**G SUITE MAIL MANAGEMENT**

**Introduction to G Suite Mail Management**

## **Welcome and Getting Started Guide**

****Introduction****

Welcome to G Suite Mail Management.

In this course you will examine your domain's Domain Name System (DNS) records and implement DNS email security measures to protect against others using your domain for spoofing and phishing attacks.

You will learn about Gmail's email safety features that are designed to protect users from inbound phishing and harmful software (malware). You will be introduced to the spam and phishing prevention measures that you can implement in the admin console such as email whitelists and blocked sender lists.

You will configure email compliance which allows you to examine messages for specific content, objectionable content or attachments and then take actions on messages that do not comply with your organizational policies. You will also be introduced to the predefined Data Loss Prevention templates that can be used as part of a compliance policy.

Finally you will be introduced to mail routing controls provided in G Suite. You will gain an understanding of the mail routing options such as split and dual delivery and know when to use them.

In order to pass the quizzes, reading the help center links provided is advised.

****Prerequisites****

You should complete the 'Introduction to G Suite', 'Managing G Suite', and 'G Suite Security' courses before taking this course.

If you have completed the previous courses but no longer have your trial domain, you should complete the exercise that immediately follows this reading before moving onto the next lesson. If your trial domain is still valid you can go straight to [Introduction to DNS Records](https://www.coursera.org/learn/g-suite-mail-management/supplement/gsc64/introduction-to-dns-records" \o "Introduction to DNS Records" \t "/home/sherwinowen/Documents\\x/_blank).

## **Exercise #1 - Prepare your G Suite Domain**

****Introduction****

This exercise only needs to be completed if the G Suite Enterprise trial domain you used in the previous course has expired. In this case you should create a new domain and populate it as described below:

****Instructions****

1. Complete the [Create your G Suite Trial Account](https://www.coursera.org/learn/introduction-g-suite/supplement/q7NRF/exercise-1-create-your-g-suite-trial-account" \o "Exercise #1 - Create your G Suite Trial Account" \t "/home/sherwinowen/Documents\\x/_blank) exercise from 'Introduction to G Suite'. You can purchase a new domain or you can use a domain that you already own. Please see the Help Center resource links below for more details on using an existing domain.

2. Create the following OUs:

* Executive
* Employees
* Contractors

3. Create the following G Suite user accounts:

| **First name** | **Last name** | **Email address** | **Employee title** | **Org Unit Path** |
| --- | --- | --- | --- | --- |
| Alex | Bell | alex.bell@yourdomain | IT Manager | /Executive |
| Ellie | Gray | ellie.gray@yourdomain | Executive Assistant | /Employees |
| Jon | Baird | jon.baird@yourdomain | HR Business Partner | /Employees |
| Lars | Ericsson | lars.ericsson@yourdomain | HR Manager | /Executive |
| Samantha | Morse | samantha.morse@yourdomain | CEO | /Executive |
| Timothy | Lee | timothy.lee@yourdomain | Finance Manager | /Executive |
| Tom | Edison | tom.edison@yourdomain | Support Engineer | /Employees |
| Will | Marconi | will.marconi@yourdomain | Support Engineer | /Employees |
| Mark | Jones | mark.jones@yourdomain | Consultant | /Contractors |

****Help Center resources****

If you are bringing your own domain, you should read:

* [Verify your domain for G Suite](https://support.google.com/a/answer/60216" \o "Verify your domain for G Suite" \t "/home/sherwinowen/Documents\\x/_blank)
* [Set up MX records for G Suite Gmail](https://support.google.com/a/answer/140034" \o "Set up MX records for G Suite Gmail" \t "/home/sherwinowen/Documents\\x/_blank)
* [Authorize email senders with SPF](https://support.google.com/a/answer/33786" \o "Authorize email senders with SPF" \t "/home/sherwinowen/Documents\\x/_blank)

Creating OUs

* [Add an organizational unit](https://support.google.com/a/answer/182537" \o "Add an organizational unit" \t "/home/sherwinowen/Documents\\x/_blank)

Adding users

* [Add several users at once](https://support.google.com/a/answer/40057" \t "/home/sherwinowen/Documents\\x/_blank)

**Domain Name System (DNS)**

## **Introduction to DNS**

DNS stands for Domain Name System. This system is essentially the phone book of the Web that organizes and identifies domains. While a phone book translates a name like "Acme Pizza" into the correct phone number to call, the DNS translates a web address like "www.google.com" into the physical IP address such as "74.125.19.147" of the computer hosting that site (in this case, the Google homepage).

As the administrator, it is important that you have an understanding of your organization's DNS configuration, in particular how that configuration works with G Suite mail.

When using G Suite services, you may need to modify your DNS settings to set up various tools and services. You do this by changing your DNS records. For example, you change your domain's Mail Exchanger (MX) records to direct email for your domain to Google's mail servers.

It's important to understand that whilst in some instances you can update your DNS records directly from the G Suite admin console, your DNS records are always hosted and managed outside of G Suite with a DNS registrar such as GoDaddy, and eNom.

In this lesson you will learn about the key types of DNS records that G Suite requires.

****Important:**** It is assumed that you are using a trial G Suite account and a test domain for this training. If you are using a live/production domain, ****DO NOT**** make any changes to any of your DNS records.

## **DNS Records for G Suite**

In this reading we will cover the DNS records used by G Suite and describe the purpose of each.

****DNS records that impact mail delivery****

MX Record

Mail Exchange (MX) records direct email to the servers hosting your user accounts. To set up Gmail if you have G Suite, you need to point your MX records to the Google mail servers. Multiple MX records can be defined for a domain, each with a different priority. If mail can't be delivered using the highest priority record, the second priority record is used, and so on.

TXT Record

A TXT record is a DNS record that provides text information to sources outside your domain that can be used for a number of arbitrary purposes. G Suite uses TXT records for a variety of purposes such as domain verification and to implement email security measures such as SPF, DKIM, and DMARC which we will discuss later.

CNAME Record

A CNAME or Canonical Name record links an alias name to another true or canonical domain name. For instance, www.example.com might link to example.com. With G Suite services you use CNAME records to customize a Google service address or the address of a website built with Google Sites.

****Other DNS record types****

A Record

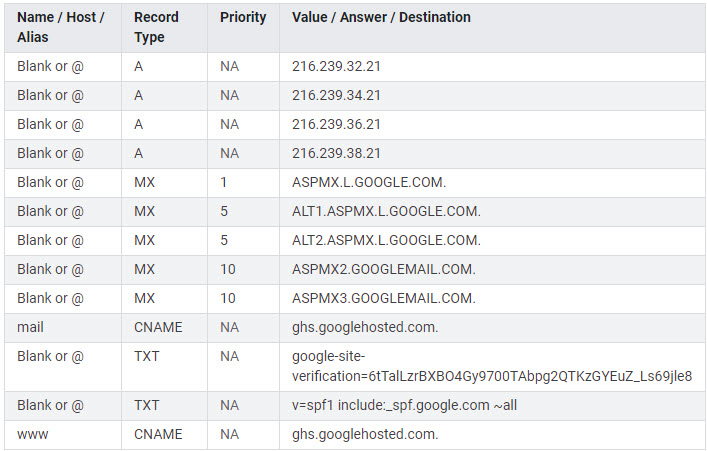
An A or Address record (also known as a host record) links a domain to the physical IP address of a computer hosting that domain's services.

NS Record

Name server (NS) records determine which servers will communicate DNS information for a domain. Generally, you have primary and secondary name server records for your domain. When using G Suite you may configure NS records that point to Google servers for DNS queries.

****Example DNS configuration****

Here are sample DNS settings for a domain used with G Suite. Note in the first column that you don't use the actual domain name in your DNS settings. Instead, you use the @ symbol (or leave it blank) to indicate the domain name.



The values shown above are for indicative purposes only and they are subject to change. Always refer to the G Suite Help Center for the latest information.

****Notes****

1. If you purchase your domain as part of the G Suite sign up flow, Google will automatically add the correct records for you. If you already own the domain, you will normally need to configure your DNS records to work with G Suite.

****Help Center resources****

* [Set up MX records for G Suite Gmail](https://support.google.com/a/answer/140034" \o "Set up MX records for G Suite Gmail" \t "/home/sherwinowen/Documents\\x/_blank)
* [About TXT records](https://support.google.com/a/answer/2716800" \o "About TXT records" \t "/home/sherwinowen/Documents\\x/_blank)
* [About CNAME records](https://support.google.com/a/answer/112037" \o "About CNAME records" \t "/home/sherwinowen/Documents\\x/_blank)
* [About A records](https://support.google.com/a/answer/2576578" \o "About A records" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #1 - Sign into your Domain Registrar**

****Introduction****

As mentioned previously, It's important to understand that whilst in some instances you can update your DNS records directly from the G Suite admin console, your DNS records are always hosted and managed outside of G Suite with a DNS registrar such as GoDaddy, and eNom.

In this exercise you will sign into your domain registrar. How you do that will depend upon whether you purchased your domain when you signed up for the G Suite trial account, or whether you are using an existing domain for this training.

****Directions****

If you purchased your domain as part of the sign up flow, complete the following steps:

1. If you are not already signed in, sign in to your domain as the administrator at [admin.google.com](https://admin.google.com/" \t "/home/sherwinowen/Documents\\x/_blank).

2. Click the ****Domains**** icon.

3. Click the ****Manage Domains****icon.

4. Click the****View Details**** link for your primary domain. Your domain details will appear on the right hand side of the screen.

5. If you purchased your domain from Google Domains, click ****MANAGE DOMAIN****. This will load the Google Domains console. You should not be required to sign into this console.

If your domain was purchased from another registrar during the G Suite sign up process, look for and expand the ****Advanced DNS Settings**** section. Expand this section and use the credentials presented to sign into your DNS console.

If you are using an existing domain sign directly into your registrar as normal.

## **Exercise #2 - Review your MX Records**

****Introduction****

Probably the most commonly known DNS records are Mail Exchange (MX) records. These ensure that inbound mail is correctly routed to your mail host, and in the case of G Suite they tell the internet to route mail to Google's mail servers for eventual delivery to your user's Gmail inbox. In this exercise you will review your MX records.

****Directions****

1. Sign into your domain registrar. See [Sign into your Domain Registrar](https://www.coursera.org/learn/g-suite-mail-management/supplement/6wpSd/exercise-1-sign-into-your-domain-registrar" \o "Sign into your Domain Registrar" \t "/home/sherwinowen/Documents\\x/_blank).

If you purchased your domain as part of the G Suite sign up process, your MX records should already be configured for you. If you did not purchase your domain as part of the sign up process you will need to add the records manually to ensure mail for your domain is routed to the Google servers.

2. Locate your MX records in your DNS records.

If Google Domains is your registrar, select ****DNS**** from the left hand menu, then scroll down to the 'Synthetic records' card and click****>**** to expand the G Suite section. If you are using another registrar the navigation will be different. Refer to your provider's help to locate your DNS records.

Your MX records should look similar to those shown in the table below. Refer to [Set up MX records for G Suite Gmail](https://support.google.com/a/answer/140034" \o "Set up MX records for G Suite Gmail" \t "/home/sherwinowen/Documents\\x/_blank) for more information.

| **Name** | **Time to Live (TTL\*)** | **Record Type** | **Priority** | **Value** |
| --- | --- | --- | --- | --- |
| Blank or @ | 3600 | MX | 1 | ASPMX.L.GOOGLE.COM. |
| Blank or @ | 3600 | MX | 5 | ALT1.ASPMX.L.GOOGLE.COM. |
| Blank or @ | 3600 | MX | 5 | ALT2.ASPMX.L.GOOGLE.COM. |
| Blank or @ | 3600 | MX | 10 | ALT3.ASPMX.L.GOOGLE.COM. |
| Blank or @ | 3600 | MX | 10 | ALT4.ASPMX.L.GOOGLE.COM. |

****Notes****

1. Always create your user accounts before switching MX records to G Suite.

2. The TTL is the number of seconds before subsequent changes to the MX record go into effect. Once the MX records are configured correctly, we recommend changing the TTL value from 3600 to 86400, which tells servers across the Internet to check every 24 hours for updates to the MX record instead of every hour.

3. If you are moving from an existing mail system to G Suite, Google recommends when switching your MX records to Google to keep your existing MX records but set them to a lower priority than the Google mail servers (i.e. assign your existing MX records a priority > 10) until all mail is routing to Google. This ensures no mail is lost.

****Help Center resources****

* [Set up MX records for G Suite Gmail](https://support.google.com/a/answer/140034" \o "Set up MX records for G Suite Gmail" \t "/home/sherwinowen/Documents\\x/_blank)
* [Avoid email bouncing from new MX records](https://support.google.com/a/answer/45679" \o "Avoid email bouncing from new MX records" \t "/home/sherwinowen/Documents\\x/_blank)
* [Troubleshoot MX records](https://support.google.com/a/answer/140038" \o "Troubleshoot MX records" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #3 - Review your DNS Settings with Check MX**

****Introduction****

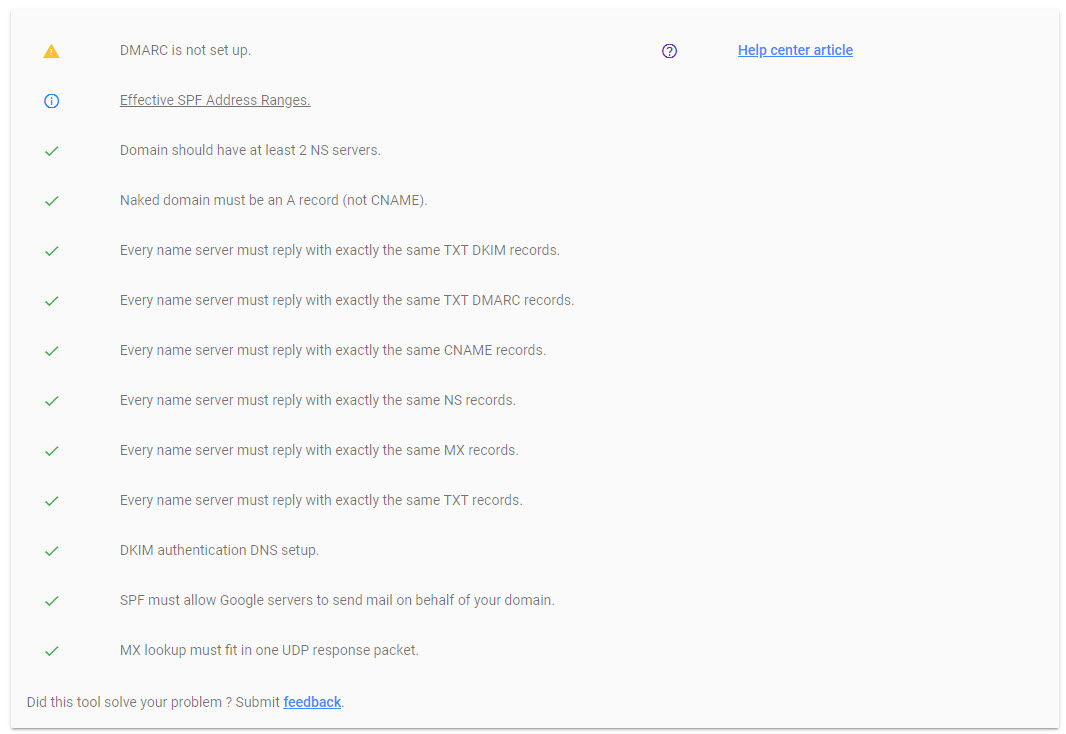
In this exercise you will check the status of your DNS records using the Check MX utility which is provided as part of the G Suite toolbox. Check MX analyses your DNS configuration and makes recommendations for changes where appropriate.

****Directions****

1. Open a new browser tab and visit [https://toolbox.googleapps.com/apps/checkmx/](https://toolbox.googleapps.com/apps/checkmx/" \o "https://toolbox.googleapps.com/apps/checkmx/" \t "/home/sherwinowen/Documents\\x/_blank)

2. Enter the name of your G Suite domain into the 'Domain name' field, and click ****RUN CHECKS!****. After a few seconds, you will see the results displayed.

The image below shows expected results for a new domain that was purchased as part of the sign up flow. Note that exact results can vary depending upon your registrar and existing DNS configuration.



****Help Center resources****

* [G Suite toolbox](https://toolbox.googleapps.com/apps/main/" \o "G Suite toolbox" \t "/home/sherwinowen/Documents\\x/_blank)

**ENHANCING EMAIL SECURITY**

## Introduction to Email Security

There are a number of ways in which you can enhance your email security by ensuring that people who receive email from your company can verify that the email really is from your organization, and that it has not been modified along the way.

In this lesson we will look at three email security measures that are used by G Suite. We recommend that you implement all three for best protection against spoofing and spammers.

In the first exercise you will learn about the **Sender Policy Framework (SPF)**. With an **SPF record you are telling receiving mail servers which domains/servers are allowed to send mail on your behalf**. Messages sent from other sources may be marked as spam.

Next you will implement the **DomainKeys Identified Mail (DKIM)** standard. **This helps prevent email spoofing on outgoing messages by adding an encrypted header to every message sent. Recipient servers decrypt this header using the DKIM record to confirm it's validity.**

Finally, you will learn how to prevent outbound spam messages using a **Domain-based Message Authentication, Reporting, and Conformance** **(DMARC)** policy. **DMARC policies tell email servers how to handle messages that fail SPF/DKIM checks**.

****Important:**** It is assumed that you are using a trial G Suite account and a test domain for this training. If you are using a live/production domain, ****DO NOT**** make any changes to any of your DNS records.

## **Exercise #1 - Authorize Senders with Sender Policy Framework (SPF)**

****Introduction****

**Sender Policy Framework (SPF) is an email security method that helps prevent spammers from sending unauthorized emails from your domain.**

To enable SPF for your domain, a TXT record is added to your DNS configuration. This record tells receiving servers which domains/servers are allowed to send messages on your behalf. Messages sent from servers that aren't in the record might be marked as spam.

Some email servers require SPF so if you don't set up SPF for your domain, messages sent from your domain might bounce or might be marked as spam by some receiving servers.

In this exercise you will review and optionally set your domain's Sender Policy Framework (SPF) record.

****Directions****

1. Sign into your domain registrar. See [Sign into your Domain Registrar](https://www.coursera.org/learn/g-suite-mail-management/supplement/6wpSd/exercise-1-sign-into-your-domain-registrar" \o "Sign into your Domain Registrar" \t "/home/sherwinowen/Documents\\x/_blank).

2. Locate your DNS records.

If you purchased your domain through Google, there should be an existing SPF record as shown in the table below. This specifies that google servers only are allowed to send email on your behalf.

| **Name** | **Record Type** | **Value** |
| --- | --- | --- |
| Blank or @ | TXT | v=spf1 include:\_spf.google.com ~all |

3. If you did not purchase the domain as part of the sign up flow and the domain you are using is for training only, you can add the SPF record as shown above to your DNS records.

4. You can check which IP addresses are covered by \_spf.google.com using the Check MX utility. Simply perform the lookup and then click the ****Effective SPF Address Ranges**** link in the results. Try that now but remember it can take a while for DNS record changes to propagate.

****Notes****

1. Multiple SPF records for a single domain can cause problems so each domain should have only one SPF record. If multiple servers send mail on your behalf, don't create an SPF record for each server. Instead, update one SPF record to include all your mail servers. For example, if you are using an outbound gateway to route mail you would want to include that gateway in your SPF record as below.

v=spf1 ip4:172.16.254.1 include:\_spf.google.com ~all (where 172.16.251.1 is the IP address of the gateway)

2. Your new SPF record takes effect within 48 hours.

****Help Center resources****

* [Authorize email senders with SPF](https://support.google.com/a/answer/33786" \o "Authorize email senders with SPF" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #2 - Authenticate with DomainKeys Identified Mail (DKIM)**

****Introduction****

DomainKeys Identified Mail (DKIM) is an email security method that helps prevent email spoofing on outgoing messages. This is where email content is changed to make the message appear from someone or somewhere other than the actual source.

DKIM adds an encrypted signature to the header of all outgoing messages. Email servers that get these messages use DKIM to decrypt the message header, and verify the message was not changed after it was sent.

Like SPF, some servers require a DKIM signature. We recommend you use your own DKIM key but if you don't Gmail will sign all outgoing messages with this default DKIM domain key: d=\*.gappssmtp.com.

Like SPF records discussed in the previous exercise, if you purchased your domain as part of the sign up flow, Google should have also added a DKIM entry to your DNS records.

In this exercise, you will review your domain's DKIM status in the admin console and check (and optionally update) your DNS records.

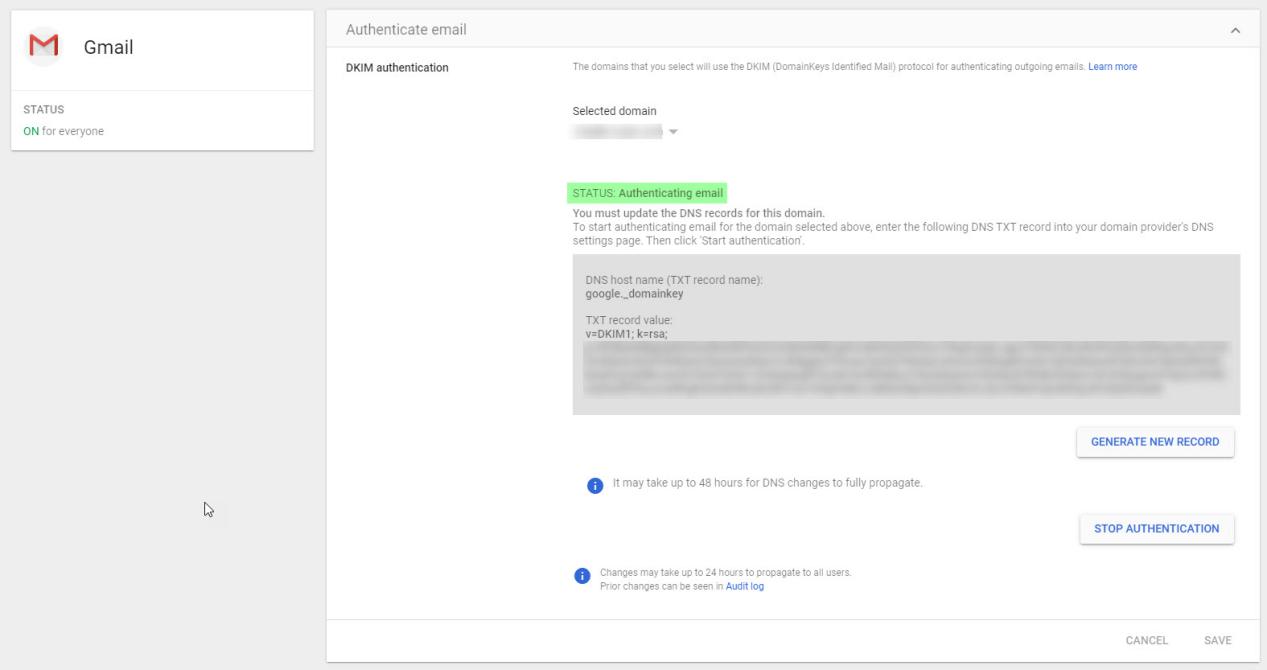
****Directions****

1. If you are not already signed in, sign in to your domain as the administrator at [admin.google.com](https://admin.google.com/" \t "/home/sherwinowen/Documents\\x/_blank).

2. Click the ****Apps**** icon, click the ****G Suite**** icon and then click the ****Gmail****service.

3. Click ****Authenticate email,****and check that STATUS is 'Authenticating email'

Note that it can take between 24 and 72 hours for DKIM to become fully activated so if you did purchase your domain through Google but mail is still not authenticating, you should wait for the process to complete.



4. Do not close the page above. Open up a new browser tab and sign into your domain registrar. See [Sign into your Domain Registrar](https://www.coursera.org/learn/g-suite-mail-management/supplement/6wpSd/exercise-1-sign-into-your-domain-registrar" \o "Sign into your Domain Registrar" \t "/home/sherwinowen/Documents\\x/_blank).

If you purchased your domain through Google

5. Locate your google.\_domainkey TXT record in your DNS records. It should match the one shown in the admin console.

If you brought your own domain to G Suite (and you wish to enable DKIM now)

6. From the admin console, click ****GENERATE NEW RECORD,****then click ****GENERATE**** in the resulting dialog box.

7. Add a new DNS record as below. The values in the 'Name' and 'Value' columns below are examples only. You should copy your values from the admin console 'TXT record name' and 'TXT record value' fields.

| **Name** | **Record Type** | **Value** |
| --- | --- | --- |
| google.\_domainkey | TXT | v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgK AQEAmGZaz9puH3hrlRsavms9CQtdajO6tqPLJ6ZgJlF464uYKnDKETK3u 6iCx6246Leopqe/SKAeO48gXOWFmie2U1qrF34vrQIbc73nlfgd6BlJ0v Jm6VrfwpRc1E0qZWu1GPzlkMm8vjnTjZegvbREBnsNTsUOT5Vpe9AyBU7 P3tpG101QdZwN4JESye4x9a7ZQQviNt07mHlYemLrtUz3vTtJ8azBkCC9 bYn+xYed2eqDEEzhZn/mxgdoaQ1mWQ50+asUTCCwZL9Vys3arbp4AxDNx |

8. Return the admin console and click ****START AUTHENTICATION****. When you turn on email signing, Gmail verifies you have a DKIM domain key. If the DKIM domain key is not found, G Suite displays a warning message so you should try again later.

****Notes****

1. DNS TXT records can have up to 255 characters in a single string. For TXT records over 255 characters, DNS chains multiple text strings together into a single record. If your domain host (registrar) limits TXT records to 255 characters, you should contact them to find out what steps are required to update your DNS records with the domain key.

****Help Center resources****

* [Set up DKIM to prevent email spoofing](https://support.google.com/a/answer/174124" \o "Set up DKIM to prevent email spoofing" \t "/home/sherwinowen/Documents\\x/_blank)
* [Generate a DKIM key for your domain](https://support.google.com/a/answer/174126" \o "Generate a DKIM key for your domain" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #3 - Manage Spam with Domain-based Message Authentication, Reporting, and Conformance (DMARC)**

****Introduction****

Gmail supports Domain-based Message Authentication, Reporting, and Conformance (DMARC) as a way to protect you from spammers forging the From address in an email to make it appear that it came from someone in your organization. Use DMARC to define how a mail server should handle messages that appear to be sent from your domain but that are actually spam.

DMARC helps email senders and receivers verify incoming messages by authenticating the sender's domain. DMARC also defines the action to take on suspicious incoming messages.

Before configuring DMARC you should set up SPF and DKIM. DMARC uses SPF and DKIM to verify that messages are authentic. Messages that do not pass SPF or DKIM can trigger your DMARC policy.

When a message triggers your DMARC policy you have three ways to handle the message:

* Take no action on the message and log it in a daily report.
* Mark the message as spam.
* Tell the receiving server to reject the message. This also causes an SMTP bounce to the sender.

We recommend you start with the first option (take no action) then monitor and analyse the results by checking your daily reports. Once you are happy you can change the policy to 'quarantine' or 'reject'.

In this exercise you will enable DMARC for your G Suite account.

****Directions****

1. Sign into your domain registrar. See [Sign into your Domain Registrar](https://www.coursera.org/learn/g-suite-mail-management/supplement/6wpSd/exercise-1-sign-into-your-domain-registrar" \o "Sign into your Domain Registrar" \t "/home/sherwinowen/Documents\\x/_blank).

2. Locate your DNS records and add a DMARC TXT record as shown below. Replace yourdomain with your G Suite primary domain name, and admin-email with your administrator's email address. Tip: If you are using Google Domains, add your DMARC TXT record as a 'Custom resource record'.

| **Name** | **Record Type** | **Value** |
| --- | --- | --- |
| \_dmarc.yourdomain | TXT | v=DMARC1; p=none; rua=mailto:admin-email |

The TXT record you added above tells receiving servers what to do if DMARC is triggered. Here, no action is taken on the message and a daily report is mailed to you as the G Suite administrator.

Now that you have configured SPF, DKIM and DMARC here is what happens when a mail is sent from someone in your organization:

i. Recipient server looks up the SPF record and confirms that the sending server matches one in your allowed list.

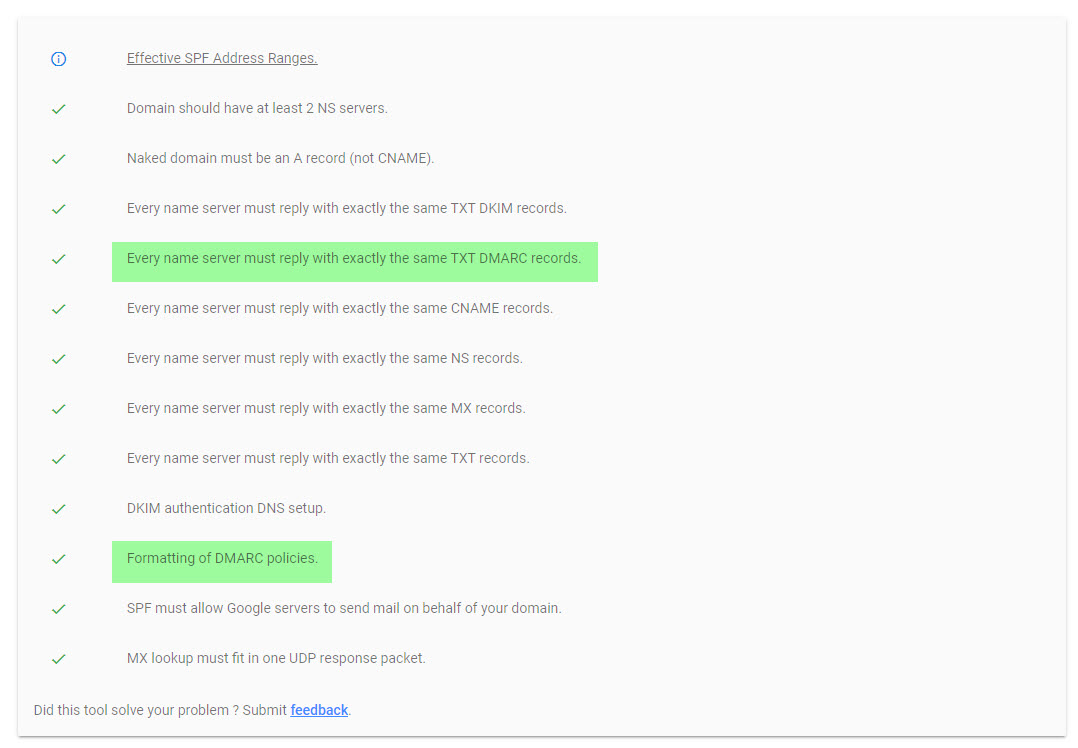
ii. Recipient server checks the DKIM signature in the message header using the DKIM key in your DNS configuration.

iii. If the above checks pass, the recipient server delivers the message, otherwise the server follows the policy defined in your DMARC record and emails a daily report.

It takes a while for your DNS changes to propagate but let's see if those changes are visible yet to the Check MX tool.

3. Open a new browser tab and visit [https://toolbox.googleapps.com/apps/checkmx/](https://toolbox.googleapps.com/apps/checkmx/" \o "https://toolbox.googleapps.com/apps/checkmx/" \t "/home/sherwinowen/Documents\\x/_blank)

4. Enter the name of your G Suite domain into the 'Domain name' field, and click ****RUN CHECKS!****. If your changes are visible, you should see the two lines highlighted below in your query results. Don't worry if you do not see the changes yet, It can take a while.



Congratulations you have successfully configured email security for your organization.

****Help Center resources****

* [About DMARC](https://support.google.com/a/answer/2466580" \o "About DMARC" \t "/home/sherwinowen/Documents\\x/_blank)
* [Turn on DMARC](https://support.google.com/a/answer/2466563" \o "Turn on DMARC" \t "/home/sherwinowen/Documents\\x/_blank)

**EMAIL SAFETY AND END USER ACCESS**

## **Introduction to Email Safety and End User Access**

In the previous lesson you saw how you can improve the security of your outbound messages by implementing SPF, DKIM, and then DMARC. Together these features allow recipient mail servers to check the messages they receive were actually sent from your organization and have not been tampered with in transit.

In this lesson we will look at how you can protect your users from **inbound phishing and harmful software (malware).** There are a number of different types of threats to your users. For example, a message may contain a harmful attachment or a link to an untrusted domain. Using Google's advanced phishing and malware protection options you can choose what actions to take when a phishing mail or malware is detected.

You will also explore the end user access features available to your users, which include:

* **POP/IMAP access** - allow users to connect desktop apps to Gmail
* **G Suite Sync for Microsoft Outlook** - allow users to work with Gmail from Microsoft Outlook
* **Gmail offline access**

## **Exercise #1 - Configure Email Safety**

****Introduction****

Gmail will always display warnings, and move messages known to be untrustworthy to spam. In addition however as the G Suite administrator Gmail provides additional controls which allow you to determine actions taken when certain threats are found. In this exercise we will explore those controls.

****Directions****

1. If you are not already signed in, sign in to your domain as the administrator at [admin.google.com](https://admin.google.com/" \t "/home/sherwinowen/Documents\\x/_blank).

2. Click the ****Apps**** icon, click the ****G Suite**** icon and then click the ****Gmail****service.

3. Click ****Safety****.

This will take you to the Safety page which is divided into three sections:

* Attachments: Policies to protect against malware.
* Links and external images: Prevent email phishing attacks.
* Spoofing and authentication: Reduce phishing due to spoofing and unauthenticated emails.

4. Click on the ****Attachments**** card. From here you can see the protections available to you and you can enable/disable them as required. You can also see the default action when a setting is enabled.

5. If it is not already enabled, check 'Protect against encrypted attachments from untrusted senders'. Now you can choose an action to take on messages that trigger this policy. You can:

* Keep email in inbox and show warning (default)
* Move email to spam
* Quarantine

If you choose to quarantine the message you will be able to select which quarantine to use. We will discuss email quarantine later in this course.

6. Choose a desired option and click ****SAVE****.

Explore the other settings in this section and also click on each of the other two cards and review the settings that are available. Note that there are links on this page which take you to the security dashboard from where you can view affected emails. See [About the security dashboard](https://support.google.com/a/answer/7492330" \o "About the security dashboard" \t "/home/sherwinowen/Documents\\x/_blank) for more details. In each section there is also an option which allows you to opt-in to any new recommendations automatically. We recommend you enable these settings to offer best protection for your users.

****Notes****

1. These advanced security features work independently of other spam settings you might have previously turned on. For example, even if you've listed a domain as a safe sender in spam settings, the enhanced security features are still applied.

2. When you select the Quarantine option for any of the advanced security settings, the quarantine you select applies only to incoming messages. This is true even if the quarantine you select specifies actions to take on outgoing messages.

## **Exercise #2 - Configure End User Access**

****Introduction****

In this exercise you will check and configure end user access to Gmail as per company policy. You will also explore the other settings available that control end user access.

****Scenario****

Your company has a strong focus on the confidentiality of their corporate information. Sam, the CEO has become aware that it is common practice for contractor staff to use their own personal email accounts to conduct business. Some contractors have created a Gmail filter which forwards all mail received to their personal account and Sam would like to stop this practice. You receive the following email from Alex Bell.

Hey G Suite Admin,

As you know we are working on a very confidential widget at the moment. To reduce the risks of leaks can you please stop the practice where contractors are auto-forwarding all company mail to their personal account.

Can you also check that we have disabled the use of POP and IMAP with Gmail. We want to ensure that with the exception of those users who are allowed to use G Suite Sync, all other users access Gmail using the web interface only.

Thanks,

Alex Bell, IT Manager

****Directions****

1. If you are not already signed in, sign in to your domain as the administrator at[admin.google.com](https://admin.google.com/" \t "/home/sherwinowen/Documents\\x/_blank).

2. Click the ****Apps**** icon, click the ****G Suite**** icon and then click the ****Gmail****service.

3. Click ****End User Access****. You may need to scroll down to see this section.

4. Click on your top level organization on the left and ensure that 'POP and IMAP access' is disabled. Note: The value for 'Disable POP and IMAP access for all users' should be set to ON.

5. If you made changes, click ****SAVE.****

6. Click the ****Contractors**** OU.

7. Click on the Automatic forwarding row and ensure Allow users to forward incoming email automatically to another address box is set to OFF. Any existing forwarding rules will now stop working.

8. Click ****OVERRIDE**** (you are overriding the inherited setting from the top level organization).

Before we move on, let's explore the settings on this particular page in a little more detail.

**POP and IMAP access**

In addition to accessing G Suite mail from the Gmail web interface, users can send and receive mail from their favorite desktop client. Depending on the client, they can use either Internet Message Access Protocol (IMAP) or Post Office Protocol (POP). With POP the client contacts the mail server, downloads the mail and then deletes it from the server. When using IMAP messages aren't downloaded until you click on a message, and attachments aren't automatically downloaded. This makes it suitable when users have multiple devices but are not using the native Gmail web interface.

If you disable POP and IMAP access, your users will not be able to access POP and IMAP settings in the Gmail interface and users cannot access their mail via POP or IMAP even if they originally had it on.

**G Suite Sync**

G Suite Sync for Microsoft Outlook (GSSMO) is a plugin for Outlook that provides email, calendar and contacts synchronization with G Suite. GSSMO uses the G Suite APIs to synchronize data. It can be installed by an individual user and it is also available as an enterprise installer.

**Automatic Forwarding**

By default, users can set up a rule or filter which will forward incoming messages to another address. In this section you have the option of disabling this feature. If you disable this feature any existing forwarding rules/filters will stop working and users will no longer see the option in their Gmail settings.

**Image URL proxy whitelist**

When a user opens a message Gmail uses Google’s secure proxy servers to serve images included in these messages. This protects you against image-based security vulnerabilities. The potential downside is that images that are dependent on internal IPs and sometimes cookies are broken. To fix broken images and cookies you can create a whitelist to bypass the Google proxy servers. However, Google strongly recommends against the use of the Image URL proxy whitelist as this can leave your users vulnerable to malicious attack.

Unlike the other settings described here which can be applied at the OU level, this setting applies to the entire organization.

**Allow per-user outbound gateways**

Gmail offers users the option to associate additional email addresses with their accounts to create custom From addresses. For example, user@yourdomain might also have an email account user@partnerdomain. When the user sends or responds to a message from Gmail, they want to be able to choose which email address appears in the From field. By default the Gmail servers will deliver all mail regardless of the From address. Some reasons why you may want to allow per-user outbound gateways are:

* Using an outbound gateway ensures that the same mail server delivers all messages from partnerdomain, regardless of whether it was composed in Gmail or another email client application.
* Recipients can verify that the message is valid by confirming that it comes from the proper mail server for partnerdomain.
* The partnerdomain mail server has a record of the mail sent from its domain using Gmail.
* Using an outbound gateway can also prevent the appearance of "on behalf of" addresses in the From field. When a user sends a message from an alternate From address through the G Suite mail servers, some recipient mail applications display the name of the sender as user@partnerdomain on behalf of user@yourdomain.

One disadvantage is:

* Mail sent from the partnerdomain is not handled by the G Suite mail servers or your domain's outbound gateway, which can be what you want.

**Unintended external reply warning**

Gmail detects if an external recipient in an email response is not someone a user interacts with regularly, or is not present in a user’s Contacts. When this setting is enabled, the user receives a warning when they send the message.

****Help Center resources****

* [Turn POP and IMAP on and off for users](https://support.google.com/a/answer/105694" \o "Turn POP and IMAP on and off for users" \t "/home/sherwinowen/Documents\\x/_blank)
* [Set up an image URL proxy whitelist](https://support.google.com/a/answer/3299041" \o "Set up an image URL proxy whitelist" \t "/home/sherwinowen/Documents\\x/_blank)
* [Work offline in Gmail](https://support.google.com/a/answer/7684186" \o "Work offline in Gmail" \t "/home/sherwinowen/Documents\\x/_blank)

**PREVENTION OF SPAM, PHISHING AND MALWARE**

## **Introduction to Prevention of Spam, Phishing and Malware**

All mail sent to your users is subject to Google's spam filters. By default, messages that are identified as spam are delivered to the user's Gmail spam folder. Spam messages are automatically deleted from the spam folder after 30 days.

As the administrator, you can customize how spam is managed in a number of ways. For example, you can:

* Be more aggressive, for strict filtering of email. (although this may result in valid messages being identified as spam)
* Bypass internal mail
* Use approved sender lists

In this lesson you will explore the advanced spam, phishing and malware controls available to you in the admin console.

## **Exercise #1 - Create an Email Whitelist and Blacklist**

****Introduction****

If you notice that legitimate emails from specific contacts are being incorrectly marked as spam, you can whitelist the contact's IP address. After you whitelist an IP address, messages originating from the whitelisted address are no longer marked as spam.

A blacklist is a list of email addresses you block from sending mail to your domain. Administrators can block domains or specific users.

In this exercise, you will create an email whitelist for your organization. You will also create a blocked senders list (blacklist) and test the results when a user in that list tries to send a message to you.

****Directions****

1. If you are not already signed in, sign in to your domain as the administrator at [admin.google.com](https://admin.google.com/" \t "/home/sherwinowen/Documents\\x/_blank).

2. Click the ****Apps**** icon, click the ****G Suite**** icon and then click the ****Gmail****service.

3. Scroll down and click ****Advanced settings****.

Create a whitelist

4. Locate the 'Spam, phishing, and malware' section and enter the following IP address into the 'Email whitelist' field:

* 172.217.25.142

If you want to add more IP addresses, separate entries with a comma.

5. Click ****SAVE****.

Messages originating from 172.217.25.142 should no longer be marked as spam. Please note though that Gmail will still mark as spam any message which it deems to be a blatant spam, phishing or malware message even if the sender's IP is listed in the email whitelist.

Create a blacklist

6. Before we create the blacklist, send a message from an external account to your super administrators email address. Then open your inbox and confirm that you have received the message. Next we will blacklist the user that just sent the message.

7. Hover over the 'Blocked senders' row and click ****CONFIGURE****.

8. Enter a short description, for example Block me.

9. We must now create a list to use for this setting. Click ****Use existing or create a new one****.

10. Enter a name for the list Blocked senders, and click ****CREATE****.

11. Once the list appears in the dialog box, hover the list name, and click ****Edit****. You can now manage the list.

12. Initially the list is empty. Click ****Add**** to add a list entry.

13. Enter the email address of your external account and click ****SAVE****. Note: In addition to user email addresses you can also enter domain names here.

14. Click ****ADD SETTING**** and click ****SAVE****.

15. Repeat Step 6. This time the message should be blocked and the sender will receive a message advising that the message could not be delivered.

16. Hover over your blocked sender setting. Note the options on the right. You can edit, disable, copy or delete it. You can also add a new setting. Click ****DELETE****and click ****SAVE****.

****Notes****

1. If you want to whitelist email addresses or domains, you should create an approved senders list. We will do that in the next exercise.

2. If you are forwarding mail to Gmail from another mail system (perhaps you are in the process of migrating users onto G Suite) you should not add your legacy server's IP address(es) to the email whitelist. Add the address(es) to the inbound gateway section instead. We will discuss the inbound gateway later in this lesson.

****Help Center resources****

* [Whitelist IP addresses in Gmail](https://support.google.com/a/answer/60751" \o "Whitelist IP addresses in Gmail" \t "/home/sherwinowen/Documents\\x/_blank)
* [Block specific senders based on email address or domain](https://support.google.com/a/answer/2364632" \o "Block specific senders based on email address or domain" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #2 - Create an Approved Sender List**

****Introduction****

In the previous exercise, you added a sender's public IP address to the email whitelist for Gmail to avoid messages from that sender from being marked as spam. In this exercise you will learn how to create an approved sender list for your organization.

The key difference between an email whitelist and approved sender list is that you can add email addresses and domain names to an approved sender list where the whitelist uses IP addresses only.

****Directions****

1. If you are not already signed in, sign in to your domain as the administrator at [admin.google.com](https://admin.google.com/" \t "/home/sherwinowen/Documents\\x/_blank).

2. Click the ****Apps**** icon, click the ****G Suite**** icon and then click the ****Gmail****service.

3. Scroll down and click ****Advanced settings****.

4. Locate the 'Spam, phishing, and malware' section.

5. Hover over the 'Spam' row and click ****CONFIGURE****.

6. Enter a short description, for example Approved senders.

The Spam setting provides the following options. You can enable any or all of them:

* Be more aggressive when filtering spam: The default is disabled. If you enable this option, it's likely that more messages will be marked spam and sent to your users' spam folders.
* Bypass spam filters for messages received from internal senders: Internal mail is not checked for spam.
* Bypass spam filters for messages received from addresses or domains within these approved senders lists: We will be using this option here.
* Put spam in administrative quarantine: If you select this option, spam messages are never directed to users' spam folders.

7. Check the 'Bypass spam filters for messages received from addresses or domains within these approved senders lists' box and click the ****Use existing or create a new one**** link.

8. Enter a name for the list Approved senders, and click ****CREATE****.

9. Once the list appears in the dialog box, hover the list name, and click ****Edit****. You can now manage the list.

10. Initially the list is empty. Click ****Add**** to add a list entry.

11. Enter one or more domain names or user email addresses external to your organization that you trust and click ****SAVE****. Separate multiple values with a comma or space.

12. Click ****ADD SETTING**** and click ****SAVE****.

You have just successfully created an approved sender list for your organization.

****Notes****

1. Sender authentication protects you from spoofed email; namely, email that appears to be from a valid sender but really isn’t. By default, sender authentication is enabled for new entries in an address list. Without sender authentication (where DMARC checks fail), Gmail has no way of knowing if the message was really sent by the person it claims to have come from. Because of this, a sender is only considered to match your address list if their mail is authenticated. Although you can do it, Google strongly recommends that you not turn off sender authentication.

2. In addition to being able to configure a spam setting that tells Gmail to be more aggressive when filtering spam, Gmail also provides the option for enhanced pre-delivery message scanning. See [Use enhanced pre-delivery message scanning](https://support.google.com/a/answer/7380368" \o "Use enhanced pre-delivery message scanning" \t "/home/sherwinowen/Documents\\x/_blank) for more details.

****Help Center resources****

* [Customize spam filter settings](https://support.google.com/a/answer/2368132" \o "Customize spam filter settings" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #3 - Security Sandbox**

****Introduction****

As an administrator, you can set up Gmail to scan (or run) all email attachments, including those sent from inside your domain and from external domains prior to delivery. Alternatively, you can create specific rules for attachment scanning.

Scanning takes place in a virtual environment called the security sandbox. Attachments identified as threats are by default placed into the recipient's spam folder.

In this exercise you will ensure that scanning of all emails is disabled and then create a sandbox rule to examine mail from a single domain only.

Note: If you enable scanning of all email attachments, this overrides any individual rules that you define.

****Scenario****

One of your users devices was recently infected by a virus and your investigations have determined that the virus may have come from a malicious attachment in an email sent from acme.com.

You are not sure if this was the source of the problem and you also do receive legitimate emails from acme.com so you do not want to blacklist them. Instead you have decided to create a sandbox rule that will examine all emails sent to your organization by acme.com.

****Directions****

1. If you are not already signed in, sign in to your domain as the administrator at [admin.google.com](https://admin.google.com/" \t "/home/sherwinowen/Documents\\x/_blank).

2. Click the ****Apps**** icon, click the ****G Suite**** icon and then click the ****Gmail****service.

3. Scroll down and click ****Advanced settings****.

4. Locate the 'Spam, phishing, and malware' section.

Disable scanning of all attachments

5. Hover over the 'Security sandbox' row and ensure 'Enable virtual execution of attachments in a sandbox environment for all the users of the Organizational Unit for protection against malware, ransomware, and zero-day threats.' is deselected. If it is selected, deselect it, and click ****SAVE****.

Now create a sandbox rule for acme.com

6. Hover over the 'Security sandbox rules' row and click ****CONFIGURE****.

7. Enter a short description, for example Check acme.com.

8. In 'Email messages to affect', check Inbound.

We can leave Internal - receiving unchecked as we are only interested in messages from the external domain acme.com.

9. Click the ****Add****link in the 'Expressions' box.

You can now choose between the following types of expressions to look for:

* Simple content match: Look in the entire message for a string value. This works just like any normal web search
* Advanced content match: Here you choose which parts of the message to examine and how to perform the search.
* Metadata match: Search on metadata items such as IP address, message size, etc.
* Predefined content match. Here you can choose to apply a predefined Data Loss Prevention (DLP) rule. For example, you might want to scan messages that contain credit card numbers only.

10. Change the 'Expression type' from Simple content match to Advanced content match.

11. Set 'Location' to Sender header.

12. Set 'Match type' to Contains text.

13. Enter acme.com into the 'Content' field and click ****SAVE****.

14. Click ****ADD SETTING**** and click ****SAVE****.

All messages received from acme.com will now be processed by the security sandbox.

****Notes****

1. Security sandbox scans run independently of other compliance and pre-delivery scans. For example, your content compliance scans might look for personal information such as credit card numbers. Or attachment compliance scans might block attachments of a specific type or size. Gmail runs those compliance and pre-delivery scans regardless of any security sandbox scans.

2. Email attachments that are blocked by compliance rules and pre-delivery scans aren't scanned by the security sandbox.

3. Malware detected by the security sandbox is put in the spam folder by default. To quarantine malware attachments, you can create a content compliance rule using the spam metadata attribute.

****Help Center resources****

* [Set up rules to detect harmful attachments](https://support.google.com/a/answer/7676854" \o "Set up rules to detect harmful attachments" \t "/home/sherwinowen/Documents\\x/_blank)

## **Inbound Gateway**

In most cases, mail destined for your organization will go straight to Google for delivery and as such you will configure your DNS MX records to point to the Google servers. In some cases however, you may need to use an inbound gateway. The gateway typically processes the mail in some way before passing it onto Google for delivery to Gmail. Common use cases for an inbound gateway are:

* Message archiving
* Spam filtering
* During migration to G Suite where you have some users on a legacy mail server and some on Gmail

When you use an inbound gateway, you point your MX records to the inbound mail gateway server, and configure the gateway server to deliver messages to Gmail servers.

It's important if you are using an inbound gateway that you add the details to the 'Inbound gateway' setting on the Gmail Advanced settings page. Google will allow a high volume of traffic from the gateway and SPF checks are more accurate as these are made against the server that sent the message to your legacy server.

When configuring an inbound gateway, you can optionally

* Reject mail that wasn’t sent from the gateway
* Configure how to handle spam based on gateway message tags.

The latter is useful if your gateway server adds a header to spam messages before it passes the email to Gmail. You can identify inbound spam messages using the header and optionally disable most of the Gmail spam filters for messages entering via the gateway.

****Help Center resources****

Even if you do not use an inbound gateway, review the following article to gain an understanding of its purpose.

* [Set up an inbound mail gateway](https://support.google.com/a/answer/60730" \o "Set up an inbound mail gateway" \t "/home/sherwinowen/Documents\\x/_blank)

**COMPLIANCE**

## **Introduction to Compliance**

As the administrator, you can set up rules to handle messages that contain content that matches one or more expressions. For example, you can:

* Reject outbound messages that might contain sensitive company information, such as when your outbound filter detects the word “confidential.”
* Route messages with content that matches specific text strings or patterns to your legal department.

A compliance rule can scan messages for:

* ****Attachment compliance****: attachments of certain types
* ****Content compliance****: search for text content
* ****Objectionable content:****identify messages that contain words in a custom word lists that you define

Content compliance rules also allow the option of applying a predefined content match using a **Data Loss Prevention (DLP)** template. DLP lets you use predefined content detectors when scanning inbound or outbound email. Google specifically designed these detectors to locate sensitive data, such as credit card, social security, or passport numbers. Predefined detectors are available for many common U.S. and international data types.

When a message matches a compliance rule, you can:

* Reject it
* Quarantine it
* Deliver it with modifications

In an earlier course you configured a compliance footer for outbound mail and created an attachment compliance rule to prevent users from receiving video, multimedia and music attachments from external users. See [Configure Compliance Policies](https://www.coursera.org/learn/managing-g-suite/supplement/0X5I2/exercise-4-configure-compliance-policies" \o "Configure Compliance Policies" \t "/home/sherwinowen/Documents\\x/_blank) for more details. In this lesson you will create a content compliance and objectionable content rule.

You will be able to identify the differences between the three rule types and what options to apply to meet specific business needs.

## **Exercise #1 - Create a Content Compliance Rule**

****Introduction****

This exercise is in two parts. In the first part you will create a content compliance rule based upon message content. In the second part you will explore the predefined DLP templates that are offered as part of a content compliance rule.

****Scenario****

Your company is considering the purchase of another company but wants to keep discussions confidential and prevent leaks. The discussions are known internally as Project Jupiter. You receive the following email from Alex Bell.

Hey G Suite Admin,

The executive has asked if G Suite can prevent messages from leaving the organization if they contain references to Project Jupiter unless they are sent by an executive member.

Any message discussing this project from anyone outside of the executive should be redirected to Sam.

Can you make this happen?

Thanks,

Alex Bell, IT Manager

****Directions****

Part 1: Create and test a content compliance rule

1. If you are not already signed in, sign in to your domain as the administrator at [admin.google.com](https://admin.google.com/" \t "/home/sherwinowen/Documents\\x/_blank).

2. Click the ****Apps**** icon, click the ****G Suite**** icon and then click the ****Gmail****service.

3. Scroll down and click ****Advanced settings****.

4. Scroll down to the 'Compliance' section and hover over the 'Content compliance' row, then click ****CONFIGURE****. The 'Content compliance' dialog box displays.

5. Enter a short description that will appear within the settings summary, such as Secure Project Jupiter.

6. In the 'Email messages to affect' section, check the Outbound box.

7. Click the ****Add****link in the 'Expressions' box.

8. Change the 'Expression type' from Simple content match to Advanced content match.

9. Set 'Location' to Body.

10. Set 'Match type' to Contains text.

11. Enter jupiter into the 'Content' field and click ****SAVE****.

12. Click ****Add**** to add another expression.

13. Change the 'Expression type' from Simple content match to Advanced content match.

14. Set 'Location' to Subject.

15. Set 'Match type' to Contains text.

16. Enter jupiter into the 'Content' field and click ****SAVE****.

17. In the next section 'If the above expressions match, do the following', set the action to Modify message.

18. Scroll down and check the Change envelope recipient box.

19. Enter samantha.morse@yourdomain into the first option 'Replace recipient' .

20. Scroll down and click the ****Show options**** link.

21. Check the Use address lists to bypass or control application of this setting box and ensure Bypass this setting for specific addresses / domains is selected.

22. Click the ****Use existing or create a new one**** link to create a new list. This will be the executive members who are allowed to discuss project Jupiter so are excluded from this rule.

23. Enter a name for the list Executive, and click ****CREATE****.

24. Once the list appears in the dialog box, hover the list name, and click ****Edit****. You can now manage the list.

25. Initially the list is empty. Click ****Add**** to add a list entry.

26. Enter the following email addresses and click ****SAVE****. Separate each email address with a comma or space.

* samantha.morse@yourdomain
* lars.ericsson@yourdomain
* timothy.lee@yourdomain

27. Click ****ADD SETTING**** and click ****SAVE****.

You have now successfully added a compliance rule. It will trigger if anyone in your organization (except Sam, Timothy, or Lars) sends an email externally with the word Jupiter in the subject line or the body of the message. The message will not be delivered. Instead it will be re-routed to Sam's inbox.

Let's test that it works!

28. Send an email from your admin account to an external address with the word Jupiter into the subject or body of the message.

Does the intended recipient receive the email? They should not because you are not allowed to discuss project Jupiter externally.

29. Sign out and sign back in to G Suite at [mail.google.com](https://mail.google.com/" \o "mail.google.com" \t "/home/sherwinowen/Documents\\x/_blank) as samantha.morse@yourdomain. The message you sent should appear in her inbox. Open the message. Note that she can still see the intended recipient in the "To" field as well as who sent the message.

30. As Sam, send a message with Jupiter in the subject or body to an external address.

Does the intended recipient receive the email? They should because Sam is allowed to send messages about Jupiter externally.

Part 2: Explore the DLP rules for Gmail

In this part you do not need to create a new rule but complete the steps below so that you are familiar with the types of predefined rules available to you for use as part of your DLP policies.

31. Hover over the 'Content compliance' row, then click ****ADD ANOTHER****. The 'Content compliance' dialog box displays.

32. Click the ****Add**** link in the 'Expressions' box.

33. Change the 'Expression type' from Simple content match to Predefined content match.

34. Click on ****Please select a predefined content**** line to reveal the list of DLP rules to choose from.

35. Select any predefined match from the list. Note how you can also specify a match frequency. This tells Gmail how many times a match must be found in a message before the rule is triggered.

36. Click ****CANCEL****, then click ****CANCEL**** again.

****Help Center resources****

* [Set up rules for content compliance](https://support.google.com/a/answer/1346934" \o "Set up rules for content compliance" \t "/home/sherwinowen/Documents\\x/_blank)
* [Scan your email traffic using DLP rules](https://support.google.com/a/answer/6280516" \o "Scan your email traffic using DLP rules" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #2 - Create an Objectionable Content Rule**

****Introduction****

In the previous exercise you created a content compliance rule that used an advanced content match to search different parts of a message for a text string. In this exercise, you will create an objectionable content rule. Unlike content compliance rules, this type of rule matches messages based upon 'word lists' that you define.

****Directions****

1. If you are not already signed in, sign in to your domain as the administrator at[admin.google.com](https://admin.google.com/" \t "/home/sherwinowen/Documents\\x/_blank).

2. Click the ****Apps**** icon, click the ****G Suite**** icon and then click the ****Gmail****service.

3. Scroll down and click ****Advanced settings****.

4. Scroll down to the 'Compliance' section and hover over the 'Objectionable content' row, then click ****CONFIGURE****. The 'Objectionable content' dialog box displays.

5. Enter a short description that will appear within the settings summary, such as Looking for bad words.

6. In the 'Email messages to affect' section, check the Outbound and Internal - sending boxes.

7. In the 'Add words you want to search for in each message', click the ****Edit**** link.

8. Click ****Add****link in the 'Custom objectionable words' box.

9. Enter one or more words separated by commas or spaces and click ****SAVE****.

10. In the next section 'If the message contains the above words, do the following', set the action to Quarantine message.

Under normal circumstances you might choose a different action such as redirecting the message to HR or perhaps just rejecting the message and notify the sender that the message was rejected. For the purposes of this exercise however, we wanted to introduce you to the admin quarantine so we will send any message detected by this rule there instead.

11. Click ****ADD SETTING**** and click ****SAVE****.

12. Sign out and sign back in to G Suite at [mail.google.com](https://mail.google.com/" \o "mail.google.com" \t "/home/sherwinowen/Documents\\x/_blank) as timothy.lee@yourdomain. Send a message to another user in your organization with one of the objectionable words in the body of the message.

13. Sign out and sign back in as the administrator at[admin.google.com](https://admin.google.com/" \t "/home/sherwinowen/Documents\\x/_blank).

14. Click the ****Apps**** icon, click the ****G Suite**** icon and then click the ****Gmail**** service.

15. Scroll down and click ****Manage quarantines****, then click ****GO TO ADMIN QUARANTINE****. This will launch the admin quarantine in a new tab. You can also navigate to the quarantine using the following link: [https://email-quarantine.google.com/adminreview](https://email-quarantine.google.com/adminreview" \o "https://email-quarantine.google.com/adminreview" \t "/home/sherwinowen/Documents\\x/_blank).

You should see the message that Timothy sent in Step 12 in the quarantine.

16. Click on the message and explore the options.

From here you can see:

* the message header
* the message (the offending word(s) should also be highlighted)
* which rule placed the message into the quarantine
* the source of the message using the SHOW ORIGINAL button.

You can now choose to allow the message to be delivered or deny it using one of the buttons provided.

17. Click ****DENY****, then click ****Denied**** on the left side of the screen. You will see the message has been moved to this view. Note: If a message isn't allowed or denied within 30 days of it being quarantined it’s automatically deleted from the quarantine.

****Help Center resources****

* [Set up rules for objectionable content](https://support.google.com/a/answer/1346936" \o "Set up rules for objectionable content" \t "/home/sherwinowen/Documents\\x/_blank)
* [Set up and manage email quarantines](https://support.google.com/a/answer/6104172" \o "Set up and manage email quarantines" \t "/home/sherwinowen/Documents\\x/_blank)

## **Other Compliance Controls**

We have just looked at compliance rules which scan messages and when certain conditions are met the rule is triggered and actions are taken on the message which include **rejecting the message**, **modifying it (perhaps by redirecting it to another recipient)** and or **putting the message into quarantine**.

In addition to rules, there are a number of other compliance controls available to you as the G Suite administrator. It's important that you understand the features available so the common controls are discussed briefly below.

****Email and chat auto-deletion****

This control allows you to automatically delete email and chat messages that are older than a number of days that you specify. You can optionally ignore messages that have specific labels applied.

Note: If you need auto-deletion for all accounts regardless of account activity, such as for legal and compliance purposes, use Google Vault instead.

****Optical Character Recognition (OCR) for email attachments****

OCR is a technology that extracts text from images. It scans GIF, JPG, PNG, and TIFF images. If you turn it on, the extracted text is then subject to any content compliance or objectionable content rules you set up for Gmail messages. For example, say you configured your content compliance setting so that messages with credit card numbers are moved to quarantine. A customer sends you a message with a PNG image attachment of an invoice that contains a credit card number. If you turn on OCR, Gmail converts the image attachment to text, detects the credit card number, and moves the message to quarantine.

****Restrict delivery****

Use this feature if you want to only allow sending or receiving of email messages from addresses or domains that you specify. This feature is useful in education where the institution wants to restrict students from sending messages externally.

**MAIL ROUTING**

## **Introduction to Mail Routing**

In the previous lesson we saw how you can use compliance settings to manage how specific messages are routed based upon specific message content. G Suite also provides routing controls that allow you to determine how email for your organization is routed and stored. For example, you may want:

* Gmail to scan your inbound mail for spam and compliance purposes, but store the mail on your external mail server.
* Some users to receive mail in Gmail inboxes, and others to access mail from your local server (split delivery)

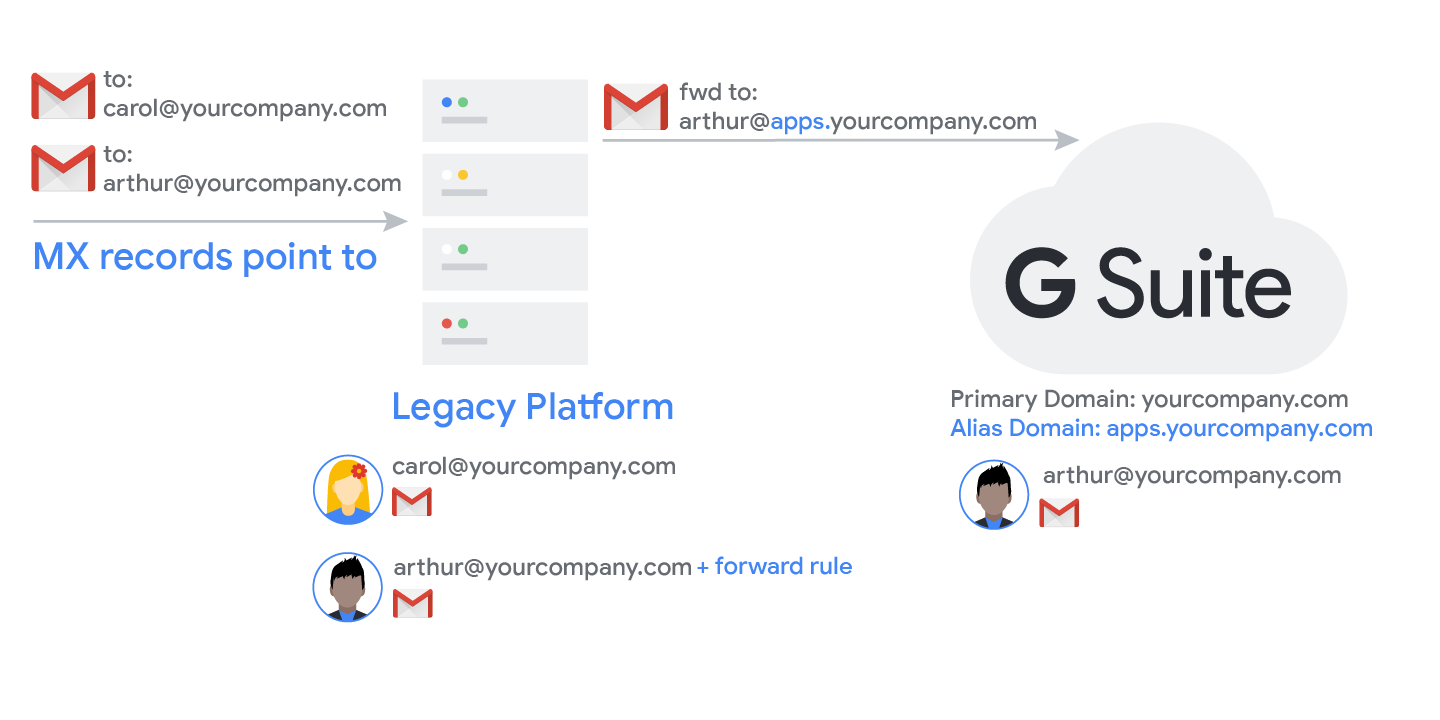
You use routing settings to configure inbound, outbound, and internal delivery options, such as dual delivery and split delivery.

Let's start by defining some important terms.

****Direct delivery****: This is the default setting and applies where your organization has all of it's users on G Suite. All messages are delivered directly to the Gmail inbox. If your environment is 100% G Suite you should not need to make changes to your mail routing settings in G Suite, however it is very useful to understand the options available to you as the administrator, so you should walk through this lesson and read the Help Center resources provided.

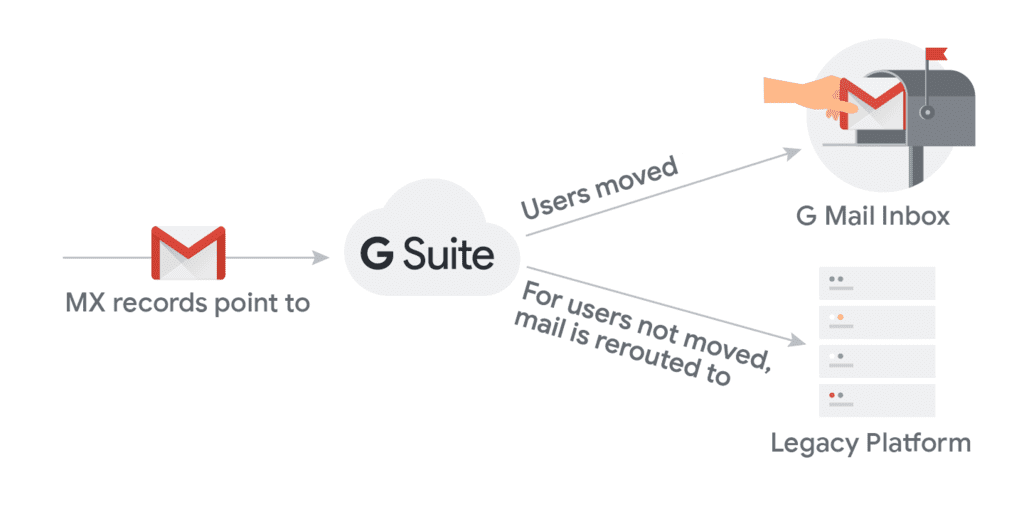
****Dual Delivery****: This is used where you want to route messages to the Gmail inbox and another system. With dual delivery, incoming mail is delivered to a primary mail server first. The primary server delivers each message to the inboxes associated with it, then forwards all messages to a secondary mail server. The secondary server delivers the messages to the secondary server inboxes. This method is useful if you are trialling G Suite for a small number of users but you wish your existing mail system to retain a copy of all messages.

In the example below, Arthur is trialling G Suite. His company's MX records are still pointing at their existing mail server, so any mail that is sent to Arthur is delivered to his legacy inbox but is also forwarded to his G Suite account using a forwarding rule to a G Suite domain alias. Carol, who has not yet migrated to G Suite will continue to receive mail in her legacy inbox.



****Split Delivery****: Incoming messages are routed to either the Gmail inbox or another mail system. This method works well if some of your users use Gmail, and others use a different mail system.

Split delivery is commonly used during a G Suite deployment once MX records have been changed to point to the Google mail servers. Users who have moved to G Suite receive messages in their Gmail inbox. Users who have not yet switched to G Suite continue to receive messages in the legacy platform.



As mentioned, both dual and split delivery methods are commonly used during a G Suite deployment where users are migrating from a legacy system to G Suite. Which one(s) are used, when and how it is implemented does depend greatly on the existing environment and needs of the customer.

In this lesson you will learn how to configure split delivery in G Suite and be introduced to some of the other routing controls available.

## **Exercise #1: Configure Split Delivery**

****Introduction****

Split delivery is where messages are routed to multiple mail systems based upon certain conditions that you specify. In G Suite split delivery is implemented through a combination of a host (or route) and a routing settings entry. In this exercise you will learn how to configure split delivery for a fictitious organization who is deploying G Suite in phases.

****Scenario****

Until now this course has assumed that you are working in a 100% G Suite environment. However many customers have existing domains and mail systems and they need to migrate data and users from the legacy platform to the cloud as part of the G Suite deployment.

Unless all users can be moved at once it is inevitable that some users will be on G Suite and others will remain on the legacy platform during different stages of the project. However, MX records for your domain can only point to one place; G Suite or legacy servers, so we need a way to ensure that mail can be correctly routed depending upon the user's location. For this we can use split delivery.

Consider you are deploying G Suite for your organization and are creating your users G Suite accounts just before they switch to the Google platform. At the start of the project, your MX records point to your legacy mail servers so you used dual delivery to ensure that mail was forwarded out to the small number of G Suite pilot users who moved early in the project.

Later you switch your MX records to Google so all mail is routed to G Suite. Once that is done you will use split delivery to ensure that users who have not yet migrated continue to receive their email on the legacy platform.

****Directions****

Create a host for your legacy mail platform

Before you create a routing setting you must add the details of your legacy server to the admin console. This is done by adding a new host (also known as a route).

1. If you are not already signed in, sign in to your domain as the administrator at [admin.google.com](https://admin.google.com/" \t "/home/sherwinowen/Documents\\x/_blank).

2. Click the ****Apps**** icon, click the ****G Suite**** icon and then click the ****Gmail****service.

3. Click ****Hosts****. The Hosts page will now open.

4. Click ****ADD ROUTE****.

5. Enter the 'Name' of Legacy Mail Platform.

This is where you enter the legacy mail server details. You must specify a public hostname or IP address. For more complex environments, you can also add a primary and secondary configuration, each of which can consist of multiple mail servers. To keep things simple let's assume you only have one mail server.

7. In the 'Specify email server' section, enter the hostname my.legacyserver.com. (This is just a test name and doesn't actually exist).

8. For the purposes of this exercise, enter a port number of 25.

9. Click ****SAVE****.

Create the routing setting

You have defined the host to route to, so now you can define the routing setting.

10. Return to the Settings for Gmail (Apps > G Suite > Gmail) page, scroll down and click the ****Advanced settings****.

11. Scroll down to the 'Routing' section and hover over the 'Routing' row, then click ****CONFIGURE****. The 'Routing' dialog box displays.

12. Enter a short description of Split Delivery.

13. In the 'Messages to affect' section, check the Inbound and Internal - receiving boxes.

12. Scroll down and in the section 'For the above type of messages, do the following', set the action to Modify message.

13. Scroll down and check the Change route box, and change Normal routing to Legacy Mail Platform.

14. Scroll down and click the ****Show options**** link.

15. In 'Account types to affect', uncheck Users and check the Unrecognized / Catch-all box.

16. Click ****ADD SETTING**** and click ****SAVE****.

You have now successfully configured split delivery. Any inbound (and internal - receiving mail) sent to a non-recognized user will be rerouted to the legacy mail server which can then deliver it to users who have not yet switched to G Suite. As you create G Suite accounts for those users, they will become recognized and mail will be delivered to their Gmail inbox.

****Note:**** The purpose of this exercise is to show how easy it is to configure mail routing (in particular, split delivery) in G Suite. For large G Suite deployments, there are best practices for split delivery setup where all accounts are provisioned in G Suite early in the project. You would then determine delivery routes based upon a user's G Suite OU.

****Help Center resources****

* [Add mail routes for advanced Gmail delivery](https://support.google.com/a/answer/2614757" \o "Add mail routes for advanced Gmail delivery" \t "/home/sherwinowen/Documents\\x/_blank)
* [Email routing and delivery](https://support.google.com/a/answer/2685650" \o "Email routing and delivery" \t "/home/sherwinowen/Documents\\x/_blank)

## **Mail Routing Controls**

In addition to custom routing options, G Suite offers a number of other routing controls that are designed for specific purposes. If your organization is using G Suite services for everything, then it is unlikely that you will ever need to configure these controls, but it is still useful to understand what is available and the key purpose of each. These additional mail routing controls are discussed briefly below.

****Outbound gateway****

An outbound mail gateway server processes email messages before they’re delivered. Typically, these servers are used for archiving or spam filtering. The gateway server should be configured to accept and forward mail from G Suite mail IPs only to prevent spammers from using it as an open relay. It's also important that your SPF record contains the gateway address. DKIM will work but only if the gateway does not modify the message in any way.

An outbound gateway can also be defined using a routing setting which is preferred as routing settings offer much more flexibility over the outbound gateway setting. The outbound gateway setting applies to everyone in the organization whereas routing settings can be applied at the OU level. Routing settings can also be configured to use specific envelope filters and address lists. For example, you may only want to archive mail from your legal department. If this is the requirement you would use a routing setting to capture all outbound mail from the legal department only and route that via the gateway.

****Recipient address map****

This feature is also known as a virtual user table. It allows the administrator to reroute a message from one address to another address. Each entry in the address map consists of two email addresses; the original intended address and the address where the message should be routed to. For example:

john@yourdomain, johnny@yourdomain

This is a basic routing concept but by using this setting, you don’t need to create individual routing settings for each address mapping. G Suite supports upto 5000 entries in the map and a single recipient can map to a maximum of 12 other addresses. There is also an option to route the message to the original intended recipient.

****Inbound email journal acceptance to Vault****

This feature allows you to use Google Vault to store messages from another mail platform.

****Third party email archiving****

This feature allows Gmail content to be archived in a third party archive system.

****Non-Gmail mailbox****

This setting is only for users whose mailboxes are located on an on-premise/non-Gmail mail server. It allows you to use Gmail's spam filtering and other G Suite features such as content compliance and mail routing but messages are delivered to the users external inbox. You must not turn this feature on for Gmail users as they will lose access to their Gmail inbox.

****SMTP Relay service****

If your organization uses a non-Gmail mail service, you can configure the SMTP Relay service to route outgoing mail through Google. You can use this setting to filter messages for spam and viruses before they reach external contacts. You can also apply G Suite email security and advanced Gmail settings to outgoing messages.

Don't confuse this with the Outbound gateway setting described above. In that setting, your users are using Gmail and you want to route all outbound mail through another SMTP server defined by the outbound gateway setting. Using the SMTP relay service, Google becomes the outbound gateway for your non-Gmail mail users.

****Alternate secure route****

You can use this setting to determine the route a message must take if it requires secure transport. For example, if you use a third-party encryption service, you can use the alternate secure route setting to route otherwise insecure traffic to it.