**Managing G Suite**

**Introduction to G Suite Management**

## **Welcome and Getting Started Guide**

****Introduction****

Welcome to Managing G Suite. In this course you will cover a variety of topics which revolve around G Suite services. You will learn how to enable and disable services and you will also become familiar with the most common settings for core services such as Gmail, Calendar and Drive.

You will also learn the fundamentals of device management with G Suite.

We will introduce you to Google Vault, Google's e-discovery service, the admin reports and dashboards that are available in the admin console, and finally we will take a look at domain management and multi domains with G Suite.

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

****Prerequisites****

This course is the second course in the G Suite Administration series. You should complete 'Introduction to G Suite' before taking this course.

If you have completed 'Introduction to G Suite' 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[G Suite Services Overview](https://www.coursera.org/learn/managing-g-suite/supplement/nIc4S/g-suite-services-overview" \o "G Suite Services Overview" \t "/home/sherwinowen/Documents\\x/_blank).

**Managing G Suite Services**

## G Suite Services Overview

****Introduction****

This lesson will focus on G Suite services, and how you as a G Suite admin are able to control your users' access to different Google services by enabling and disabling services for different groups. After you get acquainted with how to manage services for your organization, you will then go through the most used services, and the associated best practices for each service.

Just like previous modules, explore the Admin Help Center resources linked below.

****Help Center resources****

Review the following articles in order to learn more about managing services

* [Managing users access to services](https://support.google.com/a/topic/28974" \o "Manage users' access to services" \t "/home/sherwinowen/Documents\\x/_blank)
* [Set up G Suite feature releases for users](https://support.google.com/a/answer/172177/" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #1 - Turn Services On or Off for Everyone**

****Introduction****

As the G Suite administrator, you control user access to different types of Google services, including:

* ****G Suite**** which includes enterprise versions of Gmail, Calendar, Drive and Docs, and more. These are the core services that have a Terms of Service agreement and are fully supported by G Suite Support.
* ****Additional Google Services**** such as Blogger, Google Books, and more. These services are available to use in G Suite, but aren't covered by the Terms of Service agreement, nor supported by G Suite Support.
* ****Marketplace apps****. The G Suite Marketplace lets administrators browse for, purchase, and deploy integrated, business-oriented cloud applications. Warranties and support for these third-party apps are provided by the vendor, but not G Suite Support.

Administrators can turn services on or off for the **entire organization** or **for a particular OU**. In this exercise, you'll learn how to configure services to fit your company's business needs.

****Scenario****

Your company has a strong focus on the confidentiality of their corporate information. As the administrator, you've been asked by the IT Manager to remove the ability to access some Google services to align better with their business policy.

Hey G Suite Admin,

As you know we are working on a very confidential widget at the moment. To prevent any information leaks I don't want anyone to be able to create a blog or site with their company account.

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.

3. Click ****G Suite****.

4. Sites is a core service and core services are generally enabled for everyone by default. To turn off this service, locate Sites in the list and click the ellipses (three vertical dots) icon at the end of the row. Then click ****Turn OFF for everyone****.

5. Click ****TURN OFF**** to confirm.

6. To verify the service is now disabled, open a new browser tab and go to https://sites.google.com/a/yourdomain

When you try to access the Sites service you should see a message advising that you do not have access to that service.

7. You must now turn off Blogger as per Alex's request. Blogger is an additional service so from the admin console click ****Apps > Additional Google services****.

8. Locate Blogger in the list and click the ellipses (three vertical dots) icon at the end of the row. Then click ****Turn OFF for everyone****.

9. Click ****TURN OFF**** to confirm.

You've successfully turned off the two services for your whole organization.

****Notes****

1. It can take up to 24 hours for a service ON/OFF change to take effect.
2. Some services depend on other services. For example, Google+ depends on Calendar, Drive, and others. You can't turn on Google+ services, unless the other services are also on.

## **Exercise #2 - Enable/Disable a Service for a Single OU**

****Introduction****

In the previous exercise you disabled two services for your entire organization. In this exercise you will enable and disable a service at the OU level.

****Scenario****

You receive the following email from Alex.

Hey G Suite Admin,

Thanks for turning off those services for me. However, our CEO has advised me that they will want to create a site at some stage so can you enable the Sites service for our executive only?

Also, can you turn off Google+ for all contractors?

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.

3. Click ****G Suite****.

4. Click on the ****Executive**** OU (left side of the page). You are now viewing the status for Apps in the Executive OU only. Note that Sites is OFF at the moment as it inherits it's setting from the top level organization.

5. To turn Sites on for this OU only, locate Sites in the list and click the ellipses (three vertical dots) icon at the end of the row. Then click ****ON (Override)****.

5. Click ****TURN ON**** to confirm. The Sites service status should change to ON.

6. Click another OU and/or the top level organization and verify that the Sites service remains OFF for other parts of the organization.

7. Click on the ****Contractors**** OU.

8. Locate Google+ in the list and click the ellipses (three vertical dots) icon at the end of the row. Then click ****OFF (Override)****.

9. Click ****TURN OFF****to confirm. You may need to confirm a second time. If prompted, click ****TURN GOOGLE+ OFF****.

You've successfully turned a single service on and another one off at the OU level thus overriding inheritance from the higher level organization.

****Notes****

1. It can take up to 24 hours for a service ON/OFF change to take effect.

## **Exercise #3 - Enabling a Service Using Groups**

****Introduction****

In the previous exercise you learned how to enable and disable a service for an individual OU. This alignment between service status and organizational structure is very useful but what happens if you want to enable a service for some users in an OU but keep it disabled for others. In this exercise you will learn how to enable a service for specific users by leveraging a Google Group.

****Scenario****

You receive the following email from Alex.

Hey G Suite Admin,

Sam, our CEO would like to enable Sites for here Executive Assistant Ellie Gray. Can you please do that for her.

Thanks,

Alex Bell, IT Manager

****Directions****

1. Open a new incognito browser window and go to [mail.google.com](https://mail.google.com/" \o "mail.google.com" \t "/home/sherwinowen/Documents\\x/_blank).

2. Sign in as Ellie Gray ellie.gray@yourdomain

3. Navigate to https://sites.google.com/a/yourdomain to confirm that Ellie does not have access to the Sites service.

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

You are now going to create a group and make Ellie a member. Then you will enable the Sites service for this group.

5. Click the ****Groups**** icon.

6. Click ****Create group**** and enter the following information:

* Name: Access Sites
* Description: Users with access to the sites service regardless of their OU setting
* Group email: access.sites@yourdomain

7. Set the 'Access type' to Restricted (Only members can post and view topics)

8. Click ****CREATE GROUP****.

9. Click the ****Add members to Access Sites**** link and add Ellie Gray as a member.

Now we will enable Sites access for the group created above.

10. Navigate to****Apps > G Suite****.

11. Click the Groups link on the left hand side of the page.

12. Add Access Sites to the 'Search for a group' field. The right hand side of the screen will now show status for apps in Access Sites.

13. Locate Sites in the list of services and hover over the row, then click****TURN ON****.

14. Click ****TURN ON**** to confirm.

Verify that Ellie can now access the Sites service.

15. Sign out as the domain administrator and sign back in as Ellie.

16. Navigate to https://sites.google.com/a/yourdomain.

Even though Ellie's OU has Sites disabled, the sites page should load because she is a member of the access group with Sites enabled.

****Notes****

1. It can take up to 24 hours for a service ON/OFF change to take effect.
2. Groups turn on user access to G Suite core services and Google additional services. Groups can’t turn off user access to a service that’s turned on for an organization.
3. It's a good practice to develop a naming convention for access groups such as the one created in this exercise, e.g. prefix the group name/email with Access or AX.
4. An access group can contain users from any organizational unit or another group (nested groups).

****Help Center resources****

* [Control access to G Suite and Google services with groups](https://support.google.com/a/answer/9050643" \o "Control access to G Suite and Google services with groups" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #4 - Set Services Release Track**

****Introduction****

G Suite is 100 percent web, so your users receive new features and updates automatically, without needing to install or update any software. However, you can still control when new features become available for users.

Setting which release track your company is on is an important administration task. It defines when new features and updates are applied in your domain.

To help make that decision, you can choose from:

* ****Scheduled release track****: (Recommended and enabled by default) Choose this track to delay releasing new features to users, giving you extra time to train your support staff and prepare users for the coming changes. Google releases features to the Scheduled release track on Tuesdays only, at least one week after the feature was released to the Rapid release track.
* ****Rapid release track****: Choose this track if you want users to access new features as soon as Google rolls them out to consumer users. These features have been through testing and quality assurance, but users will see them at the same time you do, before you have a chance to evaluate them for your organization.

****Scenario****

For most G Suite customers, we recommend the scheduled release track. However your company has decided that they want to access new features as soon as they're available.

****Directions****

1. Review the [G Suite release calendar](https://gsuite.google.com/whatsnew/calendar/" \t "/home/sherwinowen/Documents\\x/_blank) to see which features are currently on the Rapid release track. As the administrator, you should be aware of new changes; Rapid releases are marked in red.

2. 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).

3. Click the ****Company profile**** icon.

4. Click ****Profile****. You can select domain wide settings using the Profile feature.

5. In the 'New User Features' section, select the Rapid release option.

6. Click ****SAVE****. Your users will now have access to new user features as soon as Google releases them.

****Notes****

1. It may take up to a day for changes to take effect.

****Help Center resources****

* [Set up G Suite feature releases for users](https://support.google.com/a/answer/172177" \o "Set up G Suite feature releases for users" \t "/home/sherwinowen/Documents\\x/_blank)
* [Opt in to new services](https://support.google.com/a/answer/82691" \o "Opt in to new services" \t "/home/sherwinowen/Documents\\x/_blank)

**GMAIL**

## **Introduction to Gmail**

This lesson will take you through the various Gmail settings available to you in the admin console. Before you continue, it is recommended that you explore the Help Center resources below.

****Help Center resources****

Review the following articles in order to learn more about Gmail

* [Manage email features](https://support.google.com/a/topic/4596824" \o "Manage email features" \t "/home/sherwinowen/Documents\\x/_blank)

## Exercise #1 - Configure Common User Settings

****Introduction****

In this exercise you will check and configure some of the more common user settings for your organization. You will also modify settings for a single OU as per company policy.

****Scenario****

The company has decided to configure several important Gmail features and user access settings as follows:

* Let users choose their own themes
* Don't allow email read receipts to be sent
* Let users delegate access to their mailbox to other users
* Enable Gmail web offline
* Do not allow contractors to delegate access to their mailbox or use Gmail web offline

****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 ****User settings****.

4. Review the settings for Gmail. Several policies are already configured while others must be changed.

* Click on the ‘Themes’ section. Ensure Let users choose their own themes is checked. Click ****SAVE**** if you have made any changes.
* Click on the ‘Email Read Receipts’ section. Ensure Do not allow email read receipts to be sent option is selected. Click ****SAVE**** if you have made any changes.
* Click on the ‘Mail Delegation’ section. Check the Let users delegate access to their mailbox to other users in the domain box. Click ****SAVE**** if you have made any changes.
* Click on the ‘Gmail web offline’ section. Check the Enable Gmail web offline box. Click ****SAVE**** if you have made any changes.

5. Click the ****Contractors**** OU (left side of page).

Note the OU policies are inherited from the top level organization:

* In the ‘Mail Delegation’ section deselect the Let users delegate access to their mailbox to other users in the domain box, then click ****OVERRIDE****.
* In the ‘Gmail web offline’ section deselect the Enable Gmail web offline box, then click ****OVERRIDE****.

****Help Center resources****

* [Assign Gmail settings for users](https://support.google.com/a/answer/173555" \o "Assign Gmail settings for users" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #2 - Enable Gmail Labs**

****Introduction****

While Gmail Labs are experimental, the company has decided to enable this feature for all their users. They may decide to only enable certain labs later, but have decided to see how users respond to the labs first. Complete the instructions below to verify labs are enabled for the organization.

****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 ****Labs****. Note that labs are enabled by default.

4. Check the Advanced Labs Management box and explore the options. Optionally, you can also disable labs entirely for your users.

5. Click ****DISCARD****.

## **Exercise #3 - Enable G Suite Sync for Executives**

****Introduction****

In this exercise you will check and configure end user access to Gmail as per company policy.

****Scenario****

The company wants to restrict the use of [G Suite Sync for Microsoft Outlook](https://support.google.com/a/users/topic/23333" \o "Use Outlook with G Suite" \t "/home/sherwinowen/Documents\\x/_blank) (GSSMO) to the executive only. You must ensure that only users in the Executive OU can use GSSMO.

****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 set to OFF.

5. Click on the G Suite Sync row and ensure Enable G Suite Sync for Microsoft Outlook for my users box is deselected.

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

7. Now click the ****Executive**** OU.

8. Click on the G Suite Sync row and check the Enable G Suite Sync for Microsoft Outlook for my users box.

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

****Help Center resources****

* [Assign Gmail settings for users](https://support.google.com/a/answer/173555" \o "Assign Gmail settings for users" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #4 - Configure Compliance Policies**

****Introduction****

We will be covering Gmail's advanced settings in a later course in the series, but as an introduction, in this exercise you will set a couple of compliance policies for your organization.

****Scenario****

G Suite provides a rich set of email compliance policies you can configure for an organization or the entire domain. The IT Manager has decided to follow Google's best practices to configure only a few compliance policies to start and possibly add more later.

* The company will continue to use their compliance footer which will be appended to the end of all email messages leaving the company, but not for internal messages.
* The company also wants to prevent their users from receiving attachments that are video, multimedia and music from external users. G Suite can remove these attachments, yet deliver the message. For now, these file attachments can be sent internally between employees. They may revisit this policy later.

****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 'Append footer' row, then click ****CONFIGURE****. The ‘Append footer’ dialog box displays.

5. Enter a short description that will appear within the setting's summary, such as Company compliance footer.

6. Enter (or copy and paste) the compliance footer as follows into the ‘For all outbound email messages, append the following footer’ field:

This message (and any associated files) may contain confidential and/or privileged information. If you are not the intended recipient or authorized to receive this for the intended recipient, you must not use, copy, disclose or take any action based on this message or any information herein. If you have received this message in error, please advise the sender immediately by sending a reply email and delete this message. Thank you for your cooperation.

7. Optionally modify the text by changing the font size and style.

8. Click ****ADD SETTING****.

9. Click ****SAVE****.

You will now configure a compliance rule to strip video, multimedia and music attachments from all inbound messages.

10. Scroll down and hover over the 'Attachment compliance' row, then click ****CONFIGURE****. The 'Attachment compliance' dialog box displays.

11. Enter a short description that will appear within the setting's summary, such as Remove video and music attachments.

12. In the 'Email messages to affect' section, check the Inbound box.

13. Under 'Add expressions that describe the content you want to search for in each message', click ****ADD****, then select Video and multimedia and Music and sound as the type of attachments.

14. Click ****SAVE****.

15. In the 'If the above expressions match, do the following' section, ensure Modify message is selected and check the Remove attachments from message box. Note how you can optionally append a message to notify recipients that attachments have been removed.

16. Click ****ADD SETTING****.

17. Click ****SAVE****.

18. Verify the above policies:

* Send an email from your training account to your personal email. Does it include the compliance footer?
* Reply to the email and attach a video or music file. Does the training account user receive the message with the attachment?

****Help Center resources****

* [Configure outbound messages with footer text](https://support.google.com/a/answer/2364576" \o "Configure outbound messages with footer text" \t "/home/sherwinowen/Documents\\x/_blank)
* [Set up rules for attachment compliance](https://support.google.com/a/answer/2364580" \o "Set up rules for attachment compliance" \t "/home/sherwinowen/Documents\\x/_blank)

**CALENDAR**

## **Introduction to Calendar**

Calendar is an extremely important core service that is offered as part of G Suite. Users are going to want to set up their calendars as soon as possible. This lesson will take you through how to administer the Calendar service. Ensure that you explore the Help Center resources.

****Help Center resources****

Review the following articles to learn more about Calendar

* [Calendar](https://support.google.com/a/topic/9201" \o "Calendar" \t "/home/sherwinowen/Documents\\x/_blank)
* [Managing Calendar for G Suite](https://support.google.com/a/answer/39410?hl=en&ref_topic=1033168" \t "/home/sherwinowen/Documents\\x/_blank)
* [Manage Calendar Resources](https://support.google.com/a/answer/1686462" \o "Manage Calendar Resources" \t "/home/sherwinowen/Documents\\x/_blank)
* [My Calendars list and other settings](https://support.google.com/a/answer/60766" \o "My Calendars list and other settings" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #1 - Set Calendar Sharing Settings**

****Introduction****

In this exercise you will review the sharing settings for the Calendar service.

****Scenario****

The company wants to restrict external sharing of calendars but also allow internal sharing to be managed by each user. Users can:

* Only share free/busy information publicly
* Share all information internally

****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 ****Calendar****service.

3. Click the ****Sharing settings**** card. This is where you set sharing options for primary calendars.

4. Confirm that 'External sharing options for primary calendars' is set to Only free/busy information (hide event details). This represents the highest level of sharing allowed.

5. Confirm that 'Internal sharing options for primary calendars' is set to Share all information. This represents the default setting for new users. Users can still change this setting.

6. Return to the Calendar settings page, scroll down and click the ****General settings**** card. This is where you set sharing options for secondary calendars.

7. Confirm that 'External sharing options for secondary calendars' is set to Only free/busy information (hide event details). This represents the highest level of sharing allowed.

8. Confirm that 'Internal sharing options for secondary calendars' is set to Share all information. This represents the default setting for new calendars. Users can still change this setting.

****Notes****

1. The sharing settings you set above determine the highest level of sharing that a user is allowed to make for their calendars.
2. If you lower a 'highest level of sharing' setting people may lose access to calendars they could see previously.

****Help Center resources****

* [Set Calendar visibility and sharing options](https://support.google.com/a/answer/60765" \o "Set Calendar visibility and sharing options" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #2 - Configure Access to Calendar Resources**

****Introduction****

In the previous course you created two calendar resources: Conference room, and Boardroom.

This exercise will guide you through setting access to both of these resources. Read through the scenario and then complete the steps in the exercise. Remember, if you feel you need more context, go back to the help center resources linked at the beginning of this lesson.

****Scenario****

You have received a request from Alex, IT Manager asking you to allow anyone in the organization to be able to book the Conference room but he also wants you to restrict booking access for the Boardroom to Ellie Gray only.

As Executive Assistant, Ellie should also be able to manage the Boardroom resource.

****Directions****

In G Suite, calendar resources are owned by the administrators. Calendar resource settings are managed from your own calendar.

1. Sign in as the administrator and open your Google Calendar from the Apps launcher or by visiting [calendar.google.com](https://calendar.google.com/" \t "/home/sherwinowen/Documents\\x/_blank)

Calendar resources will automatically appear in the administrator's 'My calendars' list. This can take some time however so if necessary, we'll use another technique to make them display sooner. If you cannot see the two resources you created earlier under 'My calendars':

* Click the + sign to the right of 'Other Calendars' and click ****Browse resources****. You should see the two resources listed.
* Hover over the Boardroom and tick the check box to the right of the resource. Repeat this for the Conference room.
* Go back to your calendar. Both resources should now be listed under 'My calendars'.

Make the Conference room available for all users

2. Hover over the Conference room in your 'My calendars' list and click the ellipses (three vertical dots) next to the calendar name, and then click ****Settings and sharing****.

3. Adjust the sharing settings as follows:

* In the 'Access permissions' section, ensure Make available for yourdomain is selected.

4. Return to your calendar. Hover over the Boardroom in your 'My calendars' list and click the ellipses (three vertical dots) next to the calendar name, and then click ****Settings and sharing****.

5. Adjust the sharing settings as follows:

* In the 'Access permissions' section, ensure that Make available to public and Make available for yourdomain are both deselected.
* In the 'Share with specific people' section, click ****Add people**** and add Ellie Gray.
* Set her Permissions to 'Make changes and manage sharing' and click ****Send****.

6. Verify that the Boardroom is available to Ellie and not available to other users. For more information, see[Test scheduling resources](https://support.google.com/a/answer/1037476" \t "/home/sherwinowen/Documents\\x/_blank).

* Sign in as Ellie and open Google Calendar. You should see the Boardroom listed under 'My Calendars'. You won't see the Conference room listed because you do not manage this calendar.
* Create an event. You should see both rooms listed on the 'Rooms' tab. Note: You manage the Boardroom but you can also see the Conference room because this is available to all users.
* Sign out and sign in again, this time as Jon Baird and open Google Calendar.
* Create an event and look at the 'Rooms' tab. You should see the Conference room only. You do not have access to book the Boardroom so it will not be listed.

7. Optionally, try to subscribe to the Boardroom as Jon by browsing to the resource and checking the box to the right of the resource name in the 'Resources' list. This should result in an error as Jon does not have access.

**DRIVE AND DOCS**

## **Introduction to Drive and Docs**

In these exercises, you'll learn how to configure Google Drive for your domain.

You will learn how to control the document visibility and sharing, transfer ownership, and restore deleted files. We will also discuss backup and sync options.

Finally we will take a look at Shared drives (formerly known as Team drives), a shared space where your teams can easily store, search, and access their team's files anywhere and from any device.

Ensure that you go explore the Help Center resources listed below.

****Help Center resources****

* [Drive training and help](https://support.google.com/a/users/answer/9282958" \o "Drive training and help" \t "/home/sherwinowen/Documents\\x/_blank)
* [Drive](https://support.google.com/a/topic/2490075" \o "Drive" \t "/home/sherwinowen/Documents\\x/_blank)
* [Overview: Manage Drive for an organization](https://support.google.com/a/answer/2490026" \o "Overview: Manage Drive for an organization" \t "/home/sherwinowen/Documents\\x/_blank)
* [Get started: Drive setup guide for admins](https://support.google.com/a/answer/6085538?hl=en&ref_topic=2498056&visit_id=636976121827936205-2396464404&rd=1" \o "Get started: Drive setup guide for admins" \t "/home/sherwinowen/Documents\\x/_blank)
* [Manage shared drives](https://support.google.com/a/topic/7337266" \o "Manage shared drives" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #1 - Drive Sharing Settings**

****Introduction****

Google Drive is a way for your users to access and share all their files, folders, and Google documents at any time and on any device.

As the administrator, you determine whether users can share their documents outside your organization, whether they can access documents created outside your organization, and the default visibility level for new documents.

****Scenario****

You receive the following email from Sam Morse:

Hello G Suite Admin,

I have been thinking about how I want our people to share documents inside and outside the company. I want everyone to be able to share documents with our clients and partners, but not be able to publish openly on the web.

I also want to build a strong collaboration culture, so inside the company I want everyone to be able to have permission to see each other's documents but only if they have the link first. Can you make this happen?

Regards,

Sam Morse, CEO

****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 ****Drive and Docs****service.

3. Click ****Sharing settings****. The current settings display for your organization.

Before you change any settings, read [Set Drive users' sharing permissions](https://support.google.com/a/answer/60781" \o "Set Drive users' sharing permissions" \t "/home/sherwinowen/Documents\\x/_blank) to understand what each setting indicates and the impacts of changing them. Review [Share and work with others](https://support.google.com/docs/topic/4671185" \o "Share and work with others" \t "/home/sherwinowen/Documents\\x/_blank) to get the user's perspective.

4. Sam wants users to be able to share outside the organization, but does not want users to publish anything to the web. To achieve this, click ****Sharing options**** to edit the settings.

5. Set the 'Sharing outside of yourdomain' field to ON. Files owned by users in your organization can be shared externally. This setting applies to shared drives as well.

6 Deselect the check box for 'Allow users in yourdomain to publish files on the web or make them visible to the world as public or unlisted files'.

7. Click ****SAVE****.

8. Sam also wants users to collaborate internally through sharing links so scroll down the Drive and Docs service settings page and click on ****Link Sharing****.

9. The default setting for this option is OFF. To change the file visibility so that anyone in the company can access a document once they have the link, select ON - Anyone at yourdomain with the link.

This option is recommended for two reasons:

* Allows for easy sharing, but offers protection from outside the organization, because users must sign in to access the shared documents.
* Documents with this visibility won't normally be found in search results.

10. Click ****SAVE****.

****Notes****

1. In the sharing settings area you may also have seen an option to allow sharing with whitelisted domains. This is very useful if your partners/customers have compatible domains as you can allow external sharing but restrict it to a named set of domains.
2. Sharing settings discussed here override shared drive external sharing settings. If you disable sharing outside of your organization, managers of shared drives cannot override this setting even if they are allowed to change shared drive settings.

## **Exercise #2 - Transfer Ownership**

****Introduction****

As the administrator you can transfer all documents owned by one user to another user in your organization.

There are three user types in Google Drive: **owner**, **editor**, and **viewer**. **Documents can have many editors and viewers, but only one owner at a time**.

By default, the creator of a document is also the owner, but document ownership can be transferred to another user. After the transfer, the original owner retains editing privileges of the documents unless that user is deleted or their edit permissions are removed.

We've already seen that transferring ownership of a user's documents can be useful when the user leaves the organization. When you delete a user from the admin console you are given the option to transfer files to a new user. And it's good practice to transfer ownership to avoid losing important documents.

****Scenario****

You receive the following email from Sam Morse:

Hello G Suite Admin,

My executive assistant, Ellie, is responsible for maintaining many of my important documents. Is there a way that I can make her the owner so that she has total control over them, while still allowing me to make changes?

Regards,

Sam Morse, CEO

****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 ****Drive and Docs****service.

3. Click ****Transfer ownership****

4. Enter samantha.morse into the 'From' field and ellie.gray into the 'To' field.

5. Click ****TRANSFER FILES****. You should now see a prompt advising that you, the old owner and the new owner will receive an email upon completion of the transfer. Click ****OK****.

6. Open your inbox and verify that you have received a confirmation email.

****Notes****

1. It's also possible to transfer ownership of documents using the **[Drive API](https://developers.google.com/drive/" \o "Drive API" \t "/home/sherwinowen/Documents\\x/_blank)**.

****Help Center resources****

* [Restore a deleted user's Drive files](https://support.google.com/a/answer/2993112" \o "Restore a deleted user's Drive files" \t "/home/sherwinowen/Documents\\x/_blank)
* [Transfer Drive files to a new owner](https://support.google.com/a/answer/1247799" \o "Transfer Drive files to a new owner" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #3 - Restore Deleted Files**

****Introduction****

There comes a time in every administrator's job where someone will approach you, in a panic and desperate to recover lost data. The good news is that G Suite has a way for you to restore a user's data for a certain period of time.

You can restore a user's deleted Google Drive files for a date range you specify, as long as the files were deleted within the past 25 days. This helps ensure that, if a user accidentally deleted important files, those files are not permanently lost.

In this exercise you will log into as a G Suite user, create a file and then delete it. You will then restore that file as the administrator.

****Scenario****

You receive the following email from Timothy:

Hey G Suite Admin,

I don't know how it's happened, but a really important finance report ("Super Important Budget") has vanished. It's gone. Even if I search, I can't find it, but it was there 3 days ago. It would take months of work to recreate it. I emptied the trash yesterday; it must have been in there somehow. Can you please help?!

Thanks

Timothy Lee, Finance Manager

****Directions****

Permanently delete a file

1. Sign into G Suite as Timothy Lee at [drive.google.com](https://drive.google.com/" \o "drive.google.com" \t "/home/sherwinowen/Documents\\x/_blank).

2. Create a Google sheet named Super Important Budget. Close the sheet. This will take you to your 'My Drive'.

3. Drag the sheet to the Bin on the left, or right click on the sheet and click ****Remove****.

4. Open the Bin. You should see the sheet you just deleted. Now click the ****Empty bin**** link. Alternatively, right click on the sheet and click ****Delete forever****.

5. Click ****EMPTY BIN**** or ****DELETE FOREVER**** to confirm.

Recover the deleted file

6. Sign out of G Suite and sign back in to your domain as the administrator at[admin.google.com](https://admin.google.com/" \t "/home/sherwinowen/Documents\\x/_blank).

7. Click the ****Users****icon.

8. Locate Timothy Lee in the list and hover over his name, then click ****More > Restore Data****.

9. A dialog box will now be presented where you can enter a from and to date range. Complete the date values and ensure that 'Application' is set to Drive. Then click ****RESTORE****.

Verify the file has been restored

10. Repeat Step 1 and sign into Drive as Timothy. You should see the Super Important Budget file in Timothy's My Drive.

****Help Center resources****

* [Find or recover a file](https://support.google.com/drive/answer/1716222" \o "Find or recover a file" \t "/home/sherwinowen/Documents\\x/_blank)
* [Restore a G Suite user’s Gmail and Drive data](https://support.google.com/a/answer/6052340" \o "Restore a G Suite user’s Gmail and Drive data" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #4 - Enable Docs Offline Access**

****Introduction****

Through offline access users are able to view and edit Google documents, spreadsheets, and presentations even when they don't have an Internet connection. As the administrator, it's important for you to know the options and limitations of Drive offline access.

****Scenario****

You receive the following email from Sam:

Hello G Suite Admin,

I'm traveling next week but need to prepare for a meeting. I've been told that I can have offline access to my documents in Drive even when I'm on the plane. I mostly want to view and edit presentations and spreadsheets.

Can you look into it for me? I'll have my Windows laptop with Firefox with me. How do I set it up?

Thanks

Sam Morse, CEO

****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 ****Drive and Docs****service.

3. Click ****Features and Applications****.

4. Click ****Offline**** to edit the offline settings.

5. Ensure that Allow users to enable offline access (recommended) is selected.

6. Click ****SAVE**** if you made changes in the previous step.

Sam can now enable offline access to Docs. Review [Work on Google Docs, Sheets, & Slides offline](https://support.google.com/docs/answer/6388102" \o "Work on Google Docs, Sheets, & Slides offline" \t "/home/sherwinowen/Documents\\x/_blank) and then answer the following questions.

* Can Sam use Firefox to access her docs offline?
* What app does Sam need to install?
* What steps will Sam have to take to have offline access for her trip?
* How can Sam view the docs once offline?
* Can Sam edit the docs she wants to use on the flight?

7. You should now advise Sam of the steps she needs to take to complete the offline configuration. An example email is below:

Hey Sam,

I've looked into offline access for you. You must download and install the Chrome browser and offline extension on your laptop. Instructions can be found here to set up offline access - [Work on Google Docs, Sheets, & Slides offline](https://support.google.com/docs/answer/6388102" \o "Work on Google Docs, Sheets, & Slides offline" \t "/home/sherwinowen/Documents\\x/_blank). It should only take a minute.

Once you've enabled offline access to view your files when traveling, open Chrome and visit drive.google.com. The offline version of your Drive will load. Then you can then view and edit your presentations & spreadsheets without an Internet connection.

Additionally, if you want offline access on other devices, you need to set this up on each device individually.

Please let me know if you have any questions.

Regards,

G Suite Admin

## **Exercise #5 - Stream or Sync Files**

****Introduction****

There are two ways to access Drive files and keep them in sync on all your devices.

* ****Drive File Stream**** which is best for most organizations. This application lets you stream My Drive and shared drive files directly from the cloud. You can also make Drive files available for offline access.
* ****Backup and Sync**** which is Google's consumer sync client that organizations can use, too. With Backup and Sync, all your Drive content is stored locally.

In this exercise, you will enable the use of Drive File Stream and allow users to install the software themselves.

****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 ****Drive and Docs****service.

3. Click ****Features and Applications****.

4. Click ****Drive File Stream**** to edit the settings.

5. Check the 'Allow Drive File Stream in your organization' and 'Show Drive File Stream download link' boxes. The second box allows users to install Drive File Stream from the Settings menu in Drive.

6. Click ****SAVE**** if you made changes above.

7. Go to [drive.google.com](https://drive.google.com/" \o "drive.google.com" \t "/home/sherwinowen/Documents\\x/_blank) and click the Settings menu (the gear icon). Verify that there is a 'Get Drive for desktop' option. Note: If you made changes in Step 5 you may need to wait some time for the link to appear.

****Notes****

1. You can allow Drive File Stream and Backup and Sync for your users. If a user runs Drive File Stream at the same time as Backup and Sync, the user is prompted to stop syncing My Drive in Backup and Sync. If they agree, they will now access My Drive only with Drive File Stream which frees up disk space and improves performance. If they decline they continue to use both products which nullifies disk space savings and potentially leads to confusion.
2. If you enable the download links for both tools, only the Drive File Stream link is presented.

****Help Center resources****

* [Choose a sync solution](https://support.google.com/a/answer/7491633" \o "Choose a sync solution" \t "/home/sherwinowen/Documents\\x/_blank)
* [Use Drive File Stream with work or school](https://support.google.com/drive/answer/7329379" \l "Keepoffline" \o "Use Drive File Stream with work or school" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #6 - Shared Drive Creation**

****Introduction****

Shared drives are shared spaces where teams can easily store, search, and access their files anywhere, from any device. Unlike files in My Drive, files in a shared drive belong to the team instead of an individual. Even if members leave, the files stay exactly where they are so your team can continue to share information and get work done.

In this exercise you check that shared drive creation is enabled for your organization and you will modify settings to ensure data remains confidential only to members of each drive.

****Scenario****

You receive the following email from Sam Morse:

Hello G Suite Admin,

As you know we have quite a few ongoing projects and have people join and leave those projects on a regular basis. I would like for us to be able to store project documents in a shared space so users do not need to keep these files in their personal Drive and share them with others manually.

Can you please confirm that all users can create shared drives as they require them. I would also like to ensure that shared drive files cannot be accessed by external users and non members of the shared drive but allow the shared drive owner discretion on that point.

Can you make this happen?

Regards,

Sam Morse, CEO

****Directions****

Let's start by setting the shared drive policies.

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 ****Drive and Docs****service.

3. Click ****Sharing settings****.

4. Click ****Shared drive creation**** and configure the settings as follows:

* Prevent users in yourdomain from creating new shared drives. Unchecked.
* Prevent full-access members from modifying shared drive settings. Unchecked.
* Prevent people outside yourdomain from accessing files in the shared drive. Checked.
* Prevent non-members of the shared drive from accessing files in the shared drive. Checked.
* Prevent commenters and viewers from downloading, copying and printing files in the shared drive. Unchecked

5. Click ****SAVE****.

Now we will create a shared drive.

6. Sign out and sign back into G Suite as Timothy Lee at [drive.google.com](https://drive.google.com/" \o "drive.google.com" \t "/home/sherwinowen/Documents\\x/_blank).

7. Click ****Shared drives**** on the left, and click ****Create a shared drive****.

8. Enter a drive name, e.g. Project X and click ****CREATE****.

9. Click the ****Add members**** link and add Sam Morse as a Content Manager, then click ****SEND**** to send here a notification that she has been added to the shared drive.

10. Click on the shared drive title to reveal a drop down menu, and select ****Shared drive settings****. Note that you can modify the external and non-member settings. This is because the policy above allows full-access members to modify shared drive settings.

11. Optionally, sign back in as the administrator and return to the Sharing options card. From here disable sharing outside of the domain. Then sign back in as Timothy Lee and check the shared drive settings again. You should see that sharing outside of the domain is now disabled and cannot be changed. This is because the Sharing options override and apply to shared drives.

****Help Center resources****

* [Manage shared drives](https://support.google.com/a/topic/7337266" \o "Manage shared drives" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #7 - Explore Shared Drive Management**

****Introduction****

As the administrator you have visibility and can manage all shared drives in your organization.

In this exercise you will explore the management features offered to you in the admin console.

****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 ****Drive and Docs****service.

3. Click ****Migration settings****. From here you can control if your users can migrate content into a shared drive.

4. Return to the Drive and Docs service settings and click ****Manage shared drives****. From here you can see and manage all shared drives in your organization. You can:

* Manage members
* Manage shared drive settings. Note: You can also override the policy that allows full-access members to manage shared drive settings from here at the individual shared drive level.
* Restore a drive or data to a team drive

5. Hover over the shared drive that Timothy Lee created in the previous exercise and click the ****Settings**** link on the right hand side of the screen.

6. Check the 'Prevent full-access members from modifying shared drive settings' box and click ****DONE****.

7. Sign out and sign back into G Suite as Timothy Lee at [drive.google.com](https://drive.google.com/" \o "drive.google.com" \t "/home/sherwinowen/Documents\\x/_blank).

8. Click ****Shared drives**** on the left, and open the shared drive created in the previous exercise.

9. Click on the shared drive title to reveal a drop down menu, and select ****Shared drive settings****. Note how you can see the settings but you can no longer change any of them.

****Notes****

1. If you allow users to migrate content to a shared drive, they must have edit access on the files they wish to migrate, and the owner of the files must be a member of the destination shared drive.

****Help Center resources****

* [Migrate content to a shared drive](https://support.google.com/a/answer/7374057" \o "Migrate content to a shared drive" \t "/home/sherwinowen/Documents\\x/_blank)
* [Restore deleted files or shared drives](https://support.google.com/a/answer/7376096" \o "Restore deleted files or shared drives" \t "/home/sherwinowen/Documents\\x/_blank)

**MOBILE DEVICE MANAGEMENT**

## **Introduction to Mobile Device Management**

In these exercises, you'll learn about Google mobile device management settings, and understand how to enforce device policies over your mobile fleet.

You will learn how to prevent unauthorized access to an account from a lost mobile device.

There are two levels of mobile management: basic and advanced. Each level of management gives you a different set of features:

* ****Basic:**** With basic management, you can keep corporate data safe by requiring that mobile devices have a screen lock or password. You don’t need to do anything to turn on basic management as it's on by default.
* ****Advanced:****If you want more control over mobile devices that access your organization’s data, you can use advanced management to do things like enforce stronger device passwords, or restrict access to device settings and features.

****Help Center resources****

* [Manage mobile devices](https://support.google.com/a/topic/24642" \o "Manage mobile devices" \t "/home/sherwinowen/Documents\\x/_blank)
* [Set up basic mobile device management](https://support.google.com/a/answer/7400753" \o "Set up basic mobile device management" \t "/home/sherwinowen/Documents\\x/_blank)
* [Set up advanced mobile device management](https://support.google.com/a/answer/6328699" \o "Set up advanced mobile device management" \t "/home/sherwinowen/Documents\\x/_blank)
* [Compare mobile management features](https://support.google.com/a/answer/7576736" \o "Compare mobile management features" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #1 - Configure Mobile Device Policies**

****Introduction****

In this exercise you will use G Suite Mobile Management to enforce the company's mobile policies for Android devices. You will disable iOS and Google Sync devices.

****Scenario****

You receive the following message from Alex, IT Manager:

Hey G Suite Admin,

I hope I'm not keeping you too busy with my requests, but I have another urgent one for you.

Our immediate task is to make sure we secure mobile access to G Suite. We've decided to go with the "BYOD—Bring Your Own Device" strategy so our employees can use their personal mobile devices for work too using a work profile. But they'll need to adhere to our security policies. I've read that you can enforce these policies with G Suite Mobile Management.

I've decided to go with Google's best practices and define a standard set of access policies across all devices and organizations with emphasis on password settings. Mobile policies can be adjusted later, if necessary.

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 ****Devices**** icon.

3. Click the ****Setup**** link on the left.

4. Click ****Mobile Management**** and ensure that 'Enable Mobile Management' is Enabled.

5. Select Custom and set 'Android' to Advanced, and iOS and Google Sync to Unmanaged.

6. Click ****SAVE**** if you have made any changes.

7. Scroll down and click ****Device Approvals****. Confirm 'Requires Admin approval' is checked.

8. Click ****SAVE**** if you have made any changes.

9. Scroll down and click ****Sync on Mobile****. Enable 'Android Sync' but deselect 'iOS' and 'Google Sync'.

10. Click ****SAVE****.

11. Return to the 'Device management' screen and click the ****Advanced Settings**** link on the left.

12. Click ****Security**** and ensure that 'Block Compromised Android devices' is selected and that 'Allow camera' is deselected.

13. Click ****SAVE****.

14. Return to the 'Device management' screen and click the ****Android Settings**** link on the left.

15. Click ****Work Profile****.

16. In the 'Work Profile Setup' section, set 'Work Profile in Android for Work supported devices' to Enforce. By enforcing the creation of a work profile users can’t sync corporate data unless they accept the work profile, and they don’t have the option to opt out.

17. Click ****SAVE**** if you have made any changes.

Congratulations. You’ve set up advanced mobile management for your organization. Users can enroll their devices for management by adding their corporate account to a device. After users enroll their devices, you can see the device in the admin console. There, you can manage the device, apply settings, monitor it, and more.

****Notes****

1. To enforce these policies on Android devices, your users must install the [Google Apps Device Policy](https://play.google.com/store/apps/details?id=com.google.android.apps.enterprise.dmagent" \o "Google Apps Device Policy" \t "/home/sherwinowen/Documents\\x/_blank) app on their device. This app ensures that your domain policies are set properly on the user's Android device before synchronizing any data. See [Google Apps Device Policy overview](https://support.google.com/a/users/answer/190930" \o "Google Apps Device Policy overview" \t "/home/sherwinowen/Documents\\x/_blank) for more details. If the app isn't already installed when the user adds their corporate account to their phone, the app is typically installed automatically as part of the sign up process.

****Help Center resources****

* [Apply settings for Android mobile devices](https://support.google.com/a/answer/6328708" \o "Apply settings for Android mobile devices" \t "/home/sherwinowen/Documents\\x/_blank)
* [Control what devices can access your data](https://support.google.com/a/answer/6328712" \o "Control what devices can access your data" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #2 - Enroll a Mobile Device**

****Introduction****

Now that you’ve configured your mobile device policies, we’ll walk through the steps that your users, and you, as the administrator for your organization, take to enroll mobile devices into your domain.

This exercise is optional. Only complete the exercise if you are comfortable adding a new account and work profile to your personal mobile device. If you have any concerns DO NOT complete this exercise but do read the process. Remember, if you do choose to add your own device, you will need to consider removing the account from your phone or from your domain after you’ve finished this training.

Start by ensuring you have read [Get started with Google Mobile Management](https://support.google.com/a/answer/7396025" \o "Get started with Google Mobile Management" \t "/home/sherwinowen/Documents\\x/_blank)

Now that you have configured mobile device management for your organization you will need to inform your users that they can add their corporate Google account to their personal device. After the user has enrolled you will be able to see their device in the admin console.

****Directions****

The process of adding a new account and removing the account/work profile does vary from device to device and across different versions of Android so it is not possible to provide detailed steps for every device. However, in general you will work through the following steps:

1. From your phone go to ****Settings > Accounts****

2. Click ****Add Account > Google****

3. Sign in with your training credentials. You may need to accept Google's Terms of Service at this point.

4. Install the Google Apps Device Policy app.

5. Create the work profile. If your organization requires that devices must be approved, you will be advised that the device is pending approval.

Approving a device

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 ****Devices**** icon.

3. Click the ****Device Approvals**** link on the left. From here you can see any devices pending approval.

4. To approve a device, locate it in the list and hover over it, then click the ellipses (three vertical dots) at the end of the row and click ****APPROVE DEVICE****. The user will receive a notification once the device is approved and they can then start to use their work profile alongside their personal account.

****Help Center resources****

The exercises here covered the use of personal devices at work. Read the article below to find out more about managing company-owned devices from the admin console.

* [Inventory company-owned devices](https://support.google.com/a/answer/7129612" \o "Inventory company-owned devices" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #3 - Handling a Lost or Non-Compliant Device**

****Introduction****

Don't worry if you didn't complete the previous exercise as you will not be wiping or blocking any devices today. This exercise just shows you where to go to manage a device that is believed to be lost or non-compliant and lists the actions that are available to you in the admin console.

If a user loses a computer or mobile device that has an open connection to that user's G Suite account, or maintains cookies that permit a connection without first entering a username and password, that G Suite account is potentially exposed to anyone who has possession of the computer or device.

Below, you will see the steps for both wiping a user’s device, and blocking a non-compliant device.

****Directions****

Option 1: Device management - Wiping and blocking a device

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 ****Devices**** icon.

3. Click the ****Mobile devices**** icon. From here you can see details of your mobile devices such as the device name, owner details, OS version and status.

If a user has lost a device or it is believed to have been compromised you have the following options:

* Block device
* Wipe account
* Delete device

The action you choose will depend upon the type of device (personal or company-owned) and the situation that is presented. See [Remove corporate data from a device](https://support.google.com/a/answer/173390" \o "Remove corporate data from a device" \t "/home/sherwinowen/Documents\\x/_blank) for more information.

Option 2: Using a device management rule

When a device falls out of compliance with your organization’s policies, you can automatically block it from accessing corporate data and notify the user. For example, if you enforce a minimum password length and a user's password is shorter than the length required, the device is not compliant because it doesn’t adhere to your password policy.

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 ****Rules**** icon.

3. Click the ****Device management rules**** icon.

4. Click ****ADD A RULE NOW**** or the yellow circle with the + sign to add a new rule. From here you can create a new rule from a blank template, or a rule based on an existing template.

5. Examine an existing template, e.g: 'Block account on multiple failed screen locks'. By selecting it you will be making a copy of it to create your own template.

Note the conditions and actions available:

* Users: The rule can be applied to OUs or Groups
* Filters: You can filter by OS and on a number of device events such as 'Failed screen unlock attempts'
* Actions: You can email super administrators and block or wipe the device if conditions are met

6. Do not save the new rule. Click ****DISCARD****.

Option 3: Reset a users sign in cookies

To block unauthorized access to an account, you can reset the sign-in cookies for that user, which has the effect of signing that user out from all current HTTP sessions, and requiring new authentication the next time that user tries to initiate an HTTP session to sign in to G Suite.

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 ****Users**** icon.

3. Locate the user in the list and click on the name, and click the ****Security**** card.

4. Click on the ****Sign-in cookies**** row, and click ****RESET****.

****Help Center resources****

* [Block access to your Google service on a lost device](https://support.google.com/a/answer/178854" \o "Block access to your Google service on a lost device" \t "/home/sherwinowen/Documents\\x/_blank)
* [Remove corporate data from a device](https://support.google.com/a/answer/173390" \o "Remove corporate data from a device" \t "/home/sherwinowen/Documents\\x/_blank)
* [Automate mobile management tasks with rules](https://support.google.com/a/answer/7425191" \o "Automate mobile management tasks with rules" \t "/home/sherwinowen/Documents\\x/_blank)

**ENHANCED DESKTOP SECURITY FOR WINDOWS**

## Introduction to Enhanced Desktop Security for Windows

In this lesson, you'll be introduced to Google’s Enhanced desktop security for Windows.

Enhanced desktop security for Windows allows users to sign into their Windows devices using their Google credentials. It also offers a comprehensive set of device management options which allows you, as the G Suite administrator, to manage all your devices, desktop and mobile from your admin console.

Enhanced desktop security for Windows has two complementary features that can be set up together or individually:

* ****Google Credential Provider for Windows (GCPW)****: Allows the use of Google account authentication on Windows 10 devices. Also delivers a single sign-on (SSO) experience, allowing users to sign in once to access Google resources and many other 3rd party applications.
* ****Windows device management****: Manage Windows settings on enrolled devices.

Enhanced desktop security for Windows requires Windows 10 Pro, Pro for Workstations, Enterprise, or Education, version 1803 or later. For GCPW, Chrome Browser 81 or later is required.

Let’s start with an overview of Windows device management in G Suite.

#### **VIDEO : INTRODUCTION TO ENHANCED DESKTOP SECURITY FOR WINDOWS**

## **Google Credential Provider for Windows**

The Google Credential Provider for Windows (GCPW) is a core component of Google’s Enhanced desktop security for Windows.

GCPW allows your users to sign in to a Windows device using their Google account credentials. You can configure GCPW so that a user’s Google account syncs with their Active Directory or local Windows profiles.

GCPW also provides the following benefits:

* ****Additional security****: Users get all the security benefits of their Google Account on their Windows 10 device. These features include anti-hijacking features such as 2-step verification (2SV) and login challenges.
* ****SSO experience****: Users can access Google services and SSO apps in Chrome Browser without the need to re-enter their Google credentials.
* ****Password synchronization****: Keep users’ Google passwords in sync with their Windows passwords in the Admin console or with G Suite Password Sync.
* ****Automatic enrollment in Windows device management****: If you use GCPW and Windows device management, devices can be automatically enrolled in Windows device management when the user signs in and activates GCPW.
* ****Admin actions:**** Such as viewing device details and signing users out of their Google account.

To use GCPW, you need to install it on each Windows device.

In the video that follows, you will discover some of the key features provided as part of GCPW. You will also see a demonstration of the initial sign in experience once GCPW has been installed onto a Windows device. You will also be given an insight into how the login process works behind the scenes to deliver the single sign on experience to the user.

****Help Center resources****

* [Setup GCPW](https://support.google.com/a/answer/9541083?hl=en" \l "setup" \t "/home/sherwinowen/Documents\\x/_blank)
* [Sign in to Windows after GCPW installation](https://support.google.com/a/answer/9250915" \t "/home/sherwinowen/Documents\\x/_blank)

#### **VIDEO : Google Credential Provider for Windows**

## Windows Device Management

With Windows device management, you can configure and manage enrolled devices from the admin console.

In the video that follows we will discuss:

* how to apply Windows settings on your devices. Note, that settings can be applied at the organizational unit (OU) level.
* how to manage your device inventory, including common actions that can be applied to a device.

****Help Center resources****

* [Setup Windows device management](https://support.google.com/a/answer/9541083?hl=en" \l "setup" \t "/home/sherwinowen/Documents\\x/_blank)

#### **VIDEO : Windows Device Management**

## Prepare and Deploy Enhanced Desktop Security for Windows

Now we will take a look at how you should prepare your environment to use Enhanced desktop security for Windows.

You can set up Google Credential Provider for Windows (GCPW) and Windows device management together, or you may choose to deploy just one of the two components.

Let’s start by looking at how to prepare each component.

****Prepare to use Windows Device Management****

To enable Windows device management in your environment, you must:

1. Configure your Windows device settings. This involves specifying:

* the permissions each user is granted to their device, plus any users and groups that require local admin privileges. For example, you may want to grant these privileges to your support teams.
* how the devices are to be encrypted
* how and when Microsoft updates are applied to your devices

You should understand [how to use custom settings](https://support.google.com/a/answer/9539385" \t "/home/sherwinowen/Documents\\x/_blank) with your Windows devices, and for a list of common custom settings that can be applied, please refer to this [article](https://support.google.com/a/answer/9852044" \t "/home/sherwinowen/Documents\\x/_blank).

See [Apply Windows settings](https://support.google.com/a/topic/9541297" \t "/home/sherwinowen/Documents\\x/_blank) for details.

2. Enable the Windows management service in the admin console. See [Enable Windows device management](https://support.google.com/a/answer/9539506" \t "/home/sherwinowen/Documents\\x/_blank) for details.

****Prepare GCPW for your devices****

Before you install GCPW onto your Windows devices, you will need to:

1. Decide upon your password management strategy. As part of this, you should consider password complexity.
2. Optionally, associate your user’s Google accounts with the appropriate Windows profiles. See [Associate Google accounts with existing Windows profiles](https://support.google.com/a/answer/9796679" \t "/home/sherwinowen/Documents\\x/_blank) for more information.

See [Prepare to install GCPW](https://support.google.com/a/answer/9543613?hl=en&ref_topic=9539498" \t "/home/sherwinowen/Documents\\x/_blank) for details.

After you complete the preliminary setup steps, you can install GCPW.

****How to deploy and configure GCPW****

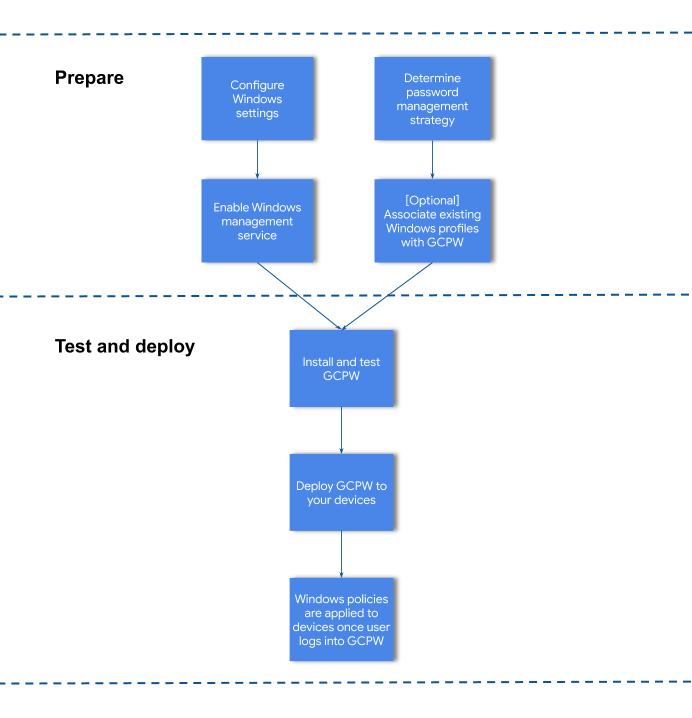
GCPW can be downloaded, installed and configured manually, or you can use a PowerShell script to download, install and configure the software. Depending upon your environment, you may choose to distribute the software though an existing software distribution tool. See [Install Google Credential Provider for Windows](https://support.google.com/a/answer/9250996?hl=en&ref_topic=9539498" \t "/home/sherwinowen/Documents\\x/_blank) for details.

Whichever method you choose, you should ensure that you test GCPW in your environment before you deploy to a large number of devices.

Once GCPW has been installed onto a device, when the user next signs in using GCPW for the first time, the device is auto enrolled into Windows management and the Windows settings will be pushed to the device. See [Sign in to Windows after GCPW installation](https://support.google.com/a/answer/9250915" \t "/home/sherwinowen/Documents\\x/_blank) for more details.

****Enhanced Desktop Security for Windows Implementation Flow****

The diagram below shows each stage of the implementation.



Note how the preparation work for Windows device management and GCPW can take place simultaneously.

****Help center resources****

* [Configure Windows settings](https://support.google.com/a/topic/9541297" \t "/home/sherwinowen/Documents\\x/_blank)
* [Enable Windows management service](https://support.google.com/a/answer/9539506" \t "/home/sherwinowen/Documents\\x/_blank)

[Determine password management strategy](https://support.google.com/a/answer/9543613" \t "/home/sherwinowen/Documents\\x/_blank)

**Video : Enhanced Desktop Security for Windows Deployment Scenarios**

**GOOGLE VAULT**

## Introduction to Google Vault

Google Vault is a service that lets you retain, hold, search, and export data to support your organization’s archiving and eDiscovery needs. Vault is used for:

* ****Archiving****: Set retention rules to control how long data is retained before being removed from user accounts and deleted from Google systems. See [How retention works](https://support.google.com/vault/answer/2990828" \o "How retention works" \t "/home/sherwinowen/Documents\\x/_blank)
* ****Legal holds****: Place holds on users to preserve their data indefinitely in order to meet legal or other retention obligations. Learn about holds. See [Place Gmail messages on hold](https://support.google.com/vault/answer/2473591" \o "Place Gmail messages on hold" \t "/home/sherwinowen/Documents\\x/_blank)
* ****Search and Export****: Search your domain's data by user account, organizational unit, date, or keyword. Vault supports Boolean and wildcard operator searches. See [Get started with Vault search and export](https://support.google.com/vault/answer/6161352" \o "Get started with Vault search and export" \t "/home/sherwinowen/Documents\\x/_blank)

Vault supports Gmail, Drive, Groups, Google Chat and Classic Hangouts (with history on), and Google Meet.

In these exercises you will explore the key features of Google Vault. You will set up a default and custom retention rule, after which you will create a matter and place accounts on legal hold. Finally you will look at how you can search and export data using Vault. Please ensure that you read the Help Center resources below.

****Help Center resources****

* [Get started: Vault administrators](https://support.google.com/vault/answer/2584132" \o "Get started: Vault administrators" \t "/home/sherwinowen/Documents\\x/_blank)
* [Supported data types](https://support.google.com/vault/answer/6127699" \o "Supported data types" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #1 - Create Retention Rules**

****Introduction****

Before Vault will preserve data you must have a retention rule. There are two types of retention rules:

**Default**: This global rule applies to your entire organization. You can define a default retention rule for each type of data supported. Default rules define how long to keep data and what to do with the data once the time has elapsed. Default rules are only triggered if no custom rules or holds apply.

**Custom**: Custom rules offer more flexibility than the default rules. For example you can create a custom rule and apply to OUs. You can set date ranges and enter search terms to match data such as Gmail messages. Custom rules always override the default rule, and if multiple retention rules apply to a message or file, it is retained according to the rule with the longest retention coverage period.

****WARNING:****An improperly configured retention rule can cause the immediate and irreversible purging of data from user accounts. Use caution when creating or changing retention rules. We recommend that you test new rules on a small group of users before applying them to your entire organization.

In this exercise we will define a default and a custom retention rule for Gmail.

****Scenario****

You receive the following email from the Sam Morse:

Hello G Suite Admin,

I have been thinking about how we retain information in G Suite. I want to ensure that we retain our email for a year even if the email has been deleted from the user account. At the same time I would like to keep executive emails for 5 years. I understand that G Suite offers us the capability to do that. Can you make this happen?

Regards,

Sam Morse, CEO

****Directions****

Sam wants all mail to be archived for a period of one year after which it can be expunged. Messages from any executives should be retained for 5 years. We'll start by creating a custom rule that will apply to the executive only.

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. Open a new browser tab and open [ediscovery.google.com/discovery](https://ediscovery.google.com/discovery/" \o "Google Vault" \t "/home/sherwinowen/Documents\\x/_blank). This will open Google Vault.

3. From the left menu, click ****Retention****, then click ****CREATE RULE****.

4. In the 'Type' field, select Mail.

5. Select the Executive OU.

For the purposes of this exercise you can skip the conditions section. This section however is useful if you want to define date criteria or search terms for this rule.

6. Change the duration value from Indefinitely to 1825 days (5 years) and ensure 'Expunge only the messages that users have already deleted.' is selected.

7. Click ****Save****. Read the informational messages that follow, tick them and click ****Confirm**** to create the rule.

This custom rule will expunge any message over 5 years old that the user has already deleted. This rule is applied to the Executive OU only. Now we will add the default rule.

8. From the left menu, click ****Retention**** and under the Default retention rules, click ****Mail****.

9. Check the 'Set a default retention rule for Mail' box. You can now choose how long to keep messages.

10. Change the default value from Indefinitely to 365 days and select 'Expunge only the messages that users have already deleted'. Note: If you choose the second option this rule may expunge messages that users want to keep.

11. Click ****Save****. Read the informational messages that follow, tick them and click ****Confirm**** to create the rule.

The default rule above will automatically expunge all deleted messages after 1 year. Note that the custom rule we created initially overrides the default rule so the Executive OU's deleted messages are retained for 5 years

****Notes****

1. The Gmail service includes a compliance setting 'Email and chat auto-deletion' that allows the administrator to automatically delete email and chat after a specified number of days. You should not use this feature alongside Vault. More details can be found in the [Control email and chat message storage](https://support.google.com/a/answer/151128" \o "Control email and chat message storage" \t "/home/sherwinowen/Documents\\x/_blank) article.

## **Exercise #2 - Create a Matter and Place Users on Hold**

****Introduction****

In Google Vault, a matter is a container for all of the data related to a specific topic, such as a litigation case or investigation. A matter includes:

* Saved search queries
* A list of accounts with data on litigation hold
* A list of the accounts that can access the matter
* Export sets for the matter
* An audit trail for the matter

In this exercise you will create a matter and place two user accounts on hold.

****Scenario****

You receive the following email from the Sam Morse:

Hello G Suite Admin,

We have an issue with Project X and I need to ensure we retain all relevant emails relating to this project. I know we expunge messages over one year old but I need them to be retained until the situation is resolved for the following employees.

lars.ericsson@yourdomain, jon.baird@yourdomain

Regards,

Sam Morse, CEO

****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. Open a new browser tab and open [ediscovery.google.com/discovery](https://ediscovery.google.com/discovery/" \o "Google Vault" \t "/home/sherwinowen/Documents\\x/_blank). This will open Google Vault.

3. From the left menu, click ****Matters****, then click ****CREATE**** and in the dialog box presented enter a 'Matter name' of Project X then click ****Create new matter****.

4. Click ****CREATE HOLD**** and enter a 'Name' of Project X related messages.

5. Select the 'Type' or ****Mail****.

6. Ensure 'User' is set to Accounts and enter the following email addresses into the box below:

lars.ericsson@yourdomain, jon.baird@yourdomain

You could at this point use the conditions section to refine the data to hold. For example, if Project X only started 2 months ago you might want to retain only messages after the project started, or you might want to use search terms to hold only messages that make reference to Project X. See [Use search operators](https://support.google.com/vault/answer/2474474" \o "Use search operators" \t "/home/sherwinowen/Documents\\x/_blank). In this case however, we will retain all messages for the two accounts above.

7. Click ****Save****.

Messages for the two users will now be retained until the hold is lifted. At this point you can share the hold from the hold list. You can also edit the hold as needed.

## **Exercise #3 - Search and Export**

****Introduction****

Now that you have created a matter, you will probably want to investigate further so you will want to search and then potentially export results for analysis. In this exercise, you will look at the search options available in Vault and export results.

Tip: Check out the video at the top of the [Get started with search and export](https://support.google.com/vault/answer/6161352" \o "Get started with search and export" \t "/home/sherwinowen/Documents\\x/_blank) article to see search and export in action.

****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. Open a new browser tab and open [ediscovery.google.com/discovery](https://ediscovery.google.com/discovery/" \o "Google Vault" \t "/home/sherwinowen/Documents\\x/_blank). This will open Google Vault and you should see a list of your matters. if you do not see the Project X matter, click ****Matters > My matters****.

3. Hover over and click onto the Project X matter row to open it.

4. Click ****Search****. Explore the search options available. Note that you can also get a count of your search results before you search (as searches can take some time) and you can also export directly from the search page.

5. Run a search (any search you like as long as you get some results).

Once you have some results you can save your query for later, or export your results.

6. From the search results, click ****Export results****. You must give the export a name and you can choose the output format for later analysis.

****Notes****

1. Exports are available for 15 days so you should download them immediately when they become available.

2. You can delete the export once you have downloaded it or allow it to be purged automatically.

****Help Center resources****

* [Get started with search and export](https://support.google.com/vault/answer/6161352" \o "Get started with search and export" \t "/home/sherwinowen/Documents\\x/_blank)

**REPORTING**

## Introduction to Reporting

As the G Suite administrator, you can run a variety of different reports that will provide you and your leadership with in-depth views of your organization's usage of G Suite.

In these exercises, you'll learn about the reporting features in G Suite. Ensure you explore the Help Center resources.

****Help Center resources****

* [About reports and alerts](https://support.google.com/a/topic/9026900" \o "About reports and alerts" \t "/home/sherwinowen/Documents\\x/_blank)
* [Admin audit log](https://support.google.com/a/answer/4579579" \o "Admin audit log" \t "/home/sherwinowen/Documents\\x/_blank)
* [Email Log Search](https://support.google.com/a/topic/2618873" \o "Email Log Search" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #1 - Monitor G Suite Usage**

****Introduction****

You can monitor G Suite usage via the admin console and Reports API. For the purpose of this exercise, we'll focus on the admin console.

As an administrator, you will want to examine potential security risks, measure user collaboration, track who signs in and when, analyze administrator activity, and much more. The admin console provides tools that you can use to analyze usage data. Reports have interactive graphics and tables that show broad, domain-level data alongside granular, user-level details.

You can hover your cursor over graphics to see specific data, set filters to adjust the scope of the data each report covers, and click table cells to see accompanying graphical representations.

You should note however that because you have only recently set up your domain, there will be limited data or no data available to view in many reports.

In this exercise you will explore some of the more common reports that you can use to determine G Suite usage in your organization.

****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 ****Reports**** icon.

View a summary of user activity

The default view gives you the highlights of your user’s app usage along with high level summaries of other reports such as the user security report. From here you can adjust the report's time frame and use the links provided to drill into more detailed reports.

View and customize the security report

3. Click on ****Users > Security****.

The main report is split into two sections: a chart above which shows changes in a category over time, and a table below which shows per-user information. On the left hand side of the page you will see the Filters pane. There are also a number of icons on the top right of the page from where you can:

* Download the report or export to Google Sheets
* Choose which columns to display (vertical column bars)
* Show/Hide the filter pane. (horizontal striped triangle)

4. Try adding a new column to the list of columns displayed. Click the vertical column bars on the top right of the page, select ****Public shares****, then click ****APPLY****.

Note: When you add a column to the table, it is also added as a category that can be applied to the chart at the top of the page.

5. Take a look at the filters pane. From here, you can set date criteria. You can also filter by OU or user, and add column constraints. Try searching on the 'Employees' OU where the 'User Account Status' is 'Active'. This filter should return Ellie, Jon, Tom and Will.

Did you notice that you must add the 'User Account Status' column to the report before you can filter by it?

View trends and administrative data

As the administrator, you can use app reports to review trends or see an overview of administrative information. The reports generate a series of charts and graphs that display information for all users in your organization. To view user-level data instead, see [Account activity reports](https://support.google.com/a/answer/4580176" \o "Accoun activity reports" \t "/home/sherwinowen/Documents\\x/_blank).

6. From the Reports page, click ****Apps**** and select a report. See [Understand app reports data](https://support.google.com/a/answer/6072773?hl=en&ref_topic=7558954" \l "understand" \o "Understand app reports data" \t "/home/sherwinowen/Documents\\x/_blank).

7. Take a look at the Gmail report. This shows total emails sent and received over time. You can use the 'Select reports' icon (vertical column bars) on the top right of the page to get insights into other metrics such as spam and encrypted messages.

8. Now look at the Accounts report. This shows metrics that include users status. Again here, you can use the 'Select reports' icon to select/deselect the reports that you want to show on this page.

View your users' account status and activity

You may want to get a consolidated view of user status and account activity. The account activity report page gives access to all data from the User account status, Admin status, and 2-Step Verification enrollment reports. It also shows details of Google Drive and Gmail usage.

9. From the Reports page, click ****Users > Account activity****. You'll note that this is very similar to the security report where you can adjust the columns displayed and set filters and conditions for the report. Try filtering the report and look for users with the Super Admin role.

****Help Center resources****

* [Highlights report](https://support.google.com/a/answer/6000244" \o "Highlights report" \t "/home/sherwinowen/Documents\\x/_blank)
* [App reports on your whole organization](https://support.google.com/a/answer/6072773" \o "App reports on your whole organization" \t "/home/sherwinowen/Documents\\x/_blank)
* [Account activity reports](https://support.google.com/a/answer/4580176" \o "Accoun activity reports" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #2 - View Audit Logs**

****Introduction****

As the administrator, you want to be aware of changes being made to your organization.

The audit section allows you to quickly review the various events which are generated by administrators, users and services and help give you a deeper understanding of how your users are interacting with your services.

You should note however that because you have only recently set up your domain, there will be limited data or no data available to view in many reports.

In this exercise you will take a brief look at the audit logs available to you for your organization.

****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 ****Reports**** icon.

3. Click ****Audit > Admin**** and explore the Admin audit log. From here you can see a record of all actions that have been performed in the admin console. For example, you can see user creations, changes made to service settings, etc. You can constrain the report by OU and date criteria and also filter by Event name, User name, and Admin name..

4. Use the ****Add a filter**** button to filter by the User Creation event.

5. Click ****CLEAR FILTERS**** to clear the search filter.

6. Go back to the Reports page and click ****Audit > Calendar****. From here you can track changes to calendars, events, and subscriptions in the Google Calendar audit log. Notice how the filter choices have changed from the previous report.

7. Explore some of the other audit reports and you will see how the filters provided are relevant to the type of data shown in the current report.

****Help Center resources****

* [Understand audit logs](https://support.google.com/a/topic/9027054" \o "Understand audit logs" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #3 - Create Email Alerts**

****Introduction****

While it's useful to view events in the admin console audit log, it's probably more helpful to be alerted immediately of significant changes, such as when a user is deleted or suspended, or if settings are changed.

You can receive email alerts when something important happens in your organization, such as a suspicious sign-in attempt, a compromised mobile device, or when another administrator changes settings. When you turn on an alert for an activity, you'll receive an email each time that activity happens, up to 25 emails in 2 hours.

In this exercise, you'll examine G Suite's predefined alerts and see how to create a custom email alerts for when something important happens in your organization.

****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 ****Rules****icon, then click the ****Security rules**** card. From here you can see the predefined rules and the status and action to take for each rule.

System defined rules

3. Scroll through the predefined rules to see the different types of alerts you can receive.

4. Click on any alert to see more details. Hover over the 'Rule details and scope', 'Conditions' and 'Actions' cards.

Notice how you can only change the 'Actions' to take for a System defined rule. You can enable/disable the rule, set the severity and manage the users that will receive the notification when the rule is triggered.

Create a custom rule

In addition to the predefined alerts you can create your own rules. Let's create a rule to check for Late spam classification.

5. Click ****NEW RULE > Activity.****

6. In the 'Rule name' field, enter Late spam classification.

7. Click ****NEXT: VIEW CONDITIONS****.

8. Set the 'Data source' to Gmail log events. In the conditions row, change the second 'Event' box to Late spam classification, then click ****NEXT: ADD ACTIONS****.

The Actions page allows you to set thresholds to apply before the rule is triggered. You can also add actions. For example, you might want to delete the message or send it to quarantine.

9. Set the 'Action' to Send to quarantine.

10. Move the 'Alerting' slider to the ON position, choose a severity, and check the 'All super administrators' box.

11. Click ****NEXT: REVIEW**** to review your new rule. Notice how you can choose to run in Monitor or Active modes.

12. Click ****CREATE RULE**** to add the custom rule and confirm you can see your new rule in the list.

****Help Center resources****

* [View and manage security rules](https://support.google.com/a/answer/9420866" \o "View and manage security rules" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #4 - Email Log Search**

****Introduction****

G Suite allows you to sort through the last month of email delivery activity and evaluate message transit.

This is useful for tracking a sender or recipient's missing messages, such as those that have been quarantined as spam or otherwise routed incorrectly. Use the Email Log Search feature to troubleshoot how Gmail policies affect mail flow.

You start by performing a search of the log, then you examine the results - analyse route and delivery states. You can also see post delivery status such as message labels.

In this exercise you will explore the Gmail Log Search options available in the admin console. Ensure you read the Help Center resources.

****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 ****Reports**** icon.

3. Click ****Audit > Email Log Search****.

4. Explore the search options:

* Date (Note that detailed delivery information is only available for messages received in the last 30 days)
* Search by sender or recipient or their IP addresses
* Search by subject or message ID

5. Perform a search for messages received by yourself in the last 7 days. Note: It can take an hour for messages to be logged.

6. Click on any valid message. From here you can view message and recipient details. You can also view the post delivery message details such as read status, labels, etc. Note: You cannot see the actual message.

****Notes****

1. You can search for messages older than 30 days but you must know the message ID and detailed delivery logs are not available for these messages.

****Help Center resources****

* [Track message delivery with Email Log Search](https://support.google.com/a/answer/2618874" \o "Track message delivery with Email Log Search" \t "/home/sherwinowen/Documents\\x/_blank)
* [View Email Log Search result details](https://support.google.com/a/answer/2618876" \o "View Email Log Search result details" \t "/home/sherwinowen/Documents\\x/_blank)
* [Interpret Email Log Search results](https://support.google.com/a/answer/2623280" \o "Interpret Email Log Search results" \t "/home/sherwinowen/Documents\\x/_blank)
* [Post-delivery message status](https://support.google.com/a/answer/2623280" \l "post-delivery" \o "Post-delivery message status" \t "/home/sherwinowen/Documents\\x/_blank)

**Domain Management**

## Introduction to Domains

When you signed up for your G Suite account you associated it with a primary domain.

In addition to your primary domain you can:

* Add up to **20 domain aliases** to the primary domain
* Add an additional **599 secondary domains**

****Domain alias:**** A domain alias gives each user in the primary domain an additional email address. For example, let's say you have a primary domain yourcompany.com and you also own yourcompany.co.uk. You add yourcompany.co.uk as a domain alias. All users in yourcompany.com can now send and receive email from/to yourcompany.co.uk. There are no additional license costs for a domain alias as there are no new accounts created.

****Secondary domains:**** This a new domain which you purchase into which you add new users each of which requires a license. Secondary domains are useful for managing separate teams or businesses at different domains.

In this lesson you'll learn about adding domains to your G Suite account. Ensure that you read through the Help Center articles linked below.

****Notes****

1. Just like you did for your primary domain, you must verify ownership of any domain alias or secondary domain you wish to add to your G Suite account.

****Help Center articles****

* [What is a domain?](https://support.google.com/a/answer/177483" \o "What is a domain?" \t "/home/sherwinowen/Documents\\x/_blank)
* [Add more domains to your G Suite or Cloud Identity account](https://support.google.com/a/answer/7502379" \o "Add more domains to your G Suite or Cloud Identity account" \t "/home/sherwinowen/Documents\\x/_blank)
* [Remove a domain or domain alias](https://support.google.com/a/answer/183028" \o "Remove a domain or domain alias" \t "/home/sherwinowen/Documents\\x/_blank)
* [Domain name basics](https://support.google.com/a/answer/2573637" \o "Domain name basics" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #1 - Add a Domain Alias or Additional Domain**

****Introduction****

This exercise can only be completed if you own another domain that you wish to add to your G Suite account. If you do not own a domain, just read through the instructions to familiarise yourself with the process.

Your organization is preparing to expand their business and will be purchasing a domain that they'll use as an alias.

This means that each user in the primary domain will automatically have an alias in the new domain. For example, Lars Ericsson can receive email as lars.ericsson@yourdomain.com or as lars.ericsson@yourdomain.org. All of his messages will go to the same inbox.

This exercise will give you practice adding a domain alias so that you understand the process before you actually purchase a new domain.

****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 ****Domains**** icon, then click the ****Manage Domains**** card.

3. Click ****Add a domain alias****.

4. Enter the domain alias of yourdomain.org and click ****CONTINUE AND VERIFY DOMAIN OWNERSHIP****.

5. Verification steps can vary depending upon the domain name provider. In some cases Google will redirect you to sign into your registrar and can verify your domain automatically. In other cases you will need to follow the instructions on the screen and manually update your DNS records. These would typically be:

* Select your domain name provider (registrar)
* Add a Google site verification TXT record to your DNS records
* Verify from the admin console.

As you can see, adding a new domain or domain alias is straightforward.

****Help Center resources****

* [Limitations with multiple domains](https://support.google.com/a/answer/182081" \o "Limitations with multiple domains" \t "/home/sherwinowen/Documents\\x/_blank)
* [Multiple domains FAQ](https://support.google.com/a/answer/175747" \o "Multiple domains FAQ" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #2 - Whitelist a Domain**

****Introduction****

As the administrator, you can let users work in ****certain**** Google products with users from other G Suite domains outside of your organization. For example, you can allow file sharing in Google Drive with organizations that you trust by first whitelisting their domain, then granting them sharing access. Users in trusted organizations can also share their files with users in your domain.

****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 ****Domains**** icon, then click the ****Whitelisted domains**** card.

3. Click ****Add new****, enter the name of a trusted domain you want to whitelist and click ****ADD DOMAIN TO WHITELIST****.

****Notes****

1. Whitelisted domains must be G Suite domains only.

2. A primary domains' subdomains and domain aliases aren't included when you whitelist a domain. You must add each domain individually if needed.

3. You can turn whitelisting off or on at the organizational unit level but the domain whitelist applies to the whole organization (all OUs). There aren't separate whitelists for each OU.

****Help Center resources****

* [Whitelist trusted G Suite domains](https://support.google.com/a/answer/6160020" \o "Whitelist trusted G Suite domains" \t "/home/sherwinowen/Documents\\x/_blank)