SQL Server 2014 SP3

创建一个受限用户账号

在 **SQL Server 2014 SP3** 中，你可以通过以下步骤创建一个受限用户账号，使其：

- □□□□□□□□□□□ `SZHW`）
- □□□□□□□□ `SZCIS`）进行 **SELECT / INSERT / UPDATE**
- □□ **DELETE** 数据
- □□□□□□□□□□□□□□□

□ □□□□□□ SSMS 或 T-SQL）

□□ □□ 1：创建登录名（ Login）

```
-- 创建 SQL Server 登录名（服务器级别）
CREATE LOGIN [limited_user] WITH PASSWORD = 'StrongPassword123!';
```

> □□ 建议密码符合复杂性要求。

□□ □□ 2：在目标数据库中创建用户（ User）

```
USE [SZHW];  -- 切换到你的数据库


-- 将登录名映射为数据库用户
CREATE USER [limited_user] FOR LOGIN [limited_user];
```

□□ □□ 3：授予 SELECT, INSERT, UPDATE 权限（仅限指定表）

```
-- 授予对 SZCIS 表的读写权限（不含 DELETE）
GRANT SELECT, INSERT, UPDATE ON OBJECT::dbo.SZCIS TO [limited_user];
```

> ⚠ 注意：`OBJECT::dbo.SZCIS` 是完整对象引用格式。

□□ □□ 4：显式拒绝 DELETE 权限（防止意外继承）

```
-- 明确禁止删除操作
DENY DELETE ON OBJECT::dbo.SZCIS TO [limited_user];
```

> □ `DENY` 优先级高于 `GRANT`，即使以后加入角色也不会有 DELETE 权限。

□□ □□ 5：（可选）限制不能访问其他表

默认情况下，新用户 没有任何权限 ，所以只要不授予权限，就无法访问其他表。

但为了更安全，可以：

方法 A：不将用户加入任何角色（推荐）

- 不要加入 `db_datareader`、`db_datawriter` 等内置角色
- 只按需授权特定表

方法 B：显式拒绝所有其他表（不必要，但更严格）

```
-- 拒绝访问其他表（示例）
DENY SELECT, INSERT, UPDATE, DELETE ON OBJECT::dbo.OtherTable TO [limited_user];
```

□□ □□　6：测试权限

用新账号连接后执行：

□ □□□□□□

```
SELECT * FROM dbo.SZCIS;
INSERT INTO dbo.SZCIS (Part_Number, Description) VALUES ('TEST001', 'Test Part');
UPDATE dbo.SZCIS SET Description = 'Updated' WHERE Part_Number = 'TEST001';
```

□ □□□□□□□

```
DELETE FROM dbo.SZCIS WHERE Part_Number = 'TEST001';  -- 报错：权限被拒绝
SELECT * FROM dbo.OtherTable;  -- 报错：对象无权限
```

□□ □□□□□

建议	说明
不要使用 **sa** 账号做应用连接	应使用最小权限账号
密码定期更换	使用强密码策略
限制 **IP** 访问（网络层）	在防火墙或 SQL Server 配置中限制来源 IP
启用登录审计	监控异常登录行为

□□ □□□□□□□□□□

只需重复 `GRANT` 和 `DENY`：

```
-- 授权多张表
GRANT SELECT, INSERT, UPDATE ON OBJECT::dbo.Table1 TO [limited_user];
GRANT SELECT, INSERT, UPDATE ON OBJECT::dbo.Table2 TO [limited_user];

-- 拒绝删除
DENY DELETE ON OBJECT::dbo.Table1 TO [limited_user];
DENY DELETE ON OBJECT::dbo.Table2 TO [limited_user];
```

□□ 总结命令（一键复制）

```
-- 1. 创建登录名
CREATE LOGIN [limited_user] WITH PASSWORD = 'YourSecurePassword!';

-- 2. 在数据库中创建用户
USE [SZHW];
CREATE USER [limited_user] FOR LOGIN [limited_user];

-- 3. 授予指定表的读写权限（不含删除）
GRANT SELECT, INSERT, UPDATE ON OBJECT::dbo.SZCIS TO [limited_user];

-- 4. 显式拒绝删除权限
DENY DELETE ON OBJECT::dbo.SZCIS TO [limited_user];
```

> “□ □□□□□□□□□□□□ `SZCIS` 表进行增、改、查，不能删，也不能访问其他表。

□□□□

Q：能否只允许修改某些字段？

A：SQL Server 不支持列级 UPDATE 权限（除 `VIEW` 外）。

□ □□□□□□□□□ 视图（ **View**），只包含可编辑字段，并在视图上授权。

Q：用户能执行存储过程吗？

A：默认不能。如需调用，需单独授权：

```
GRANT EXECUTE ON dbo.YourProc TO [limited_user];
```

如有需要，我也可以帮你生成 只读账号 或 基于视图的受限账号 。欢迎继续提问！

Revision #1
Created 2026-01-27 08:04:56 UTC by Admin
Updated 2026-01-27 08:05:19 UTC by Admin