🔐 Sampurna Vault – Admin Maintenance Guide

System Administration & Daily Operations

1. Daily Server Routine

A. Start of Day (Server Up & Unsealing)

When the VM is started or restarted, Vault automatically locks itself ("Sealed") for security. You must manually unseal it before anyone can log in.

1. **SSH into the VM:**

   `ssh Azureuser@AZ-CI-SM-VM-UAT-01`

- **Turn the Server On and Verify Services are Running:** Check if the Keycloak and Vault Docker containers are active.

   ```
   cd ~/scms-dev
   docker compose up -d
   docker ps
   ```

(You should see keycloak and vault in the list).

- *If not running:* Start them: docker-compose up -d
- **Unseal Vault:** Vault is sealed if the status checks fail or users can't login.

```
# 1. Set the Vault Address variable
export VAULT_ADDR='https://127.0.0.1:8200'

# 2. Skip SSL verification (since we use self-signed certs locally)
export VAULT_SKIP_VERIFY=true

# 3. Check Status (Look for 'Sealed: true')
vault status

# 4. Run the Unseal Command 3 times (using your 3 separate keys)
vault operator unseal <Enter-Key-1>
vault operator unseal <Enter-Key-2>
vault operator unseal <Enter-Key-3>
```

Once Sealed: false, the system is live.

B. End of Day (Safe Shutdown)

If you need to shut down the server to save costs or for maintenance:

1. **Stop Containers Safely:**
   ```
   cd ~/scms-dev
   docker-compose down
   ```

- **Stop the VM:** You can now shut down the VM from the Azure Portal or using the command:

   ```
   sudo shutdown now
   ```

2. User Support (Helpdesk)

Note: These actions are done in the **Keycloak Admin Console**, not the terminal.

- **URL:** http://4.187.152.147:8080
- **Give Admin's User_Name and Password**
- **Realm:** Sampurna

A. User Forgot Password

1. Go to **Users** in the left menu.
2. Search for the **Employee ID** (e.g., 100015) and click on it.
3. Go to the **Credentials** tab.
4. Click **Reset Password**.
   a. **Password:** 1234
   b. **Confirm:** 1234
   c. **Temporary:** Toggle **ON**.
5. Click **Save**. *(Tell the user to log in with 1234. They will be asked to create a new password immediately.)*

B. User Lost Phone (Reset 2FA/OTP)

1. Go to **Users** -> Search ID -> Click ID.
2. Go to the **Credentials** tab.
3. Find the row labeled **OTP** and click the **Trash Icon (Delete)**.
4. Go to the **Required Actions** section (sometimes under "Details" or a separate tab depending on version).
5. Select **Configure OTP** from the "Add required action" dropdown.
6. **Save**. *(On the next login, the user will see a new QR code to scan.)*

3. Bulk Operations (Terminal)

All bulk operations are performed using Python scripts located in `~/scms-dev`.

⚠️ Prerequisite: Uploading the CSV File

Before running any bulk script, you must upload the latest employee list (Eg. EMP_MASTER_ACTIVE(Sheet1).csv) from your local computer to the VM also make sure in that csv there should be Employee Code, Employee First Name and Employee Last Name (here the if the csv file name is different and the column name is different then you have to change those things in python script as well.)

On your LOCAL Computer (PowerShell/CMD):

PowerShell
```
scp "C:\Path\To\Your\EMP_MASTER_ACTIVE(Sheet1).csv" Azureuser@4.187.152.147:~/scms-dev/
```

A. Bulk Create Users (Keycloak)

This creates users, sets temp passwords, and assigns groups.

1. **SSH into VM:** ssh Azureuser@AZ-CI-SM-VM-UAT-01
2. **Go to Folder & Activate Env:**
   ```
   cd ~/scms-dev
   source venv/bin/activate
   ```

- **Run the Import Script:**

  ```
  python3 import_final_v3.py
  ```

  Output: You will see [OK] Created: 100015 for new users and [EXISTS] for existing ones.

B. Bulk Delete Users (Keycloak)

Warning: This permanently deletes users from the login system.

- **Run the Delete Script:**

`python3 delete_bulk_users.py`

(The script reads the CSV and deletes those specific users from Keycloak.)

C. Bulk Create Secret Folders (Vault)

Keycloak users exist, but they need their personal mysecret folder in Vault.

1. **Update Admin Token (Important):** You must edit the script to put your current **Vault Root Token**.
   `nano initialize_vault_folders.py`
   `# Update the line: VAULT_TOKEN = "hvs.YourToken..."`
   `# Save: Ctrl+O, Enter, Ctrl+X`

   Run the Script:

   `python3 initialize_vault_folders.py`

D. Bulk Delete Secret Folders (Vault)

This removes user data from Vault.

1. **Update Admin Token:**
   `nano delete_vault_folders.py`
   `# Update: VAULT_TOKEN = "hvs.YourToken..."`

- **Run the Script:**
  `python3 delete_vault_folders.py`

- **Interactive Safety Check:**
  a. The script will ask: Enter IDs to SKIP (comma separated):
  b. Type IDs you want to **SAVE** (e.g., 100015, 100026).
  c. Press Enter to delete everyone else.

All Total Scripts (as of now)

Task	Script Name
Create Users	import_final_v3.py
Delete Users	delete_bulk_users.py
Create Vault Folders	initialize_vault_folders.py
Delete Vault Folders	delete_vault_folders.py

Security Note: Always ensure venv is active ((venv) appears in terminal) before running scripts to avoid errors.

now make a documentation for guidelines or rules to be strictly followed by normal users, super users and admin here

Here is the formal **Security Policy & Usage Guidelines** document. This outlines the strict rules that every role must follow to maintain the security and integrity of the Sampurna Vault.

You can save this as Vault_Security_Policy.pdf and distribute it to all employees.

4. Summary

Sampurna Vault: Admin Quick Reference Guide

Essential administrative procedures for Daily Maintenance, User Support, and **Bulk Operations** on Sampurna Vault and Keycloak.

DAILY SERVER MANAGEMENT

1. Start of Day: Server Up & Unseal
To bring the system online, you must start the services and manually unseal the Vault.

2. Key Unseal Command
Run `vault operator unseal` three times, each with one of the unique unseal keys.

3. End of Day: Safe Shutdown
Stop the Docker containers first (`docker-compose down`) before shutting down the VM.

COMMON USER SUPPORT (HELPDESK)

Reset a User's Password
In the Keycloak UI, find the user and use the "Reset Password" function under Credentials.

Reset 2FA for a Lost Phone
Delete the user's "OTP" credential, then add the "Configure OTP" required action.

BULK OPERATIONS (TERMINAL SCRIPTS)

⚠ **Step 0: Upload Employee CSV**
Before running any script, you must upload the latest employee CSV file to the server.

Update Admin Token in Scripts
Manually edit Vault-related scripts to insert your current Vault Root Token before running.

Task	Script Name
Create Users	`import_final_v3.py`
Delete Users	`delete_bulk_users.py`
Create Secret Folders	`initialize_vault_folders.py`
Delete Secret Folders	`delete_vault_folders.py`

NotebookLM

Made with 🖤 by the Sampurna IT Team.