Migrating to a new IBM® Key Protect service instance

IBM® Key Protect service instances provisioned before 15 December 2017 are running on a legacy infrastructure that is based on Cloud Foundry. To enable fine-grained access control with Cloud IAM and other service improvements, we recommend that teams migrate their Key Protect keys into a newly provisioned instance of Key Protect.

Use this utility to migrate your existing encryption keys into a new Key Protect service instance, so that you may take advantage of the latest IBM Cloud platform functionalities, enhanced security, and expanded availability of our service.

> **Note:** This migration client requires the IBM Cloud CLI and a local environment that can run Bash shell scripts. To learn more about downloading the IBM Cloud CLI for your operating system, see Installing the stand-alone IBM Cloud CLI.

How it works

This utility looks for any Key Protect keys that are stored within the specified Cloud Foundry space and organization in your IBM Cloud account. When you run the client, the utility copies each encryption key into a new Key Protect service instance, where you can continue to manage the lifecycle of the keys and leverage new service capabilities.

Keep in mind the following updates:

- The identifying information for each key, such as the key metadata and the key ID, will be different after the key is migrated into the new Key Protect service instance. The client migrates only the key material (the `payload` value) for each encryption key. To run the migrated keys on your existing applications, you must update any references to the old key IDs so that they reflect the new key ID values.
- As keys are copied into a new Key Protect service instance, the service will store the payload value for each key in base64 encoded format. This client handles base64 encoding on your behalf as part of the migration process. If you want to store more keys in the new service instance, you must update your applications to handle the base64 encoding requirement.

After the migration completes, the client populates your new Key Protect service instance with your migrated encryption keys and creates a `migration.csv` file that shows how the old key IDs map to the migrated keys for easy identification.

Before you begin

> **Important:** Before you begin the migration process, back up your existing encryption keys to a secure location to ensure you maintain access to your data.

To work with Key Protect keys that are stored in a Cloud Foundry space:

- You must have access to the IBM Cloud account where your Key Protect service instance was initially provisioned.
- You must be assigned the appropriate Cloud Foundry access role to view and retrieve Key Protect resources within your IBM Cloud account. For example, if you are assigned a Developer access role, you can retrieve the Key Protect keys that are stored in a Cloud Foundry space. To learn more about viewing your existing Cloud Foundry access policy, see Cloud Foundry access.

To move keys into a new instance of Key Protect:

- You must have a new Key Protect service instance provisioned within your IBM Cloud account. To learn more about creating a new Key Protect service instance, see Provisioning the service.
- New instances of Key Protect use Cloud Identity and Access Management (IAM) for access control. You must be assigned the appropriate Cloud IAM access role to view and create resources within the new Key Protect service instance. If you are assigned a Manager or Writer Cloud IAM role, you can view and create keys in your new Key Protect service instance. To learn more about viewing your existing Cloud IAM access policy, see Working with users.

Setting up the migration client

Step 1. Create a new directory

1. Create a new directory on your computer called `migration-client`.
2. Extract the `migration-client-<your_OS>.zip` archive into the directory.
3. Change into the newly created directory to begin working with the migration client.

```
cd migration-client
```

Step 2. Generate authentication credentials

To generate authentication credentials for your legacy Key Protect service instance:

1. Log in to the IBM Cloud console.

2. From your user profile, select the account that contains the Cloud Foundry org and space where your legacy Key Protect service instance resides.
3. From the IBM Cloud dashboard, navigate to **Cloud Foundry Services**, and then select the Key Protect service instance that contains the encryption keys that you want to migrate.

   Note the **CF Org** and **CF Space** names that are associated with the legacy Key Protect service. You'll need to set these names as environment variables in a later step.
4. Create an API key to authenticate to the legacy Key Protect service instance.
   - From the console menu, click **Manage > Security > Platform API Keys > Create**.
   - Enter a name and description for your API key (for example, `legacy-kp-api-key`). Click **Create**, and copy the value.

To generate authentication credentials for your new Key Protect service instance:

1. In the IBM Cloud console, select the account and resource group where your new Key Protect service instance resides.
2. From the IBM Cloud dashboard, navigate to **Services**, and then select the Key Protect service instance where you want to migrate your existing encryption keys.

   Note the name that is associated with your Key Protect service instance. You'll need to set this name as an environment variable in a later step.
3. Create a second API key to authenticate to your new Key Protect service instance.
   - From the console menu, click **Manage > Security > Platform API Keys > Create**.
   - Enter a name and description for your API key (for example, `new-kp-api-key`). Click **Create**, and copy the value.

Step 3. Set your environment variables

1. Open the `envs` file that is located in the `migration-client` directory.
2. Set the following environment variables to authenticate to your Key Protect service instances.

   ```
   # Legacy service variables
   export CF_ORG="<organization_name>"
   export CF_SPACE="<space_name>"
   export LEGACY_ACCOUNT_API_KEY=<legacy_kp_api_key>
   # New service variables
   export KP_SERVICE_INSTANCE_NAME="<instance_name>"
   export KP_ACCOUNT_API_KEY=<new_kp_api_key>
   ```

   Replace `<organization_name>`, `<space_name>`, `<legacy_kp_api_key>`, `<instance_name>`, and `<new_kp_api_key>` with the values that you retrieved in the previous step.
3. Save the `envs` file and continue to the next step.

Migrating your keys

1. From the migration-client directory, run the following `make` command to build the binaries.

   ```
   make
   ```

   This command generates the `migration-client` and `kp` binaries and adds them to the bin folder in your directory.

2. Run the `client-wrapper.sh` script to start migrating keys from your legacy Key Protect service instance.

   ```
   ./scripts/client-wrapper.sh
   ```

   The client logs into IBM Cloud by using the IBM Cloud CLI plug-in, and then authenticates to each of your Key Protect service instances.

Success! Your existing keys are now migrated into a new Key Protect service instance. You can view how the old key IDs map to the migrated keys by inspecting the `migration.csv` file that is generated after the migration completes. The following table shows an example `migration.csv` file:

Old key ID	New key ID
ef9eb687-b508-45f0-8a3e-1def949bc9f8	e9ab551c-46fe-448a-8a3c-e0f23dfff362

The Key Protect keys that are stored in your Cloud Foundry org and space remain in the legacy Key Protect service instance until you're ready to permanently delete the keys, and then delete the legacy Key Protect service instance.

> **Note:** If migration fails in the middle of moving keys, check the `migration.csv` file to view the keys that were successfully migrated. To resume the migration process, be sure to save the `migration.csv` file, otherwise the client will move the keys again and create duplicate keys in the new instance. If you encounter more errors, check the `migration-client.log` file to understand how to proceed.

Updating your applications

To start using the new Key Protect service instance, update your applications so that they reference the new key IDs and point to the latest Key Protect API endpoint.

Connecting to the new service API endpoint

Key Protect service instances that exist within a Cloud Foundry org or space use the legacy `https://ibm-key-protect.edge.bluemix.net` endpoint to interact with the Key Protect API. To interact with your new

service instance, you must update any references to this endpoint to `https://keyprotect.<region>.bluemix.net`.

For example, if you created your new service instance in the US South region, use the following endpoint and API headers to browse keys in your service:

```
curl -X GET \
   https://keyprotect.us-south.bluemix.net/api/v2/keys \
   -H 'accept: application/vnd.ibm.collection+json' \
   -H 'authorization: <IAM_token>' \
   -H 'bluemix-instance: <instance_ID>'
```

For more information, see the Key Protect API reference.

Handling the base64 encoding requirement

Because new Key Protect service instances allow only base64 encoded key material (the `payload` value in the JSON body) for keys, you must base64 decode keys on retrieval to get the same payload data that you expected previously.

There are many libraries in the various languages that are available for this task. If you want to check your keys by hand (or if you use shell), you can use the base64 utility to decode the retrieved payload.

For example, if you want to decode the base64 encoded payload after you retrieve it from Key Protect, run the following shell command:

```
echo <base64_encoded_payload> | base64 -D
```

If you plan to use your new Key Protect service instance to import encryption keys in the future, ensure that you provide key material that is base64 encoded before you upload it to the service.

```
echo <payload> | base64
```

Testing your migration

To ensure that your apps continue to work with the new changes, perform a regression test on your associated applications to complete the migration process.

After your migration and testing is complete, please notify the Key Protect team by sending an email to the Key Protect offering manager at mosbaugh@us.ibm.com.

Getting help

If you encounter a problem during a migration or in the regression tests of your applications, you can reach out to the IBM Key Protect team for help. Connect with the Key Protect development team by sending an e-mail to Terry Mosbaugh at mosbaugh@us.ibm.com.

To find out more about the latest Key Protect service features, check out the Key Protect service documentation.