IronBench Access Manager provides:

- Audit Log of Disk Encryption History
- Automatic Encryption Key Rotation
- Remote Disk Wipe Capability
- Password Reset Self-Service
- Client Inventory
- Client Monitoring Alerts

Contact IronBench
sales@ironbench.io

IRONBENCH

Access Manager

The best way to manage secure access to Linux machines.

IRONBENCH Access Manager

Common Challenges with Linux Security Management

- Unable to ensure disk encryption for a computer that is lost or stolen.
- No way to remotely wipe a disk in a computer that is lost or stolen.
- Unable to automatically rotate encryption keys.
- No way to access an encrypted drive if the password is forgotten.

IronBench Access Manager is the best way to enforce information security policy and ensure your Linux machines are protected throughout the enterprise.

Why Access Manager?

Access Manager is the only security management tool that provides the ability to control secured access to Linux machines. Without Access Manager your Linux machines make your enterprise look like the wild west.

How does IronBench Access Manager work?

1. Clients install a small app from a secure download site.
2. Run the client app to register.
3. Administrators manage inventory and service via the web.
4. Disks are secured and solidly encrypted.