Sampurna Vault – Super User Guide

Managing Company-Wide Critical Secrets

1. Role Overview

As a **Super User**, you have elevated access beyond a normal employee.

- **Normal Users** only manage their private folder (mysecret).
- **Super Users (You)** manage the shared **scripts** engine.
- **Responsibility:** You ensure that production keys, database passwords, and automation credentials are safe, updated, and organized.

2. First-Time Setup (Mandatory)

You only need to do this **once**.

Step 1: Access the Vault

1. Open your web browser (Chrome/Edge recommended).
2. Go to the Vault URL: **https://4.187.152.147:8200** *(Note: If you see a "Not Secure" warning because of the self-signed certificate, click* ***Advanced -> Proceed****)*.

Step 2: Login via OIDC

1. On the Vault login screen, look at the **Method** dropdown.
2. Select **OIDC** (Do **not** use Token or LDAP).
3. Click the **Sign in with OIDC Provider** button.

Step 3: Authenticate & Set New Password

1. You will be redirected to the **Sampurna Secure Login** page (Dark Theme).
2. **Username:** Enter your User Name (e.g., Super_User).
3. **Password:** Enter the temporary password provided by IT: **1234**

Step 4: Configure OTP (2FA)

1. After giving your temporary password, you will see a **QR Code** on the screen.
2. Open your **Authenticator App** on your phone.
3. Tap **+** or **Add Account** -> **Scan QR Code**.
4. Scan the code on the screen.
5. Your phone will generate a 6-digit code. Enter that code into the browser.

Step 5: Set New Password and Give your Email

1. **Update Password:** The system will immediately ask you to change your password.
    a. Enter 1234 as the current password.
    b. Enter a **strong new password** (at least 8 characters).
    c. Confirm the new password and submit.
2. Give Your **Email** and submit.

☑ **Success!** You are now logged into Vault

Step 6: Verify Super User Access

1. Once logged in, look at the list of "Secret Engines".
2. You should see a folder named **scripts** (in addition to ssv).
3. Click on **scripts**.
4. If you can enter this folder and see sub-folders (like prod, dev, db), your Super User access is active.

    a. *If you get "Permission Denied", contact the IT Admin immediately.*

3. Managing Company Secrets (Daily Tasks)

How to Add a New Company Secret

Scenario: The DevOps team generated a new API Key for AWS Production.

1. Navigate to **scripts** -> **prod** -> **aws** (or create these folders if missing).
2. Click **+ Create Secret**.
3. **Path:** scripts/prod/aws/billing-api
4. **Secret Data:**
    a. **Key:** access_key | **Value:** AKIA......
    b. **Key:** secret_key | **Value:** Xy7z......
5. Click **Save**.

How to Rotate (Update) a Password

Scenario: The Database password expired and needs updating.

1. Navigate to the existing secret (e.g., scripts/prod/db/sql-master).
2. Click **Create new version** (or Edit).
3. Replace the old value with the **New Password**.
4. Click **Save**.
    a. *Note: Vault keeps a history of old versions in case you need to rollback.*

How to Organize Data (Best Practices)

Do not dump everything in the root folder. Use a hierarchy:

- scripts/prod/ (Production data - Highly Sensitive)
- scripts/uat/ (User Acceptance Testing)
- scripts/dev/ (Development keys)
- scripts/common/ (Shared Wi-Fi passwords, license keys)

4. Emergency Procedures

What if You (Super User) Forget Your Password?

1. You must contact the **IT Admin Team** immediately.
2. Since your account has elevated access, you may be required to re-verify your identity before the reset is processed.

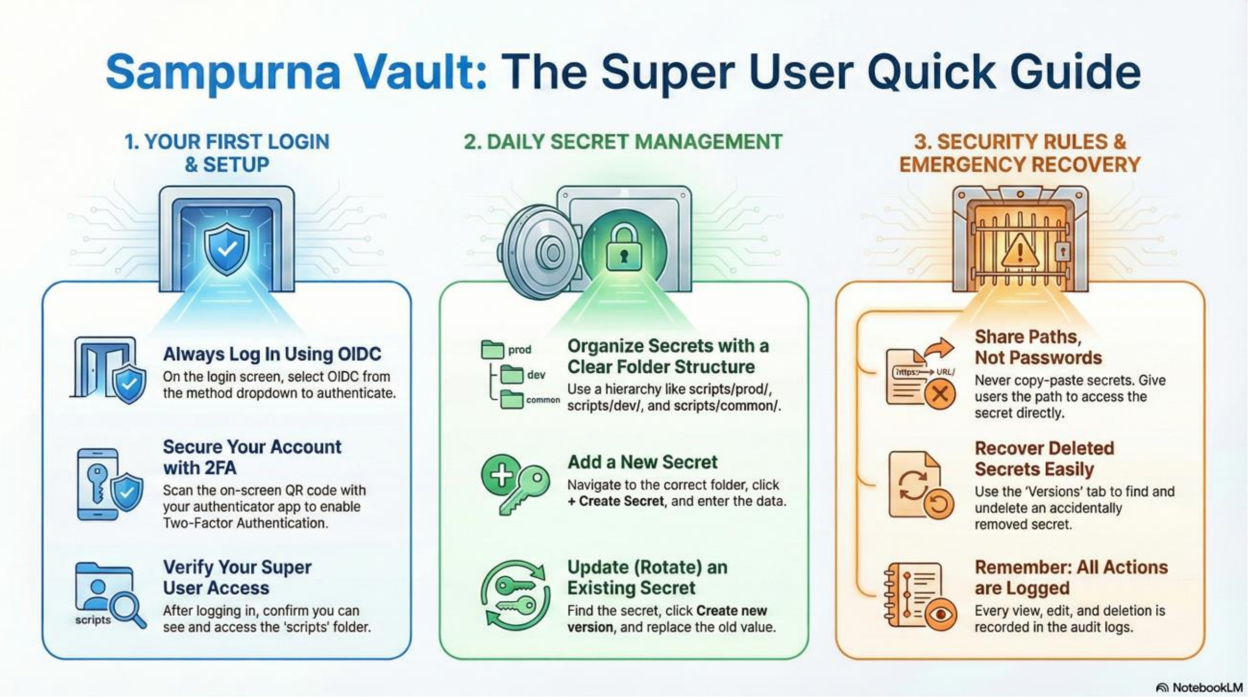
What if a Secret is Accidentally Deleted?

1. Don't panic. Vault (KV v2) supports "Soft Delete."
2. Navigate to the secret path.
3. Click on the **Versions** tab.
4. Locate the deleted version and click **Undelete** or **Rollback**.

5. Security Rules for Super Users

1. **Need-to-Know Basis:** Only share the specific secret path (e.g., scripts/dev/app) with developers, not the actual password text.
2. **No Copy-Pasting:** Do not copy secrets from Vault into Slack, Teams, or WhatsApp.
3. **Audit Logs:** Remember that **every action you take** (view, edit, delete) is logged by the system.

6. Summary



Sampurna Vault: The Super User Quick Guide

1. YOUR FIRST LOGIN & SETUP

Always Log In Using OIDC
On the login screen, select OIDC from the method dropdown to authenticate.

Secure Your Account with 2FA
Scan the on-screen QR code with your authenticator app to enable Two-Factor Authentication.

Verify Your Super User Access
After logging in, confirm you can see and access the 'scripts' folder.

2. DAILY SECRET MANAGEMENT

Organize Secrets with a Clear Folder Structure
Use a hierarchy like scripts/prod/, scripts/dev/, and scripts/common/.

Add a New Secret
Navigate to the correct folder, click **+ Create Secret**, and enter the data.

Update (Rotate) an Existing Secret
Find the secret, click **Create new version**, and replace the old value.

3. SECURITY RULES & EMERGENCY RECOVERY

Share Paths, Not Passwords
Never copy-paste secrets. Give users the path to access the secret directly.

Recover Deleted Secrets Easily
Use the 'Versions' tab to find and undelete an accidentally removed secret.

Remember: All Actions are Logged
Every view, edit, and deletion is recorded in the audit logs.

Made with ❤ by the Sampurna IT Team