### ✅ 1. ****Users Table****

| **Column Name** | **Data Type** | **Required** | **Why It's Important** |
| --- | --- | --- | --- |
| Id | GUID / INT | ✅ Yes | Primary key, unique user identifier |
| Email | VARCHAR(255) | ✅ Yes | Unique user login, main communication method |
| PhoneNumber | VARCHAR(20) | ⛔ Optional | Useful for SMS login or MFA |
| UserName | VARCHAR(100) | ⛔ Optional | Public-facing identity (not used for login usually) |
| PasswordHash | TEXT | ✅ Yes | Securely stores encrypted password |
| Salt | TEXT | ✅ Yes | Used with hash to enhance password security |
| IsEmailVerified | BOOLEAN | ✅ Yes | Prevents unauthorized access before email confirmation |
| EmailVerificationToken | VARCHAR(100) | ⛔ Optional | For email verification link |
| ResetPasswordToken | VARCHAR(100) | ⛔ Optional | For secure password reset link |
| ResetTokenExpiry | DATETIME | ⛔ Optional | Limits reset token validity |
| CreatedAt | DATETIME | ✅ Yes | Audit trail of account creation |
| UpdatedAt | DATETIME | ✅ Yes | Tracks changes (e.g., password updates) |
| IsActive | BOOLEAN | ✅ Yes | Controls user access (banned/inactive users) |
| Role | VARCHAR(50) | ✅ Yes | Assigns roles like "User", "Admin", "Support" |

### ✅ 2. ****Login History Table**** (optional but recommended)

| **Column Name** | **Data Type** | **Why It's Important** |
| --- | --- | --- |
| LoginId | GUID / INT | Primary key |
| UserId | FK to Users | Link to user |
| LoginTime | DATETIME | Security and activity tracking |
| IpAddress | VARCHAR(100) | For geo/audit/security |
| DeviceInfo | TEXT | Track suspicious logins or multi-device usage |

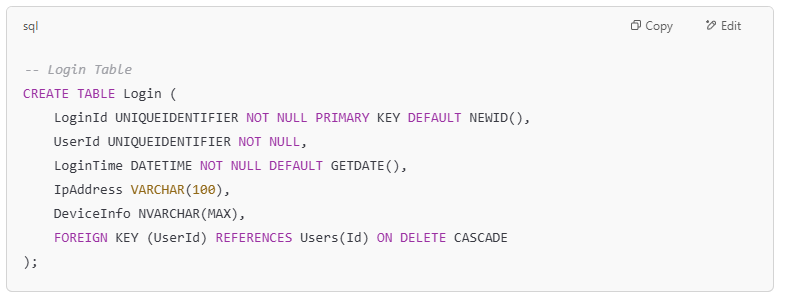
### ✅ 3. ****Tokens Table**** (for JWT or session tokens)

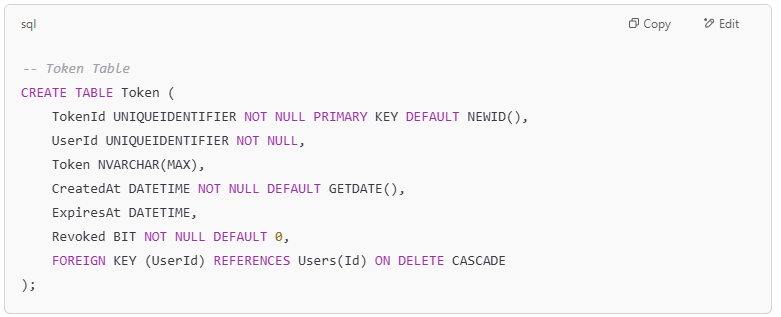
| **Column Name** | **Data Type** | **Why It's Important** |
| --- | --- | --- |
| TokenId | GUID | Unique token ID |
| UserId | FK to Users | Who the token belongs to |
| Token | TEXT | JWT or refresh token |
| CreatedAt | DATETIME | Token tracking |
| ExpiresAt | DATETIME | Token expiration |
| Revoked | BOOLEAN | Token revocation (logout or force expiry) |

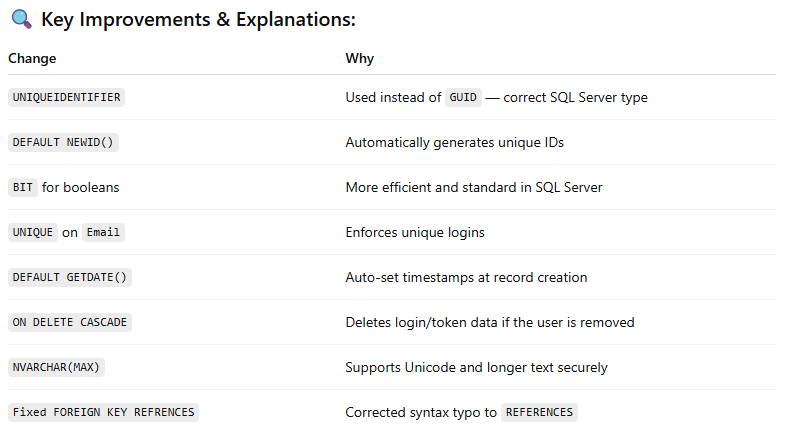
### 🔐 Best Practices

* Store PasswordHash using **bcrypt** or **PBKDF2** (never plain text).
* Use **GUIDs** or **ULIDs** for user IDs for better security across systems.
* Validate and sanitize email/phone inputs to avoid injection attacks.
* Enable **MFA (multi-factor auth)** if you want extra security.

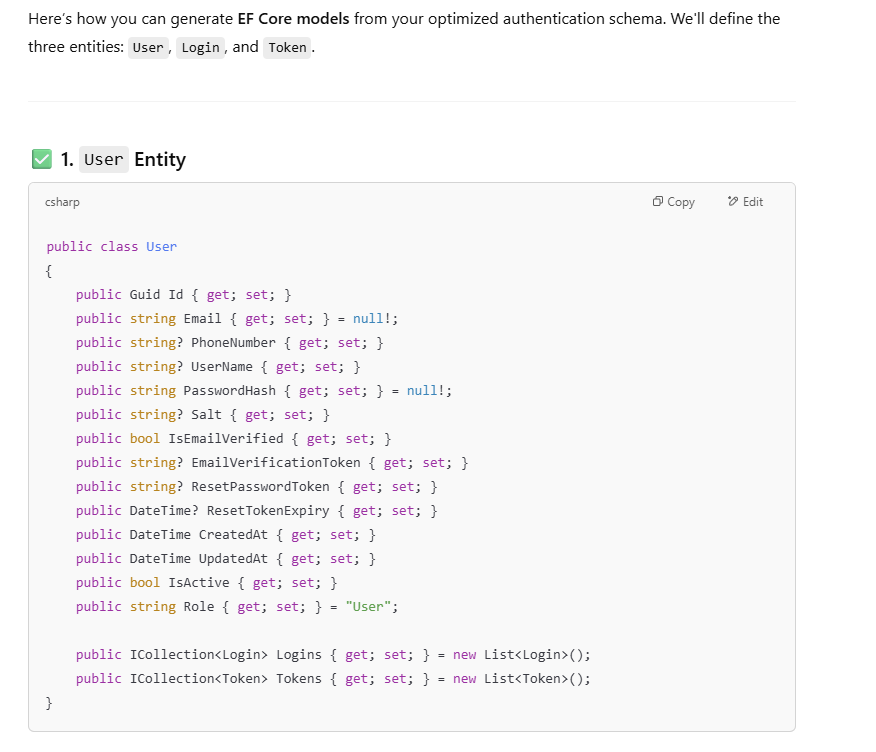
****

****

****

****

****

****

****

****

****

****