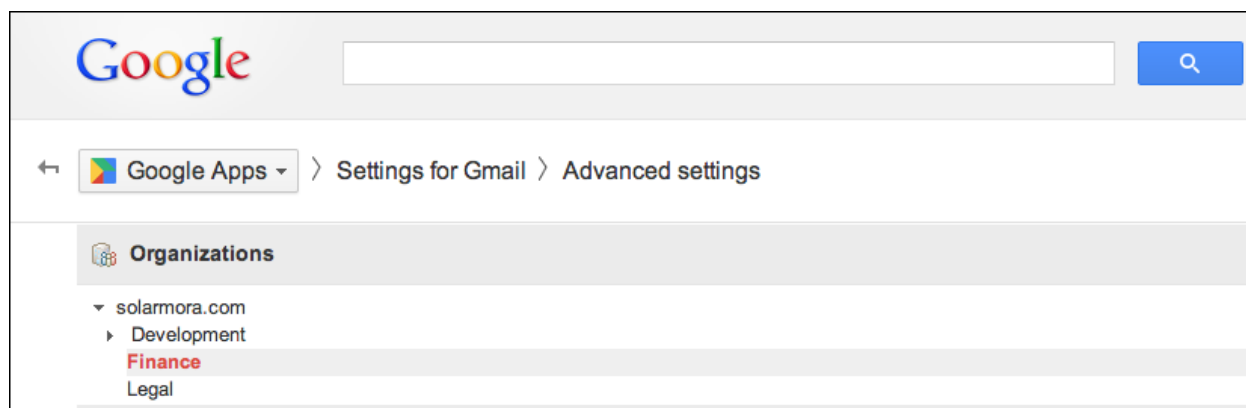
See [How to use the controls on the Gmail advanced settings page](#) for more details about how inheritance works.



Settings that are only configurable at the top level

Some settings on the Gmail advanced settings page are only configurable at the top-level organizational unit, and not at the sub-org level. (See *Email setting descriptions* above for a list of settings that are only configurable at the top level.)

Note: If you configure a setting at the sub-org level, that setting applies to that OU and any sub-organizations only. If you configure a setting at the top level, the setting applies to all OUs.



Hosts tab

The Hosts tab enables you to set up multiple routes for your Google Apps domains, and you can later use these routes for dual delivery or split delivery when you configure your settings on the Gmail advanced settings page. You can then specify different routes for different organizational units.

Click **Google Apps > Gmail > Advanced settings** to access the Hosts tab. For instructions, see [Add mail routes with the Hosts tab](#).

Default routing tab

The Default routing setting enables you to set up a routing policy for all of your Google Apps domains that includes one or more settings. The settings apply only to inbound messages.

To access the Default routing setting, click **Google Apps > Gmail > Advanced settings**, and then click the **Default routing** tab.

An important use for Default routing is for setting up split delivery to route unregistered Google Apps users to your on-premise mail server. This is useful when transitioning users from your legacy mail server to Google Apps. You can also use Default routing to designate an existing user account as a catch-all address to receive messages that are addressed to non-existent users in your Google Apps domains.

For instructions, see [Default routing setting](#).

Guidelines for configuring advanced settings for Gmail

Google Apps administrators have the flexibility to configure multiple email settings for their domains and for different groups of users, or organizational units. This chapter describes how the various email settings work and interact, and how they affect mail messages and mail flow in a predictable way.

For an overview of the Gmail advanced settings page, the available features, and instructions for how to use the various controls on the page, see *Configuring advanced settings for Gmail*.

The email security settings for your domain are located in the Google Admin Console (**Google Apps > Settings for Gmail > Advanced settings**).

Before you begin:

- Before you can customize your email settings for specific organizational units, you first need to [add organizational units](#) and [create an organizational structure](#).
- After you configure an email setting, it may take up to one hour for that configuration to propagate to individual user accounts.
- In rare cases, some users may experience message delays if you configure a very large number of Gmail advanced settings. These delays would only affect messages with a very large number of recipients. The first recipient is always accepted no matter how many settings are configured.

For an overview and details about the advanced settings, see *Configuring advanced settings for Gmail*.

Organizational units, settings, conditions, and actions

Organizational unit

An organizational unit (also known as org unit or OU) is a container for a specific subset of users within your company, and enables you to customize settings for specific groups of users within your domain.

Email setting

An email setting enables you to specify what action to perform on a message (for example, to reject it, or change its route) depending on whether or not that message matches the conditions you specify in the setting. For example, you can configure an Attachment compliance setting to reject messages with attachments that exceed 20 MB, or you can configure a Content compliance setting to reject messages that contain certain words. You can configure multiple email settings for a given OU.

Conditions and actions

If a message matches the conditions that you specify in an email setting, an action is performed on that message. If the conditions do not match, the action is not applied.

An email setting can have one or more conditions. The following are examples of conditions:

- The message body contains the word confidential.
- The envelope “from” address matches sender@example.com.



- The message contains a compressed file attachment.

The following are examples of actions:

- **Reject message**—The message is not delivered.
- **Add X-Gm-Original-To header, Add X-Gm-Spam header and X-Gm-Phishy header, and Add custom headers**—Add an additional X-header to the message headers.
- **Prepend custom subject**—Alter the subject header to include prefix text.
- **Change route**—Change where the message is routed. For example, users with non-Gmail inboxes may have their mail routed to an on-premise Exchange server.
- **Change envelope recipient**—This may alter where the message is delivered. When used in conjunction with Add more recipients, this implements the 'bcc' feature. If not, it is effectively a 'forward'.
- **Bypass spam filter for this message**—Messages that match the conditions of the setting and are identified as spam will be delivered to the intended recipient.
- **Remove attachments from message**—Attachments are removed before delivery to the intended recipient.
- **Add more recipients**—The message is also delivered to these recipients.
- **Require secure transport for onward delivery**—Outbound messages require secure delivery.

General guidelines for predicting the behavior of settings

Your Google Apps email settings are stored in a hierarchical tree of organizational units (for more details, see [Create an organizational structure](#)). Settings in child organizational units are inherited from parent organizational units, and a single user may have several associated settings. The actions of these settings can sometimes conflict when determining what should be done with a message; for example, should the message be rejected, or should it be dual delivered?

Use the following guidelines to help you predict how Google Apps email settings will behave:

- **Settings**—With a few exceptions, the ordering of the setting is not important, and is determined by the action taken when a condition matches. For example, the Append footer setting does not take precedence over any other settings, such as Content compliance or Attachment compliance.
- **The Reject message action takes precedence**—If any setting causes a rejection when the conditions match, then the message is rejected. For example, if there are two settings—one that may reject the message, and another that may add more recipients—then the Add more recipients action does not occur.

Note: If more than one setting results in a reject, and if different custom reject response messages are specified in each setting, then only one response is used.

- **Multiple re-routes/change recipient**—If two different settings cause Change route or Change envelope recipient actions, the Change route or Change envelope recipient actions are in conflict. In this case, the ordering of the setting determines which re-route or recipient change is applied to the message. The actions in a child organizational unit take precedence (or come “first”), while actions in a parent organizational unit are lower precedence.

- **Add more recipients**—If two settings specify additional recipients, then all recipients are added; there is no possibility for conflict.
- **Sender whitelists**—Any setting can specify a sender whitelist (approved senders) to bypass the actions if there's a match. Sender whitelists can be shared between settings; for example, the Spam setting enables you to create an approved sender list to bypass the spam folder. This same approved sender list could be used to bypass a Content compliance setting.
- **Prepend subject**—If two settings result in different prepend subject actions, both prefixes are prepended. The ordering of the prepended subjects depends on the location of the setting within the organizational unit structure. The actions in a child organizational unit take precedence (or come “first”), while actions in a parent organizational unit are lower precedence.
- **Add footer**—If two settings result in different add footer actions, both footers are appended. The ordering of the footers depends on the location of the setting within the organizational unit structure. The actions in a child organizational unit take precedence (or come “first”), while actions in a parent organizational unit are lower precedence.

Content compliance setting

The Google Apps Admin console offers the [Content compliance setting](#) as one of the advanced settings for Gmail. The Content compliance setting includes and improves upon many of the features available in the Postini Content Manager. Similar to Content Manager, the Content compliance setting lets you specify what action to perform for messages based on predefined sets of words, phrases, text patterns, or numerical patterns. You can also set up regular expressions to match text with patterns.

Note: Google Apps also includes an [Objectionable content setting](#), which lets you filter messages based on word lists only.

How the transition works for Content Manager and Content compliance

During transition, your Postini Content Manager settings are moved to the Content compliance setting in Google Apps.

Note the following:

- The blackhole disposition is unnecessary, often harmful, and a violation of the Simple Mail Transfer Protocol (SMTP) specification. With poorly written filters that generate false positives, blackholed mail provides no recourse to the sender; there's little evidence to suggest spammers gather any intelligence from seeing rejections. Thus, Google Apps doesn't support the delete (blackhole) disposition. If you have a blackhole disposition set in Postini, the transition tool changes this to a Reject disposition.
- Because the Postini Content Manager activity log is limited to 5,000 entries, it provides minimal visibility into corporate compliance with content policies. Therefore, Google Apps doesn't offer a content compliance activity log.
- Although IP Lock in Postini is not a component of Content Manager, if you have IP Lock settings, the transition tool copies these to equivalent Content compliance settings. After transition, you can also use Content compliance to [configure "IP lock" in Google Apps](#).

Using and configuring Content compliance setting options

To access the Google Apps Content compliance setting:

1. [Sign in to the Google Admin console](#).
2. From Home, go to Apps > Google Apps > Gmail > Advanced settings.
3. In the Organizations section, highlight your domain or the organizational unit for which you want to configure settings (see [Configure advanced settings for Gmail](#) for more details).
4. Scroll down to the Content compliance section.
5. Within the Content compliance setting, you set [configuration options](#) in the following categories:



- Email messages to affect—Select whether this configuration applies to inbound, outbound, or internal (sending or receiving) messages.
- Content to search for—Specify whether to act on messages containing all or any of the expressions you create; whether the search term consists of a simple text expression, an advanced text expression, or metadata; and, for advanced content and metadata, the parameters of the expression.
- Action to perform—Select whether to reject or modify—for example, add a header, change the delivery route, or change the envelope recipient—messages that meet the expression criteria.

[Learn more about the Content compliance setting.](#)

Feature differences and improvements

The following Google Apps Content compliance features work differently from their equivalents in Postini Content Manager:

- **Regular expressions**—Full regular expression syntax—not just a subset—is available in the Content compliance settings. Set routing options based on content type—You can choose how to route message delivery based on the message content. Content Manager doesn't offer this option.
- **Deliver a specified type of content**—Google Apps always recognizes any combination of settings—such as reject or reroute—that you set for a given content or attachment type. The Deliver disposition offered in Postini acts to bypass or override some other settings in a complex fashion, depending on which setting overrides which. By not allowing any one setting to negate another, Google Apps is based on more straightforward, easier-to-understand logic.
- **Use SSN or credit card numbers as content spam filters**—Postini includes the option to specify credit card or Social Security number filters. Google Apps doesn't have an explicit CC/SSN filter. The transition tool creates a setting that uses a regular expression to detect these patterns. Users can create additional regex filters as needed.
- **Registration required for outbound content compliance**—Postini allowed Content Manager settings for outbound messages to apply to unregistered users. In Google Apps, Content compliance settings for outbound mail apply to registered users only.

[Learn more](#) about the feature differences and improvements between Google Apps and Postini.



Attachment compliance

Similar to the Postini Attachment Manager, the Google Apps Attachment compliance setting lets you specify what action to perform for messages with attachments. With this setting, you can specify conditions based on file type, file name, and message size. Each setting can have its own actions, or method of processing filtered messages. For example, you can reject messages whose attachments cause them to exceed 20 MB, or you can detect particular attachment types or names and reroute the message, add a header, or prepend a string to the subject. You can also modify a message by stripping its attachments and adding an advisory notice to the message.

Note: Google Apps also includes a [Content compliance](#) setting and an [Objectionable content](#) setting. Both offer different ways of filtering message content.

How the transition works for Attachment compliance

During transition, most of your Postini Attachment Manager settings are moved to the Attachment compliance setting in Google Apps.

The transition tool doesn't copy the following Attachment Manager settings to the Attachment compliance setting:

- Google Apps doesn't yet include the Postini Attachment Manager "scan inside binaries" feature. From a security perspective, this feature is not needed, because Google Apps doesn't allow you to send or receive executable files (such as files ending in .exe), which can contain harmful code that might cause malicious software to download to your computer. If you have set Postini to scan inside binaries, the transition tool doesn't copy this setting to the Google Apps Attachment compliance setting.

Note: The upcoming "scan inside binaries" feature will improve the existing Attachment compliance setting to leverage binary file type information. When this feature is implemented in Google Apps, it will always scan all binary file attachments. Because there is no option to turn the feature on or off, the transition tool won't copy existing Postini "scan inside binary" settings to the new Google Apps setting.

- As mentioned above, Google Apps doesn't allow you to send or receive executable files. In addition, Google Apps scans binary files for executable and virus detection, rather than relying on the file name only. If you've set Postini to approve or ignore executable files, the transition tool doesn't copy this setting to Google Apps.
- Google Apps automatically scans every attachment, including compressed files, for viruses when an attachment is delivered to you. In addition, Google Apps scans all files (within a compressed file) that match your Attachment compliance criteria. If you've set Postini to approve or ignore compressed files, the transition tool doesn't copy this setting to Google Apps.
- Although Postini included the option to detect multiple attachment file extensions, customers didn't widely use this feature. If you have Postini set to detect multiple attachment file extensions, the transition tool doesn't copy this setting to Google Apps.

Using the Attachment compliance setting

To access the Google Apps Attachment compliance setting:

1. [Sign in to the Google Admin console](#).
2. From Home, go to **Apps > Google Apps > Gmail > Advanced settings**.
3. In the **Organizations** section, highlight your domain or the organizational unit for which you want to configure settings (see [Configure advanced settings for Gmail](#) for more details).
4. Scroll down to the Attachment compliance section.

Within this setting, you [set configuration options](#) in the following categories:

- **Email messages to affect**—Select whether this configuration applies to inbound, outbound, and/or internal (sending or receiving) messages.
- **Attachments to search for**—Specify whether to act on attachments containing all or any of the expressions you create, and then create an expression based on file type, file name, or message size.
- **Action to perform**—Select whether to reject or modify—for example, add a header, change the delivery route, or change the envelope recipient—messages containing attachments that meet the expression criteria.
- **Domains or addresses to exclude from filter**—Select whether to exclude messages sent to or from certain domains or addresses from this attachment filter.

Feature differences and improvements

The following Google Apps Attachment compliance features work differently from their equivalents in Postini Attachment Manager:

- **Attachment filtering**—In Google Apps, you can remove attachments that violate policies but allow delivery of the message text.
- **Quarantine spam messages/attachments by user**—Google Apps offers a single Spam folder, as opposed to the multiple quarantine folders (Junk, Virus, and so on) available in Postini. Postini let administrators further manually configure spam rules by sending messages to a quarantine folder based on attachments. This typically occurred to block the attachment and reduce the load on the receiving server. Google Apps always scans all attachments and blocks any with a virus. Additionally, when a Gmail user downloads an attachment, the attachment is again virus-scanned.
- **Set routing options based on attachment type**—In the Attachment compliance setting, you can choose how to route message delivery based on the message content. Attachment Manager doesn't offer this option.
- **Approve a specified type of attachment**—Google Apps always recognizes any combination of settings—such as reject or reroute—that you set for a given content or attachment type ([Learn more](#)). The Approve disposition offered in Postini acts to bypass or override some other settings in a complex fashion, depending on which setting overrides which. By not allowing any one setting to negate another, Google Apps is based on more straightforward, easier-to-understand

logic.

- **Send attachments up to 300 MB**—Unlike Postini's limit of 300 MB, Google Apps Gmail imposes a limit of 25 MB on any sent or received attachments. Because almost all attachments are smaller than this size, this limit has almost no impact on sending and receiving files. On the other hand, imposing this limit does prevent attempts at transmitting enormous files that could impact network speed and bandwidth.

[Learn more](#) about the feature differences and improvements between Google Apps and Postini.



Google Apps routing settings

The advanced Gmail settings page in the Google Admin console includes numerous routing settings that enable you to configure dual delivery, split delivery, catch-all addresses, outbound gateways, content routing, attachment routing, non-Gmail mailbox routing, and more.

We recommend that you read this section to become familiar with Google Apps mail routing settings. After your transition, [sign in to the Google Admin console](#) to review your settings. For additional detailed instructions on Google Apps mail routing, see [Mail routing and delivery: Guidelines and best practices](#).

How the transition works for routing settings

Your Postini routing settings are transferred to the Google Admin console under **Google Apps > Gmail > Advanced settings**.

In the Postini Administration Console, mail routing settings are managed from the Delivery Manager tab, but the name *Delivery Manager* is no longer used in Google Apps. Instead, Google Apps routing settings are located in multiple locations on the Gmail settings page -- including the Advanced Settings page, the Hosts tab, and the Default routing tab.

Descriptions of the Google Apps routing settings

For detailed instructions on Google Apps mail routing, see [Mail routing and delivery: Guidelines and best practices](#) and [Google Apps routing settings](#). For a list of related articles, see [Routing](#).

Hosts tab

When you follow the [basic setup instructions](#) for your domain in Google Apps, email for recipients in your domain is delivered to their Gmail inboxes. This configuration is referred to as direct delivery. However, your situation might call for a more advanced delivery option. For example, if some of your users have legacy mail accounts on Microsoft Exchange, you can have their mail delivered to their Gmail account, their legacy account, or both accounts.

To set up your email settings with such a configuration, you first need to add mail routes from the Hosts tab on the email settings page. The Hosts tab enables you to set up multiple routes that you can later use for dual delivery or split delivery when you configure your email settings. You can then specify different routes for different organizational units when configuring your domain's email settings.

For instructions, see [Add mail routes with the Hosts tab](#).

Default routing

This setting enables you to set up a domain-wide routing policy for inbound messages. Default routing is useful for setting up a split delivery configuration, for specifying a catch-all address, removing



attachments from messages, and more. For instructions, see [Default routing setting](#).

Receiving routing

The Receiving routing setting enables you to set up inbound and internal-receiving delivery options, such as dual delivery and split delivery.

Similar to other Google Apps advanced email settings, the Receiving routing setting enables you set up policies that vary by organizational unit. Users within child organizational units inherit the settings you create for the parent organization. You can add multiple Receiving routing settings to each organizational unit.

For instructions, see [Receiving routing setting](#).

Sending routing

The Sending routing setting enables you to set up outbound and internal-sending delivery options. For example, you can use the Sending routing setting to set up a smarthost (outbound mail gateway), or to route outbound mail for an organizational unit both to the intended recipients and to an external archiving server (dual delivery).

For instructions, see [Sending routing setting](#).

Routing based on message content, attachment, or TLS controls

In addition to the Receiving routing and Sending routing settings, mail routing and delivery controls are built into other email settings, such as Content compliance, Objectionable content, and Attachment compliance -- allowing more than one way to configure routing options to achieve the same results.

However, we recommend that you use these settings for the specific use cases they are intended to support. For example, you can set up the same routing options by using a Content compliance setting or a Receiving routing setting; but use a Content compliance setting for content-related use cases, and use a Receiving routing setting for general routing-related use cases, such as dual delivery.

For instructions, see [Content compliance setting](#), [Objectionable content setting](#), [Attachment compliance setting](#), and [Secure transport \(TLS\) compliance setting](#).

Non-Gmail mailbox routing

If your organization uses a non-Gmail mail server, such as Microsoft Exchange or other non-Google Simple Mail Transfer Protocol (SMTP) service, you can use the Non-Gmail mailbox setting to reroute messages to your users' non-Gmail mailboxes.

You can also use the Non-Gmail mailbox setting to allow non-Gmail users to sign in to Google Apps Message Center, and to configure Quarantine Summary reports for your non-Gmail users. Both Message Center and Quarantine Summary are only for non-Gmail users, and these features allow your non-Gmail users to manage spam.



For instructions, see [Set options for non-Gmail mailbox users](#).

SMTP relay service

If your organization uses a non-Gmail email service, such as Microsoft Exchange (or other non-Google SMTP service), you can use the SMTP relay service setting to route outgoing mail through Google. This setting enables you to filter messages for spam and viruses before they reach external contacts, and to apply Google Apps email security settings to outgoing messages. For instructions, see [SMTP relay service](#).

Vault settings for Exchange journals

If your organization uses Microsoft Exchange Server, and if you plan to use Google Apps Vault for archiving and eDiscovery, you'll need to do the following to ensure your Exchange messages are archived in Vault:

- **Configure the Vault Settings for Exchange Journals feature**—Enables you to specify an email address in your domain that will receive your Exchange journal messages.
- **Configure your Exchange server to forward journal messages to Vault**—Sets up journaling on your Exchange server, and enters the same address that you specified in the Vault Settings for Exchange Journals feature in the above step.

For instructions, see [Vault settings for Exchange Journals](#).

Recipient address map

This setting enables you to apply mappings (aliases) to recipient addresses on messages received by your domain. You can map multiple individual recipient addresses (a maximum of 2,000 entries) to other addresses. Each individual address maps to exactly one other address, and multiple addresses can map to the same other address.

This is a basic routing concept—sometimes called a *virtual user table*—that's frequently used in mail routing situations to redirect mail from one address to another. By using this setting, you don't need to create individual Default routing settings for each address mapping.

For instructions, see [Recipient address map](#).

Alternate secure route

This setting modifies routing behavior as configured in the [Secure transport \(TLS\) compliance setting](#) for messages that require secure transport—by creating a potential fallback secure route. Domains not listed in TLS rules can be rerouted to this alternate route.

You'll want an alternate route if you have a third-party encryption service. You can then use the Alternate secure route setting to route otherwise insecure traffic to it. For instructions, see [Alternate secure route](#).

For an overview of the Google Apps routing settings, and for instructions to help you get started, see [Mail](#)



[routing and delivery: Guidelines and best practices.](#)

Legacy routing settings

Following your Postini Transition to Google Apps, the routing configuration for your domain can be accessed via the routing settings described in the above section. However, a few legacy settings continue to be available on the Gmail advanced settings page. These settings include:

- [Email routing](#)
- [Inbound mail gateway](#)
- [Email whitelist](#)
- [Outbound mail gateway](#)

For more details, see also the [Legacy controls](#) topic in the help center.

In a future release, these legacy settings will be migrated to the Google Apps routing settings described above. During a transition period, both sets of controls will function simultaneously. If any conflict exists between the controls—for example, if you configure two different outbound gateways—the “non-legacy” settings described in the section above will override these legacy settings.

Users of legacy routing controls for outbound gateways and outbound BCCs should avoid any similar legacy settings (for example, [Outbound mail gateway](#)) to avoid conflicting and unpredictable behavior. These conflicts are currently being addressed.

While it's sometimes possible to use both sets of routing controls, we encourage you to use only the new and improved routing settings that are described in the section above, *Descriptions of the Google Apps routing settings*.



Append footer setting

Similar to the Postini compliance footer setting, the Google Apps **Append footer** setting lets you configure outbound messages with footer text for legal compliance, or for informational and promotional requirements. The footer is added below the last existing text portion of a message.

How the transition works for the Append footer setting

If you create a compliance footer for outbound messages in Postini, this setting transitions to the Append footer setting in Google Apps.

NOTE: Google Apps applies the footer to all outbound mail, including Domain Keys Identified Mail (DKIM)-signed outgoing mail (if you have DKIM signatures enabled), even if you didn't select this option in Postini. Because Google Apps applies the footer prior to adding the DKIM signature, the footer doesn't break the signature as it would in Postini.

Using and configuring the Append footer setting

To access the Google Apps Append footer setting:

1. [Sign in to the Google Admin console](#).
2. From Home, go to **Apps > Google Apps > Gmail > Advanced settings**.
3. In the **Organizations** section, highlight your domain or the organizational unit for which you want to configure settings (see [Configure advanced settings for Gmail](#) for more details).
4. Scroll down to the **Append footer** section, or enter **Append footer** in the search field.

Learn more about [entering and formatting your footer](#).

Feature differences and improvements

For some message types, footer functionality in Google Apps works the same as in Postini. For example, neither Google Apps nor Postini appends a footer to bounced messages. For forwarded messages, both Google Apps and Postini append a footer if the forwarded message contains a text part, but don't append a footer if the message is forwarded as an attachment—although, if the “cover” message for the forwarded attachment contains a text part, both Google Apps and Postini append a footer to that “cover” message.

The following Google Apps Append footer features work differently from their equivalents in Postini:

- **DKIM-signed outgoing mail**—In Postini, you must select an option if you want to add a compliance footer to DKIM-signed outgoing mail. In Google Apps, if you [enable DKIM signatures](#), Google Apps always applies the footer to DKIM-signed outgoing mail.
- **HTML formatting**—Compliance footers in Postini are text-only by default, with some limited options for HTML formatting using tags. The Google Apps Append footer setting includes a WYSIWYG HTML editor with a full array of formatting options, including ability to insert an image.

NOTE: Similar to Postini, if an outgoing message is plain text, Google Apps appends the footer as plain text.

- **Multipart messages**—If a message is multipart/alternative, Google Apps appends the footer to each text part. Postini appends the footer to the last text part only. For other types of multipart messages, if the message contains no text part, Google Apps adds a text part and appends the footer. Postini doesn't add a footer if a message has no text parts.
- **Quarantined messages**—Messages released from quarantine in Postini don't include a footer. In Google Apps, if the message includes a footer before it is quarantined, the message keeps the footer after being released from quarantine.
- **Character limit**—Postini sets a 4,000-character limit on footer text. In Google Apps, the limit is 10,000 characters.
- **Messages sent within the organization**—Google Apps includes an option to append the footer to messages sent within the organization. No equivalent option exists in Postini.

[Learn more](#) about the feature differences and improvements between Google Apps and Postini.

Google Apps Message Encryption

During your transition from Postini to Google Apps, your Google Message Encryption (GME) service is transitioned to Google Apps Message Encryption (GAME). GAME is available for Google Apps and includes many of the same features and functionality that are available to Postini GME customers.

Your GAME order

Encryption (GAME) orders are always offline, which means you will receive an invoice. If we can create your Google Apps order as an online order, we'll do so, but the encryption order is always offline.

The minimum order for each GAME account is 100 seats. If you have fewer than 100 seats in any domain, or have multiple domains sharing a 100 minimum-seat license in Postini, you'll still be billed for 100 seats per GAME account. To avoid being billed for seats you aren't using, we encourage you to [choose one primary domain](#) during transition, to help ensure a minimum of 100 seats per GAME account.

Note: The 100-seat minimum applies to GAME accounts only, not Google Apps accounts. If you transition a Postini domain containing fewer than 100 seats to Google Apps, you pay for only the number of seats transitioned.

In addition to the GAME order, Google will approach you to sign a GAME service level amendment (SLA). This can occur either before or after your transition, and you must complete the SLA no later than your next renewal of encryption service.

How the transition works for GAME

The transition process automatically transitions all of your domains that are currently licensed with GME for encryption via GAME. Although you can download the GAME administrator app from the Google Apps Marketplace (see "Add new users or domains", below), as a transitioning customer, you don't need the Marketplace app initially—the transition process sets up your users and settings to let you use GAME right away.

In the Google Apps Admin console, GAME settings, including those transitioned from GME, appear under [Content compliance](#). To see which Content compliance settings are included in setting up encryption, see the "Set up encryption for content compliance" section of the [Message Encryption Quick Start Guide](#).

Note: Use the material in the Message Encryption Quick Start Guide for reference only. Transitioning customers don't need to set up encryption in GAME—your GME encryption settings transition automatically.

Post-transition: Create new Zix subdomain MX records

After your transition, you need to [create new Zix subdomain MX records](#) in Google Apps. The format for Zix subdomain MX records in Google Apps is different from your current Zix subdomain MX record format:

- Old format:

zixvpm.[domain].com. MX IN 3600 mx35241.zixworks.com



zixvpm.[domain].com. MX IN 3600 mx35242.zixworks.com

- New format:

zixvpm.[yourdomain].com MX IN 3600 10 zixvpm.googlemessageencryption.com

Existing Zix subdomain MX records will continue to work for some time, but we encourage you to create new Zix subdomain records as soon as possible, to prevent issues when we eventually stop supporting the existing records. After you create new records, be sure to remove the old ones. Contact your Domain Name Service (DNS) provider if you need help with removing old subdomain MX records.

How GAME works

From an end-user perspective, GAME works the same as GME. When an encrypted message arrives, the user receives a notification email, clicks the link in the email, signs in to GAME, and reads the message in the secure portal. All encryption settings and related processes are transparent to the user.

For administrators, the [Message Encryption Quick Start Guide](#) contains all the relevant information regarding settings, users, and so on. For transitioning users, most of the material covered in the guide takes place automatically—with the exception of creating Zix subdomain MX records, as explained above.

Add new users or domains

After your transition, if you add a new user to a domain that was included in the GAME transition, that user is automatically included as an encryption user.

To add a new GAME domain post-transition, do the following:

- Download and install the [GAME Marketplace app](#) from the Google Apps Marketplace. The GAME administrator app gives you a simple way to define exactly which of your employees can access GAME email encryption functionality.
- [Contact Zix support](#) to ensure your new domain is enabled with encryption.

To add new encryption users post-transition:

- Place all encryption users in a separate organization or sub-organization with the correct encryption filters in place.
- Disable encryption filters for any organization where encryption should not be in use.

Note: If a non-encrypted user attempts to send a message using encryption, the message bounces.

Google Apps features that protect against spoofing



Spoofing occurs when a spammer forges the From address on a mail message so that the message appears to come from a domain that didn't actually send it. Both Postini and Google Apps provide several tools to protect against spoofing:

- Creating an Sender Policy Framework (SPF) record
- Adding a DomainKeys Identified Mail (DKIM) digital signature
- Creating a Domain-based Message Authentication, Reporting, and Conformance (DMARC) record
- Allowing messages from certain IP addresses only within the domain

For message senders, these tools let the sender provide information to recipients to help the recipients identify if someone is spoofing that sender's email address. For message recipients, these tools provide a way to identify incoming spoofed messages.

How the transition works for spoofing protection features

If you have customized SPF and DKIM settings in Postini, the transition tool doesn't move these to Google Apps. If you have IP Lock settings, the transition tool copies these to equivalent [Content compliance](#) settings. Learn more about which message settings [are](#) and [aren't](#) transitioned to Google Apps.

Using spoofing protection features in Google Apps

Google Apps automatically examines the SPF, DKIM, and DMARC settings associated with all incoming messages, so no configuration is necessary for these features.

For outgoing messages, you set up [SPF records](#) and [DMARC records](#) as part of your domain name service (DNS) for your domain, not as part of Google Apps. By contrast you can [add a DKIM signature](#) to outgoing messages by clicking **Authenticate email** in the Google Apps Gmail settings.

Feature differences and improvements

Message senders: Protect your domain from being spoofed

Both Google Apps and Postini users can create SPF records and DMARC records for outgoing messages.

NOTE: Because DMARC gives you more control over the disposition of unauthenticated emails, we recommend that you create a DMARC record for your domain.

In addition, Google Apps allows you to add a DKIM signature to outgoing messages. Postini doesn't add DKIM signatures to outgoing messages.

Message recipients: Identify incoming messages from spoofed domains



Google Apps automatically examines the SPF, DKIM, and DMARC settings associated with all incoming messages to classify the messages as clean or spam and, in many cases, to reject spoofed mail. Because this functionality is built in to the system, it doesn't require any configuration. This creates a more efficient, effective spoof protection approach.

Postini allows admin users to manually configure the SPF and DKIM processing of inbound messages. This is unnecessary and can lead to Postini admins needing to manage complex configurations.

NOTE: Postini doesn't support DMARC blocking of incoming messages.

Both Google Apps and Postini allow you to specify an IP address or range of addresses within a domain, and allow messages from those addresses only. In Postini, this feature is called IP Lock. In Google Apps, you [set up this feature](#) in the Content compliance setting. The feature works similarly between the two systems.

NOTE: Because IP-based spoofing protection is cumbersome and increases the risk of error—as administrators must maintain and adjust a dynamic set of sender source IP addresses—we recommend using DMARC instead.

‘Spooling’ in Google Apps: Retrying messages

The Spool Manager is an optional Postini feature for some service configurations. When your mail server becomes unavailable (for example, due to a crashed server or network connectivity problems), the Spool Manager stores or spools your mail for later release when your server is ready.

After your transition to Google Apps, spooling is no longer needed. Gmail is a store-and-forward system (unlike Postini), so it stores and retries messages automatically when your Exchange server is down. Google Apps will retry a message for a period of seven days until the message is either successfully delivered or until the 7-day retry period elapses.

Note:

- While Postini has spool quota thresholds, Gmail has no per-customer limit to the number of retry messages.
- Retries occur more frequently as a message initially becomes undeliverable. The retries become less frequent as you near the end of the 7-day retry period.

Delivery status notifications

During the 7-day retry period, the sender will receive one or more Delivery Status Notifications, which warn the sender that the message will be retried for an x number of additional days due to connection timeout. This will repeat for the number of days indicated until the message is either successfully delivered or the retry period times out—in which case, the original sender will get a final Non-Delivery Report.

Use Log Search to monitor the status of retried messages

Super administrators for your account can see the volume of email that is being retried using the Log Search feature. Messages that are retried will be logged with a status of Pending Delivery. (Log Search displays the log data details, but not the content of the messages themselves.)

Update your Host setting to redirect mail to another mail server

If you notice that your non-Gmail mail server is down and your messages are stuck in a retry state, you can change the destination mid-flow by reconfiguring delivery to go to a different server. You can do this by updating your Hosts setting in the [Google Admin console](#). By making this change, the next time the message is retried, it will retry using the updated setting. For instructions, see [Add mail routes with the Hosts tab](#).

Troubleshooting

I don't have a Postini root admin account

As you transition from Postini to Google Apps, you'll need access to the Postini Administration Console to initiate your service transition. To help you get started with your transition, Google will also send transition invitation emails and other email updates to your Postini administrator.

A small percentage of Postini customers don't have a Postini administrator account. If this is true for your organization, you won't be able to initiate your service transition. In this case, Google will automatically initiate your transition (when you become eligible) and create a new Google Apps administrator account with an auto-generated password. This new account will enable you to sign in to the Google Admin console, and get started with Google Apps and Google Apps Vault after the transition is completed.

How will I gain access to my new Google Apps admin account after my transition?

If you don't have a Postini admin account, you can get started with Google Apps and Google Apps Vault after your service transition by contacting [Google for Work Support](#). The Support team will provide your new login email and password to help you get started.

If I don't have a Postini admin account that will receive email updates about my transition, how will I know when my transition has been initiated?

If the necessary contact information is available, Google will send transition invitation emails and updates to a select number of business contacts in your organization. These updates include an email that confirms the deadline for your service transition (several weeks in advance) and an update to confirm when your service transition is completed.

NOTE: A few customers might have a Postini administrator account, but this account might be for domains that haven't been verified in Postini. In this case, Google will create a new Google Apps administrator account with an auto-generated password. For access to this account, contact [Google for Work Support](#).

Users can't sign in to Google services

After your organization transitions from Postini to Google Apps, a user might experience the result of a conflicting account.

What is a conflicting account?

A conflicting account occurs when the following takes place:

- Prior to the transition, a user in your company created a Google account using a corporate email



address.

- During the transition, you created a Google Apps account user with the same corporate email address.

As a result, the user's original Google account is now in conflict with the new Google Apps account. When a user with a conflicting account tries to sign in to a Google service, such as Adwords, Analytics, or Picasa, using his or her original Google account username and password, a message prompts the user to sign in either with a different email address or with a temporary username. This message appears because the Google service now associates the email address with the Google Apps account, so the user's original password is no longer valid for this email address.

The user must select one of the displayed options to resolve the conflict and sign in to the Google service. See [How to resolve conflicting accounts](#) for detailed instructions.

NOTE: For privacy reasons, we aren't authorized to provide a list of conflicting accounts in your organization. Instead, please educate your Help desk on how to address this end user issue.

FAQs: Postini Transition to Google Apps

If you have questions, or if you need troubleshooting assistance during or after your transition, please refer to the following frequently asked questions and answers. See also the FAQs in the [Postini Transition Resource Center](#).

How do I know when it's time for me to begin my transition to Google Apps?

Before you can begin your transition to Google Apps, you will receive a series of email communications from Google with instructions about your upcoming transition. When you receive your Transition Invitation email, which includes a link to your Transition Console, it's time for you to begin. You'll have 60 days to complete your transition once you receive this email.

Note: Online customers will have 30 days to complete their transition. For details, see [What's different if I purchased Postini online?](#) in the Postini Transition Resource Center.)

Is there a document that details how to perform specific tasks in the new Google Admin console that were previously done in Postini?

Yes. For instructions on how to perform many tasks in the Google Admin console that are comparable to Postini, and to learn how to modify specific Google Apps settings after your service transition, see [Get started with advanced settings for Gmail](#) in the Transition Guide. See also [Configure advanced settings for Gmail](#) in the Help Center. These resources link to articles that describe how to configure Postini-like email settings, such as Default routing, Content compliance, Attachment compliance, and more.

How will Google's spam and virus filtering compare to Postini's?

Although the overall filtering effectiveness is very comparable, you should expect the filters to behave differently, acting more strict or lenient on different types of mail. For details, see [How Gmail spam and virus filtering differs from Postini](#).

How can users report spam?

Google Apps spam detection technology learns from user input. If a user indicates to the system that a message is spam or not spam, this lets us know whether or not these kinds of messages should reach that user's Inbox in the future. The more a user reports spam (or indicates that a message is not spam), the more effective this filtering mechanism becomes.

Depending on how you access your mail, here's how it works:

- Gmail users can report spam by clicking Report spam (or Not spam) in the Gmail interface. Users can also view their spam by clicking the Spam folder.
- Users of Google Apps Sync for Microsoft Outlook® can view Spam by looking inside the Junk E-Mail folder located right below the Inbox. User can report spam to Gmail by moving the message from the Inbox folder to Junk E-Mail folder, and they can report non-spam to Gmail by moving the message from the Junk E-Mail folder to the Inbox.
- If you're using an on-premise/non-Gmail system, you can use Quarantine Summary and Message Center.



How do Quarantine Summary and Message Center work in the Google Apps platform?

Once your orgs, users, and settings are moved over from Postini to Google Apps, you will automatically begin using the Google Apps spam and virus protection instead of Postini's. When using the Google Apps platform with non-Gmail mail servers, users can manage spam using the Quarantine Summary and the Message Center.

Quarantine Summary

The Quarantine Summary is comparable to what users experience with Postini today. It is a digest that lists all messages that were marked as spam. It is delivered to users in their inbox and enables them to identify a message as not spam and deliver it to their on-premise inbox.

Message Center

The Message Center is a web-based console that enables users to manage their spam messages. Like the Quarantine Summary, users can identify a message as not spam and deliver it to their on-premise inbox.

NOTE: Spam messages are stored in the Apps platform for 30 days, while Postini typically stores messages for 14 days.

How does virus protection work with Google Apps?

Google Apps provides comprehensive virus protection. Like Postini, Gmail utilizes two virus filtering engines for all messages, and virus protection also includes the following:

- Messages that have executable file attachments are automatically rejected, even if those files are compressed into another file, such as a zip or rar file. We do this for many types of executable files (see [Some file types are blocked](#)).
- Messages are automatically rejected that contain a password protected zip file within another zip file.
- Every attachment is automatically scanned when it's received, and messages that contains viruses are automatically rejected.

Additionally, Google provides increased protection against phishing-based attacks and messages containing URLs that point to malicious sites. For more information, see [How Gmail spam and virus filtering differs from Postini](#).

What does it mean that my Postini Admin Console will be in read-only mode during my transition?

When you click Begin Transition Now in the Transition Console, your Postini Admin Console will be switched to read-only mode. This means you can still log in to the Admin Console and view your settings, but you cannot make any changes. Mail flow and filtering will not be interrupted during this time.

Later, when you receive confirmation that your service transition is completed, you can log in to the Google Admin console to view the email settings that were moved over. (See [Get started with advanced settings for Gmail](#).)

How do I know if my firewall is set up to allow Google Apps mail?

Your firewall must be configured to allow email from both Postini and Google IP ranges. If you configured your firewall a long time ago, it may be open to Postini IPs but not yet to Google IPs. (If you never locked down your firewall in the first place, you may not need to make changes to your firewall configuration.)



For instructions, see [Allow email from Google IPs to your email server](#).

What should I do if the Transition Console tells me I cannot proceed because my firewall is not open?

If your firewall is set up to only allow email from Postini IP ranges, and not from Google Apps IP ranges, you'll receive an error message when you click Begin Transition Now in the Transition Console. The error message will let you know that your firewall is not open to Google. To correct this, you'll need to add Google IP ranges to your firewall configuration. For instructions, see [Allow email from Google IPs to your email server](#).

NOTE: Once you make the changes to your firewall configuration, you'll need to return to the Transition Console to initiate your transition.

What does Postini passthrough mean?

With Postini passthrough, Postini settings do not take effect, and instead mail is "passed through" to Google Apps. Postini is in the passthrough state for Classic customers after you click the Begin Transition Now button and for Hybrid customers after you click the Finish Transition button in the Transition Console. Your filtering will then occur in Google Apps instead of Postini. Your mail flow continues without interruption during this process.

During my service transition, will I be able to transition individual organizational units rather than transition my entire domain?

By clicking Begin Transition Now, you'll transition all of the orgs, settings, and users for your account to Google Apps. You cannot transition from Postini to Google Apps on an org-by-org basis, but we are considering adding this capability in the future.

Note: The transition process is slightly different depending on whether you're a Postini Classic or Hybrid customer. See [Transition steps for Postini Classic customers](#) and [Transition steps for Postini Hybrid customers](#).

In my Postini configuration, I had one account org, one email config org, and one user org. Why do I see just one organizational unit in the Google Admin console after my service migration?

If your Postini configuration includes just one account org, one email config, and one user org, you will see just one organizational unit (OU) in the Google Admin console when you first log in. In Google Apps, the account org and email config org are not necessary, so the org structure will be simplified for you. If needed, you can add sub-organizations. See [Create an organizational structure](#).

What type of reporting tools are available in the Google Admin console?

There are many different reports currently available in the Google Admin console, and you can find a description of them [here](#). Additional reports are on the roadmap that are similar to what Postini offers. How long will it take to complete my service transition?

The transition time varies depending on the number of users included in the transition, and can range from a few minutes to several days.

Will dual-delivery and split-delivery configurations be automatically transitioned from Postini to Google Apps?

Mail routing configurations will be automatically transitioned to Google Apps during the service transition;

however, in some cases manual configuration will be needed, and Google will assist these customers to complete their transitions.

Postini has a "black hole" feature for spam filtering that reduces the amount of spam a user needs to look through to find valid messages. Does Google handle spam in the same way?

Google Apps email filters block blatant spam just like Postini, and questionable messages go into the Spam folder. Non-Gmail users can use the Quarantine Summary and Message Center.

What are the recommended settings for split delivery using Google Apps email filters?

See [Mail routing and delivery: Guidelines and best practices](#), and click Routing examples and use cases.

Do you provide Transport Layer Security (TLS)? If yes, do you provide both forced and opportunistic TLS?

Yes, Gmail uses "opportunistic" TLS, which means it will attempt to use TLS whenever possible. You can also configure [TLS compliance](#) policies to require TLS when communicating with specified external domains. If TLS is not available for the domains defined, inbound mail will be rejected and outbound mail will not be transmitted.

Do you provide message tracking for both inbound and outbound mail? What's the lag time?

We do provide audit logs and [message tracking logs](#). Google has a delay that is guaranteed 1 hour or less.

Do you have an Outlook plug-in? Are there any compatibility issues? What are the installation methods?

You can use any POP or IMAP clients such as Outlook or Thunderbird. We also have a sync tool for Outlook called [Google Apps Sync for Microsoft Outlook](#) (GASMO).

NOTE: If you're a reseller customer, please reach out to your reseller directly for questions regarding your transition. Google for Work Support is available to assist you once you've been invited or have begun your transition.

Transition Support

Use the following Support resources during your Postini Transition to Google Apps:

- Customers who are still transitioning from Postini - For help with general issues and questions about your Postini Transition to Google Apps, see the [Postini Support page](#).
- Google Apps administrators - If you are a Google Apps administrator and have questions about the Google Admin console or other questions about your service, see the [Google Apps Support page](#).
- Gmail users - For help in using Gmail, see the [Gmail help center](#).

Note: If you're a reseller customer, please reach out to your reseller directly for questions regarding your transition. Google for Work Support is available to assist you once you've been invited or have begun your transition.



© 2015 Google Inc. All rights reserved. Google and the Google logo are trademarks of Google Inc. All other company and product names may be trademarks of the respective companies with which they are associated.

