Rotate service account access keys

The goal of this script is to delete and create a new access key as a rotation.

Requirements

Python >= 3.8, <3.12

`pip install requests prismacloud-api`

https://pypi.org/project/prismacloud-api/

https://pypi.org/project/requests/

- This script will only rotate service account keys.
- Cannot be used to update user credentials.
- This script is tested to work with the Developer permission group as the minimal permission set.

Run the script

Credentials

- Separate credentials must be used when rotating keys
- See help command for passing credentials via CLI
- Credentials can be hardcoded but, this is often not recommended. They would be put into the settings object near line ~121
- A python file containing PRISMA_ACCESS_KEY, PRISMA_SECRET_KEY, DOMAIN can be imported and you'll see my example used on line starting with 'from creds' ~114
    - This refers to a file called creds.py containing creds.

Help Message

Rotate_keys.py -h

```
usage: rotate_key.py [-h] (--access_key ACCESS_KEY | --access_key_file ACCESS_KEY_FILE)
        [--service_account SERVICE_ACCOUNT] [--expiration_in_days EXPIRATION_IN_DAYS]
        [--key_name KEY_NAME] [--DOMAIN DOMAIN] [--PRISMA_ACCESS_KEY PRISMA_ACCESS_KEY]
        [--PRISMA_SECRET_KEY PRISMA_SECRET_KEY] [--force FORCE]
        [--new_output_filename NEW_OUTPUT_FILENAME]
```

```
Rotate Prisma access keys.


options:
  -h, --help          show this help message and exit
  --access_key ACCESS_KEY
              Prisma access key in UUID format
  --access_key_file ACCESS_KEY_FILE
              Path to the access key file generated by Prisma. Access Key ID,******** Secret Key,********
  --service_account SERVICE_ACCOUNT
              The service account name who's key is being rotated. If blank the access key owner will be
              used if it is a service account. Access key is required.
  --expiration_in_days EXPIRATION_IN_DAYS
  --key_name KEY_NAME   Override existing access key name.
  --force FORCE       Delete and Create key without prompting.
  --new_output_filename NEW_OUTPUT_FILENAME
              The new access/secret keys will be put into this new file.


  --DOMAIN DOMAIN     https://api.ca.prisma.io for Canada. Will otherwise be required in local creds.py file with
              DOMAIN variable
  --PRISMA_ACCESS_KEY PRISMA_ACCESS_KEY
              Will otherwise be required in local creds.py file with PRISMA_ACCESS_KEY variable by command
              `import creds`
  --PRISMA_SECRET_KEY PRISMA_SECRET_KEY
              Will otherwise be required in local creds.py file with PRISMA_SECRET_KEY variable by command
              `import creds`
```

Rotate by access key

```
Rotate_key.py –access_key <my access key>
```

Rotate by access key file

This is the same as by access key, but it reads the contents of a csv file containing the access key in the format:

Access Key ID, *********************

Secret Key,*********************

This is the format of the new key output. Relative paths are supported.

Rotate not found key

This can happen if the key has already been deleted or if the credentials used to run the script do not have access to that key. In this case the script will try to create a new key with the service_account given. If no service account and the key cannot be found the script will exit with an error.

Rotate with no key

The –service_account is required if no key is given. In this case it will attempt to create a new access key for this service account. Since there is a limit of 2 keys per service account it will quit and tell the user.

Key Points

- User will be prompted before creation or deletion of keys
- Credentials to execute the script must differ from access/secret keys being rotated
- --service_account has been tested without quotes and with escaped spaces
- Username of a user is the mapping to the key's createdBy value
- "My Key" is the default key name if none is given or found
- Relative file paths are used and given in relation to CWD when running the script

Links

Primary API Doc link

https://pan.dev/prisma-cloud/api/cspm/get-my-access-keys/

https://pan.dev/prisma-cloud/api/cspm/add-access-keys/

https://pan.dev/prisma-cloud/api/cspm/delete-access-keys/

https://pan.dev/prisma-cloud/api/cspm/get-user-profiles-v-3/