BackTrack Quick Start Guide

Contents

BackTrack Quick Start Guide

□ New in v0.2.0: Auto-Generated Database Key!

BackTrack now uses an **auto-generated encryption key** instead of requiring a password on every launch. This provides **better security** and **better usability**!

Security Layers

You still have multiple layers of security: 1. **OS Login** - Your computer password/biometric 2. **Database Encryption** - Auto-generated 384-bit key 3. **Application Login** - Your username and password 4. **MFA (Optional)** - Two-factor authentication

Login is now simple: Just username + password (no database password entry!)

First Time Setup

1. Install and Launch

After building the application, launch BackTrack. You'll see the login screen.

2. Initial Setup

1. Click **"Initial Setup"**
2. Fill in the setup form:
   - **Full Name**: Your name (e.g., "Dr. Jane Smith")
   - **Admin Username**: Your login username (e.g., "admin" or "jsmith")
   - **Admin Password**: Your login password
   - **Confirm Password**: Re-enter your login password
   - **Office Location Name**: Your practice name (e.g., "Downtown Chiropractic")
3. Click **"Create"**
4. **CRITICAL**: You'll see TWO important codes:
   - **Database Encryption Key** - Click "Copy Database Key" and save in password manager
   - **Support Code** - Click "Copy Support Code" and save in password manager
5. Click **"Continue to Login"**

Why save these? - **Database Key**: Needed if you move to a new computer or lose the database - **Support Code**: Allows password recovery and emergency access

3. First Login

Simple! Just two fields:

1. Enter your **Username** (from step 2) □ Your account name
2. Enter your **Password** (from step 2) □ Your account password
3. Click **"Login"**

Example: - Username: `drsmith` - Password: `DrSmith123!`

No database password needed! The application automatically unlocks the database using the stored key.

Daily Workflow

Adding a Patient

1. Click **"Patients"** in the left menu
2. Click **"Add New Patient"**
3. Fill in patient information:
    - Required: First Name, Last Name, Date of Birth (YYYY-MM-DD format)
    - Recommended: Phone, Email, Address
    - Important: Medical History, Allergies, Current Medications
    - Emergency Contact information
4. Click **"Save"**

Scheduling an Appointment

1. Click **"Appointments"** in the left menu
2. Select the date (defaults to today)
3. Click **"Schedule Appointment"**
4. Enter:
    - Patient ID (or use Search Patient)
    - Date (YYYY-MM-DD)
    - Time (HH:MM in 24-hour format, e.g., 14:30 for 2:30 PM)
    - Duration (select from dropdown)
    - Reason for visit
    - Any notes
5. Click **"Save"**

Creating Clinical Notes

1. Click **"Clinical Notes"** in the left menu
2. Enter the Patient ID (or use Search Patient)
3. Click **"Load Patient Notes"** to see existing notes
4. Click **"Add Clinical Note"**
5. Fill in the SOAP note:
    - **Chief Complaint**: Main reason for visit
    - **Subjective**: What the patient tells you (symptoms, pain description)
    - **Objective**: What you observe (posture, range of motion, test results)

- **Assessment**: Your diagnosis or clinical impression
    - **Plan**: Treatment performed and plan for next visit
    - **Follow-up**: Instructions for patient
6. Optionally link to an appointment by entering Appointment ID
7. Click **"Save"**

Common Tasks

Searching for a Patient

1. Go to **"Patients"**
2. Type patient name in the search box
3. Click on patient to view details

Viewing Patient History

1. Find the patient in **"Patients"**
2. Click **"View"**
3. Click **"View Appointments"** or **"View Clinical Notes"**

Managing Users (Admin Only)

1. Go to **"Settings"**
2. Click **"Manage Users"**
3. Click **"Add User"** to create new staff accounts
4. Assign roles:
    - **Admin**: Full access
    - **Doctor**: Can see/edit all clinical data
    - **Staff**: Can manage appointments and patient demographics

Changing Your Password

1. Go to **"Settings"**
2. Click **"Change My Password"**
3. Enter current password
4. Enter new password twice
5. Click **"Change"**

Multi-Computer Setup (Optional)

If you have multiple computers in your office:

On the Primary Computer:

1. Go to **"Settings"**
2. Check **"Enable Database Sync"**
3. Note the Sync Port (default: 8765)
4. Note the computer's IP address (e.g., 192.168.1.100)

On Secondary Computers:

1. Go to **"Settings"**
2. In the peer address field, enter: `PRIMARY_IP:8765` (e.g., `192.168.1.100:8765`)
3. Click **"Add Sync Peer"**
4. Click **"Request Sync from Peer"**
5. Select the peer
6. Enter the sync password (same as database password)
7. Click **"Sync"**

Note: The database will be backed up automatically before sync.

Security Best Practices

Passwords

- Use strong, unique passwords for database and user accounts
- Don't share passwords between users
- Change passwords if a user leaves

Support Code

- Store the support code in a secure location
- This is the ONLY way to recover from a forgotten password
- Never share it with patients or unauthorized persons

Physical Security

- Lock your computer when stepping away
- Enable auto-lock timeout in Settings (default: 15 minutes)
- Keep database backups in a secure location

Data Backup

- Regularly backup the database file:
  - **macOS**: `~/Library/Application Support/BackTrack/data/backtrack.db`
  - **Linux**: `~/.local/share/backtrack/backtrack.db`
  - **Windows**: `%LOCALAPPDATA%\BackTrack\data\backtrack.db`
- Store backups on encrypted external drives or secure cloud storage
- Test restore procedure periodically

Troubleshooting

Most Common Issue: "Authentication failed"

This usually means you're confusing the two passwords!

□ **Correct order:** 1. Database Password (unlocks the database) 2. Username 3. User Password (logs you into your account)

□ **Common mistakes:** - Entering user password in database password field - Entering database password in user password field - Forgetting you have TWO different passwords

Other Issues

See **TROUBLESHOOTING.md** for detailed help with: - “Failed to open database” - “SQL scan error” - Support code issues - Database reset procedures - And much more!

Can’t find a patient

- Check spelling of name
- Try searching by last name only
- Check if patient was archived (click “Show Archived”)

Sync isn’t working

- Verify both computers are on same network
- Check firewall isn’t blocking the sync port
- Ensure sync password is the same on both computers
- Try pinging the primary computer

Tips & Tricks

Fast Patient Lookup

- Search by last name for faster results
- Patient ID is shown in the patient list - note it for future reference

Appointment Status

- Mark appointments as “completed” after the visit
- Use “no-show” for patients who don’t arrive
- “cancelled” appointments remain in the system for records

Clinical Notes

- Link notes to appointments for better organization
- Use consistent abbreviations for efficiency
- Fill in all SOAP sections for complete documentation

Keyboard Shortcuts

- Tab: Move between fields
- Enter: Activate buttons in dialogs
- Esc: Close dialogs (in most cases)

Getting Help

Forgot Database Password?

NEW FEATURE: Password Recovery!

If you forget your database password: 1. Click **"Forgot Database Password?"** on login screen 2. Enter your support code 3. Choose a new database password 4. All your data is preserved! 5. Login with the new password

Support Login

If you forget your USER password or need emergency access:

Option A: Support Authenticator (Recommended) 1. Click **"Support Login"** on login screen 2. Enter the 6-digit code from your authenticator app 3. You'll be logged in with full admin access 4. Go to Settings □ Manage Users to reset passwords

Option B: Legacy Support Code 1. Click **"Support Login"** on login screen 2. Enter the support code from initial setup 3. You'll be logged in with full admin access 4. Go to Settings □ Manage Users to reset passwords

For Support Staff: See `SUPPORT_AUTHENTICATOR_GUIDE.md` for one-time authenticator setup.

Technical Support

- Check the README.md for detailed documentation
- Review audit logs in Settings for system activities
- Contact your IT administrator or software maintainer

Regulatory Compliance

HIPAA Considerations (US)

- Database is encrypted at rest □
- Audit logs track all access □
- User authentication required □
- Ensure physical security of computer
- Conduct regular backups
- Have a breach response plan

Data Privacy

- Only authorized staff should have user accounts
- Log out when leaving the workstation
- Don't share login credentials
- Review audit logs periodically
- Archive inactive patient records

Questions? Refer to the main README.md for comprehensive documentation.

Remember: Always keep your database password and support code secure!