GOOGLE CLOUD EKM (EXTERNAL KEY MANAGER)

Integration Guide

Applicable Devices:

CryptoHub

Applicable Versions:

7.0.2.x and above

THIS DOCUMENT CONTAINS CONFIDENTIAL INFORMATION PROPRIETARY TO FUTUREX, LP. ANY UNAUTHORIZED USE, DISCLOSURE, OR DUPLICATION OF THIS DOCUMENT OR ANY OF ITS CONTENTS IS EXPRESSLY PROHIBITED.

TABLE OF CONTENTS

[1] OVERVIEW OF THE GOOGLE CLOUD EKM / CRYPTOHUB INTEGRATION

[1.1] 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.

[1.2] TERMINOLOGY

- **External key manager (EKM)**

  The key manager used outside of Google Cloud to manage your keys (i.e., CryptoHub).

- **Cloud External Key Manager (Cloud EKM)**

  A Google Cloud service for using your external keys that are managed within a supported EKM.

- **Cloud EKM through the internet**

  A version of Cloud EKM where Google Cloud communicates with your external key manager over the internet.

- **Cloud EKM through a VPC**

  A version of Cloud EKM where Google Cloud communicates with your external key manager over a Virtual Private Cloud (VPC). For more information, see VPC network overview.

- **EKM key management from Cloud KMS**

  When using Cloud EKM through a VPC with an external key management partner that supports the Cloud EKM control plane, you can use the **Cloud KMS** EKM management mode to simplify the process of maintaining external keys in your external key management partner and in Cloud EKM.

- **Crypto space**

  A container for your resources within your external key management partner. Your crypto space is identified by a unique crypto space path. The format of the crypto space path varies by external key management partner—for example, **v0/cryptospaces/*YOUR_UNIQUE_PATH***.

- **Partner-managed EKM**

  An arrangement where your EKM is managed for you by a trusted partner (i.e., Futurex).

- **Key Access Justifications**

  When you use Cloud EKM with Key Access Justifications, each request to your external key management partner includes a field that identifies the reason for each request. You can configure your external key management partner to allow or deny requests based on the Key Access Justifications code provided. For more information about Key Access Justifications, see Key Access Justifications overview.

[1.3] KEY BENEFITS OF THE INTEGRATION

The Google Cloud EKM / CryptoHub integration provides several benefits:

- **Key provenance:** You control the location and distribution of your externally managed keys. Externally managed keys are never cached or stored within Google Cloud. Instead, Cloud EKM communicates directly with the CryptoHub for each request.
- **Access control:** You manage access to your externally managed keys. Before you can use an externally managed key in Google Cloud, you must grant the Google Cloud project access to use the key. You can revoke this access at any time.
- **Centralized key management:** You can manage your keys and access policies from a single user interface, whether the data they protect resides in the cloud or on your premises.

In all cases, the key resides on the CryptoHub, and is never sent to Google.

[1.4] GOOGLE CLOUD EKM FEATURES

- **Base Google EKM Support**

  With Google Cloud EKM, you can use keys that you manage within a supported external key management partner (i.e., CryptoHub) to protect data within Google Cloud. You can protect data at rest in supported CMEK integration services, or by calling the Cloud Key Management Service API directly.

- **Justification**

  Justification is a feature that requires users to provide a reason or justification for any critical operation they perform on the key management system. This feature is designed to enhance accountability and enable better auditing of actions taken within the system. By mandating justifications, it becomes easier to trace back decisions, identify patterns of misuse, and ensure that only authorized and necessary operations are executed.

- **VPC Support**

  Virtual Private Cloud (VPC) support allows the CryptoHub to be integrated seamlessly into a customer's existing VPC infrastructure on Google Cloud. This feature ensures that the key management server operates within a secure, isolated environment, which reduces the potential attack surface and provides better protection for sensitive data. VPC support also simplifies network configurations and allows for more granular control over access to the key management server.

- **Checksum support (validity checks on keys via a CMAC)**

  Checksum support, using a Cipher-based Message Authentication Code (CMAC), enables the CryptoHub to perform validity checks on cryptographic keys. When keys are generated, stored, or transmitted, a CMAC is calculated and attached to the key. The CMAC acts as a checksum that allows the recipient to verify the integrity of the key. This feature enhances the security of key management operations by ensuring that keys have not been tampered with or corrupted during storage or transmission. This feature is transparent to the user.

- **Asymmetric Signing (RSA keys)**

  Asymmetric signing support for RSA keys enables the CryptoHub to generate and manage RSA key pairs, which can be used for digital signatures and public key encryption. With this feature, users can create, store, and manage RSA keys in the CryptoHub, while leveraging Google Cloud External Key Manager for operations that require the private key, such as signing or decrypting data. This expands the range of cryptographic operations that can be performed using the integrated solution and provides increased flexibility for users.

- **Key Management commands**

  The Key Management commands feature enables users to execute a wider range of key management operations directly from the Google Cloud External Key Manager interface. This includes actions such as key rotation, deletion, and metadata updates. By providing a more comprehensive set of key management commands, users can streamline their workflows and manage their cryptographic keys more efficiently within the integrated environment. These new features will significantly enhance the capabilities of the CryptoHub and Google Cloud External Key Manager integration, providing users with improved security, accountability, and flexibility in managing their cryptographic keys.

[1.5] HOW CLOUD EKM WORKS

Cloud EKM key versions consist of these parts:

- **External key material**: The external key material of a Cloud EKM key is cryptographic material created and stored in your EKM. This material does not leave your EKM and it is never shared with Google.
- **Key reference**: Each Cloud EKM key version contains either a key URI or a key path. This is a unique identifier for the external key material that Cloud EKM uses when requesting cryptographic operations using the key.
- **Internal key material**: When a symmetric Cloud EKM key is created, Cloud KMS creates additional key material in Cloud KMS, which never leaves Cloud KMS. This key material is used as an extra layer of encryption when communicating with your EKM. This internal key material does not apply to asymmetric signing keys.

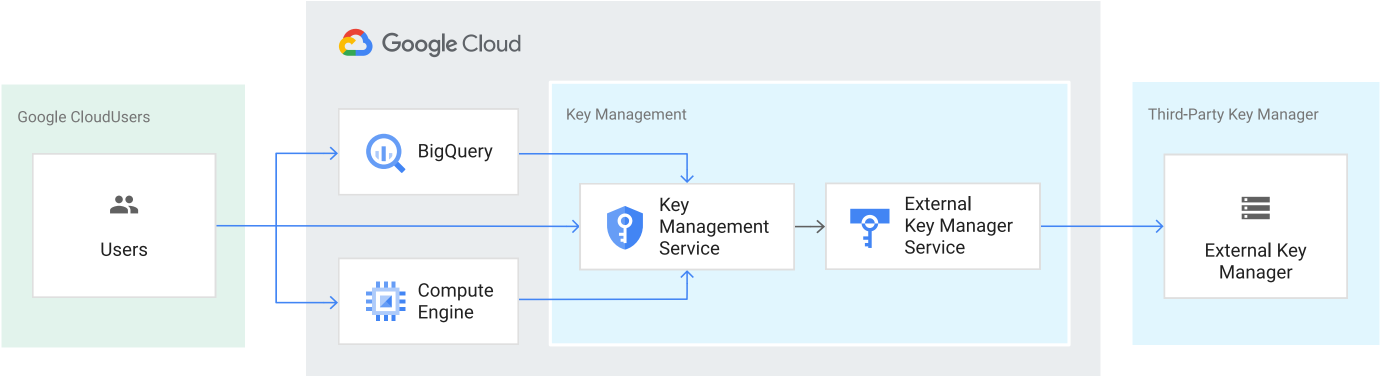
To use your Cloud EKM keys, Cloud EKM sends requests for cryptographic operations to your EKM. For example, to encrypt data with a symmetric encryption key, Cloud EKM first encrypts the data using the internal key material. The encrypted data is included in a request to the EKM. The EKM wraps the encrypted data in another layer of encryption using the external key material, and then returns the resulting ciphertext. Data encrypted using a Cloud EKM key can't be decrypted without both the external key material and the internal key material.

If your organization has enabled Key Access Justifications, your external key management partner records the provided access justification and completes the request only for justification reason codes that are allowed by your Key Access Justifications policy on the external key management partner.

Creating and managing Cloud EKM keys requires corresponding changes in both Cloud KMS and the EKM. These corresponding changes are handled differently for **manually managed external keys** and for **coordinated external keys**. All external keys accessed over the internet are manually managed. External keys accessed over a

VPC network can be manually managed or coordinated, depending on the EKM management mode of the EKM via VPC connection. The **Manual** EKM management mode is used for manually managed keys. The **Cloud KMS** EKM management mode is used for coordinated external keys.

The following diagram shows how Cloud KMS fits into the key management model. This diagram uses Compute Engine and BigQuery as two examples; you can also see the full list of services that support Cloud EKM keys.



Important: Both the Cloud EKM key version and the external key are required for each encryption and decryption request. If you lose access to either key, your data cannot be recovered. It is not possible to re-create an identical Cloud EKM key version by using the same external key URI or key path.

Please refer to Google's EKM documentation for information about the considerations and restrictions when using Cloud EKM.

You can learn about the considerations and restrictions when using Cloud EKM.

[1.6] MANUALLY MANAGED EXTERNAL KEYS

This section provides a broad overview of how Cloud EKM works with a manually managed external key.

1. You create or use an existing key in a supported external key management partner system. This key has a unique URI or key path.
2. You grant your Google Cloud project access to use the key, in the external key management partner system.
3. In your Google Cloud project, you create a Cloud EKM key version, using the URI or key path for the externally managed key.
4. Maintenance operations like key rotation must be manually managed between your EKM and Cloud EKM. For example, key version rotation or key version destruction operations need to be completed both directly in your EKM and in Cloud KMS.

Within Google Cloud, the key appears alongside your other Cloud KMS and Cloud HSM keys, with protection level **EXTERNAL** or **EXTERNAL_VPC**. The Cloud EKM key and the external key management partner key work together to protect your data. The external key material is never exposed to Google.

[1.7] COORDINATED EXTERNAL KEYS

This section provides an overview of how Cloud EKM works with a coordinated external key.

1. You set up an EKM via VPC connection, setting the **EKM management mode** to **Cloud KMS**. During setup, you must authorize your EKM to access your VPC network and authorize your Google Cloud project service account to access your crypto space in your EKM. Your EKM connection uses the hostname of your EKM and a crypto space path that identifies your resources within your EKM.
2. You create an external key in Cloud KMS. When you create a Cloud EKM key using an EKM via VPC connection with the **Cloud KMS** EKM management mode enabled, the following steps take place automatically:
    a. Cloud EKM sends a key creation request to your EKM.
    b. Your EKM creates the requested key material. This external key material remains in the EKM and is never sent to Google.
    c. Your EKM returns a key path to Cloud EKM.
    d. Cloud EKM creates your Cloud EKM key version using the key path provided by your EKM.
3. Maintenance operations on coordinated external keys can be initiated from Cloud KMS. For example, coordinated external keys used for symmetric encryption can be automatically rotated on a set schedule. The creation of new key versions is coordinated in your EKM by Cloud EKM. You can also trigger the creation or destruction of key versions in your EKM from Cloud KMS using the Google Cloud console, the gcloud CLI, the Cloud KMS API, or Cloud KMS client libraries.

Within Google Cloud, the key appears alongside your other Cloud KMS and Cloud HSM keys, with protection level **EXTERNAL_VPC**. The Cloud EKM key and the external key management partner key work together to protect your data. The external key material is never exposed to Google.

EKM key management from Cloud KMS

Coordinated external keys are made possible by EKM via VPC connections that use EKM key management from **Cloud KMS**. Futurex's **CryptoHub** product fully supports the Cloud EKM control plane, giving you the ability to use the EKM key management from Cloud KMS for your EKM via VPC connections to create coordinated external keys. With EKM key management from Cloud KMS enabled, Cloud EKM can request the following changes in your EKM:

- **Create a key**: When you create an externally managed key in Cloud KMS using a compatible EKM via VPC connection, Cloud EKM sends your key creation request to your EKM. When successful, your EKM creates the new key and key material and returns the key path for Cloud EKM to use to access the key.
- **Rotate a key**: When you rotate an externally-managed key in Cloud KMS using a compatible EKM via VPC connection, Cloud EKM sends your rotation request to your EKM. When successful, your EKM creates new key material and returns the key path for Cloud EKM to use to access the new key version.

- **Destroy a key**: When you destroy a key version for an externally-managed key in Cloud KMS using a compatible EKM via VPC connection, Cloud KMS schedules the key version for destruction in Cloud KMS. If the key version is not restored before the scheduled for destruction period ends, Cloud EKM destroys its part of the key's cryptographic material and sends a destruction request to your EKM.

Data encrypted with this key version cannot be decrypted after the key version is destroyed in Cloud KMS, even if the EKM has not yet destroyed the key version. You can see whether the EKM has successfully destroyed the key version by viewing the key's details in Cloud KMS.

When keys in your EKM are managed from Cloud KMS, the key material still resides in your EKM. Google can't make any key management requests to your EKM without explicit permission. Google can't change permissions or Key Access Justifications policies in your external key management partner system. If you revoke Google's permissions in your EKM, key management operations attempted in Cloud KMS fail.

[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.

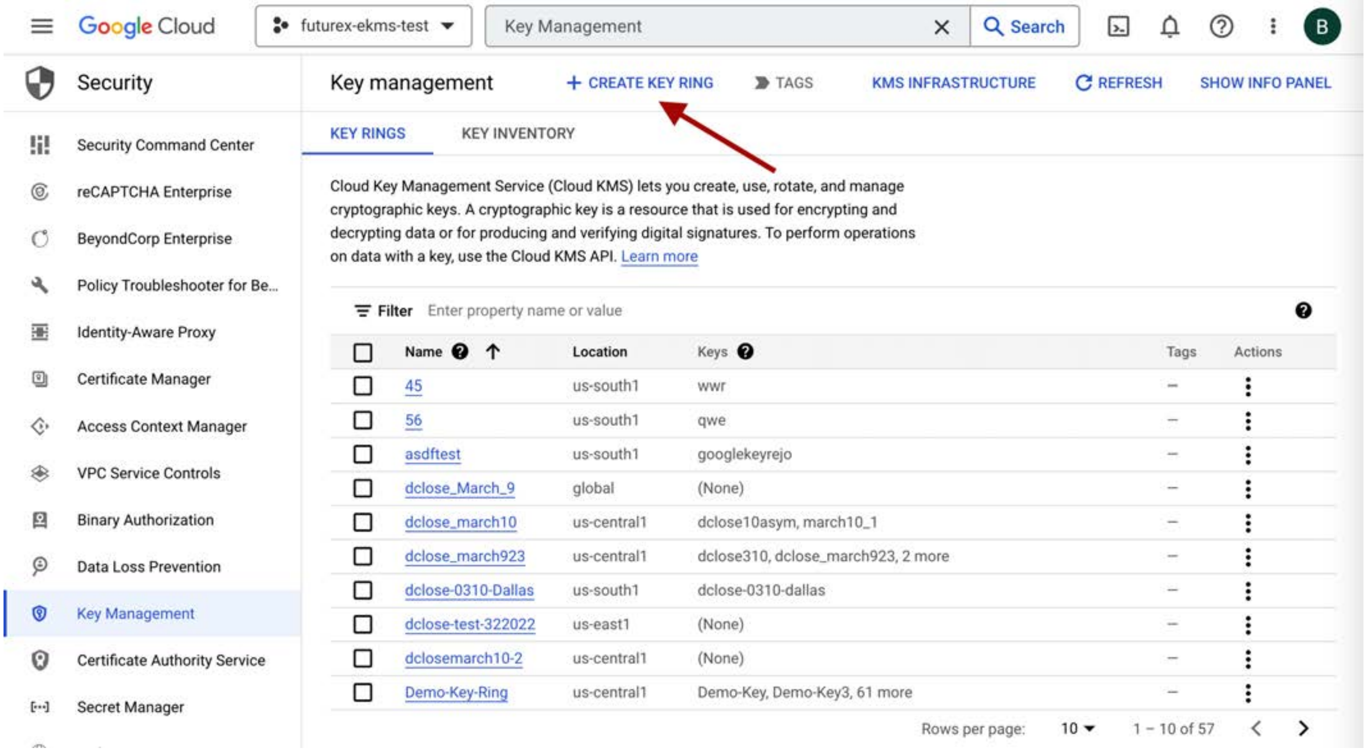
[3] INITIAL SETUP IN GOOGLE CLOUD EXTERNAL KEY MANAGER (EKM)

[3.1] NAVIGATE TO THE GOOGLE CLOUD KEY MANAGEMENT DASHBOARD

1. From the main Google Cloud dashboard, type "Key Management", into the search bar at the top of the page. Then, select **Key Management - Security** service.

[3.2] CREATE A NEW KEY RING

1. From the **Key Management** dashboard, click the **[Create Key Ring]** button at the top of the page.

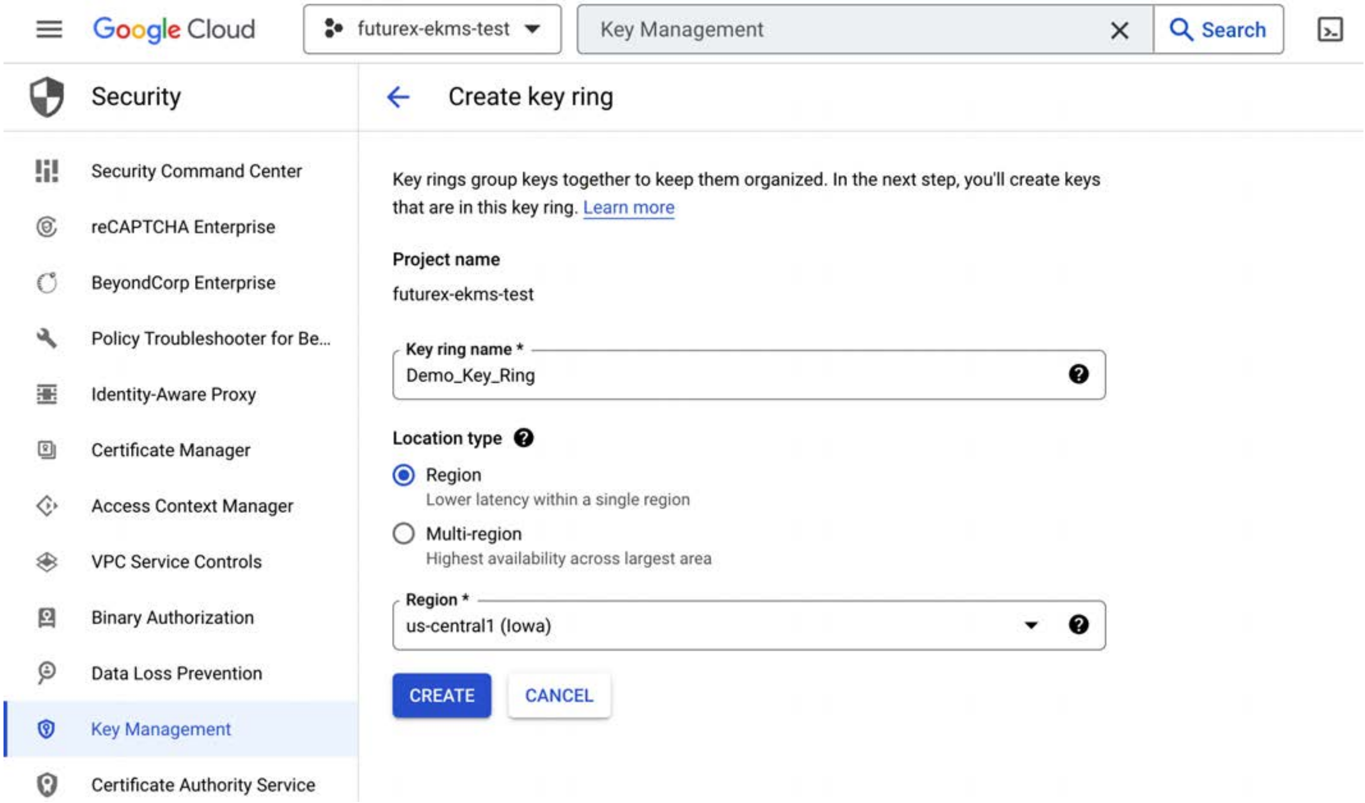


Cloud Key Management Service (Cloud KMS) lets you create, use, rotate, and manage cryptographic keys. A cryptographic key is a resource that is used for encrypting and decrypting data or for producing and verifying digital signatures. To perform operations on data with a key, use the Cloud KMS API. Learn more

□	Name ↑	Location	Keys	Tags	Actions
□	45	us-south1	wwr	–	⋮
□	56	us-south1	qwe	–	⋮
□	asdftest	us-south1	googlekeyrejo	–	⋮
□	dclose_March_9	global	(None)	–	⋮
□	dclose_march10	us-central1	dclose10asym, march10_1	–	⋮
□	dclose_march923	us-central1	dclose310, dclose_march923, 2 more	–	⋮
□	dclose-0310-Dallas	us-south1	dclose-0310-dallas	–	⋮
□	dclose-test-322022	us-east1	(None)	–	⋮
□	dclosemarch10-2	us-central1	(None)	–	⋮
□	Demo-Key-Ring	us-central1	Demo-Key, Demo-Key3, 61 more	–	⋮

Rows per page: 10 ▾ 1 – 10 of 57 ‹ ›

2. This will bring up the **Create key ring** wizard.



Create key ring

Key rings group keys together to keep them organized. In the next step, you'll create keys that are in this key ring. Learn more

Project name
futurex-ekms-test

Key ring name *
Demo_Key_Ring

Location type
● Region
Lower latency within a single region
○ Multi-region
Highest availability across largest area

Region *
us-central1 (Iowa)

3. Enter a **name** for the key ring.

   Note: Key ring names can only contain letters, numbers, underscores (_), and hyphens (-). Key rings can't be renamed or deleted.

4. Select **Region** as the **Location type** (EKM does not support Multi-region). Then, in the drop-down menu, select the Google region where you want the key ring to be created.

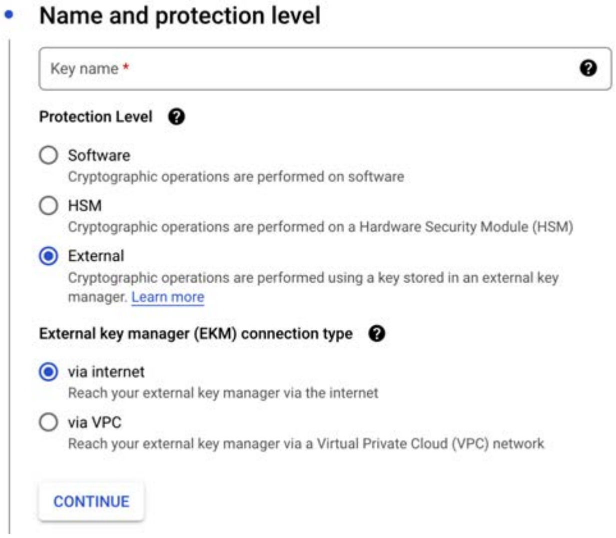
5. Click **[Create]**.

   Note the following regarding the key ring location:

   - Cloud EKM needs to be able to reach your keys quickly to avoid an error. When creating a Cloud EKM key, choose a Google Cloud location that is geographically near the location of the CryptoHub.
   - You can use Cloud EKM in any Google Cloud location supported for Cloud KMS, except for **global**.

[3.3] NOTE THE SERVICE ACCOUNT EMAIL ADDRESS

After the Key Ring is created, the browser redirects to the key creation wizard. A portion of which is shown below:



Name and protection level

Key name *

Protection Level

○ Software
Cryptographic operations are performed on software

○ HSM
Cryptographic operations are performed on a Hardware Security Module (HSM)

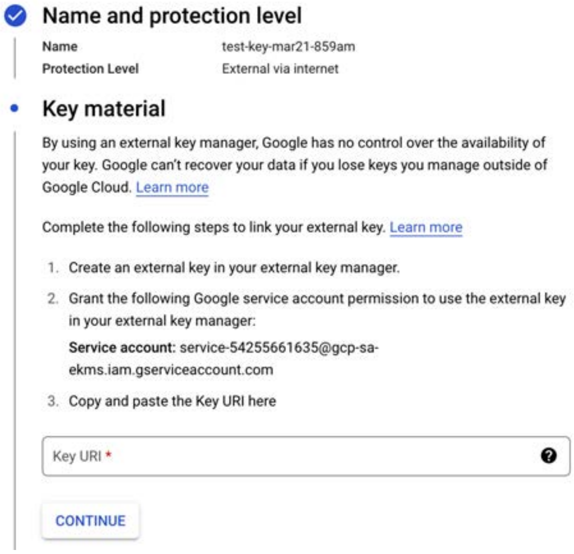
● External
Cryptographic operations are performed using a key stored in an external key manager. Learn more

External key manager (EKM) connection type

● via internet
Reach your external key manager via the internet

○ via VPC
Reach your external key manager via a Virtual Private Cloud (VPC) network

1. Enter a **name** for the key.
2. Select the **External** as the protection level for the key.
3. Select either **via internet** or **via VPC** as the External key manager (EKM) connection type.
4. Click **[Continue]**.
5. Note the **Service Account email address** in the **Key material** section. The Service account email address will be configured in CryptoHub in the next section.



Name and protection level

Name test-key-mar21-859am
Protection Level External via internet

Key material

By using an external key manager, Google has no control over the availability of your key. Google can't recover your data if you lose keys you manage outside of Google Cloud. Learn more

Complete the following steps to link your external key. Learn more

1. Create an external key in your external key manager.
2. Grant the following Google service account permission to use the external key in your external key manager:
   Service account: service-54255661635@gcp-sa-ekms.iam.gserviceaccount.com
3. Copy and paste the Key URI here

Key URI *

You will return to this dialog in the Google Cloud dashboard after creating a Google Crypto Space on the CryptoHub.

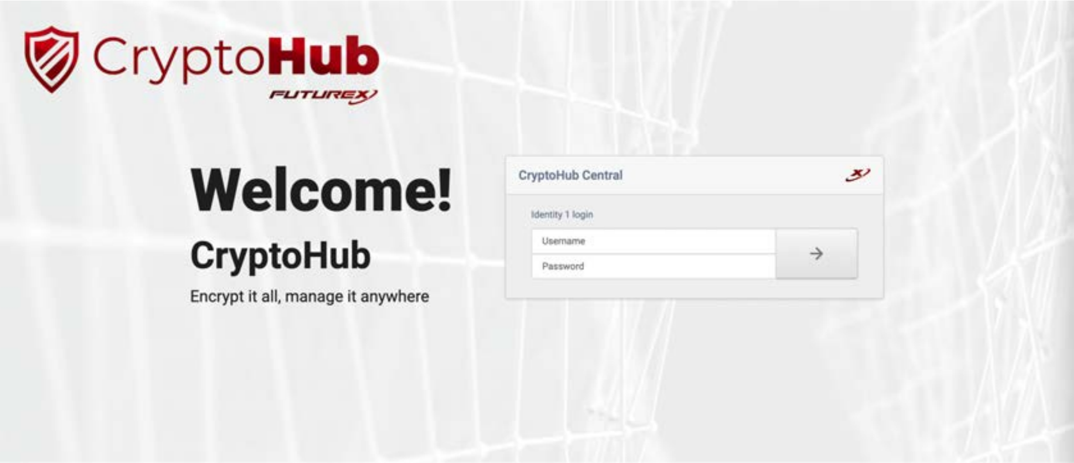
[4] DEPLOYING THE GOOGLE CLOUD EKM SERVICE IN CRYPTOHUB

Futurex offers full integration with Google Cloud External Key Manager (EKM). Create, store, and manage keys in a separate environment from your encrypted data. Our FIPS 140-2 Level 3 validated key management solution enhances data privacy and maintains control over cryptographic keys.

Keys are created inside what is referred to as a "CryptoSpace", allowing users to manage key creation, rotation, and destruction of CryptoHub-stored keys directly from the Google Cloud dashboard. Both symmetric and asymmetric keys are supported, as well as various algorithms.

[4.1] LOG IN TO THE CRYPTOHUB WEB DASHBOARD

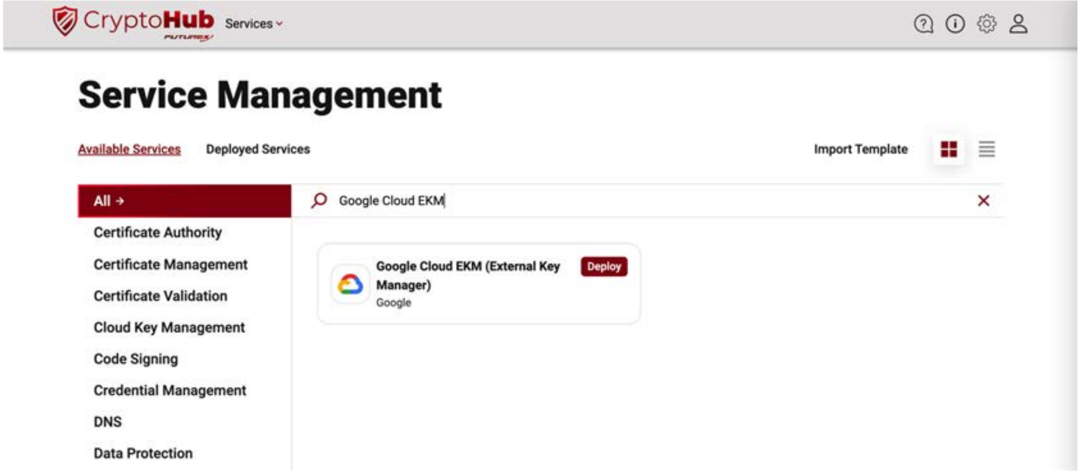
1. Open the CryptoHub web dashboard in a browser.



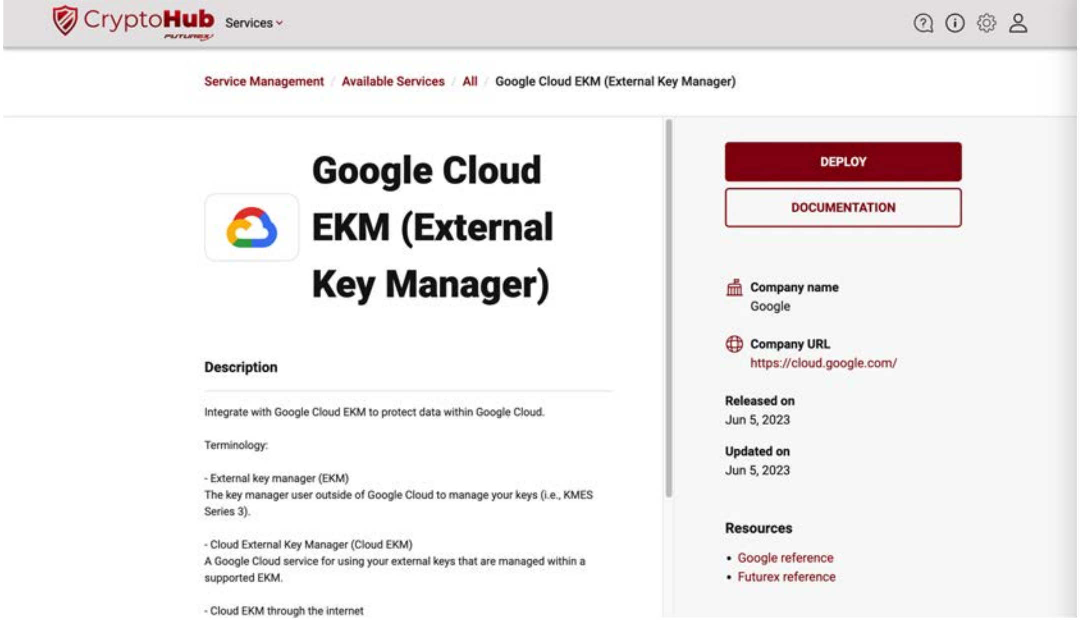
2. Log in with the default admin identities.

[4.2] DEPLOY THE GOOGLE CLOUD EKM SERVICE

1. Select the **Google Cloud EKM (External Key Manager)** service on the **Service Management** page.



2. Click **[Deploy]**.


CryptoHub
Services
Service Management / Available Services / All / Google Cloud EKM (External Key Manager)
DEPLOY
DOCUMENTATION

Google Cloud EKM (External Key Manager)

Description

Integrate with Google Cloud EKM to protect data within Google Cloud.

Terminology:

- External key manager (EKM)
The key manager user outside of Google Cloud to manage your keys (i.e., KMES Series 3).

- Cloud External Key Manager (Cloud EKM)
A Google Cloud service for using your external keys that are managed within a supported EKM.

- Cloud EKM through the internet

Company name
Google

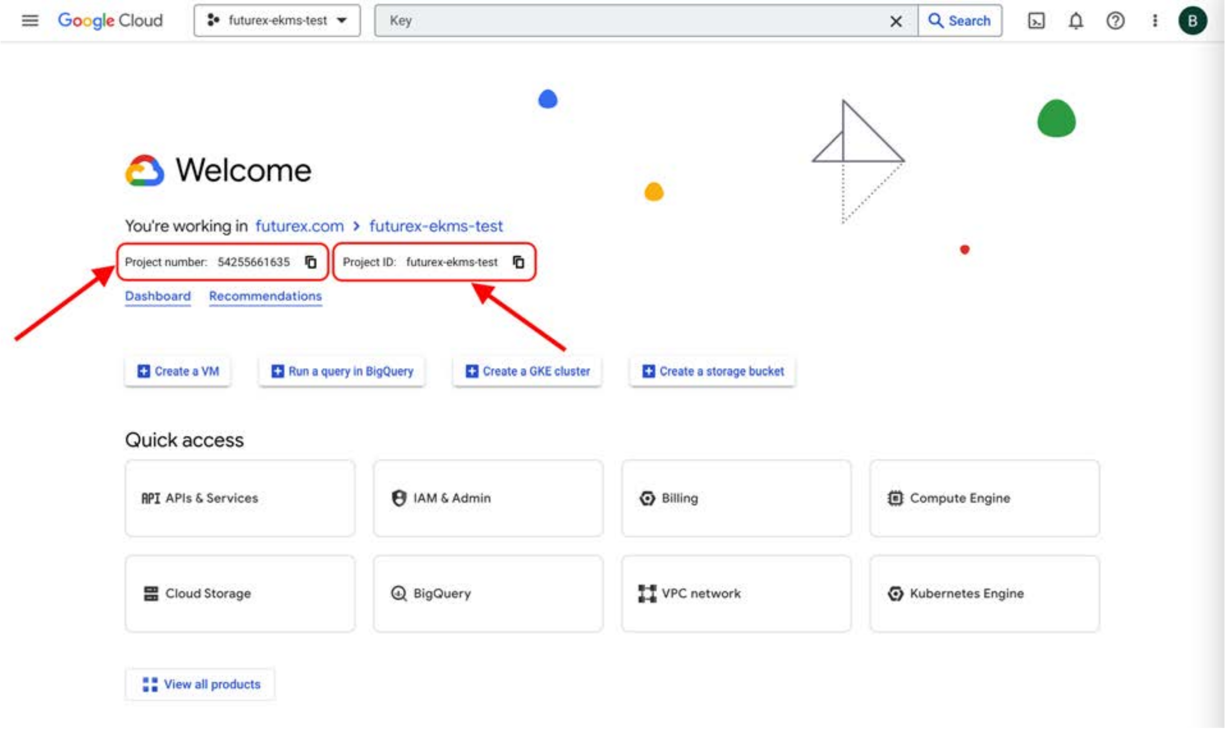
Company URL
https://cloud.google.com/

Released on
Jun 5, 2023

Updated on
Jun 5, 2023

Resources
- Google reference
- Futurex reference

3. Specify a **Service Name** and **Service Category**, then click **[Next]**.
4. (Optional) Grant any **roles** and **identities** you want to be able to access the service, then click **[Next]**.
5. Specify the **Project ID**, **Project Number**, and **Service Account** name. The Project ID and Project Number can be found on the "Welcome" page in the Google Cloud dashboard. Copy and paste the Service Account email address you noted at the end of section 2.3. Click **[Deploy]** when finished.



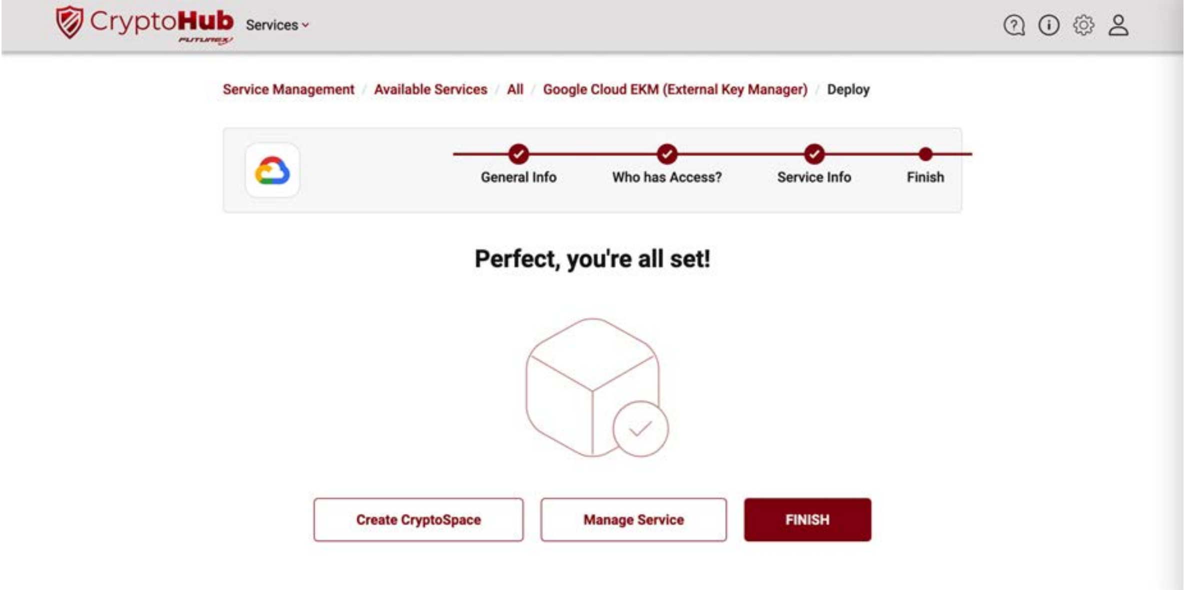
Welcome

You're working in futurex.com > futurex-ekms-test

Project number: 54255661635

Project ID: futurex-ekms-test

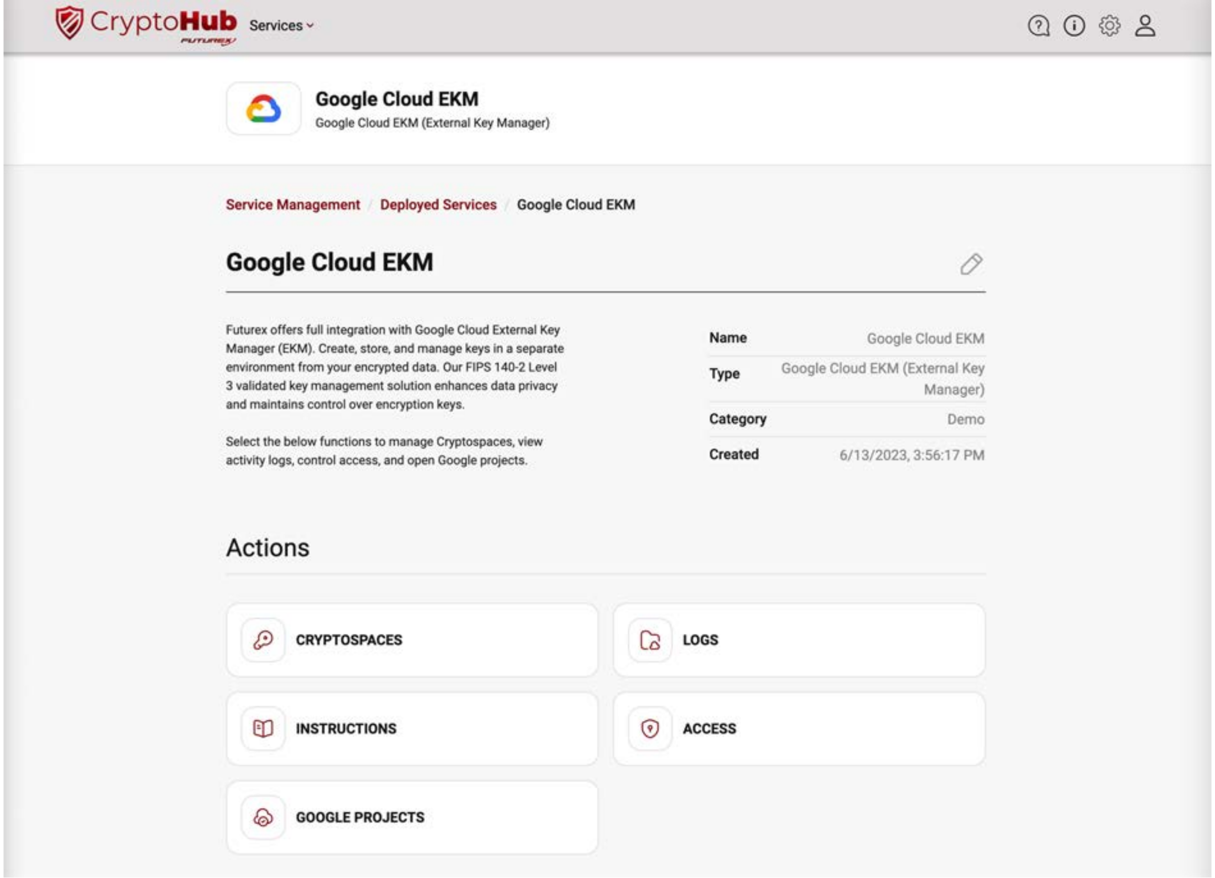
6. You will see a message confirming that the Google Cloud EKM service was successfully deployed.



Perfect, you're all set!

[4.3] CREATE A CRYPTOSPACE

If you clicked the **[Manage Service]** button on the confirmation page after deploying the Google Cloud EKM service, it will take you to this page:



CryptoHub
Services
Google Cloud EKM
Google Cloud EKM (External Key Manager)
Service Management / Deployed Services / Google Cloud EKM

Google Cloud EKM

Futurex offers full integration with Google Cloud External Key Manager (EKM). Create, store, and manage keys in a separate environment from your encrypted data. Our FIPS 140-2 Level 3 validated key management solution enhances data privacy and maintains control over encryption keys.

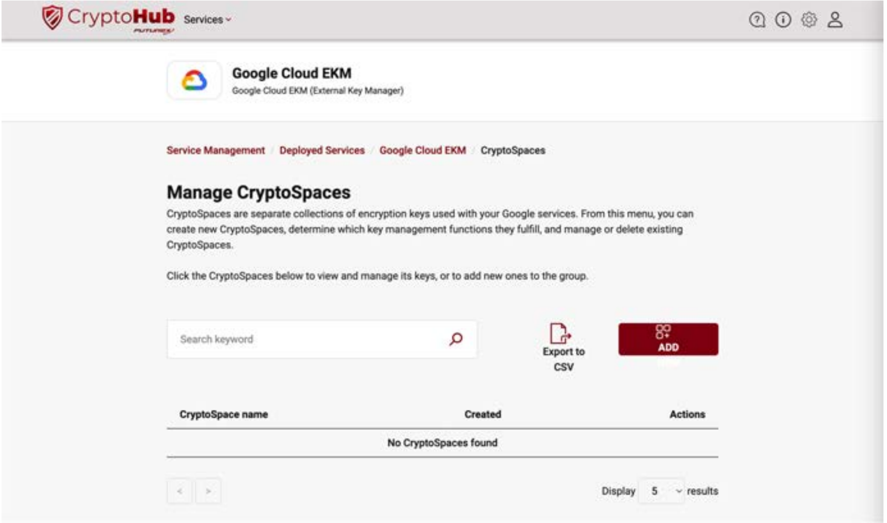
Select the below functions to manage Cryptospaces, view activity logs, control access, and open Google projects.

Name	Google Cloud EKM
Type	Google Cloud EKM (External Key Manager)
Category	Demo
Created	6/13/2023, 3:56:17 PM

Actions

Follow the steps below to create a new CryptoSpace:

1. Select the **[CryptoSpaces]** button under **Actions**.
2. Click the **[Add New]** button.


CryptoHub
Services
Google Cloud EKM
Google Cloud EKM (External Key Manager)
Service Management / Deployed Services / Google Cloud EKM / CryptoSpaces
Search keyword
Export to CSV
ADD
Display 5 results

Manage CryptoSpaces

CryptoSpaces are separate collections of encryption keys used with your Google services. From this menu, you can create new CryptoSpaces, determine which key management functions they fulfill, and manage or delete existing CryptoSpaces.

Click the CryptoSpaces below to view and manage its keys, or to add new ones to the group.

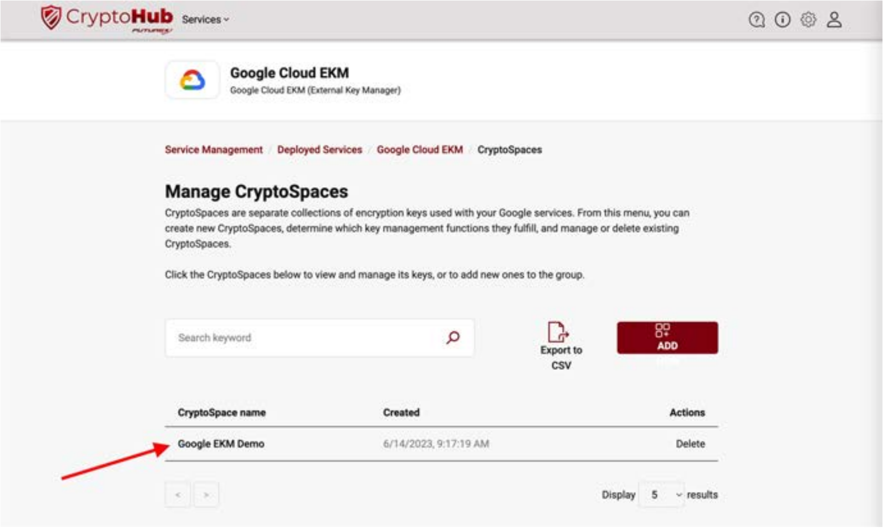
CryptoSpace name	Created	Actions
No CryptoSpaces found		

3. In the **Create CryptoSpace** wizard, specify a CryptoSpace **Name**, check the boxes for all **Justifications** that are applicable, and select the **permissions** you want your Google Cloud Project to have on the CryptoSpace. Click **[Create CryptoSpace]** when finished.

[4.4] CREATE KEYS INSIDE THE CRYPTOSPACE

Now we will create a few keys inside the CryptoSpace. Later in this guide these keys will be created as "External" keys in Google EKM. Essentially associating the key material stored in CryptoHub with the instance of the key in Google EKM.

1. The new CryptoSpace is now listed now on the **Manage CryptoSpaces** page. Click the CryptoSpace name.


CryptoHub
Services
Google Cloud EKM
Google Cloud EKM (External Key Manager)
Service Management / Deployed Services / Google Cloud EKM / CryptoSpaces
Search keyword
Export to CSV
ADD
Display 5 results

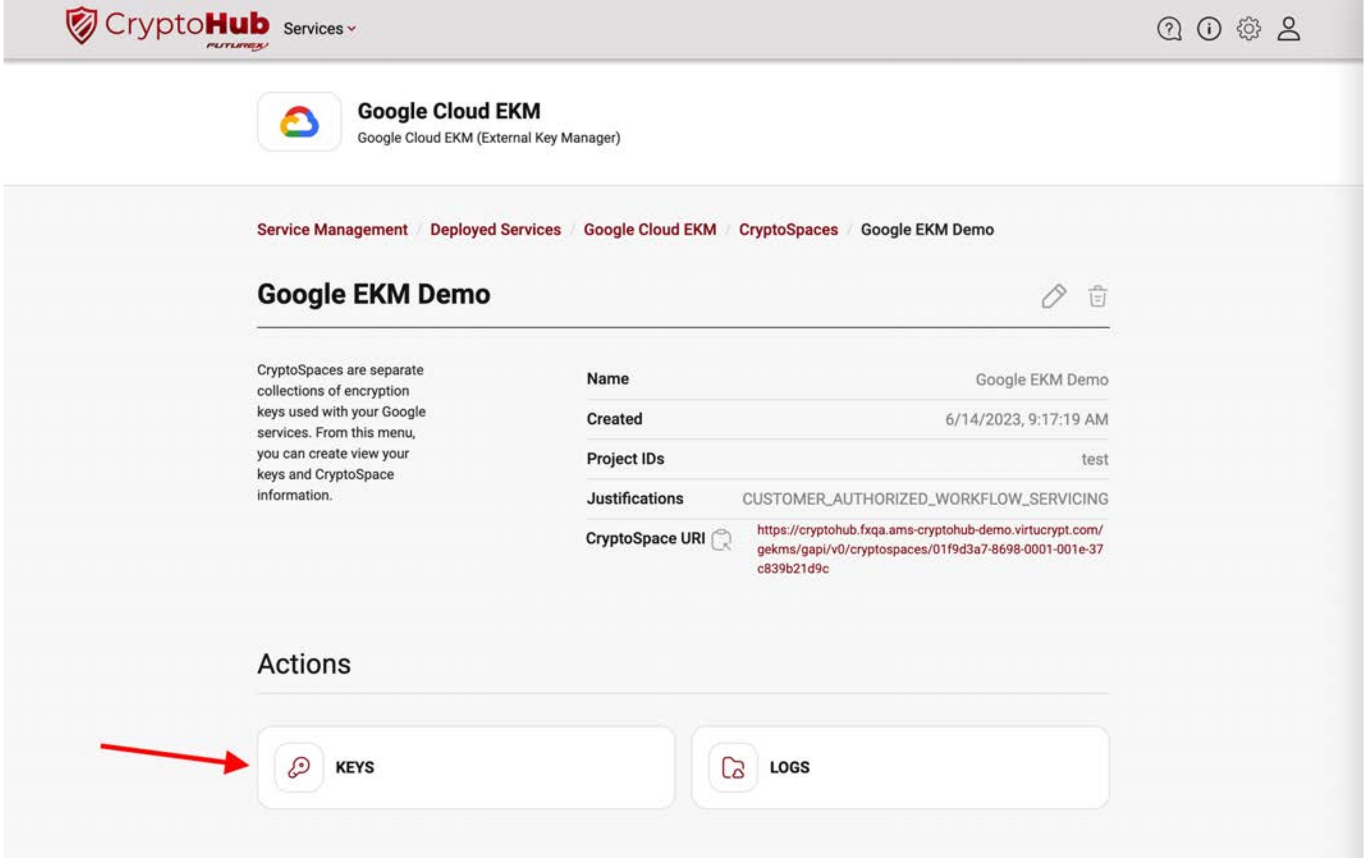
Manage CryptoSpaces

CryptoSpaces are separate collections of encryption keys used with your Google services. From this menu, you can create new CryptoSpaces, determine which key management functions they fulfill, and manage or delete existing CryptoSpaces.

Click the CryptoSpaces below to view and manage its keys, or to add new ones to the group.

CryptoSpace name	Created	Actions
Google EKM Demo	6/14/2023, 9:17:19 AM	Delete

2. Click the **[Keys]** button.

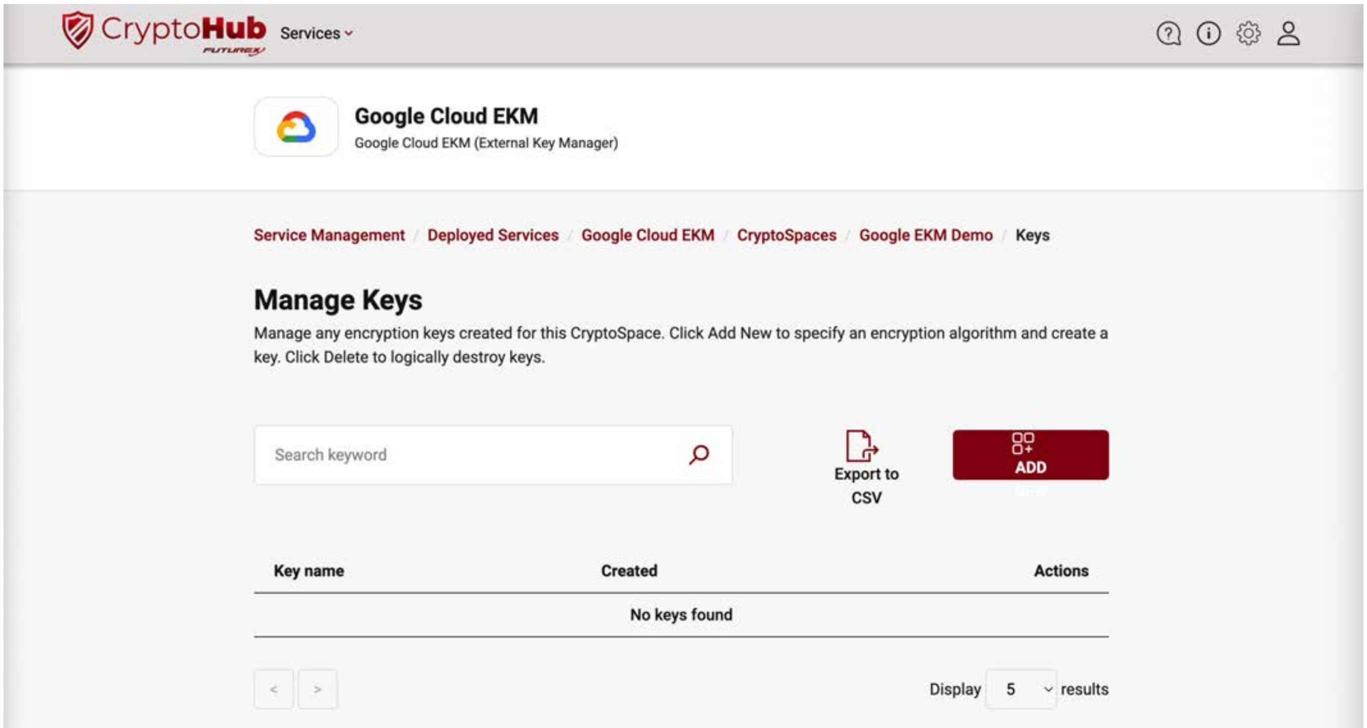

CryptoHub
Services
Google Cloud EKM
Google Cloud EKM (External Key Manager)
Service Management / Deployed Services / Google Cloud EKM / CryptoSpaces / Google EKM Demo
Actions
KEYS
LOGS

Google EKM Demo

CryptoSpaces are separate collections of encryption keys used with your Google services. From this menu, you can create view your keys and CryptoSpace information.

Name	Google EKM Demo
Created	6/14/2023, 9:17:19 AM
Project IDs	test
Justifications	CUSTOMER_AUTHORIZED_WORKFLOW_SERVICING
CryptoSpace URI	https://cryptohub.fxqa.ams-cryptohub-demo.virtucrypt.com/gekms/gapi/v0/cryptospaces/01f9d3a7-8698-0001-001e-37c839b21d9c

3. Click the **[Add New]** button.


CryptoHub
Services
Google Cloud EKM
Google Cloud EKM (External Key Manager)
Service Management / Deployed Services / Google Cloud EKM / CryptoSpaces / Google EKM Demo / Keys
Search keyword
Export to CSV
ADD
Display 5 results

Manage Keys

Manage any encryption keys created for this CryptoSpace. Click Add New to specify an encryption algorithm and create a key. Click Delete to logically destroy keys.

Key name	Created	Actions
	No keys found	

4. In the **Create Key** wizard, specify a Key **Name**, select the **Key Algorithm** you want to use, check the boxes for all **Justifications** that are applicable, and specify the **Rotation Period**. Click the **[Create Key]** button when finished.

[5] CREATING AN EXTERNAL KEY IN GOOGLE CLOUD EKM

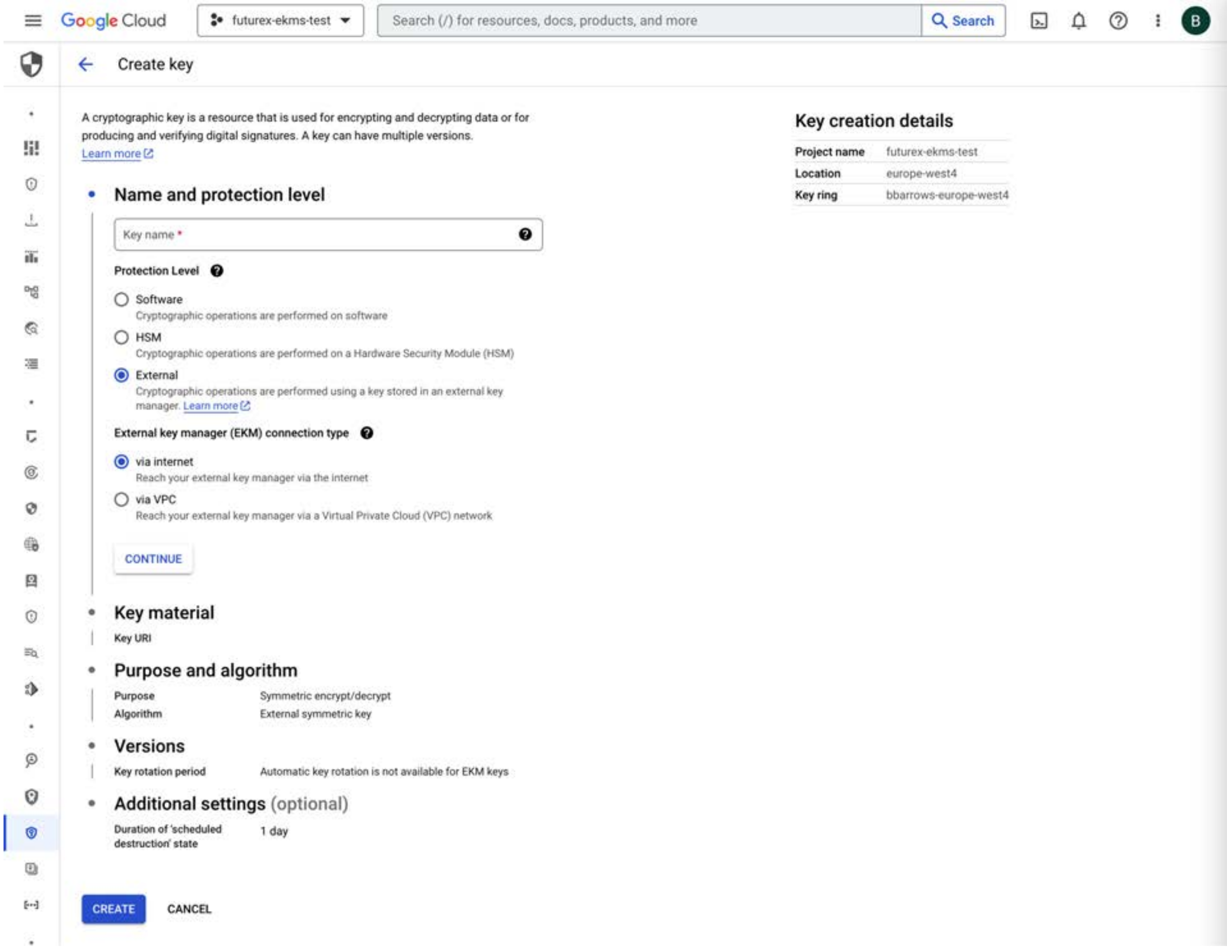
This section walks users through the process for creating an **External** key in the Google Cloud Key Management dashboard.

[5.1] NAVIGATE TO THE GOOGLE CLOUD KEY MANAGEMENT DASHBOARD

1. From the main Google Cloud dashboard, type "Key Management", into the search bar at the top of the page. Then, select **Key Management - Security** service.

[5.2] CREATE AN EXTERNAL KEY

1. Select the Key Ring you created in section 2.2.
2. Select **[Create Key]**. This will open the key creation wizard.



A cryptographic key is a resource that is used for encrypting and decrypting data or for producing and verifying digital signatures. A key can have multiple versions. Learn more

Key creation details

Project name	futurex-ekms-test
Location	europe-west4
Key ring	bbarrows-europe-west4

Name and protection level

Key name *

Protection Level

○ Software
Cryptographic operations are performed on software

○ HSM
Cryptographic operations are performed on a Hardware Security Module (HSM)

● External
Cryptographic operations are performed using a key stored in an external key manager. Learn more

External key manager (EKM) connection type

● via internet
Reach your external key manager via the internet

○ via VPC
Reach your external key manager via a Virtual Private Cloud (VPC) network

Key material

Key URI

Purpose and algorithm

Purpose	Symmetric encrypt/decrypt
Algorithm	External symmetric key

Versions

Key rotation period	Automatic key rotation is not available for EKM keys

Additional settings (optional)

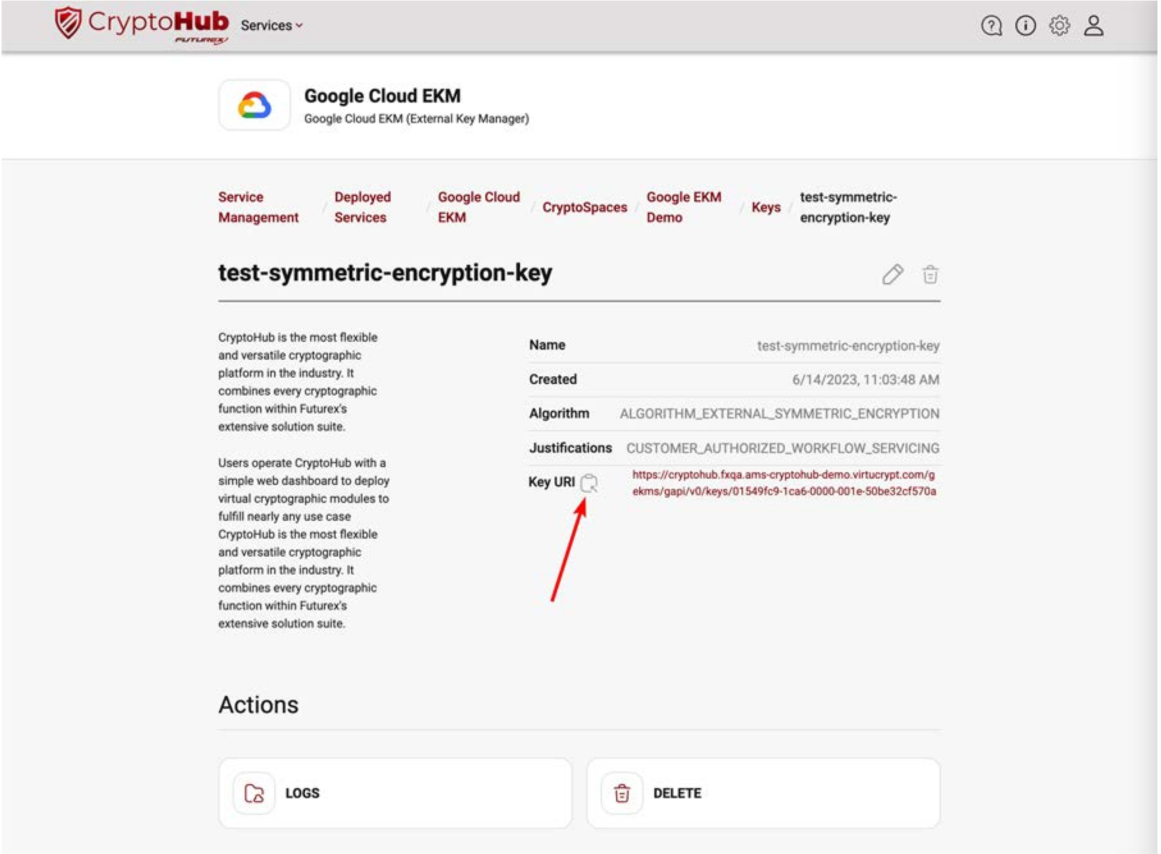
Duration of 'scheduled destruction' state	1 day

3. Enter a **name** for the key.

   Note: The key name you specify here does not need to match the name of the key that was created on the CryptoHub.

4. Select the **External** as the protection level for the key.

5. Select either **via internet** or **via VPC** as the External key manager (EKM) connection type.
6. Click **[Continue]**.
7. Enter the **Key URI**, which you can copy by clicking the Key URI button for the key in CryptoHub.



test-symmetric-encryption-key

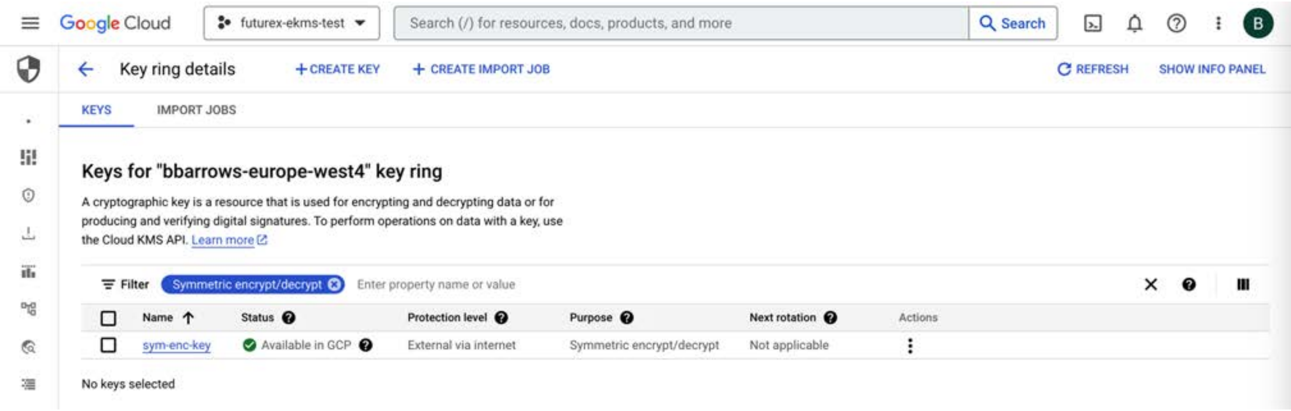
CryptoHub is the most flexible and versatile cryptographic platform in the industry. It combines every cryptographic function within Futurex's extensive solution suite.

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

Name	test-symmetric-encryption-key
Created	6/14/2023, 11:03:48 AM
Algorithm	ALGORITHM_EXTERNAL_SYMMETRIC_ENCRYPTION
Justifications	CUSTOMER_AUTHORIZED_WORKFLOW_SERVICING
Key URI	https://cryptohub.fxqa.ams-cryptohub-demo.virtucrypt.com/gekms/gapi/v0/keys/01549fc9-1ca6-0000-001e-50be32cf570a

Important: In addition to the steps above, Google must whitelist the domain specified in the Key URI field for your specific Google Cloud account.

8. Click the **[Continue]** button again. This will allow you to select either **Symmetric encrypt/decrypt** or **Asymmetric sign** in the Purpose dropdown menu.
9. Click **[Create]** to create the externally managed key. The key status should be a green checkmark, confirming that the key is successfully synced with the key material stored in CryptoHub.



Keys for "bbarrows-europe-west4" key ring

A cryptographic key is a resource that is used for encrypting and decrypting data or for producing and verifying digital signatures. To perform operations on data with a key, use the Cloud KMS API. Learn more

□	Name ↑	Status	Protection level	Purpose	Next rotation	Actions
□	sym-enc-key	✓ Available in GCP	External via internet	Symmetric encrypt/decrypt	Not applicable	⋮

No keys selected

[6] TESTING ENCRYPTION AND DECRYPTION WITH EXTERNALLY MANAGED KEY

[6.1] DOWNLOAD AND INSTALL GOOGLE CLOUD SDK

Please follow the instructions here to download, install, and configure Google Cloud SDK:

https://cloud.google.com/sdk/docs/install

[6.2] ENCRYPT A TEST FILE USING THE EXTERNALLY MANAGED KEY

NOTE: Before proceeding with next two steps, ensure the GCP user that is calling the encrypt and decrypt methods has the **cloudkms.cryptoKeyVersions.useToEncrypt** and **cloudkms.cryptoKeyVersions.useToDecrypt** permissions on the key used to encrypt or decrypt. One way to permit a user to encrypt or decrypt is to add the user to the **roles/cloudkms.cryptoKeyEncrypter, roles/cloudkms.cryptoKeyDecrypter**, or **roles/cloudkms.cryptoKeyEncrypterDecrypter** IAM roles for that key. For more information, see Permissions and Roles.

Run the following **gcloud kms** command to encrypt a test file using the externally managed key.

```
gcloud kms encrypt \
    --key [key] \
    --keyring [key-ring] \
    --location [location]  \
    --plaintext-file [file-with-data-to-encrypt] \
    --ciphertext-file [file-to-store-encrypted-data]
```

Replace *[key]* with the name of the key to use for encryption. Replace *[key-ring]* with the name of the key ring where the key is located. Replace *[location]* with the Cloud KMS location for the key ring. Replace *[file-with-data-to-encrypt]* and *[file-to-store-encrypted-data]* with the local file paths for reading the plaintext data and saving the encrypted output.

If the command is successful it will return no output.

[6.3] DECRYPT A TEST FILE USING THE EXTERNALLY MANAGED KEY

Run the following **gcloud kms** command to decrypt the file that was encrypted in the previous step, using the externally managed key.

```
gcloud kms decrypt \
    --key [key] \
    --keyring [key-ring] \
    --location [location]  \
    --ciphertext-file [file-path-with-encrypted-data] \
    --plaintext-file [file-path-to-store-plaintext]
```

Replace *[key]* with the name of the key to use for decryption. Replace *[key-ring]* with the name of the key ring where the key is located. Replace *[location]* with the Cloud KMS location for the key ring. Replace *[file-path-with-encrypted-data]* and *[file-path-to-store-plaintext]* with the local file paths for reading the encrypted data and saving the decrypted output.

If the command is successful it will return no output.

View the contents of the plaintext file that was output from this decryption command and confirm that it is identical to the original file that was encrypted. If the two files are identical then it confirms that the externally managed key is successfully performing encryption and decryption operations.

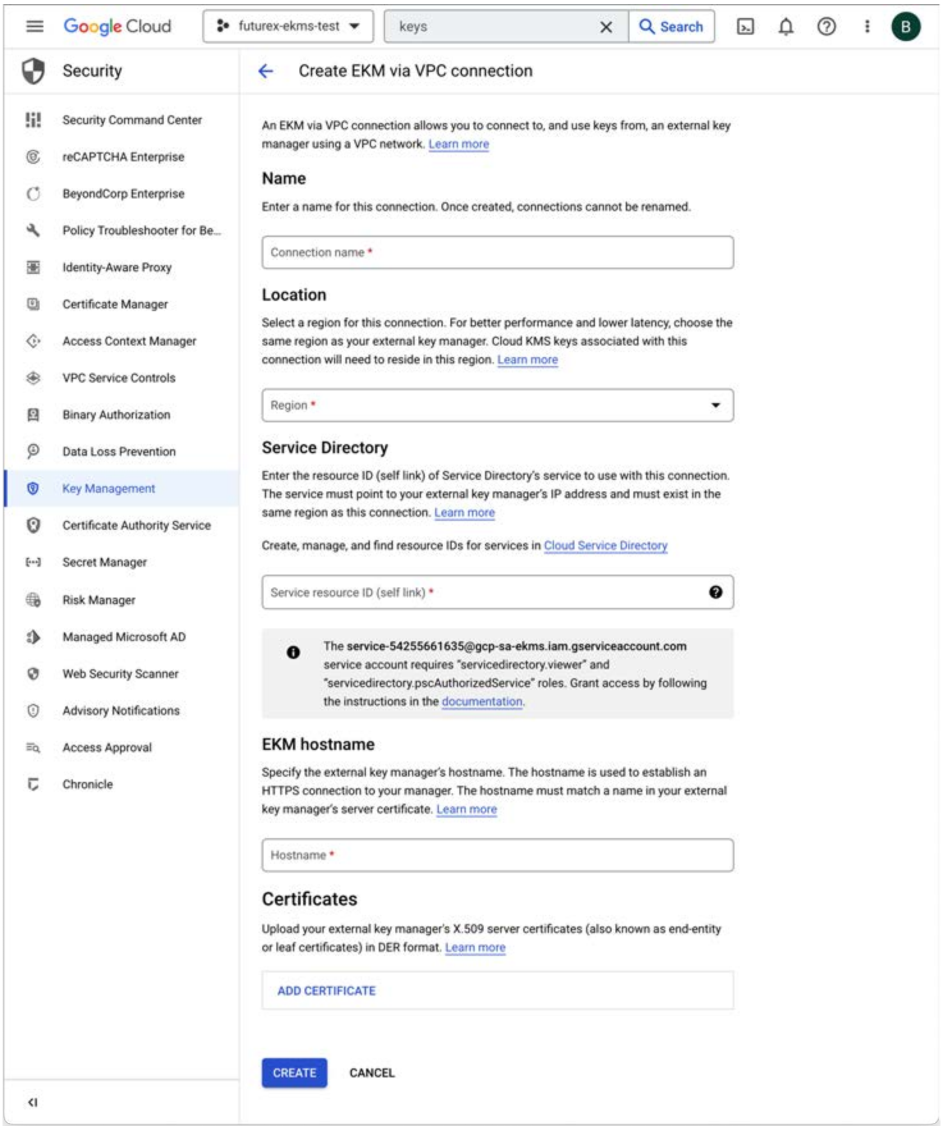
APPENDIX A: GOOGLE VPC AND KMS INFRASTRUCTURE SETUP

In this Appendix we demonstrate how to configure the Google EKM service to connect to VirtuCrypt through a Google **Virtual Private Cloud (VPC)** network. Please note that you need to have appropriate permissions for the Google Cloud project you're working on, and you should have the **Cloud Key Management Service (KMS)** and **Cloud EKM** APIs enabled for your project.

Important: Before starting this section, you need to have your VirtuCrypt instance's **hostname** and **TLS certificate**, and **Crypto Space path**. Please reach out to VirtuCrypt support for assistance.

[6.4] KMS INFRASTRUCTURE CONFIGURATION

1. In the Google Cloud console, go to the **Key management** page.
2. Click **[KMS Infrastructure]**.
3. Click **[Create Connection]**. This opens the **Create EKM via VPC connection** wizard.



An EKM via VPC connection allows you to connect to, and use keys from, an external key manager using a VPC network. Learn more

Name

Enter a name for this connection. Once created, connections cannot be renamed.

Connection name *

Location

Select a region for this connection. For better performance and lower latency, choose the same region as your external key manager. Cloud KMS keys associated with this connection will need to reside in this region. Learn more

Region *

Service Directory

Enter the resource ID (self link) of Service Directory's service to use with this connection. The service must point to your external key manager's IP address and must exist in the same region as this connection. Learn more

Create, manage, and find resource IDs for services in Cloud Service Directory

Service resource ID (self link) *

The **service-54255661635@gcp-sa-ekms.iam.gserviceaccount.com** service account requires "servicedirectory.viewer" and "servicedirectory.pscAuthorizedService" roles. Grant access by following the instructions in the documentation.

EKM hostname

Specify the external key manager's hostname. The hostname is used to establish an HTTPS connection to your manager. The hostname must match a name in your external key manager's server certificate. Learn more

Hostname *

Certificates

Upload your external key manager's X.509 server certificates (also known as end-entity or leaf certificates) in DER format. Learn more

4. In the **Create EKM via VPC connection** wizard:

a. Enter a **name** for the connection.

b. Select a **region** for the connection. It must be the same region as the VPC network.

c. Enter the **resource ID (self link)** of Service Directory's service to use with this connection, which you created in section 3. The service must point to your external key manager's IP address and must exist in the same region as this connection.

   Example : projects/futurex-ekms-test/locations/us-east1/ekmConnections/futurex-ekm-east

d. Enter the **EKM hostname**. It should match the Common Name of the TLS certificate.

e. Upload the external key manager's X.509 server certificates in DER format.

f. Select **Cloud KMS** as the **EKM management mode** and specify a Crypto Space path.

   i. Example: gekms/gapi/v0/cryptospaces/0147e96a-8698-0002-0030-e1e51ee48252

g. (Optional) Set default - will use this interface for all keys using External via VPC connection as default.

h. Click **[Create]**.

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