GOOGLE WORKSPACE CSE (CLIENT-SIDE ENCRYPTION)

Integration Guide

Applicable Devices:
CryptoHub
Applicable Versions:
7.0.2.x and above

TABLE OF CONTENTS

[1] OVERVIEW OF THE GOOGLE WORKSPACE CSE / CRYPTOHUB 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] WHAT IS CRYPTOHUB?

CryptoHub is the most flexible and versatile cryptographic platform in the industry. It combines every cryptographic function within Futurex's extensive solution suite. Users operate CryptoHub with a simple web dashboard to deploy virtual cryptographic modules to fulfill nearly any use case.

[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., CryptoHub). 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

For this step, you'll need to connect to either a third-party IdP or Google identity, using either the Admin console or a .well-known file hosted on your server. Your IdP verifies the identity of users before allowing them to encrypt content or access encrypted content. Learn more

Note: In this integration guide we demonstrate using VirtuCrypt as the identity provider.

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 Key Access Control List Service (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 CRYPTOHUB

What are Personal Keys?

Personal Keys in CryptoHub 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, CryptoHub generates a new Personal Key specifically for that user. Personal Keys created for CSE are AES-256 Data Encryption Keys. CryptoHub users can

view their Personal Keys by navigating to the **Users** menu for the deployed Google CSE service, selecting their user, and selecting **Keys**.

Automatic key rotation

By default, the **Validity Period** for newly-generated Personal Keys is set to **1** month.

Note: Only one Personal Key can be active at a time for CSE users. After a key is rotated, it remains stored in CryptoHub 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] FUTUREX CERTIFICATION PROCESS

The Futurex Certification Process is a rigorous and standardized approach to testing and certifying integrations between third-party applications and Futurex's HSMs and key management servers (i.e., KMES Series 3). The certification process is designed to ensure that third-party application integrations are fully tested and validated in a lab environment before they are deployed in a production environment. Futurex's Integration Engineering team implements this process so that customers can have confidence that third-party applications will integrate seamlessly with Futurex's HSMs and KMES Series 3 devices, and that all operations will result in the expected behavior. The certification process involves several steps, including research, testing, troubleshooting, and certification, and is fully documented in an integration guide for each integration. The full process is outlined below:

1. Research the third-party application to gain a general understanding of the solution and the protocol it uses to integrate with an HSM or KMS device (i.e., PKCS #11, Microsoft CNG, JCE, OpenSSL Engine, KMIP).
2. Determine the scope of the third-party application's use of the HSM or KMS device, including the specific functionalities it utilizes (i.e., data encryption, key protection, entropy, etc.).
3. Install and configure the third-party application in a lab environment, where all testing and validation will take place.
4. Establish a connection between the third-party application and the Futurex device, which typically involves configuring TLS certificates and creating roles and identities that the third-party application will use to connect and authenticate to the Futurex device.
5. Initiate a request from the third-party application to the Futurex device, such as generating keys or certificates, encrypting or decrypting data, or other cryptographic functions.
6. If any errors occur during the testing process, the Integration Engineering team will diagnose the issues and take necessary corrective actions. If necessary, the team will also document the error(s) by creating engineering change requests (ECRs) to ensure all issues are addressed and resolved before certification.
7. After any necessary engineering changes have been made, a new end-to-end test will be performed to ensure that all errors have been resolved and that all operations are successful.
8. Certify the integration by creating an integration guide that covers all necessary prerequisites, configurations required in both the third-party application and the Futurex device, and how to test the functionality.

Overall, following these steps helps ensure that the integration between the third-party application and the Futurex device is fully tested and validated, and that any errors or issues are resolved before the integration is certified as fully supported.

[3] IDENTITY AND ACCESS MANAGEMENT (IAM)

[3.1] CONNECTING GOOGLE WORKSPACE TO AN IDENTITY PROVIDER FOR CLIENT-SIDE ENCRYPTION

After you set up your external key service and connect it to Google Workspace, you need to connect Google Workspace to your **identity provider (IdP)**. Any IdP that supports **OAuth** can be utilized. Your external key service uses the IdP to authenticate users before they can encrypt files or access encrypted files.

[3.1.1] Choose your IdP for CSE

If you don't already use a third-party identity provider (IdP) with Google Workspace, you can set up your IdP for use with your key service in either of two ways:

- **Use a third-party IdP (recommended)**—Use a third-party IdP if your security model requires more isolation of your encrypted data from Google.
- **Use Google identity**—If your security model doesn't require additional isolation of your encrypted data from Google, you can use the default Google identity as your IdP.

[3.1.2] Choose how to connect to your IdP for CSE

You can set up your IdP—either a third party IdP or Google identity—using either a .well-known file that you host on your organization's website or the Admin console (which is your IdP fallback). There are several considerations for each method, as described in the table below.

Considerations	.well-known setup	Admin console setup (IdP fallback)
Isolation from Google	IdP settings are stored on your own server.	IdP settings are stored on Google servers.
Admin responsibilities	An IdP admin can manage your setup instead of a Google Workspace Super Admin.	Only a Google Workspace Super Admin can manage your IdP setup.
CSE availability	CSE availability (uptime) depends on availability of the server that hosts your .well-known file.	CSE availability corresponds to the general availability of Google Workspace services.
Ease of setup	Requires changing DNS settings for your server, outside of the Admin console.	Configure settings in the Admin console.
Sharing outside your organization	Your collaborator's external key service can easily access your IdP settings. This access can be automated and ensures your collaborator's service has immediate access to any changes to your IdP settings.	Your collaborator's external key service can't access your IdP settings in the Admin console. You must provide your IdP settings directly to your collaborator before you share encrypted files for the first time, as well as any time you change your IdP settings.

Please refer to the following Google Workspace knowledgebase article for further details on connecting Google Workspace to an identity provider (IdP):
https://support.google.com/a/answer/10743588?hl=en#zippy=%2Coption-to-connect-to-your-idp-using-a-well-known-file

[3.2] SETUP OF IAM IN GOOGLE WORKSPACE

You need to turn on Google Workspace 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:

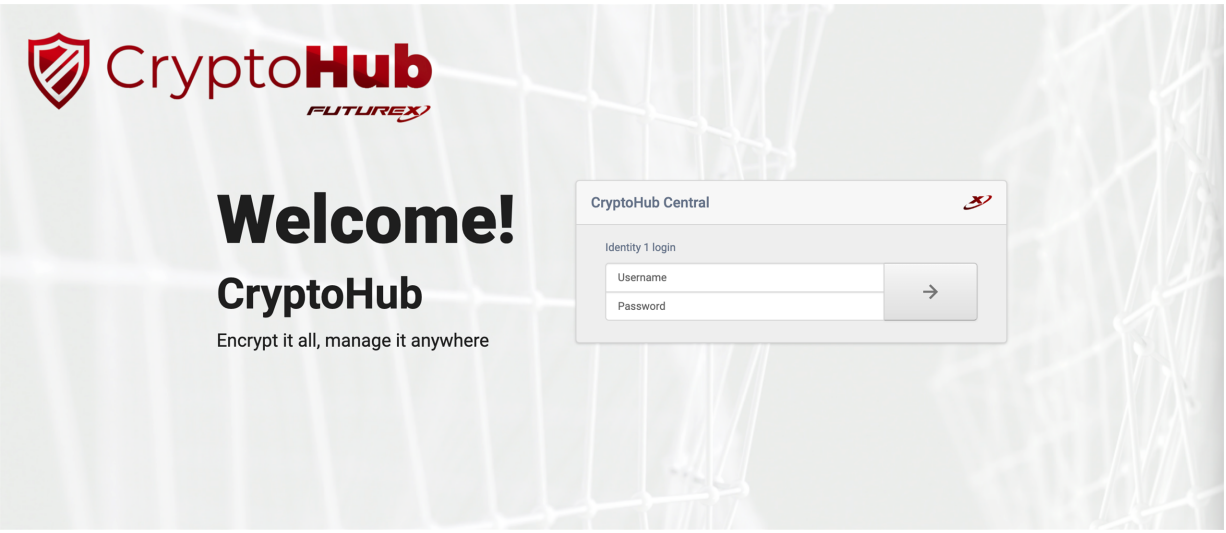
1. Set the default key service for your organization
2. Turn CSE on or off for users

[4] EXTERNAL KEY SERVICE SETUP FOR GOOGLE WORKSPACE CSE

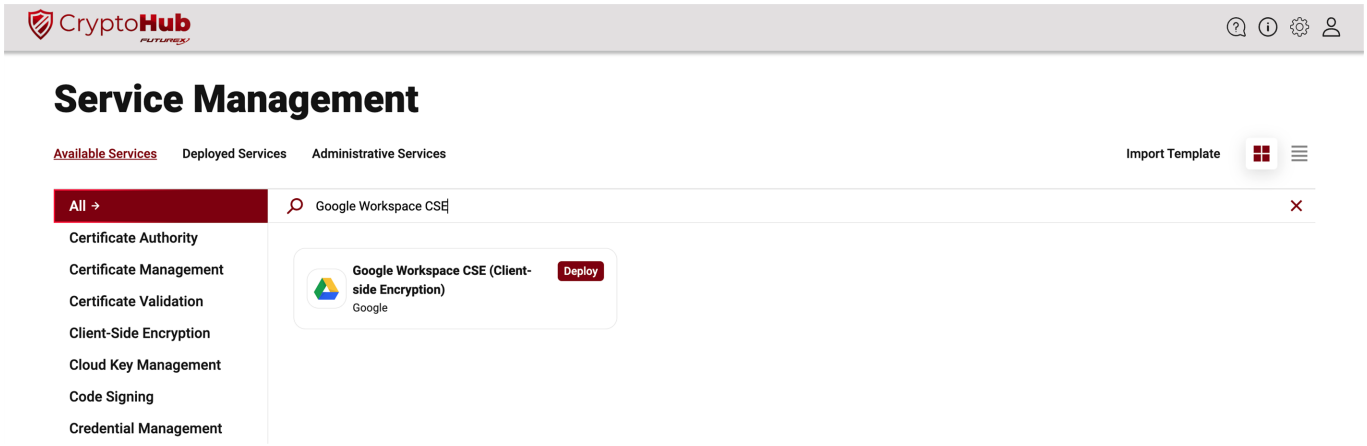
This section describes the steps required to use CryptoHub as an external key service for Google Workspace CSE. This involves deploying the Google Workspace CSE service in CryptoHub, as well as configuring a Key Access Control List Service (KACLS) and Identity Provider (IdP) in the Google Admin Console.

[4.1] DEPLOY THE GOOGLE WORKSPACE CSE SERVICE IN CRYPTOHUB

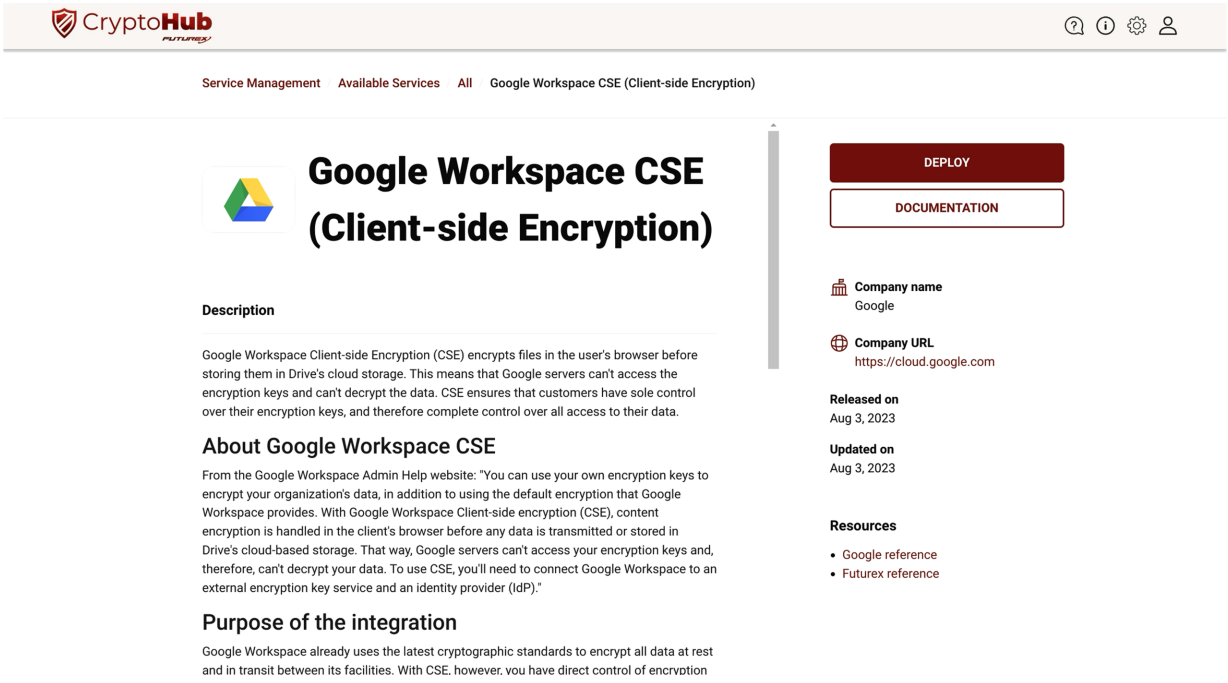
1. Open the CryptoHub web dashboard in a browser.



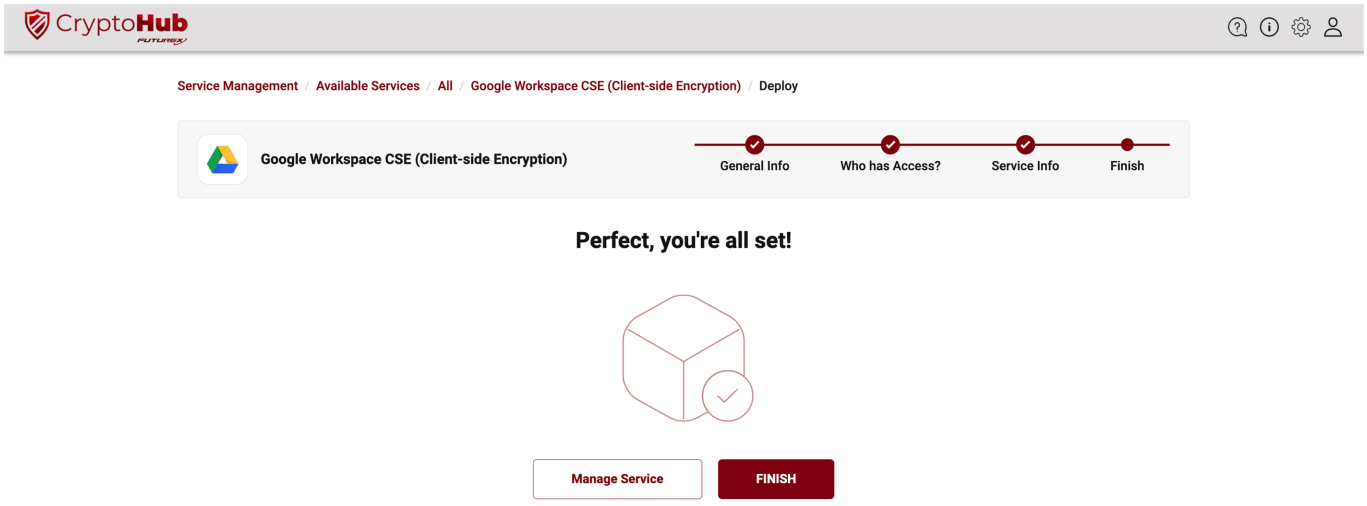
2. Log in to CryptoHub with the default Admin identities.
3. Select the **Google Workspace CSE (Client-side Encryption)** service from the list of available services on the **Service Management** page.



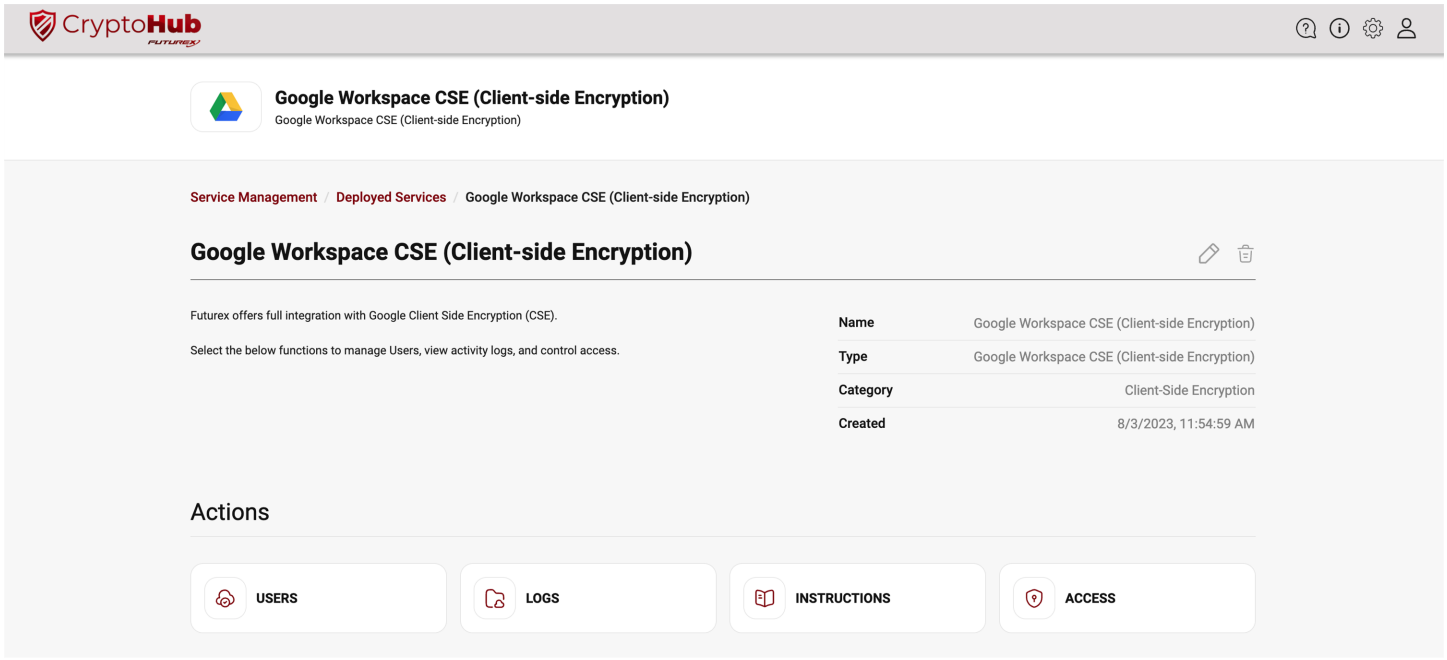
4. On the Google Workspace CSE service overview page, select **[Deploy]**.



5. Specify a **Service Name** and **Service Category**, then click **[Next]**.
6. (Optional) Select any **roles** and **identities** you want to be able to access the service, then click **[Next]**.
7. Select the **Identity Provider Type** you want to use, then fill in the required fields. Click **[Deploy]** when finished.
8. You will see a message confirming that the Google Workspace CSE service was successfully deployed.



Selecting **Manage Service** will bring you to the following page where you can create new service users, view logs, read instructions for using the service, and manage access permissions.



[4.2] CONFIGURATIONS IN THE GOOGLE ADMIN CONSOLE

[4.2.1] Configure KACLS and IdP 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., CryptoHub) that uses this API to control access to encryption keys stored in an external system. IdP's were discussed extensively in the previous section, but to reiterate, **IdP** stands for **Identity Provider**, and it is the service that authenticates users before they can encrypt files or access encrypted files. This integration uses VirtuCrypt as the IdP for demonstration purposes, but any IdP that supports OAuth can be used.

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://<server ip>/v0/key-encrypt/client).

   Note: Google requires this connection to be TLS, with a publicly-trusted certificate. The connection can be through NAT or reverse proxy.

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 your identity provider (IdP), you can use a .well-known file or the Admin console. After establishing the connection, you need to allowlist your IdP in the Admin console.

This section will walk through connecting Google Workspace to your IdP using the Admin console. However, this method is meant to serve as a fallback method for the .well-known file method. Please refer to the following Google Workspace documentation instructions on connecting Google Workspace to your IdP using a .well-known file: https://support.google.com/a/answer/10743588#config_wellknown&zippy=%2Coption-to-connect-to-your-idp-using-a-well-known-file

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).

      If you're using a third-party IdP: You generate this ID using your IdP's admin console.

      If you're using Google identity: You generate this ID using the Google Cloud Platform (GCP) Admin console. For details, go to "Create a client ID for Google identity".
   c. In the **Discovery URI** field, specify the OIDC discovery URL, as defined in this OpenID specification.

      If you're using a third-party IdP: Your IdP provides you with this URL, which usually ends with /.well-known/openid-configuration.

      If you're using Google identity: Use https://accounts.google.com/.well-known/openid-configuration

      Note: Configure your discovery URI to allow origin URLs for Cross-Origin Resource Sharing (CORS) calls, as follows:

      - Methods: GET
      - Allowed origins:

- https://admin.google.com
- https://client-side-encryption.google.com
- https://krahsc.google.com/callback
- https://krahsc.google.com/oidc/cse/callback
- https://krahsc.google.com/oidc/drive/callback
- https://krahsc.google.com/oidc/gmail/callback
- https://krahsc.google.com/oidc/meet/callback
- https://krahsc.google.com/oidc/calendar/callback
- https://krahsc.google.com/oidc/docs/callback
- https://krahsc.google.com/oidc/sheets/callback
- https://krahsc.google.com/oidc/slides/callback
- https://client-side-encryption.google.com/callback
- https://client-side-encryption.google.com/oidc/cse/callback
- https://client-side-encryption.google.com/oidc/drive/callback
- https://client-side-encryption.google.com/oidc/gmail/callback
- https://client-side-encryption.google.com/oidc/meet/callback
- https://client-side-encryption.google.com/oidc/calendar/callback
- https://client-side-encryption.google.com/oidc/docs/callback
- https://client-side-encryption.google.com/oidc/sheets/callback
- https://client-side-encryption.google.com/oidc/slides/callback

d. In the **Grant type** field, select the OAuth flow you want to use for OIDC.

   If you're using a third-party IdP: You can use either the **Implicit** or **Authorization code with PKCE** grant type.

   If you're using Google identity: You can use only the **Implicit** grant type.

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.

[5] 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., CryptoHub)
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

[5.1] VALIDATE SUCCESSFUL CONNECTION FROM GOOGLE WORKSPACE TO THE CRYPTOHUB

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 CryptoHub, a green checkmark and the "Your external key service is active" message appears.

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

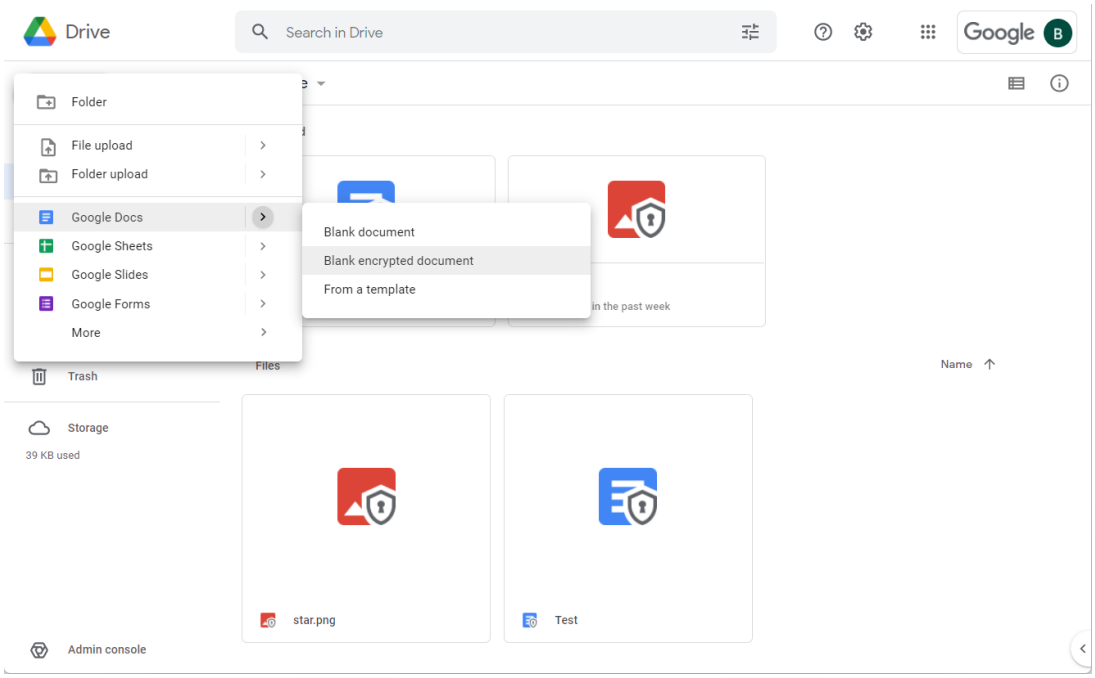
1. Sign in to your Google admin console.

   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**.

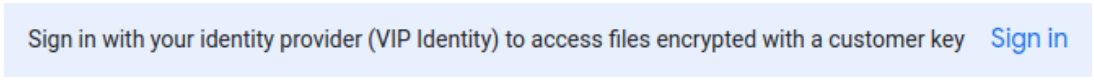
   If Google Workspace can connect to your IdP, the "Connection success" message appears.

[5.3] 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**.



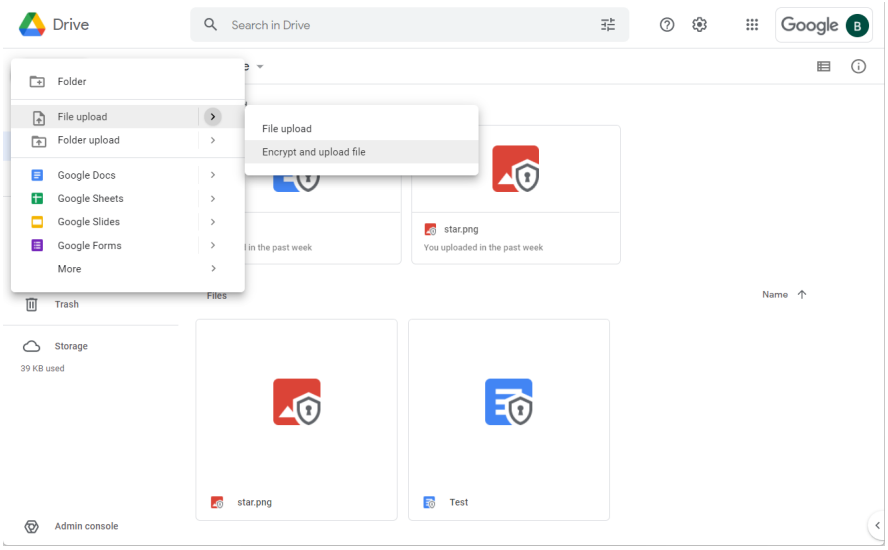
3. A message will appear warning you that intelligent features such as spelling and grammar won't work with encrypted files, collaboration features will be limited, and only certain people can access encrypted files due to admin settings. Click **Create**.
4. If this is the first encryption operation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



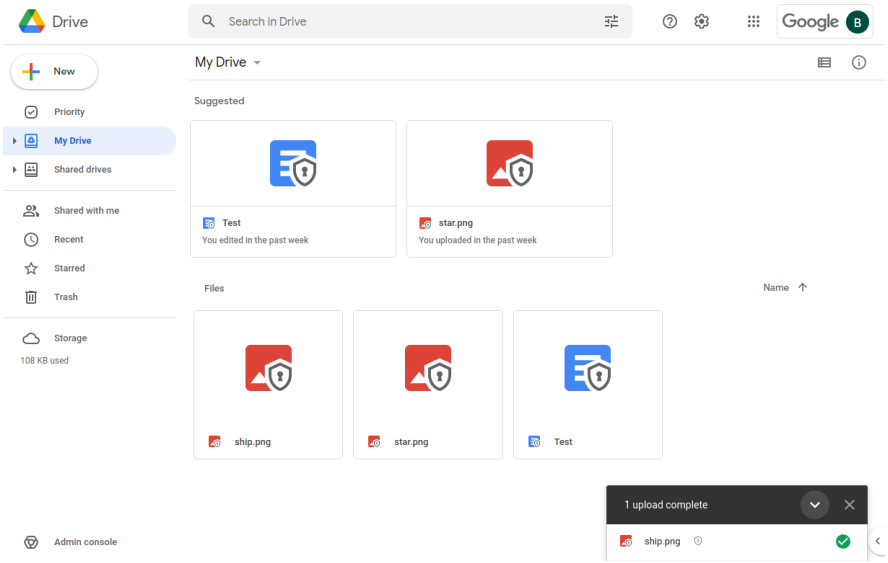
Click **Sign In**, which will redirect you to your IdP's website to sign in. After signing in and allowing your IdP access to your Google Account, you will be redirected back to the Google Doc, which should now be encrypted. A confirmation message will appear if encryption is successful. Then you can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

[5.4] 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**.



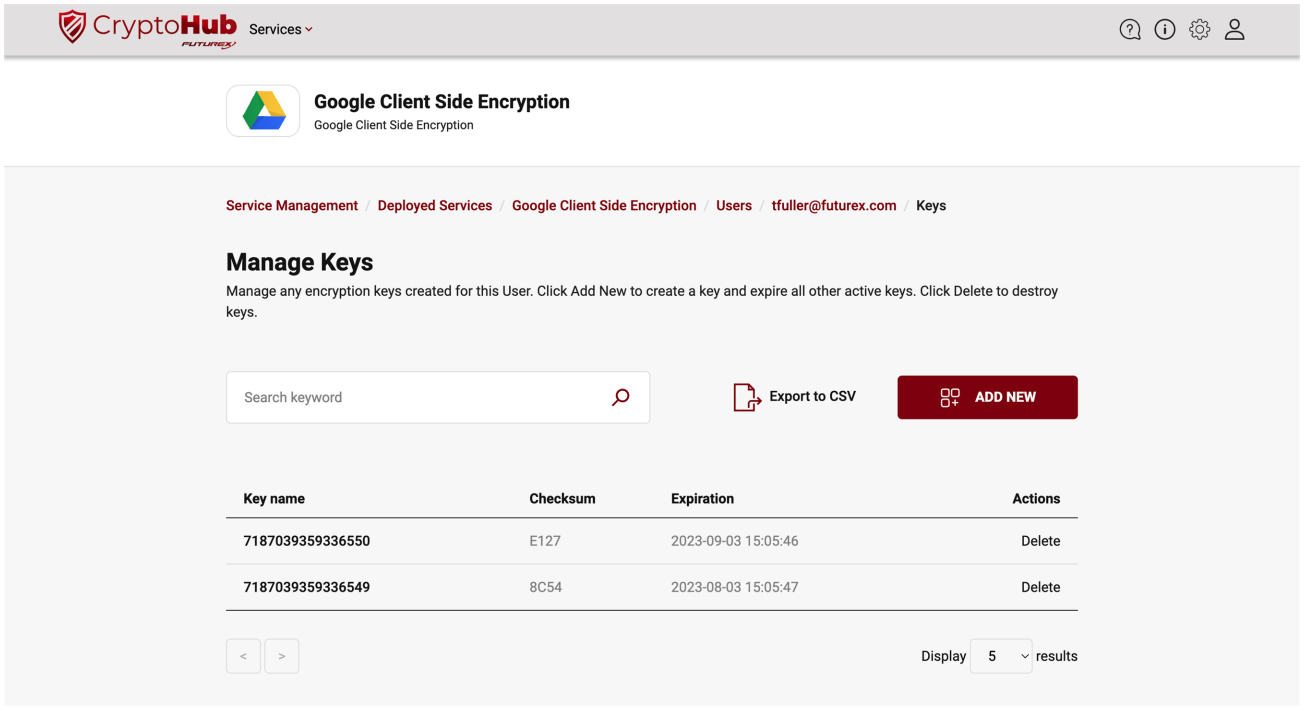
3. A message will appear warning you that some features, such as full-text search and file preview, will be unavailable and that only certain people can access encrypted files due to admin settings. Click **Select file**.
4. If this is the first encryption operation you have attempted with Google Workspace 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:



[5.5] VIEWING PERSONAL KEYS IN CRYPTOHUB

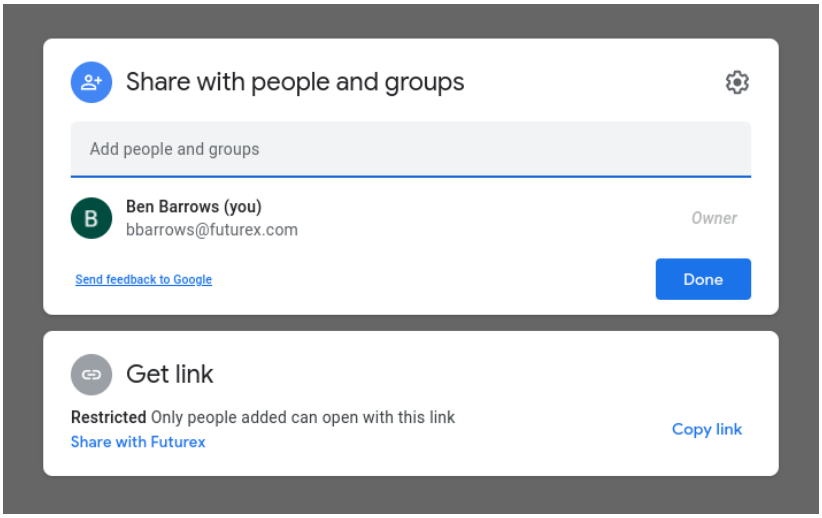
The first time that a Google CSE user creates an encrypted document or encrypts and uploads a file to Google Drive, a **Personal Key** is created in CryptoHub specifically for that user. The Personal Key is then used for all CSE operations performed by that user in Google Workspace.

CryptoHub users can view their Personal Keys by navigating to the **Users** menu for the deployed Google CSE service, selecting their user, then selecting **Keys**.



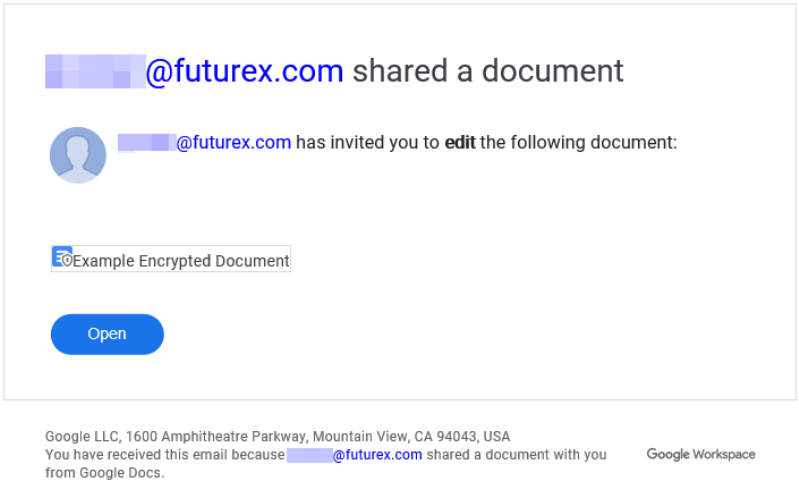
[5.6] TEST SHARING AN ENCRYPTED GOOGLE DOC

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**.

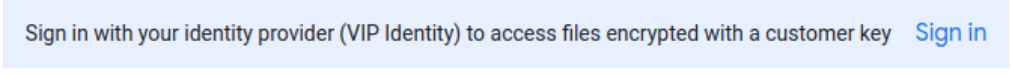


Note: Only share encrypted documents with other Google CSE users that your company administrator has set up with an account in VIP. If they do not have a user configured in VIP, they will not be able to decrypt, view, and edit the file you are sharing.

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



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**.



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