GOOGLE WORKSPACE CLIENT-SIDE ENCRYPTION

Integration Guide

Applicable Services:
VirtuCrypt Enterprise Key Management

TABLE OF CONTENTS

[1] OVERVIEW OF THE GOOGLE WORKSPACE CSE / VIRTUCRYPT INTEGRATION

[1.1] ABOUT GOOGLE WORKSPACE CSE

From the Google Workspace Admin Help website: "You can use your own encryption keys to encrypt your organization's data, in addition to using the default encryption that Google Workspace provides. With Google Workspace Client-side encryption (CSE), content encryption is handled in the client's browser before any data is transmitted or stored in Drive's cloud-based storage. That way, Google servers can't access your encryption keys and, therefore, can't decrypt your data. To use CSE, you'll need to connect Google Workspace to an external encryption key service and an identity provider (IdP)."

[1.2] ABOUT VIRTUCRYPT

The VirtuCrypt Hardened Enterprise Security Cloud service offers organizations cloud access to Futurex's innovative data security solutions suite. VirtuCrypt was designed from the ground up to provide customization and flexibility while addressing compliance mandates and industry standards. All the critical elements of a secure cloud service such as privacy, data security, continuous monitoring, incident management, and endpoint security have been incorporated into a state-of-the-art technology platform.

VirtuCrypt's Hardened Enterprise Security Cloud provides substantial benefits:

- Rapid deployment and fulfillment of a needed service
- Reduced capital and operational expenses for hardware, training, compliance, and more
- On-the-fly scalability, ensuring unexpected increases in throughput are easily met
- High availability data center architecture with SLA-backed uptime
- Immediate access to the latest firmware updates, features, and hardware
- Established reliability, with over 40 years of experience providing innovative solutions and 24x7x365 support to organizations worldwide

[1.3] PURPOSE OF THE INTEGRATION

Google Workspace already uses the latest cryptographic standards to encrypt all data at rest and in transit between its facilities. With CSE, however, you have direct control of encryption keys and the identity provider used to access those keys to further strengthen the security of your data.

Your organization might need to use CSE for various reasons—for example:

- **Privacy**—Your organization works with extremely sensitive intellectual property.
- **Regulatory compliance**—Your organization operates in a highly regulated industry, like aerospace and defense, financial services, or government.

[1.4] BASIC SETUP STEPS FOR GOOGLE WORKSPACE CSE

Step 1: Set up your external encryption key service

First, you'll set up an encryption key service through one of Google's partner services (i.e., VirtuCrypt). This service controls the top-level encryption keys that protect your data.

Step 2: Connect Google Workspace to your external key service

Next, you'll specify the location of your external key service, so Google Workspace can connect CSE for supported apps to it.

Step 3: Connect Google Workspace to your identity provider

An Identity Provider (IdP) verifies the identity of users before allowing them to encrypt content or access encrypted content.

For this version of the Google Workspace CSE integration, in addition to using VirtuCrypt as the external key service, VirtuCrypt also serves as the identity provider.

Note: The KMES Series 3 version of the Google Workspace CSE integration supports the ability to connect Google Workspace to any third-party IdP or Google identity, using either the Admin console or a .well-known file hosted on your server. Learn more

Step 4: Turn on CSE for users

You can turn on CSE for any organizational units or groups in your organization. Note, however, that you need to turn on CSE only for users that you want to create client-side encrypted content:

- **Google Drive**—You need to turn on CSE only for users who need to create client-side encrypted documents, spreadsheets, and presentations or upload client-side encrypted files to Drive. You don't need to turn on CSE for users who only view and edit files shared with them.
- **Google Meet**—You need to turn on CSE only for users who need to host client-side encrypted meetings. You don't need to turn on CSE for other participants in meetings.

For details about turning on CSE for users, see Create client-side encryption policies.

[1.5] GOOGLE SERVICE-LEVEL REQUIREMENTS FOR CSE

Administrator requirements

To set up Google Workspace Client-side encryption for your organization, you need to be a Super Admin for Google Workspace.

User requirements

- Users need a Google Workspace Enterprise Plus, Google Workspace for Education Plus, or Enterprise Essentials license to use CSE to:
    - Create or upload files
    - Host meetings
- Users can have any type of Google Workspace or Cloud Identity license to:
    - To view, edit, or download an existing file encrypted with CSE
    - Join a CSE meeting
- Users with a consumer Google Account (such as Gmail users) can't access CSE files or participate in CSE meetings.
- To view or edit encrypted files, users must use either the Google Chrome or Microsoft Edge browser.
- To join a CSE meeting, users must be invited or added during the meeting. Knocking isn't available for CSE meetings.
- Access to CSE files and meetings depends on your organization's CSE policies.

External user requirements

- During the beta, external users must have a Google Workspace license to access your content encrypted with CSE. Users with a consumer Google Account or a visitor account can't access files encrypted with CSE.
- External organizations must also set up CSE, either in the Admin console or with a .well-known file.
- Your external encryption service must allowlist the third-party IdP service that's used by the external domain or the individuals you want to use CSE. You can usually find the IdP service in their publicly available .well-known file, if they set up one. Otherwise, contact the external organization's Google Workspace admin for their IdP details.

[1.6] CLIENT-SIDE ENCRYPTION PROCESS

After an administrator enables CSE for their organization, users for whom CSE is enabled can choose to create encrypted documents using the Google Workspace collaborative content creation tools, like Docs and Sheets, or encrypt files they upload to Google Drive, such as PDFs.

After the user encrypts a document or file:

1. Google Workspace generates a DEK in the client browser to encrypt the content.
2. Google Workspace sends the DEK and authentication tokens to your third-party KACLS for encryption, using a URL you provide to the Google Workspace organization's administrator.

3. Your KACLS uses this API to encrypt the content, then sends the obfuscated, encrypted data back to Google Workspace.
4. Google Workspace stores the obfuscated, encrypted data in the cloud. Only users with CSE enabled and access to your KACLS are able to access the data.

For more details, see Encrypt and decrypt files.

[1.7] PERSONAL KEYS AND KEY ROTATION IN VIRTUCRYPT

What are Personal Keys?

Personal Keys in VirtuCrypt are used for encrypting data for Google CSE. The first time a user creates an encrypted document or encrypts and uploads a file to Google Drive, VirtuCrypt generates a Personal Key for that user. Personal Keys created for CSE are AES-256 Data Encryption Keys. VIP users can view their Personal Keys by selecting the **Google Workspace CSE // Enterprise Key Management** service in their VIP account and navigating to *Personal Keys* in the left-hand menu.

Automatic key rotation

By default, newly-generated Personal Keys are assigned a **Regenerative** rotation policy with the **Validity Period** set to **1** month. At the time of writing, the default rotation policy cannot be modified, but this functionality will be added in a later release.

Note: Only one Personal Key can be active at a time for CSE users. After a key is rotated, it remains stored in VirtuCrypt and will be used for decrypting any documents that were encrypted using that key. Every document encrypted after a key is rotated will be encrypted using the new active key.

[2] IDENTITY AND ACCESS MANAGEMENT (IAM)

[2.1] SETUP OF IAM IN THE VIRTUCRYPT INTELLIGENCE PORTAL (VIP)

VIP Users with the **Admin** role have the ability to log in to the VIP web portal and add/modify/remove user accounts from their VIP account. Since VirtuCrypt serves as the identity provider (IdP) for this version of the integration, VIP admins can control access to Google CSE services within their VIP account by assigning the **Google CSE Personal Key User** role to users.

Perform the following steps to assign the **Google CSE Personal Key** role to a user in your VIP account:

1. Log in to the VIP web portal with a user assigned the **Admin** role.
2. Select *Settings* in the left-hand menu.
3. Scroll to the bottom of the *Settings* -> *General* menu to the **User Management** section.
4. Select **Add User**.
5. Fill in the required information, and in the **Roles** dropdown, select **Google CSE Personal Key User**, then click **OK** to finish creating the user.

[2.2] SETUP OF IAM IN GOOGLE WORKSPACE

In Google Workspace, you need to turn on Client-side encryption (CSE) for all users who need to do any of the following:

- Create or upload encrypted files to Google Drive
- Host encrypted meetings with Google Meet (beta)

Note: You don't need to turn on CSE for users who only need to view or edit encrypted files or attend meetings. However, external users need to use an identity provider (IdP) allowlisted by your domain. For details, see "External user requirements" in About client-side encryption.

To turn on CSE for users, you need to turn on CSE for the organizational units or configuration groups the users belong to.

At any time, you can disable CSE for users by turning CSE off for the organizational units or configuration groups they belong to. If you disable CSE for users, any existing client-side encrypted content remains encrypted and accessible.

Please refer to this Google Workspace knowledge base article for instructions on how to perform the following steps for setting up IAM for CSE in Google Workspace:

1. Set the default key service for your organization
2. Turn CSE on or off for users

[3] CONFIGURING EXTERNAL KEY SERVICE AND IDENTITY PROVIDER FOR CSE IN THE GOOGLE ADMIN CONSOLE

This section will describe the steps required to configure VirtuCrypt as the external key service and identity provider (IdP) for CSE in the Google Admin Console.

[3.1] CONNECTING GOOGLE WORKSPACE TO VIRTUCRYPT FOR CLIENT-SIDE ENCRYPTION

Before outlining the configuration steps, a couple of terms should be defined. **KACLS** stands for **Key Access Control List Service**, and this is your external key service (i.e., VirtuCrypt) that uses this API to control access to encryption keys stored in an external system. **IdP** stands for **Identity Provider**, and it is the service that authenticates users before they can encrypt files or access encrypted files. For the VirtuCrypt version of the Google Workspace CSE integration guide, VirtuCrypt serves as both the KACLS and the IdP.

KACLS Configuration

1. Sign in to your Google admin console.

   Note: Sign in using an account with super administrator privileges.
2. In the main menu, select *Security -> Access and data control -> Client-side encryption*.
3. Click the **External key service** card to open it.
4. Click **Add external key service**.
5. Enter a name for your key service.
6. Enter the URL for your key service (i.e., https://cse.virtucrypt.com:8889/kmes/v7/key-encrypt/client).
7. To confirm that Google Workspace can communicate with the external key service, click **Test connection**.
8. To close the card, click **Continue**.

IdP Configuration

To connect Google Workspace to the VirtuCrypt identity provider (IdP) you must configure the **Client ID** and **Discovery URI** in the Admin console. After establishing the connection, you need to allowlist your IdP in the Admin console.

1. Sign in to your Google admin console.

   Note: Sign in using an account with super administrator privileges.
2. In the main menu, select *Security -> Access and data control -> Client-side encryption*.
3. Under **Identity provider configuration**, click **Configure IdP fallback**.
4. Enter the details for your IdP.

a. In the **Name** field, specify a descriptive name to help identify your IdP. It will be shown in IdP messages for users.

b. In the **Client ID** field, you need to specify the OpenID Connect (OIDC) client ID that the CSE client application uses to acquire a JSON Web Token (JWT).

   To determine the client ID, log in to the VIP web portal as an admin user and go to *Settings* -> *Credentials*. You will see the Client ID listed under **OAuth 2.0 Clients**.

c. In the **Discovery URI** field, specify the OIDC discovery URL (i.e., https://vip.virtucrypt.com/.well-known/google-cse-jwks.json).

d. In the **Grant type** field, select the **Authorization code with PKCE** OAuth flow to use for OIDC.

e. Click **Test connection**.

   If Google Workspace can connect to your IdP, the "Connection success" message appears.

f. Click **Add provider** to close the card.

[4] VALIDATION & TESTING

In this section, we will do the following:

1. Validate that Google Workspace can successfully connect to the external key service (i.e., VirtuCrypt)
2. Validate that Google Workspace can successfully connect to the configured Identity Provider (IdP)
3. Test the creation of a blank encrypted Google Doc
4. Test encrypting and uploading a file to Google Drive
5. Test sharing an encrypted Google Doc

[4.1] VALIDATE SUCCESSFUL CONNECTION FROM GOOGLE WORKSPACE TO VIRTUCRYPT

1. Sign in to your Google admin console.

   Note: Sign in using an account with super administrator privileges.

2. In the main menu, select *Security* -> *Access and data control* -> *Client-side encryption*.
3. Click **Test connection**.

   If Google Workspace can connect to VirtuCrypt, a green checkmark and the "Your external key service is active" message appears.

[4.2] VALIDATE SUCCESSFUL CONNECTION FROM GOOGLE WORKSPACE TO THE CONFIGURED IDENTITY PROVIDER (IDP)

1. Sign in to your Google admin console.

   Note: Sign in using an account with super administrator privileges.

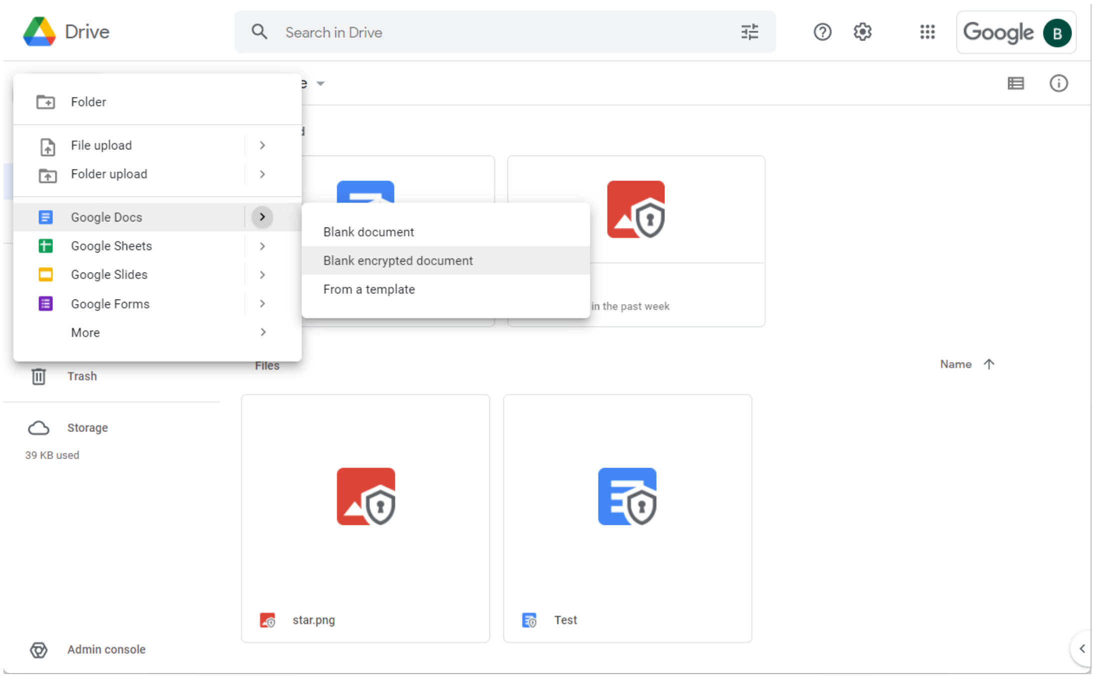
2. In the main menu, select *Security* -> *Access and data control* -> *Client-side encryption*.
3. Click the **Identity provider configuration** card to open it.
4. Click **Test connection**.

   If Google Workspace can connect to your IdP, the "Connection success" message appears.

[4.3] TEST THE CREATION OF A BLANK ENCRYPTED GOOGLE DOC

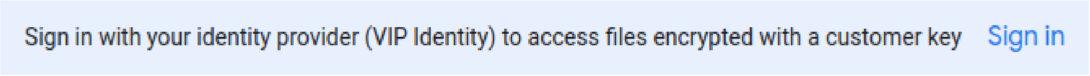
1. Sign in to Google Drive with your CSE user.

2. Click the **New** button, then select **Google Docs** -> **Blank encrypted document**.



3. A message will appear warning you that intelligent features such as spelling and grammar won't work with encrypted files, collaboration features will be limited, and only certain people can access encrypted files due to admin settings. Click **Create**.

4. If this is the first encryption operation you have attempted with Google Workspace CSE, the following message will appear at the top of the page prompting you to sign in with your identity provider.



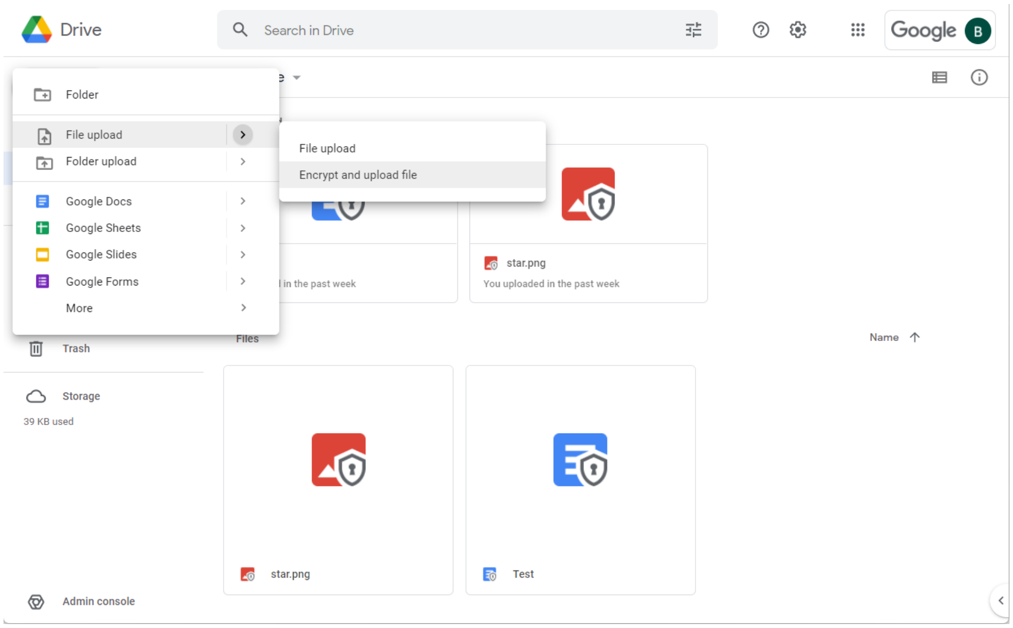
Sign in with your identity provider (VIP Identity) to access files encrypted with a customer key Sign in

Click **Sign In**, which will redirect you to your IdP's website to sign in. After signing in and allowing your IdP access to your Google Account, you will be redirected back to the Google Doc, which should now be encrypted. A confirmation message will appear if encryption is successful. Then you can edit and save the document per the normal process.

[4.4] TEST ENCRYPTING AND UPLOADING A FILE TO GOOGLE DRIVE

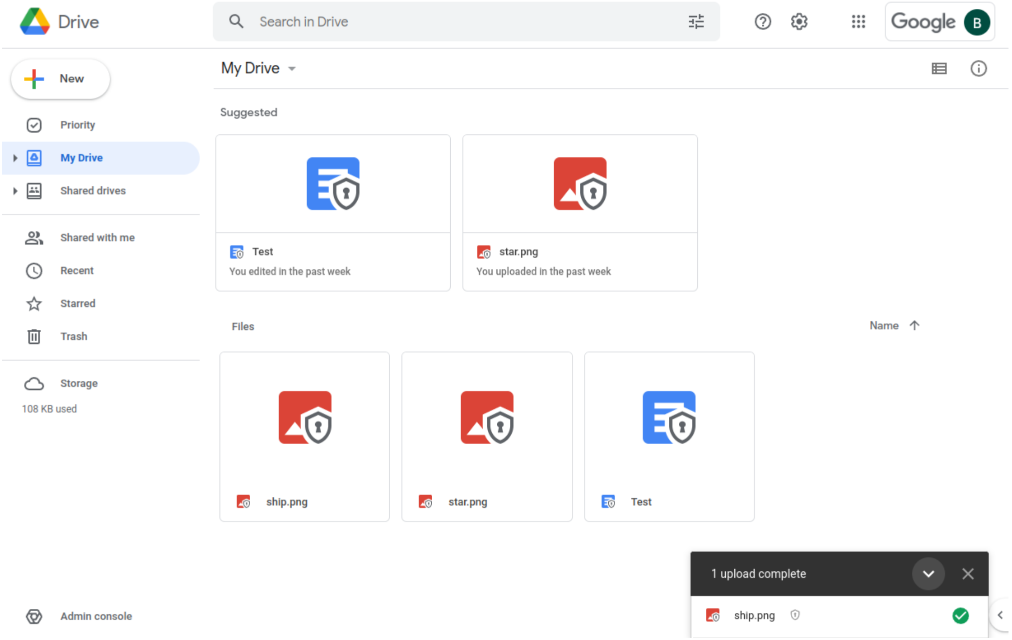
1. Sign in to Google Drive with your CSE user.

2. Click the **New** button, then select **File upload** -> **Encrypt and upload file**.



3. A message will appear warning you that some features, such as full-text search and file preview, will be unavailable and that only certain people can access encrypted files due to admin settings. Click **Select file**.

4. If this is the first encryption operation you have attempted with Google Workspace CSE, you will be prompted to sign with your identity provider. If this is the case, click **Sign In**, which will redirect you to your IdP's website to sign in. After signing in and allowing your IdP access to your Google Account, you will be redirected back to Google Drive, and the encrypted file upload will commence. Uploads are displayed in the bottom-right corner of the page, and once the upload completes, you will see a green checkmark and an updated status message similar to the image below:



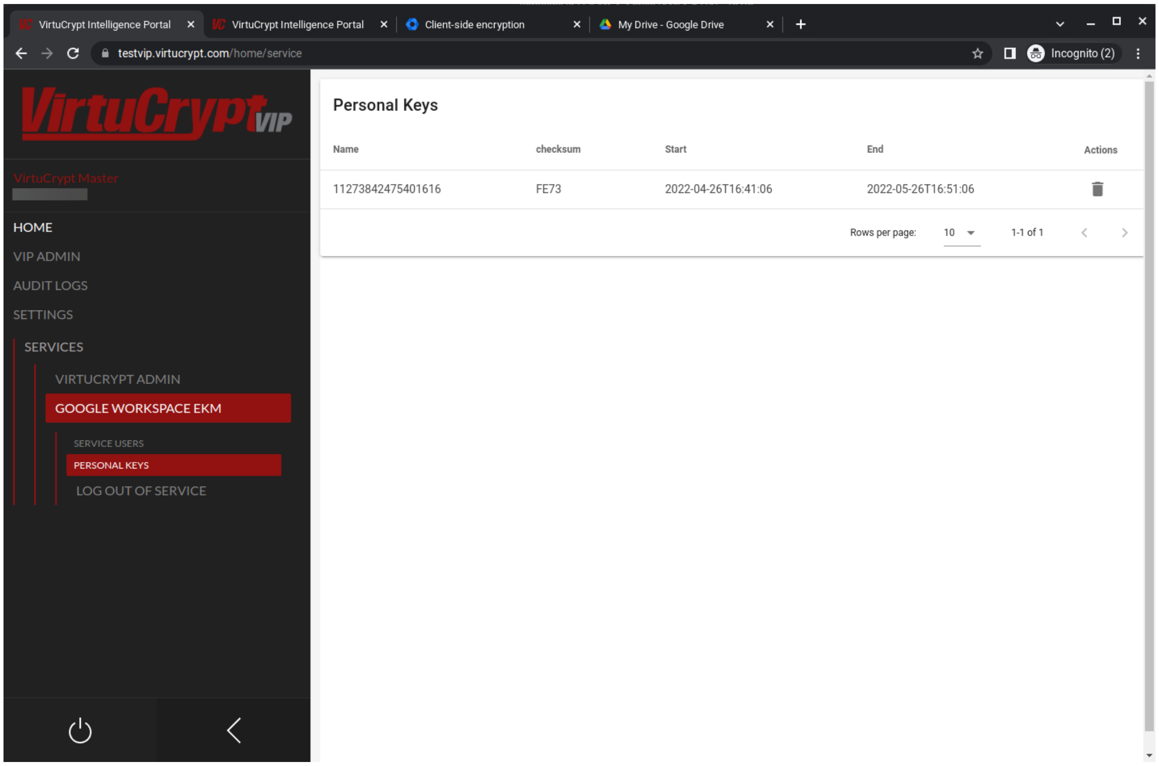
1 upload complete

ship.png ✓

[4.5] VIEWING PERSONAL KEYS IN THE VIRTUCRYPT INTELLIGENCE PORTAL (VIP)

The first time that a Google CSE user creates an encrypted document or encrypts and uploads a file to Google Drive, a **Personal Key** is created in VirtuCrypt and associated with that user. The Personal Key is then used for all CSE operations performed by that user in Google Workspace.

VIP users can view their Personal Keys by selecting the **Google Workspace CSE // Enterprise Key Management** service in their VIP account and navigating to *Personal Keys* in the left-hand menu. You will see something similar to the following:



Personal Keys

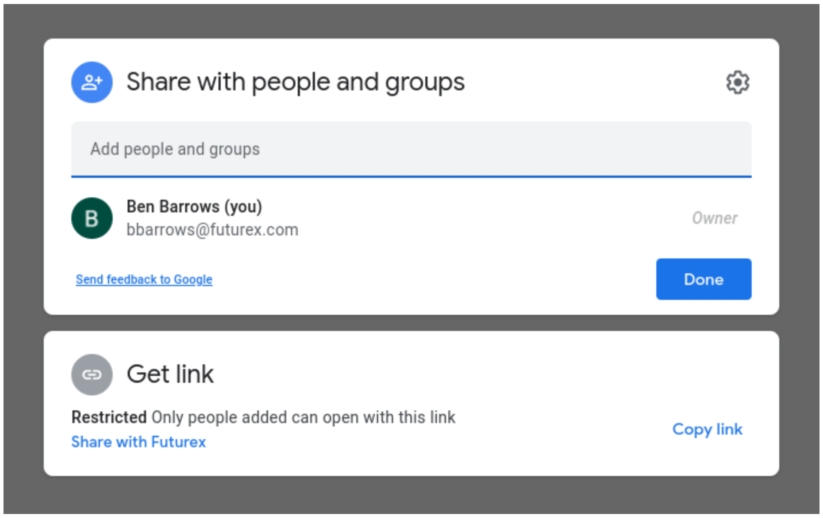
Name	checksum	Start	End	Actions
11273842475401616	FE73	2022-04-26T16:41:06	2022-05-26T16:51:06	🗑

Rows per page: 10 1-1 of 1

In addition to individual VIP users being able to manage their own keys, VIP Users with the **Admin** role can manage the Personal Keys of all Google CSE users within their VirtuCrypt account.

[4.6] TEST SHARING AN ENCRYPTED GOOGLE DOC

1. Sign in to Google Drive with your CSE user.
2. Right-click the encrypted document you would like to share and select **Share**, or, if you have the document open, you can click the **Share** button in the upper-right corner of the page.
3. In the following dialog, add people and groups you would like to share the encrypted document with and then click **Done**.



Share with people and groups

Add people and groups

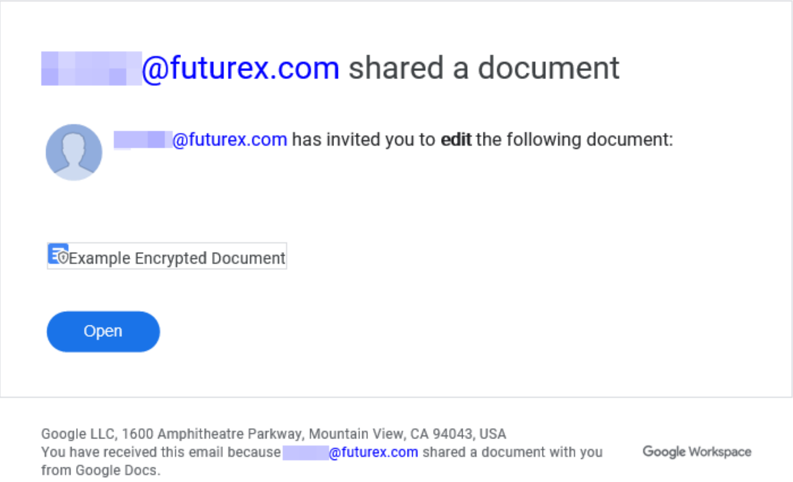
Ben Barrows (you)
bbarrows@futurex.com — Owner

Get link

Restricted Only people added can open with this link
Share with Futurex

Note: Only share encrypted documents with other Google CSE users that your company administrator has set up with an account in VIP. If they do not have a user configured in VIP, they will not be able to decrypt, view, and edit the file you are sharing.

4. Users you shared the encrypted file with will receive an email that looks similar to the image below:



[redacted]@futurex.com shared a document

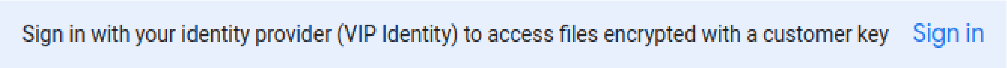
[redacted]@futurex.com has invited you to **edit** the following document:

Example Encrypted Document

Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
You have received this email because [redacted]@futurex.com shared a document with you from Google Docs.

5. After the user clicks **Open** in the email they received, their browser will be redirected to sign in to Google. After signing in to Google (using the same email configured for their user in VIP), they will be redirected to the shared Google Doc.

6. After a few seconds, the following message will appear at the top of the page. Click **Sign in**.



Sign in with your identity provider (VIP Identity) to access files encrypted with a customer key

The user will be redirected to the configured Identity Provider (IdP) to sign in. After signing in and allowing the IdP access to the Google Account, the user will be redirected back to the Google Doc, which should now be encrypted. A confirmation message will appear if encryption is successful. Then the document can be edited and saved per the normal process.

APPENDIX A: TROUBLESHOOTING GOOGLE CSE

In the early stages of the Google CSE Beta, you may encounter unintuitive errors with no clear resolution guidance, such as the ones described below.

Error 404/Not Found on callback URL

If during testing you are getting a 404 when your IdP redirects to this URL after login (for example when you're uploading a new file), this can have one of the following causes:

- (during Google CSE Beta) Google needs to whitelist your user or issuer
- (during Google CSE Beta) You signed into several Google accounts, and the test user is not the default user on your browser. Try to log out of all accounts and only sign into the target test account. Alternatively, use Incognito mode in Chrome with only the target test account.

An error occurred with the identity provider service

This can manifest as an error saying "An error occurred with the identity provider service", or "Can't decrypt file (Something went wrong and your file wasn't downloaded)", or "An error occurred with identity provider service". There are two possible causes:

- (during Google CSE Beta) Your browser did not yet authenticate with your IdP within drive.google.com. To authenticate during Beta, upload a drive file first instead, go through an "Upload failure" and force re-authentication as described below. Then you can go back to your original task (opening file, updating doc, etc.).
- Your IdP is misconfigured, such as the user you are logged in with was not assigned to the IdP app, or wrong Client ID in cse-configuration, etc. To debug, you can observe the browser network tab, or ask Google.

Upload failure

You can see an "Upload failure" on drive.google.com when you are uploading an encrypted file and have not yet been authenticated on this browser. To resolve, click the exclamation mark in a red circle (!) shown with this error. This will force re-authentication.

Re-authenticating through the encrypted file upload workflow will fix other authentication issues around the Drive/Docs apps that don't yet have their own robust auth error handling mechanism.

APPENDIX B: XCEPTIONAL SUPPORT

In today’s high-paced environment, we know you are looking for timely and effective resolutions for your mission-critical needs. That is why our Xceptional Support Team does whatever it takes to ensure you have the best experience and support possible. Every time. Guaranteed.

- 24x7x365 mission critical support
- Level 1 to level 3 support
- Extremely knowledgeable subject matter experts

At Futurex, we strive to supply you with the latest data encryption innovations as well as our best-in-class support services. Our Xceptional Support Team goes above and beyond to meet your needs and provide you with exclusive services that you cannot find anywhere else in the industry.

- Technical Services
- Onsite Training
- Virtual Training
- Customized Consulting
- Customized Software Solutions
- Secure Key Generation, Printing, and Mailing
- Remote Key Injection
- Certificate Authority Services

Toll-Free: 1-800-251-5112

E-mail: support@futurex.com

ENGINEERING CAMPUS

864 Old Boerne Road
Bulverde, Texas, USA 78163
Phone: +1 830-980-9782
+1 830-438-8782
E-mail: info@futurex.com

XCEPTIONAL SUPPORT

24x7x365
Toll-Free: 1-800-251-5112
E-mail: support@futurex.com

SOLUTIONS ARCHITECT

E-mail: solutions@futurex.com