**G Suite Security**

## **Welcome and Getting Started Guide**

****Introduction****

Welcome to the G Suite Security course.

In this course you will focus on the various aspects of G Suite security including user password policies and how to enable and enforce two step verification (2SV) for your users. You will learn about application security and understand how to whitelist and block API access to your account. You will see how G Suite can easily be integrated with a number of predefined 3rd party applications. You will also become familiar with the SSO options in G Suite. Finally you will understand how to spot potential security risks within your organization and learn how to address them using the tools available in the admin console.

In order to pass the quizzes, please remember to read the help center resources provided.

****Prerequisites****

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

If you have completed the previous courses but no longer have your trial domain, you should complete the exercise that immediately follows this reading before moving onto the next lesson. If your trial domain is still valid you can go straight to [Introduction to Common Security Settings](https://www.coursera.org/learn/g-suite-security/supplement/0Ga0f/introduction-to-common-security-settings" \o "Introduction to Common Security Settings" \t "/home/sherwinowen/Documents\\x/_blank).

**COMMON SECURITY SETTINGS**

## **Introduction to Common Security Settings**

As an administrator, there are some basic security settings you can enable and adjust in the admin console to improve the overall security of your organization, data and users.

In this lesson you will explore settings such as password policies and recovery options, and options to add secondary checks during the user sign in process which are designed to protect accounts from being compromised.

You will learn how to manage an individual user's security properties in the admin console and how to set session timeouts for your users.

## **Exercise #1 - Configure Common Security Settings**

****Introduction****

In this exercise, you’ll review and set security features and settings for your entire 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 ****Security****icon.

3. Click ****Basic settings****. Here we will review the settings for 2-step verification (2SV).

2SV puts an extra barrier between your business and cybercriminals who try to steal usernames and passwords to access business data. Turning on 2SV is the single most important thing you can do to protect your business. 2SV requires users to verify their identity through something they know (such as a password) plus something they have (such as a physical key or access code delivered to a device). It’s also called multi-factor authentication (MFA) or 2-factor authentication (2FA).

4. Ensure Allow users to turn on 2-step verification is checked. This makes 2SV available for your users, but DOES NOT automatically enroll them. To enroll, users need to configure their verification settings individually. We will discuss this later.

5. Click ****SAVE**** if you needed to change this setting.

6. Scroll down and click ****Password management****.

G Suite supports a number of password policies. Let's explore them.

You can enforce password strength and also set a password length policy by setting minimum and maximum length values. You can enforce the length and strength policies when your users next sign in to their account or when they next change their password. The default enforcement is when the password is next changed.

You can choose whether to allow users to reuse their old passwords although this is not recommended. Finally you can enforce password expiry although we recommend you allow passwords to never expire.

Note that you can apply these policies at the OU level.

7. Return to the ****Security**** page, scroll down and click ****Less secure apps****.

Some third party apps continue to use less secure sign-in technology. You can choose to deny access for these apps, which we recommend, or choose to allow access despite the risks.

8. Ensure that Disable access to less secure apps (recommended) is selected. Click ****SAVE**** if you need to change this setting.

Note that you can apply this policy at the OU level.

9. Return to the ****Security**** page, scroll down and click ****Account Recovery****.

This setting allows you to control whether a Super Admin can recover their account themselves using the Forgot Password link, or whether they must ask another Super Admin or Google Support to reset their password.

This setting is also where you control whether users can recover their own passwords. This is achieved through the use of a recovery email address or phone number. Note that password recovery is not available when using SSO, and 2-step verification users must use the email recovery option.

10. By default, only a domain administrator can reset a user’s password. To enable user password recovery, click ****User account recovery**** and check the Allow users and non-super admins to recover their account box, Then click ****SAVE****.

Note that you can apply this policy at the OU level.

****Help Center resources****

* [Set up password recovery for users](https://support.google.com/a/answer/33382" \t "/home/sherwinowen/Documents\\x/_blank)
* [Protect your business with 2-Step Verification](https://support.google.com/a/answer/175197" \t "/home/sherwinowen/Documents\\x/_blank)
* [Control access to less secure apps](https://support.google.com/a/answer/6260879" \t "/home/sherwinowen/Documents\\x/_blank)
* [Manage your users' password settings](https://support.google.com/a/answer/139399" \t "/home/sherwinowen/Documents\\x/_blank)
* [Create a strong password & a more secure account](https://support.google.com/accounts/answer/32040" \t "/home/sherwinowen/Documents\\x/_blank)
* [Allow super administrators to recover their password](https://support.google.com/a/answer/9436964" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #2 - Review a User's Security Settings**

****Introduction****

As a part of security best practice, we recommend you view and manage the security settings for your users in the admin console to reinforce and monitor the security of their Google accounts.

In this exercise, we’ll ensure you’re enforcing best practices by viewing your users' security settings.

****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 ****Users****icon.

3. Locate Alex Bell in the user list and click on his name, and click on the ****Security**** card. From here you can:

* Reset Alex's password.
* View the security keys enrolled by Alex. You can also add a key to his account. Note: Under normal circumstances, a user must enroll in 2SV themselves but if you as the administrator add a security key for the user, they are automatically enrolled.
* Determine if Alex has enrolled in 2SV. If he is enrolled but 2SV is not enforced, you can also disable 2SV for him.
* Edit Alex's account recovery information.
* Require a password change.
* Temporarily disable the login challenge. If there was a suspicious login session on a user account, they will be asked to verify their identity. If the authorized user can't verify their identity they are locked out of their account. As the administrator you can temporarily disable the login challenge (for 10 minutes) to allow the user to sign in.
* Reset Alex's sign in cookies. This signs the user out of all devices and browsers. This is useful if the user may have lost their phone as a primary measure of protection.
* View and revoke application-specific passwords. If your users use 2SV and need to sign in to apps or devices that don’t accept verification codes, they need application-specific passwords (ASPs) to access those apps. From the user's security card you can view their apps and remove an app's access to data. Note: This doesn't stop the user from using the app in the future. To prevent that, you should set up a whitelist of allowed apps. We will discuss that later in the course.
* View and remove access to third-party applications, for example G Suite Marketplace apps.

****Notes****

1. Your users can view and manage their own account security settings from [myaccount.google.com](https://myaccount.google.com/" \o "myaccount.google.com" \t "/home/sherwinowen/Documents\\x/_blank).

****Help Center resources****

* [Manage user security settings](https://support.google.com/a/answer/2537800" \o "Manage user security settings" \t "/home/sherwinowen/Documents\\x/_blank)
* [Security checklist for medium and large businesses (100+ users)](https://support.google.com/a/answer/7587183" \o "Security checklist for medium and large businesses (100+ users)" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #3 - Enforce 2-Step Verification (2SV) and Enroll**

****Introduction****

In an earlier exercise, you allowed your users to enroll in 2SV. In this exercise you will enforce 2SV for an OU as your company has decided to trial this feature. You will also sign in as one of your users and enroll into 2SV so that you can see the user experience.

****Scenario****

The company has established a policy that all managers must set up 2SV. Your job is to enforce 2SV for them. In this pilot you will allow any 2SV method to be applied. You may review this later and enforce the use of security keys as these are most secure.

****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 ****Security****icon.

3. Click ****Basic settings****, then click the ****Go to advanced settings to enforce 2-step verification**** link.

You can enforce 2SV now or choose a specific date. If you choose a date, users see reminders to enroll in 2SV when they sign in.

4. Click on the ****Executive**** OU (left side of the page).

5. Under 'Enforcement', choose Turn on enforcement from date, and use the date picker to choose an enforcement date. We suggest you select a date between 2 and 4 weeks from now. It's important to understand that users who have not enrolled by the enforcement date will be locked out of their accounts so give sufficient time for everyone to enroll. You can check enrollment status by viewing the [Enrollment report](https://admin.google.com/AdminHome" \l "Reports:subtab=security" \o "Enrollment report" \t "/home/sherwinowen/Documents\\x/_blank) in your admin console. The report can take 48 hours to update but you can always check an individual user's enrollment status from their user' security settings card on their profile.

6. Ensure that 'Allow 2-step verification methods' is set to Any, then click ****SAVE****.

At this point you would typically want to send instructions to your users advising them how to enroll. For the purposes of this exercise however, let's play the part of someone in the Executive OU and see how easy it is to enroll into 2SV.

Enroll into 2SV

Now that you have enabled enforcement, users in the Executive OU will see an interstitial page each time they log in and receive reminder emails until they enroll. Let's verify that works and then enroll as one of the Executive. The following steps are optional if you do not have a phone available or if you prefer not to enroll a user using your phone number.

7. Sign out and sign back in to G Suite at [mail.google.com](https://mail.google.com/" \o "mail.google.com" \t "/home/sherwinowen/Documents\\x/_blank) as timothy.lee@yourdomain. After you enter your password you will see a new prompt advising that your organization is enforcing 2SV. You now have the option of enrolling now or later. Click ****ENROLL****. You will be asked to re-enter your password.

8. You will now be asked to set up your phone. Enter your phone number into the box provided, choose how you want to receive codes (Text or Phone call) and click ****NEXT****.

9. At this point you will receive a call or a text from Google. Enter the code provided into the 'code' field and click ****NEXT****. Note: If the code you receive has the 'G-' prefix you can ignore that part. Enter the numeric portion only.

10. You should see a confirmation that the code was accepted. To enroll, click ****TURN ON****. You will be redirected to [myaccount.google.com](https://myaccount.google.com/" \o "myaccount.google.com" \t "/home/sherwinowen/Documents\\x/_blank) which advises that your phone has been verified. You also see a number of other secondary options listed which you can set up now or later.

* Backup codes (print a set of codes to be used in the event you are using a security key and you lose it)
* Google prompt (Get a Google prompt on your phone and just tap Yes to sign in)
* Authenticator app (Use the Authenticator app to get free verification codes, even when your phone is offline)
* Backup phone (Add a backup phone so you can still sign in if you lose your phone)
* Security Key (A Security Key is a small physical device used for signing in. It plugs into your computer's USB port)

11. Sign out and sign back in again at [mail.google.com](https://mail.google.com/" \o "mail.google.com" \t "/home/sherwinowen/Documents\\x/_blank) as timothy.lee@yourdomain. After you enter your password you should be prompted for a code which will be provided via text or a phone call. You may also be allowed to trust the device so you are not asked again. This feature is controlled from the advanced settings page, '2-step verification frequency' control.

Finally, let's return the admin console and view Timothy's profile.

12. Sign in to your domain as the administrator at[admin.google.com](https://admin.google.com/" \t "/home/sherwinowen/Documents\\x/_blank).

13. Click the****Users**** icon.

14. Locate Timothy Lee in the user list and click on his name. On the security card you can see that 2-step verification is ON for Timothy.

15. Click on the ****Security**** card and click ****2-step verification****. This is where you can get backup codes for Timothy in the event he cannot use his chosen 2SV method. You can also turn off 2SV for Timothy as the enforcement date has not yet been reached. Note that once the date has been reached you will not be able to turn it off.

16. Return to the 2SV enforcement options for the Executive OU and enforce 2SV from now. Then go back to Timothy's security card and you will notice that the ON/OFF slider is grayed out.

17. Finally, return to the 2SV enforcement options and disable 2SV enforcement, or set enforcement to a future date to ensure no one is locked out of their account.

****Notes****

1. When 2SV is enforced you can also give new users upto 6 months to enroll.

2. From the advanced settings page you can also choose which verification methods to allow. If you are using only security keys you can also allow users who have lost their key a grace period of up to one week where they can login using backup codes. These can be generated from the admin console.

****Help Center resources****

* [Deploy 2-Step Verification](https://support.google.com/a/answer/9176657" \o "Deploy 2-Step Verification" \t "/home/sherwinowen/Documents\\x/_blank)
* [Turn on 2-Step Verification](https://support.google.com/accounts/answer/185839" \o "Turn on 2-Step Verification" \t "/home/sherwinowen/Documents\\x/_blank)
* [Signing in with 2-Step Verification](https://support.google.com/accounts/topic/7189145" \o "Signing in with 2-Step Verification" \t "/home/sherwinowen/Documents\\x/_blank)

## **Use of an Exception Group**

****Introduction****

In the previous exercise you applied a 2SV enforcement policy to a single OU. This works well but consider a situation where you want to apply the policy to only some members of an OU. You could move the users who are not required to enroll into another OU but then you have a situation where you need to manage policies for multiple OUs where previously you had everyone in one place. This adds to the complexity of your organizational structure so is not desirable.

The solution to this challenge is to use an exception group. Exception groups augment the ability to turn on or off services by OU. The approach is fairly straightforward. You would:

1. Create a group and put all users who are exempt enrollment into that group.

2. Enforce the policy for the OU.

3. Disable enforcement for the group. The policy settings you give to the group are applied to the intersection of the OU and group (members of both).

The same approach could be used if you wanted to enforce enrollment for a subset of OU members only. In that case you enforce for the group but turn enforcement off for the OU.

For more information see the Help Center resources below

****Help Center resources****

* [Apply custom security policies](https://support.google.com/a/answer/2370108" \o "Apply custom security policies" \t "/home/sherwinowen/Documents\\x/_blank)
* [Avoid account lockouts when 2-Step Verification is enforced](https://support.google.com/a/answer/9176805" \o "Avoid account lockouts when 2-Step Verification is enforced" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #4 - Configure Session Controls**

****Introduction****

As an administrator, you can control how long users can access Google services, such as Gmail, without having to sign in again. You can set session lengths from 1 hour to indefinite so the session never expires. By default, the session length for Google services is 14 days.

If you want some users to have a different session length than others you can move them to a separate OU and set the session length for that OU to meet your business requirements.

In this exercise, you will learn how to reduce the session length for your contractors.

****Scenario****

Your company provides laptops to off-site contractors and wants to ensure that these devices are not compromised by someone leaving the device with an active G Suite session. They have decided to require each contractor to sign in at least once a day.

****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 ****Security****icon, scroll down and click ****Google session control****.

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

4. Set 'Session control' to 8 hrs.

5. Click ****OVERRIDE****. This will override the top level organization's setting of 14 days.

****Notes****

1. You cannot configure session length for native mobile apps.

2. It can take 24 hours for changes to propagate to all users.

****Help Center resources****

* [Set session length for Google services](https://support.google.com/a/answer/7576830" \o "Set session length for Google services" \t "/home/sherwinowen/Documents\\x/_blank)

**SINGLE SING ON**

## **Introduction to SSO**

Single Sign On (SSO) is a great benefit for your users, streamlining the login process through eliminating effort to remember different user account names and passwords across multiple apps.

In any SSO environment, there is what is known as an Identity Provider (IdP) and a Service Provider (SP). In the case of G Suite Marketplace apps, Google is the IdP as your users sign in with their Google credentials once and can then access the Marketplace apps offered by other service providers.

Alternatively, an organization may already use a 3rd party SSO service. In this case Google would be the SP, granting access to G Suite services such as Gmail and Calendar after a user has successfully signed into the 3rd party SSO system.

In this lesson you will learn how to set up SSO using Google as an IdP. You will also see the steps required to add a 3rd party IdP to your G Suite account and you should understand the differences between the two options.

If you are unable to complete all of the steps in these exercises due to your own organization's current systems and needs, you should still read through and explore the areas where these exercises are pointing you. If you don't have immediate SSO needs, you will still find it valuable to understand where to enable SSO in the future.

## **Exercise #1 - Setup SSO with Google as an Identity Provider**

****Introduction****

You can set up SSO using Google as the identity provider (IdP) using Security Assertion Markup Language (SAML). This allows the user to use their managed Google account credentials to sign in to enterprise cloud applications offered by other parties. You can establish SSO for your cloud applications through:

* Configuring one of over 200 third-party pre-integrated cloud applications as your service provider (SP)

OR

* Setting up your own custom SAML app for cloud applications that aren't in the pre-integrated apps list

In this exercise, you'll set up and enable SSO with enterprise cloud services for your organization with Google as the IdP.

****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).

Before we look at the cloud applications that have already been configured to use Google as an IdP, let's take a look at the Security section.

2. Click the ****Security**** icon, scroll down and click on ****Set up single sign-on (SSO) for SAML applications**** section.

Note that there are two URLs: the 'SSO URL' and an 'Entity ID' URL. These URLs will be required by the SP along with the Google certificate that is also shown on this page. These Google URLs are used by the SP as a user authenticates to their service. The certificate is very important as this is used to establish trust between Google and the SP.

3. Return the admin console's home page and click the ****Apps****icon, then click the ****SAML apps**** card.

4. Click the yellow circle with the + sign to enable SSO for a SAML application.

From here you can choose a pre-integrated app or you can set up your own custom app. The list of services shown represent the pre-integrated cloud applications that have already been configured for SSO and just need some minor customization from you. Clicking on a service will take you through a short setup wizard to activate SSO for that service within your organization. The setup wizards will vary slightly from app to app but as these are pre-integrated apps much of the information will pre-populate for you.

5. Click on ****15Five**** to walk through the 15Five wizard. Notice how the first page populates with the 'SSO URL' and the 'Entity ID' URL together with the 'Certificate' file that you saw in Step 2 above. You will need to copy the URLs and download the certificate as these must be added to the SP's configuration later to complete the process. We won't do that here however as the intention of this exercise is to allow you to become familiar with the process only.

Note: Instead of copying the URLs and downloading the certificate file you can download the 'IDP metadata' file. This is an XML file that contains both URLs and the certificate bundled into one file.

6. Download the 'IDP metadata' file and open it in a text editor so you can see the certificate and URLs. ****Tip:**** The idpId value in the URLs is actually your unique G Suite account number.

7. Click ****NEXT****. The 'Application Name', 'app-id' and 'Description' fields will be automatically populated for you. If you were adding your own custom app you would need to complete these values but pre-integrated apps should have these already.

8. Click on the ****Learn more**** link. This takes you to detailed setup instructions for this particular service.

9. Click ****NEXT****. As above this final screen will populate for you automatically. There are three URLs at the top of the page. These are the SP URLs that are used by Google as part of the authentication process.

10. Replace {yourdomain} with your G Suite domain name in each of the URLs, and click ****FINISH****.

You will see a prompt reminding you that you'll need to upload the Google URLs and certificate to the SP's administration panel to complete the configuration process.

11. Click ****OK****. This will take you to the 15Five service settings.

12. Return to the SAML apps list and you will see 15Five in the list. It should be OFF for everyone. You can use the ellipses (three vertical dots) at the end of the row to turn the service on and off.

At this point you should refer to the instructions specific to this application to complete the setup process. These instructions can be found in the Learn more link and will vary from app to app but are typically:

* Setup the app as the SP - Sign into the application console, upload the Google certificate and complete the Entity ID and SSO URL values.
* Enable the app in the G Suite admin console.
* Verify SSO is working - Attempt to log into the application. You should be redirected to the G Suite sign in page. After your credentials are authenticated, you are redirected back to the application.

13. Now repeat Step 4 but this time, click ****SETUP MY OWN CUSTOM APP**** and complete the details to add a fictitious app to your account. Note how the information required is the same as above but nothing is pre-populated for you.

User provisioning

Some services support user provisioning which allows the service provider to sync their user lists with your G Suite directory. Setup will vary from services to service. You can find out more about user provisioning for each service in the [Automated user provisioning](https://support.google.com/a/topic/6400789" \o "Automated user provisioning" \t "/home/sherwinowen/Documents\\x/_blank) article.

****Notes****

1. To enable SSO for one of the apps already identified by Google, your organization will have to have an account with that service.

****Help Center resources****

* [Using SAML to set up federated SSO](https://support.google.com/a/topic/7417510" \o "Using SAML to set up federated SSO" \t "/home/sherwinowen/Documents\\x/_blank) (Pre-integrated apps)
* [Set up your own custom SAML application](https://support.google.com/a/answer/6087519" \o "Set up your own custom SAML application" \t "/home/sherwinowen/Documents\\x/_blank)
* [SAML service provider URLs](https://support.google.com/a/answer/6301827" \o "SAML service provider URLs" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #2 - Setup SSO with a Third Party Identity Provider**

****Introduction****

Let's continue learning about SSO and set it up for managed Google accounts using a third party IdP.

The steps listed below describe how to set up SSO with a third party provider. You are not expected to complete this exercise but please read through the instructions and explore the Help Center resources in order to understand how to set up SSO using a third party IdP.

****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 ****Security**** icon, scroll down and click on ****Set up single sign-on (SSO) with a third party IdP**** section.

3. Check the Setup SSO with third-party identity provider box.

4. Complete the following URLs to your third-party Identity Provider (IdP). All URLs entered must use HTTPS:

* Sign-in page URL: The page where users sign in to your system and to Google
* Sign-out page URL: The page where users are redirected to after signing off

Change password URL

If you specify a 'Change password URL', it's important to note that all users, other than super administrators, who try to change their password in your organization will be directed to the URL you specify. This setting applies even if you do not enable SSO. Also, network masks do not apply.

If you are using G Suite Password Sync (GSPS) to [Sync password data with Active Directory](https://support.google.com/a/topic/2611858" \o "Sync password data with Active Directory" \t "/home/sherwinowen/Documents\\x/_blank) you can use Google Sites to create an internal webpage that instructs users to change their Microsoft Windows password instead of their Google password and enter the URL to that page into this field.

5. Create and upload the [SAML key and verification certificate](https://support.google.com/a/answer/6349922" \o "SAML key and verification certificate" \t "/home/sherwinowen/Documents\\x/_blank). Note: The certificate file you upload must be an x.509 certificate with an embedded public key. The public key must exist so Google can verify sign-in requests by your users. Tip: Use OpenSSL to generate your certificate and keys.

6. Add your 'Network masks'. These determine which addresses will be affected by single sign-on. If no masks are specified, SSO functionality will be applied to the entire network. See [Network Mapping results](https://support.google.com/a/answer/6369487" \o "Network Mapping results" \t "/home/sherwinowen/Documents\\x/_blank) for more details.

7. Click ****SAVE****.

****Notes****

1. When you are using a third party IdP the 'Require password change' option on your user's profiles is disabled.

2. Only Chrome can verify that the certificate you upload is valid. Other browsers do not.

3. Administrators signing into G Suite at [admin.google.com](https://admin.google.com/" \o "admin.google.com" \t "/home/sherwinowen/Documents\\x/_blank) are not redirected to the SSO sign in page whether they are within or outside of a network mask.

****Help Center resources****

* [Set up SSO using 3rd party IdPs](https://support.google.com/a/answer/60224" \o "Set up SSO using 3rd party IdPs" \t "/home/sherwinowen/Documents\\x/_blank)

## **Introduction to Secure LDAP**

****Introduction****

A directory service (or server) is typically used to check and grant access to a system’s resources. In its basic form, a directory can be a simple list of usernames. Over time, many proprietary directories evolved to support different systems and organizations found themselves managing multiple directories. For larger organizations in particular this can be time consuming and prone to error.

Sharing directory information across multiple systems greatly simplifies maintenance. LDAP (Lightweight Directory Access Protocol) is a commonly used method to share and maintain distributed directory information services, and systems that support LDAP can quickly be integrated into a unified directory.

G Suite includes the Secure LDAP service which provides a secure way to connect your LDAP-based applications and services to G Suite. The service supports any LDAP compliant application regardless of the hosting location, which can be on-premise, private or public cloud.

Using Secure LDAP, you can use your Google directory as an LDAP server for authentication, authorization, and directory lookups. Secure LDAP allows you to reduce the traditional directory server footprint where your applications may ordinarily point to several directory servers by pointing all of these apps only to Secure LDAP.

Setting up a Secure LDAP connection involves two main steps:

1. Create and configure the LDAP client in your admin console.
2. Configure your LDAP client to connect to the secure LDAP service.

It is not possible to provide an LDAP client to be used as part of this training so we will focus on Step 1 only. There are many different LDAP clients and configuration requirements vary considerably from one client to another. See [Connect LDAP clients to the Secure LDAP service](https://support.google.com/a/answer/9089736" \o "Connect LDAP clients to the Secure LDAP service" \t "/home/sherwinowen/Documents\\x/_blank) for Step 2 instructions for many common LDAP clients.

Watch the video that follows and then take the exercise in which you will complete Step 1 above.

****Help Center resources****

* [About the Secure LDAP service](https://support.google.com/a/answer/9048516" \o "About the Secure LDAP service" \t "/home/sherwinowen/Documents\\x/_blank)
* [Add and connect new LDAP clients](https://support.google.com/a/topic/9173976" \o "Add and connect new LDAP clients" \t "/home/sherwinowen/Documents\\x/_blank)

#### **Video : Secure LDAP Demonstration**

## **Exercise #3 - Add an LDAP Client to G Suite**

****Introduction****

In this exercise you will create and configure an LDAP client in your 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, then click the ****LDAP**** card.

3. Click****ADD LDAP CLIENT****. Enter an 'LDAP client name' and optionally add a 'Description'. Tip: You can also use the description to add contact details or to specify the owner of the application.

4. Click ****CONTINUE****.Third party idp

5. You must now configure the client’s permissions. The allowed permissions are described below:

* Access level for verifying a user’s credentials. You may grant the client access to the entire domain or to one or more organizational units to verify a user’s credentials. When organizational units are used, only users in those organizational units will be allowed to sign in to the application.
* Access level for reading user information. This setting specifies whether the client can access additional user information. This is useful where the client requests additional user details as part of the authentication process. You can choose to allow this for the entire domain or for one or more organizational units.
* Specify whether the LDAP client can read group information. This setting specifies whether the LDAP client can read group details and check a user’s group memberships for purposes such as a user’s role in the application.

6. Set 'Verify user credentials' to Entire domain.

7. Set 'Read user information' to Entire domain.

8. Click ****ADD LDAP CLIENT****. At this point the service will generate a certificate which you will upload to your LDAP client later. You can download the certificate now using the Download certificate link. You can also generate and download additional certificates at any time from the client’s details page.

9. Click ****CONTINUE TO CLIENT DETAILS****.

This completes the first part of the configuration. For details on how to complete the setup for your particular LDAP client, see the [Connect LDAP clients to the Secure LDAP service](https://support.google.com/a/answer/9089736" \o "Connect LDAP clients to the Secure LDAP service" \t "/home/sherwinowen/Documents\\x/_blank) article. There are some generic setup instructions here as well as specific instructions for popular applications. New applications are being added all the time so check back regularly. See [Add and connect new LDAP clients](https://support.google.com/a/topic/9173976" \o "Add and connect new LDAP clients" \t "/home/sherwinowen/Documents\\x/_blank) for detailed instructions on how to connect your LDAP clients and applications to the Secure LDAP service.

**APPLICATION SECURITY**

## **Introduction to Application Security**

There are hundreds of applications available that integrate with G Suite services. These apps may be cloud based enterprise apps, marketplace apps, or custom apps.

As the administrator you are responsible for protecting your user's data so it is important that you understand best practices for application integration.

In this lesson you will learn how to control access to the admin console from the Admin SDK API. You will also learn how to block access to a specific service (for example, Drive or Calendar) by turning off API access to that service whilst at the same time allowing trusted apps to use that API by creating a trusted application list.

Finally you will explore the G Suite Marketplace. You will install a marketplace app for your entire organization and create a marketplace whitelist which controls the applications that users can install from the marketplace onto their company managed devices.

## **Exercise #1 - Admin SDK API Access**

****Introduction****

G Suite has many APIs that allow third party applications to interact with G Suite services such as Gmail, Calendar, Contacts, etc. An example of usage might be a locally installed application which syncs a local contacts database with your G Suite contacts. This application would likely use the Contacts or People API to sync data.

In addition to APIs that access user data, G Suite includes the Admin SDK API. This is specifically designed to allow developers to interact with the admin console and objects such as users, calendar resources, groups, OUs, etc.

Before an application can interact with your admin console however, you must enable API access for the Admin SDK API. We recommend you disable this access if you do not have any applications that specifically require it.

The purpose of this exercise is to make you aware of this requirement and to direct you to the control 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 ****Security**** icon, scroll down and click on ****API Permissions****.

3. Click the ****MANAGE GOOGLE SERVICES**** link. From here you can see the 'G Suite admin' service. You can enable access form the 'Change access' link which is visible when you hover over the service name.

****Help Center resources****

* [Developer Offerings](https://developers.google.com/gsuite/products" \o "Developer Offerings" \t "/home/sherwinowen/Documents\\x/_blank) (G Suite APIs list)
* [Admin SDK](https://developers.google.com/admin-sdk/" \o "Admin SDK" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #2 - Whitelist Connected Apps**

****Introduction****

There are many third party applications that interact with G Suite using the G Suite APIs. These might be traditional desktop or mobile apps.

Before an application can gain access to a G Suite user's managed account, the application must request access to the data (stating what access it requires) and the user must grant that access. This is done during application installation and this flow is known as 3-legged authorization (3LO). Once authorized the application receives a token that it uses to access that particular user's account. These tokens are known as OAuth 2.0 tokens.

Each API has one or more scopes which determine the precise access allowed. For example: the Gmail API includes the https://www.googleapis.com/auth/gmail.labels scope which allows the application to manage labels only. Other scopes exist that allow messages to be read, inserted and sent. It's important that each application only requests access to the data it needs.

As an administrator you can:

* Enable and disable access to each API
* Create a list of trusted apps that you will allow to use disabled APIs

In this exercise you will block Calendar API access to all applications except for a single application that you trust, plus any applications developed by 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 ****Security**** icon, scroll down and click on the ****API Permissions**** section.

3. In the 'Settings' area of the 'App access control' card, ensure that 'Trust internal, domain-owned apps' is selected.

4. Click ****MANAGE THIRD-PARTY APP ACCESS****.

5. Click ****Add app > Android****. Enter the search string of Calendar Sync and click ****SEARCH****.

6. Select an app from the search results and click ****ADD****. The app you selected is now trusted by your organization.

7. Click the ****GOOGLE SERVICES****. Hover over the 'Calendar' row, and click ****Change access****.

8. Select 'Restricted: Only trusted apps can access a service' and click ****CHANGE****.

9. Click ****RESTRICT**** to confirm.

Now that you have disabled Calendar access, only the app you trusted above plus any internal apps will be allowed to use the Calendar API.

****Notes****

1. If you intend to disable API access but you want to trust some currently installed applications, add these applications to the trusted list before you disable API access to ensure these applications are not blocked.
2. After blocking the API/scopes, any already installed apps will stop working and tokens will be revoked.
3. When a user tries to install an app that has a blocked scope, they see the error message that you define on the App access control card.
4. Any applications you whitelist in the G Suite Marketplace, Android whitelist and iOS whitelist settings pages are also automatically trusted.

****Help Center resources****

* [3-legged OAuth Diagram](https://www.google.com/support/enterprise/static/gapps/art/admin/en/cpanel/3-legged-oauth-diagram.png" \o "3-legged OAuth Diagram" \t "/home/sherwinowen/Documents\\x/_blank)
* [Control which third-party & internal apps access G Suite data](https://support.google.com/a/answer/7281227" \o "Control which third-party & internal apps access G Suite data" \t "/home/sherwinowen/Documents\\x/_blank)
* [Using OAuth 2.0 to Access Google APIs](https://developers.google.com/identity/protocols/OAuth2" \o "Using OAuth 2.0 to Access Google APIs" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #3 - The G Suite Marketplace**

****Introduction****

The G Suite Marketplace offers a wide range of enterprise apps that add functionality and features to native Google Cloud apps. Anyone with a G Suite account can use the marketplace.

As the administrator, you can install apps for your users, and authorize which apps users can install for themselves. Once installed, apps are accessible through the App launcher alongside G Suite apps such as Gmail, Calendar and Drive.

The marketplace is available at [apps.google.com/marketplace](https://apps.google.com/marketplace" \o "G Suite Marketplace" \t "/home/sherwinowen/Documents\\x/_blank). Administrators can also access the marketplace from the admin console.

In this exercise you will install a marketplace app for your entire organization and create an apps whitelist ensuring that your user's can only install the apps which your company has approved.

****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).

Install an app for the entire organization as the G Suite administrator

2. Click the ****Apps**** icon, then click the****G Suite Marketplace apps**** card, but DO NOT click the 'Manage' link that is on the card.

3. Click ****Add app to domain install list****.

4. Locate Google Analytics in the list of apps and click on the app icon. You now have the option of installing the app for your entire organization or installing it for your own account.

5. Click ****Domain Install****.

6. Read the notification and click ****CONTINUE****.

7. You will now be prompted to authorize the application for your organization. Review the scopes that the app is requesting access to and if you are happy, check the I agree to the application's Terms of Service and G Suite Marketplace Terms of Service box and click ****Accept****, then click ****DONE****.

8. Return to the Marketplace page in the admin console. You should see 'Google Analytics' listed. If the list is empty, refresh the page. Note that it can take 24 hours for the app to become fully available to your users.

Create a whitelist of marketplace apps for your users

Now we have seen how the administrator can install an application for their users, let's see how the administrator can control what individual users can install onto their devices. We will do this by creating a marketplace whitelist.

We will start by restricting apps that users can install to only apps that are whitelisted.

9. Return to the home page in the admin console, and click the ****Apps**** icon.

10. Click the ****Manage**** link on the 'G Suite Marketplace apps' card.

11. Set 'Allow Install' to Allow users to install only whitelisted applications from G Suite Marketplace and click ****SAVE****.

12. Click the ****Manage whitelist**** link.

13. Click the ****Add the app to the whitelist**** link to add an app to the whitelist.

14. Search for Google Apps Script in the list of apps, hover over it in the results and click ****ADD TO THE WHITELIST****, then click ****CONFIRM****.

Verify the whitelist

It can take some time for apps to become available to your users but let's see if a user in your organization can see the changes you have just made.

15. Sign out and sign back in to G Suite at [apps.google.com/user/hub](https://apps.google.com/user/hub" \o "User hub" \t "/home/sherwinowen/Documents\\x/_blank) as samantha.morse@yourdomain. Can you see 'Google Apps Script' in the 'Approved apps' section?

16. Open [apps.google.com/marketplace](https://apps.google.com/marketplace" \o "G Suite Marketplace" \t "/home/sherwinowen/Documents\\x/_blank) and click on any app to try and install it. You should see a message in the top right advising you that the app cannot be installed because it has not been whitelisted.

****Notes****

1. It can take 24 hours for the app to become fully available to your users.

2. Creating a whitelist does not uninstall and previously installed apps from user's devices.

3. Just like a Google service, marketplace apps can be turned on and off at the OU level.

****Help Center resources****

* [Evaluate a Marketplace app's security](https://support.google.com/a/answer/180490" \o "Evaluate a Marketplace app's security" \t "/home/sherwinowen/Documents\\x/_blank)
* [Access Marketplace apps](https://support.google.com/a/answer/172981" \o "Access Marketplace apps" \t "/home/sherwinowen/Documents\\x/_blank)
* [Understand data access for Marketplace apps](https://support.google.com/a/answer/176367" \o "Understand data access for Marketplace apps" \t "/home/sherwinowen/Documents\\x/_blank)
* [Delete an app](https://support.google.com/a/answer/6216211" \o "Delete an app" \t "/home/sherwinowen/Documents\\x/_blank)

**SECURITY TOOLS**

## **Security Tools Overview**

In this lesson you will explore some of the tools that are available to you in the admin console that help you keep your information secure.

You will start by looking at the security center from where you can see a high level dashboard of security related events such as spam metrics and failed device login attempts. You will drill into the dashboard and filter the data for each report to show the results of interest to you.

You will explore the security health page which provides an overview of your security-related settings and gives recommendations where appropriate, and you will be introduced to the security investigation tool which can be used to identify, triage, and take action on security and privacy issues in your organization.

You will be introduced to the alert center and you will review the accounts activity report which is an aid to monitor your users' account settings and exposure to security risks.

## **Exercise #1 - Security Center**

****Introduction****

The G Suite security center brings together security analytics, actionable insights and best practice recommendations from Google to empower you to protect your organization, data and users. The security center is comprised of the following:

* Security dashboard reports
* Security health page
* Investigation tool

****Scenario****

In this exercise, you'll be introduced to the security dashboard and security health recommendations. You will also explore the investigation tool. As you have a new domain there will be little or no security related content in your logs but it is important to understand how the security center works so we will walk through each component.

****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).

Security dashboard

The security dashboard provides an overview of data from several security center reports.

2. Click the ****Security**** icon, and click ****Dashboard****. From here, you will see a number of widgets, each providing a summary of key security metrics for:

* External file sharing activity.
* Message activity including: number of messages authenticated or encrypted, spam statistics, suspicious attachments and spoofing.
* Device events such as failed login attempts, compromised device events and suspicious activity.
* OAuth grant activity - these refer to your user's granting access to third party apps and sites to their data.

You can filter by domain and date and you can view up to 180 days of data.

3. Locate the 'Spam Filter - All' widget, and click ****VIEW REPORT****. This will open the full report where you will see a chart at the top and a table beneath.

The chart shows messages that have been delivered to the user's inbox or marked as spam and at the top of the page you can apply filters to the chart such as traffic source (internal, external) and classification (spam, fishing, malware, etc..). You can also select a date range.

Hover over the chart and click on any date. Now you will see the table data populate below with data from the selected date and in that table you can pivot on message metadata such as subject, recipient and sender.

You can also export the data to a Google Sheet.

4. Return the dashboard, locate the 'Authentication' widget, and click ****VIEW REPORT****. Notice how the filters and table metadata options have changed as each report has its own set of properties.

See [About the security dashboard](https://support.google.com/a/answer/7492330" \o "About the security dashboard" \t "/home/sherwinowen/Documents\\x/_blank) for a description of all the reports available in the dashboard.

Security health page

The security health page provides an overview of your security-related settings in the admin console. You should monitor your organization's security health so you can stay ahead of potential threats by examining security analytics and flagging threats.

5. Return to the Security settings page and click ****Security health****. Each entry on this page represents a security related setting in the admin console.

* On the left you will see the name of the setting together with the navigation path in the admin console. For example: 'Calendar sharing policy' - 'Apps > G Suite > Settings for Calendar'.
* Status is shown in the center (for example, enabled/disabled plus OU counts)
* On the right there are a number of icons. Each setting is either healthy or there is a recommendation. Click on the icon to see the recommendation details.

See [Get started with the security health page](https://support.google.com/a/answer/7491656" \o "Get started with the security health page" \t "/home/sherwinowen/Documents\\x/_blank) for more details.

Security investigation tool

The security investigation tool is used to identify, triage, and take action on security and privacy issues in your organization.

6. Return to the Security settings page and click ****Investigation tool****. This will take you to a page where you can build a query to search across device, mail, drive, and user events and logs. Let's build a simple search.

7. Select the 'Data source' of Users and click ****ADD CONDITION****.

8. Select the 'Condition' of Enrolled in 2SV and set the value to False, then click ****SEARCH.****You should see all users who are not enrolled in 2SV in the search results. Note that timothy.lee@yourdomain is not listed as he enrolled in 2SV earlier.

From here you can take actions on the results. In this case the actions are specific to Users but the actions will vary depending upon the type of search you are performing.

9. Hover over any user in the list and click the ellipses (three vertical dots) icon to the right of the username, then click ****Actions****. From here you can copy the value, or restore or suspend the user.

You can also pivot to another view for the individual user. Pivoting allows you to add a new search to the tool using information from one set of results to perform a new search.

10. Hover over lars.ericsson@yourdomain and click the ellipses (three vertical dots) icon to the right of the username, then click ****Pivot to > Gmail messages > Recipient****. This will add a new search below the current search.

11. Click ****SEARCH**** to view all messages received by Lars.

12. Hover over any message in the results set and click the ellipses (three vertical dots) icon to the right of the Message ID, then click Actions. From here you have message related actions: Delete message, Mark message as phishing, Mark message as spam, Send message to inbox, Send message to quarantine, View header and View message. Note, if you want to view the actual message you will be asked to provide justification. See [View Gmail message content](https://support.google.com/a/answer/9300435" \o "View Gmail message content" \t "/home/sherwinowen/Documents\\x/_blank).

The investigation tool also allows you to do the following:

* Select multiple results and perform actions in bulk. Check the box to the left of a couple of search results. You will see an ACTIONS button appear at the top of the results. Click the button to see what actions are allowed.
* Export results to a Google sheet.
* Add a widget to the security dashboard using the results of your investigation. This feature is not available for all data sources.

See [About the security investigation tool](https://support.google.com/a/answer/7575955" \o "About the security investigation tool" \t "/home/sherwinowen/Documents\\x/_blank) for more details.

****Help Center resources****

* [Security center](https://support.google.com/a/topic/7492529" \o "Security center" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #2 - Alert Center**

****Introduction****

In the previous course we saw how an administrator can set up email alerts from the Rules area in the admin console. We also saw that G Suite has a set of predefined rules. Some of these predefined rules, when triggered will log events to the G Suite alert center.

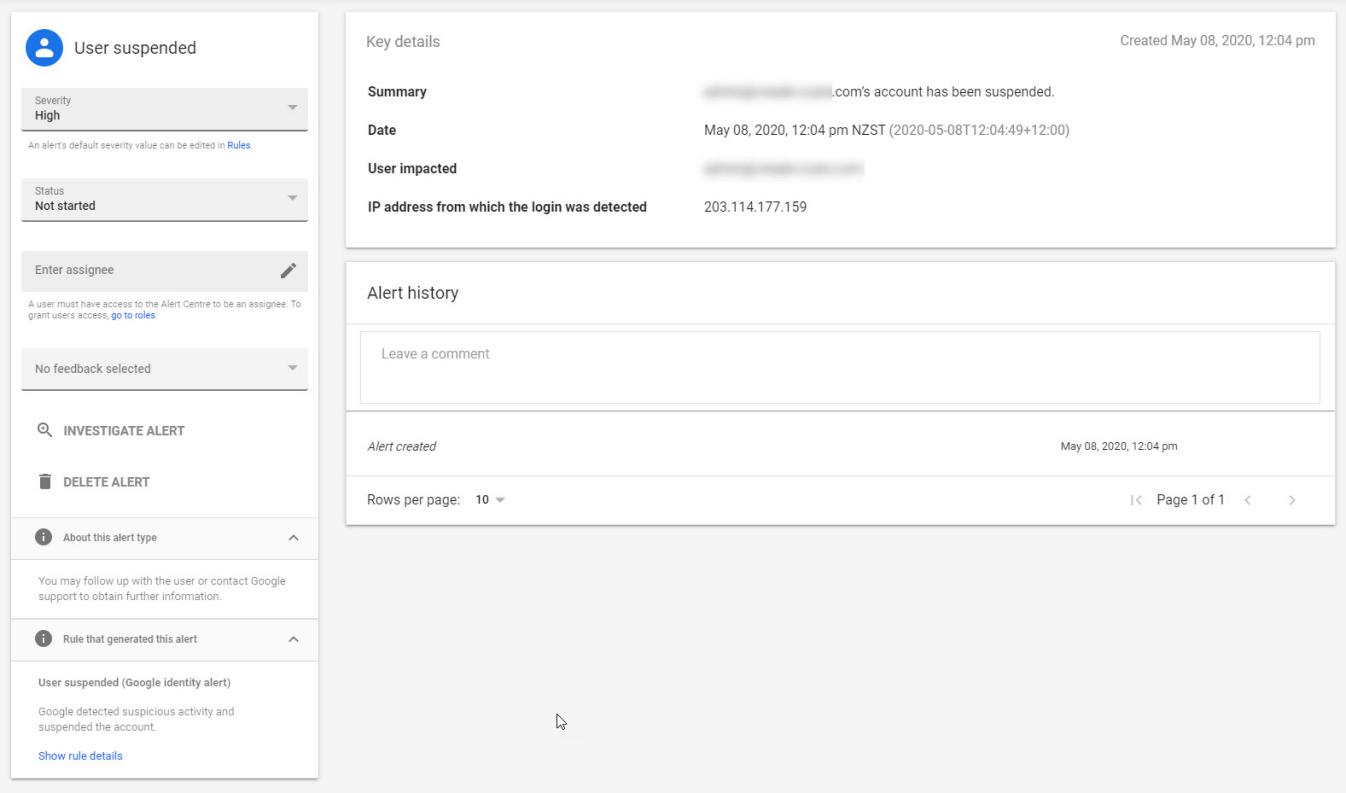
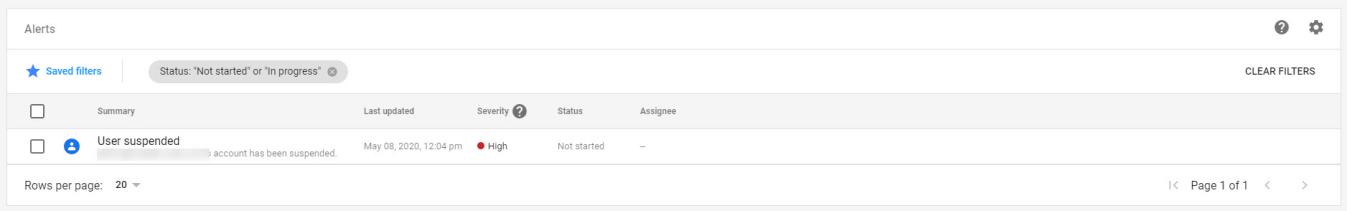
As the administrator, you will use the alert center to view notifications about potential issues within your domain, and take action to resolve the issues and protect your organization from security threats. You can view a list of alerts, and then click any item in the list to view details about those alerts. You can also start an investigation from the alert center by linking directly to the security investigation tool. Using the investigation tool, you can then make adjustments to your admin console security settings if needed, or take other actions in response to the alert.

As you have a new domain it is very unlikely that you will have any alerts in your alert center but in this exercise you will learn how to navigate to the alert center and locate and identify rules that add alerts to the center.

****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. From the menu, click the ****Security**** icon, then click****Alert center****. It is very unlikely that you will see any alerts listed so we have added two images below to let you know what to expect. The first image shows the alerts list (you will notice we only have one alert - a user has been suspended by Google). The second image shows the alert details, and from here you can manage the alert.



3. Click the gear icon (Alert rules settings) on the top right of the page. This will take you to the list of predefined rules we saw in the previous course.

You may recall that you can only edit the actions part of a predefined rule; this means:

* For rules that send alerts to the alert center you can enable/disable the alert. Disabling the alert also disables email notifications.
* For rules that do not send alerts to the alert center, you can specify email recipients to be notified when the rule is triggered.

4. Review the Alerts column. From here you can see which rules are logging events to the alert center. Note that not all rules will log to the alert center.

5. Locate and click on the ****Leaked password**** rule, then click on the ****Actions**** card. Note that this rule can log to the alert center.

6. Return the rules list, locate and click on the ****Calendar settings changed**** rule, then click on the ****Actions**** card. Note how this rule can only be configured to send an email notification when it is triggered.

****Help Center resources****

* [Alert center](https://support.google.com/a/topic/9105077" \o "Alert center" \t "/home/sherwinowen/Documents\\x/_blank)

## **Exercise #3 - User Activity Reports**

****Introduction****

As an administrator you can monitor your users' account settings and exposure to security risks by opening the accounts activity report.

The accounts activity report gives you a consolidated view of user status and account activity, where you can access all data from the user account status, admin status, and 2-step verification enrollment reports.

See [Account activity reports](https://support.google.com/a/answer/4580176" \o "Account activity reports" \t "/home/sherwinowen/Documents\\x/_blank) and the [Security checklist for medium and large businesses](https://support.google.com/a/answer/7587183" \o "Security checklist for medium and large businesses" \t "/home/sherwinowen/Documents\\x/_blank) to learn more about security best practices. In this exercise, you'll view and customize an accounts activity report for your organization. Note though that because you just set up your domain, there will be limited data or no data available to view in your report.

****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 ****Account activity**** (this link can be found under the Users category on the left).

There are a set of icons on the top right of the page from where you can download the data, choose which columns to display and show/hide the filter pane.

4. Click the ****Select columns**** icon (three vertical bars) and then choose which columns you want to display. Click on any ****Column heading.****This will change the chart above to display a representation of that column’s data.

In an earlier exercise you enrolled one of your users into 2SV. As mentioned previously it can take up to 48 hours for these reports to reflect changes made so if you check the status in the report for that user and it shows them as not being enrolled, this is normal.

On the left you will see the filters pane. From here you can filter by date, OU (or user), and column data.

5. Explore the filters and once you have the information in the report that you desire, use the download icon on the top right of the page to either download the report or export it to a Google Sheet.