Define Control Groups and Describe their Basic Workflow

Control Groups

- Control groups add an additional authorization requirement on configured paths

- When a control group is created, the following will occur:
  1. The client makes a request to a path as normal
  2. Vault returns a wrapping token – rather than the requested secrets
  3. The authorizers defined in the control group policy must approve the request
  4. Once all authorizations are satified, the client can unwrap the secrets

Control Group Factors

- Control Group requirements can be specified in either **ACL policies** or within a **Sentinel policy**

- Currently, the only supported Control Group **factor** is an Identity Group
  - An authorizer must belong to a specific identity group
  - The policy will define the group, or groups, who are approvers for the requested path

Control Group Workflow

Here's my accessor. Please approve.

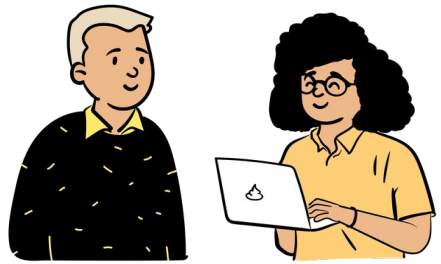
`cqL9n3r4kMeIQZekoLrMWMWN`

1. `GET kv/data/customers/orders`

2. Response

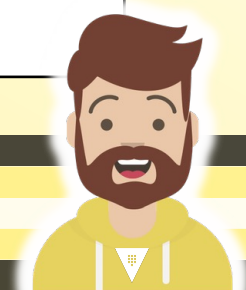
Policy with Group Control on `kv/data/customers/orders`

```
"wrap_info": {
    "token": "hvs.CAESIPvNkRgluUVNT_ccLsm6aZ-",
    "accessor": "cqL9n3r4kMeIQZekoLrMWMWN",
    "ttl": 300,
    ...
```



Account Managers

3. Share Accessor with Managers for Approval



Control Group Workflow

Note: If the authorization can not be satisfied, the token is revoked

5. `vault unwrap hvs.CAESIPvNkRg..`

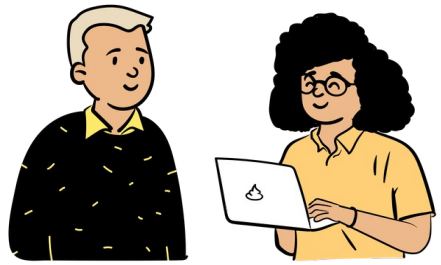
6. Response

```
"data": {
    "order": "5830375749202",
    "customer": "HCVOP9943250D2",
    "data": "25-12-2002",
    "creditcard": "1234-5678-0987-6553",
    ...
```

Policy with Group Control on `kv/data/customers/orders`

4. Authorize

4. Authorize



Account Managers

Control Groups in Vault Policies


```
path "kv/data/customers/orders" {
   capabilities = ["read"]
   control_group = {
         factor "acct_manager" {
            identity {
               group_names = ["account-managers"]
               approvals = 2
            }
         }
      }
  }
```

Regular ACL Policy

Control Group

We need two account managers to approve this request

Control Groups in Sentinel Policies (EGP)

Deploy this EGP against kv/data/customers/orders

```
import "controlgroup"

control_group = func() {
    numAuthzs = 0
    for controlgroup.authorizations as authz {
        if "account-managers" in authz.groups.by_name {
          numAuthzs = numAuthzs + 1
        }
    }
    if numAuthzs >= 2 {
       return true
    }
    return false
}

main = rule {
     control_group()
}
```

We need two account managers to approve this request

Control Groups in Action (CLI)

TERMINAL

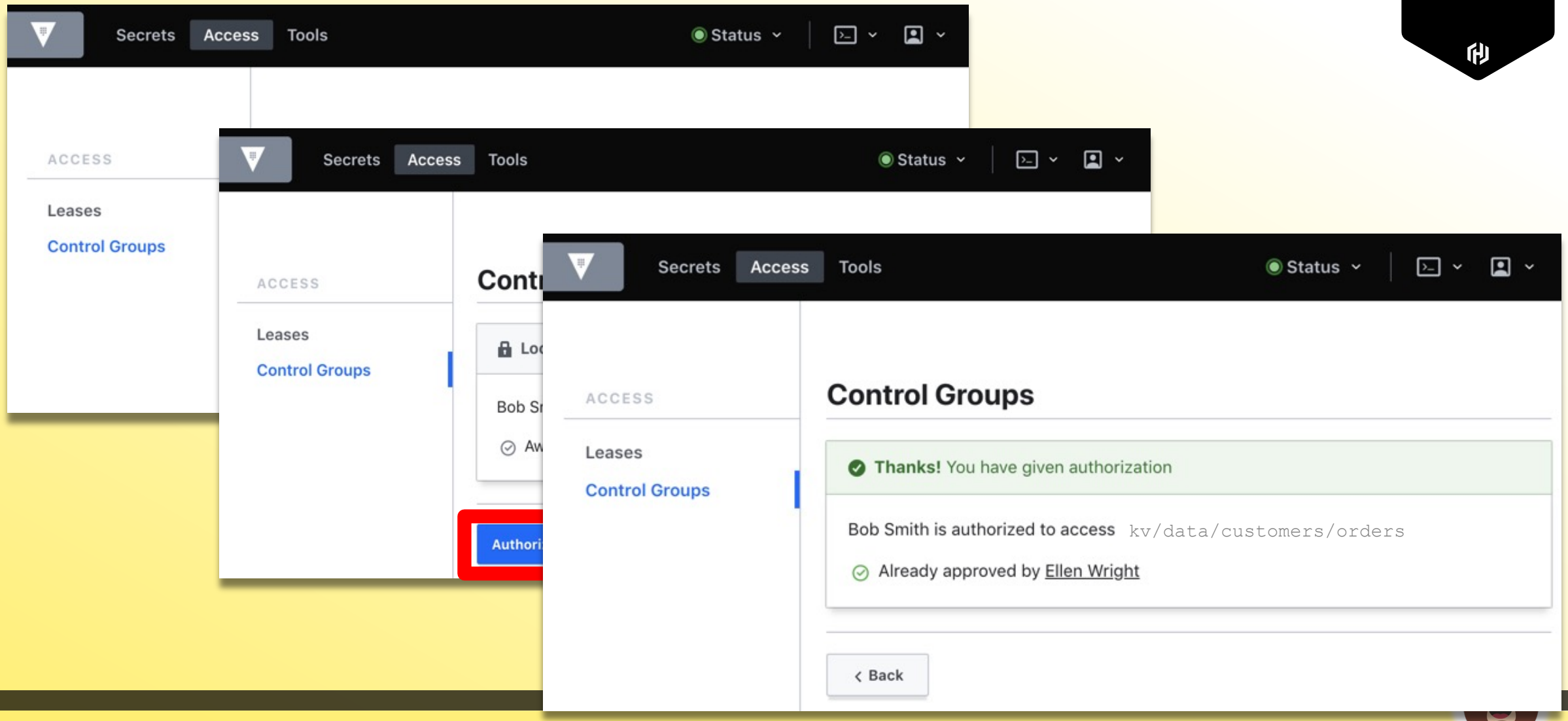
```
$ vault login hvs.CAESIA7Y-LwSxnE926onQwdxIUF7w7KJ5-
Success! You are now authenticated. The token information displayed below
is already stored in the token helper. You do NOT need to run "vault login"
again. Future Vault requests will automatically use this token.

Key                  Value
---                  -----
token                hvs.CAESIA7Y-LwSxnE926onQwdxIUF7w7KJ5-
token_accessor       72N0rIUJDuMy4LWiTbUhh8n6
token_duration       767h59m51s
token_renewable      true
token_policies       ["ctl-grp-cust-data" "default"]
identity_policies    []
policies             ["ctl-grp-cust-data" "default"]

bk~$ vault kv get kv/customers/orders
Key                                  Value
---                                  -----
wrapping_token:                      hvs.H5IATHFed2Aqk5RSvW1eEF4d
wrapping_accessor:                   vGlHUUfodJLCUho87VZjsCb4
wrapping_token_ttl:                  24h
wrapping_token_creation_time:        2022-12-25 10:00:31 -0400 EDT
wrapping_token_creation_path:        kv/data/customers/orders
```

I authenticated with a token tied to a policy with a Control Group

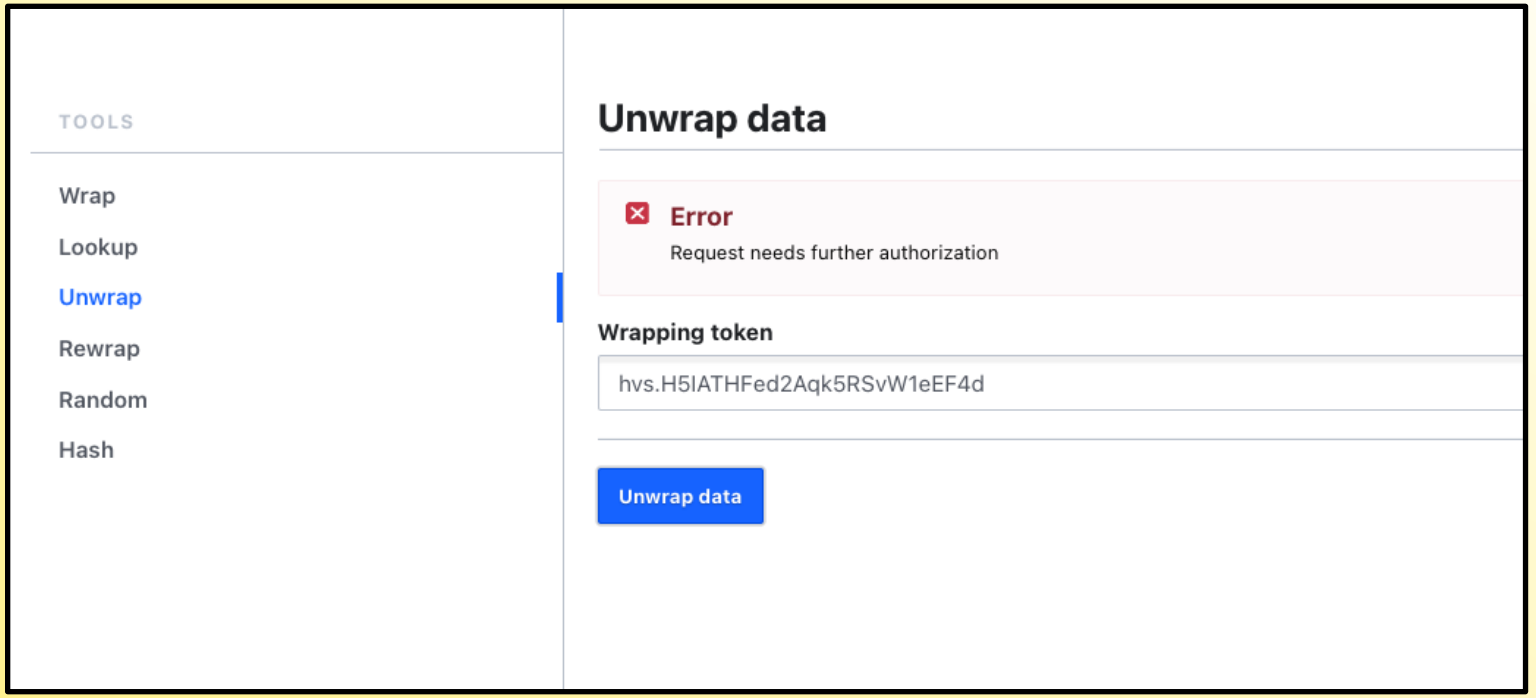
Requested data from KV store

Got wrapping token and accessor instead of data

Authorizer Actions (Account Manager)



Not yet Authorized



Unwrap the Secrets After Approvals