PART THREE

Setting up External Mail Servers
Google Apps work surprisingly well with external mail servers to route, filter, scan, archive and/or backup email. Spend enough time with Google's help documentation and you'll certainly figure it all out.

Google's help documents explain how to accomplish tasks. But Google's documents don't highlight why you might choose one specific mail server setup over another.

This guide is designed to help you quickly understand key concepts. It links tasks you might want to accomplish — with the relevant Google help pages, so you can dive into the details.
**GOOGLE APPS AND LEGACY SYSTEMS**

Most likely, you already have an email system.

If you don’t have an email system, you’re lucky. Go directly to “Set up Google Apps today”.

Everyone else is stuck dealing with what we’ll call a “legacy system”: an email system that likely requires far more care and maintenance than Google Apps. A switch to Google Apps transforms email from an on-site server into a service.

That said, Google Apps works well with legacy systems. That’s important, because you’ll need Google Apps and your legacy system to work together during your transition to Google Apps.

Ideally, the email needs of your organization could be met with Google Apps. However, there are times when that just isn’t feasible.

Speaking from experience, you’ll want Google Apps to “play nicely” with outside servers at least twice: when testing Google Apps and during the migration process.

Some organizations choose to split email delivery between a legacy system and Google Apps, with distinct groups of people on each system.

Other organizations use external mail servers alongside Google Apps for a variety of compliance, filtering and security needs — in addition to the need for archiving and backup.

This guide is your introduction to using Google Apps with external mail servers.

**No email yet? Set up Google Apps today**

A new organization can get started with Google Apps quickly.

New organizations are fortunate: there’s no legacy server or data to import, so setup is simple.
New organizations are fortunate: there's no legacy server or data to import, so setup is simple.

The basic process:
1. Sign up for a new Google Apps account at gsuite.google.com.
2. Verify that you have control of the domain you want to use.
3. Setup user accounts.
4. Change your domain's MX (mail exchange) records to route mail to Google.
5. Start using Google Apps! Learn about features at gsuite.google.com/learning-center.

Security conscious organizations might take a few extra steps:
- Enable SSL to encrypt connections to Google Apps.
- Configure DKIM, SPF and DMARC to reduce email spoofing and improve deliverability.
- Allow people to use 2-step authentication – or better: require it!

INITIAL TESTING AND MIGRATION

It is possible to switch to Google Apps immediately.

Sign up for Google Apps. Configure an account for each person in the organization and set your mail servers to route email to Google. Wait about 72 hours for your mail server settings to update across the internet. Open your browser to gmail.com and log in. Congratulations! You're now using Gmail and Google Apps with your organization's domain name.

Google Apps is a proven enterprise collaboration system: the technology works. But a 72 hour switch to Google Apps from your legacy mail system probably isn't prudent. A managed migration lets you lead people to more effective processes at a steady pace.
Another way to put it: a move to Google Apps is a chance to change how people work. With Google Groups, multiple people can share a collaborative inbox, which can result in faster responses to customers. But people need time to learn how to use new tools.

That's why we recommend you test Google Apps before you deploy. It isn't so much a test to make sure Google Apps works — we know it does! Instead, it's a test to understand exactly how Google Apps enables people to work more efficiently.

**Test with split delivery**

To start your test of Google Apps, set up what Google calls "split delivery."

With a split delivery setup, you setup Google Apps, then point your MX (mail exchange) records to Google's mail servers. All incoming email arrives at Gmail. However, be sure to only create Google Accounts for people involved in testing Google Apps.

When an email for a user with a Google Account arrives, it will arrive in Gmail. Email for other people can be routed to your legacy mail server. Email delivery is split: Gmail users use their Google Account, while everyone else continues to use the legacy system.

Learn more from Google: "Mail routing and delivery: Guidelines and best practices"

**Migrate with dual delivery**

You may also configure Google Apps for dual delivery, which delivers email to both systems. Just as with split delivery, dual delivery involves setting up Google Apps and pointing MX Records to Google's mail servers. People have accounts on both systems. When an email arrives, it is delivered to both Gmail and the legacy system.

Dual delivery is most useful during the migration process. After importing everyone's legacy data into Google Apps, people can switch from the legacy system to Google Apps.

Learn more from Google: "Receiving routing settings"
Import email from legacy systems

Google provides administrative tools to import email from legacy systems, including tools to import mail from both Microsoft Exchange and IBM Notes. The Google Apps Migration for Microsoft Exchange imports mail, personal contacts and calendar data. Google Apps Migration for Microsoft Exchange will import mail from traditional IMAP mail servers.

Individual account migration options are also available, but not recommended if you have more than a few accounts. People who use Microsoft Outlook can migrate data using the Google Apps Migration for Microsoft Outlook tool. Mac users can use the Google Email Uploader for Mac. And, unless you disable the feature as an administrator, people may also use Google’s Mail Fetcher to pull mail into the Google Account from up to five other email accounts.

Learn more from Google: “Google Apps migration options”

Sync user accounts

To add a user to Google Apps, log in as an administrator at admin.google.com, select “Users” and then select the “Add Person” icon in the upper right corner.

But if you already have a mail server, you probably have accounts set up. Here’s the good news: you don’t have to manually recreate each person’s individual account. If your system supports LDAP (lightweight directory access protocol), you can sync user accounts to Google Apps.

Google Cloud Directory Sync works with LDAP-compliant servers, most notably the Microsoft Active Directory. Sync isn’t instant, it takes some initial configuration. But in the long run, it can simplify account management.

Learn more from Google: “Google Cloud Directory Sync”
LONG-TERM SPLIT EMAIL DELIVERY

Different groups of people have different needs.

If you need to run a legacy mail server side-by-side with Google Apps long term, you can. With long term split delivery, incoming mail is split by groups within the same organization (or domain name). One group uses the legacy system, while the other group uses Google Apps.

For example, a university might deliver student email to Google Apps, while faculty email is sent to a legacy system, such as Microsoft Exchange. Or, a company might route the email of employees stationed at its headquarters to Google Apps, while sending mail for employees at a secondary location to a legacy system.

To get this to work, first setup mail routes. Next, create organizational units in Google Apps and assign people to different units. Finally, change each units’ receiving routing settings to deliver email to the correct host. Learn more from Google: “Configure email settings for an organizational unit”

Setup mail routes

To use external mail servers with Google Apps, you need to define mail routes.

A mail route identifies a legacy mail server by domain or by IP address. Mail routes may also identify multiple hosts, which is useful if you’re working with legacy systems configured to offer failover or load balancing.

To configure mail routes, log in to your Google Apps admin account at admin.google.com, then navigate to Google Apps > Gmail > Hosts.

Learn more from Google: “Add mail routes with the Hosts tab”
FILTERING / COMPLIANCE / SECURITY

Filtering inbound email

It may seem redundant to pass email through an additional external filter before it arrives in Gmail. After all, Google Apps provides excellent antivirus scanning and spam filtering. It also blocks executable attachments, which is good.

Google also places suspected spam in the user’s spam folder. That’s the potential problem. Each person can access their spam folder, which means there’s a chance that someone could click on a harmful link or fall for a phishing scheme. An external filter might identify an email as spam before it even reaches Gmail, keeping the email entirely inaccessible to the user.

To set up an inbound mail gateway, your MX records need to be configured to direct mail for your domain to the gateway server. Configure this device to route all email — post scanning — to Google’s servers. You also need to set Gmail to accept email only from the gateway server, which ensures all incoming mail has been properly processed.

Learn more from Google: “Inbound mail gateway”

Outbound email: All for one gateway or per-user gateway?

Mail passes through a gateway, but like a baton in a relay race, mail is “handed off” to a relay server. Gmail also calls these relays, per-user outbound gateways. While seemingly similar, an outbound gateway and a per-user outbound gateway solve different problems.

An outbound gateway typically is used to filter or archive email. When mail passes through the gateway, it may be scanned and/or stored. A per-user outbound gateway lets you “hand off” an email to an external server to be sent, while still using Gmail to create the email.

People with two roles may find an per-user outbound gateways useful. For example, a corporate executive might send most email from their corporate account: AnExec@Company.com. But they may also play a role in a separate corporate foundation with a different domain...
name. The per-user outbound gateway would allow them to send email from this other
domain: SameExec@Foundation.org. People who use an external help desk or customer
relationship management system (CRM) may also benefit from the per-user option.

An per-user outbound gateway solves another problem: it eliminates "on behalf of"
messages. Without per-user setting selected, a recipient might see the "From:" field
as "SameExec@Foundation.org on behalf of AnExec@ Company.com". With a per-user
gateways, the "From:" field would be "SameExec@Foundation.org".

Set up of outbound gateways and per-user gateways are slightly different. Administrators
configure outbound gateways: the user has no control over outbound gateways. Yet while
administrators may enable the use of per-user gateways, individual users must then
configure their own outbound relay account settings. (Per-user gateways/relaying may
also be prohibited.)

Per-user outbound gateways present a potential problem: mail "handed off" to an external
server isn’t stored in Gmail’s “Sent Mail” folder, since the email is sent by the outbound
relay mail server. To ensure that all mail created with Gmail is stored in Gmail — even if
it is actually sent by another mail server — an administrator needs to enable Google’s
comprehensive mail storage setting. In the Google Apps admin dashboard, go to Apps > G
Suite > Gmail > Advanced settings to enable this.

Learn more from Google: "Outbound mail gateway", "Per-user outbound gateway", and
"Comprehensive mail storage setting"

**TLS compliance**
You may choose to require a secure connection for email between your organization and
specific domains. Email between the two domains will be protected with Transport Layer
Security (TLS).
Google defines three distinct purposes for scanning: for content compliance, for objectionable content, and for attachment compliance.

Gmail will reject inbound mail, and will not send outbound mail if TLS isn't available at the specified domain.

(To enable this, log in to your Google Apps admin console. Go to Apps > G Suite > Gmail > Advanced Settings. Choose your domain or organizational unit and go to "Secure Transport (TLS) Compliance".)

Learn more from Google: "Secure transport compliance setting"

SMTP relay service

Google’s SMTP relay service is pretty much the opposite of using an outbound relay. With an outbound relay, you use Gmail, but send mail from another mail server. The SMTP service is the opposite: you use a legacy mail server, but send mail from Google's mail servers. As a result, your outbound email benefits from Google's spam and virus filters.

EMAIL CONTENT SCANNING (AND ROUTING!)

Google Apps offers automated email content scanning.

Google defines three distinct purposes for scanning: for content compliance, for objectionable content, and for attachment compliance.

The first two scan messages and text attachment content. Attachment compliance scans attachments based on attachment name, type or size. Note that attachments other than text files are not scanned for file content.

As the Google Apps administrator, you define three things:

- Which messages to scan,
- What scans should look for, and
- What to do when a match is made.
When a message or attachment matches one of your regular expressions, Gmail offers three options: reject the email, quarantine, or modify it.

The last bit makes content scanning relevant in this guide: a message that matches your scan criteria can be re-routed.

Scanning may help ensure compliance with organization policies. For example, your company might establish a policy of never permitting inbound or outbound attachments. Mail with attachments could simply be rejected, notifying the sender of the rejection. Alternatively, email with attachments could be delivered, but with attachments removed.

### Which messages to scan
First, choose which messages to scan. As with routing options, you may define different scans for different organization units. Or, you may choose to scan all mail for your Google Apps account domains.

Scanning may be restricted to external mail (outbound and/or inbound) or internal email (outbound and/or inbound). Any one — or all — of the four options may be selected. The default selection is all four sets.

### What to scan for (or, scan criteria)
Next, you’ll specify what to look for.

Content compliance and objectionable content scans may be set to scan for text strings or patterns. You’ll define these strings using regular expressions (regexp), a common method of specifying a search patterns in text.

For example, a regular expression configured to find any string containing "am Gibs" would return a match when scanning a document containing the name “William Gibson”.

Within a scan, you may specify searches for multiple regular expressions. You can choose whether the scan must match any or all of the terms.

Learn more from Google: “Guidelines for using regular expressions”
What to do when a match occurs

When a message or attachment matches one of your regular expressions, Gmail offers three options: reject the email, quarantine, or modify it. Rejected email returns it to the sender. You can explain the rejection with customized rejection notice text.

Quarantined messages are sent to and admin who can review the message and decide whether or not to send it.

Modified mail will be delivered. Note, however, that one of the ways to modify the email is to change the recipient: so modified mail may be delivered to someone other than the specified recipient!

Modifications that may be made to email include modifying the header or subject, flagging a message as spam, changing the mail route, and replacing or adding recipients. Additionally, attachments may be removed.

Learn more from Google: "Content compliance setting", "Objectionable content setting", and "Attachment compliance setting".

Restrict delivery

You may choose to limit the exchange of email between specific domains for groups of users.

A school district might choose to limit students to emailing within the district, while allowing faculty and staff to email anyone. A business might provide a long term contractor a company email address, but limit the contractor to sending email internally from that account.

(To configure this, log in to your Google Apps admin console. Go to Apps > G Suite > Gmail > Advanced settings. Choose your domain or organizational unit and go to "Restrict delivery".)

Learn more from Google: "Restrict delivery setting".
An effective email backup system changes whenever a person's email data changes, and offers **fast retrieval and restoration of email.**

**BACKUP AND ARCHIVING**

A backup provides a copy. And, since digital copies are essentially indistinguishable from originals, a backup copy can replace a missing original. An effective email backup system changes whenever a person's email data changes, and offers fast retrieval and restoration of email. The best email backup systems provide retrieval and restoration — even when the entire original email system is unavailable.

*Example: Datto Backupify for Google Apps provides a cloud-to-cloud backup system that backs up email up to three times a day, and offers fast retrieval and restoration of missing email.*

An archive is essentially a backup set that never changes. An archive preserves a historical picture: a snapshot of email preserved at a specific point in time. An email archive search will always return the same results: today, tomorrow, and any time in the future. The purpose of an archive is preservation, not restoration.

*Example: Google Vault offers archiving and retention of email based on administrator defined policies.*

System settings for data retention and user access help define the difference between a backup and an archive. If people can retrieve and restore recently deleted email easily, that's a backup. If email is permanently preserved and not user accessible, that's an archive.

Legacy mail servers may also provide email backup and/or archiving. You'd either configure the server for **long-term dual delivery,** or route all mail through the server. Running this legacy server will incur additional costs. You need to determine if the business benefit is worth the additional cost for your organization.

Learn more about backup vs. archival: "Datto Backupify Vs. G Suite Vault: How They Differ"

Learn more backup + archival: "Datto Backupify and Google Vault: Why You Need Both"
KEY THINGS TO KNOW

We suggest you first read through the entire document. Then, customize your settings with the sequence below.

1. Know how to setup mail routes and organization units
   - Create mail routes to define servers to which you connect.
   - Understand organizational structure, and
   - Define organizational units (groups of people).

*Important: You’ll use mail routes and organizational units often when working external mail servers!*

2. Learn how Google Apps handles routing
   - Learn the various inbound and outbound email configurations.

3. Understand how to configure email scanning
   - Know how to create regular expressions.
     - Learn to configure:
       - Content compliance settings,
       - Objectionable content settings, and
       - Attachment compliance settings.

4. Meet your backup and archiving needs
   - Provide a way to backup and restore missing email.
   - Make sure your organization preserves email securely for compliance purposes.

*NOTES:*

- Cross link to first 2 eBooks once they have been redesigned
- Add a ‘Sign up for a free trial’ section