User Password Fix Summary

Issue Description

When creating a user in the “Manage Users” section, administrators could enter a password for the new user. However, this password was not being used by the backend. Instead, the backend was generating a random password that nobody knew, making it impossible for the user to log in with the password set during creation.

Root Cause

1. **Frontend (`components/modals/user-modal.tsx`)**: The modal collected a password from the admin but did not send it to the backend API.
2. **Backend (`server/api/routers/user.ts`)**: The `create` mutation did not accept a password parameter and always generated a random password using `generateRandomPassword(12)`.

This disconnect meant that:
- The admin thought they were setting a password
- The backend ignored any input and created its own random password
- The random password was never communicated to anyone
- Users could not log in with the password the admin thought they had set

Solution Implemented

Backend Changes (`server/api/routers/user.ts`)

1. **Added password parameter to input schema**:
   - Made `password` an optional parameter with minimum 6 characters
   - `password: z.string().min(6).optional()`

2. **Updated password handling logic**:
   - If a password is provided, use it (after hashing with bcrypt)
   - If no password is provided, generate a random one as before
   - Code: `const passwordToUse = input.password || generateRandomPassword(12);`

3. **Conditional password reset token creation**:
   - Only create a password reset token if no password was provided
   - This maintains the original “setup link” workflow for auto-generated passwords
   - When a password is provided, no setup link is needed

4. **Updated audit logs**:
   - Different messages for password-provided vs auto-generated scenarios
   - “Created user X with provided password” vs “Created user X.”

Frontend Changes (`components/modals/user-modal.tsx`)

1. **Updated mutation call**:
   - Added `password: formData.password || undefined` to the createMutation call
   - This sends the password to the backend if provided

2. **Improved UX**:
   - Changed label from “Password *” (required) to “Password (Optional)”
   - Added helper text: “If left empty, a random password will be generated and a setup link will be created.”
   - This clarifies the behavior to admins

How It Works Now

Scenario 1: Admin provides a password

1. Admin fills in name, email, password, and role
2. Frontend sends all data including password to backend
3. Backend hashes the provided password with bcrypt
4. User is created with the hashed password
5. User can immediately log in with the password the admin set
6. No password reset token is created
7. Audit log says “Created user X with provided password”

Scenario 2: Admin leaves password empty

1. Admin fills in name, email, and role (password field left empty)
2. Frontend sends data without password to backend
3. Backend generates a random 12-character password
4. Backend creates a password reset token
5. Backend creates a setup URL for the user
6. Audit log includes the setup URL
7. Admin should send this URL to the user (via email or other means)

Benefits

- **Fixed the reported issue**: Passwords provided during user creation now work
- **Maintained backward compatibility**: Auto-generation still works if no password is provided
- **Better UX**: Clear indication that password is optional
- **Flexible workflow**: Supports both immediate password setting and email-based setup

Files Modified

1. `server/api/routers/user.ts` - Backend user creation logic
2. `components/modals/user-modal.tsx` - Frontend user creation modal

Testing Recommendations

1. **Test with password**: Create a user with a password and verify they can log in
2. **Test without password**: Create a user without a password and verify the setup link is created
3. **Test password validation**: Try to create a user with a password shorter than 6 characters
4. **Test edge cases**: Empty string password, very long password, special characters

Additional Notes

- The `mustChangePassword` flag is still set to `true` for all new users, so even users created with a password will be prompted to change it on first login (as mentioned by the user)
- Password hashing uses bcrypt with 10 salt rounds for security
- The minimum password length is 6 characters (could be increased for better security if needed)

Date: November 16, 2025
Status: ✅ Completed and ready for testing