Google Workspace

- User Management
  - Adding Users Individually
  - Add Several Users at Once
  - Sync Users to Domain with GCDS
  - Admin Roles and Privileges
  - Custom Admin Privileges
  - Resetting a User's Password
  - Rename a User
  - Suspend a User
  - Delete a User
  - Restore a Recently Deleted User
  - Create an Organization Unit
  - Create an Admin-Managed Group
- Security
  - Navigate the Security Center
  - Configure Common Security Settings

User Management

Module Overview

In this module, you'll learn about provisioning and managing users in your Cloud Identity domain. The exercises cover how to add new users in various ways and how to configure user identities, settings, and privileges.

Important information before you get started:

1. About User Passwords

In these exercises, as a G Suite administrator you have control over the user passwords. To avoid confusion or being locked out of an account, it's best to keep a consistent policy for password creation. (This isn't an issue in a real-world situation; your users, not you, will be setting their passwords the first time they sign in.)

For these exercises, the default password for all new users is **hellohello1**, unless you choose the auto-generated temporary password option.

To maintain consistency and to avoid forgotten passwords during these exercises, we suggest changing new user passwords to **G00gleidentity** (with zeros instead of letter Os) during the first sign-in process. Feel free to choose your own new password, but do remember to take note of it!

Adding Users Individually

Introduction to Exercise

Before people in your organization can begin using your Cloud Identity service, you need to create user accounts for each person. An account provides users with a name and password for signing in to their cloud services. Each user you add will require a user license.

The deployment of a Cloud Identity domain will often be done in phases. In each deployment phase, you add different types of users based on their particular focus and unique needs. The first phase of your deployment is where you'll add your technical IT users, so that they can begin using your organization's services and align the settings with your organization's IT policies.

In this exercise, you'll manually add an individual user—Alexa Bell, your IT Manager.

Exercise Directions:

1. Sign into your Google Admin console as the administrator user using **your administrator account name and password**.

2. Go to the **Users** section, then click **the yellow "Plus" button** and select **Add User**.

Because this is a new domain, there's only one Organization (Org)—the parent org—named the same as your domain. We'll add more orgs later, but for now, we can add Alexa.

Learn more about how to Add users individually.

3. In the **"Create a new user"** dialog box, create your company's IT Manager user account, entering the following information:

First name: **Alexa**

Last name: **Bell**

Primary email address: **alexa.bell@yourdomain.com**

Note: *If your account has multiple domains associated with it, use the domain (next to @) drop-down list to view the available domains. The domain you select will be the portion of the user's email address that appears after the @ symbol.*

- Each user account requires a password. You can assign a temporary, randomly generated password or manually set a temporary password. Either way, the new user will change this when signing in for the first time.

For this exercise, you should simply allow a temporary password to be assigned.

4. You can also add more profile information for Alexa, such as her contact and employee details. This information is visible in the Admin console.

Click Additional Info and enter the following user information:

Secondary Email Address: (Leave this blank if you don't have one)

Phone: 01 23 45 678

Address: 110 Main St, Cloud City

Click Next to enter Employee Details:

Employee ID:

Employee Type:

Title: IT Manager

Department: IT

Cost Center:

5. Click Create to generate Alexa's account.

Congratulations! You've added your first user in your new domain!

Notice the Show Password link that allows you to see the temporary password generated.

6. (Optional) Click Email instructions or Print instructions to deliver the account information to the new user. Use an email address that's currently accessible to the user.

7. Exit out of the window.

Now that you have a user, you can investigate some of the user-specific settings.

8. Locate Alexa's name in the Users list, click her name, and click Account.

9. In the Password section, ensure that the Require user to change password at next sign-in box is checked.

Add Several Users at Once

Introduction to Exercise

You've learned how to add users manually; however, when adding many users at once, this method is quite time consuming. Let's see how to bulk upload many users at once.

Note: This task requires being signed in as a super administrator. For more information, see Add several users at once.

Exercise Scenario

You receive this mail from the IT Manager, Alexa:

Hi Admin!

Thanks for creating my Google account. Now our next task is to get the rest of our users accounts created. Below is the list of people.

First Name	Last Name	Email	Password	Employee Title
Ellie	Gray	ellie.gray@yourdomain.com	hellohello1	Executive Assistant
Jon	Baird	jon.baird@yourdomain.com	hellohello1	HR Contractor
Lars	Ericsson	lars.ericsson@yourdomain.com	hellohello1	Project Manager
Samantha	Morse	samantha.morse@yourdomain.com	hellohello1	CEO
Jennifer	Lee	jennifer.lee@yourdomain.com	hellohello1	Finance Manager
Tom	Edison	tom.edison@yourdomain.com	hellohello1	Support Engineer

First Name	Last Name	Email	Password	Employee Title
Will	Marconi	will.marconi@yourdomain.com	hellohello1	Support Engineer

Can you create these accounts using Cloud Identity for us?

Thanks, Alexa Bell, IT Manager

Exercise Directions

In this exercise, you'll add several users via a comma-separated value (CSV) file.

To add several users at once:

1. Sign into your Google Admin console as the administrator user using **your administrator account name and password**.

2. Go to the **Users section**, hover over the yellow plus sign, and **select Add multiple users**.

In the **Add multiple users** dialog box, click the **Download as .csv button** to download a copy of a sample spreadsheet to your local machine with the proper headers formatted. Leave this dialog box open to (later) upload the file after editing.

3. Open the CSV file in a spreadsheet application, such as Microsoft Excel.

4. Edit the file to add the user data. Copy the user information into the CSV file from the table Alexa provided.

The file contains a column for each attribute that appears on the user profile in the Admin console and in your directory contacts.

Note: *You must enter values in the **Email Address, First Name, Last Name**, and **Password columns**; that information is **mandatory** for each user. Don't forget to update the domain in the email addresses. The other columns aren't mandatory, so you can enter values or leave them blank. However, Alexa has also provided a column for **Employee Title** that requires information to complete.*

5. Once the editing is complete, save a copy of the CSV file (in a CSV file format) back to your local machine.

6. Return to the **Add multiple users** dialog box, click **Attach File**, and browse to the edited spreadsheet you just saved locally.

By default, the **Require user to change password at next sign-in** checkbox is enabled. This requires the user to change the generic password you entered in the spreadsheet.

7. Click **Upload** to initiate the creation of the user accounts.

- If your file has formatting errors, a warning prompts that you may need to re-edit the file. Review the list of common errors.
- If successful, a status bar prompts how many users will be uploaded and a full report will be sent when complete.

8. Go to your email inbox associated with your Admin account and search for the email report of the bulk upload.

In the Admin console, review the list of users and explore the user settings. (This can take a couple of minutes to appear.)

Congratulations! You uploaded multiple users at once! If you're uploading more than 500 user accounts, you can optimize the experience by splitting your uploads into smaller batches.

Note: *It can take up to 24 hours for new user accounts to appear in the searchable domain directory.*

User Management

Sync Users to Domain with GCDS

Introduction to the Reading

If your organization has a large, pre-established directory, Google Cloud Directory Sync (GCDS) is a secure tool that we provide that can help you sync your users into your Cloud Identity domain. GCDS allows you to synchronize your user data in your Cloud Identity domain with your Microsoft® Active Directory® or LDAP server. GCDS will ensure that your Google users, groups, and shared contacts are synchronized to match the information in your LDAP server. The data will never be modified nor compromised.

Important Note: *Because we're unable to provide a practice instance and ensure that everyone is able to practice using GCDS during this training, and it also requires advanced and more complex setup, use the information below to learn more about GCDS. If your organization would like more information about setting up your Cloud Identity instance using GCDS, please reach out to our support channels!*

Read through the following

Step 1: Get acquainted with the GCDS

This help center article will help you understand: a) how GCDS works; and b) the key benefits of GCDS.

After reading through this article, your organization should be able to gauge the necessity of using GCDS.

Step 2: Walk through how to install and prepare to use GCDS

The steps outlined in this series of articles will explain to you how to download GCDS, and also, they will explain how to prepare your current system to use the toolset.

Remember, you must first ensure that your system meets the system requirements.

As you read through these help center steps, ensure that you are looking through each of the points that apply to your current system.

Step 3: Configure your system to use GCDS

As you configure your systems, remember that GCDS will sync all of the user data and settings that you configure. It's important that these steps are carefully executed, and this is a more advanced and intensive process.

This article will outline all of the data that is able to be synced using GCDS. Take notice of the data that is not able to be synced. Also, take advantage of the other articles that are linked here to learn more.

Other FAQs for GCDS

This article answers many of the most popular questions that come up when considering the use of GCDS.

Remember: For this training, we will not be practicing using this tool. This is simply a guided reading to serve out our knowledge base articles that exist to help you if your organization needs to do a large migration of users into your Cloud Identity domain. We will provide a larger set of advanced resources at the end of this training to point you in the direction of these more advanced toolsets and use cases.

User Management

Admin Roles and Privileges

Introduction to Exercise

In this exercise, you'll grant the super administrator role to Alexa Bell, the IT Manager. The super administrator role is an example of a pre-built administrator role that's standard in the Admin console and where you can create custom roles to suit your needs.

NOTE: *To grant the super administrator role and privileges to a user*

You can assign an administrator role to a user on the Users account information page, or on the Admin roles page where you define the administrator roles. On the Admin roles page, you can assign a role to multiple users at the same time. Because we're adding a role to just one user, we'll use the Users method.

Exercise Directions

1. Sign into your Google Admin console as the administrator user using **your administrator account name and password**

2. Click the **Users icon**

3. Locate **Alexa Bell** and click to enter her **user page**

4. Scroll down and select the **Admin roles and privileges option**. (You may need to click **Show more at the bottom of the profile**.)

- The user currently has no Admin roles assigned

5. In the **Manage roles list**, select the predefined **Super Admin role** and click **Save**

- In the Admin roles and privileges section, you should now see the super administrator role for all organizations.
- Now you can investigate the specific privileges you have granted to the user.

6. Go to to the main **Admin console dashboard** and click the **Admin Roles icon**.

- If you don't see this icon on your dashboard, click the **More controls pull-down option** (at the bottom of the page), and then click the Admin Roles icon.

7. Click the **Super Admin link** to view the current users with Super Admin role.

- At this point, this should only be your initial administrator account, plus Alexa Bell's account. You can always see this list by going to Admin Roles control.

8. In the **Super Admin list of users**, select the **Privileges tab** and review the assigned privileges.

- Because this is a pre-defined role, note how the Super Admin has all possible privileges selected and how these privileges aren't customizable.
- Now that you've granted the super administrator role to Alexa, she can sign in to the Admin console with full administrator privileges.

Further Notes:

- *When Alexa signs in to the Admin console, she'll see the default dashboard. Any previous customizations you made as your own administrator account aren't visible. Your customizations only apply to your administrator account.*
- *Creating more than three super administrators for your domain can affect some administrator account recovery options. At least one user in a domain must be a super administrator, and only a super administrator can assign administrator roles to other users.*
- *In some cases you may want to create custom user roles. For example, you want your help desk person to do only password resets. This is not necessarily in-scope for this particular training, but if you're interested in learning more check out this article.*

Custom Admin Privileges

Introduction to Exercise

In this lesson, you will practice creating custom roles that have a custom set of privileges.

Exercise Scenario

A little later you receive a request from the Project Manager, Lars Ericsson.

Hello Admin,

I would like to understand more about how our users are interacting with our cloud-based applications. That way I can create a customized training plan for the company. Is there any way I can run reports that track apps usage and user behaviors?

Regards, Lars Ericsson

You decide that, rather than giving him a pre-built role with extra privileges he doesn't need, it's best to create a custom role. That way you can delegate the ability to run reports, but not give Lars any other administrator privileges.

Note: *You can assign more than one administrator role to a user. Creating multiple roles with fewer privileges is, therefore, more versatile than one role with many privileges. If a user handles multiple tasks, just assign multiple roles.*

Exercise Directions

1. Sign into your Google Admin console as the administrator user using your **administrator account name and password**.

2. Click the **Admin Roles icon**.

- If you don't see this icon on your dashboard, click the More controls pull-down option (at the bottom of the page), and then click the Admin Roles icon.

3. Click **Create a new role**.

4. In the Create New Role dialog box, enter the **Reporting Role name**, give a **description for the role**, and click **Create**.

5. In the **Privileges tab**, you can select the privileges you want users to have with this role.

- Assigning a custom role to a user grants them access to the Admin console. The privileges determine which dashboard controls are in their console, what information the user can access, and which management tasks they can perform. Learn more about administrator privilege definitions.
- Investigate here exactly what Lars has access to once he's given Reports privileges in this role.

6. Because you want this custom role to just assign privileges for reporting only, check the **Reports box**, and click **Save**.

- You should now see **Reporting Role** in the **User Created Roles list**.

7. Creating the role is the first step in this process, but for Lars to be assigned the privileges, we must also assign the administrator role to his user account.

- In the **Users section**, go to Lars' user account page, scroll to the bottom of the page, and click **Show more > Admin roles and privileges**.
- Choose the **Reporting Role role** from the list and click **Save**. The Admin roles page lists the user's current privileges, and you should now see the new role assigned to Lars.
- Scroll down to **Privileges** in order to view combined privileges granted by all the user's roles.

Congratulations! You've now built and assigned a custom administrator role to one of your users, which allows you to better delegate administrator tasks in your domain.

Resetting a User's Password

Introduction to Exercise

Now that users are signing in and using the tools, you're likely to come across a scenario where a user needs a password reset:

- A user forgets their password
- A user's account is compromised (security concerns)

Exercise Scenario

Jennifer Lee (from Finance) has just come back from holidays, she calls to ask you to reset her password, because she's forgotten it and is now locked out of her account.

Exercise Directions

1. Sign into your Google Admin console as the administrator user using **your administrator account name and password**.

2. Click the **Users** icon.

3. Access the **reset password function** by one of two ways:

   - In the **user list**, click **Jennifer Lee**. When her page has loaded, click the **Reset password icon**.
   - In the user list, **hover over Jennifer Lee** and view the available options that display. **Click Reset password**.

4. In the **Reset password for jennifer.lee** dialog box:

   - Fill in a temporary password or click Auto-generate password to let Google create one for you.
   - Check the **Ask for a password change at the next sign-in** in the next sign in box.
   - Click **Reset > Done**.

5. Provide the user with **new sign-in information**. If you have auto-generated the password, there'll be a show password option.

The next time the user signs in, they'll be prompted to supply the current password and enter a new password.

When they enter the password, the Password strength field evaluates the security level of the password. They can click the link if they want tips for creating strong passwords. Google requires a password that's at least eight characters.

As the administrator, inform Jennifer Lee that her password is now reset and she can now sign in to change it. You can also give her some tips on creating a secure password in line with your company's security policy.

Rename a User

Exercise Introduction

When you are using Cloud Identity as your primary identity provider (IdP), you may make mistakes when entering user data into the console. If for some reason you need to change a user's name in the Google Admin Console, this exercise will walk you through how to rename a user.

More Information

See this help center article to learn more about renaming users.

Exercise Scenario

You receive this mail from the CEO:

Hello Patrick,

Thanks for creating my Google account. However I have to ask for a minor change. My username is samantha.morse@[yourdomain.com] but really most people know me as just “Sam”. Is there anyway to just have my name as Sam Morse?

Regards, Samantha Morse, CEO

Exercise Directions

1. Sign into your Cloud Identity Admin console as the administrator user using your **administrator account name and password.**

3. Click the **Users icon**.

4. Search or browse to find the user. If you created an organizational structure, select the organization to which the user belongs.

- In our case, Samantha is in the top-level organization.

5. In the user list, find Samantha, click the **pencil icon**.

6. In the **Rename user dialog box**, read the warning message and enter the following:

- First name: Sam
- Last name: Morse

Note: The First and Last name settings represent the Display Name.

7. Click **Rename user**.

If successful, you should see a banner stating that the changes have been saved.

It can take up to 10 minutes for a new primary email address to be reflected throughout the system, 24 hours for domain and personal contact changes to take effect, and up to 3 days before the user can use chat.

Suspend a User

Introduction to Exercise

As a Cloud Identity administrator, you can temporarily block a user's access to your organization's cloud services by suspending the user's account. This disables the account without deleting the user's profile and related information, such as documents, calendar events, and email. If the user has shared any documents, sites, or secondary calendars, these shared assets are still accessible to collaborators. A suspended user can't sign in to the account, and new information, such as emails and calendar invitations, are blocked.

Note: *A suspended user still requires a user license; therefore, a fee still applies.*

More Information

- Suspend a User Help Center Article

Exercise Scenario

After setting up your initial directory in Cloud Identity, you receive an email from Lars Ericsson:

Hey Cloud Identity Admin,

I had a contractor working with me last week for a project, his name is Jon Baird. He has an account to sign in to our system but for the next few weeks he'll be working somewhere else. Is there a way to prevent him from signing in without losing all the work he's done already? He'll be back to work with us soon.

Regards,

Lars Ericsson

Exercise Directions

1. Sign into your Google Admin console as the administrator user using **your administrator account name and password**.

2. Click the **Users icon**.

3. To suspend Jon Baird, find **his name** on the user list, click the three-dot elipsis, and choose Suspend user in the drop-down menu.

4. Click **Suspend**.

On Jon Baird's user account page, an exclamation point indicates Jon's suspended status.

5. Return to the **main user list**. In the **Filters list** at the side (if you don't see this list, click the Filters button), choose **Suspended users** in the **User Type drop-down list**.

The list now should contain user Jon Baird and any other currently suspended users.

Exercise Scenario Continued

A few weeks later, you receive another email from Lars Ericsson:

Hey Patrick,

I have a contractor, Jon Baird, who will be working with us again next week. He had an account before but is locked out at my request. Can you please re-enable him?

Regards, Lars Ericsson

As a Cloud Identity administrator, you can restore a user you (or another administrator) suspended.

Exercise Directions Continued

1. In the **user list**, filter for **suspended users**. Locate Jon Baird in the suspended users list and **click his name** to enter his account page.

2. To restore Jon’s suspended account, click the exclamation point and select **Reactivate**.

After Jon's user account is restored, his name should no longer be in the Suspended users list—he should now be back in Active users. Restored users can sign in and regain full access to their services.

Further Notes

- Administrators manually suspending users is just one way that a Google account can be suspended or disabled. If the user is manually suspended by an administrator, it's possible for an administrator to restore their account immediately.

- You can't restore an account that was suspended for abuse or for breaching the Google Terms of Service.
- You can't re-enable any user with an abusive account status. Administrators can contact Google Support for more information. These users won't be able to sign in to their Google Account.
- To see why a user was suspended, click the red exclamation point on their account page and view the error message. See Restore a suspended user for your corresponding recovery options.

Delete a User

Introduction to Exercise

If a user leaves your organization, you might want to delete their Google account. Data is purged within a matter of days. It's important to understand the different implications of suspending and deleting users, build a process for users leaving the company, and create a deletion policy that best suits your business needs.

However, be aware that there are many other considerations that should be handled before deleting an account; there may be many other types of data that could be lost without following proper steps.

Exercise Scenario

After some time working in your Cloud Identity domain, you get another email from Lars Ericsson:

Hey Admin,

That contractor I had working with me, Jon Baird, has finished up his project. Can you please delete his account from the system as he won't be working here anymore?

Regards,

Lars Ericsson

Exercise Directions

1. Sign into your Google Admin console as the administrator user using **your administrator account name and password**.

2. Click the **Users icon**.

3. To delete Jon Baird, find his name on the user list, **click the check box to the right of his name, click the three-dot ellipsis in the right hand corner**, and **choose Delete** user in the drop-down menu.

Note: *Because the user is suspended first, if you restore a deleted user, the Admin console restores the user as a suspended user*.

4. Return to the **user list** and confirm that Jon Baird is no longer listed. Search for the user in the **user search bar**. You should see the result: **There are no results to display.**

User Management

Restore a Recently Deleted User

Introduction to Exercise

You can restore a recently deleted user account for up to 20 days. After this period, the Admin console permanently deletes the user account and it can't be recovered, even if you contact Google technical support.

In most cases, restoring a deleted user account also restores the user's associated data, however, Google doesn't guarantee full data recovery for a deleted user.

Important:

- You must have super administrator privileges to restore a recently deleted user.
- You can't restore a recently deleted user if the deleted username matches an existing group name, another active username, or another user's email alias. If it does, you'll see a username already exists error message.
- You can't exceed your maximum number of user licenses. If you try to restore a deleted user when you don't have an available license, you'll see a domain is over user limit error message.

Exercise Scenario

The next day you get a high priority email from Lars Ericsson:

Hello Cloud Identity Admin,

I'm afraid I was a little premature in getting you to delete our HR contractor Jon Baird. We've decided to extend his contract and hire him as a full-time employee.

Is there any way you can restore his user account?

Regards, Lars Ericsson

Exercise Directions

1. Sign into your Google Admin console as the administrator user using **your administrator account name and password**.

2. Click the **Users icon**.

3. In the **Filters list** (click the **Filters button** if you don't see this list), choose **Recently deleted** users in the User Type drop-down list.

Note: *If you have multiple organizations in your domain, stay at the top-level organization—deleted users lose their organization details and are moved to the top-level organization.*

4. Locate **Jon Baird** in the list and check the box next to his name.

If a deleted user's name isn't in this list, the account has been fully deleted and can no longer be restored.

5. Click **Recover** user to restore Jon's user account and choose the organization to place him.

Note: *You can restore only one user at a time*.

- If the account restore is successful, you may see a banner message similar to “User account restore has been initiated, please wait for 2 hours for complete restore of the account.”
- It may take some time for the user to be visible again in the user list.
- If a user was suspended at the time the account was deleted, such as when you transfer ownership of a user's files, the user will still be suspended after the account is restored.

6. In the **Filters list**, choose **Suspended users** in the User Type drop-down list.

7. Restore the suspension and put Jon Baird back in the Active users list:

- In the Suspended users list, **find and click Jon's username**.
- On Jon's user account page, click the exclamation point and select **Reactivate**. Jon should now be back on the Active users list.

User Management

Create an Organization Unit

Introduction to Exercise

As a Cloud Identity administrator, you may want to create an organizational structure within your domain. There are several reasons why you would do this:

- To control which applications and services are available to users
- To configure the available services differently for different sets of users
- To configure different Chrome OS device settings for different sets of devices

Learn more about how user and device policies and organizational structures work.

Exercise Scenario

You receive a new email from the IT Manager, Alexa Bell, requesting to restructure your domain.

Hey Admin,

As you know we now have two people working in Support, their names are Will and Tom (see below for details). I want to set up a helpdesk to offer technical support to our employees and customers.

Is there any way you can set these guys up with some different settings than the rest of the employees? For example they will need access to some different services like chat, that I want blocked for everyone else.

Thanks, Alexa Bell

Employee	Position
Will Marconi	Support
Tom Edison	Support

Exercise Directions

1. Sign into your Google Admin console as the administrator user using **your administrator account name and password.**

2. Click the **Users icon**.

3. In the toolbar, click the **Filters icon** to see your organizations (also called orgs or organizational units).

4. Hover over the **top-level parent org**, most likely called yourdomain.com, to add a new sub organization, and **click the elipses that appears to the right**.

5. Click **Add sub organization**.

6. In the **Create new organization dialog box**, fill in the details of the new Support organization and **click Create Organization**.

7. Return to the parent organization users page, and from the list, select your two Support users: Will Marconi and Tom Edison.

8. In the toolbar on the top right, click the **Move to another organization** icon and choose your new Support org.

9. When the confirmation prompts, click **OK**.

You should now see your two users moved to your designated Support org.

- Users can move from one org to another.
- A user can only be in one organizational unit at a time unlike, for example, groups where a single user can be in multiple groups at once.

Create an Admin-Managed Group

Introduction to Groups

This lesson will take you through the different types of groups available in G Suite, and you'll work through how to create groups for your organization. Google Groups make it easy for your users to communicate with people they contact often. As the administrator, you can create and manage groups in the Google Admin console.

Help Center Articles

Review the following Help Center Articles in order to learn more about Groups

- Which groups best suit your service?
- Groups administrator FAQ
- Create a group
- Add users to groups
- Add all users to a group

Introduction to Exercise

Read through the scenario and directions below in order to practice creating admin-managed groups.

Exercise Scenario

The company wants to create the following groups that can be managed only by the system administrators as follows:

- OurCompany: An internal group of everyone in the company
- Management: A private or restricted group of all executives and managers

Exercise Directions:

1. Sign into your Google Admin console as the administrator user using the **your administrator account name** and **password**.

2. From the dashboard, click **Groups**

3. Click the **plus button** at the bottom of the groups page.

4. Enter the following details in the Create new group box:

- A **name** for the group: for this exercise, you'll create 2 groups one named "OurCompany" the other "Management."
- An **email address** for your new group. Ensure that you choose the appropriate domain from the list.
- **[Optional]** Add a **description** for your group.
- Choose an **Access Level** from the drop down list. See more about these options here. For this first group, choose **Team**. This will allow anyone within your domain that has an associated Google Account you're managing from the Admin console to post messages and view the members list.
- For the first group, **OurCompany**, check the box that **adds all users in the organization** to your new group

5. Click **Create**. You'll be taken to the group's page in the Admin console.

6. For the following group, **Management**, repeat the steps above, but do not add all users from the organization to this group.

- For this group, choose the **access level** restricted, which will only allow members of the group to post messages and view the member's list.
- Do **not** choose the option to add all users within your domain.
- Press **create.**

7. Once on the **Management** groups page, click **Manage users in Management**.

8. In the **"Add new members"** box, add the following users by typing their full Google accounts, including the domain, into the box. Ensure that you are adding them as "members."

- Samantha Morse - CEO - samantha.morse@[your domain]
- Ellie Gray - Lead Developer - ellie.gray@[your domain]
- Lars Ericsson - HR Manager - lars.ericsson@[your domain]

NOTE: *After you've create a group in the Admin console you can edit it to add or remove members, change a member's group role, change a group's name or description, and more.*

Security

Security Overview

This module will walk you through some of the security features that are available to you as the Cloud Identity admin. Make sure that you explore the Help Center articles that are linked below.

Help Center Articles

Review the following Help Center Articles in order to learn more about Security. We will be using these throughout these exercises to both guide our directions. You will see them referenced throughout the following exercises.

- Best practices and data privacy
- Protect against phishing
- Set up 2-step verification
- Set up SSO via a third party Identity provider (IdP)
- Security center

Navigate the Security Center

Introduction to Exercise

The Security center gives you a security dashboard and security health recommendations. The security center brings together security analytics, actionable insights and best practice recommendations from Google to empower you to protect your organization, data and users.

• See the Security Center articles to learn more.

Exercise Scenario

In this exercise, you'll navigate to the security center to view and understand your security dashboard and security health recommendations.

Exercise Directions

Access the Security Center dashboard

1. Sign into your Cloud Identity Admin Console as the administrator user using **your administrator account name and password.**

2. Click the **Security icon**.

3. Click on **Dashboard**. From here, you can get overview of key security metrics for:

Failed device login attempts — This report will show you details of failed login attempts on your corporate devices during a specified time range

Note: *See the Failed device login attempts report article to learn more.*

Compromised device events — This report will show you details of compromised device events.

Note: *Use this report to view device IDs, device owners, and the timestamps of compromised devices. See the Compromised device events report article to learn more.*

Suspicious device activities — What suspicious device activities have been detected? Details of suspicious activities on your corporate devices during a specified time range

Note: *Use this report to view device IDs, device owners, and the timestamps of the suspicious device activities. See the Suspicious device activities report article to learn more.*

OAuth grant activity report — This report is ranked by the growth in grants to apps in the current time period compared to the previous time period.

Note: *Use this report to monitor the OAuth grant activity in your organization by app, scope, or user. See the OAuth grant activity report article to learn more.*

OAuth grants to new apps report—This report shows the new apps that have been provided OAuth grants in the given time period compared to the previous similar time period.

Note: *Use this report to monitor the OAuth grant activity in your organization. See the OAuth grants to new apps report article to learn more.*

See Security dashboard to learn more**.**

Access the Security Center health page

1. From the **Admin console dashboard**, click the **Security icon**

2. Click on **Security health**. The security health page enables you to monitor the configuration of your Admin console settings and stay ahead of potential threats by examining security analytics and flagging threats.

• From here you can monitor the security health of the following settings:

Device management settings - you can monitor the configuration of the following Device management settings:

- Mobile management
- Blocking of compromised mobile devices
- Mobile password requirements
- Device encryption
- Mobile inactivity reports
- Auto account wipe for Android
- Mobile application verification for Android
- Installation of mobile applications from unknown sources

- External media storage

Security settings - you can monitor settings related to security and protection of user accounts:

- 2-step verification for users
- 2-step verification for admins
- Security key enforcement for users

See Get started with the security health page to learn more.

Congratulations! You now know how to access the Security center to view and understand your dashboard and health recommendations.

See Security dashboard to learn more.

Configure Common Security Settings

Introduction to Exercise

As an admin, there are some basic security settings you can enable and adjust in the Admin console to improve the overall security of your Cloud Identity instance.

Exercise Scenario

In this exercise, you'll modify and enable security features and settings for your entire domain.

Exercise Directions

1. Sign into your Google Admin console as the administrator user with **your administrator account name and password**.

2. From the **Admin console dashboard,** click on the **Security icon**.

3. Click on **Basic settings** to ensure **security features and settings are enabled** in the following sections:

- Password Recovery
- 2-step verification
- Less secure apps

4. By default, only a domain administrator can reset a user's password. The **Password Recovery** setting is applicable where you want to allow users to recover their own passwords. This achieved through the use of a recovery email address or phone number. To enable user password recovery, click the **Enable/disable non-admin user password recovery link**, and check **Enable non-admin user password recovery**.

Note:

- *See Set up password recovery for users for details on how to let your users reset their own passwords.*

5. In the **2-Step Verification section**, check **Allow users to turn on 2-step verification**.

- This makes 2-Step Verification available for your users, but does not automatically enroll them. To enroll, users need to configure their verification settings individually.
- Once all users have enrolled in 2-Step Verification, you can enforce 2-step verification.

Note:

- *See Set up 2-Step Verification for your domain for more information on how to enable 2-Step Verification, account recovery recommendations, and tips for deploying to your users.*

6. In **Less secure apps**, you can control access **to third-party apps that 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.

- Click on the link **Go to settings for less secure apps >>**. In the window that opens, your list of organizational units will be displayed in the left sidebar.
- **Click on the organizational unit to which you wish to apply the setting**.

Note:

- *By default, the box to Allow users to manage their access to less secure apps is checked.*
- *See Control access to less secure apps.*

7. Expand the **Password management** section. This is where password policies are set.

You can enforce strong passwords by checking the **Enforce strong password** box. You can also set a **Password length** policy by setting minimum and maximum length values. It is recommended to keep the minimum password length to at least 8 characters. You can enforce the length and strength policies when your users next login to their account or when they next change their password. The default enforcement is when the password is next changed.

The **Allow password reuse** box allows you to control whether your users can reuse their old passwords. We recommend you leave this option unchecked to prevent reuse.

You can also force your users to change their passwords after a certain number of days or allow them to never expire with the **Password expiration** setting. We recommend you allow passwords to never expire.

Note:

- *See Manage your users' password settings for more information on how to help keep your user's account secure.*
- *See Create a strong password & a more secure account for more information on how to choose a strong password.*

8. In **API reference**, check **Enable API access** to enable programmatic access to your Cloud Identity domain.

Note:

- *You have access to the Admin SDK—a collection of Application Programming Interfaces (APIs), so you can build customized administrative tools for your Google products. Before you can use the Admin SDK, you need to enable API access.*
- *See Enable API access in the Admin console*

9. In **Set up single sign-on (SSO)**, you can enable your users access to many applications without having to enter their username and password for each application.

- In the Setup SSO with Google identity provider option, you can set up SSO using Google as the identity provider using Security Assertion Markup Language (SAML), the user can use their managed Google account credentials to sign in to enterprise cloud applications.
- In the Setup SSO with third party identity provider option, you can set up SSO using a third-party as the identity providers so that Google is the service provider and users authenticate through a third-party Identity provider.

Congratulations! You can now view and modify basic security settings for your entire domain.