

QUICK START GUIDE FOR EVERYONE ON

Google Workspace

ADMIN VERSION



TABLE OF CONTENTS

Getting Started	1
Setting up Rules & Policies	1
Sending Invites	2
User Adoption	2
Kickoff Meeting	2
Admin Quick Start Guide	3
Brief Overview of the Features	4
Bulk Encryption Policies	7

GETTING STARTED

- The administrator of the Google Workspace signs in with their Google Account
- Administrator sets their own GarbleCloud Passphrase
- Administrator clicks 'Create an Organization'
- Administrator creates security questions and an organization passphrase (separate from the personal passphrase) for performing admin functions
- Organization is created and the admin dashboard becomes available
- Overview of all the Tabs in the Admin Dashboard

SETTING UP RULES & POLICIES

- Security Policies (based on what you want)
- Bulk encryption (based on how you want to proceed)



SENDING INVITES

- Creating other Admins (if applicable)
- Manual invites vs suggested users tab
- What end users see when invited to GarbleCloud (be sure to check spam folder)

USER ADOPTION

- Option 1: Bulk Encrypt files older than a certain number of days to get staff used to using the application
- Option 2: Bulk Encrypt certain types of files (Resumes only for example) to start until the end users learn the application
- Option 3: Bulk Encrypt everything and have each end user learn how to use the application Send each end user an encrypted file on how to use GarbleCloud

KICKOFF MEETING

- Explain importance of using GarbleCloud
- User learning materials
- Set expectations for use



ADMIN QUICK START GUIDE

Getting set up with GarbleCloud is a quick and straightforward process. The Google account you associate with your GarbleCloud purchase should be on the domain that you wish to add GarbleCloud to. After purchasing, you would sign in with their associated email address; it is very important that you are registered as an Admin in the backend Admin Panel of your company's Google Workspace. If you are the owner of the domain, you are already registered as an Admin.

Next you will be prompted to set up their own personal GarbleCloud Passphrase and personal Passphrase Recovery Questions. GarbleCloud requires each user to create their own passphrase and recovery questions, regardless of if you are an administrator or not. For Admins, GarbleCloud will need a second passphrase and set of recovery questions that is for the Admins only. The Organizational Passphrase will be needed to perform functions that affect the entire organization. You will be prompted to create this passphrase and recovery questions after you Create an Organization.

To Create an Organization, you will need to click the red icon on the notification bell. Next, click on the task called Create an Organization. Here a pop up will appear asking for Passphrase Recovery Questions and the Organizational Passphrase. Once you have completed both, your organization will be created. This will give you access to the Admin Panel and allow you to control users, give permissions, and bulk encrypt existing files within your Google Workspace. Any user that is given Admin permissions through the Google Admin Panel will automatically get access to the Admin Panel.



Accessing the Admin Panel is easy, on the GarbleCloud dashboard click your user profile in the top right hand corner and an option to go to the Admin Panel should appear next to the Logout option.

Here is a brief overview of the features in the Admin Panel:

USER	Shows all current users in your GarbleCloud organization. Admins are specified with '(Admin)' next to their name. Additional information like who they were invited by and if the account is Associated or Deleted from the organization.
SUGGESTED USERS	Shows all users on your domain that are not a part of your GarbleCloud organization. You may bulk invite these members by selecting the checkbox on the left side.
PENDING INVITES	Shows which users have been invited to your organization and have not yet accepted the invitation.
RESET PASSPHRASE REQUEST	Shows any passphrase reset requests submitted by users in your GarbleCloud organization.
PAYMENT SETTINGS	Shows payment information for your GarbleCloud plan. You may cancel your subscription or add a payment method here.
ACCOUNT TRANSFER	Shows all account transfers from old discontinued users to new user or existing user accounts.
BULK ENCRYPTION	Where you set rules, by a set criteria, to encrypt pre-existing files in your Google Workspace.

The next step in the process of integrating the GarbleCloud application to your organization is how you want to manage user adoption, security of encrypted files, and how information will flow in your organization.

GarbleCloud recognizes the challenge large organizations have when it comes to rolling out new technology, getting its users to learn fast, and use it without any major disruption in workflow. Ideally you want the GarbleCloud application to work for you right away and not work against your work productivity. Therefore, the GarbleCloud team recommends one of 3 ways to roll out the application to your organization.

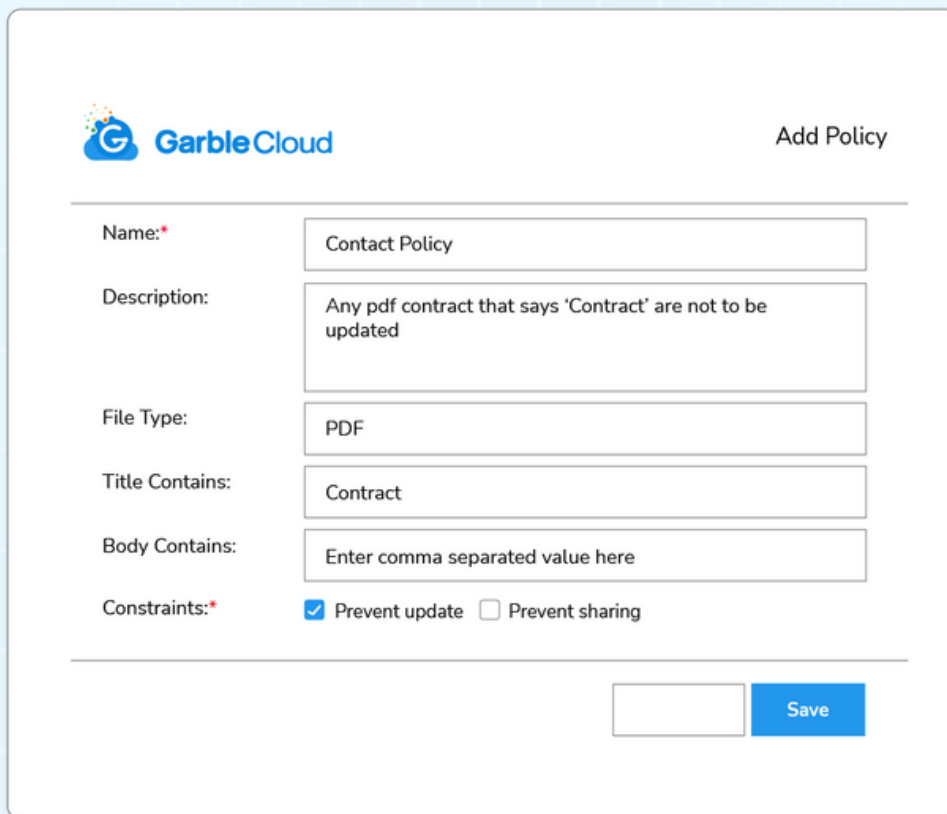
OPTION #1 LEAST FRICTION	Bulk Encrypt files older than a certain number of days to get staff used to using the application	Example: Files older than 90 days
OPTION #2 MILD FRICTION	Bulk Encrypt certain types of files to start until the end users learn the application.	Example: Legal Paperwork Only
OPTION #3 MOST FRICTION	Bulk Encrypt everything and have each end user learn how to use the application	Example: Bulk Encrypt files older than 0 days

Additionally, sending the User Quick Start Guide as an encrypted PDF may help users learn how to start using the application by opening the encrypted file in their GarbleCloud account.

Once you have chosen the rollout method you want to use within your organization, the next step is to create the necessary Security, Passphrase, and Bulk Encryption Policies to control document flow internally. The Bulk Encryption feature runs both on command and every 24 hours, allowing you to control how, when files are encrypted, and how they are shared. Security Policies specify how encrypted documents are shared. Currently you can target files you want to prevent updates on or prevent from being shared.



An example of this would be you would not want finalized contracts to be updated by anyone internally. As an Administrator, you can create a Security Policy that shows that you want anything with “Contract” in the title to not allow any updates. Here is an example:

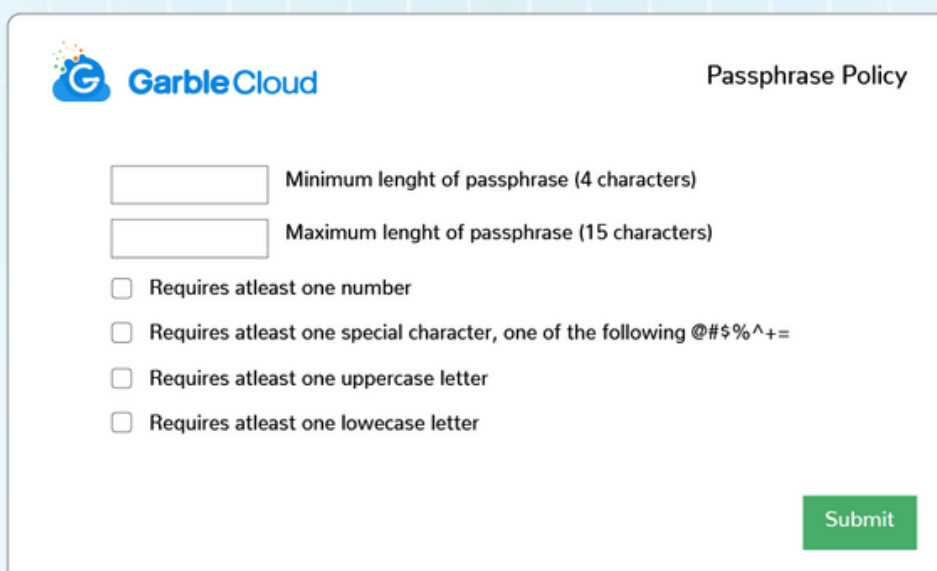


The screenshot shows the 'Add Policy' form in the GarbleCloud interface. The form includes the following fields and options:

- Name:** A text input field containing 'Contact Policy'.
- Description:** A text input field containing 'Any pdf contract that says 'Contract' are not to be updated'.
- File Type:** A text input field containing 'PDF'.
- Title Contains:** A text input field containing 'Contract'.
- Body Contains:** A text input field containing 'Enter comma separated value here'.
- Constraints:** Two checkboxes: 'Prevent update' (checked) and 'Prevent sharing' (unchecked).

At the bottom right of the form is a 'Save' button.

Once you have created your Security Policies you will then create your User Passphrase Policy. This policy will set constraints or minimums for the user's passphrases. Some constraints include Minimum or Maximum length, requirement of numbers, special characters, at least one uppercase, and at least one lowercase. To find the User Passphrase Customization page, select the first option in the settings tab within the Admin Panel.



The screenshot shows the 'Passphrase Policy' form in the GarbleCloud interface. The form includes the following fields and options:

- Minimum length of passphrase (4 characters):** A text input field.
- Maximum length of passphrase (15 characters):** A text input field.
- Requires atleast one number:** A checkbox.
- Requires atleast one special character, one of the following @\$%^+=:** A checkbox.
- Requires atleast one uppercase letter:** A checkbox.
- Requires atleast one lowercase letter:** A checkbox.

At the bottom right of the form is a green 'Submit' button.

BULK ENCRYPTION POLICIES

Once you have created your User Passphrase Policy, next you will need to create your Bulk Encryption Policies in line with how you want to roll out the GarbleCloud application to your organization. Here are examples of the policies you would add in relation to which roll-out method chosen above

Option #1

Bulk Encryption Rule

Encrypt files older than day/s

File name contains

File text contains

☒ Enable Rule

Update

Option #2

Bulk Encryption Rule

Encrypt files older than day/s

File name contains

File text contains

☒ Enable Rule

Submit

Option #3

Bulk Encryption Rule

Encrypt files older than day/s

File name contains

File text contains

☒ Enable Rule

Update

Finally, it's time to start inviting users to your organization. You have 2 options to invite users from your organization one being the invite user tab on the home interface. This invite method allows for single invites if you have a small number of users. If you have a larger number of users, you will be able to bulk invite users in the 'Suggested User' tab in the Admin Panel. In the admin panel, select the check box for all or some users on your domain address to send an invitation to your organization on the GarbleCloud application.

Once users sign up for an account they will be able to start using the GarbleCloud application. You are able to see all pending invites in the 'Pending Invites' tab within the Admin Panel. To get users started on learning the GarbleCloud application better, we recommend that you share the User Quick Start Guide with each of the users in your organization so they can get started on their GarbleCloud journey!

For ongoing support, contact our support team at: alex.ames@garblecloud.com. Our support team can answer any questions on how to get started, or can provide set up assistance.