IronClad Vault System

User Manual v5.0.0 (Refactored)

Security Protocol: AES-256-GCM + Argon2

November 26, 2025

Abstract

System Overview: IronClad Vault is a zero-trust, secure file storage system designed for high-security environments. It consists of two primary components: the **Vault Server** (which stores encrypted files and the database) and the **Remote Client** (which connects via a secure, encrypted TCP tunnel).

Contents

1 Operating the Vault Server

The server handles all encryption and storage. It can operate in two distinct modes depending on your administrative needs.

1.1 Initialization

1. Run the executable: `vault-server-windows-amd64.exe`.
2. **First Run:** You will be prompted to create an Admin account.
3. **Megakey Generation:** The system will generate a file named `recovery_megakey.bin` (approx. 1MB).

> **CRITICAL WARNING**
> SAVE THIS FILE. If you lose the `recovery_megakey.bin`, the vault is permanently locked and data cannot be recovered.

1.2 Mode 1: Desktop GUI (Local Management)

Use this mode for local administration and maintenance.

- **Usage:** Select "Desktop GUI" from the menu and login with your Username/Password.
- **View/Decrypt:** Access files directly on the server machine.
- **Admin Panel:** Create users, reset passwords, and remove accounts.
- **Import:** Drag files into the window to encrypt them locally immediately.

1.3 Mode 2: Sentinel Server (Remote Access)

This mode opens network ports (TCP 9000) allowing Remote Clients to connect.

1. Select "Sentinel Server" from the main menu.
2. The status will read: *Sentinel ready. Locked.*
3. **Unlock:** Click **Browse**, select your `recovery_megakey.bin`, and click **Unlock & Start Server**.

The Tunnel Key

Once started, the log will display:

```
TCP TUNNEL KEY (COPY THIS): <64-char-hex>
```

Click the "Copy Tunnel Key" button to save it to your clipboard. You must securely transmit this key to Client users.

Security Note: In Sentinel Mode, the Master Key is held in RAM only. If the application is closed or the server reboots, the vault automatically locks.

2 Operating the Remote Client

2.1 Connecting

1. Run the client: `./vault-client-linux-amd64`.

2. **Server Address:** Enter the Windows Server IP + Port 9000 (e.g., `192.168.1.50:9000`).
3. **Session Key:** Paste the 64-character Tunnel Key provided by the Server Admin.
4. Click **Connect** and login with your credentials.

2.2 File Management

The File Browser displays Filename, Size, and Access Level. Sorting and filtering are handled automatically by the server based on your user clearance.

2.2.1 Uploading Files

- **Button:** Click the **+** (Add) icon in the toolbar for single files.
- **Drag & Drop (Recommended):** Drag multiple files or entire folders from your OS file manager onto the Client window. The system will recursively find every file inside.
- **Classification:** You must choose a classification: Public, Internal, Secret, or Top Secret.

2.2.2 Downloading Files

- **Single File:** Click a file $\rightarrow$ Select "Download to Folder".
- **Batch Download:** Check the box next to multiple files, click the Download Icon, and select a destination. Files are decrypted and saved sequentially.

3 Administrative Features

The Admin Panel is available in both the Server (Desktop Mode) and Client (if logged in as Admin).

- **Create User:** Define username, password, and Role (Admin/Viewer).
- **Edit User:** Change Access Levels (e.g., promote a user to see "Top Secret" files).
- **Reset Password:** Force a password reset for a user.
- **Delete User:** Permanently remove access.
- **Secure Delete (File):** Admins can permanently scrub a file. This overwrites data with random noise before deletion.

4 Access Levels

IronClad uses a strict hierarchical security model. Users can only see files with an Access Level less than or equal to their own level.

5 Troubleshooting

Q: Client says "Connection Aborted" or "Target machine actively refused it".

Level	Classification	Scope & Description
01	PUBLIC	**Global Visibility.** Visible to everyone, including unauthenticated guests. No sensitive info.
05	INTERNAL	**Organization-wide.** (Default) Standard business documents, memos, and policies. Accessible to all active employees.
07	SECRET	**Restricted Access.** Sensitive operational data, financial drafts, and client lists. Requires Tier 2 Clearance.
10	TOP SECRET	**Executive Eyes Only.** Highest classification. Trade secrets, executive minutes, and critical infrastructure keys.

Table 1: Security Classification Hierarchy

A: Check the Windows Firewall. Ensure ports **9000 (TCP)** and **8443 (HTTPS)** are allowed in Inbound Rules. Additionally, verify that the Server is running specifically in *Sentinel Mode* and has been unlocked.